Perú (Peru): Digital Certificate Services Providers Official Register (ROPS)

Scheme name (es)

PE:Registro Oficial de Prestadores de Servicios de Certificación Digital bajo la Infraestructura Oficial de Firma Electrónica de acuerdo a la LEY N° 27269

Scheme name (en)

PE:Digital Certificate Services Providers Official register under the Official Framework Electronic Signatures in compliance with law N° 27269

Legal Notice (es)

El marco legal aplicado a la presente implementación del ROPS es la Ley N°27269, Ley de Firmas y Certificados Digitales y su Reglamento, aprobado por el Decreto Supremo 052-2008-PCM y modificado por el Decreto Supremo 070-2011-PCM, y las Guias de Acreditacion.

Legal Notice (en)

The applicable legal framework for the present ROPS implementation of the Trusted List is the law N°27269, law of Digital Signatures and Certificates and its Regulations (Supreme Decree 052-2008) and ammended by Supreme Decree 070-2011-PCM, and the Accreditation Guidelines.

Scheme territory	PE
Scheme status determination approach	appropriate
Issue date	2020-12-18T17:16:37.026Z
Next update	2021-06-18T12:16:37.026Z
Historical information period	3653 days
Sequence number	25
Scheme information URIs	http://www.iofe.gob.pe/ http://www.iofe.gob.pe/en/

Scheme Operator

Scheme operator name (es)	INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL - INDECOPI
Scheme operator name (en)	NATIONAL INSTITUTE FOR THE DEFENSE OF COMPETITION AND PROTECTION OF INTELLECTUAL PROPERTY
Scheme operator street address (es)	CALLE DE LA PROSA 104
Scheme operator street address (en)	CALLE DE LA PROSA 104
Scheme operator postal code (es)	LIMA 41
Scheme operator postal code (en)	LIMA 41
Scheme operator locality (es)	SAN BORJA
Scheme operator locality (en)	SAN BORJA
Scheme operator state (es)	LIMA
Scheme operator state (en)	LIMA

Scheme operator country (es)	PE
Scheme operator country (en)	PE
Scheme operator contact	http://iofe.indecopi.gob.pe mailto:iofe_sgaac@indecopi.gob.pe

Certificate Service Providers (PSC's)

Certificate Service Provider Name (en): REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Trade name (en)	RENIEC
Information URI (en)	HTTP://WWW.RENIEC.GOB.PE
Service provider street address (es)	AV. BOLIVIA 144 TORRE CENTRO CIVICO
Service provider street address (en)	AV. BOLIVIA 144 TORRE CENTRO CIVICO
Service provider postal code (es)	LIMA01
Service provider postal code (en)	LIMA01
Service provider locality (es)	LIMA
Service provider locality (en)	LIMA
Service provider state (es)	LIMA
Service provider state (en)	LIMA
Service provider country (es)	PE
Service provider country (en)	PE

SERIALNUMBER=RUC: 20295613620, CN=RENIEC Class III CA, OU=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE

Type	CA/QC
Status	undersupervision
Status starting time	2012-01-19T18:22:13.000Z

Service digital identity (X509)

Version	3
Serial number	428615119675287220864505477247851118594377606493
Signature algorithm	SHA1withRSA
Issuer	CN=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
Valid from	Wed Jul 21 17:45:32 PET 2010
Valid to	Sat Jul 18 17:45:32 PET 2020
Subject	SERIALNUMBER=RUC: 20295613620, CN=RENIEC Class III CA, OU=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE

Public key	Sun RSA public key, 4096 bits modulus: 818402506075299239463137630989807843339008791545788087277140836803578436434587954876744520028256637871114894076891740735863345313914039156950060325202769070793156152265318017726603636565466561561392504755777764233549677487008789726782222565969322892773845949748410869466659466121858426633495551234261103793969932988890267120012102503730271361313052618060292457067600325046187572471020460481743913815400714652320432989584053225913040351808881649367056581136514493170625711679536878317462890883150873980106088055421787864008776260691768207812606454789908259572628106678707147583293511558870985976005678239855264329440453308656031297543925243682249519974613774764012972314912458163979156972705451310085375220657750980525344887987476471861625676379700334214935190864999761068022388371331128783382446028627817476539238656290857727053172472366379507282528257652597515411540033515199926327389348387601247656450377361985453739096645050501016672467214822287254588927498118002145648325631136041386160143204190580039823166150077709321919645847886295651456658899699330349380851739096645050501016672467214822287254588927498118002145648325631136041386160143204190580039823166150077709321919645847886295651456658899699330349380837091845043922288645794806074792931564212551488935522668876882537857607789377576371612227696365160433698038589016721910739047516681631239758108557448732126471426151376087 9
public exponent: 65537
Subject key identifier	096ed2d93fd5c84ebb1c69e04e2ac864fb41f3fd
CRL distribution points	http://crl.reniec.gob.pe/arl/caservices01.crl
Authority key identifier	041830168014b232d021aa7affbf7eaa0b13e6bff3b527dc0323
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	464c4d1b124d87c6cdcd8531418557773245a814
SHA256 Thumbprint	6a74208eb9491508e2fa445259476f2296c45ad4d221e29299404e26a90031d7

The decoded certificate:

```
[
[
 Version: V3
 Subject: SERIALNUMBER=RUC: 20295613620, CN=RENIEC Class III CA, OU=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 4096 bits
 modulus:
818402506075299239463137630989807843339008791545788087277140836803578436434587954876744520028256637871114894076891740735863345313914039156950060325202769070793156152265318017726603636565466561561392504755777764233549677487008789726782222565969322892773845949748410869466659466121858426633495551234261103793969932988890267120012102503730271361313052618060292457067600325046187572471020460481743913815400714652320432989584053225913040351808881649367056581136514493170625711679536878317462890883150873980106088055421787864008776260691768207812606454789908259572628106678707147583293511558870985976005678239855264329440453308656031297543925243682249519974613774764012972314912458163979156972705451310085375220657750980525344887987476471861625676379700334214935190864999761068022388371331128783382446028627817476539238656290857727053172472366379507282528257652597515411540033515199926327389348387601247656450377361985453739096645050501016672467214822287254588927498118002145648325631136041386160143204190580039823166150077709321919645847886295651456658899699330349380837091845043922288645794806074792931564212551488935522668876882537857607789377576371612227696365160433698038589016721910739047516681631239758108557448732126471426151376087 9
 public exponent: 65537
 Validity: [From: Wed Jul 21 17:45:32 PET 2010,
             To: Sat Jul 18 17:45:32 PET 2020]
 Issuer: CN=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
 SerialNumber: [    4b13c445 a3676f89 cc037a45 67234567 1237655d]

Certificate Extensions: 5
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 09 6E D2 D9 3F D5 C8 4E   BB 1C 69 E0 4E 2A C8 64  .n..?..N..i.N*.d
0010: FB 41 F3 FD                                        .A..
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: B2 32 D0 21 AA 7A FF BF   7E AA 0B 13 E6 BF F3 B5  .2.!.z..........
0010: 27 DC 03 23                                        '..#
]

]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.reniec.gob.pe/arl/caservices01.crl]
]]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 23 68 74 74 70 3A 2F   2F 77 77 77 2E 72 65 6E  .#http://www.ren
```

```
0010: 69 65 63 2E 67 6F 62 2E   70 65 2F 72 65 70 6F 73  iec.gob.pe/repos
0020: 69 74 6F 72 79                                     itory

]]  ]
]

[5]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: 0D 24 5D DD 8B BF F5 81   FE FB 6C 0E AD 56 1B 07  .$].......l..V..
0010: 99 1A D8 1F CE 36 02 83   0B D6 C1 4F 44 3C 12 40  .....6.....OD<.@
0020: 71 5B 9C B6 B9 36 91 4D   28 E1 D2 65 DA 8B 8A F5  q[...6.M(..e....
0030: F2 11 B1 BF 07 60 E3 24   C6 A3 78 91 0E 0B 61 2E  .....`.$..x...a.
0040: E2 02 88 62 FB 7E 08 1A   DB E8 80 AB 03 A4 08 17  ...b............
0050: EF AB AD 81 FA 67 28 AD   0B 08 4F 55 6F 42 1A FF  .....g(...OUoB..
0060: 3E 8D CC B5 A3 0F D6 29   C6 EB EB FB 3C 68 33 D0  >......)....<h3.
0070: 79 98 20 D1 5A 31 8B 74   3F 53 5D 41 D8 96 13 C6  y. .Z1.t?S]A....
0080: 5F 1E 6D 05 EA 22 A4 81   94 38 61 69 2C 5B 70 B1  _.m.."...8ai,[p.
0090: A4 F0 7B 8F 6F F6 8C 72   7E F8 30 81 7B 0F D7 7D  ....o..r..0.....
00A0: 7A 3B 56 37 E0 78 A6 CA   57 96 D6 1D 73 81 3A 39  z;V7.x..W...s.:9
00B0: B6 68 45 61 B7 F1 7D B0   E5 2F 9F 36 10 F8 12 A0  .hEa.....}./.6....
00C0: A8 C5 45 20 AB 5C 92 B3   86 C8 0C DA 9C FC 15 03  ..E .\..........
00D0: 56 73 29 CD E3 B5 6D E4   E2 7E 2E 4A A1 44 A5 B4  Vs)...m....J.D..
00E0: 24 20 9C BD D0 93 71 30   50 E1 72 44 8A 38 A5 D6  $ ....q0P.rD.8..
00F0: 83 D0 D0 C9 BD 25 BF 50   04 C2 D6 1F B4 0B B0 A7  .....%.P........
0100: D8 37 78 6B 84 8C C5 9B   DF A1 4B 30 61 03 F8 E0  .7xk......K0a...
0110: C7 C6 D3 C1 F6 1C B7 6E   77 D5 FA 3A B0 BF BD 58  .......nw..:...X
0120: 34 6D 82 DF E6 E7 B8 41   12 8A E7 27 FC 2B 14 F1  4m.....A...'.+..
0130: 3F A3 7A BE 8C 0C B1 04   5C DB 19 A3 D7 5A 8F F3  ?.z.....\....Z..
0140: 10 32 1F E6 7D 65 7D C1   0B A4 1D 5D E0 B2 0C BD  .2...e.....]....
0150: 32 DD 9F F8 12 96 4A F0   84 73 98 8F 03 8E C4 34  2.....J..s.....4
0160: DC C3 C9 2D 50 59 5D 35   E6 8D 21 3D 8E 45 50 01  ...-PY]5..!=.EP.
0170: 42 B2 78 03 2F 06 36 37   AF E1 EB F7 4B CE 03 D3  B.x./.67....K...
0180: A7 0F DA 92 8C 46 87 39   6E 6F A0 77 89 92 42 59  .....F.9no.w..BY
0190: AB C0 76 7D 1A 07 34 28   20 6D B5 3D 14 4E 6A C1  ..v...4( m.=.Nj.
01A0: 1A 93 7D 44 5E 8A AC 68   A1 EA FD 66 18 3E 18 5A  ...D^..h...f.>.Z
01B0: 4B A4 A9 B5 08 5E 9D D5   68 B6 E0 40 19 E2 5E F8  K....^..h..@..^.
01C0: 57 8B A1 2B 3F 9C 22 EC   C5 67 D0 FB 14 F1 AF AA  W..+?."..g......
01D0: EB CA 06 CA 9D 94 49 B8   BD 45 01 13 2D 98 DF 5C  ......I..E..-..\
01E0: 04 E7 A0 A6 F1 95 35 A0   EA 0F 95 FE 48 23 4E DD  ......5.....H#N.
01F0: 6E 55 3B 00 82 82 1B 23   F3 6D C4 E4 CF 7C 36 66  nU;....#.m....6f

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGizCCBHOgAwIBAgIUSxPERaNnb4nMA3pFZyNFZxI3ZV0wDQYJKoZIhvcNAQEF
BQAwdDELMAkGA1UEBhMCUEUxPDA6BgNVBAoMM1JlZ2lzdHJvIE5hY2lvbmFsIGRl
IElkZW50aWZpY2FjacOzbiB5IEVzdGFkbyBDaXZpbDEnMCUGA1UEAwweUkVOSUVD
IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MB4XDTEwMDcyMTIyNDUzMloXDTIwMDcx
ODIyNDUzMlowga0xCzAJBgNVBAYTAlBFMTwwOgYDVQQKDDNSZWdpc3RybyBOYWNp
b25hbCBkZSBJZGVudGlmaWNhY2nDs24geSBFc3RhZG8gQ2l2aWwxJzAlBgNVBAsM
HlJFTklFQyBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTEcMBoGA1UEAwwTUkVOSUVD
IENsYXNzIElJSSBDQTEZMBcGA1UEBQwQUlVDOiAyMDI5NTYxMzYyMDCCAiIwDQYJ
KoZIhvcNAQEBBQADggIPADCCAgoCggIBAMibOcId5htddebM/cc+X7b4M2F1IyzO
1m1dD8uk3vzgsiU4jAUQCAgqZZ1+bSGaBkaWBLamxRxMOLiccjijCTpTyRe98WEJ
bLkRim9pqVzNqHkcLHKwzPTCz7u65Be8tF2fSkbECnQOyxe0SqWrR7v9Q0CahSuH
4zBDBDRfyGNGuzKgOlqgUzXJq+mXhquW43ecy0n84tWhOsRmBp2iJDzvYvCBct/u
at6q9OY02NWQB0hcMWrn1Sq7jjFIkTbtIKX4GAYR+H8Dx0au/LRug0w5ilTwb1Mv
i6OKrNdG0J031i+W9F//8eMc6zIbOOIK+FXdzeEjqLaFafTntjK0owrLENFYIka/
BigsJ5vJksrHvwMsZLvE8GCIX0lrKlojC8lYfIAoI8mPg+UAgd5/6qQEYJjaPhVn
Bt6N35pxV7mvukUZTK6dvEagI0Ppnm2dzSSxzG5zq+0aKMKWSNEwXEyxtYIK0p6/
dv6elZqAzo9iDegS0x23jG7Wsm8ltqhaeRflOFGl92Dv1IEjREDgNrpT6i72NbPg
o/a/SE7FJfTcMIkQV4dCnftgmYjuYvvTIazWQL/m5iYxwhRUcxF50xOD0lbKXX+1
xJCsN6ADpp6/c1muAhsB/7bDqM1Yc2USkVgL/n1rlpRY7leXjqF4ZxcJgxeU1JAc
HxmznpSRRfBvAgMBAAGjgdowgdcwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQU
CW7S2T/VyE67HGngTirIZPtB8/0wHwYDVR0jBBgwFoAUsjLQIap6/79+qgsT5r/z
tSfcAyMwPgYDVR0fBDcwNTAzoDGgL4YtaHR0cDovL2NybC5yZW5pZWMuZ29iLnBl
L2FybC9jYXNlcnZpY2VzMDEuY3JsMEQGA1UdIAQ9MDswOQYEVR0gADAxMC8GCCsG
AQUFBwIBFiNodHRwOi8vd3d3LnJlbmllYy5nb2IucGUvcmVwb3NpdG9yeTANBgkq
hkiG9w0BAQUFAAOCAgEADSRd3Yu/9YH++2wOrVYbB5ka2B/ONgKDC9bBT0Q8EkBx
W5y2uTaRTSjh0mXai4r18hGxvwdg4yTGo3iRDgthLuICiGL7fgga2+iAqwOkCBfv
q62B+mcorQsIT1VvQhr/Po3MtaMP1inG6+v7PGgz0HmYINFaMYt0P1NdQdiWE8Zf
Hm0F6iKkgZQ4YWksW3CxpPB7j2/2jHJ++DCBew/XfXo7VjfgeKbKV5bWHXOBOjm2
aEVht/F9sOUvnzYQ+BKgqMVFIKtckrOGyAzanPwVA1ZzKc3jtW3k4n4uSqFEpbQk
IJy90JNxMFDhckSKOKXWg9DQyb0lv1AEwtYftAuwp9g3eGuEjMWb36FLMGED+ODH
xtPB9hy3bnfV+jqwv71YNG2C3+bnuEESiucn/CsU8T+jer6MDLEEXNsZo9daj/MQ
Mh/mfWV9wQukHV3gsgy9Mt2f+BKWSvCEc5iPA47ENNzDyS1QWV015o0hPY5FUAFC
sngDLwY2N6/h6/dLzgPTpw/akoxGhzlub6B3iZJCWavAdn0aBzQoIG21PRROasEa
k31EXoqsaKHq/WYYPhhaS6SptQhendVotuBAGeJe+FeLoSs/nCLsxWfQ+xTxr6rr
ygbKnZRJuL1FARMtmN9cBOegpvGVNaDqD5X+SCNO3W5VOwCCghsj823E5M98NmY=
-----END CERTIFICATE-----
```

SERIALNUMBER=RUC: 20295613620, CN=RENIEC Class III High Grade CA, OU=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE

Type	CA/QC
Status	undersupervision
Status starting time	2012-01-19T17:37:40.000Z

Service digital identity (X509)

Version	3
Serial number	428615119675287220864505477247851118594377606494
Signature algorithm	SHA256withRSA
Issuer	CN=RENIEC High Grade Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
Valid from	Wed Jul 21 17:53:35 PET 2010
Valid to	Sat Jul 18 17:53:35 PET 2020
Subject	SERIALNUMBER=RUC: 20295613620, CN=RENIEC Class III High Grade CA, OU=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
Public key	Sun RSA public key, 4096 bits modulus: 10322105508640716486498782637964411902040075877659293686819537442119967 90198559469363433948119026557131564217264038114236654465109984448701066 57327739989265155048137894717824923489000116795001823471329776863115893 79191207442943722880115906608364151205910856438899039819433679498150068 58541410731378550930809959545791252362061612810349018782500176172439508 65888401351192133299482515524450876533706809094507055182112858278666647 50167913071499520414334317705406777532352233563609957637716353021813128 39192083164063710422114590210924970315955151673408823933185509708199977 64954167345695225699734009896079760965709551993104756699154791665401456 98590796704968270876708899456859948320992522365292317414889303214513754 51169347909073013427235469462201077019577054716666251994245762335652933 27168516365376870407749571031703990679421161853926235045283053838781593 77134089118251367837457997183411577316745948798059174363659617566353325 28850405894565167605886151298141177047189127253794293830836890748495148 37543364788482892884714902516889886748087484548251195582049997405932245 06877804163692977420904986783799379682138975642551669568655163020248815 91937451459839220628505541218415934721741868284138524183361439927043715 76904914288576247682703282 7 public exponent: 65537
Subject key identifier	12343c6172d19d8acc455c001d970dcaa8c91f4f
CRL distribution points	http://crl.reniec.gob.pe/arl/hgcaservices01.crl
Authority key identifier	04183016801446b5e85b679913828d060c6eff424a9e098d95a6
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	857f8dbfa9da2d300bd979eb6a8ff70a67882121
SHA256 Thumbprint	aa5d2081555e7ef4aae96001866e848ee1b17bf34a997d5966b62e9220d4e802

The decoded certificate:

```
[
[
 Version: V3
 Subject: SERIALNUMBER=RUC: 20295613620, CN=RENIEC Class III High Grade CA, OU=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
10322105508640716486498782637964411902040075877659293686819537442119967901985594693634339481190265571315642172640381142366544651099844487010665732773998926515504813789471782492348900011679500182347132977686311589379191207442943722880115906608364151205910856438899039819433679498150068585414107313785509308099595457912523620616128103490187825001761724395086588840135119213329948251552445087653370680909450705518211285827866664750167913071499520414334317705406777532352233563609957637716353021813128391920831640637104221145902109249703159551516734082393318550970819997764954167345695225699734009896079760965709551993104756699154791665401456985907967049682708767088994568599483209925223652923174148893032145136754511693479090730134272354694622010770195770547166662519942457623356529332716851636537687040774957103170399067942116185392623504528305383878159377134089114825136783745799718341157731674594879805917436365961756635332528850405894565167605886151298141177047189127253794293830836890748495148375433647884828928847149025168898867480874845482511955820499974059322450687780416369297742090498678379937968213897564255166956865516302024881591937451459839220628505541218415934721741868284138524183361439927043715769049142885762476827032827
 public exponent: 65537
 Validity: [From: Wed Jul 21 17:53:35 PET 2010,
             To: Sat Jul 18 17:53:35 PET 2020]
 Issuer: CN=RENIEC High Grade Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
 SerialNumber: [    4b13c445 a3676f89 cc037a45 67234567 1237655e]

Certificate Extensions: 5
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 12 34 3C 61 72 D1 9D 8A   CC 45 5C 00 1D 97 0D CA  .4<ar....E\.....
```

```
0010: A8 C9 1F 4F                                       ...O
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 46 B5 E8 5B 67 99 13 82   8D 06 0C 6E FF 42 4A 9E  F..[g......n.BJ.
0010: 09 8D 95 A6                                        ....
]

]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.reniec.gob.pe/arl/hgcaservices01.crl]
]]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 23 68 74 74 70 3A 2F   2F 77 77 77 2E 72 65 6E  .#http://www.ren
0010: 69 65 63 2E 67 6F 62 2E   70 65 2F 72 65 70 6F 73  iec.gob.pe/repos
0020: 69 74 6F 72 79                                     itory

]]  ]
]

[5]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 07 CD AD 9D 86 6E 50 09   F4 A2 83 21 C9 72 3D C7  .....nP....!.r=.
0010: 2B D7 D3 CA CB C5 1D 72   D7 7A 00 BC 64 9D 67 EA  +......r.z..d.g.
0020: 40 5E 11 D4 4E B1 D6 3D   DB B4 D1 70 7D F0 43 FF  @^..N..=...p..C.
0030: D9 D4 01 8E FD 4D B5 E3   52 97 F5 89 8F C3 3F 06  .....M..R.....?.
0040: 1C 9C D2 62 54 81 1C 32   D1 BE 59 E5 3B 63 50 C6  ...bT..2..Y.;cP.
0050: 7D 03 D9 39 8C 61 DC 9C   37 9C 78 A2 2A 73 7E 1C  ...9.a..7.x.*s..
0060: 73 84 BF 9F EA AF E8 01   01 28 25 FF 02 98 3A 46  s........(%...:F
0070: D3 9D 94 4D B9 15 2E A5   EA EC D9 D2 82 33 C4 56  ...M.........3.V
0080: D2 A1 92 8A 8C 3A F8 3D   FA 0A 50 57 C1 72 17 13  .....:.=..PW.r..
0090: D4 CF A3 65 6E 3D CD 5D   63 A2 07 B7 8C 43 FB 9D  ...en=.]c....C..
00A0: 43 1A 74 63 FA CB FD 9C   F7 19 F9 C0 AE 1A F7 5B  C.tc...........[
00B0: CE E0 8C 6D 76 E7 2B B9   9A 7A D7 57 FB 47 A0 81  ...mv.+..z.W.G..
00C0: 86 4C 29 A8 11 DA 3B 78   BC DA B0 2F 17 A9 A7 DA  .L)...;x.../....
00D0: 57 05 E0 32 D8 F0 B1 71   98 26 67 A8 92 68 11 19  W..2...q.&g..h..
00E0: 9D A5 F5 4A 7C D6 89 C9   2E 03 25 62 39 0C C7 65  ...J|.....%b9..e
00F0: 83 2C 18 ED 8F 46 A0 68   95 12 04 FC DB 76 91 91  .,...F.h.....v..
0100: 72 3A 48 48 30 44 1C C8   AB 55 DD 14 11 96 D3 C1  r:HH0D...U......
0110: 25 35 A0 8B D1 25 4A C5   5B 84 F0 C0 10 B5 2D 2A  %5...%J.[.....-*
0120: 11 9B FB 57 B1 BD AE C8   A3 28 6F 4C 83 83 E6 AA  ...W.....(oL....
0130: 04 C6 E2 1B EA BE 4A 0A   EF 97 9A 89 6F 53 77 BD  ......J.....oSw.
0140: 7D A1 44 00 DA 26 B0 6D   C4 CC 9E A3 D0 32 7B 9F  ..D..&.m.....2..
0150: 59 B8 AC 46 53 5D C9 46   2D 55 9A 84 E2 8C AC 22  Y..FS].F-U.....".
0160: C7 AD 9A 34 84 C5 9D A7   8C 42 F9 CC 84 04 9F 4A  ...4.....B.....J
0170: DE 2C 4B AA D4 C8 8B D7   3D 85 65 D7 E2 3F 62 A0  .,K.....=.e..?b.
0180: 78 7E 11 B6 55 65 A4 9B   04 8F 4C 7B BD 8A 05 20  x...Ue....L....
0190: FC 28 31 38 B9 25 A8 4A   8B 56 23 17 2F AA D2 42  .(18.%.J.V#./..B
01A0: 91 9D 61 A7 62 B3 8A FE   83 FF F6 B0 E9 A0 18 15  ..a.b...........
01B0: A7 64 17 75 10 89 9A 6D   9D 68 F7 E2 1D DD 7E DE  .d.u...m.h......
01C0: 47 AC 2F 82 DC 4D D6 74   28 76 FA 15 33 B1 46 E0  G./..M.t(v..3.F.
01D0: 81 8B 5A 20 40 C9 F2 9D   A9 ED 23 8F F0 0F 63 82  ..Z @.....#...c.
01E0: 45 0A D2 BC 27 BF 65 EE   0F E6 67 0E E4 C9 9D B7  E...'.e...g.....
01F0: B4 48 B3 14 C2 24 56 5F   2C 5C 83 15 2D 15 A2 F6  .H...$V_,\..-...

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGozCCBIugAwIBAgIUSxPERaNnb4nMA3pFZyNFZxI3ZV4wDQYJKoZIhvcNAQEL
BQAwfzELMAkGA1UEBhMCUEUxPDA6BgNVBAoMM1JlZ2lzdHJvIE5hY2lvbmFsIGRl
IElkZW50aWZpY2FjacOzbiB5IEVzdGFkbyBDaXZpbDEyMDAGA1UEAwwpUkVOSUVD
IEhpZ2ggR3JhZGUgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMTAwNzIxMjI1
MzM1WhcNMjAwNzE4MjI1MzM1WjCBuDELMAkGA1UEBhMCUEUxPDA6BgNVBAoMM1Jl
Z2lzdHJvIE5hY2lvbmFsIGRlIElkZW50aWZpY2FjacOzbiB5IEVzdGFkbyBDaXZp
bDEnMCUGA1UECwweUkVOSUVDIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MScwJQYD
VQQDDB5SRU5JRUMgQ2xhc3MgSUlJIEhpZ2ggR3JhZGUgQ0ExGTAXBgNVBAUMEFJV
QzogMjAyOTU2MTM2MjAwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQD9
A82DjJizVgZJaCyeFBnyxkM4p6RtO61Bo6blHrziFg09acGbjD6q7vpNfnlVPJM/
vwvNhmvwBLdPOu3zsIpq9mA8/5ebPdAOJFH5vbKEDjGL9kgyc/Pw0otzHuY+HDJ8
5SK0LhCbeRqXREZaRnQdY9qN9cZpJO+vPcl5LYu1UUGw6u+wfMQDHXE3047T33A5
7VG3mvcZjIqXehaIbPnPi3KX4BH6UFl7KB5Mcoy2TSTrZKpQd63ecse1R0OPlj+7
f2eRuwCebQMJKYhPtYwJfOEADSilGQxaX1p7V/ODsgIlrZF8Sk9xp6hBY5yF/EJT
33ZcISFMBDJdnxaYhlPO3ftdNvnWM8WiIrm55NBL4Tg4t32ZSf6FOQFrfDI2c7hw
YE62JYqTgZ8ebolgPCWrVK5tI2frOmFIUo0ohvKdCFYzUSrvpzuDW7VhSLzqqNSs
e0X31tXfJ/CCekQoJFMePqfD/Ux3neYC4wVZrlLiSerO32d/NqestAL3XzsH3D5Z
```

TaxpX0ItjlCnIu4uphuzDH4j34LN3s4QlEK6WtKsqPagDA0i89vB+XQuqOHXIP0n
C0SIcyCUTukt2JOeB05E7ax3o3Ccs/N4c5LRrsusB3mZd7UMEsRE4xRFvd06xjZv
7l65FM9uEEMyCj6GDRK5o65JJDWAUtg5gxE5ab08+wIDAQABo4HcMIHZMA8GA1Ud
EwEB/wQFMAMBAf8wHQYDVR0OBBYEFBI0PGFy0Z2KzEVcAB2XDcqoyR9PMB8GA1Ud
IwQYMBaAFEa16FtnmROCjQYMbv9CSp4JjZWmMEAGA1UdHwQ5MDcwNaAzoDGGL2h0
dHA6Ly9jcmwucmVuaWVjLmdvYi5wZS9hcmwvaGdjYXNlcnZpY2VzMDEuY3JsMEQG
A1UdIAQ9MDswOQYEVR0gADAxMC8GCCsGAQUFBwIBFiNodHRwOi8vd3d3LnJlbmll
Yy5nb2IucGUvcmVwb3NpdG9yeTANBgkqhkiG9w0BAQsFAAOCAgEAB82tnYZuUAn0
ooMhyXI9xyvX08rLxR1yl3oAvGSdZ+pAXhHUTrHWPdu00XB98EP/2dQBjv1NteNS
l/WJj8M/Bhyc0mJUgRwy0b5Z5TtjUMZ9A9k5jGHcnDeceKIqc34cc4S/n+qv6AEB
KCX/Apg6RtOdlE25FS6l6uzZ0oIzxFbSoZKKjDr4PfoKUFfBchcT1M+jZW49zV1j
oge3jEP7nUMadGP6y/2c9xn5wK4a91vO4IxtducruZp611f7R6CBhkwpqBHaO3i8
2rAvF6mn2lcF4DLY8LFxmCZnqJJoERmdpfVKfNaJyS4DJWI5DMdlgywY7Y9GoGiV
EgT823aRkXI6SEgwRBzIq1XdFBGW08ElNaCL0SVKxVuE8MAQtS0qEZv7V7G9rsij
KG9Mg4PmqgTG4hvqvkoK75eaiW9Td719oUQA2iawbcTMnqPQMnufWbisRlNdyUYt
VZqE4oysIsetmjSExZ2njEL5zIQEn0reLEuq1MiL1z2FZdfiP2KgeH4RtlVlpJsE
j0x7vYoFIPwoMTi5JahKi1YjFy+q0kKRnWGnYrOK/oP/9rDpoBgVp2QXdRCJmm2d
aPfiHd1+3kesL4LcTdZ0KHb6FTOxRuCBi1ogQMnynantI4/wD2OCRQrSvCe/Ze4P
5mcO5Mmdt7RIsxTCJFZfLFyDFS0VovY=
-----END CERTIFICATE-----

SERIALNUMBER=RUC: 20295613620, CN=RENIEC Class II High Grade CA, OU=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE

Type	CA/QC
Status	undersupervision
Status starting time	2012-01-19T16:49:31.000Z
Service digital identity (X509)	
Version	3
Serial number	428615119675287220864505477247851118594377606492
Signature algorithm	SHA256withRSA
Issuer	CN=RENIEC High Grade Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
Valid from	Wed Jul 21 17:36:51 PET 2010
Valid to	Sat Jul 18 17:36:51 PET 2020
Subject	SERIALNUMBER=RUC: 20295613620, CN=RENIEC Class II High Grade CA, OU=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
Public key	Sun RSA public key, 4096 bits modulus: 665304493389224454723055258394402172782744105244659834458522052986985908075626094394549571040507966002037852095990394212421305922254170852799113151448879155014256345541410785909426710180892901794298810705848775648462635775986914235388393000306921613486267800795892024392681357390401517069855366719157962710030883635078322595330918716182078507259198372683896046394809347008080997237745455462182986068574368145469552618466880034084068244320674449843090663431393182384747386477316303724721374777666913347115698752274883318738785446153999451741503145170419349435604044686240559977829723727855421850538998027237169917437849204106293777132340367317669982660414256993069736610318944880938147502136046562024688097106810758669666046519122787197503564169794226525740111843113758614810896114426952209439386083547076503847181894028010260350034686261696148452245109447253764561501804959967778418731822716477169862693464673077491087801355441650323168032475153829128811423155995031156177018034431121382140923217012897485736425056523806025665876613749693008422026785889949358565156621745788186184601129703753411715093504972164638405747761817501058541410160552148871931148089270686800332889663798295612451957296163161039424365351153851505845285012639 public exponent: 65537
Subject key identifier	edde7c4b32741e3c5882b220beac25fa5d558086
CRL distribution points	http://crl.reniec.gob.pe/arl/hgcaservices01.crl
Authority key identifier	04183016801446b5e85b679913828d060c6eff424a9e098d95a6
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	10e4f809de0f1c9acc730db45b991a9e0748614f
SHA256 Thumbprint	ba35edfd1f811efadf7401ed2c765706a22595824a9730ee8ab19acf8ffa063f

The decoded certificate:

```
[
[
 Version: V3
 Subject: SERIALNUMBER=RUC: 20295613620, CN=RENIEC Class II High Grade CA, OU=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
665304493389224454723055258394402172782744105244659834458522052986985908075626094394549571040507966002037852095990394212421305922254170852799113151448879155014256345541410785909426710180892901794298810705848775648462635775986914235388393000306921613486267800795892024392681357390401517069855366719157962710030883635078322595330918716182078507259198372683896046394809347008080997237745455462182986068574368145469552618466880034084068244320674449843090663431393182384747386477316303724721374777666913347115698752274883318738785446153999451741503145170419349435604044686240559977829723727855421850538998027237169917437849204106293777132340367317669982660414256993069736610318944880938147502136046562024688097106810758669666046519122787197503564169794226525740111843113758614810896114426952209439386083547076503847181894028010260350034686261696148452245109447253764561501804959677784187318227164771698626934646730774910878013554416503231680324751538291288114231559950311561770180344311213821409232170128974857364250565238060256658766137496930084220267858899493585651566217457881861846011297037534117150935049721646384057477618175010585414101605521488719311480892706868003328896637982956124519572961631610394243653511538515058452850126392
 public exponent: 65537
 Validity: [From: Wed Jul 21 17:36:51 PET 2010,
             To: Sat Jul 18 17:36:51 PET 2020]
 Issuer: CN=RENIEC High Grade Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
 SerialNumber: [    4b13c445 a3676f89 cc037a45 67234567 1237655c]

Certificate Extensions: 5
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: ED DE 7C 4B 32 74 1E 3C   58 82 B2 20 BE AC 25 FA  ...K2t.<X.. ..%.
0010: 5D 55 80 86                                        ]U..
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 46 B5 E8 5B 67 99 13 82   8D 06 0C 6E FF 42 4A 9E  F..[g......n.BJ.
0010: 09 8D 95 A6                                        ....
]

]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.reniec.gob.pe/arl/hgcaservices01.crl]
]]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 23 68 74 74 70 3A 2F   2F 77 77 77 2E 72 65 6E  .#http://www.ren
0010: 69 65 63 2E 67 6F 62 2E   70 65 2F 72 65 70 6F 73  iec.gob.pe/repos
0020: 69 74 6F 72 79                                     itory

]]  ]
]

[5]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 55 1C 2F CE 31 08 1E 48   B2 E3 B5 CA 85 05 60 CD  U./.1..H......`.
0010: F7 F7 60 F7 74 CB 6C E7   7A EE 10 90 96 52 55 52  ..`.t.l.z....RUR
0020: 53 40 93 23 E9 DC 9E 10   8B D8 12 68 41 3F 80 29  S@.#.......hA?.)
0030: 9D 19 40 50 3E F7 8D B7   A6 BD E8 75 F4 79 4B 9D  ..@P>......u.yK.
0040: 51 71 45 65 1B FF 39 D8   A7 1C 5E 01 C6 56 D0 D1  QqEe..9...^..V..
0050: D7 0C B6 85 1E 25 C6 BD   F9 65 12 F0 83 DD B6 35  .....%...e.....5
0060: B0 B6 00 6E C9 FA A4 D7   49 CC CC 1A ED D6 AD 31  ...n....I......1
0070: 0D 3B E5 BA B3 F0 DA 56   0A 72 8F FF 44 38 C1 A4  .;.....V.r..D8..
0080: E2 C9 87 60 DA 5A D7 80   08 B6 0B 4D CB 5B 1B 18  ...`.Z.....M.[..
0090: 28 17 63 36 B5 AE 22 B9   25 B4 F2 3C 1B 6E 1F 3C  (.c6.."%..<.n.<
00A0: EC 4A 91 C4 C0 2D 3A E0   E7 3E 1E D4 FC 2B 18 8E  .J...-:..>...+..
00B0: F8 7F 16 70 6A A1 6D A5   61 83 AE 34 50 BE D6 3E  ...pj.m.a..4P..>
00C0: 6D E5 A2 BC 96 B8 08 C6   6E D0 0B 42 62 DC 0A 1E  m.......n..Bb...
00D0: A8 A3 BA 04 07 1B 1B FD   FB E2 A6 B5 E9 89 EF EB  ................
00E0: FA 5E 37 E4 82 1D 75 39   86 7C 59 0A E6 DA B7 6A  .^7...u9..Y....j
00F0: 62 79 3C 29 EF BA 03 C6   92 C6 ED FB 95 96 E6 36  by<)............6
0100: 73 E6 B5 C2 A5 A3 41 D2   8B F8 9C 31 62 2A A6 5B  s.....A....1b*.[
0110: 20 6D 1F 5A D2 43 B6 A3   C8 33 F4 2D 3E B2 7F CE   m.Z.C...3.->...
0120: 48 A7 E8 F0 A1 C4 54 72   8C BB 9E C7 76 94 B7 88  H.....Tr....v...
0130: 51 B7 E5 A6 98 77 39 E5   CC 0F 63 37 F6 5D 6E 2B  Q....w9...c7.]n+
0140: CD 71 2C 0E BB D8 D9 21   2E D1 39 1B CE B1 EF 26  .q,....!..9....&
0150: 02 A7 ED 2E D1 A3 ED AC   CC 7F 03 74 C8 39 4C AC  ...........t.9L.
0160: 4E EB C9 56 2C 2E 7E 08   EB 3A 18 BE 56 06 58 D5  N..V,....:..V.X.
0170: A3 32 28 F0 88 49 99 5E   9A AB 57 DF B6 89 B3 D8  .2(..I.^..W.....
0180: 5D 75 6B B5 56 E6 8E 6A   D1 62 8F 4D EC 4B 7D B7  ]uk.V..j.b.M.K..
```

```
0190: 07 21 51 A5 3D 88 F2 A6   5C C2 68 4C E9 08 B8 00  .!Q.=...\.hL....
01A0: 07 B0 4B 86 CA 3C 39 27   C1 5D 84 2A 1A 23 EA CF  ..K..<9'.].*.#..
01B0: B6 6D 07 92 4B 0D D8 DC   B8 9D 87 5E DF D9 65 EA  .m..K......^..e.
01C0: AF 8A 0A 31 0D 27 95 02   4D 55 6E A2 76 25 EC 3C  ...1.'..MUn.v%.<
01D0: 35 78 3D 47 16 BD E2 BE   A3 C4 FF 35 6B 52 C0 60  5x=G.......5kR.`
01E0: EE 38 78 42 D7 52 A3 F8   55 01 F5 51 07 53 66 3C  .8xB.R..U..Q.Sf<
01F0: 1B 9E A2 68 E8 8A DC 92   65 FC C3 43 3E 41 A7 37  ...h....e..C>A.7

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGojCCBIqgAwIBAgIUSxPERaNnb4nMA3pFZyNFZxI3ZVwwDQYJKoZIhvcNAQEL
BQAwfzELMAkGA1UEBhMCUEUxPDA6BgNVBAoMM1JlZ2lzdHJvIE5hY2lvbmFsIGRl
IElkZW50aWZpY2FjacOzbiB5IEVzdGFkbyBDaXZpbDEyMDAGA1UEAwwpUkVOSUVD
IEhpZ2ggR3JhZGUgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMTAwNzIxMjIz
NjUxWhcNMjAwNzE4MjIzNjUxWjCBtzELMAkGA1UEBhMCUEUxPDA6BgNVBAoMM1Jl
Z2lzdHJvIE5hY2lvbmFsIGRlIElkZW50aWZpY2FjacOzbiB5IEVzdGFkbyBDaXZp
bDEnMCUGA1UECwweUkVOSUVDIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MSYwJAYD
VQQDDB1SRU5JRUMgQ2xhc3MgSUkgSGlnaCBHcmFkZSBDQTEZMBcGA1UEBQwQUlVD
OiAyMDI5NTYxMzYyMDCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAKMU
PNpNK9Oj5AUGYLiz5VFFUYIxxNA/6FXeqiYl2H01306FR5ABaCzOONRRQEvAFf70
NUX80NlRYrnbxY4I9YA+HZfOHGPSPYf8uGJYp9BugTS1P1qGWeYBkmUHxOTZb4Lw
WC4h3/kmG5MCfpJEhsyYYWThPl3L0NzQC1ww0KxMyEMAK/84vmU8l0D017FyBIJC
Ts0J2aso5oDIBglksW4i2Ao0r8rNwi5YtzCg2H3H7j0Dv0qnjcacb4HV5lFB8cyU
Apej/+bHb4LU1qzXXhgBtbK7cgr7gWnSstEjJfQ/Ji7ZUSwz0zIHX0GglXLiSGK0
YXZBjGhHE7N6VI0t6zIaIh/suy684i79+NykKFNdFG+sefUboeQNfQiRdB63dQjZ
lJ3ME1znWDYpAR3NrLq0noUZH4ySZO3W6Ht5uMSNcapb+1kxRxy9vhglctnjKiBf
fhGhVHBB+/DHSUAtWt5BdQzSIET2tHV0mp//jbizTN3VA98qudTumPt32tQ7HV/O
HtmW+/e3L8ph24pt7OD7kxK+POv77VdyK/GQWkbrA1wbJ2/qS2b9D/JfrIn7wwD+
XyrGy8Ojpku2qZUy5Ia7n6YU/LdV9zClj9tCF9GC5G6dyA8rzepDlk0dXYEthxTl
gAN5Apjvuh++c1aOaRTK2loWqhoE0QRULpHdhcSfAgMBAAGjgdwwgdkwDwYDVR0T
AQH/BAUwAwEB/zAdBgNVHQ4EFgQU7d58SzJ0HjxYgrIgvqwl+l1VgIYwHwYDVR0j
BBgwFoAURrXoW2eZE4KNBgxu/0JKngmNlaYwQAYDVR0fBDkwNzA1oDOgMYYvaHR0
cDovL2NybC5yZW5pZWMuZ29iLnBlL2FybC9oZ2Nhc2VydmljZXMwMS5jcmwwRAYD
VR0gBD0wOzA5BgRVHSAAMDEwLwYIKwYBBQUHAgEWI2h0dHA6Ly93d3cucmVuaWVj
LmdvYi5wZS9yZXBvc2l0b3J5MA0GCSqGSIb3DQEBCwUAA4ICAQBVHC/OMQgeSLLj
tcqFBWDN9/dg93TLbOd67hCQllJVUlNAkyPp3J4Qi9gSaEE/gCmdGUBQPveNt6a9
6HX0eUudUXFFZRv/OdinHF4BxlbQ0dcMtoUeJca9+WUS8IPdtjWwtgBuyfqk10nM
zBrt1q0xDTvlurPw2lYKco//RDjBpOLJh2DaWteACLYLTctbGxgoF2M2ta4iuSW0
8jwbbh887EqRxMAtOuDnPh7U/CsYjvh/FnBqoW2lYYOuNFC+1j5t5aK8lrgIxm7Q
C0Ji3AoeqKO6BAcbG/374qa16Ynv6/peN+SCHXU5hnxZCubat2pieTwp77oDxpLG
7fuVluY2c+a1wqWjQdKL+JwxYiqmWyBtH1rSQ7ajyDP0LT6yf85Ip+jwocRUcoy7
nsd2lLeIUbflpph3OeXMD2M39l1uK81xLA672NkhLtE5G86x7yYCp+0u0aPtrMx/
A3TIOUysTuvJViwufgjrOhi+VgZY1aMyKPCISZlemqtX37aJs9hddWu1VuaOatFi
j03sS323ByFRpT2I8qZcwmhM6Qi4AAewS4bKPDknwV2EKhoj6s+2bQeSSw3Y3Lid
h17f2WXqr4oKMQ0nlQJNVW6idiXsPDV4PUcWveK+o8T/NWtSwGDuOHhC11Kj+FUB
9VEHU2Y8G56iaOiK3JJl/MNDPkGnNw==
-----END CERTIFICATE-----
```

SERIALNUMBER=RUC: 20295613620, CN=RENIEC Class II CA, OU=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE

Type	CA/QC
Status	undersupervision
Status starting time	2012-01-19T15:51:42.000Z

Service digital identity (X509)

Version	3
Serial number	428615119675287220864505477247851118594377606491
Signature algorithm	SHA1withRSA
Issuer	CN=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
Valid from	Wed Jul 21 17:26:08 PET 2010
Valid to	Sat Jul 18 17:26:08 PET 2020
Subject	SERIALNUMBER=RUC: 20295613620, CN=RENIEC Class II CA, OU=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE

Public key	Sun RSA public key, 4096 bits modulus: 68569346110318846159922559544634351288644217617302368146001904808229769 44706701356956574814076197366773100003196550483780536997155102917486264 84251632263481917049884215885228201573073767261785552516517981661924520 03531756889646918016151388983983197993318583768965356405745615689731401 05578747223667092461859135799002767416620141682074498081148815056899670 43498332734369125871359798597410743895948799693115534873779230450867352 59995302806524702758946831465600198624224971998892846611596077470925960 70887702965117632959257423790881946589275707545443229741707099220173394 61739462415092997112104650009312923515749386105627140582933599043062755 18607683383977212913375734842372778346807895308587570581796146978193111 64193352429298975597332184054216477105264763663327333866651939369745246 18951493559703615675250993384410465194379440761577301624729616414499202 30734987603005406330339982936524169364339314301029978244221464735763121 71992850357691454632390165145536131335420028380798604038157636997664126 19483222826738495029468061617799697470191176877338879483336450794164445 71025082796336262888438917625589086585339778649952056240442986272365216 45518346680261122293071426794732778186114978613762847930674515064789989 03909048911095844121237223 public exponent: 65537
Subject key identifier	604869e68658188b2cc7a663f587af3c88fc29b9
CRL distribution points	http://crl.reniec.gob.pe/arl/caservices01.crl
Authority key identifier	041830168014b232d021aa7affbf7eaa0b13e6bff3b527dc0323
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	cc3dba8f028415e8b4b98c54852bf43264658b95
SHA256 Thumbprint	847768d38a6ec62be2bbdf513023022676c9b81d4b4942a9bc81d048a1e17c18

The decoded certificate:

```
[
[
 Version: V3
 Subject: SERIALNUMBER=RUC: 20295613620, CN=RENIEC Class II CA, OU=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 4096 bits
 modulus:
68569346110318846159922559544634351288644217617302368146001904808229769447067013569565748140761973667731000031965504837805369971551029174862648425163226348191704988421588522
8201573073767261785552516517981661924520035317568896469180161513889839831979933185837689653564057456156897314010557874722366709246185913579900276741662014168207449808114881 5
056899670434983327343691258713597985974107438959487996931155348737792304508673525999530280652470275894683146560019862422497199889284661159607747092596070887702965117632959 25
742379088194658927570754544322974170709922017339461739462415092997112104650009312923515749386105627140582933599043062755186076833839772129133757348423727783468078953085875 70
581796146978193111641933524292989755973321840542164771052647636633273338666519393697452461895149355970361567525099338441046519437944076157730162472961641449920230734987603 00
540633033998293652416936433931430102997824422146473576312171992850357691454632390165145536131335420028380798604038157636997664126194832228267384950294680616177996974701911 76
877338879483336450794164445710250827963362628884389176255890865853397786499520562404429862723652164551834668026112229307142679473277818611497861376284793067451506478998903 90
9048911095844121237223
 public exponent: 65537
 Validity: [From: Wed Jul 21 17:26:08 PET 2010,
             To: Sat Jul 18 17:26:08 PET 2020]
 Issuer: CN=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
 SerialNumber: [    4b13c445 a3676f89 cc037a45 67234567 1237655b]

Certificate Extensions: 5
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 60 48 69 E6 86 58 18 8B   2C C7 A6 63 F5 87 AF 3C  `Hi..X..,..c...<
0010: 88 FC 29 B9                                        ..).
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: B2 32 D0 21 AA 7A FF BF   7E AA 0B 13 E6 BF F3 B5  .2.!.z..........
0010: 27 DC 03 23                                        '..#
]

]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.reniec.gob.pe/arl/caservices01.crl]
]]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 23 68 74 74 70 3A 2F   2F 77 77 77 2E 72 65 6E  .#http://www.ren
```

```
0010: 69 65 63 2E 67 6F 62 2E   70 65 2F 72 65 70 6F 73  iec.gob.pe/repos
0020: 69 74 6F 72 79                                     itory

]]  ]
]

[5]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: 43 FC 42 FE 99 20 3F 27   A3 25 92 D4 35 0B 58 AB  C.B.. ?'.%..5.X.
0010: 02 4C 74 8F DB 70 ED 0F   5A 99 14 74 8E 75 0A 25  .Lt..p..Z..t.u.%
0020: 73 05 B6 70 B4 88 B5 CC   60 51 20 10 50 B4 86 56  s..p....`Q .P..V
0030: B7 8E 7B FA F7 A9 2F BC   CA E5 41 5A 7C 2C E4 39  ....../...AZ.,.9
0040: 20 33 74 77 AB 16 F5 8B   B6 42 6F 41 1D 12 C2 4F   3tw.....BoA...O
0050: 57 AB 5B D6 8C D6 65 54   F2 D7 6E 4E 51 93 EE 60  W.[...eT..nNQ..`
0060: F2 09 7E 2D 94 BF 1D 62   F1 06 55 1D 39 1D D5 10  ...-...b..U.9...
0070: CC BB 8F A2 19 A6 CA 55   EA 38 57 BA F3 65 EB D1  .......U.8W..e..
0080: 60 89 30 FA FD 62 71 96   62 0E 31 8C 61 21 8B 47  `.0..bq.b.1.a!.G
0090: 0B 35 E2 FC CB 2F 23 28   E9 50 9C 14 5E 29 01 9F  .5.../#(.P..^)..
00A0: 8A BA 32 EE C3 1A D9 02   86 47 3A BD 01 38 47 19  ..2......G:..8G.
00B0: F6 61 53 90 05 05 AA 6F   FD B2 0F 21 04 0A 3F 39  .aS....o...!..?9
00C0: DC 3C C3 89 B0 CF D1 94   4C 5F EB 37 D8 DB FB 18  .<......L_.7....
00D0: C2 03 8D 4F D3 C0 7B CD   39 E9 AE 3B A2 3C D5 21  ...O....9..;.<.!
00E0: D2 C6 BA 8E F3 2B 70 E9   3C 97 C4 7E 5A CC 09 29  .....+p.<...Z..)
00F0: 8A 50 6F C4 33 E0 FC C8   3C E9 59 48 C0 32 8B C6  .Po.3...<.YH.2..
0100: 4B 32 16 9A 10 60 1C 52   D9 AF EE 12 F8 55 DE 73  K2...`.R.....U.s
0110: 7B ED 6C 25 E1 81 B6 EB   C1 35 2F 5B E2 55 79 02  ..l%.....5/[.Uy.
0120: A9 5B 16 1B 02 9A 37 55   3B C0 BD C6 2D 73 FA 1B  .[....7U;...-s..
0130: 24 53 9C 16 1C 91 0B 6B   EF 8E 65 F4 72 1D A9 76  $S.....k..e.r..v
0140: 08 DE F0 DE DE 38 56 17   F9 EC 2E 26 E9 7C BE 69  .....8V....&...i
0150: 1D 22 85 91 48 C6 72 94   4E 3D A8 4D 9A 06 93 04  ."..H.r.N=.M....
0160: C7 3B 68 50 D6 C3 08 D1   F0 BF 93 BF FD F9 36 A5  .;hP..........6.
0170: B5 30 39 0A 04 D3 58 FE   35 A5 83 13 96 2C D0 07  .09...X.5....,..
0180: 2D C2 98 87 7C B4 75 2E   1D E2 33 BC 5B 9F D5 04  -.....u...3.[...
0190: CE A0 97 15 0B 94 08 93   A2 EA FC DF C0 EE 30 7E  ..............0.
01A0: CB 93 85 F2 86 1A E1 D0   B7 C0 CB 2A 7B BC 91 ED  ...........*....
01B0: 89 39 0C 20 0E 2D D1 4B   4B 2F 04 E2 5E 05 D9 31  .9. .-.KK/..^..1
01C0: 07 B9 E2 80 16 88 DA B3   41 07 CE 24 90 6D 37 99  ........A..$.m7.
01D0: 78 BB FF 81 74 50 3E 8A   95 43 C4 5E 5C 58 F3 B2  x...tP>..C.^\X..
01E0: 76 53 CB 11 68 21 53 2F   35 0B CB 47 89 F6 11 47  vS..h!S/5..G...G
01F0: D6 7B 71 AC 61 86 7E 83   1E 64 6C E8 BD 70 AC BE  ..q.a....dl..p..

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGijCCBHKgAwIBAgIUSxPERaNnb4nMA3pFZyNFZxI3ZVswDQYJKoZIhvcNAQEF
BQAwdDELMAkGA1UEBhMCUEUxPDA6BgNVBAoMM1JlZ2lzdHJvIE5hY2lvbmFsIGRl
IElkZW50aWZpY2FjacOzbiB5IEVzdGFkbyBDaXZpbDEnMCUGA1UEAwweUkVOSUVD
IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MB4XDTEwMDcyMTIyMjYwOFoXDTIwMDcx
ODIyMjYwOFowgawxCzAJBgNVBAYTAlBFMTwwOgYDVQQKDDNSZWdpc3RybyBOYWNp
b25hbCBkZSBJZGVudGlmaWNhY2nDs24geSBFc3RhZG8gQ2l2aWwxJzAlBgNVBAsM
HlJFTklFQyBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTEbMBkGA1UEAwwSUkVOSUVD
IENsYXNzIElJIENBMRkwFwYDVQQFDBBSVUM6IDIwMjk1NjEzNjIwMIICIjANBgkq
hkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAqBOoN5pNZ/1t28UsecPElarnGq2y0/LO
AHmJcJSr3bBQ1mWs8YoIlK+VC3jyxM1/a27jwFNB5GZ/cTApbH9Z0+o2aJ+aDl6c
FIS+Xm0Gna/I6GCG2koYfDVtWvtw5znBxeNACJ/Uo8bcYIcfO+oBjbVeF4669/Yd
rFLS5qtVZFABqZHrummHVlpQc56ZZ3Pheifmt49O1UcFpS//JheBOwnqMgHOkMN8
CKWg1KZUSDiiZgFqE4Tep+vsCeHhxrhM3c5kBttyCcEampfY/8ax5a5mxdehp46L
ZvemMrZFpbk7BPOTkP74Tb2AXC06bxXoLTT7rDL79vIBF6ymqvNAo16l8NaGDcVp
ThrLd8QlF4lbZa/FCzGh2AMHtyJEGHHbSiiG21AYe1x9d95mBg7mGt/mOKfmJlk3
E+4QSM4I8cZVXxFfy2bF6M5tjvmw/WOkL/HcCIm50uNpbgL9cUCFhxpv8hVELlL2
geBEdu0Se28CijHLfhBqBnU3kul+KeHG8uIWUsOgydJNlxZN54LJwiC7VWVN3xUS
XBkDmKKlgCW6N4MR9cXI9nRJ5tONr/SbcNhoQyb5OR0xaWJIgKlyiDbK/lrDKGEc
fn96ZebvmphFHHgeHsnfEse1lwjvVZhJ+X5eisAm5ImLMycqzeRucbUJVBj0yhyZ
/Mu7mYkOVucCAwEAAaOB2jCB1zAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBRg
SGnmhlgYiyzHpmP1h688iPwpuTAfBgNVHSMEGDAWgBSyMtAhqnr/v36qCxPmv/O1
J9wDIzA+BgNVHR8ENzA1MDOgMaAvhi1odHRwOi8vY3JsLnJlbmllYy5nb2IucGUv
YXJsL2Nhc2VydmljZXMwMS5jcmwwRAYDVR0gBD0wOzA5BgRVHSAAMDEwLwYIKwYB
BQUHAgEWI2h0dHA6Ly93d3cucmVuaWVjLmdvYi5wZS9yZXBvc2l0b3J5MA0GCSqG
SIb3DQEBBQUAA4ICAQBD/EL+mSA/J6MlktQ1C1irAkx0j9tw7Q9amRR0jnUKJXMF
tnC0iLXMYFEgEFC0hla3jnv696kvvMrlQVp8LOQ5IDN0d6sW9Yu2Qm9BHRLCT1er
W9aM1mVU8tduTlGT7mDyCX4tlL8dYvEGVR05HdUQzLuPohmmylXqOFe682Xr0WCJ
MPr9YnGWYg4xjGEhi0cLNeL8yy8jKOlQnBReKQGfiroy7sMa2QKGRzq9AThHGfZh
U5AFBapv/bIPIQQKPzncPMOJsM/RlExf6zfY2/sYwgONT9PAe8056a47ojzVIdLG
uo7zK3DpPJfEflrMCSmKUG/EM+D8yDzpWUjAMovGSzIWmhBgHFLZr+4S+FXec3vt
bCXhgbbrwTUvW+JVeQKpWxYbApo3VTvAvcYtc/obJFOcFhyRC2vvjmX0ch2pdgje
8N7eOFYX+ewuJul8vmkdIoWRSMZylE49qE2aBpMExztoUNbDCNHwv5O//fk2pbUw
OQoE01j+NaWDE5Ys0ActwpiHfLR1Lh3iM7xbn9UEzqCXFQuUCJOi6vzfwO4wfsuT
hfKGGuHQt8DLKnu8ke2JOQwgDi3RS0svBOJeBdkxB7nigBaI2rNBB84kkG03mXi7
/4F0UD6KlUPEXlxY87J2U8sRaCFTLzULy0eJ9hFH1ntxrGGGfoMeZGzovXCsvg==
-----END CERTIFICATE-----
```

SERIALNUMBER=RUC: 20295613620, CN=RENIEC Class I High Grade CA, OU=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE

Type	CA/QC
Status	undersupervision
Status starting time	2012-01-18T22:03:08.000Z

Service digital identity (X509)

Version	3
Serial number	428615119675287220864505477247851118594377606490
Signature algorithm	SHA256withRSA
Issuer	CN=RENIEC High Grade Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
Valid from	Wed Jul 21 17:18:36 PET 2010
Valid to	Sat Jul 18 17:18:36 PET 2020
Subject	SERIALNUMBER=RUC: 20295613620, CN=RENIEC Class I High Grade CA, OU=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
Public key	Sun RSA public key, 4096 bits modulus: 974829743811928602972715997485290751456037065616267009013749709364110869896072734543922191626819387829401092603268772814406302477139812232365475510345311393682826757219683954382745620418640602220960850400689849406954607578462370728747703084232820095476085757723298423257136667177283928940869614879381073789220794163675580594716930296514932018892107534670642232169811896300178005011493714040485029492607037102045780004231857647888695140176168005859064265430558936980577939641437274017561088183428495740553432110087774785879306063055849676983791356726856914845944152408422101521655291354238244793466536580118232079460383117974405926007202921365648843754683600660844165723991808455675916133523542846352091195164227032036314836450447360836925764149281654978297933151883016654232776611241581694591810901106622342905389601396041027982341913993604442356221492222624061638307923461797498873537512750106725939374662927360451901797136259130581372796671169800336733377071277438258656157300069802250990540547974337807202046388429420735654091160902252762468480620244432134426238661734233822269654714798034207313305340984195958814047607756293745440361703255732647643958863644656677883854936000687256464277291849871546201300003701421140528823303765100037014211405288233037651
public exponent: 65537
Subject key identifier	5e9dfbd619854d992ad4bea6f10c4a7cd289ea99
CRL distribution points	http://crl.reniec.gob.pe/arl/hgcaservices01.crl
Authority key identifier	04183016801446b5e85b679913828d060c6eff424a9e098d95a6
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	b15060f3c44e0f6c2ca2fab9c88e1069c847424a
SHA256 Thumbprint	6972c885202a85c75fb9292855da6325b9fe853c865ffdc3b2a7fa514bd5ae45

The decoded certificate:

```
[
[
 Version: V3
 Subject: SERIALNUMBER=RUC: 20295613620, CN=RENIEC Class I High Grade CA, OU=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
974829743811928602972715997485290751456037065616267009013749709364110869896072734543922191626819387829401092603268772814406302477139812232365475510345311393682826757219683954382745620418640602220960850400689849406954607578462370728747703084232820095476085757723298423257136667177283928940869614879381073789220794163675580594716930296514932018892107534670642232169811896300178005011493714040485029492607037102045780004231857647888695140176168005859064265430558936980577939641437274017561088183428495740553432110087774785879306063055849676983791356726856914845944152408422101521655291354238244793466536580118232079460383117974405926007202921365648843754683600660844165723991808455675916133523542846352091195164227032036314836450447360836925764149281654978297933151883016654232776611241581694591810901106622342905389601396041027982341913993604442356221492222624061638307923461797498873537512750106725939374662927360451901797136259130581372796671169800336733377071277438258656157300069802250990540547974337807202046388429420735654091160902252762468480620244432134426238661734233822269654714798034207313305340984195958814047607756293745440361703255732647643958863644656677883854936000687256464277291849871546201300003701421140528823303765100037014211405288233037651
 public exponent: 65537
 Validity: [From: Wed Jul 21 17:18:36 PET 2010,
             To: Sat Jul 18 17:18:36 PET 2020]
 Issuer: CN=RENIEC High Grade Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
 SerialNumber: [    4b13c445 a3676f89 cc037a45 67234567 1237655a]

Certificate Extensions: 5
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 5E 9D FB D6 19 85 4D 99   2A D4 BE A6 F1 0C 4A 7C  ^.....M.*.....J.
```

```
0010: D2 89 EA 99                                       ....
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 46 B5 E8 5B 67 99 13 82   8D 06 0C 6E FF 42 4A 9E  F..[g......n.BJ.
0010: 09 8D 95 A6                                       ....
]

]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.reniec.gob.pe/arl/hgcaservices01.crl]
]]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 23 68 74 74 70 3A 2F   2F 77 77 77 2E 72 65 6E  .#http://www.ren
0010: 69 65 63 2E 67 6F 62 2E   70 65 2F 72 65 70 6F 73  iec.gob.pe/repos
0020: 69 74 6F 72 79                                    itory

]]  ]
]

[5]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 5E 1E B6 8C 47 8F BB FD   BC 77 1D EA 12 8B CB 7F  ^...G....w......
0010: 0C C1 64 A0 AF 28 72 40   3A 33 E0 DC 60 23 00 40  ..d..(r@:3..`#.@
0020: 2B 4D 4C 51 54 82 60 47   A8 3E 50 8E 4E 01 2E 41  +MLQT.`G.>P.N..A
0030: EA 65 5F CD 7B BA E1 58   3F 59 1B 55 43 E7 5E 7C  .e_....X?Y.UC.^.
0040: 13 1F 65 42 6A 94 2D 51   06 D4 C6 B8 18 7D F5 30  ..eBj.-Q.......0
0050: BA D4 C9 5C 91 17 88 39   24 B5 72 6F 1F 58 E3 56  ...\...9$.ro.X.V
0060: BA 20 58 64 F5 C3 76 2D   FF 1D EC ED D1 BE 80 F9  . Xd..v-........
0070: F9 E6 68 DD F5 98 AD 56   E8 D1 CC 2D A6 B8 02 E8  ..h....V...-....
0080: 31 F5 30 97 95 DD D2 5F   A1 BA 0B 5F AB FE 23 F1  1.0...._..._..#.
0090: D2 16 7C 26 D8 B2 DC 63   ED 34 34 D6 70 F8 B4 1E  ...&...c.44.p...
00A0: 0D 69 92 96 75 EB F6 65   24 6E E5 E9 63 9D 2F C7  .i..u..e$n..c./.
00B0: F0 ED FC E6 34 8F CB 78   9E D1 C7 96 2C 49 76 F0  ....4..x....,Iv.
00C0: 67 D9 CF 65 76 72 27 28   84 84 FB 3E FA 69 3C FC  g..evr'(...>.i<.
00D0: 2D E0 13 88 50 67 2F 23   A5 A7 E2 AD 8A C9 03 60  -...Pg/#.......`
00E0: 8C CD 52 06 ED 62 3A A1   A6 7D B2 CD F4 C6 5D D4  ..R..b:.......].
00F0: 5B 24 09 3A 00 BF 61 EA   E1 13 99 A7 9C 29 E7 B0  [$.:..a......)..
0100: 2F FD D8 86 1E 51 98 B7   BB BE 87 35 19 67 97 1F  /....Q.....5.g..
0110: 70 4A 9F 85 53 F3 1C FB   FE B4 A8 D3 DE 4B 4C 9C  pJ..S........KL.
0120: 5B 45 03 3E 42 E2 75 81   B9 F0 45 97 55 DA E2 AA  [E.>B.u...E.U...
0130: 64 79 C3 F4 51 79 7C 54   76 8D CE 90 AC 15 ED 23  dy..Qy.Tv......#
0140: 5A E1 19 AC 08 5E 2A 21   E0 40 10 1A 38 70 0C 4E  Z....^*!.@..8p.N
0150: D4 F4 00 15 D4 4A EB 00   54 4F 54 2E 52 33 67 03  .....J..TOT.R3g.
0160: C9 0F 47 24 73 EC 0E 9D   2C 67 77 C1 14 F8 B1 8D  ..G$s...,gw.....
0170: 15 1E 77 9A A1 B6 04 46   EA 4D ED 09 DB 42 01 D0  ..w....F.M...B..
0180: 87 CC 2E D4 66 77 67 35   15 20 F7 64 06 51 29 69  ....fwg5. .d.Q)i
0190: FB 3E AF 85 9D 87 B9 D2   E7 56 9F 1A C1 BB C9 6C  .>.......V.....l
01A0: BB DE 52 0B 7F CA BF F2   76 A1 F3 61 D0 A5 E6 92  ..R.....v..a....
01B0: 86 62 4C 73 67 BA AC C7   4D C4 C8 92 CE 00 9F 15  .bLsg...M.......
01C0: 80 F8 50 DD 89 30 E6 36   83 A0 4E 7B 8D 0E 86 3E  ..P..0.6..N....>
01D0: BF F8 E1 BF 8C 37 60 CC   17 30 8E 9B 2E 73 57 58  .....7`..0...sWX
01E0: A1 54 B1 CD 78 51 B8 F1   8A 6F 73 40 5A 7E 13 8C  .T..xQ...os@Z...
01F0: 70 4C 9D A8 77 A0 88 F9   68 8C 6F B6 93 F1 5C 06  pL..w...h.o...\.

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGoTCCBImgAwIBAgIUSxPERaNnb4nMA3pFZyNFZxI3ZVowDQYJKoZIhvcNAQEL
BQAwfzELMAkGA1UEBhMCUEUxPDA6BgNVBAoMM1JlZ2lzdHJvIE5hY2lvbmFsIGRl
IElkZW50aWZpY2FjacOzbiB5IEVzdGFkbyBDaXZpbDEyMDAGA1UEAwwpUkVOSUVD
IEhpZ2ggR3JhZGUgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMTAwNzIxMjIx
ODM2WhcNMjAwNzE4MjIxODM2WjCBtjELMAkGA1UEBhMCUEUxPDA6BgNVBAoMM1Jl
Z2lzdHJvIE5hY2lvbmFsIGRlIElkZW50aWZpY2FjacOzbiB5IEVzdGFkbyBDaXZp
bDEnMCUGA1UECwweUkVOSUVDIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MSUwIwYD
VQQDDBxSRU5JRUMgQ2xhc3MgSSBIaWdoIEdyYWRlIENBMRkwFwYDVQQFDBBSVUM6
IDIwMjk1NjEzNjIwMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA7vMf
0qBoc89Y4aWVv8M+oQAPGCUhs5zVJTeBojvjJ3Hp/uxanh1um8C4xdu72S3AqDgg
nntxEKNuixW1opr0pyNOVcRlZ1Hxv5xoJYdz/rBBZfintUM97bJrbm+lM/2R4I9i
jGDLWhv0snDcCwMb/KoyDJzsHCL6p0kth1LiWgwDzywixDTJTR2bxOG/NztmIQLs
Cvu9Lq/HDVsxJkpk5sVYNUQz8bajwlRv310gXLhcL5S5/gG+CzHhOkWdxbW8Vgso
ufStB9zk8DW2pcv/9ikYl3l7VPg+X8/JUGnPtv/W9DK5vd6tzzLK9z5VsQJ8Lrby
PogfjTD8cxYFZdNydnz9mKe2UwAhvEetiEl36nj3YZJl7DCu8yoRt2ioWwqVG/bi
pKqzFYDLvIws4kAw0vDLaEgJzR16HbIMiGKB3tAKO3RlCOVtbHTRWjrqqquW4t6k
UDA2YEXbAn2vmRozjdxrK+gj3o+AiNmBZB8fLuR3taIAkEWqKL7IQ5DI9f2zzqjR
```

iSs+B5/eR575NVWVFsGZWt1o4lk5j73UmPHamtmF7vcXNWFOuoUKmyc1aMjuZjEx
xSHfcJ8fFM0HCjJYa+khKdro5upJk7EQfK+XKms7vOAh6vj3bpaDDEOZjRXbjGdA
CuG3nFAWxljU8lYgFcsxOQms0FX/A2C8TvFc71MCAwEAAaOB3DCB2TAPBgNVHRMB
Af8EBTADAQH/MB0GA1UdDgQWBBRenfvWGYVNmSrUvqbxDEp80onqmTAfBgNVHSME
GDAWgBRGtehbZ5kTgo0GDG7/QkqeCY2VpjBABgNVHR8EOTA3MDWgM6Axhi9odHRw
Oi8vY3JsLnJlbmllYy5nb2IucGUvYXJsL2hnY2FzZXJ2aWNlczAxLmNybDBEBgNV
HSAEPTA7MDkGBFUdIAAwMTAvBggrBgEFBQcCARYjaHR0cDovL3d3dy5yZW5pZWMu
Z29iLnBlL3JlcG9zaXRvcnkwDQYJKoZIhvcNAQELBQADggIBAF4etoxHj7v9vHcd
6hKLy38MwWSgryhyQDoz4NxgIwBAK01MUVSCYEeoPlCOTgEuQeplX817uuFYP1kb
VUPnXnwTH2VCapQtUQbUxrgYffUwutTJXJEXiDkktXJvH1jjVrogWGT1w3Yt/x3s
7dG+gPn55mjd9ZitVujRzC2muALoMfUwl5Xd0l+hugtfq/4j8dIWfCbYstxj7TQ0
1nD4tB4NaZKWdev2ZSRu5eljnS/H8O385jSPy3ie0ceWLEl28GfZz2V2cicohIT7
PvppPPwt4BOIUGcvI6Wn4q2KyQNgjM1SBu1iOqGmfbLN9MZd1FskCToAv2Hq4ROZ
p5wp57Av/diGHlGYt7u+hzUZZ5cfcEqfhVPzHPv+tKjT3ktMnFtFAz5C4nWBufBF
l1Xa4qpkecP0UXl8VHaNzpCsFe0jWuEZrAheKiHgQBAaOHAMTtT0ABXUSusAVE9U
LlIzZwPJD0ckc+wOnSxnd8EU+LGNFR53mqG2BEbqTe0J20IB0IfMLtRmd2c1FSD3
ZAZRKWn7Pq+FnYe50udWnxrBu8lsu95SC3/Kv/J2ofNh0KXmkoZiTHNnuqzHTcTI
ks4AnxWA+FDdiTDmNoOgTnuNDoY+v/jhv4w3YMwXMI6bLnNXWKFUsc14Ubjxim9z
QFp+E4xwTJ2od6CI+WiMb7aT8VwG
-----END CERTIFICATE-----

SERIALNUMBER=RUC: 20295613620, CN=RENIEC Class I CA, OU=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE

Type	CA/QC
Status	undersupervision
Status starting time	2012-01-17T22:01:38.000Z

Service digital identity (X509)

Version	3
Serial number	428615119675287220864505477247851118594377606489
Signature algorithm	SHA1withRSA
Issuer	CN=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
Valid from	Wed Jul 21 17:07:43 PET 2010
Valid to	Sat Jul 18 17:07:43 PET 2020
Subject	SERIALNUMBER=RUC: 20295613620, CN=RENIEC Class I CA, OU=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
Public key	Sun RSA public key, 4096 bits modulus: 1023088478785829859915418521264150547301057153032510998795854486407476694076378025143202468077263446546603289575073369098066255030027359674356676229431228949421270625853847309757498094173638028317259856210789860297340747847417959571520779913590891321812893313830668253634406268269218939401484548680748837141060653941321363556770750387299724013396767347981908842487990411029314924107496194537562590413674221081187581225881277008966769865207236896548190826662097166609006916865191974974363766799577736374759309197587066094960362713476896409364641697062540625669020075126701196610729650716685925442423211519500383517415305408467791265385950228564211537379362393328151461532494304286418068608551413947610926597173446307672351412312003273495405233250482063289145119940915318631501198804484596816206388503008770493185123220461938736480443857714672365707141091921472858108391539920345593030777476113933065136477851774679734583822253996155375540472055558802633319316279491597792290228109255364421200834251854410525908501465207820621557125688494895635902195505159426569267817937766007878865879687594785610467452593005418715520710315811984175412076397977908450506156411904345593073174777790786338434351329831964465182506720736272197442973800523 public exponent: 65537
Subject key identifier	60818ebdff310369780dde10be20a56f8886c0c8
CRL distribution points	http://crl.reniec.gob.pe/arl/caservices01.crl
Authority key identifier	041830168014b232d021aa7affbf7eaa0b13e6bff3b527dc0323
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	a5d0ccf78fa8c29b52b121f7118927e251b92971
SHA256 Thumbprint	5ca727c898ac83798f5e2ed98dbd6a70037710e02b12f573398eb2f3babce371

The decoded certificate:

```
[
[
 Version: V3
 Subject: SERIALNUMBER=RUC: 20295613620, CN=RENIEC Class I CA, OU=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 4096 bits
 modulus:
1023088478785829859915418521264150547301057153032510998795854486407476694076378025143202468077263446546603289575073369098066255030027359674356676229431228949421270625853847309757498094173638028317259856210789860297340747847417959571520779913590891321812893313830668253634406268269218939401484548680748837141060653941321363556770750387299724013396767347981908842487990411029314924107496194537562590413674221081187581225881277008966769865207236896548190826662097166609006916865191974974363766799577736374759309197587066094960362713476896409364641697062540625669020075126701196610729650716685925442423211519500383517415305408467791265385950228564211537379362393328151461532494304286418068608551413947610926597173446307672351412312003273495405233250482063289145119940915318631501198804484596816206388503008770493185123220461938736480443857714672365707141091921472858108391539920345593030777476113933065136477851774679734583822253996155375540472055558802633319316279491597792290228109255364421200834251854410525908501465207820621557125688494895635902195505159426569267817937766007878865879687594785610467452593005418715520710315811984175412076397979084505061564119043455930731747777907863384343513298319644651825067207362721974429730005 23
 public exponent: 65537
 Validity: [From: Wed Jul 21 17:07:43 PET 2010,
             To: Sat Jul 18 17:07:43 PET 2020]
 Issuer: CN=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
 SerialNumber: [    4b13c445 a3676f89 cc037a45 67234567 12376559]

Certificate Extensions: 5
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 60 81 8E BD FF 31 03 69   78 0D DE 10 BE 20 A5 6F  `....1.ix.... .o
0010: 88 86 C0 C8                                        ....
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: B2 32 D0 21 AA 7A FF BF   7E AA 0B 13 E6 BF F3 B5  .2.!.z..........
0010: 27 DC 03 23                                        '..#
]

]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.reniec.gob.pe/arl/caservices01.crl]
]]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 23 68 74 74 70 3A 2F   2F 77 77 77 2E 72 65 6E  .#http://www.ren
0010: 69 65 63 2E 67 6F 62 2E   70 65 2F 72 65 70 6F 73  iec.gob.pe/repos
0020: 69 74 6F 72 79                                     itory

]]  ]
]

[5]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: 20 7B 53 27 DB 5E 71 D2   51 AD 95 FE 30 79 22 E3   .S'.^q.Q...0y".
0010: B8 B4 18 5B E8 88 49 4F   A3 BB E1 55 83 CE 24 2F  ...[..IO...U..$/
0020: D7 17 A2 7E A1 62 DF 2B   F6 6C 52 C6 B3 8A 1C D1  .....b.+.lR.....
0030: 9E 54 D3 D8 04 0F 90 34   46 E3 4B 93 3A D2 F9 A1  .T.....4F.K.:...
0040: 93 E9 8A E0 AD 3B 12 08   A0 81 D1 45 9D FD 19 B2  .....;.....E....
0050: 1A 6C 40 4F BF 51 68 73   F4 E3 19 34 D4 25 24 00  .l@O.Qhs...4.%$.
0060: 7A 08 24 F5 67 13 64 A6   17 2F 00 52 B6 17 A5 1A  z.$.g.d../.R....
0070: 7E CF 96 4F 20 1C 6E 98   FD 6E 65 CA 59 00 8C 29  ...O .n..ne.Y..)
0080: 5C D1 D6 CD 33 46 91 79   CA E3 F4 76 D7 17 4A 1C  \...3F.y...v..J.
0090: 97 D6 96 45 8E 11 DB 3D   7A 92 6C CB 8B E9 AC 0B  ...E...=z.l.....
00A0: 69 69 57 A1 94 DC 23 64   1F CC 95 7F 01 B0 1B BC  iiW...#d........
00B0: 9C 75 30 4D E1 E1 96 C4   47 BF 1A 13 C4 16 1E BC  .u0M....G.......
00C0: 24 20 64 6F BC 80 78 D4   6A 26 97 08 68 CB DD C5  $ do..x.j&..h...
00D0: 9A F9 B3 B0 BF 1A B2 4A   50 97 71 BF 5A BB 3E C1  .......JP.q.Z.>.
00E0: BB 27 D2 DD E0 79 3F 07   B9 96 E2 48 CB 0F 37 43  .'...y?....H..7C
00F0: C7 03 86 06 EC E7 FD 4D   9A 1C 8F 9D 2E 6C 6B BE  .......M.....lk.
0100: BC F1 52 A8 EA 77 EB E3   F0 DD 84 15 8C A7 B1 3E  ..R..w.........>
0110: 12 7F F5 C9 1C 37 1C F3   E2 D5 99 CA 3C C1 0A 22  .....7......<.."
0120: 1C 07 94 10 12 C2 03 80   EF B1 1B CF 0D C7 C2 B2  ................
0130: 73 61 DB 89 17 67 B6 7C   AA 20 1B EA 94 F6 33 78  sa...g... ....3x
0140: C8 93 A7 C1 DC 3C 61 A8   DB 46 75 77 64 C3 CA F0  .....<a..Fuwd...
0150: 1C BA 92 E1 3D 25 1B 30   44 9E 37 2D D3 07 FC F9  ....=%.0D.7-....
0160: F2 C0 1D B4 A1 53 41 80   9B 34 DC 3F 17 39 8C 6B  .....SA..4.?.9.k
0170: F2 23 A1 C4 28 98 C6 89   3A 96 CE 23 89 D5 DA F4  .#..(...:..#....
0180: 02 FF 18 2A 15 8A 73 10   F2 7C 88 0F B9 0B 54 30  ...*..s.......T0
0190: DF A6 69 8C 91 38 24 4D   91 C3 BB E2 02 FF A5 97  ..i..8$M........
01A0: 6E C5 6D 1B D7 03 D6 2D   C0 23 DF BA 0B CE 14 C2  n.m....-.#......
```

```
01B0: 86 5E 40 C7 58 1A 56 03   16 1A 5A E5 73 B0 AC A3  .^@.X.V...Z.s...
01C0: 0A B3 B1 86 F6 D5 3C D2   D5 1B 16 B7 30 48 9C 54  ......<.....0H.T
01D0: 1B 1D DB A7 59 38 8A 91   9C 7E DB 19 9F CE E8 BF  ....Y8.........
01E0: E6 AF FB 45 2D 34 A9 BA   BA 82 31 6D C1 BD 53 1A  ...E-4....1m..S.
01F0: D5 FA EC 99 15 96 77 D7   C7 2E 6A 13 1B 93 27 15  ......w...j...'.

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGiTCCBHGgAwIBAgIUSxPERaNnb4nMA3pFZyNFZxI3ZVkwDQYJKoZIhvcNAQEF
BQAwdDELMAkGA1UEBhMCUEUxPDA6BgNVBAoMM1JlZ2lzdHJvIE5hY2lvbmFsIGRl
IElkZW50aWZpY2FjacOzbiB5IEVzdGFkbyBDaXZpbDEnMCUGA1UEAwweUkVOSUVD
IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MB4XDTEwMDcyMTIyMDc0M1oXDTIwMDcx
ODIyMDc0M1owgasxCzAJBgNVBAYTAlBFMTwwOgYDVQQKDDNSZWdpc3RybyBOYWNp
b25hbCBkZSBJZGVudGlmaWNhY2nDs24geSBFc3RhZG8gQ2l2aWwxJzAlBgNVBAsM
HlJFTklFQyBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTEaMBgGA1UEAwwRUkVOSUVD
IENsYXNzIEkgQ0ExGTAXBgNVBAUMEFJVQzogMjAyOTU2MTM2MjAwggIiMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQD6x2M2KQECvnJCFeDr3erfUKXlgGorfTMx
zXm6lnLv7oroDXTemajXy837yNPr882M2E+oG2dU30QRn1F/1U6xotJVA8gHmqwu
jkaxIvdwtSkBAjt7bEfdVeLi6u0A/tK2kFqwMYnnItwXLwlhU9b1t2Z3Ad8adTY1
UZh+aP3GUikdAtRH4+bZ4TJAr6sQSS9OYpH9fQk57vtasydy7ccxR6wQ59smGV21
AO5iBJU/z0xoYgAV4YX95imv4Yxz1zlCHOA3NLHMANPRsdfACSUGmnTX+BJZ55FY
k5S7DR2VEkpO34Ny/iMLbNH913PZzMEajaZOYDLaGzz6+BPJjifmAL9aXQXjm4CO
ggfD5JtYrYw9M+14fJEiR/lrRIW+9Na0d4hdmZN2Xaw9Qi7/5RJiowV7fJM9bhY4
O63d4OFmaAxPHTSn2j9qs8SlsAGJk3sHNsyepeO0oupvWZLEjJmN9a0yyJspehuO
4lCa//IyOhxBIQ877zbtAKs41lm6DkkQPkvtcs1xJTyLT/sEvkRSIO3G+yMUoL4n
dy2GuGqttkBuv7lS2e+d4ytMJLC7U4I2tns92fFHT6Z8CWk9tSXa2MJwzaXXi23p
tg3N3J2SSXl0dS9xTM0uPrzz8FCCoIp7erQt/dcQjKKB9cFMIKMJoHQvNSsyVRwu
Upe4pLkYSwIDAQABo4HaMIHXMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFGCB
jr3/MQNpeA3eEL4gpW+IhsDIMB8GA1UdIwQYMBaAFLIy0CGqev+/fqoLE+a/87Un
3AMjMD4GA1UdHwQ3MDUwM6AxoC+GLWh0dHA6Ly9jcmwucmVuaWVjLmdvYi5wZS9h
cmwvY2FzZXJ2aWNlczAxLmNybDBEBgNVHSAEPTA7MDkGBFUdIAAwMTAvBggrBgEF
BQcCARYjaHR0cDovL3d3dy5yZW5pZWMuZ29iLnBlL3JlcG9zaXRvcnkwDQYJKoZI
hvcNAQEFBQADggIBACB7UyfbXnHSUa2V/jB5IuO4tBhb6IhJT6O74VWDziQv1xei
fqFi3yv2bFLGs4oc0Z5U09gED5A0RuNLkzrS+aGT6YrgrTsSCKCB0UWd/RmyGmxA
T79RaHP04xk01CUkAHoIJPVnE2SmFy8AUrYXpRp+z5ZPIBxumP1uZcpZAIwpXNHW
zTNGkXnK4/R21xdKHJfWlkWOEds9epJsy4vprAtpaVehlNwjZB/MlX8BsBu8nHUw
TeHhlsRHvxoTxBYevCQgZG+8gHjUaiaXCGjL3cWa+bOwvxqySlCXcb9auz7BuyfS
3eB5Pwe5luJIyw83Q8cDhgbs5/1NmhyPnS5sa7688VKo6nfr4/DdhBWMp7E+En/1
yRw3HPPi1ZnKPMEKIhwHlBASwgOA77Ebzw3HwrJzYduJF2e2fKogG+qU9jN4yJOn
wdw8YajbRnV3ZMPK8By6kuE9JRswRJ43LdMH/PnywB20oVNBgJs03D8XOYxr8iOh
xCiYxok6ls4jidXa9AL/GCoVinMQ8nyID7kLVDDfpmmMkTgkTZHDu+IC/6WXbsVt
G9cD1i3AI9+6C84UwoZeQMdYGlYDFhpa5XOwrKMKs7GG9tU80tUbFrcwSJxUGx3b
p1k4ipGcftsZn87ov+av+0UtNKm6uoIxbcG9UxrV+uyZFZZ318cuahMbkycV
-----END CERTIFICATE-----
```

CN=RENIEC High Grade Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE

Type	CA/QC
Status	undersupervision
Status starting time	2011-11-04T22:53:59.000Z

Service digital identity (X509)

Version	3
Serial number	428615119675287220864505477247851118594377606488
Signature algorithm	SHA256withRSA
Issuer	CN=RENIEC High Grade Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
Valid from	Wed Jul 21 16:22:01 PET 2010
Valid to	Tue Jul 16 16:22:01 PET 2030
Subject	CN=RENIEC High Grade Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE

Public key	Sun RSA public key, 4096 bits modulus: 802531795212955811677995130068009796074797982549177780020614530348231469842534205065099812647334194693210727844455663071518649624218430760307190550689366985528371513507700099136358820869714295100901669591558226646552692050013931298286183992173486320213710867442468015018075377938717393080795694623422612496282798426202274988611074625957994462133210524718814821408853950783019868251860820531351854771860717933097482017163169625535636395138479919435777893659556399433512284285272821306397853827141586751823009057419157864700515694150720515671751241868248391709135089662663802861161365668999684528212589938093426245563688860442552859360941058351749436249445400059098641568316745706571788802580787506000486301010413811002142547877691874257592171128596090240009085696258394819601165704056023141568862321601193878798522627749528686837950148210670180962218232034921711633650595291773813762807465671195164733051810051349893947142374576488728133719822942156856747946187893633127886635451523529006731864184494903995002946380019066027113958094459326995768727786979160296300585915987483517626429370167044681977340013305648924713600571461284827680840172200244378683312462198693290172697153210192741828318551388164199899347325572857722212726423
public exponent: 65537
Subject key identifier	46b5e85b679913828d060c6eff424a9e098d95a6
Authority key identifier	04183016801446b5e85b679913828d060c6eff424a9e098d95a6
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	45c84d84587baa23c1e3c87c164aa483f230dc17
SHA256 Thumbprint	99362ee3ee8e59ffdb6fc26c24b231fb80dcb5f6f98cb7fa9369ab1a68fcdc45

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=RENIEC High Grade Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
802531795212955811677995130068009796074797982549177780020614530348231469842534205065099812647334194693210727844455663071518649624218430760307190550689366985528371513507700099136358820869714295100901669591558226646552692050013931298286183992173486320213710867442468015018075377938717393080795694623422612496282798426202274988611074625957994462133210524718814821408853950783019868251860820531351854771860717933097482017163169625535636395138479919435777893659556399433512284285272821306397853827141586751823009057419157864700515694150720515671751241868248391709135089662663802861161365668999684528212589938093426245563688860442552859360941058351749436249445400059098641568316745706571788802580787506000486301010413811002142547877691874257592171128596090240009085696258394819601165704056023141568862321601193878798522627749528686837950148210670180962218232034921711633650595291773813762807465671195164733051810051349893947142374576488728133719822942156856747946187893633127886635451523529006731864184494903995002946380019066027113958094459326995768727786979160296300585915987483517626429370167044681977340013305648924713600571461284827680840172200244378683312462198693290172697153210192741828318551388164199899347325572857722212726423
 public exponent: 65537
 Validity: [From: Wed Jul 21 16:22:01 PET 2010,
             To: Tue Jul 16 16:22:01 PET 2030]
 Issuer: CN=RENIEC High Grade Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
 SerialNumber: [    4b13c445 a3676f89 cc037a45 67234567 12376558]

Certificate Extensions: 3
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 46 B5 E8 5B 67 99 13 82   8D 06 0C 6E FF 42 4A 9E  F..[g......n.BJ.
0010: 09 8D 95 A6                                        ....
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 46 B5 E8 5B 67 99 13 82   8D 06 0C 6E FF 42 4A 9E  F..[g......n.BJ.
0010: 09 8D 95 A6                                        ....
]

]

[3]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 70 88 55 50 AD 75 5E F6   CC 73 36 6C 73 69 44 B3  p.UP.u^..s6lsiD.
0010: 6D 08 E6 5A 64 49 2F 6F   EF C7 44 89 F5 F8 D2 F9  m..ZdI/o..D.....
0020: 2A 4D FB A9 EA D9 C7 E7   F4 BA 05 71 96 3C C7 AD  *M.........q.<..
0030: 64 D6 CF 54 9B 9C C6 1F   DE 6B 16 5F 37 13 83 16  d..T.....k._7...
0040: 8B 67 3C 7F BE 23 65 7D   6A 12 BE 5C FA BF 5C 04  .g<..#e.j..\..\.
```

```
0050: 65 36 87 B7 3F C2 7E 8A   9F 72 51 BB 51 CC 90 3D  e6..?....rQ.Q..=
0060: 9A 76 26 F1 70 50 08 32   1D C3 1E F3 1A 6C 78 27  .v&.pP.2.....lx'
0070: 5A E5 AE 6C DD 37 1E 3D   23 9C E4 F9 2B 0E 5B 6C  Z..l.7.=#...+.[l
0080: 37 6A 7F ED D9 07 8C 35   35 B1 6E 56 A8 2B A6 A0  7j.....55.nV.+..
0090: D9 38 68 88 F6 6D B1 CE   09 FD 97 48 D1 5C 04 8B  .8h..m.....H.\..
00A0: 9C 0F 05 8C 9A 6B 6C ED   3E F1 09 DB CC 84 1D 8B  .....kl.>.......
00B0: 0C 95 92 25 4C DF A5 3D   3A E1 CC FD 46 E9 13 28  ...%L..=:...F..(
00C0: 6D 4B 41 26 FA 8E A5 C1   0F 1D 2A 7E 38 2B F2 A8  mKA&......*.8+..
00D0: 98 7B EC 96 63 DB E7 7D   4C FF 8A C7 03 32 4C 0C  ....c...L....2L.
00E0: 49 AD 85 62 42 62 78 AD   77 DF 18 7E 80 75 3A 6B  I..bBbx.w....u:k
00F0: 8A AD 3B C4 88 7F 5B A6   33 91 3F 0A 40 7C 84 18  ..;...[.3.?.@...
0100: 52 25 F2 4E E6 46 45 2B   B2 45 E0 D9 BA 9B 59 D1  R%.N.FE+.E....Y.
0110: C0 20 80 F5 36 53 49 DE   72 38 B3 25 D1 70 D3 8C  . ..6SI.r8.%.p..
0120: AD 05 BB 66 1F 06 5E 52   D7 4D 0B 88 98 06 35 56  ...f..^R.M....5V
0130: 91 F8 0A F0 1D 00 C1 0F   F3 66 3D F6 0B F7 7F 2F  .........f=..../
0140: A1 59 A5 2D 8E DA D1 3D   6D 75 54 6F 20 98 3D 5C  .Y.-...=muTo .=\
0150: C3 69 CE 0D E4 12 D2 EA   52 C7 72 41 59 FE F5 BC  .i......R.rAY...
0160: 0B 6E 38 BD BA C4 03 D6   01 92 6E 82 E4 7B A2 0A  .n8.......n.....
0170: 55 72 3F 56 5B 68 1F FD   A3 DE 39 28 B1 68 DE 66  Ur?V[h....9(.h.f
0180: 55 30 61 B2 64 A5 EE 14   BA 64 CE 80 3A 11 A3 C2  U0a.d....d..:...
0190: 80 C4 65 08 04 72 E6 CB   A8 EA 4A 01 3A 90 D8 C2  ..e..r....J.:...
01A0: F4 78 DE 32 BA 7A 0D B6   70 A0 31 D4 27 74 CB 0A  .x.2.z..p.1.'t..
01B0: F2 91 B3 BA FC 66 95 20   21 BB 66 7F 08 34 75 F2  .....f. !.f..4u.
01C0: A9 CB B3 D2 72 9E F1 24   F1 2B CC FE D8 CB 54 9F  ....r..$.+....T.
01D0: 57 7F BE 4C 19 58 E3 30   16 27 52 A9 AF 36 96 D0  W..L.X.0.'R..6..
01E0: 8C D6 BD E8 9A B9 A6 8D   79 E4 7D 7B C6 7B 90 F0  ........y.......
01F0: BC E2 0C 74 37 F9 83 37   C9 5B B6 89 15 D0 6D DF  ...t7..7.[....m.

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIF3zCCA8egAwIBAgIUSxPERaNnb4nMA3pFZyNFZxI3ZVgwDQYJKoZIhvcNAQEL
BQAwfzELMAkGA1UEBhMCUEUxPDA6BgNVBAoMM1JlZ2lzdHJvIE5hY2lvbmFsIGRl
IElkZW50aWZpY2FjacOzbiB5IEVzdGFkbyBDaXZpbDEyMDAGA1UEAwwpUkVOSUVD
IEhpZ2ggR3JhZGUgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMTAwNzIxMjEy
MjAxWhcNMzAwNzE2MjEyMjAxWjB/MQswCQYDVQQGEwJQRTE8MDoGA1UECgwzUmVn
aXN0cm8gTmFjaW9uYWwgZGUgSWRlbnRpZmljYWNpw7NuIHkgRXN0YWRvIENpdmls
MTIwMAYDVQQDDClSRU5JRUMgSGlnaCBHcmFkZSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cml0eTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAMS3VFV1mCAmYroK
RWIz3fth6awRo4LVHMJMJwPR43FNODErnOq2qbzCJp3BLR1bCsrJC53Yr6qKU4f6
cPMXF4NAKTN0LtXOzviuvqltKiWQXIjSWeHA6OyXtrZhSImnIxTpuC9nTOJb9vmL
+cGuiLrxASqZ2UGaNJ7INPFnqhtfRHJPDi2lD1Mb0si/vol++EgWPb+3YBSpiDJ5
58siUa9vcIgjWBu/Ha48yjkma/vGkBIsO2nG+QzECQVK2iowVgKDksv7gJ6Irrlg
flQjWJohjDL4MXptRTh+4HuhfCZHtdXtcQ4jV0WaGW0i5CfoK1VMgsQjZ+a2klLd
/l81TZnluq4tKNVCtDnYxQ1QHXErIjUG/X92T0V5ND0ivbj2Gt4puY92IwSQJ4d7
YNX/9PtBObAP8noHxkwKzQ6UiXofGOARtOjOCQRE9edI67MtD+ppSrHac4zphEh5
IMTE5KEhTgS8R6apxml4SKJTHvvX489GQ2Z04uniWPHd1XGpxDzunv1vbcnttIUe
HdMiOYd/yFgAhIgXEbVIqsquMCwDbR0eLJ8klt8OHv3TiulzAmtc4SoJx94GRSmT
rGxVqRKJXdYeEQzHIw1/tsG2kUOr6V+dClljE9PkaRDgcbNv8Qb1rPoq2bhNKLnK
bQVMDSbc7MrELkaPRTvIydYvKDaXAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMBAf8w
HQYDVR0OBBYEFEa16FtnmROCjQYMbv9CSp4JjZWmMB8GA1UdIwQYMBaAFEa16Ftn
mROCjQYMbv9CSp4JjZWmMA0GCSqGSIb3DQEBCwUAA4ICAQBwiFVQrXVe9sxzNmxz
aUSzbQjmWmRJL2/vx0SJ9fjS+SpN+6nq2cfn9LoFcZY8x61k1s9Um5zGH95rFl83
E4MWi2c8f74jZX1qEr5c+r9cBGU2h7c/wn6Kn3JRu1HMkD2adibxcFAIMh3DHvMa
bHgnWuWubN03Hj0jnOT5Kw5bbDdqf+3ZB4w1NbFuVqgrpqDZOGiI9m2xzgn9l0jR
XASLnA8FjJprbO0+8QnbzIQdiwyVkiVM36U9OuHM/UbpEyhtS0Em+o6lwQ8dKn44
K/KomHvslmPb531M/4rHAzJMDEmthWJCYnitd98YfoB1OmuKrTvEiH9bpjORPwpA
fIQYUiXyTuZGRSuyReDZuptZ0cAggPU2U0necjizJdFw04ytBbtmHwZeUtdNC4iY
BjVWkfgK8B0AwQ/zZj32C/d/L6FZpS2O2tE9bXVUbyCYPVzDac4N5BLS6lLHckFZ
/vW8C244vbrEA9YBkm6C5HuiClVyP1ZbaB/9o945KLFo3mZVMGGyZKXuFLpkzoA6
EaPCgMRlCARy5suo6koBOpDYwvR43jK6eg22cKAx1Cd0ywrykbO6/GaVICG7Zn8I
NHXyqcuz0nKe8STxK8z+2MtUn1d/vkwZWOMwFidSqa82ltCM1r3omrmmjXnkfXvG
e5DwvOIMdDf5gzfJW7aJFdBt3w==
-----END CERTIFICATE-----
```

CN=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE

Type	CA/QC
Status	undersupervision
Status starting time	2011-11-04T16:33:58.000Z

Service digital identity (X509)

Version	3
Serial number	428615119675287220864505477247851118594377606487
Signature algorithm	SHA1withRSA
Issuer	CN=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
Valid from	Wed Jul 21 16:03:38 PET 2010
Valid to	Tue Jul 16 16:03:38 PET 2030
Subject	CN=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE

Public key	Sun RSA public key, 4096 bits modulus: 711625386247425811631592037138037813544672934740452396502553784549371802995765261297726461882601539098924391454654266401541685996620736583656560283323503306982397685985141078450139967363670256889913475311275841141 315499954202564649121896139954570058045253209191998264306272371807953080554381671231560763808561586401123285770950498652650172775586533341362862644256015853851421756269421779766564715872495761393402301043017012745 100259896398193552080120310024735220675363551405846247190550021386253295567322665490569634348 556732266549056963434866617793718239372236959941220298994369690014799171 109838435469174333911536755853174782650296564837620501412867406947923242 256305691029603152531452760105044689415628554851949088590662359560207649 977095666236785904956860027846838235877337181299697888362857663632879577692463314306099938596131875041755170521213265471617525870626678006514302604077899804 514141057745389347145666047358344921489506816797469083236629452794090572188618720088604216759539930065302764897902580409016454478330193694540530585851988549348959300053320 531179884895430001785432924252014734906727622861189981178967368663201486514526899401521931692148369300236818211322442897912786657849438162481371623436165230215774607971 public exponent: 65537
Subject key identifier	b232d021aa7affbf7eaa0b13e6bff3b527dc0323
Authority key identifier	041830168014b232d021aa7affbf7eaa0b13e6bff3b527dc0323
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	94f055623025d70c0d3f0db0d18118f2b336731e
SHA256 Thumbprint	2d1c3a9c02a7ebf3db40e7044fe6ad4909564b9ec4a89939fd1611550faa9159

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 4096 bits
 modulus:
711625386247425811631592037138037813544672934740452396502553784549371802995765261297726461882601539098924391454654266401541685996620736583656560283323503306982397685985141078450139967363670256889913475311275841141315499954202564649121896139954570058045253209191998264306272371807953080554381671231560763808561586401123285770950498652650172775586533341362862644256015853851421756269421779766564715872495761393402301043017012745100259896398193552080120310024735220675363551405846247190550021386253295567322665490569634348666177937182393722369599412202989943696900147991710983843546917433391153675585317478265029656483762050141286740694792324256305691029603152531452760105044689415628554851949088590662359560207649770956662367859049568600278468382358773371812996978883628576636328795776924633143060999385961318750417551705212132654716175258706266780065143026040778998045141410577453893471456660473583449214895068167974690832366294527940905721886187200886042167595399300653027648979025804090164544783301936945405305858519885493489593000533207009256268353678884221105238531179884895430001785432924252014734906727622861189981178967368663201486514526899401521931692148369300236818211322442897912786657849438162481371623436165230215774607971
 public exponent: 65537
 Validity: [From: Wed Jul 21 16:03:38 PET 2010,
              To: Tue Jul 16 16:03:38 PET 2030]
 Issuer: CN=RENIEC Certification Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
 SerialNumber: [    4b13c445 a3676f89 cc037a45 67234567 12376557]

Certificate Extensions: 3
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: B2 32 D0 21 AA 7A FF BF   7E AA 0B 13 E6 BF F3 B5  .2.!.z..........
0010: 27 DC 03 23                                        '..#
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: B2 32 D0 21 AA 7A FF BF   7E AA 0B 13 E6 BF F3 B5  .2.!.z..........
0010: 27 DC 03 23                                        '..#
]

]

[3]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: 53 07 13 92 7C 7A FE 7E   7B 9E C2 59 3A 3D 8F 6B  S....z.....Y:=.k
0010: A6 F6 69 E7 6D BD D6 A5   B9 84 92 5D E7 F3 59 54  ..i.m......]..YT
0020: D5 E5 AF FE 97 2D A7 9A   0D 17 0B FE 15 30 4B 62  .....-.......0Kb
0030: 73 37 EF A9 F5 AF 2D 87   52 3A 81 B7 1E F3 86 10  s7.....-.R:......
0040: E7 F3 53 97 29 71 EB 0C   D9 F7 15 AC 12 7A 96 95  ..S.)q.......z..
```

```
0050: 80 4E EF BB AE 95 BD 2D   A5 8B 5A A1 5F FB F7 62  .N.....-..Z._..b
0060: 7A B7 59 28 58 9B 68 39   DF 44 A4 F4 4B F9 A3 AE  z.Y(X.h9.D..K...
0070: 2C 58 8B 2D 8B 54 D3 EF   6E 91 87 BF AE 2F 16 E7  ,X.-.T..n..../..
0080: A1 AA 36 D8 A3 8B BB 80   84 6E E1 FC 7F C9 10 7D  ..6......n......
0090: 87 96 88 28 0B 67 97 0E   28 D7 32 59 EF 75 62 D4  ...(.g..(.2Y.ub.
00A0: 44 E3 DD C9 99 9F F1 1F   20 14 22 1A 4D 9B 19 BD  D....... .".M...
00B0: 01 E2 8F 3F 14 8A A0 4A   5B DD F2 3F 4A D3 D6 8D  ...?...J[..?J...
00C0: 54 D5 44 6D 18 A6 A2 5E   18 16 68 1A 33 0F EA 89  T.Dm...^..h.3...
00D0: 9C 72 DF 69 52 0C 29 D4   6F FC 35 D1 6A 96 05 CA  .r.iR.).o.5.j...
00E0: DA 4A 38 EE 53 0A 0E 67   BA 25 8A 4E 08 0F 1B 97  .J8.S..g.%.N....
00F0: 5F 25 6F F8 CA 37 F7 4B   DB E6 FF D1 67 43 BC 0A  _%o..7.K....gC..
0100: 1F 28 0B 34 4A 2E DB D5   C5 12 2D 45 34 4D 24 51  .(.4J.....-E4M$Q
0110: 32 70 94 23 E2 57 A9 24   2C 07 EE 9A 5D A0 F3 22  2p.#.W.$,...].."
0120: 12 EC D7 F1 84 3C B4 0E   3A A9 4D 56 AC 94 AD 75  .....<..:.MV...u
0130: CF EC 2C 64 19 02 4F 34   61 8D E5 B2 90 55 05 E8  ..,d..O4a....U..
0140: 25 99 EE A5 43 51 B2 12   A6 D7 42 CA D6 2D 0C AE  %...CQ....B..-..
0150: 77 88 85 98 73 F0 79 F0   3C 84 4C 2C 2F 44 16 14  w...s.y.<.L,/D..
0160: FA 9F 00 FC 3E 63 A0 D1   47 88 1D E0 58 C1 41 7A  ....>c..G...X.Az
0170: F6 50 45 8E E3 CB AC 94   90 C4 08 E3 53 C1 CA A2  .PE.........S...
0180: F0 EC E8 B6 6B 73 B8 68   D5 18 73 6E 24 4E 21 FC  ....ks.h..sn$N!.
0190: D7 D9 70 A3 5A B7 2C E0   AA 8E AC 33 D0 89 93 3B  ..p.Z.,....3...;
01A0: 92 E3 DE AF 3B D2 D6 1C   85 5B 89 E8 F1 7B 32 56  ....;....[....2V
01B0: E0 13 EA 6A AC A7 24 A0   FD D2 42 EE BF 53 87 35  ...j..$...B..S.5
01C0: 6E 1F DC DC C6 57 15 39   07 42 2A C7 39 64 48 6C  n....W.9.B*.9dHl
01D0: 0E 48 9C B1 97 59 11 F8   C5 77 B9 1D EC C6 55 98  .H...Y...w....U.
01E0: 0C BA 94 41 53 DB C4 12   13 97 D6 8B DB 49 93 3E  ...AS........I.>
01F0: 8F 49 55 35 71 2D 44 30   42 50 C7 38 B2 1B 2E CC  .IU5q-D0BP.8....

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIFyTCCA7GgAwIBAgIUSxPERaNnb4nMA3pFZyNFZxI3ZVcwDQYJKoZIhvcNAQEF
BQAwdDELMAkGA1UEBhMCUEUxPDA6BgNVBAoMM1JlZ2lzdHJvIE5hY2lvbmFsIGRl
IElkZW50aWZpY2FjacOzbiB5IEVzdGFkbyBDaXZpbDEnMCUGA1UEAwweUkVOSUVD
IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MB4XDTEwMDcyMTIxMDMzOFoXDTMwMDcx
NjIxMDMzOFowdDELMAkGA1UEBhMCUEUxPDA6BgNVBAoMM1JlZ2lzdHJvIE5hY2lv
bmFsIGRlIElkZW50aWZpY2FjacOzbiB5IEVzdGFkbyBDaXZpbDEnMCUGA1UEAwwe
UkVOSUVDIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEArm7mdj6EvMHqzCIZuL9qIDYzj7wYq4hjDFJM5o+yDu6I
36pn46Go3BBaDeFndRR9uFFyKcZbluAc7TdWRYbqcvN74qYFjKEorzmAc2+5pH8q
NX6A0rjVGNMmwHRZEWCa1A8Q1aQ6vx4XhSdNii4ps7eaV52HQoNeaRMHnG0n+kpD
Cwuz4i3rmrJ7YNNQoEc+RhiHMidz2ceZ8NJhm49QhFIh5rCRlzMBnExhHjlixkjj
DaMtnaV8ZNA7+xBsdVEUEaeQEtvNaA5FZVNAyhE8WeylDMrRUzfKmI7Ng4Mej3LO
cnQPH+hE5mspYOhCcJYZwVaBp54cSERtkK8V58ROtlm4GPPba9K4uq7erThYgGN8
OSq8NDkac0o88ITvMgakYVwaXi2XFsdK9v/FK1/4GUsMUrQImSgMe9gP3zKqb6QG
n+9WYZnf+W3Q98siO145f2MdPLkSmm7hd3CtUz4kfrGtZd2YqTQ0ZWahnlFw49Da
ppLm8Hksju8lHdVH+tiJtiuuNGk1hvEJZxoQoJFiWDsUDKhUYiBI7LYCZazGsZb8
ZdgnSbIZ0aMe/EoJYM8sKmPuFWa+AhnzU6dzULxHovtbQpDMIveMIg+FgUoj9tP0
YqWSjALtP1KkEkPLuSn6oG9gc8nhd8uic9PBjRjqumUhsMbhE0RFxfrjyEsdmmMC
AwEAAaNTMFEwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUsjLQIap6/79+qgsT
5r/ztSfcAyMwHwYDVR0jBBgwFoAUsjLQIap6/79+qgsT5r/ztSfcAyMwDQYJKoZI
hvcNAQEFBQADggIBAFMHE5J8ev5+e57CWTo9j2um9mnnbb3WpbmEkl3n81lU1eWv
/pctp5oNFwv+FTBLYnM376n1ry2HUjqBtx7zhhDn81OXKXHrDNn3FawSepaVgE7v
u66VvS2li1qhX/v3Ynq3WShYm2g530Sk9Ev5o64sWIsti1TT726Rh7+uLxbnoao2
2KOLu4CEbuH8f8kQfYeWiCgLZ5cOKNcyWe91YtRE493JmZ/xHyAUIhpNmxm9AeKP
PxSKoEpb3fI/StPWjVTVRG0YpqJeGBZoGjMP6omcct9pUgwp1G/8NdFqlgXK2ko4
7lMKDme6JYpOCA8bl18lb/jKN/dL2+b/0WdDvAofKAs0Si7b1cUSLUU0TSRRMnCU
I+JXqSQsB+6aXaDzIhLs1/GEPLQOOqlNVqyUrXXP7CxkGQJPNGGN5bKQVQXoJZnu
pUNRshKm10LK1i0MrneIhZhz8HnwPIRMLC9EFhT6nwD8PmOg0UeIHeBYwUF69lBF
juPLrJSQxAjjU8HKovDs6LZrc7ho1RhzbiROIfzX2XCjWrcs4KqOrDPQiZM7kuPe
rzvS1hyFW4no8XsyVuAT6mqspySg/dJC7r9ThzVuH9zcxlcVOQdCKsc5ZEhsDkic
sZdZEfjFd7kd7MZVmAy6lEFT28QSE5fWi9tJkz6PSVU1cS1EMEJQxziyGy7M
-----END CERTIFICATE-----
```

Certificate Service Provider Name (en): WISEKEY S.A.

Trade name (en)	WISEKEY S.A.
Information URI (en)	HTTPS://WWW.WISEKEY.COM/
Service provider street address (es)	ROUTE DE PRE-BOIS 29
Service provider street address (en)	ROUTE DE PRE-BOIS 29
Service provider postal code (es)	CH-1215 GENEVE 15
Service provider postal code (en)	CH-1215 GENEVE 15
Service provider locality (es)	SWITZERLAND
Service provider locality (en)	SWITZERLAND
Service provider state (es)	GENEVE

Service provider state (en)	GENEVE
Service provider country (es)	CH
Service provider country (en)	CH

CN=WISeKey CertifyID Advanced GB CA 2, O=WISeKey, C=CH

Type	CA/QC
Status	undersupervision
Status starting time	2017-06-05T21:19:34.000Z

Service digital identity (X509)

Version	3
Serial number	687834607324232377
Signature algorithm	SHA256withRSA
Issuer	CN=WISeKey CertifyID Policy GB CA 1, O=WISeKey, C=CH
Valid from	Wed May 27 10:22:04 PET 2015
Valid to	Thu Dec 01 10:10:31 PET 2039
Subject	CN=WISeKey CertifyID Advanced GB CA 2, O=WISeKey, C=CH
Public key	Sun RSA public key, 2048 bits modulus: 30337547528942006267353543430178699897514218074033697247936474690038342 99068050724454089169333968453893383909272233886924534704373142844193386 22120658475834781371575221355760855869652266102727121662715272378731217 07574889708575859924072083643971237821145199600309346220414599730571049 37613127223195776527840685808772815793796035756419165647035983165114608 64630553598949007755463127135415413336751950302418700965620521525982583 17367168809159692488617257475826114789226831118842774617384192882784776 28892251402610829195158662404752418989496557734256176931959227845946948 37225106805296054974787516569278842733161594911 49 public exponent: 65537
Subject key identifier	a01cb23f3f6a4aa0bf83bbfc79c3aacb1ddfde75
CRL distribution points	http://public.wisekey.com/crl/wcidpgbca1.crl
Authority key identifier	041830168014d1e60b822574252c5591d503187bbfc1eeaf1d80
Key usage	digitalSignature keyCertSign cRLSign
Basic constraints	CA=true; PathLen=0
SHA1 Thumbprint	5bde30a026c75c36c850e32668e296c819a0e2d3
SHA256 Thumbprint	68e6292fd4aa384d63a5f4fa8bd885bd1656e3509ba4206673e0660a169fe701

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=WISeKey CertifyID Advanced GB CA 2, O=WISeKey, C=CH
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
303375475289420062673535434301786998975142180740336972479364746900383429906805072445408916933396845389338390927223388692453470437314284419338622120658475834781371575221355760855869652266102727121662715272378731217
075748897085758599240720836439712378211451996003093462204145997305710493761312722319577652784068580877281579379603575641916564703598316511460864630553598949007755463127135415413336751950302418700965620521525982583
173671688091596924886172574758261147892268311188427746173841928827847762889225140261082919515
866240475241898949655773425617693195922784594694837225106805296054974787516569278842733161594911 49
 public exponent: 65537
 Validity: [From: Wed May 27 10:22:04 PET 2015,
             To: Thu Dec 01 10:10:31 PET 2039]
 Issuer: CN=WISeKey CertifyID Policy GB CA 1, O=WISeKey, C=CH
 SerialNumber: [    098badee 59c7fab9]

Certificate Extensions: 7
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: A0 1C B2 3F 3F 6A 4A A0   BF 83 BB FC 79 C3 AA CB  ...??jJ.....y...
```

```
0010: 1D DF DE 75                                       ...u
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: D1 E6 0B 82 25 74 25 2C   55 91 D5 03 18 7B BF C1  ....%t%,U.......
0010: EE AF 1D 80                                        ....
]

]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://public.wisekey.com/crl/wcidpgbca1.crl]
]]

[4]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 DigitalSignature
 Key_CertSign
 Crl_Sign
]

[5]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.16.756.5.14.7.3]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 21 68 74 74 70 3A 2F   2F 77 77 77 2E 77 69 73  .!http://www.wis
0010: 65 6B 65 79 2E 63 6F 6D   2F 72 65 70 6F 73 69 74  ekey.com/reposit
0020: 6F 72 79                                           ory

]]  ]
 [CertificatePolicyId: [2.5.29.32.0]
[]  ]
]

[6]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:0
]

[7]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://public.wisekey.com/crt/wcidpgbca1.crt,
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://ocsp2.wisekey.com/]
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 4B BB 55 28 A3 69 CA 77   BA 76 7D E6 AB 3E 26 4B  K.U(.i.w.v...>&K
0010: 69 0C F8 EB 51 E4 25 35   F8 9D 02 93 0D B7 05 88  i...Q.%5........
0020: 4C 26 2A 43 19 DD 41 BB   8B 1A EB 8E 2C 58 B3 49  L&*C..A.....,X.I
0030: 93 C9 64 7F 74 6B E2 37   6E 4D D0 6A 36 6F 96 10  ..d.tk.7nM.j6o..
0040: 28 56 3D FC 6A 3C D3 DB   9E E5 E3 2D 52 DD DC 09  (V=.j<.....-R...
0050: C3 17 DC 1C E8 12 B1 AE   FE 90 2B C2 B0 E4 C8 D0  ..........+.....
0060: E0 71 C9 D1 1A 9A 8C AC   6A 38 7D 37 7E 63 CC FC  .q......j8.7.c..
0070: 59 C7 55 CA 4B 07 54 32   2B 52 FE 7C 20 6D 35 64  Y.U.K.T2+R.. m5d
0080: 57 5F 4A FC 68 E1 8B 6C   EF 6E C8 AF 60 7A A2 E3  W_J.h..l.n..`z..
0090: 49 6B C2 0D 0D 1D B3 B7   1B 1F 80 16 40 92 C5 AD  Ik..........@...
00A0: D3 1B A4 0C A1 9B 63 68   25 C5 68 1E DC FF 2B 92  ......ch%.h...+.
00B0: 40 B7 F0 27 59 BD F5 0D   6D 8C AC EA 07 E1 E1 64  @..'Y...m......d
00C0: BA 0A 87 A6 F0 61 46 75   AB 29 54 5E 1A BA 2E 76  .....aFu.)T^...v
00D0: B4 42 21 61 18 A1 45 89   0F F4 0B 99 85 84 30 60  .B!a..E.......0`
00E0: 4A 4F 55 EC FC 99 60 66   2B 5B 88 F3 86 90 F3 FE  JOU...`f+[......
00F0: D4 17 99 73 51 D1 05 5B   CC AA EA 4F CA 8B C4 4F  ...sQ..[...O...O

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIEgTCCA2mgAwIBAgIICYut7lnH+rkwDQYJKoZIhvcNAQELBQAwSjELMAkGA1UE
BhMCQ0gxEDAOBgNVBAoTB1dJU2VLZXkxKTAnBgNVBAMTIFdJU2VLZXkgQ2VydGlm
eUlEIFBvbGljeSBHQiBDQSAxMB4XDTE1MDUyNzE1MjIwNFoXDTM5MTIwMTE1MTAz
MVowTDELMAkGA1UEBhMCQ0gxEDAOBgNVBAoMB1dJU2VLZXkxKzApBgNVBAMMIldJ
U2VLZXkgQ2VydGlmeUlEIEFkdmFuY2VkIEdCIENBIDIwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQDwUdXB1k9zlZo0+cuD72DSfubC02ybUHYvmX2Uo2aF
cGKpbHt1v3CTETe8ICkPjFV9TdAnfUqM4skAY2XiergGR9/TEsxzcqSSnPzcz5/S
lj8MtqVibiTUN9d7JtVZQrspxXAGzfkRaIwROb0BECQbkwMoObXwDpkvJ8Yyvqp/
D3Cw9vX/3cuqBs2l7Mdu0thRB97+HEE26H+zobQoUSfUwl0TfXQHYg+gC/dpXdA+
mtqliyFgWC1LQurLDIdodZsIszwbGx98brm7cENP7e/68wyZCndpzTDVgOB88liA
VHHVI2b8b0mA5uAgHsRtQkrJppMv1QTr9w1RBse6JwxNAgMBAAGjggFnMIIBYzBv
BggrBgEFBQcBAQRjMGEwOAYIKwYBBQUHMAKGLGh0dHA6Ly9wdWJsaWMud2lzZWtl
eS5jb20vY3J0L3djaWRwZ2JjYTEuY3J0MCUGCCsGAQUFBzABhhlodHRwOi8vb2Nz
cDIud2lzZWtleS5jb20vMB0GA1UdDgQWBBSgHLI/P2pKoL+Du/x5w6rLHd/edTAS
BgNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaAFNHmC4IldCUsVZHVAxh7v8Hu
```

rx2AME0GA1UdIARGMEQwOgYHYIV0BQ4HAzAvMC0GCCsGAQUFBwIBFiFodHRwOi8v
d3d3Lndpc2VrZXkuY29tL3JlcG9zaXRvcnkwBgYEVR0gADA9BgNVHR8ENjA0MDKg
MKAuhixodHRwOi8vcHVibGljLndpc2VrZXkuY29tL2NybC93Y2lkcGdiY2ExLmNy
bDAOBgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggEBAEu7VSijacp3unZ9
5qs+JktpDPjrUeQlNfidApMNtwWITCYqQxndQbuLGuuOLFizSZPJZH90a+I3bk3Q
ajZvlhAoVj38ajzT257l4y1S3dwJwxfcHOgSsa7+kCvCsOTI0OBxydEamoysajh9
N35jzPxZx1XKSwdUMitS/nwgbTVkV19K/Gjhi2zvbsivYHqi40lrwg0NHbO3Gx+A
FkCSxa3TG6QMoZtjaCXFaB7c/yuSQLfwJ1m99Q1tjKzqB+HhZLoKh6bwYUZ1qylU
Xhq6Lna0QiFhGKFFiQ/0C5mFhDBgSk9V7PyZYGYrW4jzhpDz/tQXmXNR0QVbzKrq
T8qLxE8=
-----END CERTIFICATE-----

CN=WISeKey CertifyID Advanced Services CA 4, OU=International, OU=Copyright (c) 2016 WISeKey SA, O=WISeKey, C=CH

Type	CA/QC
Status	undersupervision
Status starting time	2017-06-05T16:44:10.000Z

Service digital identity (X509)

Version	3
Serial number	273809063985261462945805
Signature algorithm	SHA256withRSA
Issuer	CN=OISTE WISeKey Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WISeKey, C=CH
Valid from	Wed Feb 10 11:53:24 PET 2016
Valid to	Fri Dec 11 11:09:51 PET 2037
Subject	CN=WISeKey CertifyID Advanced Services CA 4, OU=International, OU=Copyright (c) 2016 WISeKey SA, O=WISeKey, C=CH
Public key	Sun RSA public key, 2048 bits modulus: 22998960246314316614078373118493787911621436538469497722422881644910586 29473412439811514415394070640769245663880207278520336407266240756528546 68378412356543589409526435848576770842203379644687451353264590173585155 08131820053061012152391619805300786512120141537009441996913106171733916 14325596304477884726988185991654970457104161303022408796903823454613298 85588968448680719908527209845980625731237879035473503970231639929277231 97949683517759252197179235856321808442133657768184478293836128485387001 60866146406532753718398592607236390189313532386152808463998200805506049 32686141174983405210357448261431914462766949611 61 public exponent: 65537
Subject key identifier	f4e49b57d2aec29e884d00ba2baf65c963a9879b
CRL distribution points	http://public.wisekey.com/crl/owgrgaca.crl
Authority key identifier	041830168014b3037eae36bcb079d1dc9426b611be21b2698694
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=0
SHA1 Thumbprint	df02fbdea820ac7ed75e4befaea5097ea64401d2
SHA256 Thumbprint	41144bd4174c3152e1ca526f77d9f9ce89debc4eba6c778f815c21164b5101d3

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=WISeKey CertifyID Advanced Services CA 4, OU=International, OU=Copyright (c) 2016 WISeKey SA, O=WISeKey, C=CH
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
22998960246314316614078373118493787911621436538469497722422881644910586294734124398115144153940706407692456638802072785203364072662407565285466837841235654358940952643584857677084220337964468745135326459017358551150813182005306101215239161980530078651212014153700944199691310617173391614325596304477884726988185991654970457104161303022408796903823454613298855889684486807199085272098459806257312378790354735039702316399292772319794968351775925219717923585632180844213365776818447829383612848538700160866146406532757371839859260723639018931353238615280846399820080550604932686141174983405210357448261431914462766949611 61
 public exponent: 65537
 Validity: [From: Wed Feb 10 11:53:24 PET 2016,
             To: Fri Dec 11 11:09:51 PET 2037]
 Issuer: CN=OISTE WISeKey Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WISeKey, C=CH
 SerialNumber: [    39fb3817 00000000 000d]

Certificate Extensions: 9
```

```
[1]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://ocsp.wisekey.com/,
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://public.wisekey.com/crt/owgrgaca.crt]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: B3 03 7E AE 36 BC B0 79   D1 DC 94 26 B6 11 BE 21  ....6..y...&...!
0010: B2 69 86 94                                        .i..
]

]

[3]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: F4 E4 9B 57 D2 AE C2 9E   88 4D 00 BA 2B AF 65 C9  ...W.....M..+.e.
0010: 63 A9 87 9B                                        c...
]
]

[4]: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
Extension unknown: DER encoded OCTET string =
0000: 04 03 02 01 00                                     .....


[5]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.16.756.5.14.4.3.1]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 21 68 74 74 70 3A 2F   2F 77 77 77 2E 77 69 73  .!http://www.wis
0010: 65 6B 65 79 2E 63 6F 6D   2F 72 65 70 6F 73 69 74  ekey.com/reposit
0020: 6F 72 79                                           ory

]]  ]
 [CertificatePolicyId: [2.5.29.32.0]
[]  ]
]

[6]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:0
]

[7]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://public.wisekey.com/crl/owgrgaca.crl]
]]

[8]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[9]: ObjectId: 1.3.6.1.4.1.311.20.2 Criticality=false
Extension unknown: DER encoded OCTET string =
0000: 04 0C 1E 0A 00 53 00 75   00 62 00 43 00 41        .....S.u.b.C.A


]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 65 CC 7A 55 20 56 FB 72   5E 8B 0B 4C 34 AB 66 CF  e.zU V.r^..L4.f.
0010: 31 E8 9A 7F 23 5B 9C 66   4F 1C 9D 90 FC E9 C5 B8  1...#[.fO.......
0020: 4B AB 19 78 6D CD E9 6D   3E E8 C5 03 99 49 84 50  K..xm..m>....I.P
0030: 6C 29 69 B9 43 BB 8B 78   9D F7 2C BF 7E E1 45 4C  l)i.C..x..,...EL
0040: FF 23 62 72 D4 DC 60 36   8C A8 83 21 24 37 D2 55  .#br..`6...!$7.U
0050: 67 21 D3 31 B2 D5 33 FE   75 B3 CC 7E 0C F6 25 BA  g!.1..3.u.....%.
0060: A5 9E EA 37 E4 56 07 9C   A9 2D 04 EB BC 21 72 B9  ...7.V...-...!r.
0070: 23 60 E4 FD 6F 59 33 0F   DF 84 62 D7 2B D6 F3 15  #`..oY3...b.+...
0080: 6F 0E BD E8 E4 58 CE 9B   EA 4D 78 98 31 F7 E8 AE  o....X...Mx.1...
0090: 59 06 CF BE 9E E0 29 85   54 44 B0 CA A7 FF AA 4E  Y.....).TD.....N
00A0: B7 0B 5A D4 47 C4 ED 72   1C FE C1 FB 44 32 29 C6  ..Z.G..r....D2).
00B0: 7E D0 10 4A 80 71 6D FB   72 ED 25 BD 12 69 0C D9  ...J.qm.r.%..i..
00C0: 6B 7F A6 34 97 43 D1 D1   10 6A E5 1F C2 E1 D0 38  k..4.C...j.....8
00D0: CF 03 E7 2B 71 43 B3 98   21 21 E0 AC 9C 1E E7 49  ...+qC..!!.....I
00E0: B5 75 E6 18 A4 AE A5 89   FE 82 DD D4 F3 A7 49 E1  .u..........I.
00F0: 66 D0 C1 B2 B1 06 C5 B0   C9 BE AB 92 61 83 D4 DA  f...........a...

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIFNDCCBBygAwIBAgIKOfs4FwAAAAAADTANBgkqhkiG9w0BAQsFADCBijELMAkG
A1UEBhMCQ0gxEDAOBgNVBAoTB1dJU2VLZXkxGzAZBgNVBAsTEkNvcHlyaWdodCAo
YykgMjAwNTEiMCAGA1UECxMZT0lTVEUgRm91bmRhdGlvbiBFbmRvcnNlZDEoMCYG
A1UEAxMfT0lTVEUgV0lTZUtleSBHbG9iYWwgUm9vdCBHQSBDQTAeFw0xNjAyMTAx
NjUzMjRaFw0zNzEyMTExNjA5NTFaMIGSMQswCQYDVQQGEwJDSDEQMA4GA1UEChMH
V0lTZUtleTEmMCQGA1UECxMdQ29weXJpZ2h0IChjKSAyMDE2IFdJU2VLZXkgU0Ex
FjAUBgNVBAsTDUludGVybmF0aW9uYWwxMTAvBgNVBAMTKFdJU2VLZXkgQ2VydGlm
eUlEIEFkdmFuY2VkIFNlcnZpY2VzIENBIDQwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQC2L9X7Ban4aQ6ilphaaAFk5SCf+bnLfsdJdjzOYGexsY7ZIdiU
SyU6bx8u7AZ9InzYm/0AQ2+UfxhtO+hRpMMyF60zbIEEz8jF7+RFiZauM8Tu6GR+
t2+MEDVFzCRCiBVm6iCLusHQ6oBjbtzgNWeezKpXBW5f8e0GWmf05HtLw0m6050I
mk7I6+XYhRUruVWS1U8kQom1qXp86OoSS+eRqZAFiXB2h10A94wdrosHwl3vClBX
RF7pa+gK5j7bB5F9w4bWVX/a41J+Y8WihanlVASRkzhnt5Jf+cRBCOhppjt57uBv
OnpX9IHdv6KpWiB27ycmYQrXDJTEab6FFWwJAgMBAAGjggGQMIIBjDAOBgNVHQ8B
Af8EBAMCAQYwEAYJKwYBBAGCNxUBBAMCAQAwHQYDVR0OBBYEFPTkm1fSrsKeiE0A
uiuvZcljqYebME4GA1UdIARHMEUwOwYIYIV0BQ4EAwEwLzAtBggrBgEFBQcCARYh
aHR0cDovL3d3dy53aXNla2V5LmNvbS9yZXBvc2l0b3J5MAYGBFUdIAAwGQYJKwYB
BAGCNxQCBAweCgBTAHUAYgBDAEEwEgYDVR0TAQH/BAgwBgEB/wIBADAfBgNVHSME
GDAWgBSzA36uNrywedHclCa2Eb4hsmmGlDA7BgNVHR8ENDAyMDCgLqAshipodHRw
Oi8vcHVibGljLndpc2VrZkuY29tL2NybC9vd2dyZ2FjYS5jcmwwbAYIKwYBBQUH
AQEEYDBeMCQGCCsGAQUFBzABhhhodHRwOi8vb2NzcC53aXNla2V5LmNvbS8wNgYI
KwYBBQUHMAKGKmh0dHA6Ly9wdWJsaWMud2lzZWtleS5jb20vY3J0L293Z3JnYWNh
LmNydDANBgkqhkiG9w0BAQsFAAOCAQEAZcx6VSBW+3JeiwtMNKtmzzHomn8jW5xm
TxydkPzpxbhLqxl4bc3pbT7oxQOZSYRQbClpuUO7i3id9yy/fuFFTP8jYnLU3GA2
jKiDISQ30lVnIdMxstUz/nWzzH4M9iW6pZ7qN+RWB5ypLQTrvCFyuSNg5P1vWTMP
34Ri1yvW8xVvDr3o5FjOm+pNeJgx9+iuWQbPvp7gKYVURLDKp/+qTrcLWtRHxO1y
HP7B+0QyKcZ+0BBKgHFt+3LtJb0SaQzZa3+mNJdD0dEQauUfwuHQOM8D5ytxQ7OY
ISHgrJwe50m1deYYpK6lif6C3dTzp0nhZtDBsrEGxbDJvquSYYPU2g==
-----END CERTIFICATE-----
```


CN=WISeKey CertifyID Advanced Services CA 2, OU=International, OU=Copyright 2011 WISeKey SA, O=WISeKey, C=CH

Type	CA/QC
Status	undersupervision
Status starting time	2011-10-27T23:27:04.000Z
Service digital identity (X509)	
Version	3
Serial number	246007577873566738153498
Signature algorithm	SHA1withRSA
Issuer	CN=WISeKey CertifyID Advanced G1 CA, OU=International, OU=Copyright (c) 2005 WISeKey SA, O=WISeKey, C=CH
Valid from	Wed Feb 09 10:37:32 PET 2011
Valid to	Fri Dec 11 13:00:47 PET 2020
Subject	CN=WISeKey CertifyID Advanced Services CA 2, OU=International, OU=Copyright 2011 WISeKey SA, O=WISeKey, C=CH
Public key	Sun RSA public key, 2048 bits modulus: 24288478345426820300170647212650028183209172240700549408406936117107702 74803850970162639301987931305064120330877556637836770761441159944800058 00067422341275647291578062728338789257749837629581788260245742338557110 44851430752958107675122050547567033550120802632908841908516336065559667 07107256996505788105039037018831615858096998713437400310144168979735425 16413296476970768525294161764162278363174487117866772958700346310703729 20537492494984080471754795473983145338817813850123814149393750660160797 19937286155714212533310814218301260455793041747081866702681435953380525 32794754874642595511065305602202720676304868432 59 public exponent: 65537
Subject key identifier	d72f2ff309f15621531de74c2e48444ada86fd98
CRL distribution points	http://public.wisekey.com/crl/wcidag1ca.crl
Authority key identifier	041830168014501f30c093928d712338345cb90af6d32beb8145
Key usage	digitalSignature keyCertSign cRLSign
Basic constraints	CA=true; PathLen=0
SHA1 Thumbprint	0497a10d775e09873ba6ff84d7799cf3d7e0a1a9
SHA256 Thumbprint	0ad741d98a84c3b9c4e7552e15bff1e369b6806839455dbafcac638124d5f100

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=WISeKey CertifyID Advanced Services CA 2, OU=International, OU=Copyright 2011 WISeKey SA, O=WISeKey, C=CH
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 2048 bits
 modulus:
2428847834542682030017064721265002818320917224070054940840693611710770274803850970162639301987931305064120330877556637836770761441159944800058000674223412756472915780627283387892577498376295817882602457423385571104485143075295810767512205054756703355012080263290884190851633606555966707107256996505788105039037018831615858096998713437400310144168979735425164132964769707685252941617641622783631744871178667729587003463107037292053749249498408047175479547398314533881781385012381414939375066016079719937286155714212533310814218301260455793041747081866702681435953380525327947548746425955110653056022027206763048684325 9
 public exponent: 65537
 Validity: [From: Wed Feb 09 10:37:32 PET 2011,
             To: Fri Dec 11 13:00:47 PET 2020]
 Issuer: CN=WISeKey CertifyID Advanced G1 CA, OU=International, OU=Copyright (c) 2005 WISeKey SA, O=WISeKey, C=CH
 SerialNumber: [    341818f7 00000000 001a]

Certificate Extensions: 9
[1]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://public.wisekey.com/crt/wcidag1ca.crt]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 50 1F 30 C0 93 92 8D 71   23 38 34 5C B9 0A F6 D3  P.0....q#84\....
0010: 2B EB 81 45                                        +..E
]

]

[3]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: D7 2F 2F F3 09 F1 56 21   53 1D E7 4C 2E 48 44 4A  .//...V!S..L.HDJ
0010: DA 86 FD 98                                        ....
]
]

[4]: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
Extension unknown: DER encoded OCTET string =
0000: 04 03 02 01 00                                     .....


[5]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.16.756.5.14.4.3.1]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 21 68 74 74 70 3A 2F   2F 77 77 77 2E 77 69 73  .!http://www.wis
0010: 65 6B 65 79 2E 63 6F 6D   2F 72 65 70 6F 73 69 74  ekey.com/reposit
0020: 6F 72 79                                           ory

]]  ]
 [CertificatePolicyId: [2.5.29.32.0]
[]  ]
]

[6]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:0
]

[7]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://public.wisekey.com/crl/wcidag1ca.crl]
]]

[8]: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
 DigitalSignature
 Key_CertSign
 Crl_Sign
]

[9]: ObjectId: 1.3.6.1.4.1.311.20.2 Criticality=false
Extension unknown: DER encoded OCTET string =
0000: 04 0C 1E 0A 00 53 00 75   00 62 00 43 00 41        .....S.u.b.C.A


]
 Algorithm: [SHA1withRSA]
 Signature:
0000: 94 41 DA BA A0 C9 2A 5C   52 F2 0A C0 51 E3 5E 13  .A....*\R...Q.^.
0010: A8 1C E6 C3 02 26 FB 79   A1 2A DB AA A8 5D F9 B5  .....&.y.*...]..
0020: 6C 18 1A 0B B9 EB 78 F8   06 CB 9D 82 15 C7 F6 C5  l.....x.........
```

```
0030: 6C CC C1 14 D6 75 6C DC   0C 43 B8 2E A9 7B 37 7D  l....ul..C....7.
0040: 32 10 4E D8 D3 E3 2C 8B   F7 49 B1 2C F0 48 07 8D  2.N...,..I.,.H..
0050: FB 82 5A C9 1C E7 29 1E   5C D6 59 59 19 00 64 35  ..Z...).\.YY..d5
0060: 01 1A 65 5E A3 BF 5D EF   98 19 3E 39 63 08 6F 2A  ..e^..]...>9c.o*
0070: 16 5A 14 6D 30 B7 60 A4   8C 03 49 E1 19 F8 10 20  .Z.m0.`...I....
0080: 60 13 8C 03 7C 7C B3 80   D6 D1 7A D7 5B 70 14 92  `.....|.|.....z.[p..
0090: 57 D6 07 62 A0 3A 2E 82   9E 5C A5 23 F0 44 98 60  W..b.:...\.#.D.`
00A0: E2 3D 50 81 4E D2 29 83   E6 04 EC D2 51 5B 57 31  .=P.N.).....Q[W1
00B0: 13 F2 BF C6 62 10 ED BC   14 E3 6B 51 62 09 66 99  ....b.....kQb.f.
00C0: E9 85 2F AD 51 07 5C AF   CA A3 9E 5A A7 84 DE C5  ../.Q.\....Z....
00D0: A4 41 4E 2D AA 1A CA B1   6B 59 53 34 68 C8 1C 12  .AN-....kYS4h...
00E0: 35 B5 1B 2E C0 6C 07 66   91 2C 62 ED E8 E7 1B A7  5....l.f.,b.....
00F0: F0 D4 A5 FD BE 25 36 43   6A 04 D6 9A 25 74 3B 0A  .....%6Cj...%t;.

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIFCTCCA/GgAwIBAgIKNBgY9wAAAAAAGjANBgkqhkiG9w0BAQUFADCBijELMAkG
A1UEBhMCQ0gxEDAOBgNVBAoTB1dJU2VLZXkxJjAkBgNVBAsTHUNvcHlyaWdodCAo
YykgMjAwNSBXSVNlS2V5IFNBMRYwFAYDVQQLEw1JbnRlcm5hdGlvbmFsMSkwJwYD
VQQDEyBXSVNlS2V5IENlcnRpZnlJRCBBZHZhbmNlZCBHMSBDQTAeFw0xMTAyMDkx
NTM3MzJaFw0yMDEyMTExODAwNDdaMIGOMQswCQYDVQQGEwJDSDEQMA4GA1UEChMH
V0lTZUtleTEiMCAGA1UECxMZQ29weXJpZ2h0IDIwMTEgV0lTZUtleSBTQTEWMBQG
A1UECxMNSW50ZXJuYXRpb25hbDExMC8GA1UEAxMoV0lTZUtleSBDZXJ0aWZ5SUQg
QWR2YW5jZWQgU2VydmljZXMgQ0EgMjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAMBm3QJR+dIYJ/RKHG5W1vmQKyihHp6dcClZ26FjcNTx/gArnGaJFb3/
JbC6wbT1pcD5eyeVAgp8Xss0OCOXr6EAhfE+M47JLgNRessR31PVDSEaalBIuMS5
ZlfcJEZ/AhTwtZ+KtJdp59F1OPL9uYcZSsIFB5eLJy5TlK6rJM6cCD8QBeDW98rH
2gOY0QXiJkGAn2LRV1TrOOPAkZ5l1fLQ8y9Eb7XaWRC4ycywjkB0Tw184ODQH8bQ
ToIE3+U62bsUSFg4pkIAouxhyozNyBKHvPXz0MKiB+/QVpBwykEIrE/Mb7C/rATw
VsMqNKQFdQW1bAfxKFNUz7eJSX/873sCAwEAAaOCAWkwggFlMBIGA1UdEwEB/wQI
MAYBAf8CAQAwHQYDVR0OBBYEFNcvL/MJ8VYhUx3nTC5IRErahv2YMAsGA1UdDwQE
AwIBhjAQBgkrBgEEAYI3FQEEAwIBADBOBgNVHSAERzBFMDsGCGCFdAUOBAMBMC8w
LQYIKwYBBQUHAgEWIWh0dHA6Ly93d3cud2lzZWtleS5jb20vcmVwb3NpdG9yeTAG
BgRVHSAAMBkGCSsGAQQBgjcUAgQMHgoAUwB1AGIAQwBBMB8GA1UdIwQYMBaAFFAf
MMCTko1xIzg0XLkK9tMr64FFMDwGA1UdHwQ1MDMwMaAvoC2GK2h0dHA6Ly9wdWJs
aWMud2lzZWtleS5jb20vY3JsL3djaWRhZzFjYS5jcmwwRwYIKwYBBQUHAQEEOzA5
MDcGCCsGAQUFBzAChitodHRwOi8vcHVibGljLndpc2VrZXkuY29tL2NydC93Y2lk
YWcxY2EuY3J0MA0GCSqGSIb3DQEBBQUAA4IBAQCUQdq6oMkqXFLyCsBR414TqBzm
wwIm+3mhKtuqqF35tWwYGgu563j4BsudghXH9sVszMEU1nVs3AxDuC6pezd9MhBO
2NPjLIv3SbEs8EgHjfuCWskc5ykeXNZZWRkAZDUBGmVeo79d75gZPjljCG8qFloU
bTC3YKSMA0nhGfgQIGATjAN8fLOA1tF611twFJJX1gdioDougp5cpSPwRJhg4j1Q
gU7SKYPmBOzSUVtXMRPyv8ZiEO28FONrUWIJZpnphS+tUQdcr8qjnlqnhN7FpEFO
LaoayrFrWVM0aMgcEjW1Gy7AbAdmkSxi7ejnG6fw1KX9viU2Q2oE1poldDsK
-----END CERTIFICATE-----
```

CN=OISTE WISeKey Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WISeKey, C=CH

Type	CA/QC
Status	undersupervision
Status starting time	2011-10-19T22:03:21.000Z

Service digital identity (X509)

Version	3
Serial number	867188778711331590900805559118235483 14
Signature algorithm	SHA1withRSA
Issuer	CN=OISTE WISeKey Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WISeKey, C=CH
Valid from	Sun Dec 11 11:03:44 PET 2005
Valid to	Fri Dec 11 11:09:51 PET 2037
Subject	CN=OISTE WISeKey Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WISeKey, C=CH
Public key	Sun RSA public key, 2048 bits modulus: 25665677062212238926425337868672790984523975826397568772898393679835223792153614724762740678604367146408964988667765557243033332178811994430318219268013722781103894177164275471652790891504767126316554543949167872658969863516618824989331325931780164035733540663902032602128347596286518566584151611317161853994959558560371644489493985276200542872135499524906266101570594184350439825376600594334041210551635356267876550219526079884846250242014323238477351950638683648063570726696890119634093256994831495514930650585834843321731988150901499839807631719357367983669218163461065125420004275703859743682152491140031902515461 public exponent: 65537
Subject key identifier	b3037eae36bcb079d1dc9426b611be21b2698694

Key usage	digitalSignature keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	5922a1e15aea163521f898396a4646b0441b0fa9
SHA256 Thumbprint	41c923866ab4cad6b7ad578081582e020797a6cbdf4fff78ce8396b38937d7f5

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=OISTE WISeKey Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WISeKey, C=CH
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 2048 bits
 modulus:
25665677062212238926425337868672790984523975826397568772898393679835223792153614724762740678604367146408964988667765557243033332178811994430318219268013722781103894177164275
47165279089150476712631655454394916787265896986351661882498933132593178016403573354066390203260212834759628651856658415161131716185399495955856037164448949398527620054287213
54995249062661015705941843504398253766005943340412105516353562678765502195260798848462502420143232384773519506386836480635707266968901196340932569948314955149306505858348433
21731988150901499839807631719357367983669218163461065125420004275038597436821524911400319025154 61
 public exponent: 65537
 Validity: [From: Sun Dec 11 11:03:44 PET 2005,
             To: Fri Dec 11 11:09:51 PET 2037]
 Issuer: CN=OISTE WISeKey Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WISeKey, C=CH
 SerialNumber: [    413d72c7 f46b1f81 437df1d2 2854df9a]

Certificate Extensions: 4
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: B3 03 7E AE 36 BC B0 79   D1 DC 94 26 B6 11 BE 21  ....6..y...&...!
0010: B2 69 86 94                                        .i..
]
]

[2]: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
 DigitalSignature
 Key_CertSign
 Crl_Sign
]

[3]: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
Extension unknown: DER encoded OCTET string =
0000: 04 03 02 01 00                                     .....


[4]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: 4B A1 FF 0B 87 6E B3 F9   C1 43 B1 48 F3 28 C0 1D  K....n...C.H.(..
0010: 2E C9 09 41 FA 94 00 1C   A4 A4 AB 49 4F 8F 3D 1E  ...A.......IO.=.
0020: EF 4D 6F BD BC A4 F6 F2   26 30 C9 10 CA 1D 88 FB  .Mo.....&0......
0030: 74 19 1F 85 45 BD B0 6C   51 F9 36 7E DB F5 4C 32  t...E..lQ.6...L2
0040: 3A 41 4F 5B 47 CF E8 0B   2D B6 C4 19 9D 74 C5 47  :AO[G...-....t.G
0050: C6 3B 6A 0F AC 14 DB 3C   F4 73 9C A9 05 DF 00 DC  .;j....<.s......
0060: 74 78 FA F8 35 60 59 02   13 18 7C BC FB 4D B0 20  tx..5`Y......M.
0070: 6D 43 BB 60 30 7A 67 33   5C C5 99 D1 F8 2D 39 52  mC.`0zg3\....-9R
0080: 73 FB 8C AA 97 25 5C 72   D9 08 1E AB 4E 3C E3 81  s....%\r....N<..
0090: 31 9F 03 A6 FB C0 FE 29   88 55 DA 84 D5 50 03 B6  1......).U...P..
00A0: E2 84 A3 A6 36 AA 11 3A   01 E1 18 4B D6 44 68 B3  ....6..:...K.Dh.
00B0: 3D F9 53 74 84 B3 46 91   46 96 00 B7 80 2C B6 E1  =.St..F.F....,..
00C0: E3 10 E2 DB A2 E7 28 8F   01 96 62 16 3E 00 E3 1C  ......(...b.>...
00D0: A5 36 81 18 A2 4C 52 76   C0 11 A3 6E E6 1D BA E3  .6...LRv...n....
00E0: 5A BE 36 53 C5 3E 75 8F   86 69 29 58 53 B5 9C BB  Z.6S.>u..i)XS...
00F0: 6F 9F 5C C5 18 EC DD 2F   E1 98 C9 FC BE DF 0A 0D  o.\..../........

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIID8TCCAtmgAwIBAgIQQT1yx/RrH4FDffHSKFTfmjANBgkqhkiG9w0BAQUFADCB
ijELMAkGA1UEBhMCQ0gxEDAOBgNVBAoTB1dJU2VLZXkxGzAZBgNVBAsTEkNvcHly
aWdodCAoYykgMjAwNTEiMCAGA1UECxMZT0lTVEUgRm91bmRhdGlvbiBFbmRvcnNl
ZDEoMCYGA1UEAxMfT0lTVEUgV0lTZUtleSBHbG9iYWwgUm9vdCBHQSBDQTAeFw0w
NTEyMTExNjAzNDRaFw0zNzEyMTExNjA5NTFaMIGKMQswCQYDVQQGEwJDSDEQMA4G
A1UEChMHV0lTZUtleTEbMBkGA1UECxMSQ29weXJpZ2h0IChjKSAyMDA1MSIwIAYD
VQQLExlPSVNURSBGb3VuZGF0aW9uIEVuZG9yc2VkMSgwJgYDVQQDEx9PSVNURSBX
SVNlS2V5IEdsb2JhbCBSb290IEdBIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAy0+zAJs9Nt350UlqaxBJH+zYK7LG+DKBKUOVTJoZIyEVRd7jyBxR
VVuuk+g3/ytr6dTqvirdqFEr12bDYVxgAsj1znJ7O7jyTmUIms2kahnBAbtzptf2
w93NvKSLtZlhuAGio9RN1AU9ka34tAhxZK9w8Rxrfvb Dd50kc3vkDIzh2TbhmYsF
```

mQvtRTEJysIA2/dyoJaqlYfQjse2YXMNdmaM3Bu0Y6Kff5MTMPGhJ9vZ/yxViJGg
4E8HsChWjBgbl0SOid3gF27nKu+POQoxhILYQBRJLnpB5Kf+42TMwVlxSywhp1t9
4B3RLoGbw9ho972WG6xwsRYUC9tguSYBBQIDAQABo1EwTzALBgNVHQ8EBAMCAYYw
DwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUswN+rja8sHnR3JQmthG+IbJphpQw
EAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEFBQADggEBAEuh/wuHbrP5wUOx
SPMowB0uyQlB+pQAHKSkq0lPjz0e701vvbyk9vImMMkQyh2I+3QZH4VFvbBsUfk2
ftv1TDI6QU9bR8/oCy22xBmddMVHxjtqD6wU2zz0c5ypBd8A3HR4+vg1YFkCExh8
vPtNsCBtQ7tgMHpnM1zFmdH4LTlSc/uMqpclXHLZCB6rTjzjgTGfA6b7wP4piFXa
hNVQA7bihKOmNqoROgHhGEvWRGizPflTdISzRpFGlgC3gCy24eMQ4tui5yiPAZZi
Fj4A4xylNoEYokxSdsARo27mHbrjWr42U8U+dY+GaSlYU7Wcu2+fXMUY7N0v4ZjJ
/L7fCg0=
-----END CERTIFICATE-----

Certificate Service Provider Name (en): COMODO CA

Trade name (en)	COMODO CA
Information URI (en)	HTTP://WWW.COMODO.COM
Service provider street address (es)	3RD FLOOR, 26 OFFICE VILLAGE, EXCHANGE QUAY, TRAFFORD ROAD
Service provider street address (en)	3RD FLOOR, 26 OFFICE VILLAGE, EXCHANGE QUAY, TRAFFORD ROAD
Service provider postal code (es)	M53EQ
Service provider postal code (en)	M53EQ
Service provider locality (es)	SALFORD
Service provider locality (en)	SALFORD
Service provider state (es)	GREATER MANCHESTER
Service provider state (en)	GREATER MANCHESTER
Service provider country (es)	GB
Service provider country (en)	GB

CN=COMODO SHA-256 Client Authentication and Secure Email CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB

Type	CA/QC
Status	undersupervision
Status starting time	2015-05-26T16:27:18.000Z

Service digital identity (X509)

Version	3
Serial number	297932920444540322541367631881431378721
Signature algorithm	SHA256withRSA
Issuer	CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
Valid from	Sun Dec 21 19:00:00 PET 2014
Valid to	Sat May 30 05:48:38 PET 2020
Subject	CN=COMODO SHA-256 Client Authentication and Secure Email CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB

Public key	Sun RSA public key, 2048 bits modulus: 17381956418472897693969508582162636024071659346032269263382920739842150 46927852583721629177141067585711669815205981016630186318209317314096541 07720087605003458793700292047194169818313172767256880241716377274896565 13268578962317477213526962462814834799916604856420564188483147729326012 68887050317289933363413210836814144588908306807619551332068593151938913 24046887022413555455855897507018984996629041020918774445528628794543541 14087477024339081277305067166369850131192375668524023885103462072163379 93341532819217188097696906154184879163683035610752922252847847628488563 50803535820583870169556782313076212691127154529 61 public exponent: 65537
Subject key identifier	92616b82e1a2a0aa4fec67f1c2a3f7b48000c1ec
CRL distribution points	http://crl.usertrust.com/AddTrustExternalCARoot.crl
Authority key identifier	041830168014adbd987a34b426f7fac42654ef03bde024cb541a
Key usage	digitalSignature keyCertSign cRLSign
Basic constraints	CA=true; PathLen=0
SHA1 Thumbprint	59b825fc08860b04b392cc25fec48c760753b689
SHA256 Thumbprint	5344871d8e168212539644f9aa081b78fff2179950145ac0e4ebfcd037fb04f4

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=COMODO SHA-256 Client Authentication and Secure Email CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
17381956418472897693969508582162636024071659346032269263382920739842150467927852583721629177141067585711669815205981016630186318209317314096541077200876050034587937002920471941698183131727672568802417163772748965651326857896231747721352696246281483479991660485642056418848314772932601268887050317289933363413210836814144588908306807619551332068593151938913240468870224135554558558975070189849966290410209187744455286279454354114087477024339081277305067166369850131192375668524023885103462072163379933415328192171880976969061541848791636830356107529222528478476284885639
 public exponent: 65537
 Validity: [From: Sun Dec 21 19:00:00 PET 2014,
             To: Sat May 30 05:48:38 PET 2020]
 Issuer: CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
 SerialNumber: [    e023cb15 12835389 ad616e7a 54676b21]

Certificate Extensions: 8
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 92 61 6B 82 E1 A2 A0 AA   4F EC 67 F1 C2 A3 F7 B4  .ak.....O.g.....
0010: 80 00 C1 EC                                        ....
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: AD BD 98 7A 34 B4 26 F7   FA C4 26 54 EF 03 BD E0  ...z4.&...&T....
0010: 24 CB 54 1A                                        $.T.
]

]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.usertrust.com/AddTrustExternalCARoot.crl]
]]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[]  ]
]

[5]: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
 clientAuth
 emailProtection
]

[6]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 DigitalSignature
```

```
 Key_CertSign
 Crl_Sign
]

[7]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://ocsp.usertrust.com]
]

[8]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:0
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 1B 2A 6E AC 55 C1 3A AB   88 C5 D8 ED CD 55 F3 AA  .*n.U.:......U..
0010: 6B 61 2B C0 09 10 23 99   0F C5 66 6A 6F B1 F5 B4  ka+...#...fjo...
0020: B5 77 5E 0F 02 61 00 DF   7D 05 FE 12 B3 A4 80 80  .w^..a..........
0030: 00 FC FB 1D 5B 6A 72 02   0A 41 BC 05 BA C1 58 D5  ....[jr..A....X.
0040: 26 C2 EA D5 4D 84 FB FE   82 98 CF 58 1B E3 22 63  &...M......X.."c
0050: 9C 52 F8 BB 05 36 AB 7D   58 A5 DE AB 3B 63 E5 DA  .R...6..X...;c..
0060: D5 73 EF EC E0 FB 7B E2   A3 FF F0 42 23 9C CA B6  .s.........B#...
0070: 8D 4D 3E E4 4B 18 03 B2   A8 2D D4 D8 BB 42 4B 90  .M>.K....-...BK.
0080: 69 85 10 DB A6 37 34 E8   7B E0 01 10 A5 9C CA 3A  i....74........:
0090: C7 9F 4F 88 34 6E 8A 65   D0 1A 8A BB A9 DC CA CA  ..O.4n.e........
00A0: 36 D1 F4 FC C2 64 29 35   AF D6 B1 A7 71 11 D2 03  6....d)5....q...
00B0: 43 B1 8F 3E 9A EC 9E 32   53 F4 76 92 CA 86 34 07  C..>...2S.v...4.
00C0: B9 2C CA E6 1C 4A D8 99   0D C1 86 E2 90 92 FB 5A  .,...J.........Z
00D0: 42 6A 23 21 10 E9 65 C7   F5 D5 BB 7E EA 8C 85 20  Bj#!..e........
00E0: 02 62 EA D1 3A 07 2C 59   C5 99 33 F2 38 89 E5 B6  .b..:.,Y..3.8...
00F0: E9 16 7A 1F 79 14 F6 4A   10 1A 26 FA 7C 8A FB 9B  ..z.y..J..&.....

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIErzCCA5egAwIBAgIRAOAjyxUSg1OJrWFuelRnayEwDQYJKoZIhvcNAQELBQAw
bzELMAkGA1UEBhMCU0UxFDASBgNVBAoTC0FkZFRydXN0IEFCMSYwJAYDVQQLEx1B
ZGRUcnVzdCBFeHRlcm5hbCBUVFAgTmV0d29yazEiMCAGA1UEAxMZQWRkVHJ1c3Qg
RXh0ZXJuYWwgQ0EgUm9vdDAeFw0xNDEyMjIwMDAwMDBaFw0yMDA1MzAxMDQ4Mzha
MIGbMQswCQYDVQQGEwJHQjEbMBkGA1UECBMSR3JlYXRlciBNYW5jaGVzdGVyMRAw
DgYDVQQHEwdTYWxmb3JkMRowGAYDVQQKExFDT01PRE8gQ0EgTGltaXRlZDFBMD8G
A1UEAxM4Q09NT0RPIFNIQS0yNTYgQ2xpZW50IEF1dGhlbnRpY2F0aW9uIGFuZCBT
ZWN1cmUgRW1haWwgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCJ
sQ3aelMZTnBSHbxWpgYmt7hJ4JbnUavx8FoTSRWjtIwbYLx6UUKneYykIt8XYU6R
1XYjChTTSgJ/th0JgG6lBD3ZursW/qGHqS5DUkMWfK8yUMimT1rpCNjPkyWce4jo
MGTmpPhWgP0qJBQzF5msROVpi6NGBkvCM9TpQJ8GsLGsk0C5tQiTOpwqU6MQ2z0g
YTxVA47ZTnYlAiEp+qN8cXZP7uFfgen7VIDbw3s1UreE3iI9LDAtMX9ZvVI3sDNp
LUPr+tal8Zd3Z1GM2e4n67ylBzh2jKSpOP/fjPUDrEm+yvdzmToPMquclToTPQ5G
Old0YVC+xkA/y+Tin6IhAgMBAAGjggEXMIIBEzAfBgNVHSMEGDAWgBStvZh6NLQm
9/rEJlTvA73gJMtUGjAdBgNVHQ4EFgQUkmFrguGioKpP7GfxwqP3tIAAwewwDgYD
VR0PAQH/BAQDAgGGMBIGA1UdEwEB/wQIMAYBAf8CAQAwHQYDVR0lBBYwFAYIKwYB
BQUHAwIGCCsGAQUFBwMEMBEGA1UdIAQKMAgwBgYEVR0gADBEBgNVHR8EPTA7MDmg
N6A1hjNodHRwOi8vY3JsLnVzZXJ0cnVzdC5jb20vQWRkVHJ1c3RFeHRlcm5hbENB
Um9vdC5jcmwwNQYIKwYBBQUHAQEEKTAnMCUGCCsGAQUFBzABhhlodHRwOi8vb2Nz
cC51c2VydHJ1c3QuY29tMA0GCSqGSIb3DQEBCwUAA4IBAQAbKm6sVcE6q4jF2O3N
VfOqa2ErwAkQI5kPxWZqb7H1tLV3Xg8CYQDffQX+ErOkgIAA/PsdW2pyAgpBvAW6
wVjVJsLq1U2E+/6CmM9YG+MiY5xS+LsFNqt9WKXeqztj5drVc+/s4Pt74qP/8EIj
nMq2jU0+5EsYA7KoLdTYu0JLkGmFENumNzToe+ABEKWcyjrHn0+ING6KZdAairup
3MrKNtH0/MJkKTWv1rGncRHSA0Oxjz6a7J4yU/R2ksqGNAe5LMrmHErYmQ3BhuKQ
kvtaQmojIRDpZcf11bt+6oyFIAJi6tE6ByxZxZkz8jiJ5bbpFnofeRT2ShAaJvp8
ivub
-----END CERTIFICATE-----
```

CN=COMODO Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB

Type	CA/QC
Status	undersupervision
Status starting time	2012-03-20T15:25:27.000Z

Service digital identity (X509)

Version	3
Serial number	433908180328428185406354883091244892 34
Signature algorithm	SHA1withRSA
Issuer	CN=COMODO Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
Valid from	Fri Dec 31 19:00:00 PET 2010
Valid to	Tue Dec 31 18:59:59 PET 2030

Subject	CN=COMODO Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
Public key	Sun RSA public key, 2048 bits modulus: 26289395806318381231692261863750242292037560230101026221289605413810223 12391137129643347841898046763569002755778666260558750066381003035515686 00382145246656294294911839047616598043405957853074035084659771952441464 50258342619785062327256172269584127117720656015993450905176834046100109 53270431696513519356433527274923661810035291369082738108001201526306613 39792683744834685477466252935847104367829705960299566072962573971128784 88296778798242823077976044671664128062033831583733197184764809865978613 13597246609316367464960423824590420063072815179756696697895087682210709 38158100443669278281043684294736378120564613547 43 public exponent: 65537
Subject key identifier	0b58e58bc64c1537a440a930a921be47365a56ff
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	ee869387fffd8349ab5ad14322588789a457b012
SHA256 Thumbprint	1a0d20445de5ba1862d19ef880858cbce50102b36e8f0a040c3c69e74522fe6e

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=COMODO Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 2048 bits
 modulus:
26289395806318381231692261863750242292037560230101026221289605413810223123911371296433478418980467635690027557786662605587500663810030355156860038214524665629429491183904761659804340595785307403508465977195244146450258342619785062327256172269584127117720656015993450905176834046100109532704316965135193564335272749236618100352913690827381080012015263066133979268374483468547746625293584710436782970596029956607296257397112878488296778798242823077976044671664128062033831583733197184764809865978613135972466093163674649604238245904200630728151797566966978950876822107093815810044366927828104368429473637812056461354743
 public exponent: 65537
 Validity: [From: Fri Dec 31 19:00:00 PET 2010,
             To: Tue Dec 31 18:59:59 PET 2030]
 Issuer: CN=COMODO Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
 SerialNumber: [    20a4c47f dddfe1c7 53630713 88776012]

Certificate Extensions: 3
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 0B 58 E5 8B C6 4C 15 37   A4 40 A9 30 A9 21 BE 47  .X...L.7.@.0.!.G
0010: 36 5A 56 FF                                        6ZV.
]
]

[2]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[3]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: 2F C9 C4 1C 07 3B CF 61   02 00 B1 D9 21 51 75 72  /....;.a....!Qur
0010: 03 30 B0 C4 16 1F 6C 00   8B 10 AC AF F1 47 D4 AE  .0....l......G..
0020: 10 3C 0C 1A F8 D4 93 6C   AC 10 37 7C B7 A6 83 64  .<.....l..7....d
0030: AD CD DF 0E 87 33 9D 37   B0 C6 7B 38 72 B1 F3 1A  .....3.7...8r...
0040: 0E A3 F9 55 7A 6D 03 66   03 17 95 4A F1 B1 7A DF  ...Uzm.f...J..z.
0050: 56 21 06 42 8F B1 D3 A8   85 DE EE 97 1D 62 EB A7  V!.B.........b..
0060: E7 31 12 66 C3 0F A6 4B   2E 41 82 F7 FD C9 1B A8  .1.f...K.A......
0070: 1B AF EE 3C CE E3 9C AE   28 07 A1 2C 9B 24 C2 0F  ...<....(..,.$..
0080: 23 26 83 32 8B 86 0F 1F   2B 12 46 25 16 8F 76 90  #&.2....+.F%..v.
0090: 03 6B DE BC AA 22 68 6B   8C A1 AC 2B 11 39 A6 DB  .k..."hk...+.9..
00A0: 70 C2 7D 72 E9 33 E7 FC   26 F1 74 5A 91 E6 9D 84  p..r.3..&.tZ....
00B0: AC F8 A8 06 19 46 E6 A7   E9 AA 34 22 A4 A1 9F 7A  .....F....4"...z
00C0: AD B7 B2 A4 9A 33 88 71   02 3C 2E D6 7A B2 1F A2  .....3.q.<..z...
00D0: CA C0 DD 2F 10 94 FD B3   8C 84 20 79 46 D5 05 D4  .../...... yF...
00E0: 10 E4 D2 DB 64 4F B8 5B   EE 1B C5 20 47 5B 94 AB  ....dO.[... G[..
00F0: 6E D4 95 33 1D A6 15 71   F1 F8 94 CA 54 39 3E C1  n..3...q....T9>.

]
```

The certificate in PEM format:


```
-----BEGIN CERTIFICATE-----
MIID0DCCArigAwIBAgIQIKTEf93f4cdTYwcTiHdgEjANBgkqhkiG9w0BAQUFADCB
gTELMAkGA1UEBhMCR0IxGzAZBgNVBAgTEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4G
A1UEBxMHU2FsZm9yZDEaMBgGA1UEChMRQ09NT0RPIENBIExpbWl0ZWQxJzAlBgNV
BAMTHkNPTU9ETyBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAeFw0xMTAxMDEwMDAw
MDBaFw0zMDEyMzEyMzU5NTlaMIGBMQswCQYDVQQGEwJHQjEbMBkGA1UECBMSR3Jl
YXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHEwdTYWxmb3JkMRowGAYDVQQKExFDT01P
RE8gQ0EgTGltaXRlZDEnMCUGA1UEAxMeQ09NT0RPIENlcnRpZmljYXRpb24gQXV0
aG9yaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0ECLi3LjkRv3
UcEbVASY06m/weaKXTuH+7uIzg3jLz8GlvCiKVCZrts7oVewdFFxze1CkU1B/qnI
2GqGd0S7WWaXUF601CxwRM/aN5VCaTwwxHGzUvAhTaHYujl8HJ6jJJ3ygxaYqhZ8
Q5sVW7euNJH+1GImGEaaP+vB+fGQV+useg2L23IwambV4EajcNxo2f8ESIl33rXp
+2dtQem8Ob0y2WIC8bGoPW43nOIv4tOiJovGuFVDiOEjPqXSJDlqR6sA1KGzqSX+
DT+nHbrTUcELpNqsOO9VUCQFZUaTNE8tja3G1CEZ0o7KBWFxB3NH5YoZEr0ETc5O
nKVIrLsm9wIDAQABo0IwQDAdBgNVHQ4EFgQUC1jli8ZMFTekQKkwqSG+RzZaVv8w
DgYDVR0PAQH/BAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQEFBQAD
ggEBAC/JxBwHO89hAgCx2SFRdXIDMLDEFh9sAIsQrK/xR9SuEDwMGvjUk2ysEDd8
t6aDZK3N3w6HM503sMZ7OHKx8xoOo/lVem0DZgMXlUrxsXrfViEGQo+x06iF3u6X
HWLrp+cxEmbDD6ZLLkGC9/3JG6gbr+48zuOcrigHoSybJMIPIyaDMouGDx8rEkYl
Fo92kANr3ryqImhrjKGsKxE5pttwwn1y6TPn/CbxdFqR5p2ErPioBhlG5qfpqjQi
pKGfeq23sqSaM4hxAjwu1nqyH6LKwN0vEJT9s4yEIHlG1QXUEOTS22RPuFvuG8Ug
R1uUq27UlTMdphVx8fiUylQ5PsE=
-----END CERTIFICATE-----
```


Certificate Service Provider Name (en): REGISTRO NACIONAL DE IDENTIDAD

Trade name (en)	RENIEC/PERU
Information URI (en)	HTTPS://WWW.RENIEC.GOB.PE/
Service provider street address (es)	JR.BOLIVIA 109 CENTRO CIVICO CDO DE LIMA
Service provider street address (en)	JR.BOLIVIA 109 CENTRO CIVICO CDO DE LIMA
Service provider postal code (es)	LIMA01
Service provider postal code (en)	LIMA01
Service provider locality (es)	LIMA
Service provider locality (en)	LIMA
Service provider state (es)	LIMA
Service provider state (en)	LIMA
Service provider country (es)	PE
Service provider country (en)	PE

CN=ECERNEP PERU CA ROOT 3, O=Entidad de Certificación Nacional para el Estado Peruano, C=PE

Type	CA/QC
Status	undersupervision
Status starting time	2018-01-18T23:37:44.000Z

Service digital identity (X509)

Version	3
Serial number	6809427473258457679
Signature algorithm	SHA512withRSA
Issuer	CN=ECERNEP PERU CA ROOT 3, O=Entidad de Certificación Nacional para el Estado Peruano, C=PE
Valid from	Thu Aug 10 12:31:52 PET 2017
Valid to	Sun Aug 10 12:31:52 PET 2042
Subject	CN=ECERNEP PERU CA ROOT 3, O=Entidad de Certificación Nacional para el Estado Peruano, C=PE

Public key	Sun RSA public key, 4096 bits modulus: 74550301454764894858436895359988151894690624301296360185771452280477813900622709762782941840370780218481835330304090022671694974429768543407114010421320638577157215826721076491384610221868785174509514660662491662618505907207470855398103566335609382634843911981971482630127862414247844029200116795663914330316020556259133796534127177915042071171068491356817421545841175528292005042854392603720225977326942801070901462590160720475706426375478858666286365925035377798139874138369273681303523318737632620546138901617102137210410352161732143851839584271676644427677583568464175727385090243756420837890999346025353276684527356021997577838295030513972090732028204029310269883173494927466629664139328360283411924483102946029411614830468930589045029166481375336996868934901593141542467430862257017134563417222706548377769543484439105105922405283338706016073360199584632162005720089348815919945079272488979872500831670414088472191597411217687767005150316763781926930678744496382436181880547789762457882216737596138555783160226739021278561627571220356170189018023201049266769145592655962061277567019556313065142238688850848699228124566758595593957427076489582437847115035273598236823769296523580551647943882973206941777158479847928048218751478370831372804821875147837083137 public exponent: 65537
Subject key identifier	1fe9292061d23142b5ddfd5222bedd0ecff24787
Authority key identifier	0418301680141fe9292061d23142b5ddfd5222bedd0ecff24787
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=2
SHA1 Thumbprint	e611d33d29857be83b5003704bb61c9883ed8ded
SHA256 Thumbprint	96508217c36f3bbc556e2e07d7ab50c40da8027c388235813322e41b87a568be

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=ECERNEP PERU CA ROOT 3, O=Entidad de Certificación Nacional para el Estado Peruano, C=PE
 Signature Algorithm: SHA512withRSA, OID = 1.2.840.113549.1.1.13

 Key:  Sun RSA public key, 4096 bits
 modulus:
74550301454764894858436895359988151894690624301296360185771452280477813900622709762782941840370780218481835330304090022671694974429768543407114010421320638577157215826721076491384610221868785174509514660662491662618505907207470855398103566335609382634843911981971482630127862414247844029200116795663914330316020556259133796534127177915042071171068491356817421545841175528292005042854392603720225977326942801070901462590160720475706426375478858666286365925035377798139874138369273681303523318737632620546138901617102137210410352161732143851839584271676644427677583568464175727385090243756420837890999346025353276684527356021997577838295030513972090732028204029310269883173494927466629664139328360283411924483102946029411614830468930589045029166481375336996868934901593141542467430862257017134563417222706548377769543484439105105922405283338706016073360199584632162005720089348815919945079272488979872500831670414088472191597411217687767005150316763781926930678744496382436181880547789762457882216737596138555783160226739021278561627571220356170189018023201049266769145592655962061277567019556313065142238688850848699228124566758595593957427076489582437847115035273598236823769296523580551647943882973206941777158479847928048218751478370831372804821875147837083137
 public exponent: 65537
 Validity: [From: Thu Aug 10 12:31:52 PET 2017,
              To: Sun Aug 10 12:31:52 PET 2042]
 Issuer: CN=ECERNEP PERU CA ROOT 3, O=Entidad de Certificación Nacional para el Estado Peruano, C=PE
 SerialNumber: [    5e7ff235 835b2a4f]

Certificate Extensions: 6
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 1F E9 29 20 61 D2 31 42   B5 DD FD 52 22 BE DD 0E  ..) a.1B...R"...
0010: CF F2 47 87                                        ..G.
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 1F E9 29 20 61 D2 31 42   B5 DD FD 52 22 BE DD 0E  ..) a.1B...R"...
0010: CF F2 47 87                                        ..G.
]

]

[3]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[]  ]
```

```
]

[5]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://www.reniec.gob.pe/crt/sha2/ecernep.crt]
]

[6]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2
]

]
 Algorithm: [SHA512withRSA]
 Signature:
0000: 44 0F F2 B5 38 75 22 18   F5 94 2D B3 76 BA FE F1  D...8u"...-.v...
0010: 6F 6F 58 4D BC 44 E6 BF   18 71 FC 38 48 EC 69 16  ooXM.D...q.8H.i.
0020: 02 E8 97 00 D5 41 2F FC   75 8D E0 C9 9C A9 97 68  .....A/.u......h
0030: E4 E1 41 60 33 04 25 5B   BB 2A C3 D4 B0 7E A6 DB  ..A`3.%[.*.....
0040: CE 18 1E 8B B6 2E 8C 1B   58 5E 1A F3 A6 14 C8 33  ........X^.....3
0050: A6 BA 87 F4 9E 00 17 CC   36 21 FC 9F 6E 0C C2 69  ........6!..n..i
0060: 34 CE AC 6A 7C F2 54 BD   E7 D8 77 9A A3 8B 99 F7  4..j..T...w.....
0070: 2A DF 14 7E 30 50 0D EC   91 AF 58 F7 2C 6D A2 E3  *...0P....X.,m..
0080: F2 C1 6A 60 8D 6D D4 93   7F 86 86 77 F9 7D 08 96  ..j`.m.....w....
0090: BD D7 5B D4 10 32 67 45   1B 94 C8 CF FC AA 00 4F  ..[..2gE.......O
00A0: 67 F5 03 3C C1 1B 28 07   9B AF 5C 11 AF 53 A0 88  g..<..(...\..S..
00B0: CF 22 23 CE A9 E7 3B 7D   3C 57 87 98 81 8D 56 2F  ."#...;.<W....V/
00C0: 78 8A 39 5E DE 61 EB A6   29 0D 4B 9C D3 2C E4 DD  x.9^.a..).K..,..
00D0: BB CE 20 EC D6 83 E4 05   E2 E1 BD 31 F2 F0 AA B4  .. ........1....
00E0: EF AE 54 1C A1 D5 30 2D   D8 74 71 F6 CE 5F CB 0F  ..T...0-.tq..._..
00F0: A6 6E 56 58 17 66 58 00   9B 1E 84 1B 36 F3 E0 F9  .nVX.fX.....6...
0100: AA 5F A8 83 7A 7D DA CC   8F 29 B3 90 A7 29 83 CF  ._..z....)...)..
0110: A8 EB EA 49 80 8B 19 34   D9 A2 C7 DA 38 78 5B 81  ...I...4....8x[.
0120: B4 02 08 F3 57 53 7C 47   9F FE 63 FA 39 EA 56 7B  ....WS.G..c.9.V.
0130: 68 51 75 49 2A 35 4A D3   F9 93 AE 7F 7E 2C E6 30  hQuI*5J......,.0
0140: A3 F9 44 BE 93 71 3F 02   96 2B 92 85 A1 B0 2E 5D  ..D..q?..+.....]
0150: AE 18 F3 AF F4 58 76 F8   8C D9 42 CD BF FF E1 59  .....Xv...B....Y
0160: 2B 67 EF F7 1E EE D7 D9   0B 61 02 FE 36 02 54 7A  +g.......a..6.Tz
0170: DF 18 05 5F 2D D3 FC 65   5F 2F 0F 15 D1 19 54 FB  ..._-..e_/....T.
0180: 57 A0 E2 C3 45 81 A1 45   1F 5A 92 3E 87 CD FF 6F  W...E..E.Z.>...o
0190: 0D 84 FE A9 9B 46 B2 B4   89 7E DA 0E 38 C4 9E 49  .....F......8..I
01A0: D0 1B 00 53 1B FA 22 92   13 1E 8E B9 63 AB 0B F7  ...S.."....c...
01B0: 54 11 34 5E 22 F4 DD F1   15 7B DD 65 07 B2 03 91  T.4^".....e....
01C0: 8D C3 51 9E 16 D7 16 31   0B 93 CE AA 0E 61 23 7A  ..Q....1.....a#z
01D0: 0E 2A 66 0C 33 BA 2E 7C   BD 66 3F 9E 6B 1B 5F 8C  .*f.3....f?.k._.
01E0: 68 D0 63 4F E4 3A 80 BA   3D A6 93 9F BA E4 1F 4F  h.cO.:..=......O
01F0: E9 A4 6D 57 2A 26 22 E8   6C 5E 71 3F 4C 51 04 2C  ..mW*&".l^q?LQ.,

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGLDCCBBSgAwIBAgIIXn/yNYNbKk8wDQYJKoZIhvcNAQENBQAwcjELMAkGA1UE
BhMCUEUxQjBABgNVBAoMOUVudGlkYWQgZGUgQ2VydGlmaWNhY2nDs24gTmFjaW9u
YWwgcGFyYSBlbCBFc3RhZG8gUGVydWFubzEfMB0GA1UEAwwWRUNFUk5FUCBQRVJV
IENBIFJPT1QgMzAeFw0xNzA4MTAxNzMxNTJaFw00MjA4MTAxNzMxNTJaMHIxCzAJ
BgNVBAYTAlBFMUIwQAYDVQQKDDlFbnRpZGFkIGRlIENlcnRpZmljYWNpw7NuIE5h
Y2lvbmFsIHBhcmEgZWwgRXN0YWRvIFBlcnVhbm8xHzAdBgNVBAMMFkVDRVJORVAg
UEVSVSBDQSBST09UIDMwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQC2
vL2la6NIgUWwoyA7CdnqjuiVlYrp5/MX01RCXrn5tDvuobS/Afb2unu0oVRsw6jY
cpDP0bNnaPuBhlaOFKhjbOVJvA3US+b+9Ek2cKekCzJyQLNWb6R/m2ggTGGGGITO
GayNklsrMOvNPP8F/T48bxOnUDupGVMpuKLMzz9xASBF0DhofKOxC/eEuU/irr6d
nmbFDtFFdrJr/4cGlnYiYerwPw4Knu4br6uJ6KfKXE1P5r7eoli4n3JxBhUi0NK/
mMc8CypJkZXC+LZ2bv7nNGgZpVk0v4yen/uX5VkuIevMYPyNi2EengxwIJOSexZP
BMITH37RqiGQ2NDsN1EopFqXpddwyMIJMClr4ZsVnQZhddOKLxZmPt1P/GPy8VM7
63LkKWnHueq842GQ2CWrUa0U8R8Y4iJRUn/qOlyJYdveDNfLufgF/5YML5UrcXjq
+j6r54je02nY6dgZ3oI8CP9HaNRvsrFbRt9bnRlwVlXQr8/iFoyAyBnClhs0KpxG
Ay0v4pBB6OtL0yTp7NeBY1FMY8tFAQNP5HkZ3v684j2kJ/T3wPwfCQuQuLY1bztb
p/bfxjZGkkrznqSLbOO/+tJUBeAeditx8H3d61RpAo1QNpXHLKIXJz6k5/bpYT4n
QuUDkHZ0vv68j9SVEyd77lfMt0qWHV/yp3uEYZ0OAQIDAQABo4HFMIHCMBIGA1Ud
EwEB/wQIMAYBAf8CAQIwHwYDVR0jBBgwFoAUH+kpIGHSMUK13f1SIr7dDs/yR4cw
SQYIKwYBBQUHAQEEPTA7MDkGCCsGAQUFBzAChi1odHRwOi8vd3d3LnJlbmllYy5n
b2IucGUvY3J0L3NoYTIvZWNlcm5lcC5jcnQwEQYDVR0gBAowCDAGBgRVHSAAMB0G
A1UdDgQWBBQf6SkgYdIxQrXd/VIivt0Oz/JHhzAOBgNVHQ8BAf8EBAMCAQYwDQYJ
KoZIhvcNAQENBQADggIBAEQP8rU4dSIY9ZQts3a6/vFvb1hNvETmvxhx/DhI7GkW
AuiXANVBL/x1jeDJnKmXaOThQWAzBCVbuyrD1LB+ptvOGB6Lti6MG1heGvOmFMgz
prqH9J4AF8w2IfyfbgzCaTTOrGp88lS959h3mqOLmfcq3xR+MFAN7JGvWPcsbaLj
8sFqYI1t1JN/hoZ3+X0Ilr3XW9QQMmdFG5TIz/yqAE9n9QM8wRsoB5uvXBGvU6CI
zyIjzqnnO308V4eYgY1WL3iKOV7eYeumKQ1LnNMs5N27ziDs1oPkBeLhvTHy8Kq0
765UHKHVMC3YdHH2zl/LD6ZuVlgXZlgAmx6EGzbz4PmqX6iDen3azI8ps5CnKYPP
qOvqSYCLGTTZosfaOHhbgbQCCPNXU3xHn/5j+jnqVntoUXVJKjVK0/mTrn9+LOYw
o/lEvpNxPwKWK5KFobAuXa4Y86/0WHb4jNlCzb//4VkrZ+/3Hu7X2QthAv42AlR6
3xgFXy3T/GVfLw8V0RlU+1eg4sNFgaFFH1qSPofN/28NhP6pm0aytIl+2g44xJ5J
0BsAUxv6IpITHo65Y6sL91QRNF4i9N3xFXvdZQeyA5GNw1GeFtcWMQuTzqoOYSN6
DipmDDO6Lny9Zj+eaxtfjGjQY0/kOoC6PaaTn7rkH0/ppG1XKiYi6GxecT9MUQQs
-----END CERTIFICATE-----
```

CN=ECEP-RENIEC, O=Registro Nacional de Identificación y Estado Civil, C=PE

Type	CA/QC
Status	undersupervision
Status starting time	2018-01-16T21:31:25.000Z

Service digital identity (X509)

Version	3
Serial number	496878701977333053
Signature algorithm	SHA512withRSA
Issuer	CN=ECERNEP PERU CA ROOT 3, O=Entidad de Certificación Nacional para el Estado Peruano, C=PE
Valid from	Thu Aug 10 15:31:59 PET 2017
Valid to	Wed Aug 10 15:31:59 PET 2033
Subject	CN=ECEP-RENIEC, O=Registro Nacional de Identificación y Estado Civil, C=PE
Public key	Sun RSA public key, 4096 bits modulus: 671546800946152241714944127429519816734616877316480963325301876321071596613309798441205521376202472020813667464847116965000923604400375541689380727244060023530337987062449703399170879547186940392709114729226771716000307524637220470057867058188661228507657414914148826216459261368715210108192616437229669592854474073619543808968649314654626306320975562551134403130387719395733631148618357639367007751742033806558140267461699582091166485963561654741407490594080488731475849339180547253246945364236926956696026515190573540453730580732949781032433443611895483985250137609808157674512567009773585230411451405463389084114973156261429586027293668677253433040148199482428357051308808978711112352180234727367673211131499723626907452317797244252169032356495383644974331261198400458393259025698988977092103815477801980456818434999110766291677340890298248029966878216916987278779300027026226215375526600428306096216611020840683054879871423969137501242697401554775886976650971279164765751394733901452059404543216133475830669796040927727092099854407483950353174856772286917477155736716448767307454744162795193428460627361044052090228179802705140744473420261621010439480528110638091658390385087343246368129651375732685485955092166546518455231915187 7
public exponent: 65537
Validity: [From: Thu Aug 10 15:31:59 PET 2017,
To: Wed Aug 10 15:31:59 PET 2033]
Issuer: CN=ECERNEP PERU CA ROOT 3, O=Entidad de Certificación Nacional para el Estado Peruano, C=PE
SerialNumber: [06e5448b ffd0ed3d]

Certificate Extensions: 6

Subject key identifier	22aff35feee1457d4cef7ee3dfd2527ccbce7b75
CRL distribution points	http://crl.reniec.gob.pe/arl/sha2/ecernep.crl http://crl2.reniec.gob.pe/arl/sha2/ecernep.crl
Authority key identifier	0418301680141fe9292061d23142b5ddfd5222bedd0ecff24787
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=1
SHA1 Thumbprint	2fe0a4ab97544334c122bb142e39e91f69607647
SHA256 Thumbprint	91520e1f381a46402b9490c06749b2d81ddad4b53e7f252a1dd79b55dfcb340b

The decoded certificate:

```
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 22 AF F3 5F EE E1 45 7D   4C EF 7E E3 DF D2 52 7C  "..._..E.L.....R.
0010: CB CE 7B 75                                        ...u
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 1F E9 29 20 61 D2 31 42   B5 DD FD 52 22 BE DD 0E  ..) a.1B...R"...
0010: CF F2 47 87                                        ..G.
]

]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.reniec.gob.pe/arl/sha2/ecernep.crl]
, DistributionPoint:
    [URIName: http://crl2.reniec.gob.pe/arl/sha2/ecernep.crl]
]]

[4]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[5]: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
 clientAuth
 emailProtection
 1.3.6.1.4.1.311.20.2.2
 OCSPSigning
 serverAuth
]

[6]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:1
]

]
 Algorithm: [SHA512withRSA]
 Signature:
0000: 6A B2 11 98 84 B4 13 3F   66 E4 3F D9 40 71 5C 7B  j......?f.?.@q\.
0010: 62 70 F8 27 44 CA D6 D2   9D CA 0F EE C9 6E 21 AB  bp.'D........n!.
0020: 49 32 AF 45 43 9C CD EA   A6 E0 EC 11 3F 88 F6 FB  I2.EC.......?...
0030: 01 58 02 54 C6 D5 4B 41   CF 61 78 AD C6 35 9E FC  .X.T..KA.ax..5..
0040: 9C 0D 74 70 F9 0E C3 5D   FE 8F A2 92 1B 9D C3 E2  ..tp...]........
0050: 60 0C E2 66 EA B0 D0 31   F4 0E 5E 5C AC 5C 68 43  `..f...1..^\.\hC
0060: E0 19 85 62 61 FA F9 A2   D9 12 CA DA 92 4B 1D DE  ...ba........K..
0070: E0 00 46 14 18 99 A2 01   65 CA E5 13 7A 6F DA DB  ..F.....e...zo..
0080: E8 A0 3E 37 D6 CD BD E9   00 F5 01 8D 9B B2 A7 85  ..>7............
0090: 9A 39 16 EE 17 35 BA 7B   15 D9 50 13 72 15 07 16  .9...5....P.r...
00A0: 47 DC 9E 9E 89 6B 4E 6A   5D 75 4A 96 40 3F B7 98  G....kNj]uJ.@?..
00B0: 06 30 ED 6B 2D A3 51 69   5A D1 7A D3 13 AD 96 2A  .0.k-.QiZ.z....*
00C0: 18 FA 9F EC 81 8A 8C 0F   2C F4 8F FC 45 BE 0E 00  ........,...E...
00D0: 14 C3 47 CF 0D 6F 01 2A   85 D4 88 3B 10 55 4D 5E  ..G..o.*...;.UM^
00E0: C0 D0 B7 16 0C 1C 86 E0   0C F9 AF 84 EF EE 8E A0  ................
00F0: E2 E8 98 D4 35 A5 3A 93   F1 03 3B 5D 3A B5 45 6D  ....5.:...;]:.Em
0100: 5C FB 1E 5F C6 51 A7 12   72 75 E1 40 02 DA 7C F5  \.._.Q..ru.@....
0110: 29 61 7A 70 39 17 AD E8   7A 0B 98 E9 39 5F 59 55  )azp9...z...9_YU
0120: 0F 7F 9C 8D 39 B7 20 16   BC 43 73 D2 52 95 35 AA  ....9. ..Cs.R.5.
0130: DE 23 44 CF 6D 00 02 9B   A3 46 61 AC B5 C0 B0 9E  .#D.m....Fa.....
0140: 64 85 EC CB B6 C1 96 5D   04 85 D4 61 2F C9 38 86  d......]...a/.8.
0150: B7 43 49 EA 27 4B CF A8   27 01 D5 54 64 43 46 51  .CI.'K..'..TdCFQ
0160: 8F 17 86 8C EB 51 C3 0B   17 62 E4 FA 27 FD 79 88  .....Q...b..'.y.
0170: 5A A0 BA 0C C5 7F 8F DE   CB 56 A8 D5 39 77 8E 9A  Z........V..9w..
0180: FA C6 3E 25 AA 05 9B B8   8D 59 96 92 D8 89 C3 5A  ..>%.....Y.....Z
0190: 1A 3C F4 CC D8 10 3E 8F   F2 89 2C DF F1 96 6D CE  .<....>...,...m.
01A0: D4 0A 44 56 BB 5B 1A 55   2A 1C 34 F1 7A EA CE 04  ..DV.[.U*.4.z...
01B0: 6B EA 64 E2 79 BA 52 86   3C EC F2 33 58 01 EF 55  k.d.y.R.<..3X..U
01C0: 36 A4 22 70 9F DD D6 FE   0C 55 C4 2C 69 22 1B 42  6."p.....U.,i".B
01D0: A1 5C FF 29 D3 D2 C7 3D   A9 A4 8C 7F 6D 86 16 A3  .\.)...=....m...
01E0: AB BD 15 DF 84 F1 CE 86   51 71 FC EF BF D5 44 A5  ........Qq....D.
01F0: 6B 9B 4A 5F DA 7B 56 9D   28 D1 8E 1E 7F EA 06 3E  k.J_..V.(......>

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGdDCCBFygAwIBAgIIBuVEi//Q7T0wDQYJKoZIhvcNAQENBQAwcjELMAkGA1UE
BhMCUEUxQjBABgNVBAoMOUVudGlkYWQgZGUgQ2VydGlmaWNhY2nDs24gTmFjaW9u
YWwgcGFyYSBlbCBFc3RhZG8gUGVydWFubzEfMB0GA1UEAwwWRUNFUk5FUCBQRVJV
IENBIFJPT1QgMzAeFw0xNzA4MTAyMDMxNTlaFw0zMzA4MTAyMDMxNTlaMGExCzAJ
BgNVBAYTAlBFMTwwOgYDVQQKDDNSZWdpc3RybyBOYWNpb25hbCBkZSBJZGVudGlm
aWNhY2nDs24geSBFc3RhZG8gQ2l2aWwxFDASBgNVBAMMC0VDRVAtUkVOSUVDMIIC
IjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEApJvyMiRwB1BO0KMkFH9tkjCq
nyF9ZkTMkQg3SIk+qxFWq8Bv4K1MaO0aWe4/5vdaRI2NW/E61C+q76bAAaR/nwfP
```

TBPStBW6WKerwZ4w+2OFCF0UaioCJ6P1SRETsRYesNDFeU/FJD7+o7MTt1s3nxPz
sqcQgiORXO7Zs8RmhRdLmhi+LOZHxx6xXngd7bpk/ustCb3XHKHJFjSdLED5EInA
Z+JhTZsI8qvMqE5nV0+cBNCpvvAazFp4R9J2vH4W1Abr8xIXoxXhQXIxTjoJWDX0
RgANBbv10NqHf6xOwCtJgALc2bzUzNZd6QhsiVe18kDJGjD34KvqTO8Oyk98gwKo
mzrkEavXA3LrP8aCxtxX9URugtSKdH9GRgu4zm8632A9X76MjkhdApvyQa7iA+s4
JZWhN5QbGYTTDBWeYjktcbEnGyfX/o1zEOqnYsPqn8nS0O1b52pV6OYwYuRKhw1b
D/flk0Z28CQI20sJM1LBXHgXtALE8n59/m/yElk7u71QZqGdCY2e2wi6H+7L7V9C
7eOeJnf/5WD1oUa6F/yswj47Lelp4peVXZg7PJ3IGugCbBHtl42j04Je+/+8E2DJ
omVJl6oFlZzk38dIF00QaWGp6dv4L1PFVDRG5XkIIdF7GmLcbO5iY01/sRbhBrue
jx+VmtA2zwGOUlpfbwUCAwEAAaOCAR0wggEZMBIGA1UdEwEB/wQIMAYBAf8CAQEw
HwYDVR0jBBgwFoAUH+kpIGHSMUK13f1SIr7dDs/yR4cwPQYDVR0lBDYwNAYIKwYB
BQUHAwIGCCsGAQUFBwMEBgorBgEEAYI3FAICBggrBgEFBQcDCQYIKwYBBQUHAwEw
dAYDVR0fBG0wazAzoDGgL4YtaHR0cDovL2NybC5yZW5pZWMuZ29iLnBlL2FybC9z
aGEyL2VjZXJuZXAuY3JsMDSgMqAwhi5odHRwOi8vY3JsMi5yZW5pZWMuZ29iLnBl
L2FybC9zaGEyL2VjZXJuZXAuY3JsMB0GA1UdDgQWBBQir/Nf7uFFfUzvfuPf0lJ8
y857dTAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQENBQADggIBAGqyEZiEtBM/
ZuQ/2UBxXHticPgnRMrW0p3KD+7JbiGrSTKvRUOczeqm4OwRP4j2+wFYAlTG1UtB
z2F4rcY1nvycDXRw+Q7DXf6PopIbncPiYAziZuqw0DH0Dl5crFxoQ+AZhWJh+vmi
2RLK2pJLHd7gAEYUGJmiAWXK5RN6b9rb6KA+N9bNvekA9QGNm7KnhZo5Fu4XNbp7
FdlQE3IVBxZH3J6eiWtOal11SpZAP7eYBjDtay2jUWla0XrTE62WKhj6n+yBiowP
LPSP/EW+DgAUw0fPDW8BKoXUiDsQVU1ewNC3FgwchuAM+a+E7+6OoOLomNQ1pTqT
8QM7XTq1RW1c+x5fxlGnEnJ14UAC2nz1KWF6cDkXreh6C5jpOV9ZVQ9/nI05tyAW
vENz0lKVNareI0TPbQACm6NGYay1wLCeZIXsy7bBll0EhdRhL8k4hrdDSeonS8+o
JwHVVGRDRlGPF4aM61HDCxdi5Pon/XmIWqC6DMV/j97LVqjVOXeOmvrGPiWqBZu4
jVmWktiJw1oaPPTM2BA+j/KJLN/xlm3O1ApEVrtbGlUqHDTxeurOBGvqZOJ5ulKG
POzyM1gB71U2pCJwn93W/gxVxCxpIhtCoVz/KdPSxz2ppIx/bYYWo6u9Fd+E8c6G
UXH877/VRKVrm0pf2ntWnSjRjh5/6gY+
-----END CERTIFICATE-----

CN=RENIEC EREP Persona Natural DNIe, OU=RENIEC Registration Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE

Type	RA
Status	ted
Status starting time	2013-07-11T18:04:59.000Z

Service digital identity (X509)

Version	3
Serial number	1
Signature algorithm	SHA1withRSA
Issuer	CN=RENIEC EREP Persona Natural DNIe, OU=RENIEC Registration Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
Valid from	Tue Mar 19 06:55:00 PET 2013
Valid to	Sun Mar 19 06:55:00 PET 2023
Subject	CN=RENIEC EREP Persona Natural DNIe, OU=RENIEC Registration Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
Public key	Sun RSA public key, 2048 bits modulus: 22049080826349849073929231571857745080792825156349745752321416196524981851716938629857153665171764207020656770483302653546201001789267522196522616954922479307118048930114030646087703603414845892110633938664328182446878612069446305708519913011036088299485134949224193666648550579483141992361203201459254225276122106564523154622620123278243926301228667612303178451812778346617947516433408191311760977441127082499217265764528535449271193543991418454538809735726697736528764121555324149222711071520223761738241413934614172505523570059420731588785128498223656286439259426272115291325851607773789958873344237570509543769563 public exponent: 65537
Subject key identifier	d44b9a04348187bf1f38ebcafad8a1efa6d48c35
Basic constraints	CA=false
SHA1 Thumbprint	d6e40831185c8dbf8b103a2a83d01ce6eef73774
SHA256 Thumbprint	ce6408bd05a240c9d9832edb1549e86a00d9d72f2b9ccb6cb1cc15921255f12b

The decoded certificate:

[
[
 Version: V3
 Subject: CN=RENIEC EREP Persona Natural DNIe, OU=RENIEC Registration Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key: Sun RSA public key, 2048 bits
 modulus:
22049080826349849073929231571857745080792825156349745752321416196524981851716938629857153665171764207020656770483302653546201001789267522196522616954922479307118048930114030646087703603414845892110633938664328182446878612069446305708519913011036088299485134949224193666648550579483141992361203201459254225276122106564523154622620123278243926301228667612303178451812778346617947516433408191311760977441127082499217265764528535449271193543991418454538809735726697736528764121555324149222711071520223761738241413934614172505523570059420731588785128498223656286439259426272115291325851607773789958873344237570509543769563

```
055235700594207315887851284982236562864392594262721152913258516077737899588733442375705095437695 63
 public exponent: 65537
 Validity: [From: Tue Mar 19 06:55:00 PET 2013,
             To: Sun Mar 19 06:55:00 PET 2023]
 Issuer: CN=RENIEC EREP Persona Natural DNIe, OU=RENIEC Registration Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
 SerialNumber: [    01]

Certificate Extensions: 1
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: D4 4B 9A 04 34 81 87 BF   1F 38 EB CA FA D8 A1 EF  .K..4....8......
0010: A6 D4 8C 35                                        ...5
]
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: 73 F8 34 F1 51 7D 35 A6   9D E0 DF 78 49 D7 BE FE  s.4.Q.5....xI...
0010: E1 80 D2 AB BE AA 69 95   2D 1E A1 CA A8 EB 6E FF  ......i.-.....n.
0020: 67 90 E3 F3 E7 C9 9E 0A   6C D0 0B 37 21 21 B6 D0  g.......l..7!!..
0030: 78 E6 A7 C0 AF E9 02 D9   2B 42 5F BB 61 C0 7C 7E  x.......+B_.a...
0040: 10 9E E9 11 B4 E0 05 AA   77 32 39 A3 9E 13 5B 7B  ........w29...[.
0050: 48 5D 94 40 52 16 68 7C   F6 64 77 FD A3 64 AA B4  H].@R.h..dw..d..
0060: A0 A1 41 3D 96 A7 54 BA   93 B7 B1 02 C6 CF 55 1F  ..A=..T.......U.
0070: 6B C2 56 3E 3F 66 37 73   3B DF CF 8E 70 C5 FC 44  k.V>?f7s;...p..D
0080: 28 7F 31 58 2C FC 9B 5A   33 A7 D2 20 28 F2 D9 84  (.1X,..Z3.. (...
0090: 8E C8 C1 4C 48 A2 8E 7C   E2 34 5A E7 00 C1 1E 9B  ...LH....4Z.....
00A0: 62 FB CE B0 84 7C 95 94   5D 8C 82 50 2D 16 48 EF  b.......]..P-.H.
00B0: EA C1 D9 D7 5E D1 16 00   0E 2A DE 83 99 81 AE 17  ....^....*......
00C0: 6A 1F 69 83 D6 8A A6 1C   C6 C0 ED 97 66 84 FE 5E  j.i.........f..^
00D0: 13 65 36 D1 B2 6A 54 F1   81 F1 51 84 E2 4A 2E 85  .e6..jT...Q..J..
00E0: 7C EA 46 7E 34 AF 88 10   B4 80 66 6D 9E 29 78 EE  ..F.4.....fm.)x.
00F0: 97 7D 75 7E 0C 4B 41 A0   21 A9 75 44 97 BA 2D A0  ..u..KA.!.uD..-.

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIID2jCCAsKgAwIBAgIBATANBgkqhkiG9w0BAQUFADCBnjELMAkGA1UEBhMCUEUx
PDA6BgNVBAoMM1JlZ2lzdHJvIE5hY2lvbmFsIGRlIElkZW50aWZpY2FjacOzbiB5
IEVzdGFkbyBDaXZpbDEmMCQGA1UECxMdUkVOSUVDIFJlZ2lzdHJhdGlvbiBBdXRo
b3JpdHkxKTAnBgNVBAMTIFJFTklFQyBFUkVQIFBlcnNvbmEgTmF0dXJhbCBETkll
MB4XDTEzMDMxOTExNTUwMFoXDTIzMDMxOTExNTUwMFowgZ4xCzAJBgNVBAYTAlBF
MTwwOgYDVQQKDDNSZWdpc3RybyBOYWNpb25hbCBkZSBJZGVudGlmaWNhY2nDs24g
eSBFc3RhZG8gQ2l2aWwxJjAkBgNVBAsTHVJFTklFQyBSZWdpc3RyYXRpb24gQXV0
aG9yaXR5MSkwJwYDVQQDEyBSRU5JRUMgRVJFUCBQZXJzb25hIE5hdHVyYWwgRE5J
ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK6pkLcGhLwlvPTbGDQS
PZAyGVp4x1wnk9AV4tdQV3gv77RWwpgFXCF4E+2MxSz1P1GjVn0Wg1EPpKRULSaO
pL3yZZec9jLVtVbZIZHAv/90pYsHKHPUrR/qs8+jZr9dkYGwyiyalbBjYcCTGzHD
cfpl3ME/N46OJhUf83ceNnIp6w0iyIu6k2zucZBAnUmfbkxADnajZcsNjXj7UHM7
JRcRpg2O3reMcLcI1qyQAAxt3virX5mC3tULs7261dp+ZCPBwdy97azKxNghINjr
6ufV8ibN54QTgm7a1cMfIqHbJgYVLOEmqQ1I0U237AVogNHUwJMJgE24zC8a/Ip3
BdsCAwEAAaMhMB8wHQYDVR0OBBYEFNRLmgQ0gYe/HzjryvrYoe+m1Iw1MA0GCSqG
SIb3DQEBBQUAA4IBAQBz+DTxUX01pp3g33hJ177+4YDSq76qaZUtHqHKqOtu/2eQ
4/PnyZ4KbNALNyEhttB45qfAr+kC2StCX7thwHx+EJ7pEbTgBap3MjmjnhNbe0hd
lEBSFmh89mR3/aNkqrSgoUE9lqdUupO3sQLGz1Ufa8JWPj9mN3M738+OcMX8RCh/
MVgs/JtaM6fSICjy2YSOyMFMSKKOfOI0WucAwR6bYvvOsIR8lZRdjIJQLRZI7+rB
2dde0RYADireg5mBrhdqH2mD1oqmHMbA7ZdmhP5eE2U20bJqVPGB8VGE4kouhXzq
Rn40r4gQtIBmbZ4peO6XfXV+DEtBoCGpdUSXui2g
-----END CERTIFICATE-----
```

CN=RENIEC EREP Persona Natural DNIe, OU=RENIEC Registration Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE

Type	RA
Status	undersupervision
Status starting time	2013-07-11T16:31:30.000Z

Service digital identity (X509)

Version	3
Serial number	1
Signature algorithm	SHA1withRSA
Issuer	CN=RENIEC EREP Persona Natural DNIe, OU=RENIEC Registration Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
Valid from	Tue Mar 19 06:55:00 PET 2013
Valid to	Sun Mar 19 06:55:00 PET 2023
Subject	CN=RENIEC EREP Persona Natural DNIe, OU=RENIEC Registration Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE

Public key	Sun RSA public key, 2048 bits modulus: 22049080826349849073929231571857745080792825156349745752321416196524981 85171693862985715366517176420702065677048330265354620100178926752219652 26169549224793071180489301140306460877036034148458921106339386643281824 46878612069446305708519913011036088299485134949224193666648550579483141 99236120320145925422527612210656452315462262012327824392630122866761230 31784518127783466179475164334081913117609774411270824992172657645285354 49271193543991418454538809735726697736528764121555324149222711071520223 76173824141393461417250552357005942073158878512849822365628643925942627 21152913258516077737899588733442375705095437695 63 public exponent: 65537
Subject key identifier	d44b9a04348187bf1f38ebcafad8a1efa6d48c35
Basic constraints	CA=false
SHA1 Thumbprint	d6e40831185c8dbf8b103a2a83d01ce6eef73774
SHA256 Thumbprint	ce6408bd05a240c9d9832edb1549e86a00d9d72f2b9ccb6cb1cc15921255f12b

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=RENIEC EREP Persona Natural DNIe, OU=RENIEC Registration Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 2048 bits
 modulus:
22049080826349849073929231571857745080792825156349745752321416196524981851716938629857153665171764207020656770483302653546201001789267522196522616954922479307118048930114030646087703603414845892110633938664328182446878612069446305708519913011036088299485134949224193666648550579483141992361203201459254225276122106564523154622620123278243926301228667612303178451812778346617947516433408191311760977441127082499217265764528535449271193543991418454538809735726697736528764121555324149222711071520223767382414139346141725055235700594207315887851284982236562864392594262721152913258516077737899588733442375705095437695 63
 public exponent: 65537
 Validity: [From: Tue Mar 19 06:55:00 PET 2013,
             To: Sun Mar 19 06:55:00 PET 2023]
 Issuer: CN=RENIEC EREP Persona Natural DNIe, OU=RENIEC Registration Authority, O=Registro Nacional de Identificación y Estado Civil, C=PE
 SerialNumber: [    01]

Certificate Extensions: 1
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: D4 4B 9A 04 34 81 87 BF   1F 38 EB CA FA D8 A1 EF  .K..4....8......
0010: A6 D4 8C 35                                        ...5
]
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: 73 F8 34 F1 51 7D 35 A6   9D E0 DF 78 49 D7 BE FE  s.4.Q.5....xI...
0010: E1 80 D2 AB BE AA 69 95   2D 1E A1 CA A8 EB 6E FF  ......i.-.....n.
0020: 67 90 E3 F3 E7 C9 9E 0A   6C D0 0B 37 21 21 B6 D0  g.......l..7!!..
0030: 78 E6 A7 C0 AF E9 02 D9   2B 42 5F BB 61 C0 7C 7E  x.......+B_.a...
0040: 10 9E E9 11 B4 E0 05 AA   77 32 39 A3 9E 13 5B 7B  ........w29...[.
0050: 48 5D 94 40 52 16 68 7C   F6 64 77 FD A3 64 AA B4  H].@R.h..dw..d..
0060: A0 A1 41 3D 96 A7 54 BA   93 B7 B1 02 C6 CF 55 1F  ..A=..T.......U.
0070: 6B C2 56 3E 3F 66 37 73   3B DF CF 8E 70 C5 FC 44  k.V>?f7s;...p..D
0080: 28 7F 31 58 2C FC 9B 5A   33 A7 D2 20 28 F2 D9 84  (.1X,..Z3.. (...
0090: 8E C8 C1 4C 48 A2 8E 7C   E2 34 5A E7 00 C1 1E 9B  ...LH....4Z.....
00A0: 62 FB CE B0 84 7C 95 94   5D 8C 82 50 2D 16 48 EF  b.......]..P-.H.
00B0: EA C1 D9 D7 5E D1 16 00   0E 2A DE 83 99 81 AE 17  ....^....*......
00C0: 6A 1F 69 83 D6 8A A6 1C   C6 C0 ED 97 66 84 FE 5E  j.i.........f..^
00D0: 13 65 36 D1 B2 6A 54 F1   81 F1 51 84 E2 4A 2E 85  .e6..jT...Q..J..
00E0: 7C EA 46 7E 34 AF 88 10   B4 80 66 6D 9E 29 78 EE  ..F.4.....fm.)x.
00F0: 97 7D 75 7E 0C 4B 41 A0   21 A9 75 44 97 BA 2D A0  ..u..KA.!.uD..-.

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIID2jCCAsKgAwIBAgIBATANBgkqhkiG9w0BAQUFADCBnjELMAkGA1UEBhMCUEUx
PDA6BgNVBAoMM1JlZ2lzdHJvIE5hY2lvbmFsIGRlIElkZW50aWZpY2FjacOzbiB5
IEVzdGFkbyBDaXZpbDEmMCQGA1UECxMdUkVOSUVDIFJlZ2lzdHJhdGlvbiBBdXRo
b3JpdHkxKTAnBgNVBAMTIFJFTklFQyBFUkVQIFBlcnNvbmEgTmF0dXJhbCBETkll
MB4XDTEzMDMxOTExNTUwMFoXDTIzMDMxOTExNTUwMFowgZ4xCzAJBgNVBAYTAlBF
MTwwOgYDVQQKDDNSZWdpc3RybyBOYWNpb25hbCBkZSBJZGVudGlmaWNhY2nDs24g
eSBFc3RhZG8gQ2l2aWwxJjAkBgNVBAsTHVJFTklFQyBSZWdpc3RyYXRpb24gQXV0
aG9yaXR5MSkwJwYDVQQDEyBSRU5JRUMgRVJFUCBQZXJzb25hIE5hdHVyYWwgRE5J
ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK6pkLcGhLwlvPTbGDQS
PZAyGVp4x1wnk9AV4tdQV3gv77RWwpgFXCF4E+2MxSz1P1GjVn0Wg1EPpKRULSaO
pL3yZZec9jLVtVbZIZHAv/90pYsHKHPUrR/qs8+jZr9dkYGwyiyalbBjYcCTGzHD
cfpl3ME/N46OJhUf83ceNnIp6w0iyIu6k2zucZBAnUmfbkxADnajZcsNjXj7UHM7
JRcRpg2O3reMcLcI1qyQAAxt3virX5mC3tULs7261dp+ZCPBwdy97azKxNghINjr
6ufV8ibN54QTgm7a1cMfIqHbJgYVLOEmqQ1I0U237AVogNHUwJMJgE24zC8a/Ip3
BdsCAwEAAaMhMB8wHQYDVR0OBBYEFNRLmgQ0gYe/HzjryvrYoe+m1Iw1MA0GCSqG
SIb3DQEBBQUAA4IBAQBz+DTxUX01pp3g33hJ177+4YDSq76qaZUtHqHKqOtu/2eQ
4/PnyZ4KbNALNyEhttB45qfAr+kC2StCX7thwHx+EJ7pEbTgBap3MjmjnhNbe0hd
```

lEBSFmh89mR3/aNkqrSgoUE9lqdUupO3sQLGz1Ufa8JWPj9mN3M738+OcMX8RCh/
MVgs/JtaM6fSICjy2YSOyMFMSKKOfOI0WucAwR6bYvvOsIR8lZRdjIJQLRZI7+rB
2dde0RYADireg5mBrhdqH2mD1oqmHMbA7ZdmhP5eE2U20bJqVPGB8VGE4kouhXzq
Rn40r4gQtIBmbZ4peO6XfXV+DEtBoCGpdUSXui2g
-----END CERTIFICATE-----

CN="Registro Nacional de Identificación y Estado Civil, RENIEC", OU=Gerencia de Informática, O="Registro Nacional de Identificación y Estado Civil, RENIEC", L=Lima, ST=Lima, C=PE

Type	unspecified
Status	undersupervision
Status starting time	2012-11-12T22:22:32.000Z

Service digital identity (X509)

Version	3
Serial number	618865942572342973503663339984959173O
Signature algorithm	SHA1withRSA
Issuer	CN=DigiCert Assured ID Code Signing CA-1, OU=www.digicert.com, O=DigiCert Inc, C=US
Valid from	Sun Oct 14 19:00:00 PET 2012
Valid to	Wed Oct 23 07:00:00 PET 2013
Subject	CN="Registro Nacional de Identificación y Estado Civil, RENIEC", OU=Gerencia de Informática, O="Registro Nacional de Identificación y Estado Civil, RENIEC", L=Lima, ST=Lima, C=PE
Public key	Sun RSA public key, 2048 bits modulus: 179191847824950145164581155117107662509903195415915151701228172648417936302230967935505601642835648433561790210879617361880348456401597288256467298805675225400383669828648545 63022309679355056016428356484335617902108796173618803484564015972882564 67298805675225400383669828648565566371144915451122420710246198187631005 50486793202622047840555144926483753464365720616817514646914303869361760 03659923632989719140535106666179076634498143318507545903045182875218447 97269086008492164500389319997100012344837618919019831038131743755551941 61371322576853439721603499752472091693466966627541440239615134661874995 21814915222913904937346787839877295607468652788242200778407118283231878 87647131051911009345761341229220710342252729777773 public exponent: 65537
Subject key identifier	6fa1125be39f3913c41ef1a23734c8fcd13b0fcf
CRL distribution points	http://crl3.digicert.com/assured-cs-2011a.crl http://crl4.digicert.com/assured-cs-2011a.crl
Authority key identifier	0418301680147b68ce29aac017be497ae1e53fd6a7f7458f3532
Key usage	digitalSignature
Basic constraints	CA=false
SHA1 Thumbprint	f4c38f36352079fbf62b0810287d067047a3ccb4
SHA256 Thumbprint	54aac9bfbae6d923c6afe7041ecbb59b82a02b250d0e2682a9a2c19bb7353ccd

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN="Registro Nacional de Identificación y Estado Civil, RENIEC", OU=Gerencia de Informática, O="Registro Nacional de Identificación y Estado Civil, RENIEC",
L=Lima, ST=Lima, C=PE
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 2048 bits
 modulus:
179191847824950145164581155117107662509903195415915151701228172648417936302230967935505601642835648433561790210879617361880348456401597288256467298805675225400383669828648565
556637114491545112242071024619818763100550486793202622047840555144926483753464365720616817514646914303869361760036599236329897191405351066661790766344981433185075459030451828752184479726908600849216450038931999710001234483761891901983103813174375555194161371322576853439721603499752472091693466966627541440239615134661874995218149152229139049373467878398772956074686527882422007784071182832318788764713105191100934576134122922071034225272977773
 public exponent: 65537
 Validity: [From: Sun Oct 14 19:00:00 PET 2012,
             To: Wed Oct 23 07:00:00 PET 2013]
 Issuer: CN=DigiCert Assured ID Code Signing CA-1, OU=www.digicert.com, O=DigiCert Inc, C=US
 SerialNumber: [    04a7e477 a07bf99f 169d983b 562f23b2]

Certificate Extensions: 8
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 6F A1 12 5B E3 9F 39 13   C4 1E F1 A2 37 34 C8 FC  o..[..9.....74..
```

```
0010: D1 3B 0F CF                                        .;..
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 7B 68 CE 29 AA C0 17 BE   49 7A E1 E5 3F D6 A7 F7  .h.)....Iz..?...
0010: 45 8F 35 32                                        E.52
]

]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl3.digicert.com/assured-cs-2011a.crl]
, DistributionPoint:
    [URIName: http://crl4.digicert.com/assured-cs-2011a.crl]
]]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.16.840.1.114412.3.1]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 2E 68 74 74 70 3A 2F   2F 77 77 77 2E 64 69 67  ..http://www.dig
0010: 69 63 65 72 74 2E 63 6F   6D 2F 73 73 6C 2D 63 70  icert.com/ssl-cp
0020: 73 2D 72 65 70 6F 73 69   74 6F 72 79 2E 68 74 6D  s-repository.htm

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 82 01 56 1E 82 01 52   00 41 00 6E 00 79 00 20  0..V...R.A.n.y.
0010: 00 75 00 73 00 65 00 20   00 6F 00 66 00 20 00 74  .u.s.e. .o.f. .t
0020: 00 68 00 69 00 73 00 20   00 43 00 65 00 72 00 74  .h.i.s. .C.e.r.t
0030: 00 69 00 66 00 69 00 63   00 61 00 74 00 65 00 20  .i.f.i.c.a.t.e.
0040: 00 63 00 6F 00 6E 00 73   00 74 00 69 00 74 00 75  .c.o.n.s.t.i.t.u
0050: 00 74 00 65 00 73 00 20   00 61 00 63 00 63 00 65  .t.e.s. .a.c.c.e
0060: 00 70 00 74 00 61 00 6E   00 63 00 65 00 20 00 6F  .p.t.a.n.c.e. .o
0070: 00 66 00 20 00 74 00 68   00 65 00 20 00 44 00 69  .f. .t.h.e. .D.i
0080: 00 67 00 69 00 43 00 65   00 72 00 74 00 20 00 43  .g.i.C.e.r.t. .C
0090: 00 50 00 2F 00 43 00 50   00 53 00 20 00 61 00 6E  .P./.C.P.S. .a.n
00A0: 00 64 00 20 00 74 00 68   00 65 00 20 00 52 00 65  .d. .t.h.e. .R.e
00B0: 00 6C 00 79 00 69 00 6E   00 67 00 20 00 50 00 61  .l.y.i.n.g. .P.a
00C0: 00 72 00 74 00 79 00 20   00 41 00 67 00 72 00 65  .r.t.y. .A.g.r.e
00D0: 00 65 00 6D 00 65 00 6E   00 74 00 20 00 77 00 68  .e.m.e.n.t. .w.h
00E0: 00 69 00 63 00 68 00 20   00 6C 00 69 00 6D 00 69  .i.c.h. .l.i.m.i
00F0: 00 74 00 20 00 6C 00 69   00 61 00 62 00 69 00 6C  .t. .l.i.a.b.i.l
0100: 00 69 00 74 00 79 00 20   00 61 00 6E 00 64 00 20  .i.t.y. .a.n.d.
0110: 00 61 00 72 00 65 00 20   00 69 00 6E 00 63 00 6F  .a.r.e. .i.n.c.o
0120: 00 72 00 70 00 6F 00 72   00 61 00 74 00 65 00 64  .r.p.o.r.a.t.e.d
0130: 00 20 00 68 00 65 00 72   00 65 00 69 00 6E 00 20  . .h.e.r.e.i.n.
0140: 00 62 00 79 00 20 00 72   00 65 00 66 00 65 00 72  .b.y. .r.e.f.e.r
0150: 00 65 00 6E 00 63 00 65   00 2E                    .e.n.c.e..

]]  ]
]

[5]: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
 codeSigning
]

[6]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 DigitalSignature
]

[7]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:false
 PathLen: undefined
]

[8]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://ocsp.digicert.com,
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://cacerts.digicert.com/DigiCertAssuredIDCodeSigningCA-1.crt]
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: 07 7C 67 B7 83 DF 8A 88   64 BF 48 B2 BF 30 51 8A  ..g.....d.H..0Q.
0010: D0 00 C4 84 72 6D 25 DE   EA 7D 88 6C EC D3 AE 96  ....rm%....l....
0020: 53 F7 F3 DC 94 C0 96 5F   56 BB A8 47 6B 0D 8E 57  S......_V..Gk..W
0030: FE 80 89 C0 9B 74 A6 CD   E1 99 C0 21 00 E6 8C A9  .....t.....!....
0040: 16 B2 45 42 E2 D4 31 45   6D 82 AD 28 AA 0B 77 6A  ..EB..1Em..(..wj
0050: 83 74 1D 20 62 32 E3 BD   52 FD 33 F2 3E 35 DE F3  .t. b2..R.3.>5..
0060: 37 5B FA 74 3C FB C8 BE   CD 2C 2E D7 08 5F 91 68  7[.t<....,..._.h
0070: 70 55 63 2D 01 14 BA 74   D3 7A 08 7A 2C CD 2D 36  pUc-...t.z.z,.-6
```

```
0080: 2F 62 B0 FA FE 69 FB 9C   31 E0 79 EF 14 90 EA 7D  /b...i..1.y.....
0090: C5 F3 85 74 F3 80 22 7B   2A D3 2F 37 4E 49 C7 91  ...t..".*./7NI..
00A0: FF E7 13 DB 9B 9F D1 58   9A 47 11 EA A7 3B 27 55  .......X.G...;'U
00B0: AB E9 5E 8E 62 40 5A F6   6E 29 4B 2C CE BF 72 5B  ..^.b@Z.n)K,..r[
00C0: 56 01 8D 1D BB 08 46 CA   DA 6E BD BE EB 9A BD 6C  V.....F..n.....l
00D0: C6 81 82 D1 B2 2E A4 0B   1F E2 78 82 0A B1 1E 52  ..........x....R
00E0: D4 CD 99 D2 7B 87 C1 62   62 D8 A5 39 AB EE C0 2D  .......bb..9...-
00F0: 23 F0 C3 56 1B 19 1A AC   04 D9 BB 2A 46 C6 87 91  #..V.......*F...

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIHDzCCBfegAwIBAgIQBKfkd6B7+Z8WnZg7Vi8jsjANBgkqhkiG9w0BAQUFADBv
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMS4wLAYDVQQDEyVEaWdpQ2VydCBBc3N1cmVkIElEIENv
ZGUgU2lnbmluZyBDQS0xMB4XDTEyMTAxNTAwMDAwMFoXDTEzMTAyMzEyMDAwMFow
gdoxCzAJBgNVBAYTAlBFMQ0wCwYDVQQIEwRMaW1hMQ0wCwYDVQQHEwRMaW1hMUQw
QgYDVQQKDDtSZWdpc3RybyBOYWNpb25hbCBkZSBJZGVudGlmaWNhY2nDs24geSBF
c3RhZG8gQ2l2aWwsIFJFTklFQzEhMB8GA1UECwwYR2VyZW5jaWEgZGUgSW5mb3Jt
w6F0aWNhMUQwQgYDVQQDDDtSZWdpc3RybyBOYWNpb25hbCBkZSBJZGVudGlmaWNh
Y2nDs24geSBFc3RhZG8gQ2l2aWwsIFJFTklFQzCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAI3ygVZHAT+HBTv1X8t1RXr0H7GM1h9tglwh8URmATSF2xpy
WICPeWtG7s3lc81Na5sSLHEu8oQFTOqAQTiqbSjMgtNKZGyWLeOpBHYvzp8q4Yk2
YdUU7MqYM9vt/KNCSl7gNoX0KDuwDgow5xrecmistbPMdX60B7i8TdW6AS9u+2x0
r8o7zrrMQafp208jjcRMyq11fMv5WBPjqIx4lCRNLt8SdOkFevv5nDoWZAtDfDbh
cYD+po0EqU3Q9dPuKdQ4n5B1Jt3y0hJnniJ93aV3xT8yXHsQEUY+qN0TNJ6kIup4
Alx7a6X3899H5X2mgzeHuzCLy0C8vWA9/yCyeW0CAwEAAaOCAzkwggM1MB8GA1Ud
IwQYMBaAFHtozimqwBe+SXrh5T/Wp/dFjzUyMB0GA1UdDgQWBBRvoRJb4585E8Qe
8aI3NMj80TsPzzAOBgNVHQ8BAf8EBAMCB4AwEwYDVR0lBAwwCgYIKwYBBQUHAwMw
cwYDVR0fBGwwajAzoDGgL4YtaHR0cDovL2NybDMuZGlnaWNlcnQuY29tL2Fzc3Vy
ZWQtY3MtMjAxMWEuY3JsMDOgMaAvhi1odHRwOi8vY3JsNC5kaWdpY2VydC5jb20v
YXNzdXJlZC1jcy0yMDExYS5jcmwwggHEBgNVHSAEggG7MIIBtzCCAbMGCWCGSAGG
/WwDATCCAaQwOgYIKwYBBQUHAgEWLmh0dHA6Ly93d3cuZGlnaWNlcnQuY29tL3Nz
bC1jcHMtcmVwb3NpdG9yeS5odG0wggFkBggrBgEFBQcCAjCCAVYeggFSAEEAbgB5
ACAAdQBzAGUAIABvAGYAIAB0AGgaAQBzACAAQwBlAHIAdABpAGYAaQBjAGEAdABl
ACAAYwBvAG4AcwB0AGkAdAB1AHQAZQBzACAAYQBjAGMAZQBwAHQAYQBuAGMAZQAg
AG8AZgAgAHQAaABlACAARABpAGcAaQBDAGUAcgB0ACAAQwBQAC8AQwBQAFMAIABh
AG4AZAAgAHQAaABlACAAUgBlAGwAeQBpAG4AZwAgAFAAYQByAHQAeQAgAEEAZwBy
AGUAZQBtAGUAbgB0ACAAdwBoAGkAYwBoACAAbABpAG0aQB0ACAAbABpAGEAYgBp
AGwAaQB0AHkAIABhAG4AZAAgAGEAcgBlACAAaQBuAGMAbwByAHAAbwByAGEAdABl
AGQAIABoAGUAcgBlAGkAbgAgAGIAeQAgAHIAZQBmAGUAcgBlAG4AYwBlAC4wgYIG
CCsGAQUFBwEBBHYwdDAkBggrBgEFBQcwAYYYaHR0cDovL29jc3AuZGlnaWNlcnQu
Y29tMEwGCCsGAQUFBzAChkBodHRwOi8vY2FjZXJ0cy5kaWdpY2VydC5jb20vRGln
aUNlcnRBc3N1cmVkSURDb2RlU2lnbmluZ0NBLTEuY3J0MAwGA1UdEwEB/wQCMAAw
DQYJKoZIhvcNAQEFBQADggEBAAd8Z7eD34qIZL9Isr8wUYrQAMSEcm0l3up9iGzs
066WU/fz3JTAll9Wu6hHaw2OV/6AicCbdKbN4ZnAIQDmjKkWskVC4tQxRW2CrSiq
C3dqg3QdIGIy471S/TPyPjXe8zdb+nQ8+8i+zSwu1whfkWhwVWMtARS6dNN6CHos
zS02L2Kw+v5p+5wx4HnvFJDqfcXzhXTzgCJ7KtMvN05Jx5H/5xPbm5/RWJpHEeqn
OydVq+lejmJAWvZuKUsszr9yW1YBjR27CEbK2m69vuuavWzGgYLRsi6kCx/ieIIK
sR5S1M2Z0nuHwWJi2KU5q+7ALSPww1YbGRqsBNm7KkbGh5E=
-----END CERTIFICATE-----
```

Certificate Service Provider Name (en): INDENOVA S.L.

Trade name (en)	INDENOVA S.L.
Information URI (en)	HTTP://WWW.INDENOVA.COM
Service provider street address (es)	C/DELS TRAGINERS 14-2ºB 46014 VALENCIA (ESPAÑA)
Service provider street address (en)	C/DELS TRAGINERS 14-2ºB 46014 VALENCIA (ESPAÑA)
Service provider postal code (es)	46014
Service provider postal code (en)	46014
Service provider locality (es)	VALENCIA
Service provider locality (en)	VALENCIA
Service provider state (es)	VALENCIA
Service provider state (en)	VALENCIA
Service provider country (es)	ES
Service provider country (en)	ES

CN=INDENOVA DESARROLLOS, OU=DESARROLLOS, O=INDENOVA, L=VALENCIA, ST=VALENCIA, C=ES

Type	unspecified
Status	undersupervision
Status starting time	2013-03-01T21:37:13.000Z

Service digital identity (X509)

Version	3
Serial number	193
Signature algorithm	SHA1withRSA
Issuer	CN=AC Camerfirma Codesign v2, O=AC Camerfirma SA, OU=http://www.camerfirma.com, SERIALNUMBER=A82743287, L=Madrid (see current address at www.camerfirma.com/address), EMAILADDRESS=info@camerfirma.com, C=ES
Valid from	Tue Nov 16 07:56:24 PET 2010
Valid to	Fri Nov 15 07:56:24 PET 2013
Subject	CN=INDENOVA DESARROLLOS, OU=DESARROLLOS, O=INDENOVA, L=VALENCIA, ST=VALENCIA, C=ES
Public key	Sun RSA public key, 1024 bits modulus: 122757737512434538197709461545554076100134991761681458491776546256401250376723989557240381258762879304730969851383159933569144446535612080767026887482900599667102367709729124760758849708042854475220596254813184297415872074698732020543288671186217681070540313508716222115784619078488110509485917528478089788769 public exponent: 65537
Subject key identifier	fad024ee579e605394c29314764c30bbeb6d903c
CRL distribution points	http://crl.camerfirma.com/codesign_v2.crl http://crl1.camerfirma.com/codesign_v2.crl
Authority key identifier	0481a33081a08014691a9472a0d196ff3d562ad8fe2b4718159db0eea18184a48181307f310b3009060355040613024555312730250603550 40a131e41432043616d65726669726d6120534120434946204138323734333238373123302106035504 0b131a687474703a2f2f7777772e6368616d6265727369676e2e6f726731223020060355040313194368616d62657273206f6620436f6d6d6572636520526f6f7482010c
Key usage	digitalSignature nonRepudiation
Basic constraints	CA=false
SHA1 Thumbprint	7981a7952f5a8446195a2eed54bb686d40160208
SHA256 Thumbprint	32757c5025fdc67c4440c70fbf0925af320c5c84717fefc7fb14fb9941f8dc22

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=INDENOVA DESARROLLOS, OU=DESARROLLOS, O=INDENOVA, L=VALENCIA, ST=VALENCIA, C=ES
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 1024 bits
 modulus:
122757737512434538197709461545554076100134991761681458491776546256401250376723989557240381258762879304730969851383159933569144446535612080767026887482900599667102367709729124760758849708042854475220596254813184297415872074698732020543288671186217681070540313508716222115784619078488110509485917528478089788769
 public exponent: 65537
 Validity: [From: Tue Nov 16 07:56:24 PET 2010,
             To: Fri Nov 15 07:56:24 PET 2013]
 Issuer: CN=AC Camerfirma Codesign v2, O=AC Camerfirma SA, OU=http://www.camerfirma.com, SERIALNUMBER=A82743287, L=Madrid (see current address at
www.camerfirma.com/address), EMAILADDRESS=info@camerfirma.com, C=ES
 SerialNumber: [    c1]

Certificate Extensions: 8
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: FA D0 24 EE 57 9E 60 53   94 C2 93 14 76 4C 30 BB  ..$.W.`S....vL0.
0010: EB 6D 90 3C                                        .m.<
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
```

```
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 69 1A 94 72 A0 D1 96 FF   3D 56 2A D8 FE 2B 47 18  i..r....=V*..+G.
0010: 15 9D B0 EE                                        ....
]

[CN=Chambers of Commerce Root, OU=http://www.chambersign.org, O=AC Camerfirma SA CIF A82743287, C=EU]
SerialNumber: [    0c]
]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.camerfirma.com/codesign_v2.crl]
, DistributionPoint:
    [URIName: http://crl1.camerfirma.com/codesign_v2.crl]
]]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [1.3.6.1.4.1.17326.10.12.2]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 1C 68 74 74 70 3A 2F   2F 70 6F 6C 69 63 79 2E  ..http://policy.
0010: 63 61 6D 65 72 66 69 72   6D 61 2E 63 6F 6D        camerfirma.com

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 7C 1A 7A 43 65 72 74   69 66 69 63 61 64 6F 20  0..zCertificado
0010: 64 65 20 46 69 72 6D 61   20 64 65 20 43 F3 64 69  de Firma de C.di
0020: 67 6F 20 43 61 6D 65 72   66 69 72 6D 61 20 43 6F  go Camerfirma Co
0030: 64 65 73 69 67 6E 20 70   65 72 74 65 6E 65 63 69  design perteneci
0040: 65 6E 74 65 20 61 20 6C   61 20 6F 72 67 61 6E 69  ente a la organi
0050: 7A 61 63 69 F3 6E 20 63   6F 6E 20 69 64 65 6E 74  zaci.n con ident
0060: 69 66 69 63 61 63 69 F3   6E 20 66 69 73 63 61 6C  ificaci.n fiscal
0070: 20 43 49 46 3D 42 39 37   34 35 38 39 39 36         CIF=B97458996

]]  ]
]

[5]: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
 codeSigning
 1.3.6.1.4.1.311.2.1.22
]

[6]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 DigitalSignature
 Non_repudiation
]

[7]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://www.camerfirma.com/certs/CODESIGN_v2.crt,
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://ocsp.camerfirma.com]
]

[8]: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
 CA:false
 PathLen: undefined
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: B5 5B B6 5C 1E 0C AC DD   49 DA 3E 4D 44 6D B2 FE  .[.\....I.>MDm..
0010: 92 AC A4 13 7A B2 84 22   5A 63 B9 12 B4 C0 FD 13  ....z.."Zc......
0020: 06 2A B1 E9 80 21 80 5A   32 4E 53 50 46 AE FD 7E  .*...!.Z2NSPF...
0030: 36 43 7C 55 5E 81 1E 83   A8 85 7A FA CB CF 8B F5  6C.U^.....z.....
0040: AE 61 DD 2D E0 57 D6 88   5E 25 20 2A C2 08 D7 2E  .a.-.W..^% *....
0050: 4E D9 D3 A0 8A DE C4 3E   A6 FA 18 50 82 29 9F 9E  N......>...P.)..
0060: 15 42 D7 DE 13 DF FC 40   A0 14 BB CF BB EC 91 3F  .B.....@.......?
0070: D5 87 3B 37 D1 07 90 15   96 E5 ED EA E2 70 56 07  ..;7.........pV.
0080: 3D 58 81 1D 51 F3 FF 50   96 BF 04 FF 5E D6 01 EF  =X..Q..P....^...
0090: 6C D0 16 8C 87 A2 A2 5A   5C EE 8B CD FB AC 55 77  l......Z\.....Uw
00A0: FB D9 BD B2 F4 E7 CD A2   AD 38 89 42 97 24 34 28  .........8.B.$4(
00B0: 54 A3 48 C5 D9 9F 3A CD   70 20 36 BB 14 A8 A2 53  T.H...:.p 6....S
00C0: 41 FB 0B FC 70 21 40 B0   3A BA C3 2D D7 39 41 F6  A...p!@.:...-.9A.
00D0: 6F DE 87 BF 1C 3E EF 8B   48 AC F3 17 8C 6C A1 29  o....>..H....l.)
00E0: 65 A1 2F 38 61 EF AE F2   24 0D 39 DE 9E 59 5E C3  e./8a...$.9..Y^.
00F0: 9F 5F 04 90 88 82 D9 C4   F1 D0 BD 6F AE E9 16 8D  ._.........o....

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGKTCCBRGgAwIBAgICAMEwDQYJKoZIhvcNAQEFBQAwge0xCzAJBgNVBAYTAkVT
MSIwIAYJKoZIhvcNAQkBFhNpbmZvQGNhbWVyZmlybWEuY29tMUMwQQYDVQQHEzpN
YWRyaWQgKHNlZSBjdXJyZW50IGFkZHJlc3MgYXQgd3d3LmNhbWVyZmlybWEuY29t
```

L2FkZHJlc3MpMRIwEAYDVQQFEwlBODI3NDMyODcxIjAgBgNVBAsTGWh0dHA6Ly93
d3cuY2FtZXJmaXJtYS5jb20xGTAXBgNVBAoTEEFDIENhbWVyZmlybWEgU0ExIjAg
BgNVBAMTGUFDIENhbWVyZmlybWEgQ29kZXNpZ24gdjIwHhcNMTAxMTE2MTI1NjI0
WhcNMTMxMTE1MTI1NjI0WjB7MQswCQYDVQQGEwJFUzERMA8GA1UECBMIVkFMRU5D
SUExETAPBgNVBAcTCFZBTEVOQ0lBMREwDwYDVQQKEwhJTkRFTk9WQTEUMBIGA1UE
CxMLREVTQVJST0xMT1MxHTAbBgNVBAMTFElOREVOT1ZBIERFU0FSUk9MTE9TMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCu0BUH8GwJMMwBJqIq2dHS46kwE44v
rLfrwqOpE92Rgsmae57AEGR5BeLQRDs0GDt/o6l6wbZo0D+NJtYw5UMYgxlmKdRm
ilMZ9dt8/3OHzlwKD+OfW0+V1yT2KhmpfAJ/eP9IQAyVe1X6GpIv6/MPLWi4bpCM
FGXbeLFU0my9YQIDAQABo4ICxjCCAsIwCQYDVR0TBAIwADAOBgNVHQ8BAf8EBAMC
BsAwHQYDVR0OBBYEFPrQJO5XnmBTlMKTFHZMMLvrbZA8MIGrBgNVHSMEgaMwgaCA
FGkalHKg0Zb/PVYq2P4rRxgVnbDuoYGEpIGBMH8xCzAJBgNVBAYTAkVVMScwJQYD
VQQKEx5BQyBDYW1lcmZpcm1hIFNBIENJRiBBODI3NDMyODcxIzAhBgNVBAsTGmh0
dHA6Ly93d3cuY2hhbWJlcnNpZ24ub3JnMSIwIAYDVQQDExlDaGFtYmVycyBvZiBD
b21tZXJjZSBSb290ggEMMB8GA1UdJQQYMBYGCCsGAQUFBwMDBgorBgEEAYI3AgEW
MHMGCCsGAQUFBwEBBGcwZTA7BggrBgEFBQcwAoYvaHR0cDovL3d3dy5jYW1lcmZp
cm1hLmNvbS9jZXJ0cy9DT0RFU0lHTl92Mi5jcnQwJgYIKwYBBQUHMAGGGmh0dHA6
Ly9vY3NwLmNhbWVyZmlybWEuY29tMGwGA1UdHwRlMGMwL6AtoCuGKWh0dHA6Ly9j
cmwuY2FtZXJmaXJtYS5jb20vY29kZXNpZ25fdjIuY3JsMDCgLqAshipodHRwOi8v
Y3JsMS5jYW1lcmZpcm1hLmNvbS9jb2Rlc2lnbl92Mi5jcmwwgdMGA1UdIASByzCB
yDCBxQYLKwYBBAGBhy4KDAIwgbUwKAYIKwYBBQUHAgEWHGh0dHA6Ly9wb2xpY3ku
Y2FtZXJmaXJtYS5jb20wgYgGCCsGAQUFBwICMHwaekNlcnRpZmljYWRvIGRlIEZp
cm1hIGRlIEPzZGlnbyBDYW1lcmZpcm1hIENvZGVzaWduIHBlcnRlbmVjaWVudGUg
YSBsYSBvcmdhbml6YWNp824gY29uIGlkZW50aWZpY2fjafNuIGZpc2NhbCBDSUY9
Qjk3NDU4OTk2MA0GCSqGSIb3DQEBBQUAA4IBAQC1W7ZcHgys3UnaPk1EbbL+kqyk
E3qyhCJaY7kStMD9EwYqsemAIYBaMk5TUEau/X42Q3xVXoEeg6iFevrLz4v1rmHd
LeBX1oheJSAqwgjXLk7Z06CK3sQ+pvoYUIIpn54VQtfeE9/8QKAUu8+77JE/1Yc7
N9EHkBWW5e3q4nBWBz1YgR1R8/9Qlr8E/17WAe9s0BaMh6KiWlzui837rFV3+9m9
svTnzaKtOIlClyQ0KFSjSMXZnzrNcCA2uxSoolNB+wv8cCFAsDq6wy3XOUH2b96H
vxw+74tIrPMXjGyhKWWhLzhh767yJA053p5ZXsOfXwSQiILZxPHQvW+u6RaN
-----END CERTIFICATE-----

Certificate Service Provider Name (en): ENTRUST

Trade name (en)	ENTRUST
Information URI (en)	HTTP://WWW.ENTRUST.NET
Service provider street address (es)	THREE LINCOLN CENTRE 5430 LDJ FREE WAY SUITE 1250
Service provider street address (en)	THREE LINCOLN CENTRE 5430 LDJ FREE WAY SUITE 1250
Service provider postal code (es)	75240
Service provider postal code (en)	75240
Service provider locality (es)	DALLAS
Service provider locality (en)	DALLAS
Service provider state (es)	TEXAS
Service provider state (en)	TEXAS
Service provider country (es)	US
Service provider country (en)	US

CN=Entrust.net Secure Server Certification Authority, OU=(c) 1999 Entrust.net Limited, OU=www.entrust.net/CPS incorp. by ref. (limits liab.), O=Entrust.net, C=US

Type	CA/QC
Status	undersupervision
Status starting time	2013-07-23T21:21:08.000Z

Service digital identity (X509)

Version	3
Serial number	927650371
Signature algorithm	SHA1withRSA
Issuer	CN=Entrust.net Secure Server Certification Authority, OU=(c) 1999 Entrust.net Limited, OU=www.entrust.net/CPS incorp. by ref. (limits liab.), O=Entrust.net, C=US

Valid from	Tue May 25 11:09:40 PET 1999
Valid to	Sat May 25 11:39:40 PET 1999
Subject	CN=Entrust.net Secure Server Certification Authority, OU=(c) 1999 Entrust.net Limited, OU=www.entrust.net/CPS incorp. by ref. (limits liab.), O=Entrust.net, C=US
Public key	Sun RSA public key, 1024 bits modulus: 144067023913051061401427662951005762134922353734488468053603530223452408322326917369347612678930500793708458747092762943382762018047024013938414215872028527163969125655573945488614401571467677066488315957153441759858575776484848611157850921563438091296557524842885335944479053857025193408242979060399539152451 public exponent: 3
Subject key identifier	f0176213553db3ff0a006bfb508497f3ed62d01a
CRL distribution points	http://www.entrust.net/CRL/net1.crl
Authority key identifier	041830168014f0176213553db3ff0a006bfb508497f3ed62d01a
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	99a69be61afe886b4d2b82007cb854fc317e1539
SHA256 Thumbprint	62f240278c564c4dd8bf7d9d4f6f366ea894d22f5f34d989a983acec2fffed50

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=Entrust.net Secure Server Certification Authority, OU=(c) 1999 Entrust.net Limited, OU=www.entrust.net/CPS incorp. by ref. (limits liab.), O=Entrust.net, C=US
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 1024 bits
 modulus:
144067023913051061401427662951005762134922353734488468053603530223452408322326917369347612678930500793708458747092762943382762018047024013938414215872028527163969125655573945488614401571467677066488315957153441759858575776484848611157850921563438091296557524842885335944479053857025193408242979060399539152451
 public exponent: 3
 Validity: [From: Tue May 25 11:09:40 PET 1999,
             To: Sat May 25 11:39:40 PET 2019]
 Issuer: CN=Entrust.net Secure Server Certification Authority, OU=(c) 1999 Entrust.net Limited, OU=www.entrust.net/CPS incorp. by ref. (limits liab.), O=Entrust.net, C=US
 SerialNumber: [    374ad243]

Certificate Extensions: 8
[1]: ObjectId: 1.2.840.113533.7.65.0 Criticality=false
Extension unknown: DER encoded OCTET string =
0000: 04 0C 30 0A 1B 04 56 34   2E 30 03 02 04 90        ..0...V4.0....


[2]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: F0 17 62 13 55 3D B3 FF   0A 00 6B FB 50 84 97 F3  ..b.U=....k.P...
0010: ED 62 D0 1A                                        .b..
]
]

[3]: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
  SSL CA
  S/MIME CA
  Object Signing CA]

[4]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: F0 17 62 13 55 3D B3 FF   0A 00 6B FB 50 84 97 F3  ..b.U=....k.P...
0010: ED 62 D0 1A                                        .b..
]

]

[5]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [CN=CRL1, CN=Entrust.net Secure Server Certification Authority, OU=(c) 1999 Entrust.net Limited, OU=www.entrust.net/CPS incorp. by ref. (limits liab.), O=Entrust.net,
C=US]
, DistributionPoint:
    [URIName: http://www.entrust.net/CRL/net1.crl]
]]

[6]: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
 Key_CertSign
 Crl_Sign
```

```
]

[7]: ObjectId: 2.5.29.16 Criticality=false
PrivateKeyUsage: [
From: Tue May 25 11:09:40 PET 1999, To: Sat May 25 11:09:40 PET 2019]

[8]: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: 90 DC 30 02 FA 64 74 C2   A7 0A A5 7C 21 8D 34 17  ..0..dt.....!.4.
0010: A8 FB 47 0E FF 25 7C 8D   13 0A FB E4 98 B5 EF 8C  ..G..%..........
0020: F8 C5 10 0D F7 92 BE F1   C3 D5 D5 95 6A 04 BB 2C  ............j..,
0030: CE 26 36 65 C8 31 C6 E7   EE 3F E3 57 75 84 7A 11  .&6e.1...?.Wu.z.
0040: EF 46 4F 18 F4 D3 98 BB   A8 87 32 BA 72 F6 3C E2  .FO.......2.r.<.
0050: 3D 9F D7 1D D9 C3 60 43   8C 58 0E 22 96 2F 62 A3  =.....`C.X."./b.
0060: 2C 1F BA AD 05 EF AB 32   78 87 A0 54 73 19 B5 5C  ,.......2x..Ts..\
0070: 05 F9 52 3E 6D 2D 45 0B   F7 0A 93 EA ED 06 F9 B2  ..R>m-E.........

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIE2DCCBEGgAwIBAgIEN0rSQzANBgkqhkiG9w0BAQUFADCBwzELMAkGA1UEBhMC
VVMxFDASBgNVBAoTC0VudHJ1c3QubmV0MTswOQYDVQQLEzJ3d3cuZW50cnVzdC5u
ZXQvQ1BTIGluY29ycC4gYnkgcmVmLiAobGltaXRzIGxpYWIuKTElMCMGA1UECxMc
KGMpIDE5OTkgRW50cnVzdC5uZXQgTGltaXRlZDE6MDgGA1UEAxMxRW50cnVzdC5u
ZXQgU2VjdXJlIFNlcnZlciBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAeFw05OTA1
MjUxNjA5NDBaFw0xOTA1MjUxNjM5NDBaMIHDMQswCQYDVQQGEwJVUzEUMBIGA1UE
ChMLRW50cnVzdC5uZXQxOzA5BgNVBAsTMnd3dy5lbnRydXN0Lm5ldC9DUFMgaW5j
b3JwLiBieSByZWYuIChsaW1pdHMgbGlhYi4pMSUwIwYDVQQLExwoYykgMTk5OSBF
bnRydXN0Lm5ldCBMaW1pdGVkMTowOAYDVQQDEzFFbnRydXN0Lm5ldCBTZWN1cmUg
U2VydmVyIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MIGdMA0GCSqGSIb3DQEBAQUA
A4GLADCBhwKBgQDNKIM0VBuJ8w+vN5Ex/68xYMmo6LIQaO2f55M28Qpku0f1BBc/
I0dNxScZgSYMVHINiC3ZH5oSn7yzcdOAGT9HZnuMNSjSuQrfJNqc1lB5gXpa0zf3
wkrYKZImZNHkmGw6AIr1NJtl+O3jEP/9uElY3KDegjlrgbEWGWG5VLbmQwIBA6OC
AdcwggHTMBEGCWCGSAGG+EIBAQQEAwIABzCCARkGA1UdHwSCARAwggEMMIHeoIHb
oIHYpIHVMIHSMQswCQYDVQQGEwJVUzEUMBIGA1UEChMLRW50cnVzdC5uZXQxOzA5
BgNVBAsTMnd3dy5lbnRydXN0Lm5ldC9DUFMgaW5jb3JwLiBieSByZWYuIChsaW1p
dHMgbGlhYi4pMSUwIwYDVQQLExwoYykgMTk5OSBFbnRydXN0Lm5ldCBMaW1pdGVk
MTowOAYDVQQDEzFFbnRydXN0Lm5ldCBTZWN1cmUgU2VydmVyIENlcnRpZmljYXRp
b24gQXV0aG9yaXR5MQ0wCwYDVQQDEwRDUkwxMCmgJ6AlhiNodHRwOi8vd3d3LmVu
dHJ1c3QubmV0L0NSTC9uZXQxLmNybDArBgNVHRAEJDAigA8xOTk5MDUyNTE2MDk0
MFqBDzIwMTkwNTI1MTYwOTQwWjALBgNVHQ8EBAMCAQYwHwYDVR0jBBgwFoAU8Bdi
E1U9s/8KAGv7UISX8+1i0BowHQYDVR0OBBYEFPAXYhNVPbP/CgBr+1CEl/PtYtAa
MAwGA1UdEwQFMAMBAf8wGQYJKoZIhvZ9B0EABAwwChsEVjQuMAMCBJAwDQYJKoZI
hvcNAQEFBQADgYEAkNwwAvpkdMKnCqV8IY00F6j7Rw7/JXyNEwr75Ji174z4xRAN
95K+8cPV1ZVqBLsszi Y2ZcgxxufuP+NXdYR6Ee9GTxj005i7qIcyunL2POI9n9cd
2cNgQ4xYDiKWL2KjLB+6rQXvqzJ4h6BUcxm1XAX5Uj5tLUUL9wqT6u0G+bI=
-----END CERTIFICATE-----
```

CN=Entrust.net Secure Server Certification Authority, OU=(c) 1999 Entrust.net Limited, OU=www.entrust.net/CPS incorp. by ref. (limits liab.), O=Entrust.net, C=US

Type	CA/QC
Status	ted
Status starting time	2013-06-19T17:56:23.000Z

Service digital identity (X509)

Version	3
Serial number	927650371
Signature algorithm	SHA1withRSA
Issuer	CN=Entrust.net Secure Server Certification Authority, OU=(c) 1999 Entrust.net Limited, OU=www.entrust.net/CPS incorp. by ref. (limits liab.), O=Entrust.net, C=US
Valid from	Tue May 25 11:09:40 PET 1999
Valid to	Sat May 25 11:39:40 PET 2019
Subject	CN=Entrust.net Secure Server Certification Authority, OU=(c) 1999 Entrust.net Limited, OU=www.entrust.net/CPS incorp. by ref. (limits liab.), O=Entrust.net, C=US

Public key	Sun RSA public key, 1024 bits modulus: 144067023913051061401427662951005762134922353734488468053603530223452408322326917369347612678930500793708458747092762943382762018047024013938414215872028527163969125655573945488614401571467677066488315957153441759858575776484848611157850921563438091296557524842885335944479053857025193408242979060399539152451 public exponent: 3
Subject key identifier	f0176213553db3ff0a006bfb508497f3ed62d01a
CRL distribution points	http://www.entrust.net/CRL/net1.crl
Authority key identifier	041830168014f0176213553db3ff0a006bfb508497f3ed62d01a
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	99a69be61afe886b4d2b82007cb854fc317e1539
SHA256 Thumbprint	62f240278c564c4dd8bf7d9d4f6f366ea894d22f5f34d989a983acec2fffed50

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=Entrust.net Secure Server Certification Authority, OU=(c) 1999 Entrust.net Limited, OU=www.entrust.net/CPS incorp. by ref. (limits liab.), O=Entrust.net, C=US
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 1024 bits
 modulus:
144067023913051061401427662951005762134922353734488468053603530223452408322326917369347612678930500793708458747092762943382762018047024013938414215872028527163969125655573945488614401571467677066488315957153441759858575776484848611157850921563438091296557524842885335944479053857025193408242979060399539152451
 public exponent: 3
 Validity: [From: Tue May 25 11:09:40 PET 1999,
             To: Sat May 25 11:39:40 PET 2019]
 Issuer: CN=Entrust.net Secure Server Certification Authority, OU=(c) 1999 Entrust.net Limited, OU=www.entrust.net/CPS incorp. by ref. (limits liab.), O=Entrust.net, C=US
 SerialNumber: [    374ad243]

Certificate Extensions: 8
[1]: ObjectId: 1.2.840.113533.7.65.0 Criticality=false
Extension unknown: DER encoded OCTET string =
0000: 04 0C 30 0A 1B 04 56 34   2E 30 03 02 04 90        ..0...V4.0....


[2]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: F0 17 62 13 55 3D B3 FF   0A 00 6B FB 50 84 97 F3  ..b.U=....k.P...
0010: ED 62 D0 1A                                        .b..
]
]

[3]: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
  SSL CA
  S/MIME CA
  Object Signing CA]

[4]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: F0 17 62 13 55 3D B3 FF   0A 00 6B FB 50 84 97 F3  ..b.U=....k.P...
0010: ED 62 D0 1A                                        .b..
]

]

[5]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [CN=CRL1, CN=Entrust.net Secure Server Certification Authority, OU=(c) 1999 Entrust.net Limited, OU=www.entrust.net/CPS incorp. by ref. (limits liab.), O=Entrust.net,
C=US]
, DistributionPoint:
    [URIName: http://www.entrust.net/CRL/net1.crl]
]]

[6]: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[7]: ObjectId: 2.5.29.16 Criticality=false
PrivateKeyUsage: [
From: Tue May 25 11:09:40 PET 1999, To: Sat May 25 11:09:40 PET 2019]

[8]: ObjectId: 2.5.29.19 Criticality=false
```

```
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: 90 DC 30 02 FA 64 74 C2   A7 0A A5 7C 21 8D 34 17  ..0..dt.....!.4.
0010: A8 FB 47 0E FF 25 7C 8D   13 0A FB E4 98 B5 EF 8C  ..G..%..........
0020: F8 C5 10 0D F7 92 BE F1   C3 D5 D5 95 6A 04 BB 2C  ............j..,
0030: CE 26 36 65 C8 31 C6 E7   EE 3F E3 57 75 84 7A 11  .&6e.1...?.Wu.z.
0040: EF 46 4F 18 F4 D3 98 BB   A8 87 32 BA 72 F6 3C E2  .FO.......2.r.<.
0050: 3D 9F D7 1D D9 C3 60 43   8C 58 0E 22 96 2F 62 A3  =.....`C.X."./b.
0060: 2C 1F BA AD 05 EF AB 32   78 87 A0 54 73 19 B5 5C  ,.......2x..Ts..\
0070: 05 F9 52 3E 6D 2D 45 0B   F7 0A 93 EA ED 06 F9 B2  ..R>m-E.........

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIE2DCCBEGgAwIBAgIEN0rSQzANBgkqhkiG9w0BAQUFADCBwzELMAkGA1UEBhMC
VVMxFDASBgNVBAoTC0VudHJ1c3QubmV0MTswOQYDVQQLEzJ3d3cuZW50cnVzdC5u
ZXQvQ1BTIGluY29ycC4gYnkgcmVmLiAobGltaXRzIGxpYWIuKTElMCMGA1UECxMc
KGMpIDE5OTkgRW50cnVzdC5uZXQgTGltaXRlZDE6MDgGA1UEAxMxRW50cnVzdC5u
ZXQgU2VjdXJlIFNlcnZlciBDZXJ0aW9uIEF1dGhvcml0eTAeFw05OTA1
MjUxNjA5NDBaFw0xOTA1MjUxNjM5NDBaMIHDMQswCQYDVQQGEwJVUzEUMBIGA1UE
ChMLRW50cnVzdC5uZXQxOzA5BgNVBAsTMnd3dy5lbnRydXN0Lm5ldC9DUFMgaW5j
b3JwLiBieSByZWYuIChsaW1pdHMgbGlhYi4pMSUwIwYDVQQLExwoYykgMTk5OSBF
bnRydXN0Lm5ldCBMaW1pdGVkMTowOAYDVQQDEzFFbnRydXN0Lm5ldCBTZWN1cmUg
U2VydmVyIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MIGdMA0GCSqGSIb3DQEBAQUA
A4GLADCBhwKBgQDNKIM0VBuJ8w+vN5Ex/68xYMmo6LIQaO2f55M28Qpku0f1BBc/
I0dNxScZgSYMVHINiC3ZH5oSn7yzcdOAGT9HZnuMNSjSuQrfJNqc1lB5gXpa0zf3
wkrYKZImZNHkmGw6AIr1NJtl+O3jEP/9uElY3KDegjlrgbEWGWG5VLbmQwIBA6OC
AdcwggHTMBEGCWCGSAGG+EIBAQQEAwIABzCCARkGA1UdHwSCARAwggEMMIHeoIHb
oIHYpIHVMIHSMQswCQYDVQQGEwJVUzEUMBIGA1UEChMLRW50cnVzdC5uZXQxOzA5
BgNVBAsTMnd3dy5lbnRydXN0Lm5ldC9DUFMgaW5jb3JwLiBieSByZWYuIChsaW1p
dHMgbGlhYi4pMSUwIwYDVQQLExwoYykgMTk5OSBFbnRydXN0Lm5ldCBMaW1pdGVk
MTowOAYDVQQDEzFFbnRydXN0Lm5ldCBTZWN1cmUgU2VydmVyIENlcnRpZmljYXRp
b24gQXV0aG9yaXR5MQ0wCwYDVQQDEwRDUkwxMCmgJ6AlhiNodHRwOi8vd3d3LmVu
dHJ1c3QubmV0L0NSTC9uZXQxLmNybDArBgNVHRAEJDAigA8xOTk5MDUyNTE2MDk0
MFqBDzIwMTkwNTI1MTYwOTQwWjALBgNVHQ8EBAMCAQYwHwYDVR0jBBgwFoAU8Bdi
E1U9s/8KAGv7UISX8+1i0BowHQYDVR0OBBYEFPAXYhNVPbP/CgBr+1CEl/PtYtAa
MAwGA1UdEwQFMAMBAf8wGQYJKoZIhvZ9B0EABAwwChsEVjQuMAMCBJAwDQYJKoZI
hvcNAQEFBQADgYEAkNwwAvpkdMKnCqV8IY00F6j7Rw7/JXyNEwr75Ji174z4xRAN
95K+8cPV1ZVqBLsszi Y2ZcgxxufuP+NXdYR6Ee9GTxj005i7qIcyunL2POI9n9cd
2cNgQ4xYDiKWL2KjLB+6rQXvqzJ4h6BUcxm1XAX5Uj5tLUUL9wqT6u0G+bI=
-----END CERTIFICATE-----
```

Certificate Service Provider Name (en): DIGI SIGN

Trade name (en)	DIGI SIGN
Information URI (en)	HTTP://WWW.DIGI-SIGN.COM
Service provider street address (es)	SIBTHORPE LANE, RANELAGH
Service provider street address (en)	SIBTHORPE LANE, RANELAGH
Service provider postal code (es)	DUBLIN6
Service provider postal code (en)	DUBLIN6
Service provider locality (es)	DUBLIN
Service provider locality (en)	DUBLIN
Service provider state (es)	DUBLIN
Service provider state (en)	DUBLIN
Service provider country (es)	IR
Service provider country (en)	IR

CN=Digi-Sign CA Digi-ID Xp, OU=Terms and Conditions of use: http://www.digi-sign.com/repository, O=Digi-Sign Limited, L=Dublin, ST=Dublin, C=IE

Type	CA/QC
Status	undersupervision
Status starting time	2014-04-16T15:46:37.000Z

Service digital identity (X509)

Version	3
Serial number	59580510237220695488987717461609009860
Signature algorithm	SHA1withRSA
Issuer	CN=UTN-USERFirst-Client Authentication and Email, OU=http://www.usertrust.com, O=The USERTRUST Network, L=Salt Lake City, ST=UT, C=US
Valid from	Wed Sep 14 19:00:00 PET 2005
Valid to	Tue Jul 09 12:36:58 PET 2019
Subject	CN=Digi-Sign CA Digi-ID Xp, OU=Terms and Conditions of use: http://www.digi-sign.com/repository, O=Digi-Sign Limited, L=Dublin, ST=Dublin, C=IE
Public key	Sun RSA public key, 2048 bits modulus: 26926110584125833537545895214890737273777428404404833368187117345006353 82206638854907255639402631268858109027218760522716093024105309782301692 65481846584276983952678130101005855442277347425780801269842466729514406 88741166302606251599719471211392251867004715622651257111592580722121660 76612259199373641977697325865559113275998785588195551750877764477686073 72211213578864171253109087411666203612809460357649088867687580847748313 83168428605113815928621791735306799688796888810566743964231434014331403 99701330234317974533752792385384527070400262428637000565650050606326008 72128545354715718880241849397782838049182886337 03 public exponent: 65537
Subject key identifier	91b38ae87e166ff9121c3f29a45010440bd97776
CRL distribution points	http://crl.usertrust.com/UTN-USERFirst-ClientAuthenticationandEmail.crl
Authority key identifier	04183016801489826 77dc49d2670004bb450487cde3dae046e7d
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=1
SHA1 Thumbprint	82d06f4188a91dbec05cf0b1a7014b6b84679caf
SHA256 Thumbprint	4709d81e77c0990c38ec8d4577701f9753bac0723a7ecd90706f8ff5568f5bb8

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=Digi-Sign CA Digi-ID Xp, OU=Terms and Conditions of use: http://www.digi-sign.com/repository, O=Digi-Sign Limited, L=Dublin, ST=Dublin, C=IE
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 2048 bits
 modulus:
269261105841258335375458952148907372737774284044048333681871173450063538220663885490725563940263126885810902721876052271609302410530978230169265481846584276983952678130101005855442277347425780801269842466729514406887411663026062515997194712113922518670047156226512571115925807221216607661225919937364197769732586555911327599878558819555175087776447768607372211213578864171253109087411666203612809460357649088867687580847748313831684286051138159286217917353067996887968888105667439642314340143314039970133023431797453375279238538452707040026242863700056565005060632600872128545354715718880241849397782838049182886337 03
 public exponent: 65537
 Validity: [From: Wed Sep 14 19:00:00 PET 2005,
             To: Tue Jul 09 12:36:58 PET 2019]
 Issuer: CN=UTN-USERFirst-Client Authentication and Email, OU=http://www.usertrust.com, O=The USERTRUST Network, L=Salt Lake City, ST=UT, C=US
 SerialNumber: [    2cd2c9f3 d40626af a7c8d70f 74a7d2c4]

Certificate Extensions: 6
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 91 B3 8A E8 7E 16 6F F9   12 1C 3F 29 A4 50 10 44  ......o...?).P.D
0010: 0B D9 77 76                                        ..wv
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 89 82 67 7D C4 9D 26 70   00 4B B4 50 48 7C DE 3D  ..g...&p.K.PH..=
0010: AE 04 6E 7D                                        ..n.
]

]
```

```
[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.usertrust.com/UTN-USERFirst-ClientAuthenticationandEmail.crl]
]]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [1.3.6.1.4.1.6449.1.2.3.1]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 23 68 74 74 70 3A 2F   2F 77 77 77 2E 75 73 65  .#http://www.use
0010: 72 74 72 75 73 74 2E 63   6F 6D 2F 72 65 70 6F 73  rtrust.com/repos
0020: 69 74 6F 72 79                                     itory

]]  ]
 [CertificatePolicyId: [1.3.6.1.4.1.6449.1.2.2.9]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 23 68 74 74 70 3A 2F   2F 77 77 77 2E 64 69 67  .#http://www.dig
0010: 69 2D 73 69 67 6E 2E 63   6F 6D 2F 72 65 70 6F 73  i-sign.com/repos
0020: 69 74 6F 72 79                                     itory

]]  ]
]

[5]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[6]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:1
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: 6E CD 28 36 A9 0F 6C 40   61 76 D3 7C CF 6F 1B 23  n.(6..l@av...o.#
0010: 87 84 AB 5D C9 A9 92 3F   0C 4C EC 90 6C 09 05 5D  ...]...?.L..l..]
0020: DF 58 C8 56 3D D1 3C 3B   C5 81 8D C2 43 A3 77 3D  .X.V=.<;....C.w=
0030: E9 A9 96 5E 21 11 EE 5B   A3 E6 EC C9 87 58 4D 09  ...^!..[.....XM.
0040: A5 8F 01 28 0D 54 74 25   AF 8D 34 58 45 B0 F2 96  ...(.Tt%..4XE...
0050: 1D 5B 8E D0 D6 C8 F8 88   49 C9 E8 E4 B0 86 51 56  .[......I.....QV
0060: BC 3D 3F 69 ED 16 A9 2D   78 E8 E1 A2 30 89 21 4A  .=?i...-x...0.!J
0070: EE 30 9D DB CF 87 36 BC   8E 9B 42 2E 3E CD 57 BE  .0....6...B.>.W.
0080: 4A 4B B7 4E 9E D2 0A 55   14 C5 E3 BC 99 95 81 30  JK.N...U.......0
0090: 0B E5 17 EA 1D C3 AE 9D   B4 77 BF 6E 43 8E 4A 37  .........w.nC.J7
00A0: 69 21 D7 DF 4B 7A 04 19   03 F9 7D 78 48 9C D3 46  i!..Kz.....xH..F
00B0: 5F FD 7C 78 41 D1 69 11   F7 6A 91 39 77 B4 97 78  _..xA.i..j.9w..x
00C0: 29 25 79 2A CF 8C AE B8   98 68 19 02 23 20 1F 54  )%y*.....h..# .T
00D0: 28 1F 01 26 D1 FB 47 5C   CB 1E B6 39 3F 6C 87 67  (..&..G\...9?l.g
00E0: BA 80 58 AB 78 74 E8 E4   D8 CF 17 FF B4 9D DD 9E  ..X.xt..........
00F0: E9 C4 E1 30 36 AB 8B 46   6F EB 8A 7C 8C DA 48 45  ...06..Fo.....HE

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIFSDCCBDCgAwIBAgIQLNLJ89QGJq+nyNcPdKfSxDANBgkqhkiG9w0BAQUFADCB
rjELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAlVUMRcwFQYDVQQHEw5TYWx0IExha2Ug
Q2l0eTEeMBwGA1UEChMVVGhlIFVTRVJUUlVTVCBOZXR3b3JrMSEwHwYDVQQLExho
dHRwOi8vd3d3LnVzZXJ0cnVzdC5jb20xNjA0BgNVBAMTLVVUTi1VU0VSRmlyc3Qt
Q2xpZW50IEF1dGhlbnRpY2F0aW9uIGFuZCBFbWFpbDAeFw0wNTA5MTUwMDAwMDBa
Fw0xOTA3MDkxNzM2NThaMIG4MQswCQYDVQQGEwJJRTEPMA0GA1UECBMGRHVibGlu
MQ8wDQYDVQQHEwZEdWJsaW4xGjAYBgNVBAoTEURpZ2ktU2lnbiBMaW1pdGVkMUkw
RwYDVQQLE0BUZXJtcyBhbmQgQ29uZGl0aW9ucyBvZiB1c2U6IGh0dHA6Ly93d3cu
ZGlnaS1zaWduLmNvbS9yZXBvc2l0b3J5MSAwHgYDVQQDExdEaWdpLVNpZ24gQ0Eg
RGlnaS1JRCBYcDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANVLvuog
GXqclXfAY/jbbPNgI+FY0412xWwGWhdmc4JA2Girci4krL4/KFwKPUdRHvk3DKRN
34i+1QG/PW04L8tkfI7ElDkxGH6dujLorW9lLjjOiYscZaIPnfv+Z8tdg6s77Qrh
G7WbtlAQ3En30HVgQ4NZvbxASOBAFjnIATYKZLCJNZ/pAdGk3o/thfzYKQO+6HVX
752VAwIB2IRtSH9jvuGMoqtllyMlNAa4ZNwuiznYMY3TduaUZY/J+0j/s9cCMz38
A0ah3Ct4sEIfy8KmQJjDwt8MLLxdEBE+lDp+i81MeFY1Yw124Dhl5QRlo+dgMbyF
ptF1f5YSIY7iT2cCAwEAAaOCAVQwggFQMB8GA1UdIwQYMBaAFImCZ33EnSZwAEu0
UEh83j2uBG59MB0GA1UdDgQWBBSRs4rofhZv+RIcPymkUBBEC9l3djAOBgNVHQ8B
Af8EBAMCAQYwEgYDVR0TAQH/BAgwBgEB/wIBATBYBgNVHR8EUTBPME2gS6BJhkdo
dHRwOi8vY3JsLnVzZXJ0cnVzdC5jb20vVVROLVVTRVJGaXJzdC1DbGllbnRBdXRo
ZW50aWNhdGlvbmFuZEVtYWlsLmNybDCBjwYDVR0gBIGHMIGEMEAGCysGAQQBsjEB
AgMBMDEwLwYIKwYBBQUHAgEWI2h0dHA6Ly93d3cudXNlcnRydXN0LmNvbS9yZXBv
c2l0b3J5MEAGCysGAQQBsjEBAgIJMDEwLwYIKwYBBQUHAgEWI2h0dHA6Ly93d3cu
ZGlnaS1zaWduLmNvbS9yZXBvc2l0b3J5MA0GCSqGSIb3DQEBBQUAA4IBAQBuzSg2
qQ9sQGF203zPbxsjh4SrXcmpkj8MTOyQbAkFXd9YyFY90Tw7xYGNwkOjdz3pqZZe
IRHuW6Pm7MmHWE0JpY8BKA1UdCWvjTRYRbDylh1bjtDWyPiISCno5LCGUVa8PT9p
7RapLXjo4aIwiSFK7jCd28+HNryOm0IuPs1XvkpLt06e0gpVFMXjvJmVgTAL5Rfq
HcOunbR3v25Djko3aSHX30t6BBkD+X14SJzTRl/9fHhB0WkR92qROXe0l3gpJXkq
z4yuuJhoGQIjIB9UKB8BJtH7R1zLHrY5P2yHZ7qAWKt4dOjk2M8X/7Sd3Z7pxOEw
NquLRm/rinyM2khF
-----END CERTIFICATE-----
```

Certificate Service Provider Name (en): INTERCAMBIO ELECTRÓNICO DE DATOS Y COMUNICACIONES

Trade name (en)	EDICOM
Information URI (en)	HTTP://ACEDICOM.EDICOMGROUP.COM
Service provider street address (es)	PARQUE TECN. PATERNA. VALENCIA ESPAÑA
Service provider street address (en)	PARQUE TECN. PATERNA. VALENCIA ESPAÑA
Service provider postal code (es)	46980
Service provider postal code (en)	46980
Service provider locality (es)	PATERNA
Service provider locality (en)	PATERNA
Service provider state (es)	VALENCIA
Service provider state (en)	VALENCIA
Service provider country (es)	ES
Service provider country (en)	PE

C=ES, L=Calle Charles Robert Darwin 8 - 46980 - Paterna, O=EDICOM, SERIALNUMBER=B96490867, CN=CAEDICOM01

Type	CA/QC
Status	undersupervision
Status starting time	2015-04-01T21:09:38.000Z

Service digital identity (X509)

Version	3
Serial number	2849013759586421594
Signature algorithm	SHA256withRSA
Issuer	C=ES, O=EDICOM, CN=CAEDICOM Root
Valid from	Tue Jul 22 06:00:43 PET 2014
Valid to	Wed May 22 05:20:00 PET 2024
Subject	C=ES, L=Calle Charles Robert Darwin 8 - 46980 - Paterna, O=EDICOM, SERIALNUMBER=B96490867, CN=CAEDICOM01

Public key	Sun RSA public key, 4096 bits modulus: 56751191118072880989610088055580594823266667966228474915328207766893240 85248832370515078578240603680634239006146099934381739106442693153315879 53572170527005870884253249638403560253212180957381100239914929181940478 65555481954187868399678983340515098614799232418576470475513820603286663 80139562259906710770546776164153950713621513836181994892225447708736150 65960678602875142624352455958565138358378876521740536262840856403242177 76623813412783973465567582770427993563903927844594782973230660558115488 59403040776304910265004099101832448768767837957213719376018073389567978 04000519325395575506192845150033546286871993881447185133413278391350874 88546958501766989824459398957345992951274544225193423823446732889675865 41406758196773277833010356236351083320799333448393774867964179808103446 42856236592102445939981808719888072920423467157590529643119412812863263 53226378429581470468645986708474415721536880925244714283309289133888140 68274387213713513699173652092536878942572099372630678525638920908605308 69454340632775620803107102710952430991101339548454536537408649665863689 59005560890573695998862460480157602830175946875378868335115769954750054 94052243762972713941011453707494046940115619230652407243663782071647445 7346188651102998588178828 1 public exponent: 65537
Subject key identifier	6d6a88f82eea7f2fcdc0f4767793e64532ef8b05
CRL distribution points	http://acedicom.edicomgroup.com/caedicomroot.crl
Authority key identifier	04183016801414cd2a597863ab6119e8b83da1e05ac075e7f9cb
Key usage	digitalSignature keyCertSign cRLSign
Basic constraints	CA=true; PathLen=0
SHA1 Thumbprint	317574de257dba53dae80676a675249d64d7c134
SHA256 Thumbprint	339d15b165ca8161e4d3792618c6fde84e4904d04669541cee6bd333bcd5b5f4

The decoded certificate:


```
[
[
 Version: V3
 Subject: C=ES, L=Calle Charles Robert Darwin 8 - 46980 - Paterna, O=EDICOM, SERIALNUMBER=B96490867, CN=CAEDICOM01
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
56751191118072880989610088055580594823266667966228474915328207766893240852488323705150785782406036806342390061460999343817391064426931533158795357217052700587088425324963840
35602532121809573811002399149291819404786555548195418786839967898334051509861479923241857647047551382060328666380139562259906710770546776164153950713621513836181994892225447
70873615065960678602875142624352455958565138358378876521740536262840856403242177766238134127839734655675827704279935639039278445947829732306605581154885940304077630491026500
40991018324487687678379572137193760180733895679780400051932539557550619284515003354628687199388144718513341327839135087488546958501766989824459398957345992951274544225193423
82344673288967586541406758196773277833010356236351083320799333448393774867964179808103446428562365921024459399818087198880729204234671575905296431194128128632635322637842958
14704686459867084744157215368809252447142833092891338881406827438721371351369917365209253687894257209937263067852563892090860530869454340632775620803107102710952430991101339
54845453653740864966586368959005560890573695998862460480157602830175946875378868335115769954750054940522437629727139410114537074940469401156192306524072436637820716474457346
1886511029985881788281
 public exponent: 65537
 Validity: [From: Tue Jul 22 06:00:43 PET 2014,
             To: Wed May 22 05:20:00 PET 2024]
 Issuer: C=ES, O=EDICOM, CN=CAEDICOM Root
 SerialNumber: [    2789baeb 6c594b5a]

Certificate Extensions: 8
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 6D 6A 88 F8 2E EA 7F 2F   CD C0 F4 76 77 93 E6 45  mj...../...vw..E
0010: 32 EF 8B 05                                        2...
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 14 CD 2A 59 78 63 AB 61   19 E8 B8 3D A1 E0 5A C0  ..*Yxc.a...=..Z.
0010: 75 E7 F9 CB                                        u...
]

]

[3]: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
 RFC822Name: acedicom@edicomgroup.com
]
```

```
[4]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://acedicom.edicomgroup.com/caedicomroot.crl]
]]

[5]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 DigitalSignature
 Key_CertSign
 Crl_Sign
]

[6]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [1.3.6.1.4.1.30051.2.3.1.1]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 42 1E 40 00 43 00 65   00 72 00 74 00 69 00 66  0B.@.C.e.r.t.i.f
0010: 00 69 00 63 00 61 00 74   00 69 00 6F 00 6E 00 20  .i.c.a.t.i.o.n.
0020: 00 50 00 72 00 61 00 63   00 74 00 69 00 63 00 65  .P.r.a.c.t.i.c.e
0030: 00 20 00 53 00 74 00 61   00 74 00 65 00 6D 00 65  . .S.t.a.t.e.m.e
0040: 00 6E 00 74                                        .n.t

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 1F 68 74 74 70 3A 2F   2F 61 63 65 64 69 63 6F  ..http://acedico
0010: 6D 2E 65 64 69 63 6F 6D   67 72 6F 75 70 2E 63 6F  m.edicomgroup.co
0020: 6D                                                 m

]]  ]
]

[7]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:0
]

[8]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://acedicom.edicomgroup.com/certs/caedicomroot.cer,
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://ocsp.acedicom.edicomgroup.com/caedicomroot]
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 3F AA 3D 4B 11 B6 39 4D   7F 49 8F D7 8B F6 19 7F  ?.=K..9M.I......
0010: 5B 02 11 9D 0D 5D 1A 70   6E C0 85 4E 56 14 8C 5A  [....].pn..NV..Z
0020: DC 9A 37 D4 B5 96 75 78   E4 27 AF DE F5 D4 ED 26  ..7...ux.'.....&
0030: 74 2F CC 60 88 81 5A F1   92 95 AA 15 E8 15 05 BA  t/.`..Z.........
0040: 89 4E 73 E3 70 29 9A F9   89 A2 2D 99 53 71 66 A8  .Ns.p)....-.Sqf.
0050: E7 6A BC E3 E1 20 80 FE   1C BC F5 45 E0 E1 16 7A  .j... .....E...z
0060: 1D AA F0 CD 17 01 0A AC   4F 3F BE 0D 8C 8B C1 49  ........O?.....I
0070: 8B F9 27 82 DC C6 91 85   0B EB 3A F0 B1 76 52 FA  ..'.......:..vR.
0080: 2F CA 26 B9 C9 F2 B1 C7   D5 7D 0E 42 38 1C 06 80  /.&........B8...
0090: 50 A6 F0 A9 4A 3C 67 86   D5 4C 2C 6F BB 37 36 A1  P...J<g..L,o.76.
00A0: 79 43 7E E1 59 D3 76 35   EC B6 AB C5 D1 B6 49 B2  yC..Y.v5......I.
00B0: BF FA AE 19 08 C7 EF 20   30 E7 9D 9A A0 78 0B 73  ....... 0....x.s
00C0: F2 B2 62 B1 01 A6 A0 4F   B5 AA FA E0 1F EF C9 78  ..b....O.......x
00D0: BF 78 27 60 AB 58 51 BE   0A 46 CB D1 2E 0F 65 1D  .x'`.XQ..F....e.
00E0: 55 DA 3D B3 14 47 0D 3B   93 90 9F E6 5C D3 8D E0  U.=..G.;....\...
00F0: 44 F0 E6 F1 62 8F 70 D7   8A 30 26 15 27 7F D3 32  D...b.p..0&.'..2
0100: 60 70 E4 4D F1 75 49 55   BC 49 89 37 67 CB 7F 16  `p.M.uIU.I.7g...
0110: 36 92 E0 F0 8E C0 1C 8D   67 43 45 F7 BA F9 5F F7  6.......gCE..._.
0120: 3B 87 8C B8 0D D4 FB 96   F9 40 46 0F 21 00 18 42  ;........@F.!..B
0130: AB 5F 36 2E 6A 02 05 46   58 05 92 1B D9 E4 20 2B  ._6.j..FX..... +
0140: 9C B1 22 80 AE A1 C6 14   6F 82 DD 06 A1 7C 0C DE  .."".....o.......
0150: AA ED 6B 9E 88 C7 A3 74   DC F7 DB 9E 17 75 A5 84  ..k....t.....u..
0160: EB A2 A2 57 23 A8 9C 27   C8 37 3C A7 AB F1 A9 5E  ...W#..'.7<....^
0170: 20 DC CB 82 6F E7 94 8A   7F E1 8F F5 4E F1 0E C7   ...o.......N...
0180: 66 C2 AE FE C3 3B 4E E5   CC 99 13 5D C4 F3 14 99  f....;N....]....
0190: 67 BD F7 8E 7C 9B B2 F4   00 90 47 F8 E2 80 77 1D  g.........G...w.
01A0: CE 59 02 3D 25 7B 94 9D   76 99 1E 40 3C 53 19 01  .Y.=%...v..@<S..
01B0: 46 9E A4 BF BF 8C 3A 51   8B 45 B7 1F 43 BD 4C 98  F.....:Q.E..C.L.
01C0: 96 C2 11 19 6B 93 02 CB   ED 7E 44 94 67 34 F6 24  ....k.....D.g4.$
01D0: 20 A7 85 59 DF 14 3E E6   8B 00 D7 8F 92 3A 3C E3   ..Y..>......:<.
01E0: AE E4 32 42 38 5B 11 C9   82 33 B3 D6 87 57 57 06  ..2B8[...3...WW.
01F0: 61 32 70 A4 3E 97 DD 7F   48 51 B8 57 12 31 0B 24  a2p.>...HQ.W.1.$

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIHQDCCBSigAwIBAgIIJ4m662xZS1owDQYJKoZIhvcNAQELBQAwNjEWMBQGA1UE
AwwNQ0FFRElDT00gUm9vdDEPMA0GA1UECgwGRURJQ09NMQswCQYDVQQGEwJFUzAe
Fw0xNDA3MjIxMTAwNDNaFw0yNDA1MjIxMDIwMDBaMIGBMRMwEQYDVQQDDApDQUVE
SUNPTTAxMRIwEAYDVQQFEwlCOTY0OTA4NjcxDzANBgNVBAoMBkVESUNPTTE4MDYG
A1UEBwwvQ2FsbGUgQ2hhcmxlcyBSb2JlcnQgRGFyd2luIDggLSA0Njk4MCAtIFBh
dGVybmExCzAJBgNVBAYTAkVTMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKC
```

AgEAixuyfCbKiXqKaCIv1C5O+xy3/RkC8tJ6Ef/l8cr5Hk6N53eYGGrHcG/B6L43
jgbc8/CVp6py7VldalAaIm56dL9WqHqq6Bvg2DFssYYKcmzRT2gIHYE74/x92m1d
n6jo4o8MXi8mvfhywX4L7QllnwqtH1mAMPSB8X8bE9+6azf8zGTKiU8vh836uWY2
3p3VIwpoFsMFxSTtqU4SnUk7aXrRt9wRfmVZQFl3/Rc47VHnUPtAgqGZ1zflBGc0
35Qh9sk7yQXPm9Tf1+xOrsK251vgfinlUpnDomFPaWfy9t7cnuCbnbZXiE3beKXW
I9hy+J0dqHVI9mTjFt89vmAYRZcvSHF7RmsTkRnbuSA8MpE++aU5jc6PUR8IHbhJ
aWKJWSsZv2p9S38FP7Clk54dO+FixlOHiQZq5PG7z6oEFZl+YFE3IcwvXrsUlLYw
ohyjEwqyw2rEhTW39YklQSX2NO2ciHL0M50oJAN/JH/zHusUbtzPmGEhIdccevIc
U6N8WxBKR+9rF8UbLv98EOWry+qgXr7VLTnzhQEbJB2xfoWcVqnlJDSQ62E8Ydu+
VesB42eLywQtceR+JKtj2swDGQsOP6sVt5nsqI98CkacjUalwroT77CJqCWIjSj4
RWk2A1SfmgiTDk8l3b8dl+Y5zczz/ba5KNtq8oaK0mFGj3kCAwEAAaOCAgQwggIA
MIGTBggrBgEFBQcBAQSBhjCBgzBCBggrBgEFBQcwAoY2aHR0cDovL2FjZWRpY29t
LmVkaWNvbWdyb3VwLmNvbS9jZXJ0cy9jYWVkaWNvbXJvb3QuY2VyMD0GCCsGAQUF
BzABhjFodHRwOi8vb2NzcC5hY2VkaWNvbS5lZGljb21ncm91cC5jb20vY2FlZGlj
b21yb290MB0GA1UdDgQWBBRtaoj4Lup/L83A9HZ3k+ZFMu+LBTASBgNVHRMBAf8E
CDAGAQH/AgEAMB8GA1UdIwQYMBaAFBTNKll4Y6thGei4PaHgWsB15/nLMIGbBgNV
HSAEgZMwgZAwgY0GDCsGAQQBgepjAgMBATB9ME4GCCsGAQUFBwICMEIeQABDAGUA
cgB0AGkAZgBpAGMAYQB0AGkAbwBuACAAUAByAGEAYwB0AGkAYwBlACAAUwB0AGEA
dABlAG0AZQBuAHQwKwYIKwYBBQUHAgEWH2h0dHA6Ly9hY2VkaWNvbS5lZGljb21n
cm91cC5jb20wQQYDVR0fBDowODA2oDSgMoYwaHR0cDovL2FjZWRpY29tLmVkaWNv
bWdyb3VwLmNvbS9jYWVkaWNvbXJvb3QuY3JsMA4GA1UdDwEB/wQEAwIBhjAjBgNV
HREEHDAagRhhY2VkaWNvbUBlZGljb21ncm91cC5jb20wDQYJKoZIhvcNAQELBQAD
ggIBAD+qPUsRtjlNf0mP14v2GX9bAhGdDV0acG7AhU5WFIxa3Jo31LWWdXjkJ6/e
9dTtJnQvzGCIgVrxkpWqFegVBbqJTnPjcCma+YmiLZlTcWao52q84+EggP4cvPVF
4OEWeh2q8M0XAQqsTz++DYyLwUmL+SeC3MaRhQvrOvCxdlL6L8omucnyscfVfQ5C
OBwGgFCm8KlKPGeG1Uwsb7s3NqF5Q37hWdN2Ney2q8XRtkmyv/quGQjH7yAw552a
oHgLc/KyYrEBpqBPtar64B/vyXi/eCdgqlhRvgpGy9EuD2UdVdo9sxRHDTuTkJ/m
XNON4ETw5vFij3DXijAmFSd/0zJgcORN8XVJVbxJiTdny38WNpLg8I7AHI1nQ0X3
uvlf9zuHjLgN1PuW+UBGDyEAGEKrXzYuagIFRlgFkhvZ5CArnLEigK6hxhRvgt0G
oXwM3qrta56Ix6N03Pfbnhd1pYTroqJXI6icJ8g3PKer8aleINzLgm/nlIp/4Y/1
TvEOx2bCrv7DO07lzJkTXcTzFJlnvfeOfJuy9ACQR/jigHcdzlkCPSV7lJ12mR5A
PFMZAUaepL+/jDpRi0W3H0O9TJiWwhEZa5MCy+1+RJRnNPYkIKeFWd8UPuaLANeP
kjo8467kMkI4WxHJgjOz1odXVwZhMnCkPpfdf0hRuFcSMQsk
-----END CERTIFICATE-----

C=ES, O=EDICOM, CN=CAEDICOM Root

Type	CA/QC
Status	undersupervision
Status starting time	2015-04-01T15:44:52.000Z

Service digital identity (X509)

Version	3
Serial number	6412029366930714179
Signature algorithm	SHA256withRSA
Issuer	C=ES, O=EDICOM, CN=CAEDICOM Root
Valid from	Mon May 19 07:08:20 PET 2014
Valid to	Fri May 19 06:22:00 PET 2034
Subject	C=ES, O=EDICOM, CN=CAEDICOM Root
Public key	Sun RSA public key, 4096 bits modulus: 89549450400115540560970202287952704516491243874493294738279582900604072 42515845312155373223736471147034862051786172475918613659751402556933395 82645752642058010180821862982971290216131179870084210000486188212550897 13808920375894294133082740063153237222900563678207129383207655698053029 21271536887318869979619942872243522713411666587306009714680046765302273 55386302027521790543889759312651222374115828267523307825409872128113486 78143299864291692504610513748161762302684572933202543680612811378288732 89941525086068754828825114462737346927631431614201326591581955329042168 15843679544391305831575648385248691373618253646955718566049720129724882 47327407827047221472233721838606944438004624815416072704203653341168999 72844994700851347359748941878345276262228522694143919394165432251630627 02928787967454588425466652790682946539520344846402953024104799389670982 14951614219181419820902977617011939709596294775467170793869134967674269 40147716745519033717744736525356004907395855809731001165063613408132585 41129894520430137200505994855946734104117608732109237174470625484217119 33231244189714158643370058724238642629311557994713609984863044774499154 61063832669514206474394636080826032512898129520050668180056206471892181 20798676352677555510749107 public exponent: 65537
Subject key identifier	14cd2a597863ab6119e8b83da1e05ac075e7f9cb
Authority key identifier	04183016801414cd2a597863ab6119e8b83da1e05ac075e7f9cb

Key usage	digitalSignature keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	0293c20278eaf87010d7e37c1759e24bf501f220
SHA256 Thumbprint	b9b7c9e893b91ca3b49cb195a530f0bbc791425e123b3b8162eacdf8626f8a8d

The decoded certificate:

```
[
[
 Version: V3
 Subject: C=ES, O=EDICOM, CN=CAEDICOM Root
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
895494504001155405609702022879527045164912438744932947382795829006040724251584531215537322373647114703486205178617247591861365975140255693339582645752642058010180821862982971290216131179870084210000486188212550897138089203758942941330827400631532372229005636782071293832076556980530292127153688731886997961994287224352271341166658730600971468004676530227355386302027521790543889759312651222374115828267523307825409872128113486781432998642916925046105137481617623026845729332025436806128113782887328994152508606875482882511446273734692763143161420132659158195532904216815843679544391305831575648385248691373618253646955718566049720129724882473274078270472214722337218386069444380046248154160727042036533411689997284499470085134735974894187834527626222852269414391939416543225163062702928787967454588425466652790682946539520344846402953024104799389670982149516142191814198209029776170119397095962947754671707938691349676742694014771674551903371774473652535600490739585580973100116506361340813258541129894520430137200505994855946734104117608732109237174470625484217119332321244189714158643370058724238642629311557994713609984863044774499154610638326695142064743946360808260325128981295200506681800562064718921812079867635267755551074910 7
 public exponent: 65537
 Validity: [From: Mon May 19 07:08:20 PET 2014,
             To: Fri May 19 06:22:00 PET 2034]
 Issuer: C=ES, O=EDICOM, CN=CAEDICOM Root
 SerialNumber: [    58fc1abc a1472e43]

Certificate Extensions: 4
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 14 CD 2A 59 78 63 AB 61   19 E8 B8 3D A1 E0 5A C0  ..*Yxc.a...=..Z.
0010: 75 E7 F9 CB                                        u...
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 14 CD 2A 59 78 63 AB 61   19 E8 B8 3D A1 E0 5A C0  ..*Yxc.a...=..Z.
0010: 75 E7 F9 CB                                        u...
]

]

[3]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 DigitalSignature
 Key_CertSign
 Crl_Sign
]

[4]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 49 51 6E 60 B9 6E A5 F9   E1 48 23 83 D1 0F 19 14  IQn`.n...H#.....
0010: F2 03 C9 F7 76 7F 72 21   F0 97 49 CD 77 BF F7 FD  ....v.r!..I.w...
0020: A2 9D 79 DE 2F 71 94 25   2E C8 05 82 C1 D6 D5 1F  ..y./q.%........
0030: C0 FA 24 0D F7 BF DA C6   9C 7C 77 AF 68 62 4E C2  ..$.......w.hbN.
0040: 35 7C 32 B6 55 51 1A 10   15 FC 94 6F 16 C7 3C 02  5.2.UQ.....o..<.
0050: 28 5F 54 72 25 73 43 FC   08 D1 0B E4 00 3C EC 16  (_Tr%sC......<..
0060: B0 97 E0 4A 03 AB 86 87   54 39 D3 47 17 FA 39 C6  ...J....T9.G..9.
0070: 00 FA 2E 42 7D 74 A8 72   3B C5 8A 70 34 82 DB 9D  ...B.t.r;..p4...
0080: 8C B0 9B 8E 74 CA B0 96   F5 C4 B7 3F F1 54 9A 20  ....t......?.T.
0090: D1 B1 99 D3 DC B5 F6 E6   48 94 D5 22 F3 22 99 41  ........H..".".A
00A0: 3B C1 71 C6 D4 28 78 69   99 69 28 E1 3F 1F 78 95  ;.q..(xi.i(.?.x.
00B0: 39 F0 43 2B CA 39 48 FF   55 CB 62 82 0E 09 6A 37  9.C+.9H.U.b...j7
00C0: 56 AB DB E6 BB DD E7 4A   94 CC 67 74 8A 07 4D 00  V......J..gt..M.
00D0: B8 84 46 9C 1E 2F 2B 88   56 EA 93 F9 78 F8 A1 28  ..F../+.V...x..(
00E0: 0D 36 70 F6 B4 D3 43 05   33 E4 15 2E 95 A5 AA BB  .6p...C.3.......
00F0: CF 7C 73 E3 2C 6B 08 D6   F9 65 48 2E D7 D5 BC 0E  ..s.,k...eH.....
0100: 29 63 C2 81 EE C2 CF 98   75 F9 35 67 39 09 87 3A  )c......u.5g9..:
0110: 82 EF E1 23 0E 37 55 8C   2F B5 1E D6 F9 8E FD 55  ...#.7U./......U
0120: C8 05 EF 2F AD A2 25 74   6A 88 4A CA 94 FE D6 83  .../..%tj.J.....
0130: 41 A8 FA 3B 4D EC 29 2B   F9 3C C9 2B D0 06 15 C1  A..;M.)+.<.+....
0140: 64 E5 32 A9 9D 8A E3 3F   41 7B DC 62 18 9D B3 B8  d.2....?A..b....
0150: 3E 5B 80 CA 54 4B 6D AB   CB 94 23 D5 10 97 7A B0  >[..TKm...#...z.
0160: 59 CF 54 1B 2B 5F A4 D0   0D 51 33 6F E3 F5 97 00  Y.T.+_...Q3o....
0170: C0 BE 7F 7E 11 E5 F7 10   5C B4 6C 87 0D C8 BA B9  ........\.l.....
```

```
0180: AA 1F 15 0C B9 17 AE FD   48 C6 DC 26 A0 77 E7 3C  ........H..&.w.<
0190: 62 62 3F 32 4D 58 4F AA   72 F5 2F 53 ED 7B C5 44  bb?2MXO.r./S...D
01A0: F4 C5 66 EB 8C 64 D5 94   87 63 45 ED 1A 43 9A 3B  ..f..d...cE..C.;
01B0: EB 3D 2F 87 CC 6C 0B 84   CA 3F 4E D6 11 0D 3F 30  .=/..l...?N...?0
01C0: 37 AB 31 61 0E 80 67 C8   B2 BA F6 28 73 D5 FE 56  7.1a..g....(s..V
01D0: D8 AB EB DF 39 37 B5 D2   46 0E 3B 4C 48 ED 5F 1F  ....97..F.;LH._.
01E0: 14 F5 2B 91 EC DB E1 9E   2E 6A D3 B5 BF E4 1D 46  ..+......j.....F
01F0: 12 6B 2A ED AE AD 6A 7A   CC 95 97 BA 57 D8 A6 AE  .k*...jz....W...

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIFUTCCAzmgAwIBAgIIWPwavKFHLkMwDQYJKoZIhvcNAQELBQAwNjEWMBQGA1UE
AwwNQ0FFRElDT00gUm9vdDEPMA0GA1UECgwGRURJQ09NMQswCQYDVQQGEwJFUzAe
Fw0xNDA1MTkxMjA4MjBaFw0zNDA1MTkxMTIyMDBaMDYxFjAUBgNVBAMMDUNBRURJ
Q09NIFJvb3QxDzANBgNVBAoMBkVESUNPTTELMAkGA1UEBhMCRVMwggIiMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQDbgMroSXTH0zgu8cUjYvw2jC8efjkL6Qb0
VZulmCmU7YZHMoPzxZJ6BdcpAj4Wwyh/NWQpenm7oeIeYRSN5wDQ3KJUZYrfablx
R384OBZGp2kxETVM4Sp//21PlT3jXUhNGVMIWmsh1RIwaZeQry3B9X9BX0k2j024
HhqVX9oPb1wVNcQRvF+Fm72tO1Veu9/Ou69cmWDdH2kaSUgh+QkKz3Kn8PLe5XgZ
vhLdzYd5Qc4vRdcLkRARBB4SnfI4A18Waa6gCtrA+eugDRgPeV6RneQfFJw0ExkC
RLpRw+55smAUo6+8SC0oOGgBQ2TKDoaDYtCKGaYn8St7SykhW5rMaEIQyEtPDyOy
iHzEXG4XcMV3r5XAJaQiCtN8+dhyyNAtvafo0i2LTKFuCvy0QDO7mmv8pOrJ/uA0
iEPMxrw/ddKlqa/6l7k+t85UoE3AXS7BKNhjVHK4rFr1OvsgYQY69KArOKvMgwxJ
1G4+bQ8+cy825vNPs8AA0UVJW4z2o5gdhH+ZCsPqCjzD0yR4SGf1GzsOHQ5DsQR1
waA5dov22QKlHeGeWwe7NldKIU35iWm0bA/Xr6AVJJnn+NdTlOwSv6Sl1+3ujjV3
d9ymfyBUktZjlnKeTSq2j3PzGaHEsB/mNKMLAD6XSSdhqqoEQTM4tVBRzDYV2x//
vcpIg0inswIDAQABo2MwYTAdBgNVHQ4EFgQUFM0qWXhjq2EZ6Lg9oeBawHXn+csw
DwYDVR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBQUzSpZeGOrYRnouD2h4FrAdef5
yzAOBgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggIBAElRbmC5bqX54Ugj
g9EPGRTyA8n3dn9yIfCXSc13v/f9op153i9xlCUuyAWCwdbVH8D6JA33v9rGnHx3
r2hiTsI1fDK2VVEaEBX8lG8WxzwCKF9UciVzQ/wI0QvkADzsFrCX4EoDq4aHVDnT
Rxf6OcYA+i5CfXSocjvFinA0gtudjLCbjnTKsJb1xLc/8VSaINGxmdPctfbmSJTV
IvMimUE7wXHG1Ch4aZlpKOE/H3iVOfBDK8o5SP9Vy2KCDglqN1ar2+a73edKlMxn
dIoHTQC4hEacHi8riFbqk/l4+KEoDTZw9rTTQwUz5BUulaWqu898c+MsawjW+WVI
LtfVvA4pY8KB7sLPmHX5NWc5CYc6gu/hIw43VYwvtR7W+Y79VcgF7y+toiV0aohK
ypT+1oNBqPo7TewpK/k8ySvQBhXBZOUyqZ2K4z9Be9xiGJ2zuD5bgMpUS22ry5Qj
1RCXerBZz1QbK1+k0A1RM2/j9ZcAwL5/fhHl9xBctGyHDci6uaofFQy5F679SMbc
JqB35zxiYj8yTVhPqnL1L1Pte8VE9MVm64xk1ZSHY0XtGkOaO+s9L4fMbAuEyj9O
1hENPzA3qzFhDoBnyLK69ihz1f5W2Kvr3zk3tdJGDjtMSO1fHxT1K5Hs2+GeLmrT
tb/kHUYSayrtrq1qesyVl7pX2Kau
-----END CERTIFICATE-----
```

Certificate Service Provider Name (en): FIRMA PROFESIONAL S.A.

Trade name (en)	FIRMA PROFESIONAL S.A.
Information URI (en)	HTTP://WWW.FIRMAPROFESIONAL.COM
Service provider street address (es)	PASEO BONANOVA 47
Service provider street address (en)	PASEO BONANOVA 47
Service provider postal code (es)	BARCELONA 08017
Service provider postal code (en)	BARCELONA 08017
Service provider locality (es)	PASEO BONANOVA 47
Service provider locality (en)	PASEO BONANOVA 47
Service provider state (es)	BARCELONA
Service provider state (en)	BARCELONA
Service provider country (es)	ES
Service provider country (en)	ES

CN=AC Firmaprofesional - CUALIFICADOS, SERIALNUMBER=A62634068, OU=Certificados Cualificados, O=Firmaprofesional S.A., C=ES

Type	CA/QC
Status	undersupervision
Status starting time	2015-11-26T21:42:27.000Z

Service digital identity (X509)

Version	3
Serial number	937705595546249684
Signature algorithm	SHA256withRSA
Issuer	CN=Autoridad de Certificacion Firmaprofesional CIF A62634068, C=ES
Valid from	Thu Sep 18 05:00:54 PET 2014
Valid to	Mon Dec 30 23:02:55 PET 2030
Subject	CN=AC Firmaprofesional - CUALIFICADOS, SERIALNUMBER=A62634068, OU=Certificados Cualificados, O=Firmaprofesional S.A., C=ES
Public key	Sun RSA public key, 2048 bits modulus: 23535818509823618888152413102470237449998648353116926521981512524876912 34705778186813805391418977715864772242720358902404967061179901950050542 08350595712997028680194169300864961249173424863299940848046792995283151 15196168576242861787723948908337368748466385208674982179941072314695686 12373180653597168756143683955794759354362231520259463560780129902368912 46465546466140981670836180452983972915828108197068789576159544763755554 99733892834322901516577131588169593957711909991705304966435872307664480 19622402871629406612727153234791797323753819169179439501989910332306796 89532406211030404832189145748592323665664325129 97 public exponent: 65537
Subject key identifier	8c71cc93076fd1d586687d823a41d94c02f8965d
CRL distribution points	http://crl.firmaprofesional.com/fproot.crl
Authority key identifier	04183016801465cdebab351e003e7ed574c01cb473470e1a642f
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=0
SHA1 Thumbprint	3486ed23622155459e9b25ff3f21ad7627987387
SHA256 Thumbprint	2b75cc4f36759cfc4c6637b1e0e54359457db57e74de4d2dc5d02cddff2960cf

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=AC Firmaprofesional - CUALIFICADOS, SERIALNUMBER=A62634068, OU=Certificados Cualificados, O=Firmaprofesional S.A., C=ES
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
23535818509823618888152413102470237449998648353116926521981512524876912347057781868138053914189777158647722427203589024049670611799019500505420835059571299702868019416930086496124917342486329994084804679299528315115196168576242861787723948908337368748466385208674982179941072314695686123731806535971687561436839557947593543622315202594635607801299023689124646554646614098167083618045298397291582810819706878957615954476375555499733892834322901516577131588169593957711909991705304966435872307664480196224028716294066127271532347917973237538191691794395019899103323067968953240621103040483218914574859232366566432512997
 public exponent: 65537
 Validity: [From: Thu Sep 18 05:00:54 PET 2014,
             To: Mon Dec 30 23:02:55 PET 2030]
 Issuer: CN=Autoridad de Certificacion Firmaprofesional CIF A62634068, C=ES
 SerialNumber: [    0d036645 5e6e29d4]

Certificate Extensions: 7
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 8C 71 CC 93 07 6F D1 D5   86 68 7D 82 3A 41 D9 4C  .q...o...h..:A.L
0010: 02 F8 96 5D                                        ...]
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 65 CD EB AB 35 1E 00 3E   7E D5 74 C0 1C B4 73 47  e...5..>..t...sG
0010: 0E 1A 64 2F                                        ..d/
]

]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.firmaprofesional.com/fproot.crl]
]]

[4]: ObjectId: 2.5.29.15 Criticality=true
```

```
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[5]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 81 E5 1E 81 E2 00 43   00 65 00 72 00 74 00 69  0......C.e.r.t.i
0010: 00 66 00 69 00 63 00 61   00 64 00 6F 00 20 00 64  .f.i.c.a.d.o. .d
0020: 00 65 00 20 00 41 00 75   00 74 00 6F 00 72 00 69  .e. .A.u.t.o.r.i
0030: 00 64 00 61 00 64 00 20   00 64 00 65 00 20 00 43  .d.a.d. .d.e. .C
0040: 00 65 00 72 00 74 00 69   00 66 00 69 00 63 00 61  .e.r.t.i.f.i.c.a
0050: 00 63 00 69 00 F3 00 6E   00 2E 00 20 00 43 00 6F  .c.i...n... .C.o
0060: 00 6E 00 73 00 75 00 6C   00 74 00 65 00 20 00 6C  .n.s.u.l.t.e. .l
0070: 00 61 00 73 00 20 00 63   00 6F 00 6E 00 64 00 69  .a.s. .c.o.n.d.i
0080: 00 63 00 69 00 6F 00 6E   00 65 00 73 00 20 00 64  .c.i.o.n.e.s. .d
0090: 00 65 00 20 00 75 00 73   00 6F 00 20 00 65 00 6E  .e. .u.s.o. .e.n
00A0: 00 20 00 68 00 74 00 74   00 70 00 3A 00 2F 00 2F  . .h.t.t.p.:././
00B0: 00 77 00 77 00 77 00 2E   00 66 00 69 00 72 00 6D  .w.w.w...f.i.r.m
00C0: 00 61 00 70 00 72 00 6F   00 66 00 65 00 73 00 69  .a.p.r.o.f.e.s.i
00D0: 00 6F 00 6E 00 61 00 6C   00 2E 00 63 00 6F 00 6D  .o.n.a.l...c.o.m
00E0: 00 2F 00 63 00 70 00 73                            ./.c.p.s

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 23 68 74 74 70 3A 2F   2F 77 77 77 2E 66 69 72  .#http://www.fir
0010: 6D 61 70 72 6F 66 65 73   69 6F 6E 61 6C 2E 63 6F  maprofesional.co
0020: 6D 2F 63 70 73                                     m/cps

]]  ]
]

[6]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:0
]

[7]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://crl.firmaprofesional.com/caroot.crt,
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://ocsp.firmaprofesional.com]
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 0A 52 EB CD FA CA E7 DC   9C E5 F1 36 6C 71 6B CD  .R.........6lqk.
0010: 16 3B 78 8D 4C EF F1 88   5D 6C 40 7D C6 7D 48 4D  .;x.L...]l@...HM
0020: 28 AF 71 ED 00 25 D8 C2   D3 33 41 6F 67 C6 59 DB  (.q..%...3Aog.Y.
0030: 74 65 2E 40 A7 4A B6 02   54 8E 40 24 20 6F 02 81  te.@.J..T.@$ o..
0040: 37 7F 1A 9D 57 B4 34 6B   8E 43 1F BF C3 37 2C D3  7...W.4k.C...7,.
0050: BC E1 27 C9 41 87 B1 D5   82 CC 24 8C FD 74 1D 8B  ..'.A.....$..t..
0060: 5F 9F AA E2 E7 CB E0 ED   EE AF 58 92 AC C7 35 CC  _.........X...5.
0070: CE 54 81 A0 F4 33 8F BD   71 D7 51 6B 12 73 ED 3A  .T...3..q.Qk.s.:
0080: 23 78 4C ED 83 43 B0 90   F8 86 5B E8 EB C3 44 60  #xL..C....[...D`
0090: F5 65 A3 8F AE 37 89 3E   DD E7 5F 10 0F 72 44 21  .e...7.>.._..rD!
00A0: A8 0E 13 65 CE 1D 45 2D   00 47 67 75 A2 B3 D3 95  ...e..E-.Ggu....
00B0: 1F EF 71 97 AA 18 85 81   8D CC 44 86 60 E2 1E C2  ..q.......D.`...
00C0: 9C 4B 7E 56 C5 E8 B7 72   00 28 A9 9B CC B0 01 98  .K.V...r.(......
00D0: 3E 35 18 1D 0D 4E 2D CB   FF 9D 74 FF A8 06 E8 91  >5...N-...t.....
00E0: 9E EC CB 65 92 3D CD FC   A5 0B 40 D0 60 49 5C 0B  ...e.=....@.`I\.
00F0: AF 4B 29 0E 63 73 7D A8   00 DF E4 D2 6E 55 DF 95  .K).cs......nU..
0100: 4A A9 D1 1C D8 95 0B 9F   4C E5 4C 3C E7 A7 56 A7  J.......L.L<..V.
0110: AF FB A5 4E EE AC 38 B0   A1 6F B2 CE 84 66 63 23  ...N..8..o...fc#
0120: 50 5A C2 43 00 99 94 7E   D9 DA F5 85 D5 51 34 9F  PZ.C.........Q4.
0130: E1 9C 18 65 9A CA 5B FE   8E F0 23 DA F3 A0 16 25  ...e..[...#....%
0140: 32 9A 86 23 11 C1 CE 95   55 26 18 4E E6 0D 58 5E  2..#....U&.N..X^
0150: AA B7 5F 5D A8 48 BD BB   C5 8E 8B 4B 5F FC 7E AC  .._].H.....K_...
0160: 1F 60 BA 2F 54 EC DE 7A   0A F6 4A 00 4D 0E 4E CC  .`./T..z..J.M.N.
0170: A0 88 D3 24 9C 68 08 D1   B7 F5 DF A1 B6 34 C7 55  ...$.h.......4.U
0180: E7 84 CE 9D F3 F8 E7 3C   1E 55 34 19 FF 7C F8 E9  .......<.U4.....
0190: DF 8C EF 53 CC 60 33 D4   F8 A3 A9 76 BB EE 6D C8  ...S.`3....v..m.
01A0: BB DF 36 82 C6 89 1F CA   8A E4 3C B1 18 5C 8C 37  ..6.......<..\.7
01B0: 90 9A 36 AD B7 A7 FE 60   FC 04 F3 16 B4 CE 7F EF  ..6....`........
01C0: A3 A7 CE 7E 30 16 90 78   34 FF CC 2D 2B AB 8E 1E  ....0..x4..-+...
01D0: C1 57 36 4D CC 42 37 A1   9B 89 E7 A9 30 39 3A EE  .W6M.B7.....09:.
01E0: 74 B5 1D 22 82 64 91 3F   7B 6F 61 2A E1 89 A7 79  t.."d.?.oa*...y
01F0: 1D D4 F3 B5 58 79 42 DB   D5 CE 68 A4 63 9B 20 C2  ....XyB...h.c. .

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGyDCCBLCgAwIBAgIIDQNmRV5uKdQwDQYJKoZIhvcNAQELBQAwUTELMAkGA1UE
BhMCRVMxQjBABgNVBAMTOUF1dG9yaWRhZCBkZSBDZXJ0aWZpY2FjaW9uIEZpcm1h
cHJvZmVzaW9uYWwgQ0lGIEE2MjYzNDA2ODAeFw0xNDA5MTgxMDAwNTRaFw0zMDEy
MzEwNDAyNTVaMIGSMQswCQYDVQQGEwJFUzEeMBwGA1UEChMVRmlybWFwcm9mZXNp
```

b25hbCBTLkEuMSIwIAYDVQQLExlDZXJ0aWZpY2Fkb3MgQ3VhbGlmaWNhZG9zMRIw
EAYDVQQFEwlBNjI2MzQwNjgxKzApBgNVBAMTIkFDIEZpcm1hcHJvZmVzaW9uYWwg
LSBDVUFMSUZJQ0FET1MwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC6
cIlUCaCe12gMnFsVFePe9Z52zvebP/J30UrhNH0H4vny6VS7oVOd+aMQvvqW9JmT
rYIA1i72jp8TnWNHq0RNlQMzjd+uQkeVSIOrohSHMejah0yx+yUusoWDSXOdhKV+
CCjN+nvcCDUxJW+jmiN/UVZkHzQRK3M0cbQRGRNADeKPsrUrB0028OhBgyPOxM6S
x3BIxXz8r2mXXtlFkkgtVYOtU8zyT4OM+c6mPEmnWL+uHpuL4MlzvZ/1RrO+ynyu
a54hGkh4iijt1a3PecgdY7269FfhlsIWMSnXvKOeY6u6+F+CkkxwqiRO4xvCEVXY
1ObIHPgXON3VYWIzLxvlAgMBAAGjggJgMIICXDB0BggrBgEFBQcBAQRoMGYwNgYI
KwYBBQUHMAKGKmh0dHA6Ly9jcmwuZmlybWFwcm9mZXNpb25hbC5jb20vY2Fyb290
LmNydDAsBggrBgEFBQcwAYYgaHR0cDovL29jc3AuZmlybWFwcm9mZXNpb25hbC5j
b20wHQYDVR0OBBYEFIxxzJMHb9HVhmh9gjpB2UwC+JZdMBIGA1UdEwEB/wQIMAYB
Af8CAQAwHwYDVR0jBBgwFoAUZc3rqzUeAD5+1XTAHLRzRw4aZC8wggFBBgNVHSAE
ggE4MIIBNDCCATAGBFUdIAAwggEmMIHyBggrBgEFBQcCAjCB5R6B4gBDAGUAcgB0
AGkAZgBpAGMAYQBkAG8AIABkAGUAIABBAHUAdABvAHIAaQBkAGEAZAAgAGQAZQAg
AEMAZQByAHQAaQBmAGkAYwBhAGMAaQDzAG4ALgAgAEMAbwBuAHMAdQBsAHQAZQAg
AGwAYQBzACAAYwBvAG4AZABpAGMAaQBvAG4AZQBzACAAZABlACAAdQBzAG8AIABl
AG4AIABoAHQAdABwADoALwAvAHcAdwB3AC4AZgBpAHIAbQBhAHAAcgBvAGYAZQBz
AGkAbwBuAGEAbAAuAGMAbwBtAC8AYwBwAHMwLwYIKwYBBQUHAgEWI2h0dHA6Ly93
d3cuZmlybWFwcm9mZXNpb25hbC5jb20vY3BzMDsGA1UdHwQ0MDIwMKAuoCyGKmh0
dHA6Ly9jcmwuZmlybWFwcm9mZXNpb25hbC5jb20vZnByb290LmNybDAOBgNVHQ8B
Af8EBAMCAQYwDQYJKoZIhvcNAQELBQADggIBAApS6836yufcnOXxNmxxa80WO3iN
TO/xiF1sQH3GfUhNKK9x7QAl2MLTM0FvZ8ZZ23RllkCnSrYCVI5AJCBvAoE3fxqd
V7Q0a45DH7/DNyzTvOEnyUGHsdWCzCSM/XQdi1+fquLny+Dt7q9YkqzHNczOVIGg
9DOPvXHXUWsSc+06I3hM7YNDsJD4hlvo68NEYPVlo4+uN4k+3edfEA9yRCGoDhNl
zh1FLQBHZ3Wis9OVH+9xl6oYhYGNzESGYOIewpxLflbF6LdyACipm8ywAZg+NRgd
DU4ty/+ddP+oBuiRnuzLZZI9zfylC0DQYElcC69LKQ5jc32oAN/k0m5V35VKqdEc
2JULn0zlTDznp1anr/ulTu6sOLChb7LOhGZjI1BawkMAmZR+2dr1hdVRNJ/hnBhl
mspb/o7wI9rzoBYlMpqGIxHBzpVVJhhO5g1YXqq3X12oSL27xY6LS1/8fqwfYLov
VOzeegr2SgBNDk7MoIjTJJxoCNG39d+htjTHVeeEzp3z+Oc8HlU0Gf98+OnfjO9T
zGAz1PijqXa77m3Iu982gsaJH8qK5DyxGFyMN5CaNq23p/5g/ATzFrTOf++jp85+
MBaQeDT/zC0rq44ewVc2TcxCN6GbieepMDk67nS1HSKCZJE/e29hKuGJp3kd1PO1
WHlC29XOaKRjmyDC
-----END CERTIFICATE-----

Certificate Service Provider Name (en): CERTISIGN

Trade name (en)	CERTISIGN
Information URI (en)	HTTPS://WWW.CERTISIGN.COM.BR/
Service provider street address (es)	RUA BELA CINTRA 904 16. ANDAR SÃO PAULO
Service provider street address (en)	RUA BELA CINTRA 904 16. ANDAR SÃO PAULO
Service provider postal code (es)	01415-000
Service provider postal code (en)	01415-000
Service provider locality (es)	SAO PAULO
Service provider locality (en)	SAO PAULO
Service provider state (es)	SP
Service provider state (en)	SP
Service provider country (es)	BR
Service provider country (en)	BR

CN=AC Certisign Parceria, O=Certisign Certificadora Digital S.A., C=BR

Type	CA/QC
Status	undersupervision
Status starting time	2016-01-22T20:51:59.000Z

Service digital identity (X509)

Version	3
Serial number	219998364771459427093914652840603246 80
Signature algorithm	SHA1withRSA
Issuer	CN=AC Certisign Parceria, O=Certisign Certificadora Digital S.A., C=BR
Valid from	Thu Aug 18 19:00:00 PET 2011

Valid to	Wed Aug 18 18:59:59 PET 2021
Subject	CN=AC Certisign Parceria, O=Certisign Certificadora Digital S.A., C=BR
Public key	Sun RSA public key, 2048 bits modulus: 25680538283525265187038795187562153405958393862848369453954941920316686 92436938206011933129460467819888918092971440029465094832010749582858267 74552350136130482118577293092420477168742419732995918665755868027706433 20765096475507704077237106448552595838300006493215725388449932197861928 57662688804493669338261842043516314011101027486084834483204490928679 78 53298969527055553330202398286589695489642858577694803416337698521274058 47281216174248082539208956559946309055859152012169401579755172994056663 67033770108581155110153750951972985948202976879283731693914356206985814 92125626502174642569420621245000106920755415598 21 public exponent: 65537
Subject key identifier	3330906272985873765 66d3e5ba25408bfd2c797
CRL distribution points	http://onsitecrl.certisign.com.br/repositorio/lcr/ACCertisignParceria/LatestCRL.crl
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=0
SHA1 Thumbprint	5f92058c6e3699401a492988b24c7fc978fff8a7
SHA256 Thumbprint	4eeba686fce5308b9c1c9d14edb9c0592a6d31ef16fb0a65a19a2d0b8a6fc12b

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=AC Certisign Parceria, O=Certisign Certificadora Digital S.A., C=BR
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 2048 bits
 modulus:
25680538283525265187038795187562153405958393862848369453954941920316686924369382060119331294604678198889180929714400294650948320107495828582677455235013613048211857729309242047716874241973299591866575586802770643320765096475507704077237106448552595838300006493215725388449932197861928576626888044936693382618420435163140111010274860848344832044909286797853298969527055553330202398286589695489642858577694803416337698521274058472812161742480825392089565599463090558591520121694015797551729940566367033770108581155110153750951972985948202976879283731693914356206985814921256265021746425694206212450001069207554155982 1
 public exponent: 65537
 Validity: [From: Thu Aug 18 19:00:00 PET 2011,
             To: Wed Aug 18 18:59:59 PET 2021]
 Issuer: CN=AC Certisign Parceria, O=Certisign Certificadora Digital S.A., C=BR
 SerialNumber: [    108d03ae b07005f8 2e1e76a5 50042348]

Certificate Extensions: 6
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 33 30 90 62 72 98 58 73   76 56 6D 3E 5B A2 54 08  30.br.XsvVm>[.T.
0010: BF D2 C7 97                                        ....
]
]

[2]: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
  SSL CA
  S/MIME CA
]

[3]: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
 CN=CertisignPriv1-60
]

[4]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://onsitecrl.certisign.com.br/repositorio/lcr/ACCertisignParceria/LatestCRL.crl]
]]

[5]: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[6]: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
 CA:true
 PathLen:0
]

]
```

```
 Algorithm: [SHA1withRSA]
 Signature:
0000: 53 D3 18 FE 71 77 41 D5   8B 33 5F 95 7E 5C 95 7E  S...qwA..3_..\..
0010: 65 AD E1 4D E9 98 BE 4B   0F CB A7 59 7E 05 E1 9F  e..M...K...Y....
0020: E2 2A D8 08 AF 55 38 E1   F7 09 E9 90 57 74 F0 27  .*...U8.....Wt.'
0030: 6E E8 D7 3F 12 95 74 97   7D 8B 62 27 9E 0F CD BF  n..?..t...b'....
0040: 39 13 07 D0 5F 85 32 23   A7 95 D9 D4 1F 40 6E BA  9..._.2#.....@n.
0050: ED D5 68 26 D7 7F C4 B8   6A 5A 10 7E 71 4B 04 B2  ..h&....jZ..qK..
0060: D5 7D 6E E2 AC 19 D7 7A   CC 22 0D 3E E4 83 42 92  ..n....z.".>..B.
0070: 6A DC 58 F8 32 5B 9A 9B   C0 71 B9 4C 5C 46 39 B1  j.X.2[...q.L\F9.
0080: 76 2A 72 FE F3 A6 89 86   E2 2A 3E CF 4D 7A 17 D2  v*r......*>.Mz..
0090: 66 34 27 40 EE BB 59 DC   E5 EA B8 D3 22 38 4D C8  f4'@..Y......"8M.
00A0: 7A 6D 36 1F 0B E1 F7 94   E6 6E 5D 4D B3 60 B7 93  zm6......n]M.`..
00B0: E8 E7 97 42 6A 0F F7 F9   9E 54 98 7A AF 0F DD 81  ...Bj....T.z....
00C0: F3 B9 3E B5 45 B4 12 66   D1 5A 4F 5F AC 6B 3F C4  ..>.E..f.ZO_.k?.
00D0: EC EF B2 DC C9 70 7B 61   E3 03 17 C2 B6 AA 6F 99  .....p.a......o.
00E0: FA 6F 94 BC 06 DA CA 32   F9 5A F9 84 2A 88 FE DE  .o.....2.Z..*...
00F0: FC 53 71 2B FF 3C 4C C8   DB 7A 8A 11 B6 F6 67 CC  .Sq+.<L..z....g.

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIEJzCCAw+gAwIBAgIQEI0DrrBwBfguHnalUAQjSDANBgkqhkiG9w0BAQUFADBc
MQswCQYDVQQGEwJCUjEtMCsGA1UEChMkQ2VydGlzaWduIENlcnRpZmljYWRvcmEg
RGlnaXRhbCBTLkEuMR4wHAYDVQQDExVBQyBDZXJ0aXNpZ24gUGFyY2VyaWEwHhcN
MTEwODE5MDAwMDAwWhcNMjEwODE4MjM1OTU5WjBcMQswCQYDVQQGEwJCUjEtMCsG
A1UEChMkQ2VydGlzaWduIENlcnRpZmljYWRvcmEgRGlnaXRhbCBTLkEuMR4wHAYD
VQQDExVBQyBDZXJ0aXNpZ24gUGFyY2VyaWEwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQDLbdYiBUZjEAJOqn473hdcxshGdHxvzFKsmoecLZHsqxdFQf9d
RcMWzLHB1JbV2Ly3ChoyakEXNXKaKI0Kffvd1eE7ZB4C86nvwXARFdRk8c0lDAdI
c9F5fu6sN0ot5M1mKcaMZNtIKVq9n4UVOX7Daedo/XzYuyWjPj9jr9lZcKzbWgLh
mRDsjDI4ZZwYkcr4HQ/mo5mEWg2Oi/+nWCyvx3Ac53RdaB8FMxTOIfp4nSExe1sA
LRTzVFeFmO4GUeuu2VTcaZtWKsObZYpknNT2fHNqdptOR/ShGHpvNKwrgxmKSQiT
VkZ6r8Hnc2kHvqfAsCXAWckvRjR66rhHYPoNAgMBAAGjgeQwgeEwDwYDVR0TBAgw
BgEB/wIBADBkBgNVHR8EXTBbMFmgV6BVhlNodHRwOi8vb25zaXRlY3JsLmNlcnRp
c2lnbi5jb20uYnIvcmVwb3NpdG9yaW8vbGNyL0FDQ2VydGlzaWduUGFyY2VyaWEv
TGF0ZXN0Q1JMLmNybDARBglghkgBhvhCAQEEBAMCAQYwKQYDVR0RBCIwIKQeMBwx
GjAYBgNVBAMTEUNlcnRpc2lnblByaXYxLTYwMB0GA1UdDgQWBBQzMJBicphYc3ZW
bT5bolQIv9LHlzALBgNVHQ8EBAMCAQYwDQYJKoZIhvcNAQEFBQADggEBAFPTGP5x
d0HVizNflX5clX5lreFN6Zi+Sw/Lp1l+BeGf4irYCK9VOOH3CemQV3TwJ27o1z8S
lXSXfYtiJ54Pzb85EwfQX4UyI6eV2dQfQG667dVoJtd/xLhqWhB+cUsEstV9buKs
Gdd6zCINPuSDQpJq3Fj4Mluam8BxuUxcRjmxdipy/vOmiYbiKj7PTXoX0mY0J0Du
u1nc5eq40yI4Tch6bTYfC+H3lOZuXU2zYLeT6OeXQmoP9/meVJh6rw/dgfO5PrVF
tBJm0VpPX6xrP8Ts77LcyXB7YeMDF8K2qm+Z+m+UvAbayjL5WvmEKoj+3vxTcSv/
PEzI23qKEbb2Z8w=
-----END CERTIFICATE-----
```

Certificate Service Provider Name (en): GSE

Trade name (en)	GSE
Information URI (en)	WWW.GSE.COM.CO
Service provider street address (es)	CALLE 64G NRO 90
Service provider street address (en)	CALLE 64G NRO 90
Service provider postal code (es)	111071
Service provider postal code (en)	111071
Service provider locality (es)	BOGOTA
Service provider locality (en)	BOGOTA
Service provider state (es)	BOGOTA
Service provider state (en)	BOGOTA
Service provider country (es)	CO
Service provider country (en)	CO

OID.1.3.6.1.4.1.31136.1.1.10.2=Entidad de Certificación Digital Abierta Autorizada por la Superintendencia de Industria y Comercio de Colombia. https://www.gse.com.co/ResolucionSIC.pdf, C=CO, L="BOGOTÁ, D.C.", STREET=Carrera 21 A No 124 - 55 Oficina 303.

https://www.gse.com.co/direccion, OU=http://www.gse.com.co, SERIALNUMBER=NIT 9002042728, O=GESTION DE SEGURIDAD ELECTRONICA S.A., CN=ROOT AC GSE S.A., EMAILADDRESS=ca@gse.com.co

Type	CA/QC
Status	undersupervision
Status starting time	2016-01-22T22:27:15.000Z

Service digital identity (X509)

Version	3
Serial number	0
Signature algorithm	SHA1withRSA
Issuer	OID.1.3.6.1.4.1.31136.1.1.10.2=Entidad de Certificación Digital Abierta Autorizada por la Superintendencia de Industria y Comercio de Colombia. https://www.gse.com.co/ResolucionSIC.pdf, C=CO, L="BOGOTÁ, D.C.", STREET=Carrera 21 A No 124 - 55 Oficina 303. https://www.gse.com.co/direccion, OU=http://www.gse.com.co, SERIALNUMBER=NIT 9002042728, O=GESTION DE SEGURIDAD ELECTRONICA S.A., CN=ROOT AC GSE S.A., EMAILADDRESS=ca@gse.com.co
Valid from	Mon May 11 10:00:27 PET 2009
Valid to	Wed May 04 10:00:27 PET 2039
Subject	OID.1.3.6.1.4.1.31136.1.1.10.2=Entidad de Certificación Digital Abierta Autorizada por la Superintendencia de Industria y Comercio de Colombia. https://www.gse.com.co/ResolucionSIC.pdf, C=CO, L="BOGOTÁ, D.C.", STREET=Carrera 21 A No 124 - 55 Oficina 303. https://www.gse.com.co/direccion, OU=http://www.gse.com.co, SERIALNUMBER=NIT 9002042728, O=GESTION DE SEGURIDAD ELECTRONICA S.A., CN=ROOT AC GSE S.A., EMAILADDRESS=ca@gse.com.co
Public key	Sun RSA public key, 4096 bits modulus: 859367881919772247312246693394761905888547005565534714178624266316800937804296915252009457116343912404363906487813233279201421953337560582277039405242058279688403482414263122393459329943195479838975657997256471569949859985691150946194655578388230130118641239743399900153666625135299638880810122383461917392898790806551456837046319166165126141321188577399897035475635318605039478697680647580174163868800818010134953620128890883946571270608035154358921095196657647834403659695402241577978279817451976997325501871685381556748646623698465443826134979223945935463677019554145948886450136031437768713209612381697796901537264656432881523955998027367582172685407297120897321243511790904023668208103647285796566206269630157818773992746145995202984827948289120992737098492359168638252562827781109814140471531152421335674321960403435555897081669508536892130381187265887337392540494681953770586448826608854362725269111328681327263126812579309792859997579701737886661097257958980244303677061486885940952642789759747012905365580501326964239374747384170381324886085079225829536915950639515542252668928123125268230699807947318672947888882837562251298253626067383579473322452924704446699494009604108293904934784951779347822000273224918432842333822268 1 public exponent: 65537
Subject key identifier	7892332b0c1924a0b72faaf64b6783894f8e3b41
CRL distribution points	http://crl.gse.com.co/root/crl_ac_gse.crl http://crl1.gse.com.co/root/crl_ac_gse.crl

Authority key identifier	048201f2308201ee80147892332b0c1924a0b72faaf64b6783894f8e3b41a18201d1a4820 1cd308201c9311c301a06092a864886f70d010901160d6361406773652e636f6d2e636f31 19301706035504030c10524f4f5420414320475345205320532e412e312e302c060355040a0c 2547455354494f4e20445205345475552494441442045 4c454354524f4e49434120532e 412e311730150603550405130e4e4954203930303230343237323831 1e301c060355040 b0c15687474703a2f2f7777772e6773652e636f6d2e636f314f304d06035504090c464361 72726572612032312041204e6f20313234202d203535204f666963696e61203330332e20 68747470733a2f2f7777772e6773652e636f6d2e636f2f64697265636369 6f6e3116301406 035504070c0d424f474f54c3812c20442e432e310b3009060355040613024 34f3181ae308 1ab060c2b0601040181f32001010a020c819a456e7469646164206465204365727469666 963616369c3b36e204469676974616c204162696572746120417574 6f72697a616461207 06f72206c6120537570657269 6e74656e64656e6369612064652049 6e647573747269612 07920436f6d657263696f20646520436f6c6f6d6269612e2068747470733a2f2f7777772e6 773652e636f6d2e636f2f5265736f6c7563696f6e5349432e706466820100
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=3
SHA1 Thumbprint	ba6c243d6f71cc03becf240734aec784d2206cea
SHA256 Thumbprint	c6b2d6b64ec0dd41a5aabf68e604313c9528e99d9ffdf9990a04967f0eeeed89

The decoded certificate:

```
[
[
 Version: V3
 Subject: OID.1.3.6.1.4.1.31136.1.1.10.2=Entidad de Certificación Digital Abierta Autorizada por la Superintendencia de Industria y Comercio de Colombia.
https://www.gse.com.co/ResolucionSIC.pdf, C=CO, L="BOGOTÁ, D.C.", STREET=Carrera 21 A No 124 - 55 Oficina 303. https://www.gse.com.co/direccion, OU=http://www.gse.com.co,
SERIALNUMBER=NIT 9002042728, O=GESTION DE SEGURIDAD ELECTRONICA S.A., CN=ROOT AC GSE S.A., EMAILADDRESS=ca@gse.com.co
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 4096 bits
 modulus:
859367881919772247312246693394761905888547005565534714178624266316800937804296915252009457116343912404363906487813233279201421953337560582277039405242058279688403482414263122393459329943195479838975657997256471569949859985691150946194655578388230130118641239743399900153666625135299638880810122383461917392898790806551456837046319166165126141321188577399897035475635318605039478697680647580174163686800818010134953620128890883946571270608035154358921095196657647834403659695402241577978279817451976997325501871685381556748646623698465443826134979223945935463677019554145948886450136031437768713209612381697796901537264656432881523955998027367582172685407297120897321243511790904023668208103647285796566206269630157818773992746145995202984827948289120992737098492359168638252562827781109814140471531152421335674321960403435555897081669508536892130381187265887337392504049468195377058644882660885436272526911132868132726312681579309792859997579701737886661097257958980244303677061486885940952642789759747012905365580501326964239374747384170381324886085079225829536915950639515542252668928123125268230699807947318672947888882837562251298253626067383579473322452924704446699494009604108293904934784951779347822000273224918432842333822268 1
 public exponent: 65537
 Validity: [From: Mon May 11 10:00:27 PET 2009,
              To: Wed May 04 10:00:27 PET 2039]
 Issuer: OID.1.3.6.1.4.1.31136.1.1.10.2=Entidad de Certificación Digital Abierta Autorizada por la Superintendencia de Industria y Comercio de Colombia.
https://www.gse.com.co/ResolucionSIC.pdf, C=CO, L="BOGOTÁ, D.C.", STREET=Carrera 21 A No 124 - 55 Oficina 303. https://www.gse.com.co/direccion, OU=http://www.gse.com.co,
SERIALNUMBER=NIT 9002042728, O=GESTION DE SEGURIDAD ELECTRONICA S.A., CN=ROOT AC GSE S.A., EMAILADDRESS=ca@gse.com.co
 SerialNumber: [    00]

Certificate Extensions: 9
[1]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://certs.gse.com.co/root/crt_ac_gse.crt]
]

[2]: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
 RFC822Name: info@gse.com.co
]

[3]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 78 92 33 2B 0C 19 24 A0   B7 2F AA F6 4B 67 83 89  x.3+..$../..Kg..
0010: 4F 8E 3B 41                                        O.;A
]
]

[OID.1.3.6.1.4.1.31136.1.1.10.2=Entidad de Certificación Digital Abierta Autorizada por la Superintendencia de Industria y Comercio de Colombia.
https://www.gse.com.co/ResolucionSIC.pdf, C=CO, L="BOGOTÁ, D.C.", STREET=Carrera 21 A No 124 - 55 Oficina 303. https://www.gse.com.co/direccion, OU=http://www.gse.com.co,
SERIALNUMBER=NIT 9002042728, O=GESTION DE SEGURIDAD ELECTRONICA S.A., CN=ROOT AC GSE S.A., EMAILADDRESS=ca@gse.com.co]
SerialNumber: [    00]
]

[4]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 78 92 33 2B 0C 19 24 A0   B7 2F AA F6 4B 67 83 89  x.3+..$../..Kg..
0010: 4F 8E 3B 41                                        O.;A
]
]

[5]: ObjectId: 2.5.29.18 Criticality=false
IssuerAlternativeName [
 URIName: http://www.gse.com.co
```

```
]

[6]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 2A 68 74 74 70 73 3A   2F 2F 64 70 63 2E 67 73  .*https://dpc.gs
0010: 65 2E 63 6F 6D 2E 63 6F   2F 72 6F 6F 74 2F 64 70  e.com.co/root/dp
0020: 63 5F 61 63 5F 67 73 65   2E 70 64 66              c_ac_gse.pdf

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 81 94 1A 81 91 53 75   6A 65 74 6F 20 61 20 44  0.....Sujeto a D
0010: 50 43 20 41 43 20 47 53   45 20 53 2E 41 2E 20 45  PC AC GSE S.A. E
0020: 6E 74 69 64 61 64 20 64   65 20 43 65 72 74 69 66  ntidad de Certif
0030: 69 63 61 63 69 F3 6E 20   44 69 67 69 74 61 6C 20  icaci.n Digital
0040: 41 62 69 65 72 74 61 20   2D 20 61 75 74 6F 72 69  Abierta - autori
0050: 7A 61 64 61 20 70 6F 72   20 6C 61 20 53 75 70 65  zada por la Supe
0060: 72 69 6E 74 65 6E 64 65   6E 63 69 61 20 64 65 20  rintendencia de
0070: 49 6E 64 75 73 74 72 69   61 20 79 20 43 6F 6D 65  Industria y Come
0080: 72 63 69 6F 20 28 53 49   43 29 20 64 65 20 43 6F  rcio (SIC) de Co
0090: 6C 6F 6D 62 69 61 2E                               lombia.

]]  ]
]

[7]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:3
]

[8]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.gse.com.co/root/crl_ac_gse.crl]
, DistributionPoint:
    [URIName: http://crl1.gse.com.co/root/crl_ac_gse.crl]
]]

[9]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: 6B E3 C3 9C 95 FE BE B1   34 AB 7F 6A 25 09 12 A3  k.......4..j%...
0010: 5F 89 D5 8C 80 0E CE D3   F9 74 C3 CE DF 99 A0 5E  _........t.....^
0020: 0F 3A 8A F9 57 E6 EC 20   82 07 8D 03 47 A2 52 FC  .:..W.. ....G.R.
0030: B3 0F C5 C7 80 62 4E 15   80 4D CF 01 54 06 96 3A  .....bN..M..T..:
0040: 97 B8 2C D9 C1 BB F1 CF   0C 77 85 D2 94 A3 B9 B8  ..,......w......
0050: EB 2B 2E FD D2 2F 6D D1   43 B2 8E 29 F5 75 5D D1  .+.../m.C..).u].
0060: A4 1D FC 2E F1 A0 41 32   9D D1 2E 6E B2 F9 47 97  ......A2...n..G.
0070: 39 CE D7 6C 7C B2 D3 27   36 4E 92 64 D3 F8 80 73  9..l...'6N.d...s
0080: 37 FB 22 6F 19 11 EE 5F   F6 06 EE D2 4E 5B 20 98  7."o..._....N[ .
0090: C0 0F 1F 7E 98 5F D5 46   D1 75 AC 7F 2E D6 60 98  .....F.u....`.
00A0: 69 CD 3D 4D 7A 4C 8B DA   82 0F 19 6A 2C 92 A4 9C  i.=MzL.....j,...
00B0: E5 75 04 18 AE 04 2A 68   94 8B 97 3A C5 04 B8 DF  .u....*h...:....
00C0: E6 8E 42 5E D3 20 76 9D   BA 16 CF 89 4B EE BF 6A  ..B^. v.....K..j
00D0: B6 CF 5E 77 C0 15 70 19   88 F0 9B 17 01 1E AB 8C  ..^w..p.........
00E0: 36 93 A3 F8 BC 4D 20 38   5B 35 F2 37 3A 04 8C 4D  6....M 8[5.7:..M
00F0: 72 76 E5 41 FB 75 9B 56   7B F1 AC C9 F4 40 51 0C  rv.A.u.V.....@Q.
0100: 76 5B 86 28 68 69 E2 E0   F1 EB 23 EC 34 C1 EB 48  v[.(hi....#.4..H
0110: A2 33 63 87 1B C6 84 26   7B 05 3A 3D 96 03 BC 50  .3c....&..:=...P
0120: 14 2D 3F 2A 4C 93 7F 47   83 C7 82 74 75 91 C7 76  .-?*L..G...tu..v
0130: E6 F8 03 98 74 CC B9 AF   F4 D2 4F 5F C3 AF 69 AE  ....t.....O_..i.
0140: 0D 1A 96 9C 06 05 B4 DD   B4 9E C6 17 60 27 44 46  ............`'DF
0150: 74 16 0C C6 01 6F AA 88   64 1C 4A DC D8 D3 86 F5  t....o..d.J.....
0160: 03 2B 44 78 C6 87 64 3B   AC 96 A1 8D EA ED AC 29  .+Dx..d;.......)
0170: 78 ED 60 FB DE 50 DF F9   C1 10 1E 65 52 C3 6E 1F  x.`..P.....eR.n.
0180: 7E 48 E5 74 0C B7 CC B0   95 51 AC 5C 5E 06 80 DB  .H.t.....Q.\^...
0190: 71 C0 5D AB EA 3B BA 4E   62 49 17 D9 95 54 33 B2  q.]..;.NbI...T3.
01A0: 05 95 17 B3 4F 26 44 C8   8A 00 F7 25 4A 15 CD AB  ....O&D....%J...
01B0: F9 BC 74 4C FB 0C 7C CC   41 FA 95 80 E6 DE 81 44  ..tL....A......D
01C0: 0C DD 62 99 F4 D3 A5 8D   1D A5 FE B2 23 0C A4 DC  ..b.........#...
01D0: B2 34 D5 C0 6C 49 C1 8A   5E 09 68 69 8E 98 5C 64  .4..lI..^.hi..\d
01E0: 3C 17 A1 48 E7 AB D1 19   35 FD 9F 49 B2 99 0F C1  <..H....5..I....
01F0: 66 F8 1C 52 53 AC F0 2E   CE FF 45 9C D9 36 E6 3E  f..RS.....E..6.>

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIMRDCCCiygAwIBAgIBADANBgkqhkiG9w0BAQUFADCCAckxHDAaBgkqhkiG9w0B
CQEWDWNhQGdzZS5jb20uY28xGTAXBgNVBAMMEFJPT1QgQUMgR1NFIFMuQS4xLjAs
BgNVBAoMJUdFU1RJT04gREUgU0VHVVJJREFEIEVMRUNUUk9OSUNBIFMuQS4xFzAV
BgNVBAUTDk5JVCA5MDAyMDQyNzI4MR4wHAYDVQQLDBVodHRwOi8vd3d3LmdzZS5j
b20uY28xTzBNBgNVBAkMRkNhcnJlcmEgMjEgQSBOObyAxMjQgLSA1NSBPZmljaW5h
IDMwMy4gaHR0cHM6Ly93d3cuZ3NlLmNvbS5jby9kaXJlY2Npb24xFjAUBgNVBAcM
DUJPR09Uw4EsIEQuQy4xCzAJBgNVBAYTAkNPMYGuMIGrBgwrBgEEAYHzIAEBCgIM
```

gZpFbnRpZGFkIGRlIENlcnRpZmljYWNpw7NuIERpZ2l0YWwgQWJpZXJ0YSBBdXRv
cml6YWRhIHBvciBsYSBTdXBlcmludGVuZGVuY2lhIGRlIEluZHVzdHJpYSB5IENv
bWVyY2lvIGRlIENvbG9tYmlhLiBodHRwczovL3d3dy5nc2UuY29tLmNvL1Jlc29s
dWNpb25TSUMucGRmMB4XDTA5MDUxMTE1MDAyN1oXDTM5MDUwNDE1MDAyN1owgggHJ
MRwwGgYJKoZIhvcNAQkBFg1jYUBnc2UuY29tLmNvMRkwFwYDVQQDDBBST09UIEFD
IEdTRSBTLkEuMS4wLAYDVQQKDCVHRVNUSU9OIERFIFNFR1VSSURBRCBFTEVDVFJP
TklDQSBTLkEuMRcwFQYDVQQFEw5OSVQgOTAwMjA0MjcyODEeMBwGA1UECwwVaHR0
cDovL3d3dy5nc2UuY29tLmNvMU8wTQYDVQQJDEZDYXJyZXJhIDIxIEEgTm8gMTI0
IC0gNTUgT2ZpY2luYSAzMDMuIGh0dHBzOi8vd3d3LmdzZS5jb20uY28vZGlyZWNj
aW9uMRYwFAYDVQQHDA1CT0dPVMOBLCBELkMuMQswCQYDVQQGEwJDTzGBrjCBqwYM
KwYBBAGB8yABAQoCDIGaRW50aWRhZCBkZSBDZXJ0aWZpY2FjacOzbiBEaWdpdGFs
IEFiaWVydGEgQXV0b3JpemFkYSBwb3IgbGEgU3VwZXJpbnRlbmRlbmNpYSBkZSBJ
bmR1c3RyaWEgeSBDb21lcmNpbyBkZSBDb2xvbWJpYS4gaHR0cHM6Ly93d3cuZ3Nl
LmNvbS5jby9SZXNvbHVjaW9uU0lDLnBkZjCCAiIwDQYJKoZIhvcNAQEBBQADggIP
ADCCAgoCggIBANKl0464KOXxsLqAKsMD09ib1F5usGP+vsnPZtITySFbI/NntX46
Mxy5E+XfAJqJYFzp9IhXN+M2L+DvLwRo/oxiYJK+XBs17arKfbR5/16lPSqTZt3Y
kxHQ/3i1ha1FRA/y1f5NGZAtUADP6BcdbSVjAeQVDQrZjZKZ3vvlibFq1YSKWgfm
pWB7SH5cnNXdxB/a9wDNgZNtSLhupOHv5NCHWgDB3oxWWZLaHXnQisOsLrFiM1Ff
WBGH+2UNkcodi4yBLZ/LlcZbpW+0x0V7QfQWGJh7Uob37EtLxWSufM0ig5BKBC/D
pJwfuNnEJiRLpVtOKOVIl01yPDGv6cH5tZkYnjnekJZsoak6DIFHx1s1rddSqIYt
mJxVlh9ApViUMUZ5ti2s2mZVFQIGqGldCO8SggL44h0SPuZM6cq9+saCPzPwomwB
3GO/jVwDEx98y8epbJIltS/TfVd6Xd6hmuUS0YUSZpxgXPhmggGj5MbMjr8APbfz
W15VOx36gqS9h9cavWCAHcgAfx/YKVjbFRBbOh2aRftvr4+XfJzsq7EAXkZvoHaQ
I8AnYOSoeBvL3oiIfOvYUTXFynA7SFKCp8drny1EGyIj1lSZDW4QaeB15qVhpg6u
gc++ovVaeRzzaoBm0BnumMZ30mR5SfjycEq3bGucV07zY5+gRZ/22SRZAgMBAAGj
ggQxMIIELTASBgNVHRMBAf8ECDAGAQH/AgEDMB0GA1UdDgQWBBR4kjMrDBkkoLcv
qvZLZ4OJT447QTCCAfsGA1UdIwSCAfIwggHugBR4kjMrDBkkoLcvqvZLZ4OJT447
QaGCAdGkggHNMIIByTEcMBoGCSqGSIb3DQEJARYNY2FAZ3NlLmNvbS5jbzEZMBcG
A1UEAwwQUk9PVCBBQyBHU0UgUy5BLjEuMCwGA1UECgwlR0VTVElPTiBERSBTRUdV
UklEQUQgRUxFQ1RST05JQ0EgUy5BLjEXMBUGA1UEBRMOTklUIDkwMDIwNDI3Mjgx
HjAcBgNVBAsMFWh0dHA6Ly93d3cuZ3NlLmNvbS5jbzFPME0GA1UECQxGQ2FycmVy
YSAyMSBBIE5vIDEyNCAtIDU1IE9maWNpbmEgMzAzLiBodHRwczovL3d3dy5nc2Uu
Y29tLmNvL2RpcmVjY2lvbjEWMBQGA1UEBwwNQk9HT1TDgSwgRC5DLjELMAkGA1UE
BhMCQ08xga4wgasGDCsGAQQBgfMgAQEKAgyBmkVudGlkYWQgZGUgQ2VydGlmaWNh
Y2nDs24gRGlnaXRhbCBBYmllcnRhIEF1dG9yaXphZGEgcG9yIGxhIFN1cGVyaW50
ZW5kZW5jaWEgZGUgSW5kdXN0cmlhIHkgQ29tZXJjaW8gZGUgQ29sb21iaWEuIGh0
dHBzOi8vd3d3LmdzZS5jb20uY28vUmVzb2x1Y2lvblNJQy5wZGaCAQAwDgYDVR0P
AQH/BAQDAgEGMEcGCCsGAQUFBwEBBDswOTA3BggrBgEFBQcwAoYraHR0cDovL2Nl
cnRzLmdzZS5jb20uY28vcm9vdC9jcnRfYWNfZ3NlLmNydDAgBgNVHRIEGTAXhhVo
dHRwOi8vd3d3LmdzZS5jb20uY28wGgYDVR0RBBMwEYEPaW5mb0Bnc2UuY29tLmNv
MIHzBgNVHSAEgeswgegwgeUGBFUdIAAwgdwwNgYIKwYBBQUHAgEWKmh0dHBzOi8v
ZHBjLmdzZS5jb20uY28vcm9vdC9kcGNfYWNfZ3NlLnBkZjCBoQYIKwYBBQUHAgIw
gZQagZFTdWpldG8gYSBEUEMgQUMgR1NFIFMuQS4gRW50aWRhZCBkZSBDZXJ0aWZp
Y2FjafNuIERpZ2l0YWwgQWJpZXJ0YSAtIGF1dG9yaXphZGEgcG9yIGxhIFN1cGVy
aW50ZW5kZW5jaWEgZGUgSW5kdXN0cmlhIHkgQ29tZXJjaW8gKFNJQykgZGUgQ29s
b21iaWEuMGwGA1UdHwRlMGMwL6AtoCuGKWh0dHA6Ly9jcmwuZ3NlLmNvbS5jby9y
b290L2NybF9hY19nc2UuY3JsMDCgLqAshipodHRwOi8vY3JsMS5nc2UuY29tLmNv
L3Jvb3QvY3JsX2FjX2dzZS5jcmwwDQYJKoZIhvcNAQEFBQADggIBAGvjw5yV/r6x
NKt/aiUJEqNfidWMgA7O0/l0w87fmaBeDzqK+Vfm7CCCB40DR6JS/LMPxceAYk4V
gE3PAVQGljqXuCzZwbvxzwx3hdKUo7m46ysu/dIvbdFDso4p9XVd0aQd/C7xoEEy
ndEubrL5R5c5ztdsfLLTJzZOkmTT+IBzN/sibxkR7l/2Bu7STlsgmMAPH36YX9VG
0XWsfy7WYJhpzT1NekyL2oIPGWoskqSc5XUEGK4EKmiUi5c6xQS43+aOQl7TIHad
uhbPiUvuv2q2z153wBVwGYjwmxcBHquMNpOj+LxNIDhbNfI3OgSMTXJ25UH7dZtW
e/GsyfRAUQx2W4YoaGni4PHrI+w0wetIojNjhxvGhCZ7BTo9lgO8UBQtPypMk39H
g8eCdHWRx3bm+AOYdMy5r/TST1/Dr2muDRqWnAYFtN20nsYXYCdERnQWDMYBb6qI
ZBxK3NjThvUDK0R4xodkO6yWoY3q7awpeO1g+95Q3/nBEB5lUsNuH35I5XQMt8yw
lVGsXF4GgNtxwF2r6ju6TmJJF9mVVDOyBZUXs08mRMiKAPclShXNq/m8dEz7DHzM
QfqVgObegUQM3WKZ9NOljR2l/rIjDKTcsjTVwGxJwYpeCWhpjphcZDwXoUjnq9EZ
Nf2fSbKZD8Fm+BxSU6zwLs7/RZzZNuY+
-----END CERTIFICATE-----

Certificate Service Provider Name (en): CERTICAMARA

Trade name (en)	CERTICAMARA
Information URI (en)	HTTPS://WWW.CERTICAMARA.COM
Service provider street address (es)	CALLE 7 26-20
Service provider street address (en)	CALLE 7 26-20
Service provider postal code (es)	110311
Service provider postal code (en)	110311
Service provider locality (es)	BOGOTA
Service provider locality (en)	BOGOTA
Service provider state (es)	CUNDINAMARCA
Service provider state (en)	CUNDINAMARCA

Service provider country (es)	CO
Service provider country (en)	CO

CN=AC Raíz Certicámara S.A., O=Sociedad Cameral de Certificación Digital - Certicámara S.A., C=CO

Type	CA/QC
Status	undersupervision
Status starting time	2016-04-05T21:32:43.000Z

Service digital identity (X509)

Version	3
Serial number	389082039731826069547528437385083 00
Signature algorithm	SHA1withRSA
Issuer	CN=AC Raíz Certicámara S.A., O=Sociedad Cameral de Certificación Digital - Certicámara S.A., C=CO
Valid from	Mon Nov 27 15:46:29 PET 2006
Valid to	Tue Apr 02 16:42:02 PET 2030
Subject	CN=AC Raíz Certicámara S.A., O=Sociedad Cameral de Certificación Digital - Certicámara S.A., C=CO
Public key	Sun RSA public key, 4096 bits modulus: 699332867387283653582902217535678854922983994839884548011419368411534465213154349013282321742155763009187644204997336150495690194807910576508992020568075150541515432818884960717734109703474444075161302740294266154021891527563544539930312351074874622787802426234493315959992394713552524352262580450710795446075362506350572335512700533484533131926044888989289200029284468750357421429760094241036977839937173662532437076621056628198923803407480655651106184193812559534543045223696807705246215922841826500322979943259136642203749765319401980252205999627182730113666529497150491644868912568518472495096398166939297181696394303152350057492894264545234512537607792182614738016165559915772218581273652180979990539626763760452545241200846064599277834425182938421402284042479167849023073511063435200143060667589230825132980322501180023386994135110386253314908387576756889268542497109905880632914239331654256138879871005778316385374518704083056624842273851601858290422002881778802543804176755918275683663673081429132022541779976649392245749554370138554192760633227167902586210216565882658621159552989598313448377140188793420472709247674492617004554191680839620221408077818614566836332975113215254835969908675980112877883109915276289123444737363175923
public exponent: 65537
Subject key identifier	d109d0e9d7ce797454f93a30b3f46d2c03031b68
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	cba1c5f8b0e35eb8b94512d3f934a2e90610d336
SHA256 Thumbprint	a6c51e0da5ca0a9309d2e4c0e40c2af9107aae8203857fe198e3e769e343085c

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=AC Raíz Certicámara S.A., O=Sociedad Cameral de Certificación Digital - Certicámara S.A., C=CO
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 4096 bits
 modulus:
699332867387283653582902217535678854922983994839884548011419368411534465213154349013282321742155763009187644204997336150495690194807910576508992020568075150541515432818884960717734109703474444075161302740294266154021891527563544539930312351074874622787802426234493315959992394713552524352262580450710795446075362506350572335512700533484533131926044888989289200029284468750357421429760094241036977839937173662532437076621056628198923803407480655651106184193812559534543045223696807705246215922841826500322979943259136642203749765319401980252205999627182730113666529497150491644868912568518472495096398166939297181696394303152350057492894264545234512537607792182614738016165559915772218581273652180979990539626763760452545241200846064599277834425182938421402284042479167849023073511063435200143060667589230825132980322501180023386994135110386253314908387576756889268542497109905880632914239331654256138879871005778316385374518704083056624842273851601858290422002881778802543804176755918275683663673081429132022541779976649392245749554370138554192760633227167902586210216565882658621159552989598313448377140188793420472709247674492617004554191680839620221408077818614566836332975113215254835969908675980112877883109915276289123444737363175923
 public exponent: 65537
 Validity: [From: Mon Nov 27 15:46:29 PET 2006,
```

```
             To: Tue Apr 02 16:42:02 PET 2030]
 Issuer: CN=AC Raíz Certicámara S.A., O=Sociedad Cameral de Certificación Digital - Certicámara S.A., C=CO
 SerialNumber: [    077e5293 7be015e3 57f0698c cbec0c]

Certificate Extensions: 4
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: D1 09 D0 E9 D7 CE 79 74   54 F9 3A 30 B3 F4 6D 2C  ......ytT.:0..m,
0010: 03 03 1B 68                                        ...h
]
]

[2]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 1F 68 74 74 70 3A 2F   2F 77 77 77 2E 63 65 72  ..http://www.cer
0010: 74 69 63 61 6D 61 72 61   2E 63 6F 6D 2F 64 70 63  ticamara.com/dpc
0020: 2F                                                 /

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 4E 1A 4C 4C 69 6D 69   74 61 63 69 6F 6E 65 73  0N.LLimitaciones
0010: 20 64 65 20 67 61 72 61   6E 74 ED 61 73 20 64 65   de garant.as de
0020: 20 65 73 74 65 20 63 65   72 74 69 66 69 63 61 64   este certificad
0030: 6F 20 73 65 20 70 75 65   64 65 6E 20 65 6E 63 6F  o se pueden enco
0040: 6E 74 72 61 72 20 65 6E   20 6C 61 20 44 50 43 2E  ntrar en la DPC.

]]  ]
]

[3]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[4]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: 5C 94 B5 B8 45 91 4D 8E   61 1F 03 28 0F 53 7C E6  \...E.M.a..(.S..
0010: A4 59 A9 B3 8A 7A C5 B0   FF 08 7C 2C A3 71 1C 21  .Y...z.....,.q.!
0020: 13 67 A1 95 12 40 35 83   83 8F 74 DB 33 5C F0 49  .g...@5...t.3\.I
0030: 76 0A 81 52 DD 49 D4 9A   32 33 EF 9B A7 CB 75 E5  v..R.I..23....u.
0040: 7A CB 97 12 90 5C BA 7B   C5 9B DF BB 39 23 C8 FF  z....\.....9#..
0050: 98 CE 0A 4D 22 01 48 07   7E 8A C0 D5 20 42 94 44  ...M".H..... B.D
0060: EF BF 77 A2 89 67 48 1B   40 03 05 A1 89 EC CF 62  ..w..gH.@......b
0070: E3 3D 25 76 66 BF 26 B7   BB 22 BE 6F FF 39 57 74  .=%vf.&.."o.9Wt
0080: BA 7A C9 01 95 C1 95 51   E8 AB 2C F8 B1 86 20 E9  .z.....Q..,... .
0090: 3F CB 35 5B D2 17 E9 2A   FE 83 13 17 40 EE 88 62  ?.5[...*....@..b
00A0: 65 5B D5 3B 60 E9 7B 3C   B8 C9 D5 7F 36 02 25 AA  e[.;`..<....6.%.
00B0: 68 C2 31 15 B7 30 65 EB   7F 1D 48 79 B1 CF 39 E2  h.1..0e...Hy..9.
00C0: 42 80 16 D3 F5 93 23 FC   4C 97 C9 5A 37 6C 7C 22  B.....#.L..Z7l."
00D0: D8 4A CD D2 8E 36 83 39   91 90 10 C8 F1 C9 35 7E  .J...6.9......5.
00E0: 3F B8 D3 81 C6 20 64 1A   B6 50 C2 21 A4 78 DC D0  ?.... d..P.!.x..
00F0: 2F 3B 64 93 74 F0 96 90   F1 EF FB 09 5A 34 40 96  /;d.t.......Z4@.
0100: F0 36 12 C1 A3 74 8C 93   7E 41 DE 77 8B EC 86 D9  .6...t...A.w....
0110: D2 0F 3F 2D D1 CC 40 A2   89 66 48 1E 20 B3 9C 23  ..?-..@..fH. ..#
0120: 59 73 A9 44 73 BC 24 79   90 56 37 B3 C6 29 7E A3  Ys.Ds.$y.V7..)..
0130: 0F F1 29 39 EF 7E 5C 28   32 70 35 AC DA B8 C8 75  ..)9..\(2p5....u
0140: 66 FC 9B 4C 39 47 8E 1B   6F 9B 4D 02 54 22 33 EF  f..L9G..o.M.T"3.
0150: 61 BA 9E 29 84 EF 4E 4B   33 47 76 97 6A CB 7E 5F  a..)..NK3Gv.j..~_
0160: FD 15 A6 9E 42 43 5B 66   5A 8A 88 0D F7 16 B9 3F  ....BC[fZ......?
0170: 51 65 2B 66 6A 8B D1 38   52 A2 D6 46 11 FA FC 9A  Qe+fj..8R..F....
0180: 1C 74 9E 8F 97 0B 02 4F   64 C6 F5 68 D3 4B 2D FF  .t.....Od..h.K-.
0190: A4 37 1E 8B 3F BF 44 BE   61 46 A1 84 3D 08 27 4C  .7..?.D.aF..=.'L
01A0: 81 20 77 89 08 EA 67 40   5E 6C 08 51 5F 34 5A 8C  . w...g@^l.Q_4Z.
01B0: 96 68 CD D7 F7 89 C2 1C   D3 32 00 AF 52 CB D3 60  .h.......2..R..`
01C0: 5B 2A 3A 47 7E 6B 30 33   A1 62 29 7F 4A B9 E1 2D  [*:G.k03.b).J..-
01D0: E7 14 23 0E 0E 18 47 E1   79 FC 15 55 D0 B1 FC 25  ..#...G.y..U...%
01E0: 71 63 75 33 1C 23 2B AF   5C D9 ED 47 77 60 0E 3B  qcu3.#+.\..Gw`.;
01F0: 0F 1E D2 C0 DC 64 05 89   FC 78 D6 5C 2C 26 43 A9  .....d...x.\,&C.

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGZjCCBE6gAwIBAgIPB35Sk3vgFeNX8GmMy+wMMA0GCSqGSIb3DQEBBQUAMHsx
CzAJBgNVBAYTAkNPMUcwRQYDVQQKDD5Tb2NpZWRhZCBDYW1lcmFsIGRlIENlcnRp
ZmljYWNpw7NuIERpZ2l0YWwgLSBDZXJ0aWPDoW1hcmEgUy5BLjEjMCEGA1UEAwwa
QUMgUmHDrXogQ2VydGljw6FtYXJhIFMuQS4wHhcNMDYxMTI3MjA0NjI5WhcNMzAw
NDAyMjE0MjAyWjB7MQswCQYDVQQGEwJDTzFHMEUGA1UECgw+U29jaWVkYWQgQ2Ft
ZXJhbCBkZSBDZXJ0aWZpY2FjacOzbiBEaWdpdGFsIC0gQ2VydGljw6FtYXJhIFMu
QS4xIzAhBgNVBAMMGkFDIFJhw6l6IENlcnRpY8OhbWFyYSBTLkEuMIICIjANBgkq
hkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAq2uJo1PMSCMI+8PPUZYILrgIem08kBeG
qentLhM0R7LQcNzJPNCNyu5LF6vQhbCnIwTLqKL85XXbQMpiiY9QngE9JlsYhBzL
```

fDe3fezTf3MZsGqy2IiKLUV0qPezuMDU2s0iiXRNWhU5cxh0T7XrmafBHoi0wpOQ
Y5fzp6cSsgkiBzPZkc0OnB8OIMfuuzONj8LSWKdf/WU34ojC2I+GdV75LaeHM/J4
Ny+LvB2GNzmxlPLYvEqcgxhaBvzz1NS6jBUJJfD5to0EfhcSM2tXSExP2yYe68yQ
54v5aHxwD6Mq0Do43zeX4lvegGHTgNiRg0JaTASJaBE8rF9ogEHMYELODVoqDA+b
MMCm8Ibbq0nXl21Ii/kDwFJnmxL3wvIumGVC2daa49AZMQyth9VXAnow6IYm+48j
ilSH5L887uvDdUhfHjlvgWJsxS3EF1QZtzeNnDeRyPYL1epjb4OsOMLzP96a++Ej
YfDIJss2yKHzMI+ko6Kh3VOz3vCaMh+DkXkwwakfU5tTohVTP92dsxA7SH2JD/zt
A/X7JWR1DhcZDY8AFmd5ekD8LVkH2ZD6mq093ICK5lw1omdMEWux+IBkAC1vImHF
rEsm5VoQgpukg3s0956JkSCXjrdCx2bD0Omk1vUgjcTDlaxECp1bczwmPS9KvqfJ
pxAe+59QafMCAwEAAaOB5jCB4zAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQE
AwIBBjAdBgNVHQ4EFgQU0QnQ6df0eXRU+Tows/RtLAMDG2gwgaAGA1UdIASBmDCB
lTCBkgYEVR0gADCBiTArBggrBgEFBQcCARYfaHR0cDovL3d3dy5jZXJ0aWNhbWFy
YS5jb20vZHBjLzBaBggrBgEFBQcCAjBOGkxMaW1pdGFjaW9uZXMgZGUgZ2FyYW50
7WFzIGRlIGVzdGUgY2VydGlmaWNhZG8gc2UgcHVlZGVuIGVuY29udHJhciBlbiBs
YSBEUEMuMA0GCSqGSIb3DQEBBQUAA4ICAQBclLW4RZFNjmEfAygPU3zmpFmps4p6
xbD/CHwso3EcIRNnoZUSQDWDg4902zNc8El2CoFS3UnUmjIz75uny3XlesuXEpBc
unvFm9+7OSPI/5jOCk0iAUgHforA1SBClETvv3eiiWdIG0ADBaGJ7M9i4z0ldma/
Jre7Ir5v/zlXdLp6yQGVwZVR6Kss+LGGIOk/yzVb0hfpKv6DExdA7ohiZVvVO2Dp
ezy4ydV/NgIlqmjCMRW3MGXrfx1IebHPOeJCgBbT9ZMj/EyXyVo3bHwi2ErN0o42
gzmRkBDI8ck1fj+404HGIGQatlDCIaR43NAvO2STdPCWkPHv+wlaNECW8DYSwaN0
jJN+Qd53i+yG2dIPPy3RzECiiWZIHiCznCNZc6lEc7wkeZBWN7PGKX6jD/EpOe9+
XCgycDWs2rjIdWb8m0w5R44bb5tNAlQiM+9hup4phO9OSzNHdpdqy35f/RWmnkJD
W2ZaiogN9xa5P1FlK2Zqi9E4UqLWRhH6/JocdJ6PlwsCT2TG9WjTSy3/pDceiz+/
RL5hRqGEPQgnTIEgd4kI6mdAXmwIUV80WoyWaM3X94nCHNMyAK9Sy9NgWyo6R35r
MDOhYil/SrnhLecUIw4OGEfhefwVVdCx/CVxY3UzHCMrr1zZ7Ud3YA47Dx7SwNxk
BYn8eNZcLCZDqQ==
-----END CERTIFICATE-----

Certificate Service Provider Name (en): GLOBALSIGN

Trade name (en)	GLOBALSIGN
Information URI (en)	WWW.GLOBALSIGN.COM
Service provider street address (es)	2 INT DRIVE SUITE 105
Service provider street address (en)	2 INT DRIVE SUITE 105
Service provider postal code (es)	NH 03801
Service provider postal code (en)	NH 03801
Service provider locality (es)	PORTSMOUNTH
Service provider locality (en)	PORTSMOUNTH
Service provider state (es)	NEW HAMPSHIRE
Service provider state (en)	NEW HAMPSHIRE
Service provider country (es)	US
Service provider country (en)	US

CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE

Type	CA/QC
Status	undersupervision
Status starting time	2016-04-06T14:35:09.000Z

Service digital identity (X509)

Version	3
Serial number	48357032784597076690052O4
Signature algorithm	SHA1withRSA
Issuer	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE
Valid from	Tue Sep 01 07:00:00 PET 1998
Valid to	Fri Jan 28 07:00:00 PET 2028
Subject	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE

Public key	Sun RSA public key, 2048 bits modulus: 27527298331346624659307815003393871405544020859223571253338520804765223 43098245824609877232115194167296164062767518627620505152624264337810015 88855132177420580564661683926500550131001048491763122941672420411403104 35772026717601763184706480259485212806902223894888566729634266984619221 16886242183819220349515189376221677774833012990958821020329977858189817 53208829083719309844518090545096453792773097910849097057583724773208933 36152882629891014286744815684371510751674825920204180490258122986862539 58520193415522094573293783030883438710804665700536345207177639670718128 31434632139721599256129760064339495631803354687 51 public exponent: 65537
Subject key identifier	607b661a450d97ca89502f7d04cd34a8fffcfd4b
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	b1bc968bd4f49d622aa89a81f2150152a41d829c
SHA256 Thumbprint	ebd41040e4bb3ec742c9e381d31ef2a41a48b6685c96e7cef3c1df6cd4331c99

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 2048 bits
 modulus:
27527298331346624659307815003393871405544020859223571253338520804765223430982458246098772321151941672961640627675186276205051526242643378100158885513217742058056466168392650055013100104849176312294167242041140310435772026717601763184706480259485212806902223894888566729634266984619221168862421838192203495151893762216777748330129909588210203299778581898175320882908371930984451809054509645379277309791084909705758372477320893336152882629891014286744815684371510751674825920204180490258122986862539585201934155220945732937830308834387108046657005363452071776396707181283143463213972159925612976006433949563180335468751
 public exponent: 65537
 Validity: [From: Tue Sep 01 07:00:00 PET 1998,
             To: Fri Jan 28 07:00:00 PET 2028]
 Issuer: CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE
 SerialNumber: [    04000000 0001154b 5ac394]

Certificate Extensions: 3
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 60 7B 66 1A 45 0D 97 CA   89 50 2F 7D 04 CD 34 A8  `.f.E....P/...4.
0010: FF FC FD 4B                                        ...K
]
]

[2]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[3]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: D6 73 E7 7C 4F 76 D0 8D   BF EC BA A2 BE 34 C5 28  .s..Ov.......4.(
0010: 32 B5 7C FC 6C 9C 2C 2B   BD 09 9E 53 BF 6B 5E AA  2...l.,+...S.k^.
0020: 11 48 B6 E5 08 A3 B3 CA   3D 61 4D D3 46 09 B3 3E  .H......=aM.F..>
0030: C3 A0 E3 63 55 1B F2 BA   EF AD 39 E1 43 B9 38 A3  ...cU.....9.C.8.
0040: E6 2F 8A 26 3B EF A0 50   56 F9 C6 0A FD 38 CD C4  ./.&;..PV....8..
0050: 0B 70 51 94 97 98 04 DF   C3 5F 94 D5 15 C9 14 41  .pQ......_.....A
0060: 9C C4 5D 75 64 15 0D FF   55 30 EC 86 8F FF 0D EF  ..]ud...U0......
0070: 2C B9 63 46 F6 AA FC DF   BC 69 FD 2E 12 48 64 9A  ,.cF.....i...Hd.
0080: E0 95 F0 A6 EF 29 8F 01   B1 15 B5 0C 1D A5 FE 69  .....).........i
0090: 2C 69 24 78 1E B3 A7 1C   71 62 EE CA C8 97 AC 17  ,i$x....qb......
00A0: 5D 8A C2 F8 47 86 6E 2A   C4 56 31 95 D0 67 89 85  ]...G.n*.V1..g..
00B0: 2B F9 6C A6 5D 46 9D 0C   AA 82 E4 99 51 DD 70 B7  +.l.]F......Q.p.
00C0: DB 56 3D 61 E4 6A E1 5C   D6 F6 FE 3D DE 41 CC 07  .V=a.j.\...=.A..
00D0: AE 63 52 BF 53 53 F4 2B   E9 C7 FD B6 F7 82 5F 85  .cR.SS.+......_.
00E0: D2 41 18 DB 81 B3 04 1C   C5 1F A4 80 6F 15 20 C9  .A..........o. .
00F0: DE 0C 88 0A 1D D6 66 55   E2 FC 48 C9 29 26 69 E0  ......fU..H.)&i.

]
```

The certificate in PEM format:

-----BEGIN CERTIFICATE-----
MIIDdTCCAl2gAwIBAgILBAAAAAABFUtaw5QwDQYJKoZIhvcNAQEFBQAwVzELMAkG
A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNpZ24gUm9vdCBDQTAeFw05ODA5MDExMjAw
MDBaFw0yODAxMjgxMjAwMDBaMFcxCzAJBgNVBAYTAkJFMRkwFwYDVQQKExBHbG9i
YWxTaWduIG52LXNhMRAwDgYDVQQLEwdSb290IENBMRswGQYDVQQDExJHbG9iYWxT
aWduIFJvb3QgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDaDuaZ
jc6j40+Kfvvxi4Mla+pIH/EqsLmVEQS98GPR4mdmzxzdzxtIK+6NiY6arymAZavp
xy0Sy6scTHAHoT0KMM0VjU/43dSMUBUc71DuxC73/OlS8pF94G3VNTCOXkNz8kHp
1Wrjsok6Vjk4bwY8iGlbKk3Fp1S4bInMm/k8yuX9ifUSPJJ4ltbcdG6TRGHRjcdG
snUOhugZitVtbNV4FpWi6cgKOOvyJBNPc1STE4U6G7weNLWLBYy5d4ux2x8gkasJ
U26Qzns3dLlwR5EiUWMWea6xrkEmCMgZK9FGqkjWZCrXgzT/LCrBbBlDSgeF59N8
9iFo7+ryUp9/k5DPAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIBBjAPBgNVHRMBAf8E
BTADAQH/MB0GA1UdDgQWBBRge2YaRQ2XyolQL30EzTSo//z9SzANBgkqhkiG9w0B
AQUFAAOCAQEA1nPnfE920I2/7LqivjTFKDK1fPxsnCwrvQmeU79rXqoRSLblCKOz
yj1hTdNGCbM+w6DjY1Ub8rrvrTnhQ7k4o+YviiY776BQVvnGCv04zcQLcFGUl5gE
38NflNUVyRRBnMRddWQVDf9VMOyGj/8N7yy5Y0b2qvzfvGn9LhJIZJrglfCm7ymP
AbEVtQwdpf5pLGkkeB6zpxxxYu7KyJesF12KwvhHhm4qxFYxldBniYUr+WymXUad
DKqC5JlR3XC321Y9YeRq4VzW9v493kHMB65jUr9TU/Qr6cf9tveCX4XSQRjbgbME
HMUfpIBvFSDJ3gyICh3WZlXi/EjJKSZp4A==
-----END CERTIFICATE-----

Certificate Service Provider Name (en): CAMERFIRMA PERU S.A.C.

Trade name (en)	CAMERFIRMA PERU S.A.C.
Information URI (en)	WWW.CAMERFIRMA.COM
Service provider street address (es)	AV. REPUBLICA DE PANAMA 3591, OFICINA 301, SAN ISIDRO, LIMA
Service provider street address (en)	AV. REPUBLICA DE PANAMA 3591, OFICINA 301, SAN ISIDRO, LIMA
Service provider postal code (es)	LIMA27
Service provider postal code (en)	LIMA27
Service provider locality (es)	SAN ISIDRO
Service provider locality (en)	SAN ISIDRO
Service provider state (es)	LIMA
Service provider state (en)	LIMA
Service provider country (es)	PE
Service provider country (en)	PE

CN=Camerfirma TSA II - 2014, L=Madrid (see current address at https://www.camerfirma.com/address), SERIALNUMBER=A82743287, O=AC Camerfirma S.A., OU=AC CAMERFIRMA, C=ES

Type	CA/QC
Status	undersupervision
Status starting time	2019-07-01T16:32:01.000Z

Service digital identity (X509)

Version	3
Serial number	2712386042892456504
Signature algorithm	SHA256withRSA
Issuer	CN=Chambers of Commerce Root - 2008, O=AC Camerfirma S.A., SERIALNUMBER=A82743287, L=Madrid (see current address at www.camerfirma.com/address), C=EU
Valid from	Tue Dec 16 11:45:33 PET 2014
Valid to	Tue Dec 15 11:45:33 PET 2037
Subject	CN=Camerfirma TSA II - 2014, L=Madrid (see current address at https://www.camerfirma.com/address), SERIALNUMBER=A82743287, O=AC Camerfirma S.A., OU=AC CAMERFIRMA, C=ES

Public key	Sun RSA public key, 4096 bits modulus: 836972814660267615624595344346087789280546060001061351361322188147011910802823163391284814505163200665760046243357181905822651911183039204277081178032780638806372623129012197695602409221000120537762482289796312029548326430655895804335277346513050755345274797241546442672927300268476853624848973449330020805141897324186057302892589660038561736848450772817210191739261320372259253937828830164818347077669864935637867751476656389595548326430655895804335277346513050755345274797241546442672927300268476853624848973449330020805141897324186057302892589660038561736848450772817210191739261320372259253937828830164818347077669864935637867751476656389558502271331732311287899474235072563645345909679091228303369098443417992711597402321123257383361907010139276108638524759011976218082301417845923211232573833619070101392761086385247590119762180823014178459298931658819425958754232188149956501533330630882345565263087492371812160223516409648190478072774685781222721859616384628346847545387268527840316907435741485346775848425640678816101838432964749238897555246177361743193749667589845861108259634862065893872872959182008790314093816581237153890469058747116207587672112646388807725832061006454537740345314037017059278664168713937292889133453918593136936028152756393425000953060730407697832029780715334184619355873881500949035087507865841024835394504199511220797845363757404036339615793852592416957673266728244539743349771502744892176042902472435595060069744549792163998667300445899554501331805232492404179602493870037081595 9 public exponent: 65537
Subject key identifier	17c540bc2af845b8ab33bff86f496cf617cab7d4
CRL distribution points	http://crl.camerfirma.com/chambersroot-2008.crl http://crl1.camerfirma.com/chambersroot-2008.crl
Authority key identifier	0481db3081d88014f924ac0fb2b5f879c0fa60881bc4d94d029e1719a181b4a481b13081ae310b3009060355040613024555314330410603550407133a4d6164726964202873656520637572726e74206164647265737320617420777772e63616d65726669726d612e636f6d2f6164726573732931123010060355040513094138323733433323837311b3019060355040a131241432043616d65726669726d6120532e412e312930270603550403132043686616d626572732063206f6620436f6d6d6572636520526f6f74202d2032303038820900a3da427ea4b1aeda
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=2
SHA1 Thumbprint	19ebdcededebc9251f3a098ff4c951ae555248b1
SHA256 Thumbprint	65695d500117fd7270f1027ed121f05942670075461d337eeec7f6a5b757a47a

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=Camerfirma TSA II - 2014, L=Madrid (see current address at https://www.camerfirma.com/address), SERIALNUMBER=A82743287, O=AC Camerfirma S.A., OU=AC CAMERFIRMA,
C=ES
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
836972814660267615624595344346087789280546060001061351361322188147011910802823163391284814505163200665760046243357181905822651911183039204277081178032780638806372623129012197695602409221000120537762482289796312029548326430655895804335277346513050755345274797241546442672927300268476853624848973449330020805141897324186057302892589660038561736848450772817210191739261320372259253937828830164818347077669864935637867751476656389558502271331732311287899474235072563645345909679091228303369098443417992711597402321123257383361907010139276108638524759011976218082301417845929893165881942595875423218814995650153333063088234556526308749237181216022351640964819047807277468578122721859616384628346847545387268527840317870435741485346775848425640678816101838432964749238897555246177361743193749667589845861108259634862065893872872959182008790314093816581237153890469058747116207587672112646388807725832061006454537740345314037017059278664168713937292889133453918593136936028152756393425000953060730407697832029780715334184619355873881500949035087507865841024835394504199511220797845363757404036339615793852592416957673266728244539743349771502744892176042902472435595060069744549792163998667300445899554501331805232492404179602493870037081595
 public exponent: 65537
 Validity: [From: Tue Dec 16 11:45:33 PET 2014,
             To: Tue Dec 15 11:45:33 PET 2037]
 Issuer: CN=Chambers of Commerce Root - 2008, O=AC Camerfirma S.A., SERIALNUMBER=A82743287, L=Madrid (see current address at www.camerfirma.com/address), C=EU
 SerialNumber: [    25a454bc 34551238]

Certificate Extensions: 8
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 17 C5 40 BC 2A F8 45 B8   AB 33 BF F8 6F 49 6C F6  ..@.*.E..3..oIl.
0010: 17 CA B7 D4                                        ....
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: F9 24 AC 0F B2 B5 F8 79   C0 FA 60 88 1B C4 D9 4D  .$.....y..`....M
0010: 02 9E 17 19                                        ....
```

```
]

[CN=Chambers of Commerce Root - 2008, O=AC Camerfirma S.A., SERIALNUMBER=A82743287, L=Madrid (see current address at www.camerfirma.com/address), C=EU]
SerialNumber: [    a3da427e a4b1aeda]
]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.camerfirma.com/chambersroot-2008.crl]
, DistributionPoint:
    [URIName: http://crl1.camerfirma.com/chambersroot-2008.crl]
]]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 1D 68 74 74 70 73 3A   2F 2F 70 6F 6C 69 63 79  ..https://policy
0010: 2E 63 61 6D 65 72 66 69   72 6D 61 2E 63 6F 6D     .camerfirma.com

]]  ]
]

[5]: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
 timeStamping
]

[6]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[7]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://www.camerfirma.com/certs/root_chambers-2008.crt,
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://ocsp.camerfirma.com]
]

[8]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 79 F5 51 F4 89 41 60 89   5D A0 7F 05 EA AC C5 A3  y.Q..A`.].......
0010: 9B A9 06 C5 B4 DD 43 CA   3B AA 07 7B 5C 87 62 22  ......C.;...\.b"
0020: 21 AF 87 BE 91 6A 67 78   9D 42 E5 ED 6F 50 2B BE  !....jgx.B..oP+.
0030: C5 C1 28 72 31 E1 38 72   16 09 1A E1 E7 04 41 AE  ..(r1.8r......A.
0040: 98 A0 0C D6 70 8A 86 0A   33 3C 0E A1 5C 85 02 A6  ....p...3<..\...
0050: 20 74 6B DA 87 4D BF 53   B4 7E 2A 08 9E E6 5B E6   tk..M.S..*...[.
0060: 8B 10 1F 4D 40 01 5A 65   53 8D 97 DC AF FF 83 BA  ...M@.ZeS.......
0070: 18 43 5A 77 58 93 3A 73   DB 34 94 D1 DF 19 7A FA  .CZwX.:s.4....z.
0080: 6B 2E 5A D0 71 B4 03 3E   8D FE 1C EC 90 1B 2E 4E  k.Z.q..>.......N
0090: FD 15 25 C5 94 FC 93 CE   BB A1 EA 96 79 A8 75 FC  ..%.........y.u.
00A0: 24 B1 4F BF F9 74 41 5B   20 7D 9C C6 7B A6 AB 48  $.O..tA[ ......H
00B0: BB 03 DB 83 68 08 6D 33   E6 E2 20 77 29 06 48 1F  ....h.m3.. w).H.
00C0: 2E D5 DC 2A 1B 34 7F F5   64 D6 34 13 8D 5B 3B CD  ...*.4..d.4..[;.
00D0: E0 D4 0E 15 06 88 43 05   77 BE F2 D8 E2 E6 1E C4  ......C.w.......
00E0: 2E EB 7D 12 ED 9B B7 1D   4F E9 69 C8 FC 43 F5 3F  ........O.i..C.?
00F0: 25 3F FE D1 28 9F D3 A9   23 25 EB 59 8A 77 DB BA  %?..(...#%.Y.w..
0100: B4 6E EC C1 7A 8C B4 EF   07 34 F8 4C 0C A4 B5 55  .n..z....4.L...U
0110: 86 39 FB 1E 2F 1F EA 65   36 42 7C D0 8B 85 D5 5D  .9../..e6B.....]
0120: 8B 7C 5D 52 1F FC C6 FB   A6 99 88 C1 A4 7C BC 54  ..]R...........T
0130: 14 13 D3 46 AA FD F5 9A   FA C6 F8 A6 46 3B 16 1D  ...F........F;..
0140: 3A 58 72 88 12 E4 7C 8B   B9 98 C6 DC 74 D9 C8 3E  :Xr.........t..>
0150: 1E 4A E0 4A 37 12 74 70   A1 48 40 FB 2C BF 84 C8  .J.J7.tp.H@.,...
0160: 7E 02 82 DE 0A 9E 9E 07   C1 BD 77 DE 27 DA C4 91  ..........w.'...
0170: 55 F5 05 DC 8B FC 28 AB   8F 2D 21 25 D6 AB 46 FE  U.....(..-!%..F.
0180: 1E 9C 9C 4F 19 FD 07 02   95 15 9E 4A 47 FA 05 F4  ...O.......JG...
0190: 05 CB B4 AE 7D 12 11 3F   87 2B DA 78 0C 0A D8 2C  .......?.+.x...,
01A0: B3 A8 AA 3C 08 3F 28 FC   3F DC F5 0E 20 CC 34 CD  ...<.?(.?... .4.
01B0: 36 FC E7 75 7F B3 9F C9   AA 51 D4 C7 C4 77 73 D6  6..u.....Q...ws.
01C0: 2F 7A 86 07 C0 DC 5E B4   F2 DB 94 DA 25 F5 99 8F  /z....^.....%...
01D0: 33 A0 4D BD 2D 20 D5 A4   4C 4B D3 17 6B 85 61 9E  3.M.- ..LK..k.a.
01E0: D0 CC 45 E7 9E E0 67 FC   5A D3 16 CE 57 2C DA D0  ..E...g.Z...W,..
01F0: 61 E3 02 D6 CC AB AC C3   70 7C A1 04 85 62 28 E6  a.......p....b(.

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIIcjCCBlqgAwIBAgIIJaRUvDRVEjgwDQYJKoZIhvcNAQELBQAwga4xCzAJBgNV
BAYTAkVVMUMwQQYDVQQHEzpNYWRyaWQgKHNlZSBjdXJyZW50IGFkZHJlc3MgYXQg
d3d3LmNhbWVyZmlybWEuY29tL2FkZHJlc3MpMRIwEAYDVQQFEwlBODI3NDMyODcx
```

GzAZBgNVBAoTEkFDIENhbWVyZmlybWEgUy5BLjEpMCcGA1UEAxMgQ2hhbWJlcnMg
b2YgQ29tbWVyY2UgUm9vdCAtIDIwMDgwHhcNMTQxMjE2MTY0NTMzWhcNMzcxMjE1
MTY0NTMzWjCBxjELMAkGA1UEBhMCRVMxFjAUBgNVBAsMDUFDIENBTUVSRklSTUEx
GzAZBgNVBAoMEkFDIENhbWVyZmlybWEgUy5BLjESMBAGA1UEBRMJQTgyNzQzMjg3
MUswSQYDVQQHDEJNYWRyaWQgKHNlZSBjdXJyZW50IGFkZHJlc3MgYXQgaHR0cHM6
Ly93d3cuY2FtZXJmaXJtYS5jb20vYWRkcmVzcykxITAfBgNVBAMMGENhbWVyZmly
bWEgVFNBIElJIC0gMjAxNDCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIB
AM0oheqBP9Qmiao6wpB2L+YcBScYURNMRYL2tf89yS3/aNiZgwTDYlmsR53z+tkB
RdHdEUjVMgDcQxUuqxg8NySktyVu5Vb8e4E4+SI9CfDcHLuriPDZX5+sSG2ATWMt
WibjjlGxiJnQhVl8eZNQuPyGP4qRt5QIVnvFLKm3Ec3AvIDFXPA1gxMY34aH9Ub/
h/jgO4hIdl8cjCg456eLMyf7v/xTLLhylcCET7JbDIXMasHTB5B+1absFpLTgRna
SN7RdDnHLpDc+JRam5kXsxrGE3BGK70suqLFWtBksPuY80+tBVvu36UvYOCBi7OJ
66dRCd+0AGFZ9BL3uB0c1m21Y7oHvkJA/QToWDQRjyg/SvAHEIvltRN+yUYa8OAE
1VKmZjnX0PkntzcmmaQhEa/zhKnUZyQpAFz+1+YKJJNNqwaPuYLyXp0bi3zV5GkO
nZpf5yhrj3BTzuytbl9MpWzKMaKdcWFdvgMNbdfalDV6u9C+K7LAcIu6mzyJ1Rl7
7WfiWn4STP65WwdS1KxHOgbBsy7MP2MObfkc+iQYxz4NzzMGN3qk9bflT1BKtmhi
HJXYDvT6Hw9ilcpXbFSE7INu/rTV70/REBTeioBnAE/Ouq4TG/CZU8UQ1Ze/DhwL
p0+YCpaRbEH5G0pNc5tg6xrxAJv3gIapvdBujAKHUyvXAgMBAAGjggJ4MIICdDAS
BgNVHRMBAf8ECDAGAQH/AgECMB0GA1UdDgQWBBQXxUC8KvhFuKszv/hvSWz2F8q3
1DCB4wYDVR0jBIHbMIHYgBT5JKwPsrX4ecD6YIgbxNlNAp4XGaGBtKSBsTCBrjEL
MAkGA1UEBhMCRVUxQzBBBgNVBAcTOk1hZHJpZCAoc2VlIGN1cnJlbnQgYWRkcmVz
cyBhdCB3d3cuY2FtZXJmaXJtYS5jb20vYWRkcmVzcykxEjAQBgNVBAUTCUE4Mjc0
MzI4NzEbMBkGA1UEChMSQUMgQ2FtZXJmaXJtYSBTLkEuMSkwJwYDVQQDEyBDaGFt
YmVycyBvZiBDb21tZXJjZSBSb290IC0gMjAwOIIJAKPaQn6ksa7aMHoGCCsGAQUF
BwEBBG4wbDBCBggrBgEFBQcwAoY2aHR0cDovL3d3dy5jYW1lcmZpcm1hLmNvbS9j
ZXJ0cy9yb290X2NoYW1iZXJzLTIwMDguY3J0MCYGCCsGAQUFBzABhhpodHRwOi8v
b2NzcC5jYW1lcmZpcm1hLmNvbTAOBgNVHQ8BAf8EBAMCAQYwEwYDVR0lBAwwCgYI
KwYBBQUHAwgwPgYDVR0gBDcwNTAzBgRVHSAAMCswKQYIKwYBBQUHAgEWHWh0dHBz
Oi8vcG9saWN5LmNhbWVyZmlybWEuY29tMHgGA1UdHwRxMG8wNaAzoDGGL2h0dHA6
Ly9jcmwuY2FtZXJmaXJtYS5jb20vY2hhbWJlcnNyb290LTIwMDguY3JsMDagNKAy
hjBodHRwOi8vY3JsMS5jYW1lcmZpcm1hLmNvbS9jaGFtYmVyc3Jvb3QtMjAwOC5j
cmwwDQYJKoZIhvcNAQELBQADggIBAHn1UfSJQWCJXaB/BeqsxaObqQbFtN1Dyjuq
B3tch2IiIa+HvpFqZ3idQuXtb1ArvsXBKHIx4ThyFgka4ecEQa6YoAzWcIqGCjM8
DqFchQKmIHRr2odNv1O0fioInuZb5osQH01AAVplU42X3K//g7oYQ1p3WJM6c9s0
lNHfGXr6ay5a0HG0Az6N/hzskBsuTv0VJcWU/JPOu6Hqlnmodfwks U+/+XRBWyB9
nMZ7pqtIuwPbg2gIbTPm4iB3KQZIHy7V3CobNH/1ZNY0E41bO83g1A4VBohDBXe+
8tji5h7ELut9Eu2btx1P6WnI/EP1PyU//tEon9OpIyXrWYp327q0buzBeoy07wc0
+EwMpLVVhjn7Hi8f6mU2QnzQi4XVXYt8XVIf/Mb7ppmIwaR8vFQUE9NGqv31mvrG
+KZGOxYdOlhyiBLkfIu5mMbcdNnIPh5K4Eo3EnRwoUhA+yy/hMh+AoLeCp6eB8G9
d94n2sSRVfUF3Iv8KKuPLSEl1qtG/h6cnE8Z/QcClRWeSkf6BfQFy7SufRIRP4cr
2ngMCtgss6iqPAg/KPw/3PUOIMw0zTb853V/s5/JqlHUx8R3c9YveoYHwNxetPLb
lNol9ZmPM6BNvS0g1aRMS9MXa4VhntDMReee4Gf8WtMWzlcs2tBh4wLWzKusw3B8
oQSFYijm
-----END CERTIFICATE-----

CN=AC CAMERFIRMA PERÚ - 2016, O=AC CAMERFIRMA S.A., OID.2.5.4.97=VATES-A82743287, SERIALNUMBER=A82743287, OU=AC CAMERFIRMA PERÚ - 2016, OU=see current address at https://www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES

Type	CA/QC
Status	undersupervision
Status starting time	2018-06-07T21:02:25.000Z

Service digital identity (X509)

Version	3
Serial number	2807055470371932274
Signature algorithm	SHA256withRSA
Issuer	CN=GLOBAL CHAMBERSIGN ROOT - 2016, O=AC CAMERFIRMA S.A., OID.2.5.4.97=VATES-A82743287, SERIALNUMBER=A82743287, OU=GLOBAL CHAMBERSIGN ROOT - 2016, OU=see current address at www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES
Valid from	Tue Oct 11 03:37:59 PET 2016
Valid to	Sat Mar 10 03:37:59 PET 2040
Subject	CN=AC CAMERFIRMA PERÚ - 2016, O=AC CAMERFIRMA S.A., OID.2.5.4.97=VATES-A82743287, SERIALNUMBER=A82743287, OU=AC CAMERFIRMA PERÚ - 2016, OU=see current address at https://www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES

Public key

Sun RSA public key, 4096 bits
modulus:
665951606647505166658889470798122225428937440418830768530898564645406216744345864534477733338107892076008300650285092745178229484216228407877786946264208789275682888851610002187727135260301491027747250520919461113511231977956366388444335788156391967956751684950421173105958098965512808612995125132623438461450357323065271945370860125896404344668522421398659528540421178534719175649512308344686598631256869196614575598925005623049738607819025590861572013201762385105815366248584578202797685079134517369427970620243935399882403865979817090561523207098974938446022626118430979039929920989181915901414400656009231705293866177096061744465187297422918766133113649484326951864714134690983993479862444384363619217738777251708828734391571673577011536590261589625585065879942714125471501042352007035102991793585049504195269847835892671242263636394834409896318684130114505702707141794804317696063105059971910121408353233237271746565929166123565046832808010816676436720761693017207108301296084471993971982860116170664632376211441916858788941710231239358663155388604556676288871088123401338708254402460461585314778881017900018639924552342583665388380842031742442925088440791410583474516811132953276777843023094972373257204238327736510101493313711
public exponent: 65537

Subject key identifier

b76a026d2cd9b036b32b6c05aa345e06edb2b99b

CRL distribution points

http://crl.camerfirma.com/globalchambersignroot-2016.crl

http://crl1.camerfirma.com/globalchambersignroot-2016.crl

Authority key identifier

048201383082013480 14e89bcd7e86629b7a4d8c00973985cf1c7890703aa1820110a482010c30820108310b3009060355040613024553310f300d06035504080c064d414452494 4310f300d06035504070c064d4144524944313a3038060355040b0c31736565206375727 2656e74206164647265737320617420777772e63616d65726669726d612e636f6d2f616 4647265737331273025060355040b0c1e474c4f42414c204348414d4245525349474e205 24f4f54202d203230313631123010060355040513094138323734333238373118301606035504610c0f56415445532d413832373433323837311b3019060355040a0c12414320434 14d45524649524d4120532e412e312730250603550403 0c1e474c4f42414c204348414d4 245525349474e20524f4f54202d203230313682082dd22e5030a65e13

Key usage

keyCertSign

cRLSign

Basic constraints

CA=true; PathLen=2

SHA1 Thumbprint

45a256443a1631c851a1156310f5f385736bd2c5

SHA256 Thumbprint

71a0214d43e5b3596ddb36af8459e9e579ae929b800d94a9e3f671e9f431c4f3

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=AC CAMERFIRMA PERÚ - 2016, O=AC CAMERFIRMA S.A., OID.2.5.4.97=VATES-A82743287, SERIALNUMBER=A82743287, OU=AC CAMERFIRMA PERÚ - 2016, OU=see current address at
https://www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
665951606647505166658889470798122225428937440418830768530898564645406216744345864534477733338107892076008300650285092745178229484216228407877786946264208789275682888851610002187727135260301491027747250520919461113511231977956366388444335788156391967956751684950421173105958098965512808612995125132623438461450357323065271945370860125896404344668522421398659528540421178534719175649512308344686598631256869196614575598925005623049738607819025590861572013201762385105815366248584578202797685079134517369427970620243935399882403865979817090561523207098974938446022626118430979039929920989181915901414400656009231705293866177096061744465187297422918766133113649484326951864714134690983993479862444384363619217738767177250882873439157167357701153659026158962558506587994271412547150104235200703510299179358504950419526984783589267124226363639483440989631868413011450570227071417948043176960631050599719101214083532332372717465659291661235650468328080108166764367207616930172071083012960844719939719828601161706646323762114419168587889417102312393586631553886045566728887108812340133870825440246046158531477888101790001863992455234258366538838084203174244292508844079141058347451681113295327677784302309497237325720423832773651010149331371
 public exponent: 65537
 Validity: [From: Tue Oct 11 03:37:59 PET 2016,
              To: Sat Mar 10 03:37:59 PET 2040]
 Issuer: CN=GLOBAL CHAMBERSIGN ROOT - 2016, O=AC CAMERFIRMA S.A., OID.2.5.4.97=VATES-A82743287, SERIALNUMBER=A82743287, OU=GLOBAL CHAMBERSIGN ROOT - 2016, OU=see current
address at www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES
 SerialNumber: [    26f4aa13 f0560872]

Certificate Extensions: 7
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: B7 6A 02 6D 2C D9 B0 36   B3 2B 6C 05 AA 34 5E 06  .j.m,..6.+l..4^.
0010: ED B2 B9 9B                                        ....
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
```

```
KeyIdentifier [
0000: E8 9B CD 7E 86 62 9B 7A   4D 8C 00 97 39 85 CF 1C  .....b.zM...9...
0010: 78 90 70 3A                                        x.p:
]

[CN=GLOBAL CHAMBERSIGN ROOT - 2016, O=AC CAMERFIRMA S.A., OID.2.5.4.97=VATES-A82743287, SERIALNUMBER=A82743287, OU=GLOBAL CHAMBERSIGN ROOT - 2016, OU=see current address at
www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES]
SerialNumber: [    2dd22e50 30a65e13]
]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.camerfirma.com/globalchambersignroot-2016.crl]
, DistributionPoint:
    [URIName: http://crl1.camerfirma.com/globalchambersignroot-2016.crl]
]]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 1D 68 74 74 70 73 3A   2F 2F 70 6F 6C 69 63 79  ..https://policy
0010: 2E 63 61 6D 65 72 66 69   72 6D 61 2E 63 6F 6D     .camerfirma.com

]]  ]
]

[5]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[6]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://www.camerfirma.com/certs/globalchambersignroot-2016.crt,
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://ocsp.camerfirma.com]
]

[7]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: C1 26 DF 8F 7B B8 07 26   6A 0E 64 60 27 B3 5C F3  .&.....&j.d`'.\.
0010: FF 0F B8 B0 9F BE 49 E4   F9 5E 3D EE 54 9A 50 CC  ......I..^=.T.P.
0020: 1E B7 FA 10 6B C5 CE F3   09 23 DE 8B 56 DF 3B BB  ....k....#..V.;.
0030: 77 1F 24 43 97 BE 11 D1   E3 13 B5 C7 9D 7B 33 12  w.$C..........3.
0040: 5D C4 AB 33 C4 B5 5E CC   3C D7 19 3A C8 5D C4 49  ]..3..^.<..:.].I
0050: 63 FE F2 23 29 24 01 D3   EC 8A 44 45 DE 43 E6 53  c..#)$....DE.C.S
0060: BF 0A 0D 5A 4E DE CE B9   6A 37 DC 07 5E 9B 92 B9  ...ZN...j7..^...
0070: D0 2B B1 1B 27 4A F0 5C   64 2D E2 69 FD CF DA 92  .+..'J.\d-.i....
0080: B8 DC 77 94 AF 1C 9F B0   4B 2D AA C3 3F D4 DA 3D  ..w.....K-..?..=
0090: D1 F4 C1 37 81 9F 77 F9   33 7C D0 42 74 0D F0 2C  ...7..w.3..Bt..,
00A0: 84 A5 0D 9D 01 1B B8 76   20 20 AE 83 B8 BF EE 09  .......v  ......
00B0: B6 F5 6D 0D 6B 0A 6A 54   35 01 5B 0E 70 2F 4E 13  ..m.k.jT5.[.p/N.
00C0: 2C 9D 67 4D B9 24 C1 34   78 DA A5 24 8B 0F 2D 70  ,.gM.$.4x..$..-p
00D0: EE 54 4C CE AA 5B BA 78   21 63 34 32 C0 B6 A0 A7  .TL..[.x!c42....
00E0: A4 DC 1D 84 41 BA C2 23   D7 23 D7 6D 94 EA A8 B0  ....A..#.#.m....
00F0: 52 1F 9E C4 BA 28 05 E7   7D F2 F8 7E 10 9C 80 D2  R....(.........
0100: E9 82 96 BB AF 91 5D 4D   AE 57 A6 A4 36 9E F4 97  ......]M.W..6...
0110: 9E 03 65 A8 28 79 68 74   73 2D 16 76 E7 16 90 4F  ..e.(yhts-.v...O
0120: F4 63 02 FE 03 FE 53 2F   8F 30 33 8E 06 A9 45 93  .c....S/.03...E.
0130: 47 11 B8 F5 A2 3A DA 41   2F 3E FB FF 1C 3A EA 96  G....:.A/>...:..
0140: 01 91 E4 53 04 5D 2D 24   DF 28 DB E8 98 A2 4D 08  ...S.]-$.(....M.
0150: 7E 65 E4 96 7A 9F 76 54   0E 41 8F 87 81 2A 88 4B  .e..z.vT.A...*.K
0160: 49 B2 CC 03 24 AA B8 12   EC 43 EB 0B 7E C9 F0 67  I...$....C.....g
0170: F7 A3 CB DB A5 B8 00 E1   2F 2B D7 3F 61 7E D5 06  ......../+.?a...
0180: 5C 6F E3 0A C2 B6 EA 68   3A F6 D9 96 BF 53 A1 1E  \o.....h:....S..
0190: 68 A3 17 53 40 6C 52 6F   3C 6A E6 14 38 5A 03 88  h..S@lRo<j..8Z..
01A0: 9C 1A AB 03 CE F8 1F 25   E6 F1 4C 4F 71 72 23 D8  .......%..LOqr#.
01B0: 7E 17 E1 89 FD 0F 07 01   CA 8D 16 21 8D B9 50 B3  ...........!..P.
01C0: 67 4E D9 D0 F6 3E 10 14   78 4C 0A C7 EB 9A 1D 66  gN...>..xL.....f
01D0: 42 17 F4 96 A2 8E 20 F1   24 DB 44 D5 8A 13 ED CE  B..... .$.D.....
01E0: F8 8D B3 FB 93 A0 5A E4   36 1A B7 27 54 97 04 C2  ......Z.6..'T...
01F0: E2 C2 E6 AF 6E 45 61 08   75 15 C6 5E 24 87 BE 59  ....nEa.u..^$..Y

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIJeDCCB2CgAwIBAgIIJvSqE/BWCHIwDQYJKoZIhvcNAQELBQAwggEIMQswCQYD
VQQGEwJFUzEPMA0GA1UECAwGTUFEUklEMQ8wDQYDVQQHDAZNQURSSUQxOjA4BgNV
BAsMMXNlZSBjdXJyZW50IGFkZHJlc3MgYXQgd3d3LmNhbWVyZmlybWEuY29tL2Fk
ZHJlc3MxJzAlBgNVBAsMHkdMT0JBTCBDSEFNQkVSU0lHTiBST09UIC0gMjAxNjES
```

MBAGA1UEBRMJQTgyNzQzMjg3MRgwFgYDVQRhDA9WQVRFUy1BODI3NDMyODcxGzAZ
BgNVBAoMEkFDIENBTUVSRklSTUEgUy5BLjEnMCUGA1UEAwweR0xPQkFMIENIQU1C
RVJTSUdOIFJPT1QgLSAyMDE2MB4XDTE2MTAxMTA4Mzc1OVoXDTQwMDMxMDA4Mzc1
OVowggEIMQswCQYDVQQGEwJFUzEPMA0GA1UECAwGTUFEUklEMQ8wDQYDVQQHDAZN
QURSSUQxQjBABgNVBAsMOXNlZSBjdXJyZW50IGFkZHJlc3MgYXQgaHR0cHM6Ly93
d3cuY2FtZXJmaXJtYS5jb20vYWRkcmVzczEjMCEGA1UECwwaQUMgQ0FNRVJGSVJN
QSBQRVLDmiAtIDIwMTYxEjAQBgNVBAUTCUE4Mjc0MzI4NzEYMBYGA1UEYQwPVkFU
RVMtQTgyNzQzMjg3MRswGQYDVQQKDBJBQyBDQU1FUkZJUk1BIFMuQS4xIzAhBgNV
BAMMGkFDIENBTUVSRklSTUEgUEVSw5ogLSAyMDE2MIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEAozzYLMgB+MNXIch8o5dOO/Mto++IIgqyAPBOWFgT6sCY
ZGoQp3t+m5fRATsSgx4QYn28RGcdBgEBhYt77Dl4W1OODbmkaPJJrAiA5ww/IF19
yB8Wlzfaa0aqwKKH9wzfFro5cHh6vkWUp6LwYSxGSN9dvMXnye9KgsmrHLZ9QKAt
UsUN9ktWXjYpS4ASO3ICbih3WU3Awy5xtws0dZvWfSZNLlheZPpKR5KPOgFFTXkl
gwOf2WFuv+Po6G5xZk9LPt+U+50IqB3hRPLPjzmS805/6WnhrGujPyLWXEmNg8fD
Nuqzk0L0hwy9F3jGC7pMZIGkKV+3tpcV/QaVm8EQZE2L4xkq+vWs+x/PWoaVugg9
Kkp/k9JxCAs7SQ0AlSLuN1brSeQndFgktF3FkUx7XoBWdGPCL3ux9j/4lSDjgyNE
T+vCm80+vHA497UL41bswredV4qXDqmuVVBL0qI2bKfUG7wKEMIsN1gQbtOJr6Ul
VeycZasfltZ866fVaphaFBCH7Et0XAD/M1ge3fUI5hG+7X15qu51lPZUoWH/z6IR
Wbl1M0HIfs5Wk+Px70iO4RjNT2E6j+ZqOcfRty3ylodyhAyaPIOrA2099kJq6JH4
5gYjO7hy5oXaGk1uiZpwUzPJfdDCm/CKp2OO9woNjUTtm7jV66gInI8MkB9ysasC
AwEAAaOCAuAwggLcMBIGA1UdEwEB/wQIMAYBAf8CAQIwHQYDVR0OBBYEFLdqAm0s
2bA2sytsBao0XgbtsrmbMIIBQQYDVR0jBIIBODCCATSAFOibzX6GYpt6TYwAlzmF
zxx4kHA6oYIBEKSCAQwwggEIMQswCQYDVQQGEwJFUzEPMA0GA1UECAwGTUFEUklE
MQ8wDQYDVQQHDAZNQURSSUQxOjA4BgNVBAsMMXNlZSBjdXJyZW50IGFkZHJlc3Mg
YXQgd3d3LmNhbWVyZmlybWEuY29tL2FkZHJlc3MxJzAlBgNVBAsMHkdMT0JBTCBD
SEFNQkVSU0lHTiBST09UIC0gMjAxNjESMBAGA1UEBRMJQTgyNzQzMjg3MRgwFgYD
VQRhDA9WQVRFUy1BODI3NDMyODcxGzAZBgNVBAoMEkFDIENBTUVSRklSTUEgUy5B
LjEnMCUGA1UEAwweR0xPQkFMIENIQU1CRVJTSUdOIFJPT1QgLSAyMDE2gggt0i5Q
MKZeEzCBggYIKwYBBQUHAQEEdjB0MEoGCCsGAQUFBzAChj5odHRwOi8vd3d3LmNh
bWVyZmlybWEuY29tL2NlcnRzL2dsb2JhbGNoYW1iZXJzaWducm9vdC0yMDE2LmNy
dDAmBggrBgEFBQcwAYYaaHR0cDovL29jc3AuY2FtZXJmaXJtYS5jb20wDgYDVR0P
AQH/BAQDAgEGMD4GA1UdIAQ3MDUwMwYEVR0gADArMCkGCCsGAQUFBwIBFh1odHRw
czovL3BvbGljeS5jYW1lcmZpcm1hLmNvbTCBjAYDVR0fBIGEMIGBMD6gPKA6hjho
dHRwOi8vY3JsLmNhbWVyZmlybWEuY29tL2dsb2JhbGNoYW1iZXJzaWducm9vdC0y
MDE2LmNybDA/oD2gO4Y5aHR0cDovL2NybDEuY2FtZXJmaXJtYS5jb20vZ2xvYmFs
Y2hhbWJlcnNpZ25yb290LTIwMTYuY3JsMA0GCSqGSIb3DQEBCwUAA4ICAQDBJt+P
e7gHJmoOZGAns1zz/w+4sJ++SeT5Xj3uVJpQzB63+hBrxc7zCSPei1bfO7t3HyRD
l74R0eMTtcedezMSXcSrM8S1Xsw81xk6yF3ESWP+8iMpJAHT7IpERd5D5lO/Cg1a
Tt7OuWo33Adem5K50CuxGydK8FxkLeJp/c/akrjcd5SvHJ+wSy2qwz/U2j3R9ME3
gZ93+TN80EJ0DfAshKUNnQEbuHYgIK6DuL/uCbb1bQ1rCmpUNQFbDnAvThMsnWdN
uSTBNHjapSSLDy1w7lRMzqpbunghYzQywLagp6TcHYRBusIj1yPXbZTqqLBSH57E
uigF533y+H4QnIDS6YKWu6+RXU2uV6akNp70l54DZagoeWh0cy0WducWkE/0YwL+
A/5TL48wM44GqUWTRxG49aI62kEvPvv/HDrqlgGR5FMEXS0k3yjb6JiiTQh+ZeSW
ep92VA5Bj4eBKohLSbLMAySquBLsQ+sLfsnwZ/ejy9uluADhLyvXP2F+1QZcb+MK
wrbqaDr22Za/U6EeaKMXU0BsUm88auYUOFoDiJwaqwPO+B8l5vFMT3FyI9h+F+GJ
/Q8HAcqNFiGNuVCzZ07Z0PY+EBR4TArH65odZkIX9JaijiDxJNtE1YoT7c74jbP7
k6Ba5DYatydUlwTC4sLmr25FYQh1FcZeJIe+WQ==
-----END CERTIFICATE-----

CN=GLOBAL CHAMBERSIGN ROOT - 2016, O=AC CAMERFIRMA S.A., OID.2.5.4.97=VATES-A82743287, SERIALNUMBER=A82743287, OU=GLOBAL CHAMBERSIGN ROOT - 2016, OU=see current address at www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES

Type	CA/QC
Status	undersupervision
Status starting time	2018-06-07T20:27:38.000Z

Service digital identity (X509)

Version	3
Serial number	3301752398764465683
Signature algorithm	SHA256withRSA
Issuer	CN=GLOBAL CHAMBERSIGN ROOT - 2016, O=AC CAMERFIRMA S.A., OID.2.5.4.97=VATES-A82743287, SERIALNUMBER=A82743287, OU=GLOBAL CHAMBERSIGN ROOT - 2016, OU=see current address at www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES
Valid from	Thu Apr 14 02:50:06 PET 2016
Valid to	Sun Apr 08 02:50:06 PET 2040
Subject	CN=GLOBAL CHAMBERSIGN ROOT - 2016, O=AC CAMERFIRMA S.A., OID.2.5.4.97=VATES-A82743287, SERIALNUMBER=A82743287, OU=GLOBAL CHAMBERSIGN ROOT - 2016, OU=see current address at www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES

Public key	Sun RSA public key, 4096 bits modulus: 850285548181317716069847514845428663677976425444186733370058027201843229271079108792675161809256966232726803252427917340062237657966670027617915568186854741401641272923666868338864221165242144490589352194930367167615470109757643277175659581685712407264904976535479252324932718022612854458509960017957069616636209126355729032867882332806970249728843043014013044144335557084001423588934087518309296807454201349475344874550395885286308096166968866876419404746928420754193835639647356236703708332336338496527055109780991433741766982084286120115881754424031959717332618271322729228238191686648813897487297809146656093450109429229946738890850215108992755461794676349701204047225032782020908740872285945559782805271265310454237546716905573176296543324781659300489720426846078453130186703806233333280531772842595216812443599715781995740050172292706618631074402541386887782325987980435224462329439174922523180952866571669091776951822856553317225976072376538699004286389725812479294937009231104767127839161597841702170681370187136835307509981620176777920027850550309172501571659766623858076199638186627517313449643824444491909802965139933575027010156732808661732276378744574973579661657536262685474601898821313464435123681310247609403306347771341170978121
public exponent: 65537
Subject key identifier	e89bcd7e86629b7a4d8c00973985cf1c7890703a
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	1139a49e8484aaf2d90d985ec4741a65dd5d94e2
SHA256 Thumbprint	c1d80ce474a51128b77e794a98aa2d62a0225da3f419e5c7ed73dfbf660e7109

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=GLOBAL CHAMBERSIGN ROOT - 2016, O=AC CAMERFIRMA S.A., OID.2.5.4.97=VATES-A82743287, SERIALNUMBER=A82743287, OU=GLOBAL CHAMBERSIGN ROOT - 2016, OU=see current
address at www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
850285548181317716069847514845428663677976425444186733370058027201843229271079108792675161809256966232726803252427917340062237657966670027617915568186854741401641272923666868
838864221165242144490589352194930367167615470109757643277175659581685712407264904976535479252324932718022612854458509960017957069616636209126355729032867882332806970249728843043014433414335570840014235889340875183092968074542013494753448745503958852863080961669688668764194047469284207541938356396473562367037083323363384965270551097809914337417669820842861201158817544240319597173326182713227292282381916866488138974872978091466560934501094292299467388908502151089927554617946763497012040472250327820209087408722859455978280527126531045423754671690557317629654332478165930048972042684607845313018670380623333328053177284259521681244359971578199574005017229270661863107440254138688770823259879804352244623294391749225231809528665716690917769518228565533172259760723765386990042863897258124792949370092311047671278391615978417021706813701871368353075099816201767779200278505503091725015765976662385807619963818662751731344964382444449190980296513993357502701015673280866173227637874457497357966165753626268547460189882131346443512368131024760940330634777134117781
 public exponent: 65537
 Validity: [From: Thu Apr 14 02:50:06 PET 2016,
             To: Sun Apr 08 02:50:06 PET 2040]
 Issuer: CN=GLOBAL CHAMBERSIGN ROOT - 2016, O=AC CAMERFIRMA S.A., OID.2.5.4.97=VATES-A82743287, SERIALNUMBER=A82743287, OU=GLOBAL CHAMBERSIGN ROOT - 2016, OU=see current
address at www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES
 SerialNumber: [    2dd22e50 30a65e13]

Certificate Extensions: 3
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: E8 9B CD 7E 86 62 9B 7A   4D 8C 00 97 39 85 CF 1C  .....b.zM...9...
0010: 78 90 70 3A                                        x.p:
]
]

[2]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[3]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 7B FD 2A C3 CB 1B 29 02   10 09 AD EB 2E B3 2B 6D  ..*...).......+m
0010: D9 4B A0 DB 35 98 F5 8F   02 A7 D3 42 0B 43 AB 83  .K..5......B.C..
0020: B5 77 47 88 46 85 DD D1   B6 1E 7D 98 1B 8C 71 BE  .wG.F.........q.
0030: AA C8 F0 EF C6 6A 2D 56   98 52 E8 96 89 FB D5 EA  .....j-V.R......
```

```
0040: 00 DF FE E6 22 CA A7 B9   3E 65 44 75 C3 8A BF 8B  ....">...eDu....
0050: 77 89 C3 6A 57 FA BC C8   E1 10 DE F1 DA 85 27 F1  w..jW.........'.
0060: ED 07 FF D5 C2 42 D4 A2   61 2F DF 88 71 E3 34 E6  .....B..a/..q.4.
0070: 67 64 9B C6 7A 19 EB 39   EF F3 EA 04 A8 74 69 4C  gd..z..9.....tiL
0080: 80 B5 FC AD BD 0D 08 F4   C8 EF 28 27 82 CA DD E8  ..........('....
0090: F3 BA 57 67 A2 EA 29 C1   99 E1 76 66 F9 F6 78 5D  ..Wg..)...vf..x]
00A0: 9C 3E F0 F6 CF A1 19 34   D3 F1 3C 33 A1 CC 82 32  .>.....4..<3...2
00B0: B6 48 E3 83 3E 0F BF 67   95 C1 A2 99 78 42 43 F7  .H..>..g....xBC.
00C0: 03 4D 13 57 6F DD 71 DD   16 F3 FB 79 38 1B 62 9A  .M.Wo.q....y8.b.
00D0: A4 CD 5E 50 DE 11 20 90   8A 22 98 AB DA 46 7A 4C  ..^P.. .."...FzL
00E0: 34 D1 48 DD D9 66 65 62   54 05 D9 74 99 67 74 57  4.H..febT..t.gtW
00F0: B1 3A 2E 18 B0 AE AC 9F   3F 2E EB 1F B2 9C CD 8E  .:......?.......
0100: F8 DB 78 8E D4 06 CF A3   93 31 6B 7F ED 52 72 B7  ..x......1k..Rr.
0110: 8B CF 28 6F C9 F9 54 4F   01 D4 3A 86 E8 2E FA E1  ..(o..TO..:.....
0120: D0 25 84 E3 16 FC 8C 8D   24 E3 64 CC 2A 8C B2 60  .%......$.d.*..`
0130: 53 9F 59 92 45 09 94 5B   A8 10 85 32 CB 77 F2 8E  S.Y.E..[...2.w..
0140: 95 8A 44 72 CF 6E 17 DE   44 BD 0A AE FD 26 B6 3D  ..Dr.n..D....&.=
0150: 79 66 3D 4D BC 7E 32 43   5D DB E0 65 B5 28 69 BA  yf=M..2C]..e.(i.
0160: 7C 9E 32 4A 8F EA 7A B0   3D 16 5D FD 3E FA 1B 04  ..2J..z.=.].>...
0170: F8 10 35 78 CC ED C1 D9   2D BF 6B D2 EF E9 9F C0  ..5x....-.k.....
0180: 5B 8F EA BE 7A D1 31 E7   06 3D AD 84 AB EC 3B F1  [...z.1..=....;.
0190: 12 C7 7F F1 F8 46 2F 09   78 97 C0 27 3D B1 3F 71  .....F/.x..'=.?q
01A0: 23 8B 1A A7 5C E6 16 25   0E 26 4D B9 0E 56 A7 52  #...\..%.&M..V.R
01B0: A4 38 09 AF 49 05 FE 7F   CE 3F C2 FC E6 E4 4A 94  .8..I....?....J.
01C0: 27 E5 53 C4 88 34 EB 02   57 BC CE 8E 2B AD 77 53  '.S..4..W...+.wS
01D0: 72 40 BB 85 16 55 19 2F   83 76 95 A3 76 39 A8 B2  r@...U./.v..v9..
01E0: F4 7D A4 DB 00 42 7A A0   7B 8E 19 06 E4 97 CD 5B  .....Bz........[
01F0: 3D 3A B4 5C C0 69 1F 32   66 BF 08 9F 84 9B 22 65  =:.\.i.2f....."e

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIG2DCCBMCgAwIBAgIILdIuUDCmXhMwDQYJKoZIhvcNAQELBQAwggEIMQswCQYD
VQQGEwJFUzEPMA0GA1UECAwGTUFEUklEMQ8wDQYDVQQHDAZNQURSSUQxOjA4BgNV
BAsMMXNlZSBjdXJyZW50IGFkZHJlc3MgYXQgd3d3LmNhbWVyZmlybWEuY29tL2Fk
ZHJlc3MxJzAlBgNVBAsMHkdMT0JBTCBDSEFNQkVSU0lHTiBST09UIC0gMjAxNjES
MBAGA1UEBRMJQTgyNzQzMjg3MRgwFgYDVQRhDA9WQVRFUy1BODI3NDMyODcxGzAZ
BgNVBAoMEkFDIENBTUVSRklSTUEgUy5BLjEnMCUGA1UEAwweR0xPQkFMIENIQU1C
RVJTSUdOIFJPT1QgLSAyMDE2MB4XDTE2MDQxNDA3NTAwNloXDTQwMDQwODA3NTAw
NlowggEIMQswCQYDVQQGEwJFUzEPMA0GA1UECAwGTUFEUklEMQ8wDQYDVQQHDAZN
QURSSUQxOjA4BgNVBAsMMXNlZSBjdXJyZW50IGFkZHJlc3MgYXQgd3d3LmNhbWVy
ZmlybWEuY29tL2FkZHJlc3MxJzAlBgNVBAsMHkdMT0JBTCBDSEFNQkVSU0lHTiBS
T09UIC0gMjAxNjESMBAGA1UEBRMJQTgyNzQzMjg3MRgwFgYDVQRhDA9WQVRFUy1B
ODI3NDMyODcxGzAZBgNVBAoMEkFDIENBTUVSRklSTUEgUy5BLjEnMCUGA1UEAwwe
R0xPQkFMIENIQU1CRVJTSUdOIFJPT1QgLSAyMDE2MIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEA0GvnniIrU3YVVa9MSsBta/v5hEQFoX1gzgXsnphz+luE
BzH3/z1rx35WBmKlXJaW0/FeWX7rMRy/d1cwVO8exczEsurb5orQ9CiEyLBILSyW
bfsiqDWOvt5wFRD5ZkFGFqBDZD+NSvOAMc+TgH6a26Wvj2ws/Q7vHHncD6JuhFwi
iQ5ELkiolHPsOTKRHOIUvX1l5nL+W+dUdS99DuLGymkuXqIO1eiF3j9rf6WCsEZ9
XZ5xuhS06+3HwhRkDFhuT5U2YTZFYDZmGEuVGj5YrIsmHiXm+pUA+60SnvoSYb4a
3qZ86av/15SJckL8u0UR7D9w/BnEmuqXbqzkOAQ74T8BKHGj4q5DZHgWmQJav9fE
77W31cNYgUGG5LKMAKWImJjrCedYMWgx3u3iSTXz0rNX3MRCn/0879D1KzluYa56
4cd6PW0XMGwCrInWWoScKcCeEI64IDYzyoAraH82dWUV+MPa/3Gi/O2bd9wZ+vHI
tgX05XCSqcjduLAaVVuR3LjlmrUDwK22rvGZe0u1iQ7eZAtkflTup8OKmBnF/DwT
CEU+35/7x32xoII2FD3AYwABZsTk8Jk7HlF4XbkXPFiTFa+o9SUgGY0jPRI8Qusv
XUKO8jCoJVrm+vdPbb4mWPWPf/eK+LNuwxvyMYU2cY79O9bmMDXLJY1liVeoM5UC
AwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQU6JvNfoZim3pNjACX
OYXPHHiQcDowDgYDVR0PAQH/BAQDAgEGMA0GCSqGSIb3DQEBCwUAA4ICAQB7/SrD
yxspAhAJresusytt2Uug2zWY9Y8Cp9NCC0Org7V3R4hGhd3Rth59mBuMcb6qyPDv
xmotVphS6JaJ+9XqAN/+5iLKp7k+ZUR1w4q/i3eJw2pX+rzI4RDe8dqFJ/HtB//V
wkLUomEv34hx4zTmZ2SbxnoZ6znv8+oEqHRpTIC1/K29DQj0yO8oJ4LK3ejzuldn
ouopwZnhdmb59nhdnD7w9s+hGTTT8TwzocyCMrZI44M+D79nlcGimXhCQ/cDTRNX
b91x3Rbz+3k4G2KapM1eUN4RIJCKIpir2kZ6TDTRSN3ZZmViVAXZdJlndFexOi4Y
sK6snz8u6x+ynM2O+Nt4jtQGz6OTMWt/7VJyt4vPKG/J+VRPAdQ6hugu+uHQJYTj
FvyMjSTjZMwqjLJgU59ZkkUJlFuoEIUyy3fyjpWKRHLPbhfeRL0Krv0mtj15Zj1N
vH4yQl3b4GW1KGm6fJ4ySo/qerA9Fl39PvobBPgQNXjM7cHZLb9r0u/pn8Bbj+q+
etEx5wY9rYSr7DvxEsd/8fhGLwl4l8AnPbE/cSOLGqdc5hYlDiZNuQ5Wp1KkOAmv
SQX+f84/wvzm5EqUJ+VTxIg06wJXvM6OK613U3JAu4UWVRkvg3aVo3Y5qLL0faTb
AEJ6oHuOGQbkl81bPTq0XMBpHzJmvwifhJsiZQ==
-----END CERTIFICATE-----
```

CN=AC CAMERFIRMA PERÚ CERTIFICADOS - 2016, O=CAMERFIRMA PERÚ S.A.C., OID.2.5.4.97=NTRPE-20566302447, SERIALNUMBER=20566302447, OU=AC CAMERFIRMA PERÚ CERTIFICADOS - 2016, OU=see current address at www.camerfirma.com.pe/address, L=LIMA, ST=LIMA, C=PE

Type	CA/QC
Status	undersupervision
Status starting time	2017-08-16T15:24:37.000Z

Service digital identity (X509)

Version	3
Serial number	10117976432277337926
Signature algorithm	SHA256withRSA

Issuer	CN=AC CAMERFIRMA PERÚ - 2016, O=AC CAMERFIRMA S.A., OID.2.5.4.97=VATES-A82743287, SERIALNUMBER=A82743287, OU=AC CAMERFIRMA PERÚ - 2016, OU=see current address at https://www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES
Valid from	Tue Oct 11 03:57:05 PET 2016
Valid to	Thu Feb 09 03:57:05 PET 2040
Subject	CN=AC CAMERFIRMA PERÚ CERTIFICADOS - 2016, O=CAMERFIRMA PERÚ S.A.C., OID.2.5.4.97=NTRPE-20566302447, SERIALNUMBER=20566302447, OU=AC CAMERFIRMA PERÚ CERTIFICADOS - 2016, OU=see current address at www.camerfirma.com.pe/address, L=LIMA, ST=LIMA, C=PE
Public key	Sun RSA public key, 4096 bits modulus: 662338133557932095088050121118023035004442212513159638601442264722364823851586277683227362118121325834327139312650466251695846779372856615900044134647016604824853754408671056099205270425954594898365088019396681928072503301359882705091410151778380834520958537994109597599539757209769768601902016055892539115251794753759718968575113982965683166488337534241774398473639812276805876539363347087586948016944965069775950538960645549155410644200938097288915793112866047967822857596336726703358834798286132357760432789016178063026822065472706283112409538646560320320376596541891358293674596649266447473708289297948173244544830396747539038471753345796298803219387129100029382166731999926670418074391353923672781309379052846816668860735728951810446116996748214547533509080413562994395978615714894294940487941672203698388931793258377258430990750363686643894909057275633989303815501761888823424907298086548148333615739348258214788123827534559991456119818285378763912427555024408123392103016063825147911255672442849303798110019288542493979745765968609086448881161995700905809238161733983146758055770206544433828664759571479544934265767024254701897601337195835625748319870706793560253041145444514645171234325627029591709535488686530997600804696976117
public exponent: 65537
Subject key identifier	3a6e6518e756d2e4f32ddda57c726dff30e18627
CRL distribution points	http://crl.camerfirma.com/ac_camerfirma_peru-2016.crl http://crl1.camerfirma.com/ac_camerfirma_peru-2016.crl
Authority key identifier	048201383082013480 14b76a026d2cd9b036b32b6c05aa345e06edb2b99ba1820110a482010c30820108310b300906035504061302455331 0f300d06035504080c064d4144524944310f300d06035504070c064d4144524944313a3038060355040b0c3173656520637572656e74206164647265737320617420777772e63616d65726669726d612e636f6d2f6164726573733127302506035504 0b0c1e474c4f42414c204348414d4245525349474e20524f4f54202d203230313631123010060355040513094138323734333238373118301606035504610c0f56415445532d413832373433323837311b3019060355040a0c1241432043414d45524649524d4120532e412e312730250603550403 0c1e474c4f42414c204348414d4245525349474e20524f4f54202d203230313682082 6f4aa13f0560872
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=0
SHA1 Thumbprint	421239733f9ceabf7a524ad41f9b7c704fb9695c
SHA256 Thumbprint	5b4bfc749a8158dfd4ebf3df20782b0c284928bc40e89728cfaebfca7f85033d

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=AC CAMERFIRMA PERÚ CERTIFICADOS - 2016, O=CAMERFIRMA PERÚ S.A.C., OID.2.5.4.97=NTRPE-20566302447, SERIALNUMBER=20566302447, OU=AC CAMERFIRMA PERÚ CERTIFICADOS - 2016, OU=see current address at www.camerfirma.com.pe/address, L=LIMA, ST=LIMA, C=PE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
662338133557932095088050121118023035004442212513159638601442264722364823851586277683227362118121325834327139312650466251695846779372856615900044134647016604824853754408671056099205270425954594898365088019396681928072503301359882705091410151778380834520958537994109597599539757209769768601902016055892539115251794753759718968575113982965683166488337534241774398473639812276805876539363347087586948016944965069775950538960645549155410644200938097288915793112866047967822857596336726703358834798286132357760432789016178063026822065472706283112409538646560320320376596541891358293674596649266447473708289297948173244544830396747539038471753345796298803219387129100029382166731999926670418074391353923672781309379052846816668860735728951810446116996748214547533509080413562994395978615714894294940487941672203698388931793258377258430990750363686643894909057275633989303815501761888823424907298086548148333615739348258214788123827534559991456119818285378763912427555024408123392103016063825147911255672442849303798110019288542493979745765968609086448881161995700905809238161733983146758055770206544433828664759571479544934265767024254701897601337195835625748319870706793560253041145444514645171234325627029591709535488686530997600804696976117
 public exponent: 65537
 Validity: [From: Tue Oct 11 03:57:05 PET 2016,
```

```
             To: Thu Feb 09 03:57:05 PET 2040]
 Issuer: CN=AC CAMERFIRMA PERÚ - 2016, O=AC CAMERFIRMA S.A., OID.2.5.4.97=VATES-A82743287, SERIALNUMBER=A82743287, OU=AC CAMERFIRMA PERÚ - 2016, OU=see current address at
https://www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES
 SerialNumber: [    8c6a45f5 33aa3746]

Certificate Extensions: 8
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 3A 6E 65 18 E7 56 D2 E4   F3 2D DD A5 7C 72 6D FF  :ne..V...-...rm.
0010: 30 E1 86 27                                        0..'
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: B7 6A 02 6D 2C D9 B0 36   B3 2B 6C 05 AA 34 5E 06  .j.m,..6.+l..4^.
0010: ED B2 B9 9B                                        ....
]

[CN=GLOBAL CHAMBERSIGN ROOT - 2016, O=AC CAMERFIRMA S.A., OID.2.5.4.97=VATES-A82743287, SERIALNUMBER=A82743287, OU=GLOBAL CHAMBERSIGN ROOT - 2016, OU=see current address at
www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES]
SerialNumber: [    26f4aa13 f0560872]
]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.camerfirma.com/ac_camerfirma_peru-2016.crl]
, DistributionPoint:
    [URIName: http://crl1.camerfirma.com/ac_camerfirma_peru-2016.crl]
]]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 1D 68 74 74 70 73 3A   2F 2F 70 6F 6C 69 63 79  ..https://policy
0010: 2E 63 61 6D 65 72 66 69   72 6D 61 2E 63 6F 6D     .camerfirma.com

]]  ]
]

[5]: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
 emailProtection
 clientAuth
]

[6]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[7]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://www.camerfirma.com/certs/ac_camerfirma_peru-2016.crt,
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://ocsp.camerfirma.com]
]

[8]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:0
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 76 3C 67 F7 3E 4B 15 3C   6D 94 7A 63 89 7E A8 06  v<g.>K.<m.zc....
0010: 9F DA F2 63 66 80 4A 8F   E7 4A 84 DA 5C B2 94 16  ...cf.J..J..\...
0020: 92 9E 47 A4 92 DF 30 32   02 EF BB 82 2B BE 1F D3  ..G...02....+...
0030: 39 75 38 25 F4 4A 58 82   B4 71 31 02 22 D2 EE FD  9u8%.JX..q1."...
0040: 25 E8 1D 90 93 AB A8 34   85 17 FD 53 58 69 FD 62  %......4...SXi.b
0050: DD 4E BE F2 DB 45 88 81   B2 AD 23 3B 78 A1 D7 F8  .N...E....#;x...
0060: 36 FA 4E 78 31 B3 71 1E   FE DC 72 30 40 CC 57 A4  6.Nx1.q...r0@.W.
0070: D6 82 E8 D5 0B B3 07 C3   CE 6A 10 40 76 8D 6D 74  .........j.@v.mt
0080: B1 88 AF 0A 73 F8 F4 C8   6B AD E4 F0 F0 72 68 D3  ....s...k....rh.
0090: 8F 62 EB FF EF 9F C9 7D   91 5E EE 5C 91 B3 6F C0  .b.......^.\..o.
00A0: AC 8A 3F 4E C4 1C CA DF   8B 3F D6 FB 3B FB 81 CE  ..?N.....?..;...
00B0: F5 EF 10 DA A6 55 DA 91   E3 4A 04 E8 B0 6E B6 4F  .....U...J...n.O
00C0: 6F B8 41 1C 44 4E F2 E6   07 FA 77 53 2E 41 0A 76  o.A.DN....wS.A.v
00D0: 8F 03 F3 09 3C 3C 82 2D   46 BA 33 BC 78 B0 5A 11  ....<<.-F.3.x.Z.
00E0: 43 94 DF E4 C4 4F 25 90   79 57 AA 08 B2 FB EC 6D  C....O%.yW.....m
00F0: 9F A4 1B B1 A4 DE B3 F1   09 81 67 AD 25 BD C1 5B  ..........g.%..[
0100: EE 7A FE C9 AC F7 96 4B   E1 7E C4 D1 D1 16 8A 7D  .z.....K........
0110: 6F C1 24 70 46 2C D7 44   41 AE C8 91 41 56 CD 36  o.$pF,.DA...AV.6
0120: 1F 0A D7 B0 F6 AD A8 FF   46 FA 0D F5 89 81 E1 9C  ........F.......
```

```
0130: 12 0C 0F C1 B3 9E 1B 52   17 7A A3 AB 06 18 2B 71  .......R.z....+q
0140: BA 10 F6 AE 86 F0 BA 06   A3 18 C2 57 72 DE 04 DB  ...........Wr...
0150: F4 0F 7C A5 7D FA F0 4D   7B 02 B5 C1 9F 40 18 C7  .......M.....@..
0160: A0 79 31 A1 01 74 66 52   64 3C 2B AD 4B E1 0F 46  .y1..tfRd<+.K..F
0170: 84 91 AA FF 87 4B 19 A8   0F 3E AB 13 3D 2F 45 BD  .....K...>..=/E.
0180: 68 33 2E D4 A5 E0 A9 BA   10 78 F7 6F 8B 6C 1A 89  h3.......x.o.l..
0190: 31 2B 1E C9 B7 C8 C7 E3   2D 15 8B 28 30 71 A5 CC  1+......-..(0q..
01A0: 20 C4 E4 C6 36 51 6D E3   4A DC EC DD 6C 6B 5A 3F   ...6Qm.J...lkZ?
01B0: DC 47 80 5C EC E6 63 FE   AE B3 16 66 8F C1 BD 36  .G.\..c....f...6
01C0: 2E EE 49 DE B3 08 94 9E   11 78 E2 E1 E8 1C DB 89  ..I......x......
01D0: BC FA DC 6C D7 9C 03 B5   5F DB BB 03 53 C3 2D A9  ...l...._...S.-.
01E0: C4 19 6F EA AC D0 BD B4   1F 51 65 2F C3 68 CF 56  ..o......Qe/.h.V
01F0: E1 B9 41 AB 42 56 8E 97   74 58 36 21 46 72 B5 B7  ..A.BV..tX6!Fr..

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIJpjCCB46gAwIBAgIJAIxqRfUzqjdGMA0GCSqGSIb3DQEBCwUAMIIBCDELMAkG
A1UEBhMCRVMxDzANBgNVBAgMBk1BRFJJRDEPMA0GA1UEBwwGTUFEUklEMUIwQAYD
VQQLDDlzZWUgY3VycmVudCBhZGRyZXNzIGF0IGh0dHBzOi8vd3d3LmNhbWVyZmly
bWEuY29tL2FkZHJlc3MxIzAhBgNVBAsMGkFDIENBTUVSRklSTUEgUEVSw5ogLSAy
MDE2MRIwEAYDVQQFEwlBODI3NDMyODcxGDAWBgNVBGEMD1ZBVEVTLUE4Mjc0MzI4
NzEbMBkGA1UECgwSQUMgQ0FNRVJGSVJNQSBTLkEuMSMwIQYDVQQDDBpBQyBDQU1F
UkZJUk1BIFBFUsOaIC0gMjAxNjAeFw0xNjEwMTEwODU3MDVaFw00MDAyMDkwODU3
MDVaMIIBIjELMAkGA1UEBhMCUEUxDTALBgNVBAgMBExJTUExDTALBgNVBAcMBExJ
TUExPTA7BgNVBAsMNHNlZSBjdXJyZW50IGFkZHJlc3MgYXQgd3d3LmNhbWVyZmly
bWEuY29tLnBlL2FkZHJlc3MxMDAuBgNVBAsMJ0FDIENBTUVSRklSTUEgUEVSw5og
Q0VSVElGSUNBRE9TIC0gMjAxNjEUMBIGA1UEBRMLMjA1NjYzMDI0NDcxGjAYBgNV
BGEMEU5UUlBFLTIwNTY2MzAyNDQ3MSAwHgYDVQQKDBdDQU1FUkZJUk1BIFBFUsOa
IFMuQS5DLjEwMC4GA1UEAwwnQUMgQ0FNRVJGSVJNQSBQRVLDmiBDRVJUSUZJQ0FE
T1MgLSAyMDE2MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAoloY0FaZ
Dx6DvYYP+oYIuvrw2bhNMrErr8ZjLC2WyYbKOmliOutF2/vPJDfwP5NKZ0bbCX8v
tcicr/tW26scqgDW/2V/V9pYLajmls1+6Fec7+omKzJ83e9hF0SSVwOlaR/ds0Vt
blpmO90RuxDWdokbPaE/v5cwp5M7ChqEmBakW4a68NQVIOokmds+U94tABgKawl/
Ji1Xgcq7DabO99gvPkasFE2cU1oJnUyjhqV2o44vuMO6OAs3hGdxCGBbsLiNRByc
05wH6COWHyewPHtFHT4p+3nAi4Rf2SOY6O1cvhOTRpIdK0dpSKf8kXLijy7FJvRD
a1PRJpbCIztKuRYkYnsaxYofLgACrHymHCV7bX0M0SbZuq02YpRu9Zog9JfR2u28
XEqCyOQs3T3l+fxBXJ0qRS/ajnpu3zk3wAYSqaGF6xYAopMRw77u+fjtHFzqZiGK
NQ9twAIafJzb/xBHyNA2udOzr2HhSqmgFOyX48SflDXqpk/rR6lcmPzFEh7qlSBk
a2CZKgMXpQKBY0Ii/05HoCxLR7c26Qyw/IqlmYJSRQ7cggzn8DtA9k7ey+CIKj7+
KPBJ2d6EhRSk/1zuksrLLW6v1zOaGqCbHOwzF3p8puwV9a/kn07tdpB7A0ARTnP0
k0CTbZj9nSmjPAB39Lw6pbt0S+pwuVu9JEsCAwEAAaOCAvMwggLvMBIGA1UdEwEB
/wQIMAYBAf8CAQAwHQYDVR0OBBYEFDpuZRjnVtLk8y3dpXxybf8w4YYnMIIBQQYD
VR0jBIIBODCCATSAFLdqAm0s2bA2sytsBao0XgbtsrmboYIBEKSCAQwwggEIMQsw
CQYDVQQGEwJFUzEPMA0GA1UECAwGTUFEUklEMQ8wDQYDVQQHDAZNQURSSUQxOjA4
BgNVBAsMMXNlZSBjdXJyZW50IGFkZHJlc3MgYXQgd3d3LmNhbWVyZmlybWEuY29t
L2FkZHJlc3MxJzAlBgNVBAsMHkdMT0JBTCBDSEFNQkVSU0lHTiBST09UIC0gMjAx
NjESMBAGA1UEBRMJQTgyNzQzMjg3MRgwFgYDVQRhDA9WQVRFUy1BODI3NDMyODcx
GzAZBgNVBAoMEkFDIENBTUVSRklSTUEgUy5BLjEnMCUGA1UEAwweR0xPQkFMIENI
QU1CRVJTSUdOIFJPT1QgLSAyMDE2gggm9KoT8FYIcjB/BggrBgEFBQcBAQRzMHEw
RwYIKwYBBQUHMAKGO2h0dHA6Ly93d3cuY2FtZXJmaXJtYS5jb20vY2VydHMvYWNf
Y2FtZXJmaXJtYV9wZXJ1LTIwMTYuY3J0MCYGCCsGAQUFBzABhhpodHRwOi8vb2Nz
cC5jYW1lcmZpcm1hLmNvbTAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0lBBYwFAYIKwYB
BQUHAwQGCCsGAQUFBwMCMD4GA1UdIAQ3MDUwMwYEVR0gADArMCkGCCsGAQUFBwIB
Fh1odHRwczovL3BvbGljeS5jYW1lcmZpcm1hLmNvbTCBhAYDVR0fBH0wezA7oDmg
N4Y1aHR0cDovL2NybC5jYW1lcmZpcm1hLmNvbS9hY19jYW1lcmZpcm1hX3BlcnUt
MjAxNi5jcmwwPKA6oDiGNmh0dHA6Ly9jcmwxLmNhbWVyZmlybWEuY29tL2FjX2Nh
bWVyZmlybWFfcGVydS0yMDE2LmNybDANBgkqhkiG9w0BAQsFAAOCAgEAdjxn9z5L
FTxtlHpjiX6oBp/a8mNmgEqP50qE2lyylBaSnkekkt8wMgLvu4Irvh/TOXU4JfRK
WIK0cTECItLu/SXoHZCTq6g0hRf9U1hp/WLdTr7y20WIgbKtIzt4odf4NvpOeDGz
cR7+3HIwQMxXpNaC6NULswfDzmoQQHaNbXSxiK8Kc/j0yGut5PDwcmjTj2Lr/++f
yX2RXu5ckbNvwKyKP07EHMrfiz/W+zv7gc717xDaplXakeNKBOiwbrZPb7hBHERO
8uYH+ndTLkEKdo8D8wk8PIItRrozvHiwWhFDlN/kxE8lkHlXqgiy++xtn6QbsaTe
s/EJgWetJb3BW+56/sms95ZL4X7E0dEWin1vwSRwRizXREGuyJFBVs02HwrXsPat
qP9G+g31iYHhnBIMD8GznhtSF3qjqwYYK3G6EPauhvC6BqMYwldy3gTb9A98pX36
8E17ArXBn0AYx6B5MaEBdGZSZDwrrUvhD0aEkar/h0sZqA8+qxM9L0W9aDMu1KXg
qboQePdvi2waiTErHsm3yMfjLRWLKDBxpcwgxOTGNlFt40rc7N1sa1o/3EeAXOzm
Y/6usxZmj8G9Ni7uSd6zCJSeEXji4egc24m8+txs15wDtV/buwNTwy2pxBlv6qzQ
vbQfUWUvw2jPVuG5QatCVo6XdFg2IUZytbc=
-----END CERTIFICATE-----
```

CN=RACER, O=AC Camerfirma SA, SERIALNUMBER=A82743287, L=Madrid (see current address at www.camerfirma.com/address), EMAILADDRESS=caracer@camerfirma.com, C=ES

Type	CA/QC
Status	undersupervision
Status starting time	2016-08-19T17:01:59.000Z

Service digital identity (X509)

Version	3
Serial number	1
Signature algorithm	SHA1withRSA
Issuer	CN=AC Camerfirma, O=AC Camerfirma SA, L=Madrid (see current address at www.camerfirma.com/address), SERIALNUMBER=A82743287, EMAILADDRESS=ac_camerfirma@camerfirma.com, C=ES

Valid from	Thu Dec 04 12:26:41 PET 2003
Valid to	Mon Dec 04 12:26:41 PET 2023
Subject	CN=RACER, O=AC Camerfirma SA, SERIALNUMBER=A82743287, L=Madrid (see current address at www.camerfirma.com/address), EMAILADDRESS=caracer@camerfirma.com, C=ES
Public key	Sun RSA public key, 2047 bits modulus: 15565749306815017290572910947913251485658394816871391150519718224752092 68062858659048834366990073975612048779674255897336661658525739042980763 96962976353445306837806698655728708292472338989005934885983563402612261 83154176055624147148998129032292188368010388116242523363115157164130163 43176123522599137408629429484799643338581635645863414670014191985157325 86393279366017314962554998063803944333549469215466510981194042445206770 51782788353164428264902673736604837858615396404885079624196345816148593 32812610429024079594383730463692359849025706062513980948184969165681176 27866845993860866200943565157504139865925210316 19 public exponent: 3
Subject key identifier	bebc08d42eba004c80dc2667b4a5d8ddc34a1af9
CRL distribution points	http://crl.camerfirma.com/racer.crl
Authority key identifier	0481a030819d801470c195fa5da516be62e8a47de3d4645fc4e13e9da18181a47f307d310 b30090603550406130245553127302506035504 0a131e41432043616d65726669726d61 20534120434946204138323734333238373123302106035504 0b131a687474703a2f2f77 77772e6368616d6265727369676e2e6f72673120301e06035504031317476c6f62616c20 4368616d6265727369676e20526f6f74820102
Key usage	digitalSignature keyCertSign cRLSign
Basic constraints	CA=true; PathLen=10
SHA1 Thumbprint	f82701f8e04770f3448c19070f9b2158b16621a0
SHA256 Thumbprint	f1712177935dba40bdbd99c5f753319cf6293549b7284741e43916ad3bfbdd75

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=RACER, O=AC Camerfirma SA, SERIALNUMBER=A82743287, L=Madrid (see current address at www.camerfirma.com/address), EMAILADDRESS=caracer@camerfirma.com, C=ES
 Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

 Key:  Sun RSA public key, 2047 bits
 modulus:
15565749306815017290572910947913251485658394816871391150519718224752092680628586590488343669900739756120487796742558973366616585257390429807639696297635344530683780669865572870829247233898900593488598356340261226183154176055624147148998129032292188368010388116242523363115157164130163431761235225991374086294294847996433385816356458634146700141919851573258639327936601731496255499806380394433354946921546651098119404244520677051782788353164428264902673736604837858615396404885079624196345816148593328126104290240795943837304636923598490257060625139809481849691656811762786684599386086620094356515750413986592521031619
 public exponent: 3
 Validity: [From: Thu Dec 04 12:26:41 PET 2003,
             To: Mon Dec 04 12:26:41 PET 2023]
 Issuer: CN=AC Camerfirma, O=AC Camerfirma SA, L=Madrid (see current address at www.camerfirma.com/address), SERIALNUMBER=A82743287,
EMAILADDRESS=ac_camerfirma@camerfirma.com, C=ES
 SerialNumber: [    01]

Certificate Extensions: 9
[1]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://www.camerfirma.com/certs/ac_camerfirma.crt]
]

[2]: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
 RFC822Name: caracer@camerfirma.com
]

[3]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 70 C1 95 FA 5D A5 16 BE   62 E8 A4 7D E3 D4 64 5F  p...]...b.....d_
0010: C4 E1 3E 9D                                        ..>.
]

[CN=Global Chambersign Root, OU=http://www.chambersign.org, O=AC Camerfirma SA CIF A82743287, C=EU]
SerialNumber: [    02]
]

[4]: ObjectId: 2.5.29.14 Criticality=false
```

```
SubjectKeyIdentifier [
KeyIdentifier [
0000: BE BC 08 D4 2E BA 00 4C   80 DC 26 67 B4 A5 D8 DD  .......L..&g....
0010: C3 4A 1A F9                                        .J..
]
]

[5]: ObjectId: 2.5.29.18 Criticality=false
IssuerAlternativeName [
 RFC822Name: ac_camerfirma@camerfirma.com
]

[6]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [1.3.6.1.4.1.17326.10.8.1]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 28 68 74 74 70 3A 2F   2F 63 70 73 2E 63 61 6D  .(http://cps.cam
0010: 65 72 66 69 72 6D 61 2E   63 6F 6D 2F 63 70 73 2F  erfirma.com/cps/
0020: 72 61 63 65 72 2E 68 74   6D 6C                    racer.html

]]  ]
]

[7]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:10
]

[8]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.camerfirma.com/racer.crl]
]]

[9]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 DigitalSignature
 Key_CertSign
 Crl_Sign
]

]
 Algorithm: [SHA1withRSA]
 Signature:
0000: 54 FA 8E 00 B0 F1 97 61   7C AE 0B BA EC E7 2A A2  T......a......*.
0010: 63 17 47 76 8F 23 21 44   E2 61 5E 28 EC D5 A5 01  c.Gv.#!D.a^(....
0020: 6C 45 1C E4 96 CD DC D5   90 D3 19 89 55 87 D5 E7  lE..........U...
0030: 2F 80 08 04 9F D4 D6 E9   11 90 6B 88 64 72 18 51  /.........k.dr.Q
0040: 68 8D 00 35 9D D0 72 26   3D BE 47 CE 08 A9 D1 1F  h..5..r&=.G.....
0050: 5D 35 73 F6 4A B4 A8 E1   DD A2 07 B8 2A 47 CE 97  ]5s.J.......*G..
0060: D6 DD DB 8D D7 F5 E7 63   EE 0A 6F ED 13 AB 25 99  .......c..o...%.
0070: 1D 77 56 A2 A6 8D 27 75   B1 8C 53 34 02 9E 3E ED  .wV...'u..S4..>.
0080: C8 60 36 60 18 B9 CD 15   DD EA 37 64 1B 3D 6A BA  .`6`......7d.=j.
0090: F5 9F F5 AA 5F BB 2F B6   B5 E5 35 DC 04 D4 17 B1  ...._./...5.....
00A0: F4 04 38 B1 B1 E6 2F 59   78 D0 D5 9A 94 87 27 AB  ..8.../Yx.....'.
00B0: 30 1C ED C6 AA 5D A7 FE   A3 6E 34 78 1B C3 BF 90  0....]...n4x....
00C0: 65 F6 47 6A BC B6 02 B8   0C 09 4D 92 9A 90 A6 A7  e.Gj......M.....
00D0: 26 E4 B6 BB 8A C0 66 DE   95 01 D8 0B 6A 09 6A F4  &.....f.....j.j.
00E0: C7 A0 B7 79 19 E1 C8 E0   68 AF 3C 81 3D 73 18 73  ...y....h.<.=s.s
00F0: 7F C5 E3 65 71 02 28 BE   78 6B FE 28 F4 84 81 70  ...eq.(.xk.(...p

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGDzCCBPegAwIBAgIBATANBgkqhkiG9w0BAQUFADCBxjELMAkGA1UEBhMCRVMx
KzApBgkqhkiG9w0BCQEWHGFjX2NhbWVyZmlybWFAY2FtZXJmaXJtYS5jb20xEjAQ
BgNVBAUTCUE4Mjc0MzI4NzFDMEEGA1UEBxM6TWFkcmlkIChzZWUgY3VycmVudCBh
ZGRyZXNzIGF0IHd3dy5jYW1lcmZpcm1hLmNvbS9hZGRyZXNzKTEZMBcGA1UEChMQ
QUMgQ2FtZXJmaXJtYSBTQTEWMBQGA1UEAxMNQUMgQ2FtZXJmaXJtYTAeFw0wMzEy
MDQxNzI2NDFaFw0yMzEyMDQxNzI2NDFaMIG4MQswCQYDVQQGEwJFUzElMCMGCSqG
SIb3DQEJARYWY2FyYWNlckBjYW1lcmZpcm1hLmNvbTFDMEEGA1UEBxM6TWFkcmlk
IChzZWUgY3VycmVudCBhZGRyZXNzIGF0IHd3dy5jYW1lcmZpcm1hLmNvbS9hZGRy
ZXNzKTESMBAGA1UEBRMJQTgyNzQzMjg3MRkwFwYDVQQKExBBQyBDYW1lcmZpcm1h
IFNBMQ4wDAYDVQQDEwVSQUNFUjCCAR8wDQYJKoZIhvcNAQEBBQADggEMADCCAQcC
ggEAe03yy1HZxgtdg1b2NocXqtM73x6992kg9feecE3t36NAdYmy+oh6MKrT3CIQ
RiHLm+/RyyudD6o0D0LNeGrRYpcFw7zEOYX/mMGTIXKLPku7BdoCvgyx4amyBigZ
V6AjGn4+xIzQy5ljOyVlnfFfI49awkfX0+BNv5qWKpshg+WnFOW1Gd0MJXMH6uNs
u2/HdqSgsvUQ1dQNelKxz+EbTfiuw+HwgQbpf/nse4oGv0cq0pA85gdEoO+fLOwR
Z8DOfAaVYATnqfTvYexwYYcQ7NWDxCX05iVs51rbt5QrwIq/St7L/6xQd++0mlfA
JoC7TF5Casqh2uS5KSMgI9WPwwIBA6OCAhUwggIRMBIGA1UdEwEB/wQIMAYBAf8C
AQowNAYDVR0fBC0wKzApoCegJYYjaHR0cDovL2NybC5jYW1lcmZpcm1hLmNvbS9y
YWNlci5jcmwwHQYDVR0OBBYEFL68CNQuugBMgNwmZ7Sl2N3DShr5MIGoBgNVHSME
gaAwgZ2AFHDBlfpdpRa+YuikfePUZF/E4T6doYGBpH8wfTELMAkGA1UEBhMCRVUx
JzAlBgNVBAoTHkFDIENhbWVyZmlybWEgU0EgQ0lGIEE4Mjc0MzI4NzEjMCEGA1UE
CxMaaHR0cDovL3d3dy5jaGFtYmVyc2lnbi5vcmcxIDAeBgNVBAMTF0dsb2JhbCBD
aGFtYmVyc2lnbiBSb290ggECME0GCCsGAQUFBwEBBEEwPzA9BggrBgEFBQcwAoYx
aHR0cDovL3d3dy5jYW1lcmZpcm1hLmNvbS9jZXJ0cy9hY19jYW1lcmZpcm1hLmNy
dDAOBgNVHQ8BAf8EBAMCAYYwIQYDVR0RBBowGIEWY2FyYWNlckBjYW1lcmZpcm1h
LmNvbTAnBgNVHRIEIDAegRxhY19jYW1lcmZpcm1hQGNhbWVyZmlybWEuY29tMFAG
A1UdIARJMEcwRQYLKwYBBAGBhy4KCAEwNjA0BggrBgEFBQcCARYoaHR0cDovL2Nw
cy5jYW1lcmZpcm1hLmNvbS9jcHMvcmFjZXIuaHRtbDANBgkqhkiG9w0BAQUFAAOC
```

AQEAVPqOALDxl2F8rgu67OcqomMXR3aPIyFE4mFeKOzVpQFsRRzkls3c1ZDTGYlV
h9XnL4AIBJ/U1ukRkGuIZHIYUWiNADWd0HImPb5Hzgip0R9dNXP2SrSo4d2iB7gq
R86X1t3bjdf152PuCm/tE6slmR13VqKmjSd1sYxTNAKePu3IYDZgGLnNFd3qN2Qb
PWq69Z/1ql+7L7a15TXcBNQXsfQEOLGx5i9ZeNDVmpSHJ6swHO3Gql2n/qNuNHgb
w7+QZfZHary2ArgMCU2SmpCmpybktruKwGbelQHYC2oJavTHoLd5GeHI4GivPIE9
cxhzf8XjZXECKL54a/4o9ISBcA==
-----END CERTIFICATE-----

Certificate Service Provider Name (en): ANF AC ENTIDAD DE CERTIFICACION PERU S.A.C

Trade name (en)	ANF AC ENTIDAD DE CERTIFICACION PERU S.A.C
Information URI (en)	HTTP://WWW.ANF.PE
Service provider street address (es)	AV. AREQUIPA 2618 OF. 402 – SAN ISIDRO
Service provider street address (en)	AV. AREQUIPA 2618 OF. 402 – SAN ISIDRO
Service provider postal code (es)	LIMA 27
Service provider postal code (en)	LIMA 27
Service provider locality (es)	LIMA
Service provider locality (en)	LIMA
Service provider state (es)	LIMA
Service provider state (en)	LIMA
Service provider country (es)	PE
Service provider country (en)	PE

O=ANF Autoridad de Certificacion, OU=ANF Clase 1 CA, C=ES, CN=ANF Global Root CA, SERIALNUMBER=G63287510

Type	CA/QC
Status	undersupervision
Status starting time	2017-05-18T14:37:49.000Z

Service digital identity (X509)

Version	3
Serial number	100369942780184400
Signature algorithm	SHA256withRSA
Issuer	O=ANF Autoridad de Certificacion, OU=ANF Clase 1 CA, C=ES, CN=ANF Global Root CA, SERIALNUMBER=G63287510
Valid from	Fri May 20 09:08:40 PET 2016
Valid to	Thu May 15 09:08:40 PET 2036
Subject	O=ANF Autoridad de Certificacion, OU=ANF Clase 1 CA, C=ES, CN=ANF Global Root CA, SERIALNUMBER=G63287510

Public key	Sun RSA public key, 4096 bits modulus: 812840161774929372023202320254361596370819940266063187111270702412539050408446136434913399323723803615251896261271544542881579361314638084062084365494748422357768833502551510424656389288186586276729321927953655318759960476792490398293700392904112577326137518314833351094324711025952389317060061018587766619892435959953508187711090600912688356119386538643111334496896649294428677295224535970801613034488405280873669718417591648468431928332660103085811501195086662786618900268175126553015636724393939715471614747459402118748830704155163500155642854228499704923621912620547914933283316837982492933854289003827178253037038884563510148033413474800878886576283262414846606368281581471663887502368178278952384203436764566215252684197747938783117508378328949847013235654637439119771230838579516615677090578017643657303668553817055455424584495441169117087649478738171993921649801111234232925139137446675796845722453597080161303448840528087366971841759164846843192833266010308581150119508666278661890026817512655301563672439393971547161474745940211877883070415516350015564285422849970492362191262054791493328331683798249293385428900382717825303703888456351014803341347480878886576283262414846606368281581471663887502368178278952384203436764521525268419774793878311750837832894984701323565463743911977123083857951661567709057801764365730366855381705545542458449544116911708764947873817199392164980211123423292513913744667579684125663618594923814871137225401634432613901431934131968198214062046647827712560273526591040983745668010900391190760312860735946806991841638115636577630509406264370541940480567269692368815960014424921548850598813298416532953348679466070087134275832261331167545550763021100300796527704495008325428571202646745576071634116071969511066445575011 public exponent: 65537
Subject key identifier	87fa9edf527675ec494a206f5b70968f9defbb17
Authority key identifier	04183016801487fa9edf527675ec494a206f5b70968f9defbb17
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	fc9843cc9922615001a17374ce8a3d79580fea51
SHA256 Thumbprint	e0afbd2c0ee95a68cd9a3c590b2d3fe07c0a6d0be796ae5291e424d47792178e

The decoded certificate:

```
[
[
 Version: V3
 Subject: O=ANF Autoridad de Certificacion, OU=ANF Clase 1 CA, C=ES, CN=ANF Global Root CA, SERIALNUMBER=G63287510
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
812840161774929372023202320254361596370819940266063187111270702412539050408446136434913399323723803615251896261271544542881579361314638084062084365494748422357768833502551514245656389288186586276729321927953655318759960476792490398293700392904112577326137518314833351094324711025952389317060061018587766619892435959953508187711090600912688356119386538643111334496896649294428677295224535970801613034488405280873669718417591648468431928332660103085811501195086662786618900268175126553015636724393939715471614747459402118748830704155163500155642854228499704923621912620547914933283316837982492933854289003827178253037038884563510148033413474800878886576283262414846606368281581471663887502368178278952384203436764566215252684197747938783117508378328949847013235654637439119771230838579516615677090578017643657303668553817055455424584495441169117087649478738171993921649801111234232925139137446675796845722453597080161303448840528087366971841759164846843192833266010308581150119508666278661890026817512655301563672439393971547161474745940211877883070415516350015564285422849970492362191262054791493328331683798249293385428900382717825303703888456351014803341347480087888657628326241484660636828158147166388750236817827895238420343676452152526841977479387831175083783289498470132356546374391197712308385795166156770905780176436573036685538170554554245844954411691170876494787381719939216498021112342329251391374466757968412566361859492381487113722540163443261390143193413196819821406204664782771256027352659104098374566801900391190760312860735946806991841638115636577630509406264370541940480567269692368815960014424921548850598813298416532953348679466070087134275832261331167545550763021100300796527704495008325428571202646745576071634116071969511066445575011
 public exponent: 65537
 Validity: [From: Fri May 20 09:08:40 PET 2016,
             To: Thu May 15 09:08:40 PET 2036]
 Issuer: O=ANF Autoridad de Certificacion, OU=ANF Clase 1 CA, C=ES, CN=ANF Global Root CA, SERIALNUMBER=G63287510
 SerialNumber: [    016495ee 618a0750]

Certificate Extensions: 4
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 87 FA 9E DF 52 76 75 EC   49 4A 20 6F 5B 70 96 8F  ....Rvu.IJ o[p..
0010: 9D EF BB 17                                        ....
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 87 FA 9E DF 52 76 75 EC   49 4A 20 6F 5B 70 96 8F  ....Rvu.IJ o[p..
0010: 9D EF BB 17                                        ....
]

]

[3]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[4]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
```

```
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 85 68 C0 31 82 70 F2 FA   39 DE 1F 0E 86 51 6A 72  .h.1.p..9....Qjr
0010: 95 E8 D7 6E CF A3 C6 BA   55 C7 EF A9 0C 54 55 96  ...n....U....TU.
0020: 4F D9 E6 13 44 57 D7 5A   50 9C 03 6B 5C B1 A6 73  O...DW.ZP..k\..s
0030: 3F 9B 1F 6D C4 FD 81 57   3C 89 4F 5D DC D6 2E 80  ?..m...W<.O]....
0040: 5F 33 29 B1 24 06 2D DB   62 0C 3C 5B E7 4E 38 E8  _3).$.-.b.<[.N8.
0050: 3F E0 B7 BD 40 B7 1F FF   3C 96 B1 A5 6C AC FA E8  ?...@...<...l...
0060: 30 9E 49 C4 66 F1 BB CD   85 01 86 4B D7 A8 87 33  0.I.f......K...3
0070: A5 F8 01 68 EB 19 E5 CD   B2 AE C5 47 13 A5 0A 5E  ...h.......G...^
0080: 5E FB D0 85 AF 98 B0 01   7B 2E 91 DA 9E D0 66 57  ^.............fW
0090: 44 7F 51 0D E8 05 8B AD   41 11 AD B2 5E C0 69 DA  D.Q.....A...^.i.
00A0: 40 59 1A 25 5C 47 A6 B9   F7 92 D1 53 56 1B 14 68  @Y.%\G.....SV..h
00B0: 7B 5A 60 3F 7C 9C B5 8F   E1 80 DD 4A 9B B4 B5 21  .Z`?.......J...!
00C0: C3 65 D8 31 DB 91 94 FE   1F 16 6A B1 92 F1 D5 24  .e.1......j....$
00D0: 14 B9 F6 D2 75 D0 AA 0A   7B F1 70 C5 22 02 3B 6C  ....u.....p.".;l
00E0: 7F 48 51 9E AB 36 02 BA   52 F6 1E 9D 0D 80 98 FB  .HQ..6..R.......
00F0: EB 5E C3 9B 2E 51 5F A1   37 81 AE 0A 0F E9 5F A8  .^...Q_.7....._.
0100: B8 AF DC 5B AC 6B F8 9E   3D 39 03 C9 15 A3 E3 8E  ...[.k..=9......
0110: 11 11 E6 2A 95 F1 AA 76   28 73 E7 31 D7 A7 E7 E7  ...*...v(s.1....
0120: 88 56 07 91 6A 2F F5 F4   E7 1A 3E 5B D2 FC BA 9B  .V..j/....>[....
0130: 83 8A 6A 5F E8 DB 63 1C   07 69 38 26 65 AB 0A 74  ..j_..c..i8&e..t
0140: C5 92 5C 44 07 18 AA 0D   30 0E 5E F8 07 34 E6 1F  ..\D....0.^..4..
0150: 53 D6 06 B8 FA 7F E6 40   C6 03 60 BE DE 00 F3 D9  S......@..`.....
0160: 66 50 93 FF 90 15 D6 7A   22 9B 8C 74 71 C1 0A 74  fP.....z"..tq..t
0170: 23 CC 09 45 62 8B E2 33   18 4A 7E F5 18 32 84 E4  #..Eb..3.J...2..
0180: 5B CD 30 EA 22 82 F9 B4   E7 FA D2 7F F6 65 60 FC  [.0."........e`.
0190: 77 EA 0F 3F D1 4D B6 37   FD 02 4C 20 2C 73 8B 0A  w..?.M.7..L ,s..
01A0: F0 68 EA 17 8B 8C 88 69   68 FD E1 20 AC AE 1A 29  .h.....ih.. ...)
01B0: 0D 81 B8 4B 83 13 DE F7   0A 40 3F AA D8 34 90 7D  ...K.....@?..4..
01C0: 4C 26 60 6B 6E A3 C3 66   6E 1C 04 C7 CB 4C 6B D6  L&`kn..fn....Lk.
01D0: 97 5A F4 97 9F 69 98 48   C4 A7 9D FC 0C 5E AB AC  .Z...i.H.....^..
01E0: B9 CF A3 F8 0A 81 91 73   65 D4 B1 D6 7E F2 A1 49  .......se.....I
01F0: 1C E9 15 EC 87 2A B1 99   B5 FE D0 94 F2 CB 4D D2  .....*.......M.

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIF5zCCA8+gAwIBAgIIAWSV7mGKB1AwDQYJKoZIhvcNAQELBQAwgYAxEjAQBgNV
BAUTCUc2MzI4NzUxMDEbMBkGA1UEAwwSQU5GIEdsb2JhbCBSb290IENBMQswCQYD
VQQGEwJFUzEXMBUGA1UECwwOQU5GIENsYXNlIDEgQ0ExJzAlBgNVBAoMHkFORiBB
dXRvcmlkYWQgZGUgQ2VydGlmaWNhY2lvbjAeFw0xNjA1MjAxNDA4NDBaFw0zNjA1
MTUxNDA4NDBaMIGAMRIwEAYDVQQFEwlHNjMyODc1MTAxGzAZBgNVBAMMEkFORiBH
bG9iYWwgUm9vdCBDQTELMAkGA1UEBhMCRVMxFzAVBgNVBAsMDkFORiBDbGFzZSAx
IENBMScwJQYDVQQKDB5BTkYgQXV0b3JpZGFkIGRlIENlcnRpZmljYWNpb24wggIi
MA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDHPi9xy4wynbcUbWjorVUgQKeU
AVh937J7P37XmsfHZLOBZKIIlhhCtRwnDlg7x+BUvtJOTkIbEGMujDygUQ2s3HDY
r5I41hTyM2Pl0cq2EuSGEbPIHb3dEX8NAguFexM0jqNjrreN3hM2/+TOkAxSdDJP
2aMurlySC5zwl47KZLHtcVrkZnkDa0o5iN24hJT4vBDT4t2q9khQ+qb1D8KgCOb0
2r1PxWXu3vfd6Ha2mkdB97iGuEh5gO2n4yOmFS5goFlVA2UdPbbhJsb8oKVKDd+Y
dCKGQDCkQyG4AjmCYiNm3UPG/qtftTH5cWri67DlLtm6fyUFOMmO6NSh0RtR745p
L8GyWJUanyq/Q4bFHQB21E+WtTsCaqjGaoFcrBunMypmCd+jUZXl27TYENRFbrwN
dAh7m2UztcIyb+SgVJFyfvVsBQNvnp7GPimVxXZNc4VpxEXObRuPWQN1oZN/90Pc
ZVqTia/SHzEyTryLckhiLG3jZiaFZ7pTZ5I9wti9Pn+4kOHvE3Y/4nEnUo4mTxPX
9pOlinF+VCiybtV2u1KSlc+YaIM7VmuyndDZCJRXm3v0/qTE7t5A5fArZl9lvibi
gMbWB8fpD+c1GpGHEo8NRY0lkaM+DkIqQoaziIsz3IKJrfdKaq9bQMSlIfameKBZ
8fNYTBZrH9KZAIhzYwIDAQABo2MwYTAdBgNVHQ4EFgQUh/qe31J2dexJSiBvW3CW
j53vuxcwHwYDVR0jBBgwFoAUh/qe31J2dexJSiBvW3CWj53vuxcwDwYDVR0TAQH/
BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQELBQADggIBAIVowDGC
cPL6Od4fDoZRanKV6Nduz6PGulXH76kMVFWWT9nmE0RX11pQnANrXLGmcz+bH23E
/YFXPIlPXdzWLoBfMymxJAYt22IMPFvnTjjoP+C3vUC3H/88lrGlbKz66DCeScRm
8bvNhQGGS9eohzOl+AFo6xnlzbKuxUcTpQpeXvvQha+YsAF7LpHantBmV0R/UQ3o
BYutQRGtsl7AadpAWRolXEemufeS0VNWGxRoe1pgP3yctY/hgN1Km7S1IcNl2DHb
kZT+HxZqsZLx1SQUufbSddCqCnvxcMUiAjtsf0hRnqs2ArpS9h6dDYCY++tew5su
UV+hN4GuCg/pX6i4r9xbrGv4nj05A8kVo+OOERHmKpXxqnYoc+cx16fn54hWB5Fq
L/X05xo+W9L8upuDimpf6NtjHAdpOCZlqwp0xZJcRAcYqg0wDl74BzTmH1PWBrj6
f+ZAxgNgvt4A89lmUJP/kBXWeiKbjHRxwQp0I8wJRWKL4jMYSn71GDKE5FvNMOoi
gvm05/rSf/ZlYPx36g8/0U22N/0CTCAsc4sK8GjqF4uMiGlo/eEgrK4aKQ2BuEuD
E973CkA/qtg0kH1MJmBrbqPDZm4cBMfLTGvWl1r0l59pmEjEp538DF6rrLnPo/gK
gZFzZdSx1n7yoUkc6RXshyqxmbX+0JTyy03S
-----END CERTIFICATE-----
```

O=ANF AC Entidad de Certificacion Peru SAC, OU=ANF Autoridad Raiz Peru, C=PE, CN=ANF Peru CA1, SERIALNUMBER=20601216281

Type	CA/QC
Status	undersupervision
Status starting time	2017-01-16T21:06:30.000Z

Service digital identity (X509)

Version	3
Serial number	218575887221501568
Signature algorithm	SHA256withRSA

Issuer	O=ANF Autoridad de Certificacion, OU=ANF Clase 1 CA, C=ES, CN=ANF Global Root CA, SERIALNUMBER=G63287510
Valid from	Thu Jul 21 09:30:27 PET 2016
Valid to	Fri Dec 24 09:30:27 PET 2032
Subject	O=ANF AC Entidad de Certificacion Peru SAC, OU=ANF Autoridad Raiz Peru, C=PE, CN=ANF Peru CA1, SERIALNUMBER=20601216281
Public key	Sun RSA public key, 4096 bits modulus: 7531018405275051070673543348421014707158442447594875455299570029952971164845105416519833197852497654307285787624233888137661295438003597451032861106348192337668722892981649003726878258288278314453694568162835696486211051092767654761572916166963091964985117567529725672746369295785033196331126500335066974745814142902682643269078172703759499850282526536529007918937019287904536662907087080592656150292316717071808449587469898978038052258064613579808036396415400703832086197564456177214539007294525594276473411597127730766583528397260701138212410008577206486054276905689247949456359759374183163243847617175991457209433994069724579883913498158885221438956144138606282616839717054577416384467473739655989903439057203142313941164187484030100814671690299901449807290851434155358348909127462470446730326646098247601555770464142960440542031065063698846261199087922268741053333282440827507120825696561095698669752882058237869062917448445512570781555796127663306927036915923996652297574480233632754031075167086574100376032028063264072430440878459924306107697531625377712523034556980021335167533193194262533809450266643304138931051278311697257387959029778405190293627705120973943047777160963418144588529734365781729066823833079587257929864735633 public exponent: 65537
Subject key identifier	0226d098071ab7bf9d69398cfdb4e17527a400d2
CRL distribution points	https://www.anf.es/crl/ANF_Global_Root_CA_arl.crl https://crl.anf.es/crl/ANF_Global_Root_CA_arl.crl
Authority key identifier	04183016801487fa9edf527675ec494a206f5b70968f9defbb17
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	fc7444b9d2f22813d7a9dd298ef2afc08b1c5fee
SHA256 Thumbprint	464bbeebc557b5eaee5ddb01dd1c816cec471256553da73f604be09c476067e8

The decoded certificate:

```
[
[
 Version: V3
 Subject: O=ANF AC Entidad de Certificacion Peru SAC, OU=ANF Autoridad Raiz Peru, C=PE, CN=ANF Peru CA1, SERIALNUMBER=20601216281
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
753101840527505107067354334842101470715844244759487545529957002995297116484510541651983319785249765430728578762423388813766129543800359745103286110634819233766872289298164900
037268782582882783144536945681628356964862110510927676547615729161669630919649851175675297256727463692957850331963311265003350669747458141429026826432690781727037594998502825
265365290079189370192879045366629070870805926561502923167170718084495874698989780380522580646135798080363964154007038320861975644561772145390072945255942764734115971277307665
835283972607011382124100085772064860542769056892479494563597593741831632438476171759914572094339940697245798839134981588852214389561441386062826168397170545774163844674737396
559899034390572031423139411641874840301008146716902999014498072908514341553583489091274624704467303266460982476015557704641429604405420310650636988462611990879222687410533332
824408275071208256965610956986697528820582378690629174484455125707815557961276633069270369159239966522975744802336327540310751670865741003760320280632640724304408784599243061
076975316253777125230345569800213351675331931942625338094502666433041389310512783116972573879590297784051902936277051209739430477771609634181445885297343657817290668238
3307958725792986473563
 public exponent: 65537
 Validity: [From: Thu Jul 21 09:30:27 PET 2016,
             To: Fri Dec 24 09:30:27 PET 2032]
 Issuer: O=ANF Autoridad de Certificacion, OU=ANF Clase 1 CA, C=ES, CN=ANF Global Root CA, SERIALNUMBER=G63287510
 SerialNumber: [    0308899c 824dae80]

Certificate Extensions: 7
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 02 26 D0 98 07 1A B7 BF   9D 69 39 8C FD B4 E1 75  .&.......i9....u
0010: 27 A4 00 D2                                        '...
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 87 FA 9E DF 52 76 75 EC   49 4A 20 6F 5B 70 96 8F  ....Rvu.IJ o[p..
```

```
0010: 9D EF BB 17                                        ....
]

]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: https://www.anf.es/crl/ANF_Global_Root_CA_arl.crl]
, DistributionPoint:
    [URIName: https://crl.anf.es/crl/ANF_Global_Root_CA_arl.crl]
]]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 81 CC 1A 81 C9 41 4E   46 20 41 43 20 65 6D 69  0.....ANF AC emi
0010: 73 6F 72 20 64 65 20 63   65 72 74 69 66 69 63 61  sor de certifica
0020: 64 6F 73 20 72 65 63 6F   6E 6F 63 69 64 6F 73 20  dos reconocidos
0030: 63 6F 6E 66 6F 72 6D 65   20 6C 61 20 6C 65 67 69  conforme la legi
0040: 73 6C 61 63 69 6F 6E 20   64 65 20 50 65 72 75 2E  slacion de Peru.
0050: 20 43 75 61 6C 71 75 69   65 72 20 75 73 6F 20 64   Cualquier uso d
0060: 65 20 65 73 74 65 20 63   65 72 74 69 66 69 63 61  e este certifica
0070: 64 6F 20 69 6D 70 6C 69   63 61 20 6C 61 20 61 63  do implica la ac
0080: 65 70 74 61 63 69 6F 6E   20 64 65 20 6C 61 20 43  eptacion de la C
0090: 50 53 20 79 20 64 65 20   6C 61 73 20 6C 69 6D 69  PS y de las limi
00A0: 74 61 63 69 6F 6E 65 73   20 64 65 20 72 65 73 70  taciones de resp
00B0: 6F 6E 73 61 62 69 6C 69   64 61 64 20 65 6E 20 65  onsabilidad en e
00C0: 6C 20 65 73 74 61 62 6C   65 63 69 64 61 73 2E     l establecidas.

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 20 68 74 74 70 73 3A   2F 2F 77 77 77 2E 61 6E  . https://www.an
0010: 66 2E 65 73 2F 70 65 2F   64 6F 63 75 6D 65 6E 74  f.es/pe/document
0020: 6F 73                                              os

]]  ]
]

[5]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[6]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://ocsp.anf.es/spain/AV,
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: https://www.anf.es/es/certificates_download/ANF_Global_Root_CA_SHA256_2036.cer]
]

[7]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: B0 EF 7E A7 9B 67 59 CA   90 58 43 AD 0D 5C A6 48  .....gY..XC..\.H
0010: 06 91 A3 4C EA 8B 26 23   B0 C5 13 42 0B F3 03 40  ...L..&#...B...@
0020: 63 84 C1 BD A5 7D E9 6F   FE 92 D1 F5 37 92 60 7A  c......o....7.`z
0030: 1C 2C 60 29 DD BF 9D A9   E7 A1 CE 37 2C 2C 0F 2C  .,`).......7,,.,
0040: 6D 1A BA 7C 27 A1 93 3C   C1 20 EC D9 89 33 27 15  m...'..<. ...3'.
0050: 48 21 18 C2 15 08 0E 32   F1 D8 AE B4 DE B4 18 D5  H!.....2........
0060: D3 5D 4D A1 C0 9D 2E 15   5F C0 AE 04 2A 37 56 D6  .]M....._...*7V.
0070: 62 B3 74 CF 0C 54 5E AB   63 DB AF 66 BA BA 1E 79  b.t..T^.c..f...y
0080: 0B 06 CA 91 42 25 1B FB   E7 D5 B4 9A 0E 3A 3F B6  ....B%.......:?.
0090: 9C 1C 2F 76 E6 4D 5F FB   7F 48 78 C1 62 9C 3D 17  ../v.M_..Hx.b.=.
00A0: 7E 4F 03 C6 53 F8 44 57   F5 53 7A 9B 07 CB 2C 65  .O..S.DW.Sz...,e
00B0: CD 8A F4 61 24 ED 99 0D   C1 09 3B 3E EE 32 DE F1  ...a$.....;>.2..
00C0: 13 4E 17 8A 6E 56 6D 0F   48 B6 41 8E B7 22 8A B9  .N..nVm.H.A.."..
00D0: DE 07 82 C0 CE 23 A3 E2   F6 1D EB 94 53 4B 93 01  .....#......SK..
00E0: 3A 0E 13 A3 97 77 BD 23   5C E4 64 92 0B 22 59 1D  :....w.#\.d.."Y.
00F0: 1C FC A4 7E 81 1D 75 AA   6C 51 F6 2B AA 14 FE 61  ......u.lQ.+...a
0100: 58 18 A8 79 1E 5A CE BE   9B 35 74 31 90 0A 00 FA  X..y.Z...5t1....
0110: 21 34 C1 61 2D 93 23 BE   15 50 B6 90 40 A5 76 C3  !4.a-.#..P..@.v.
0120: 08 67 A9 05 2D A7 21 AF   12 E2 E0 34 18 F1 D4 60  .g..-.!....4...`
0130: 9A 64 5C 2D F6 52 51 AC   2C F0 CE 1A CF D2 08 49  .d\-.RQ.,......I
0140: DE A1 F5 AA F8 DC 35 00   46 A2 3C 77 1A 40 0E A5  ......5.F.<w.@..
0150: 4C 1F A9 4E 00 1D 21 C9   9F 0D 2C 5E 1D D0 8E 1F  L..N..!...,^....
0160: 08 B8 83 A0 08 74 83 C1   A9 D1 49 D6 54 FD 7D 91  .....t....I.T...
0170: F0 35 D2 58 B6 25 E4 77   4F BC 9A 2A 27 A6 C2 34  .5.X.%.wO..*'..4
0180: 24 89 EF 7C 9E 0C A2 87   9F 66 E6 E6 FA 24 74 2C  $........f...$t,
0190: 61 EA 3D 4E 71 8C 78 03   46 6B 94 AA FA 2E 0F A2  a.=Nq.x.Fk......
01A0: B7 61 8E DD C0 41 7A F6   B0 6E E7 EE 23 DA 1B 06  .a...Az..n..#...
01B0: 48 0B B2 B0 22 B7 D8 68   55 35 99 BB 3C CF 54 F3  H..."..hU5..<.T.
01C0: 8D C1 F1 07 D3 25 6E 89   3F 95 8A DE 3D C9 63 49  .....%n.?...=.cI
```

```
01D0: D9 D0 93 6C 35 20 75 45   46 AD 9E DE B9 0A C9 DB  ...l5 uEF.......
01E0: 8C 3E 9B 17 03 2F 82 7C   F9 1D 13 1D 0B DC D5 75  .>.../.........u
01F0: B5 CE 67 0D 98 BA BA 80   F3 AE 1D 60 79 37 BD 90  ..g........`y7..

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIIODCCBiCgAwIBAgIIAwiJnIJNroAwDQYJKoZIhvcNAQELBQAwgYAxEjAQBgNV
BAUTCUc2MzI4NzUxMDEbMBkGA1UEAwwSQU5GIEdsb2JhbCBSb290IENBMQswCQYD
VQQGEwJFUzEXMBUGA1UECwwOQU5GIENsYXNlIDEgQ0ExJzAlBgNVBAoMHkFORiBB
dXRvcmlkYWQgZGUgQ2VydGlmaWNhY2lvbjAeFw0xNjA3MjExNDMwMjdaFw0zMjEy
MjQxNDMwMjdaMIGPMRQwEgYDVQQFEwsyMDYwMTIxNjI4MTEVMBMGA1UEAwwMQU5G
IFBlcnUgQ0ExMQswCQYDVQQGEwJQRTEgMB4GA1UECwwXQU5GIEF1dG9yaWRhZCBS
YWl6IFBlcnUxMTAvBgNVBAoMKEFORiBBQyBFbnRpZGFkIGRlIENlcnRpZmljYWNp
b24gUGVydSBTQUMwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQC4mZJM
y96W4rRVhQca75aBGW9JXrCT6WZwceTUdTJpqhFVXtJtWsHGaMAkzJB7LCUY/BEN
R77fBJSdENwDOqwciwmwkNrxqDesryPbXMFF0LC+GZ5/hzCSfyqdpnskc01WBCyj
PYm+22fywIYpdUq67SRy76bYBYhVo9+fWaltcW4qKSA+snZv0kAz2t7HT/VCahbR
RmPoNAvP6jxonHv9hyQn9LRBr/MdCagYSqMckpEkmj8p8h2607NBlpwtM9gV+vE6
VIbWiODqDqQjcK8F8o1XfrgS+4+HBc4NSV/iW5kkl6fLj1abdCu7J3zIJYkWeGAY
WxPVYI5l/2PXXgN2Ah2HkgqMs69zvTZ3W4haFWic7oTp/sNasq2uwtZD5SooV4E7
A65wT//JcfyxRAFLzrdeuWfSueb+eULHaa5K3fhRQEq4zcvj2RRkhU2QPUOHePnj
jEKAw7TqJzCErAlHTbCuOvEErRhzd7skQNgcpZY5fIOP5Ws/RlRBWUSy4wHyFQRD
OuuSVoe4gbFnVOPaTffpR9kOBhOSxbmeUQT0X0TvZvsapuXWXwOOBxPzJDAwahZS
oTYkOKDic8ccr1Sd4EDOHrItfgvrUiJuE0LyKJHoaKE896kCQPSbsM9t/m4wM6E8
6qDdBGxS/OuHQ4TzEEvxcs7iIqmvPxLUQEKkWwIDAQABo4ICozCCAp8wHQYDVR0O
BBYEFAIm0JgHGre/nWk5jP204XUnpADSMB8GA1UdIwQYMBaAFIf6nt9SdnXsSUog
b1twlo+d77sXMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQDAgEGMIIBJQYD
VR0gBIIBHDCCARgwggEUBgRVHSAAMIIBCjCB2QYIKwYBBQUHAgIwgcwagclBTkYg
QUMgZW1pc29yIGRlIGNlcnRpZmljYWRvcyByZWNvbm9jaWRvcyBjb25mb3JtZSBs
YSBsZWdpc2xhY2lvbiBkZSBQZXJ1LiBDdWFscXVpZXIgdXNvIGRlIGVzdGUgY2Vy
dGlmaWNhZG8gaW1wbGljYSBsYSBhY2VwdGFjaW9uIGRlIGxhIENQUyB5IGRlIGxh
cyBsaW1pdGFjaW9uZXMgZGUgcmVzcG9uc2FiaWxpZGFkIGVuIGVsIGVzdGFibGVj
aWRhcy4wLAYIKwYBBQUHAgEWIGh0dHBzOi8vd3d3LmFuZi5lcy9wZS9kb2N1bWVu
dG9zMHsGA1UdHwR0MHIwN6A1oDOGMWh0dHBzOi8vd3d3LmFuZi5lcy9jcmwvQU5G
X0dsb2JhbF9Sb290X0NBX2FybC5jcmwwN6A1oDOGMWh0dHBzOi8vY3JsLmFuZi5l
cy9jcmwvQU5GX0dsb2JhbF9Sb290X0NBX2FybC5jcmwwgZUGCCsGAQUFBwEBBIGI
MIGFMCcGCCsGAQUFBzABhhtodHRwOi8vb2NzcC5hbmYuZXMvc3BhaW4vQVYwWgYI
KwYBBQUHMAKGTmh0dHBzOi8vd3d3LmFuZi5lcy9lcy9jZXJ0aWZpY2F0ZXNfZG93
bmxvYWQvQU5GX0dsb2JhbF9Sb290X0NBX1NIQTI1Nl8yMDM2LmNlcjANBgkqhkiG
9w0BAQsFAAOCAgEAsO9+p5tnWcqQWEOtDVymSAaRo0zqiyYjsMUTQgvzA0BjhMG9
pX3pb/6S0fU3kmB6HCxgKd2/nannoc43LCwPLG0aunwnoZM8wSDs2YkzJxVIIRjC
FQgOMvHYrrTetBjV011NocCdLhVfwK4EKjdW1mKzdM8MVF6rY9uvZrq6HnkLBsqR
QiUb++fVtJoOOj+2nBwvduZNX/t/SHjBYpw9F35PA8ZT+ERX9VN6mwfLLGXNivRh
JO2ZDcEJOz7uMt7xE04Xim5WbQ9ItkGOtyKKud4HgsDOI6Pi9h3rlFNLkwE6DhOj
l3e9I1zkZJILIlkdHPykfoEddapsUfYrqhT+YVgYqHkeWs6+mzV0MZAKAPohNMFh
LZMjvhVQtpBApXbDCGepBS2nIa8S4uA0GPHUYJpkXC32UlGsLPDOGs/SCEneofWq
+Nw1AEaiPHcaQA6lTB+pTgAdIcmfDSxeHdCOHwi4g6AIdIPBqdFJllT9fZHwNdJY
tiXkd0+8mionpsI0JInvfJ4MooefZubm+iR0LGHqPU5xjHgDRmuUqvouD6K3YY7d
wEF69rBu5+4j2hsGSAuysCK32GhVNZm7PM9U843B8QfTJW6JP5WK3j3JY0nZ0JNs
NSB1RUatnt65CsnbjD6bFwMvgnz5HRMdC9zVdbXOZw2YurqA864dYHk3vZA=
-----END CERTIFICATE-----
```

Certificate Service Provider Name (en): BMTECH PERU S.A.C.

Trade name (en)	BMTECH PERU S.A.C.
Information URI (en)	WWW.BMCERT.PE
Service provider street address (es)	AV. JOSE LARCO, 1116, 3ER PISO, MIRAFLORES, LIMA
Service provider street address (en)	AV. JOSE LARCO, 1116, 3ER PISO, MIRAFLORES, LIMA
Service provider postal code (es)	LIMA18
Service provider postal code (en)	LIMA18
Service provider locality (es)	MIRAFLORES
Service provider locality (en)	MIRAFLORES
Service provider state (es)	LIMA
Service provider state (en)	LIMA
Service provider country (es)	PE
Service provider country (en)	PE

CN=BMCERT Issuing CA, OU=Certification Authorities, O=BMCERT, C=PE

Type	CA/QC
Status	undersupervision
Status starting time	2017-11-03T21:26:54.000Z

Service digital identity (X509)

Version	3
Serial number	1464276687
Signature algorithm	SHA256withRSA
Issuer	CN=BMCERT Root CA, OU=Certification Authorities, O=BMCERT, C=PE
Valid from	Thu May 26 13:24:42 PET 2016
Valid to	Sun Dec 26 13:54:42 PET 2027
Subject	CN=BMCERT Issuing CA, OU=Certification Authorities, O=BMCERT, C=PE
Public key	Sun RSA public key, 2048 bits modulus: 26168245373349582101216451831842430467040508106906591062594362181961089 86654404735660738650398417015127111184956101927316584959878173013721870 90850573375524684228591719440674477111579339554775426087033556267333369 15296108898809482847415009377264263073427754297701195616926482303667272 73384555166046201536162261294646114414424552984781652869757584553968454 88581301363532004406998187793220022540657369120212192431274090846096892 26107752395420822540229142648859124127565465928971077309350815086558414 81608223178632183450998548366579852833690634391349935526407901354437987 37066915689062943601633475756528413284374320165467 public exponent: 65537
Subject key identifier	5dafffd3fc42110d88e8ad71e94f63fc218ff848
CRL distribution points	http://bmcertcrl.managed.entrust.com/CRLs/BMCertRootCA.crl
Authority key identifier	041830168014129ad9aa85e941edbed66df089ee897cb43c6f95
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=0
SHA1 Thumbprint	ac1b125b818e8a9fae881efc5cc0c6dbe816a751
SHA256 Thumbprint	7ed67e18634114054906135de2f257ee88ba40de5d0cd744e82e252f6922abee

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=BMCERT Issuing CA, OU=Certification Authorities, O=BMCERT, C=PE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
26168245373349582101216451831842430467040508106906591062594362181961089866544047356607386503984170151271111849561019273165849598781730137218709085057337552468422859171944067447711157933955477542608703355626733336915296108898809482847415009377264263073427754297701195616926482303667272733845551660462015361622612946461144144245529847816528697575845539684548858130136353200440699818779322002254065736912021219243127409084609689226107752395420822540229142648859124127565465928971077309350815086558414816082231786321834509985483665798528336906343913499355264079013544379873706691568906294360163347575652841328374320165467
 public exponent: 65537
 Validity: [From: Thu May 26 13:24:42 PET 2016,
              To: Sun Dec 26 13:54:42 PET 2027]
 Issuer: CN=BMCERT Root CA, OU=Certification Authorities, O=BMCERT, C=PE
 SerialNumber: [    574716cf]

Certificate Extensions: 7
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 5D AF FF D3 FC 42 11 0D   88 E8 AD 71 E9 4F 63 FC  ]....B.....q.Oc.
0010: 21 8F F8 48                                        !..H
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 12 9A D9 AA 85 E9 41 ED   BE D6 6D F0 89 EE 89 7C  ......A...m.....
0010: B4 3C 6F 95                                        .<o.
]

]
```

```
[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://bmcertcrl.managed.entrust.com/CRLs/BMCertRootCA.crl]
, DistributionPoint:
    [CN=CRL1, CN=BMCERT Root CA, OU=Certification Authorities, O=BMCERT, C=PE]
]]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.16.840.1.114027.200.3.10.39.1]
[]  ]
 [CertificatePolicyId: [2.16.840.1.114027.200.3.10.39.2]
[]  ]
 [CertificatePolicyId: [2.16.840.1.114027.200.3.10.39.3]
[]  ]
]

[5]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[6]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://bmcertcrl.managed.entrust.com/AIA/CertsIssuedtoBMCertRootCA.p7c,
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://bmcertocsp.managed.entrust.com]
]

[7]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:0
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 06 86 EF 81 6F CB 73 A9   2D 30 E6 16 F3 BA 99 35  ....o.s.-0.....5
0010: C2 5C BD 29 E1 FD 55 19   53 49 F8 A1 93 CB 1A 40  .\.)..U.SI.....@
0020: FC 3D EE 43 AC AF E8 00   FC 7A 7C B9 CD 58 27 B0  .=.C.....z...X'.
0030: C0 32 90 32 24 DD A5 D4   14 3D 75 5C F5 37 77 28  .2.2$....=u\.7w(
0040: 93 56 35 42 DD F2 FF B1   78 90 0A B7 4F BC 9B 42  .V5B....x...O..B
0050: AE B8 CA FD A4 0A F4 05   B3 B5 2C 51 F0 02 96 15  ..........,Q....
0060: 1F 4C ED 23 F6 4C 39 54   32 92 24 A7 0E F6 8B 3E  .L.#.L9T2.$....>
0070: 16 C7 92 20 AB 14 AE 19   94 35 20 96 73 38 1C DB  ... .....5 .s8..
0080: 66 B7 B8 32 9F CB 6A 4E   6D C1 7D 17 96 F4 56 C2  f..2..jNm.....V.
0090: BF 9C 29 E7 16 89 36 DF   A1 71 66 4C BB FA 2C 5D  ..)...6..qfL..,]
00A0: AD 5E AD 5F B2 7C 37 70   A0 3D 9A 33 62 15 38 7B  .^._..7p.=.3b.8.
00B0: 53 31 2D 78 33 EB 2B 65   B5 8F 87 AF 67 C3 69 18  S1-x3.+e....g.i.
00C0: 44 C0 64 CA 64 1B A4 91   80 0B 60 5B B0 D9 1E 46  D.d.d.....`[...F
00D0: 8A 28 4B 48 5B 87 BC 51   F0 60 7B 5D B4 5A 14 5E  .(KH[..Q.`.].Z.^
00E0: BB 95 E2 83 9D B2 D7 AC   3A 6E 7D C3 64 C9 60 02  ........:n..d.`.
00F0: 6F D0 80 1F DD 56 09 26   3B E9 1A 23 13 73 77 B0  o....V.&;..#.sw.

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIFPTCCBCWgAwIBAgIEV0cWzzANBgkqhkiG9w0BAQsFADBbMQswCQYDVQQGEwJQ
RTEPMA0GA1UEChMGQk1DRVJUMSIwIAYDVQQLExlDZXJ0aWZpY2F0aW9uIEF1dGhv
cml0aWVzMRcwFQYDVQQDEw5CTUNFUlQgUm9vdCBDQTAeFw0xNjA1MjYxODI0NDJa
Fw0yNzEyMjYxODU0NDJaMF4xCzAJBgNVBAYTAlBFMQ8wDQYDVQQKEwZCTUNFUlQx
IjAgBgNVBAsTGUNlcnRpZmljYXRpb24gQXV0aG9yaXRpZXMxGjAYBgNVBAMTEUJN
Q0VSVCBJc3N1aW5nIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
z0rc43389Em/+TX5ASV2ydpJvqpj3Ady2UMEA2n7lTAT50nkAZr4/vxQWZZd/Sbp
MPUh+Hh06ilW/REx+4/uvqx7S5KrP0dvy8vrs5BmHI+HLvnFWLNtEo9AfQUO1RA/
8Mn5ANMY+FQUhdnXjH76iw36PWER3Lb9nI7EuVaookOoqHh/Jwe2FaEVE8iiSRl5
TXCbxcfoFxZC4ixaILUd+JfFl7pzc1LnHt0RgnJNL+UwLoFnDSQ5jsjUF+/EZGn5
mGwLAtoI+A/ebYS6eAkasVaBe1PqPOUyLtGq9FNpiU7mQosZcn6dHY/zpLif6PJE
7NnNxA5Mgkzzw7MXOd9yWwIDAQABo4ICBDCCAgAwDgYDVR0PAQH/BAQDAgEGMBIG
A1UdEwEB/wQIMAYBAf8CAQAwPAYDVR0gBDUwMzAPBg1ghkgBhvprgUgDCicBMA8G
DWCGSAGG+muBSAMKJwIwDwYNYIZIAYb6a4FIAwonAzCBlwYIKwYBBQUHAQEEgYow
gYcwUgYIKwYBBQUHMAKGRmh0dHA6Ly9ibWNlcnRjcmwubWFuYWdlZC5lbnRydXN0
LmNvbS9BSUEvQ2VydHNJc3N1ZWR0b0JNQ2VydFJvb3RDQS5wN2MwMQYIKwYBBQUH
MAGGJWh0dHA6Ly9ibWNlcnRvY3NwLm1hbmFnZWQuZW50cnVzdC5jb20wgcEGA1Ud
HwSBuTCBtjBAoD6gPIY6aHR0cDovL2JtY2VydGNybC5tYW5hZ2VkLmVudHJ1c3Qu
Y29tL0NSTHMvQk1DZXJ0Um9vdENBLmNybDByoHCgbqRsMGoxCzAJBgNVBAYTAlBF
MQ8wDQYDVQQKEwZCTUNFUlQxIjAgBgNVBAsTGUNlcnRpZmljYXRpb24gQXV0aG9y
aXRpZXMxFzAVBgNVBAMTDkJNQ0VSVCBSb290IENBMQ0wCwYDVQQDEwRDUkwxMB8G
A1UdIwQYMBaAFBKa2aqF6UHtvtZt8InuiXy0PG+VMB0GA1UdDgQWBBRdr//T/EIR
DYjorXHpT2P8IY/4SDANBgkqhkiG9w0BAQsFAAOCAQEABobvgW/Lc6ktMOYW87qZ
NcJcvSnh/VUZU0n4oZPLGkD8Pe5DrK/oAPx6fLnNWCewwDKQMiTdpdQUPXVc9Td3
KJNWNULd8v+xeJAKt0+8m0KuuMr9pAr0BbO1LFHwApYVH0ztI/ZMOVQykiSnDvaL
PhbHkiCrFK4ZlDUglnM4HNtmt7gyn8tqTm3BfReW9FbCv5wp5xaJNt+hcWZMu/os
Xa1erV+yfDdwoD2aM2IVOHtTMS14M+srZbWPh69nw2kYRMBkymQbpJGAC2BbsNke
RoooS0hbh7xR8GB7XbRaFF67leKDnbLXrDpufcNkyWACb9CAH91WCSY76RojE3N3
sA==
-----END CERTIFICATE-----
```

CN=BMCERT Root CA, OU=Certification Authorities, O=BMCERT, C=PE

Type	CA/QC
Status	undersupervision
Status starting time	2017-11-03T20:33:44.000Z

Service digital identity (X509)

Version	3
Serial number	1464276628
Signature algorithm	SHA256withRSA
Issuer	CN=BMCERT Root CA, OU=Certification Authorities, O=BMCERT, C=PE
Valid from	Thu May 26 10:00:29 PET 2016
Valid to	Thu Dec 26 10:30:29 PET 2030
Subject	CN=BMCERT Root CA, OU=Certification Authorities, O=BMCERT, C=PE
Public key	Sun RSA public key, 2048 bits modulus: 21105001002344140151492484529797311906803757209758675972155282949428193 36355451532940039620915166880336436776159292268773815147607887332237598 92824198641988125089876477464352427138023801919535992755520049471917687 90864426763104327169866340589548100642961517356034338217101856040741175 86156900193815543403614633936936418870324078879114211460380528292701715 84865941361493643068714926052483798630610890125620381595735614126913515 87657576294885726645246923339127966146100692540903564766867631377322816 63851032436696316760187362226413682193136020285351474642315641748815247 31388764632823551555113944041719766099151459259 37 public exponent: 65537
Subject key identifier	129ad9aa85e941edbed66df089ee897cb43c6f95
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	b669d104228df706e877d8d532223cddf21e77c1
SHA256 Thumbprint	754c0c860a38400115e356f1ade976156283f01f29a54f53d7721b2b003053f2

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=BMCERT Root CA, OU=Certification Authorities, O=BMCERT, C=PE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
21105001002344140151492484529797311906803757209758675972155282949428193363554515329400396209151668803364367761592922687738151476078873322375989282419864198812508987647746435
24271380238019195359927555200494719176879086442676310432716986634058954810064296151735603433821710185604074117586156900193815543403614633936936418870324078879114211460380528
29270171584865941361493643068714926052483798630610890125620381595735614126913515876575762948857266452469233391279661461006925409035647668676313773228166385103243669631676018
73622264136821931360202853514746423156417488152473138876463282355155511394404171976609915145925937
 public exponent: 65537
 Validity: [From: Thu May 26 10:00:29 PET 2016,
             To: Thu Dec 26 10:30:29 PET 2030]
 Issuer: CN=BMCERT Root CA, OU=Certification Authorities, O=BMCERT, C=PE
 SerialNumber: [    57471694]

Certificate Extensions: 3
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 12 9A D9 AA 85 E9 41 ED   BE D6 6D F0 89 EE 89 7C  ......A...m.....
0010: B4 3C 6F 95                                        .<o.
]
]

[2]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[3]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
```

```
 Algorithm: [SHA256withRSA]
 Signature:
0000: 81 43 0C 85 84 8A B5 C2   27 92 8D 05 6E 39 60 28  .C......'...n9`(
0010: 82 00 34 1E 41 9E 75 3D   3A 5B A0 3B BE 1E D9 08  ..4.A.u=:[.;....
0020: A9 41 54 E7 DA 9F A1 E3   79 A9 68 39 2D 9D FE 24  .AT.....y.h9-..$
0030: 60 B8 F4 1A 13 57 0B 1B   12 FA 2C F1 61 57 F1 5F  `....W....,.aW._
0040: 4D 87 6C B9 D6 FF DB F5   0E 9A 29 AD 25 76 86 08  M.l.......).%v..
0050: 45 EA 14 2F 64 72 6B 37   DB A8 9D 99 08 0B CB 94  E../drk7........
0060: 2C EE 2E B0 71 B9 63 96   BF 0E B4 E0 68 73 21 98  ,...q.c.....hs!.
0070: 7A A9 BA BC 94 8F CC 4E   4D 0C 4B 2E 0B CB BF E5  z......NM.K.....
0080: 79 C5 49 61 78 71 3F 47   4E 95 D9 CB F3 2A CD 5D  y.Iaxq?GN....*.]
0090: 7D F2 E0 CE 14 2C CB 63   C6 D6 C5 E6 A6 09 11 1B  .....,.c........
00A0: 1F 7C 8C B5 88 B6 09 F7   89 84 61 52 D8 DD 35 F0  ..........aR..5.
00B0: 2A A1 43 FE AB 9E 27 6C   AA 78 C3 A8 C3 CC CA A9  *.C...'l.x......
00C0: 0C 7D CA 11 6C DE 21 F5   02 AB 9B 5C FD A0 1B D1  ....l.!....\....
00D0: 7F 88 56 DD 1B 9B 73 04   D4 D1 BE AF 4E 80 DD 79  ..V...s.....N..y
00E0: BF 2D 4E 07 BB 62 13 1A   84 81 B8 D9 92 91 A8 53  .-N..b.........S
00F0: DD A0 36 C1 63 51 4A 14   FC 14 91 2A AE DC AF EF  ..6.cQJ....*....

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIDdjCCAl6gAwIBAgIEV0cWlDANBgkqhkiG9w0BAQsFADBbMQswCQYDVQQGEwJQ
RTEPMA0GA1UEChMGQk1DRVJUMSIwIAYDVQQLExlDZXJ0aWZpY2F0aW9uIEF1dGhv
cml0aWVzMRcwFQYDVQQDEw5CTUNFUlQgUm9vdCBDQTAeFw0xNjA1MjYxNTAwMjla
Fw0zMDEyMjYxNTMwMjlaMFsxCzAJBgNVBAYTAlBFMQ8wDQYDVQQKEwZCTUNFUlQx
IjAgBgNVBAsTGUNlcnRpZmljYXRpb24gQXV0aG9yaXRpZXMxFzAVBgNVBAMTDkJN
Q0VSVCBSb290IENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApy8O
SAFzMGYPVWUiS+ybv7LOnBgXAbQ+SKDbuGj2o4orW+VysGbdgXjWhZcVkweeQjb1
HYBd1vEGqCgKOWYfKPfb6nyt6JX4J+edqtcFHfNn6zsQUumuzwb9ZwC7QF+NxQNQ
caQO7w3titnoHcZffTnlCByJQf68kOuNztimlQHU+tmTc8HF/DkVb0uThCTqghez
PZFTuA3d1EcdE+9eN6KKtgumtj74i45+k3/FE6padP9yhrksUpGBkljxg/Wj77BT
GMPEZbBQ7MtnJ0TJu6e1hRxhAR+yz6L8JZH2mdV2/vglDLPe1UqPhe77bcok14bU
jPzq91nMAqfu6rG1MQIDAQABo0IwQDAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/
BAUwAwEB/zAdBgNVHQ4EFgQUEprZqoXpQe2+1m3wie6JfLQ8b5UwDQYJKoZIhvcN
AQELBQADggEBAIFDDIWEirXCJ5KNBW45YCiCADQeQZ51PTpboDu+HtkIqUFU59qf
oeN5qWg5LZ3+JGC49BoTVwsbEvos8WFX8V9Nh2y51v/b9Q6aKa0ldoYIReoUL2Ry
azfbqJ2ZCAvLlCzuLrBxuWOWvw604GhzIZh6qbq8lI/MTk0MSy4Ly7/lecVJYXhx
P0d0ldnL8yrNXX3y4M4ULMtjxtbF5qYJERsffIy1iLYJ94mEYVLY3TXwKqFD/que
J2yqeMOow8zKqQx9yhFs3iH1AqubXP2gG9F/iFbdG5tzBNTRvq9OgN15vy1OB7ti
ExqEgbjZkpGoU92gNsFjUUoU/BSRKq7cr+8=
-----END CERTIFICATE-----
```

Certificate Service Provider Name (en): INDENOVA SUCURSAL DEL PERU

Trade name (en)	INDENOVA PERU
Information URI (en)	WWW.INDENOVA.COM
Service provider street address (es)	JR. JUNIN NO. 198, INTERIOR 802. MAGDALENA DEL MAR
Service provider street address (en)	JR. JUNIN NO. 198, INTERIOR 802. MAGDALENA DEL MAR
Service provider postal code (es)	17
Service provider postal code (en)	17
Service provider locality (es)	JR. JUNIN NO. 198, INTERIOR 802. MAGDALENA DEL MAR
Service provider locality (en)	JR. JUNIN NO. 198, INTERIOR 802. MAGDALENA DEL MAR
Service provider state (es)	LIMA
Service provider state (en)	LIMA
Service provider country (es)	PE
Service provider country (en)	PE

C=PE, L=LIMA, STREET=http://www.indenova.com, OU=Internet Certification Authority http://www.indenova.com, T=Subordinate Certificate Perú, O=inDenova Sucursal del Perú, EMAILADDRESS=sub_ca_pe@indenova.com, SERIALNUMBER=20549615709, CN=inDenova SUB001_PE, OID.2.5.4.13=inDenova Subordinate Certificate 001 Perú HW-KUSU

Type	CA/QC
Status	undersupervision
Status starting time	2017-12-11T20:56:27.000Z

Service digital identity (X509)

Version	3
Serial number	6
Signature algorithm	SHA256withRSA
Issuer	C=CO, L="BOGOTÁ, D.C.", STREET=http://www.gse.co/address, OU=Internet Certification Authority http://www.gse.co, SERIALNUMBER=9002042728, O=GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE, CN=Global Certification Authority Root GSE, EMAILADDRESS=ca@gse.co
Valid from	Tue Jan 19 02:00:00 PET 2016
Valid to	Wed Jan 10 02:00:00 PET 2046
Subject	C=PE, L=LIMA, STREET=http://www.indenova.com, OU=Internet Certification Authority http://www.indenova.com, T=Subordinate Certificate Perú, O=inDenova Sucursal del Perú, EMAILADDRESS=sub_ca_pe@indenova.com, SERIALNUMBER=20549615709, CN=inDenova SUB001_PE, OID.2.5.4.13=inDenova Subordinate Certificate 001 Perú HW-KUSU
Public key	Sun RSA public key, 4096 bits modulus: 860814725636931809993454105410147616612044436705843172422350522582668573507355116711488691792511646317161168653150748994365319160917467279024112706760658395806619009237844324 461480547667749686040406283452557728069134328347521143391642711090168260176846597569217217263623770465224227067175964436068397616342717830316512327124008256826648512566777996219474153589483926945247509023767760903711417784607185612852621547032158194375369772137141497928176807991037051419712253721289944186677235023619555792408849771648842834206296053834619188320643911605157055729557704733769944524841701464491318369058789003250622646476591932046735627151011868823477787577158198017495024541787909717366027114986100056564109262144847197351179278837038520943322450297318071638913578817219016822498367233324176940502743363633717889882925059543705323321433347106457068575173377347191141954238993017166370437551842834535289829004712827699803610551409978152322406644239425519032605516901488255768963591059702218334559014736598736575647190539453251818098442666771922147 public exponent: 65537
Subject key identifier	82d1eee25fb7eb3066b0919d75900d0da02d8367
CRL distribution points	http://crl.gse.co/root/crl_root_gse_sha2.crl http://crl1.gse.co/root/crl_root_gse_sha2.crl
Authority key identifier	04183016801447a00c09878f6a3841d3beaf7fa2e6143a81bfa0
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=0
SHA1 Thumbprint	b728d04a0ddd7e71f4209e1e98128b46643eaf93
SHA256 Thumbprint	dc05b2736e7ba1719c062b5f3c48cdabd518e153a26afb966e36cac109f91c4e

The decoded certificate:

```
[
[
 Version: V3
 Subject: C=PE, L=LIMA, STREET=http://www.indenova.com, OU=Internet Certification Authority http://www.indenova.com, T=Subordinate Certificate Perú, O=inDenova Sucursal del
Perú, EMAILADDRESS=sub_ca_pe@indenova.com, SERIALNUMBER=20549615709, CN=inDenova SUB001_PE, OID.2.5.4.13=inDenova Subordinate Certificate 001 Perú HW-KUSU
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
860814725636931809993454105410147616612044436705843172422350522582668573507355116711488691792511646317161168653150748994365319160917467279024112706760658395806619009237844324
461480547667749686040406283452557728069134328347521143391642711090168260176846597569217217263623770465224227067175964436068397616342717830316512327124008256826648512566777996219474153589483926945247509023767760903711417784607185612852621547032158194375369772137141497928176807991037051419712253721289944186677235023619555792408849771648842834206
296053834619188320643911605157055729557704733769944524841701464491318369058789003250622646476591932046735627151011868823477787577158198017495024541787909717366027114986100056564109262144847197351179278837038520943322450297318071638913578817219016822498367233324176940502743363633717889882925059543705323321433347106457068575173377347191141954238993017166370437551842834535289829004712827699803610551409978152322406644239425519032605516901488255768963591059702218334559014736598736575647190539453251818098442666771922147<br>930171663704375518428345352898290047128276998036105514099781523224066442394255190326055169014882557689635910597022183345590147365987367575647190539453251818098442666771922147
```

```
430702188785077776568472410704923655052841033792315691198000538754567559578486292406899959929560417398564953557583967174394733549408849031713875728327558580389421577423824458785474442637565095 91
 public exponent: 65537
 Validity: [From: Tue Jan 19 02:00:00 PET 2016,
             To: Wed Jan 10 02:00:00 PET 2046]
 Issuer: C=CO, L="BOGOTÁ, D.C.", STREET=http://www.gse.co/address, OU=Internet Certification Authority http://www.gse.co, SERIALNUMBER=9002042728, O=GESTION DE SEGURIDAD
ELECTRONICA S.A. - GSE, CN=Global Certification Authority Root GSE, EMAILADDRESS=ca@gse.co
 SerialNumber: [    06]

Certificate Extensions: 9
[1]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://certs.gse.co/root/crt_root_gse_sha2.crt]
]

[2]: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
 RFC822Name: info@indenova.com
]

[3]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 47 A0 0C 09 87 8F 6A 38   41 D3 BE AF 7F A2 E6 14  G.....j8A.......
0010: 3A 81 BF A0                                        :...
]

]

[4]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 82 D1 EE E2 5F B7 EB 30   66 B0 91 9D 75 90 0D 0D  ...._..0f...u...
0010: A0 2D 83 67                                        .-.g
]
]

[5]: ObjectId: 2.5.29.18 Criticality=false
IssuerAlternativeName [
 RFC822Name: info@gse.co
]

[6]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 2C 68 74 74 70 3A 2F   2F 63 70 73 2E 65 73 69  .,http://cps.esi
0010: 67 6E 61 2E 65 73 2F 73   75 62 2F 63 70 73 5F 73  gna.es/sub/cps_s
0020: 75 62 30 30 31 70 65 5F   63 61 2E 70 64 66        ub001pe_ca.pdf

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 42 1A 40 54 65 72 6D   73 20 6F 66 20 75 73 65  0B.@Terms of use
0010: 20 61 74 20 43 50 53 20   68 74 74 70 3A 2F 2F 63   at CPS http://c
0020: 70 73 2E 65 73 69 67 6E   61 2E 65 73 2F 73 75 62  ps.esigna.es/sub
0030: 2F 63 70 73 5F 73 75 62   30 30 31 70 65 5F 63 61  /cps_sub001pe_ca
0040: 2E 70 64 66                                        .pdf

]]  ]
]

[7]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:0
]

[8]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.gse.co/root/crl_root_gse_sha2.crl]
, DistributionPoint:
    [URIName: http://crl1.gse.co/root/crl_root_gse_sha2.crl]
]]

[9]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 3B DB 32 BD F9 7E 3D F2   10 87 6B 42 35 9C 88 EC  ;.2...=...kB5...
0010: 6B 5C E4 09 88 87 F1 7B   9C A6 56 59 30 B9 58 46  k\........VY0.XF
0020: A8 20 15 96 7F 9B 5B D8   34 71 54 D1 79 0A 4E 7C  . ....[.4qT.y.N.
0030: 49 57 A7 50 26 6B 09 A1   FC F1 86 5D 2D C6 43 A0  IW.P&k.....]-.C.
0040: CD 33 F7 2A E8 0E C6 B5   0F 65 E7 2E 9C E2 5E A5  .3.*.....e....^.
0050: 36 06 A3 3F EF 10 80 52   44 21 A8 E7 E0 4F 40 F2  6..?...RD!...O@.
0060: FF 78 99 93 E7 B9 27 7B   77 89 E0 5B 9A 53 39 46  .x....'.w..[.S9F
```

```
0070: 68 0D 55 A5 9B 88 9E 8A   63 7A C7 36 5D F7 6D 91  h.U.....cz.6].m.
0080: B6 2C 9F C4 40 7F 59 EC   98 BE E3 62 A6 61 BF D6  .,..@.Y....b.a..
0090: 4B F9 22 F5 EE C3 1C 7A   B8 24 EB 1E 16 B2 6F 06  K."....z.$....o.
00A0: 72 24 C1 EE 11 07 EB 61   0C 84 4B 8C 63 FE 8B 18  r$.....a..K.c...
00B0: 96 5B D3 67 7F D2 9D 20   4A 94 2E E6 1F B4 39 49  .[.g... J.....9I
00C0: 8A 38 A5 1F E9 86 8C AD   D7 80 CB 87 5B 8D 95 57  .8..........[..W
00D0: 43 C7 DB D1 1E 5B 38 7A   B5 1C 95 52 13 E4 AB 56  C....[8z...R...V
00E0: F5 0A 1D A2 11 82 BF 8A   51 02 56 47 04 36 25 9B  ........Q.VG.6%.
00F0: 90 77 49 AA BA FE FF AC   68 B8 0D 1E CA DE 11 46  .wI.....h......F
0100: DF AA FF A1 E4 31 6E 31   3F 4A 74 F8 1D 90 72 21  .....1n1?Jt...r!
0110: 96 46 8E 3D 25 53 06 BD   72 32 D6 84 5E 40 20 C9  .F.=%S..r2..^@ .
0120: 27 E9 3F D4 F9 F4 6D 0B   3E 4B 80 EF 07 7F D3 91  '.?...m.>K......
0130: 1F AF 87 B1 43 93 E2 97   CE 88 B0 58 B5 04 F0 81  ....C......X....
0140: 50 67 0D ED EE 68 1D D8   3E 6F 9B 9C 9A A3 E1 9C  Pg...h..>o......
0150: E2 98 D4 7F 76 6E F7 9C   3E 71 24 A9 61 11 C7 12  ....vn..>q$.a...
0160: EF FD A6 11 74 0F 71 A9   65 10 7A B0 6B F5 B9 AE  ....t.q.e.z.k...
0170: BB ED 52 E6 6A 95 FE 76   88 FC 9E DA 31 F3 CC 0C  ..R.j..v....1...
0180: 02 4A EA 29 67 A0 EC 91   31 20 DB 4C FE 2B 50 CD  .J.)g...1 .L.+P.
0190: 78 A1 02 C6 91 E3 94 32   DE FC 5C 50 FA F3 2F A8  x......2..\P../.
01A0: 7E CA 16 B3 30 10 3B D8   16 D4 43 08 B5 D1 3D 51  ....0.;...C...=Q
01B0: CE 0F 79 EF B8 44 EF E4   A2 5A 80 A0 25 BB DD DE  ..y..D...Z..%...
01C0: A8 69 79 3E 83 66 AC A3   D8 8A A6 2B 2D F2 DC FD  .iy>.f.....+-...
01D0: 73 BB 34 92 32 41 44 E7   4E 25 34 85 B7 B6 67 27  s.4.2AD.N%4...g'
01E0: 2C 45 0D 00 A6 75 A3 96   C0 E5 16 A7 06 C4 01 42  ,E...u.........B
01F0: 64 AC 42 0B BA C7 54 28   65 7C 76 55 72 8E 5A 4A  d.B...T(e.vUr.ZJ

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIJBjCCBu6gAwIBAgIBBjANBgkqhkiG9w0BAQsFADCCAR0xGDAWBgkqhkiG9w0B
CQEWCWNhQGdzZS5jbzEwMC4GA1UEAwwnR2xvYmFsIENlcnRpZmljYXRpb24gQXV0
aG9yaXR5IFJvb3QgR1NFMTQwMgYDVQQKDCtHRVNUSU9OIERFIFNFR1VSSURBRCBF
TEVDVFJPTklDQSBTLkEuIC0gR1NFMRMwEQYDVQQFEwo5MDAyMDQyNzI4MTswOQYD
VQQLDDJJbnRlcm5ldCBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSBodHRwOi8vd3d3
LmdzZS5jbzEiMCAGA1UECQwZaHR0cDovL3d3dy5nc2UuY28vYWRkcmVzczEWMBQG
A1UEBwwNQk9HT1TDgSwgRC5DLjELMAkGA1UEBhMCQ08wHhcNMTYwMTE5MDcwMDAw
WhcNNDYwMTEwMDcwMDAwWjCCAWYxOzA5BgNVBA0MMmluRGVub3ZhIFN1Ym9yZGlu
YXRlIENlcnRpZmljYXRlIDAwMSBQZXLDuiBIVy1LVVNVMRswGQYDVQQDDBJpbkRl
bm92YSBTVUIwMDFfUEUxFDASBgNVBAUTCzIwNTQ5NjE1NzA5MSUwIwYJKoZIhvcN
AQkBFhZzdWJfY2FfcGVAaW5kZW5vdmEuY29tMSQwIgYDVQQKDBtpbkRlbm92YSBT
dWN1cnNhbCBkZWwgUGVyw7oxJjAkBgNVBAwMHVN1Ym9yZGluYXRlIENlcnRpZmlj
YXRlIFBlcsO6MUEwPwYDVQQLDDhJbnRlcm5ldCBDZXJ0aWZpY2F0aW9uIEF1dGhv
cml0eSBodHRwOi8vd3d3LmluZGVub3ZhLmNvbTEgMB4GA1UECQwXaHR0cDovL3d3
dy5pbmRlbm92YS5jb20xDTALBgNVBAcMBExJTUExCzAJBgNVBAYTAlBFMIICIjAN
BgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA0wCd3e/XTnwMN447WXOePWUki27n
bg8Twvqv6PFFmUfEAHCMUBBJW2K49cezbR+nw9JsCHgRH560liPaCciKzUD27EQM
GmW5lT6grFAasz0Y81vQkOSqePxP9Oendsjvk B+YckUgmyvLA28nOGycCZXjuXxB
l6vC3rKZp8RmzSvHgzb1zdoS1G67YyWzj2HmNAqtD5MpSpCW7Lpl3cM4hUmqTxLU
Itvxs2iRfffM/gL1vP/YtXNGv5EFkViGBZmbiB35O98Xnms3xPhvmHyIiZAUwh4k
oPNa0VCPDvv0pG7ne0br1pkRcwGm4Xpmlq+t3F4tM3IyUw1b5Fvb+tS/gQywzstp
h432vQYlbikUtuYaTy0t4qZYyimSMaKIDX1hV2SROfmr/akuCzHP4ubHduOfCpCN
3hx2zH/czR2jckjycQeIxOHBQOIf1//YO+Wg2GUJzGpeZt17MOF9mAj8BCkAL7q2
EbXQ+9BHJtdpAPMygA4TMNZnzEeu7n0OE5BW7LCFM/Tspur+3I0chQHeE/Qv+I5D
kJh3AbzdMilcs4o7RF/NGB8LFkvNUr9Ll2r2aVsPB71kJp5KhznwsH1DphKod1JE
9Rt1/HHcAeD+WKbCsu8r0ynQoJ79Q1OcgXRMbtuOOUDLgEZvhtGubHCTlA1ZGrMb
YHD6Dq/quE6gMZcCAwEAAaOCAgIwggH+MB0GA1UdDgQWBBSC0e7iX7frMGawkZ11
kA0NoC2DZzAfBgNVHSMEGDAWgBRHoAwJh49qOEHTvq9/ouYUOoG/oDAOBgNVHQ8B
Af8EBAMCAQYwgaEGA1UdIASBmTCBljCBkwYEVR0gADCBijA4BggrBgEFBQcCARYs
aHR0cDovL2Nwcy5lc2lnbmEuZXMvc3ViL2Nwc19zdWIwMDFwZV9jYS5wZGYwTgYI
KwYBBQUHAgIwQhpAVGVybXMgb2YgdXNlIGF0IENQUyBodHRwOi8vY3BzLmVzaWdu
YS5lcy9zdWIvY3BzX3N1YjAwMXBlX2NhLnBkZjAcBgNVHREEFTATgRFpbmZvQGlu
ZGVub3ZhLmNvbTAWBgNVHRIEDzANgQtpbmZvQGdzZS5jbzBKBggrBgEFBQcBAQQ+
MDwwOgYIKwYBBQUHMAKGLmh0dHA6Ly9jZXJ0cy5nc2UuY28vcm9vdC9jcnRfcm9v
dF9nc2Vfc2hhMi5jcnQwEgYDVR0TAQH/BAgwBgEB/wIBADByBgNVHR8EazBpMDKg
MKAuhixodHRwOi8vY3JsLmdzZS5jby9yb290L2NybF9yb290X2dzZV9zaGEyLmNy
bDAzoDGgL4YtaHR0cDovL2NybDEuZ3NlLmNvL3Jvb3QvY3JsX3Jvb3RfZ3NlX3No
YTIuY3JsMA0GCSqGSIb3DQEBCwUAA4ICAQA72zK9+X498hCHa0I1nIjsa1zkCYiH
8XucplZZMLlYRqggFZZ/m1vYNHFU0XkKTnxJV6dQJmsJofzxhl0txkOgzTP3KugO
xrUPZecunOJepTYGoz/vEIBSRCGo5+BPQPL/eJmT57kne3eJ4FuaUzlGaA1VpZuI
nopjesc2XfdtkbYsn8RAf1nsmL7jYqZhv9ZL+SL17sMcergk6x4Wsm8GciTB7hEH
62EMhEuMY/6LGJZb02d/0p0gSpQu5h+0OUmKOKUf6YaMrdeAy4dbjZVXQ8fb0R5b
OHq1HJVSE+SrVvUKHaIRgr+KUQJWRwQ2JZuQd0mquv7/rGi4DR7K3hFG36r/oeQx
bjE/SnT4HZByIZZGjj0lUwa9cjLWhF5AIMkn6T/U+fRtCz5LgO8Hf9ORH6+HsUOT
4pfOiLBYtQTwgVBnDe3uaB3YPm+bnJqj4ZzimNR/dm73nD5xJKlhEccS7/2mEXQP
callEHqwa/W5rrvtUuZqlf52iPye2jHzzAwCSuopZ6DskTEg20z+K1DNeKECxpHj
lDLe/FxQ+vMvqH7KFrMwEDvYFtRDCLXRPVHOD3nvuETv5KJagKAlu93eqGl5PoNm
rKPYiqYrLfLc/XO7NJIyQUTnTiU0hbe2ZycsRQ0ApnWjlsDlFqcGxAFCZKxCC7rH
VChlfHZVco5aSg==
-----END CERTIFICATE-----
```

C=CO, L="BOGOTÁ, D.C.", STREET=http://www.gse.co/address, OU=Internet Certification Authority http://www.gse.co, SERIALNUMBER=9002042728, O=GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE, CN=Global Certification Authority Root GSE, EMAILADDRESS=ca@gse.co

Type	CA/QC
Status	undersupervision
Status starting time	2017-11-27T15:58:05.000Z

Service digital identity (X509)

Version	3
Serial number	0
Signature algorithm	SHA256withRSA
Issuer	C=CO, L="BOGOTÁ, D.C.", STREET=http://www.gse.co/address, OU=Internet Certification Authority http://www.gse.co, SERIALNUMBER=9002042728, O=GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE, CN=Global Certification Authority Root GSE, EMAILADDRESS=ca@gse.co
Valid from	Tue Jan 19 02:00:00 PET 2016
Valid to	Thu Jan 11 02:00:00 PET 2046
Subject	C=CO, L="BOGOTÁ, D.C.", STREET=http://www.gse.co/address, OU=Internet Certification Authority http://www.gse.co, SERIALNUMBER=9002042728, O=GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE, CN=Global Certification Authority Root GSE, EMAILADDRESS=ca@gse.co
Public key	Sun RSA public key, 4096 bits modulus: 72572835994780775492875925070862987372443670527309335903398815080640529 45093174229469030805165919963210053041599575887558564417398167403470712 95364060059338230007413307444899555779043009623245457108586157810404281 01763430720961554757123482853895232115260525752375226339264331945357831 38518586399944466486933082405912652602925304500166841338409659319544194 98756829065806392203680239126800266036716767407595758072636041149554000 43585370944239372375176031556720780026403545722015958097030196272629830 00984987521852866145775995027056218417716935072531816088487131767100078 40085834952732026913944033654455393336495638593484783802878033555166272 39116725091216859313381312649014620377814849966952622095531896896378881 65150363561047646158370062584548327817642544825103635595013018381733213 55995858220772726986402643870672357224521547275346693568994862500361238 45185687878427149793037100626845261346139311889941822155561731233224191 87771596628060680933960137978429148479051798111583390387420466412989750 12237417859428757763660121112346320189786847928865698716888911224327426 18385669610593719787852161630416434678660563056465444917465415934123432 64740800360384655629367620438795262853960906156927825428733656562959223 98077824716955641695122189 public exponent: 65537
Subject key identifier	47a00c09878f6a3841d3beaf7fa2e6143a81bfa0
Authority key identifier	0418301680144 7a00c09878f6a3841d3beaf7fa2e6143a81bfa0
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=3
SHA1 Thumbprint	ecb1fc5784ee972751c15a7ab2eea15285273162
SHA256 Thumbprint	1d9f50320b6e20391be9741518466943d8a41a960d29872abe9713324b87a7c9

The decoded certificate:

```
[
[
 Version: V3
 Subject: C=CO, L="BOGOTÁ, D.C.", STREET=http://www.gse.co/address, OU=Internet Certification Authority http://www.gse.co, SERIALNUMBER=9002042728, O=GESTION DE SEGURIDAD
ELECTRONICA S.A. - GSE, CN=Global Certification Authority Root GSE, EMAILADDRESS=ca@gse.co
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
72572835994780775492875925070862987372443670527309335903398815080640529450931742294690308051659199632100530415995758875585644173981674034707129536406005933823000741330744489
95557790430096232454571085861578104042810176343072096155475712348285389523211526052575237522633926433194535783138518586399944466486933082405912652602925304500166841338409659
31954419498756829065806392203680239126800266036716767407595758072636041149554000435853709442393723751760315567207800264035457220159580970301962726298300098498752185286614577
59950270562184177169350725318160884871317671000784008583495273202691394403365445539333649563859348478380287803355516627239116725091216859313381312649014620377814849966952622
09553189689637888165150363561047646158370062584548327817642544825103635595013018381733213559958582207727269864026438706723572245215472753466935689948625003612384518568787842
71497930371006268452613461393118899418221555617312332241918777159662806068093396013797842914847905179811158339038742046641298975012237417859428757763660121112346320189786847
92886569871688891122432742618385669610593719787852161630416434678660563056465444917465415934123432647408003603846556293676204387952628539609061569278254287336565629592239807
7824716955641695122189
 public exponent: 65537
 Validity: [From: Tue Jan 19 02:00:00 PET 2016,
               To: Thu Jan 11 02:00:00 PET 2046]
 Issuer: C=CO, L="BOGOTÁ, D.C.", STREET=http://www.gse.co/address, OU=Internet Certification Authority http://www.gse.co, SERIALNUMBER=9002042728, O=GESTION DE SEGURIDAD
ELECTRONICA S.A. - GSE, CN=Global Certification Authority Root GSE, EMAILADDRESS=ca@gse.co
 SerialNumber: [    00]

Certificate Extensions: 8
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
```

```
KeyIdentifier [
0000: 47 A0 0C 09 87 8F 6A 38   41 D3 BE AF 7F A2 E6 14  G.....j8A.......
0010: 3A 81 BF A0                                        :...
]
]

[2]: ObjectId: 2.5.29.18 Criticality=false
IssuerAlternativeName [
 URIName: http://www.gse.co
]

[3]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 47 A0 0C 09 87 8F 6A 38   41 D3 BE AF 7F A2 E6 14  G.....j8A.......
0010: 3A 81 BF A0                                        :...
]

]

[4]: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
 RFC822Name: info@gse.co
]

[5]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 25 68 74 74 70 3A 2F   2F 63 70 73 2E 67 73 65  .%http://cps.gse
0010: 2E 63 6F 2F 72 6F 6F 74   2F 63 70 73 5F 63 61 5F  .co/root/cps_ca_
0020: 67 73 65 2E 70 64 66                               gse.pdf

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 42 1A 40 54 65 72 6D   73 20 6F 66 20 75 73 65  0B.@Terms of use
0010: 20 61 74 20 43 50 53 20   43 41 20 47 53 45 20 68   at CPS CA GSE h
0020: 74 74 70 3A 2F 2F 63 70   73 2E 67 73 65 2E 63 6F  ttp://cps.gse.co
0030: 2F 72 6F 6F 74 2F 63 70   73 5F 63 61 5F 67 73 65  /root/cps_ca_gse
0040: 2E 70 64 66                                        .pdf

]]  ]
]

[6]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[7]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:3
]

[8]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://certs.gse.co/root/crt_root_gse_sha2.crt]
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 5F 88 79 0B A4 47 B0 C5   5D 93 34 95 8C 99 19 8A  _.y..G..].4.....
0010: 10 0D CC 5E 15 37 BF 8C   8D 8F 18 CA 7E DF 97 2C  ...^.7.........,
0020: 94 54 DF A8 27 2A 4E 0F   6E C6 E2 5E 55 86 C5 FF  .T..'*N.n..^U...
0030: 3F 21 DC FF 0D CF 9D 00   2E 86 45 AB 81 D4 E4 81  ?!........E.....
0040: A5 C1 DE 1E 9D A1 C3 1D   D4 B4 02 D6 8F 1C C0 C4  ................
0050: A0 27 DE C8 68 BE 95 79   50 91 00 92 6E 36 07 EA  .'..h..yP...n6..
0060: 23 CB 58 A0 94 26 FD 75   01 9A BC 57 5B EF 38 DF  #.X..&.u...W[.8.
0070: 4B 8A DE A0 BF EF FC 4F   49 3D 9F D5 B1 12 CD FA  K......OI=......
0080: 93 77 A7 EF 29 CF 1C BA   E6 E0 93 D5 58 C5 77 20  .w..).......X.w
0090: CE 8E D3 2F 50 69 85 0D   F3 B9 01 48 AC 2A C9 C7  .../Pi.....H.*..
00A0: BC B4 F4 6D E6 23 41 C2   76 43 68 2B 1A 5A 1E 0F  ...m.#A.vCh+.Z..
00B0: CB 93 17 72 78 7B 3F 2C   7B 50 C8 5B 71 42 DD D0  ...rx.?,.P.[qB..
00C0: 09 C7 C9 AE 63 1B 21 0B   EA 8D 54 1B 56 70 88 39  ....c.!...T.Vp.9
00D0: 28 D8 B0 B3 DA 13 87 25   24 C0 25 37 6E DE FA 77  (......%$.%7n..w
00E0: B3 C5 35 85 C5 BC 9C 7C   BA 0C 17 D1 B0 7C BE 08  ..5.............
00F0: FC 3C 61 20 73 31 5E 9F   6F 48 1B F9 A8 20 9A 76  .<a s1^.oH... .v
0100: 9B 4E FB 4B 66 46 0E 57   E0 5F 55 89 F8 A9 E5 CE  .N.KfF.W._U.....
0110: 28 21 06 8F 77 FE 4F D5   E4 6E 8F 4F C0 62 A5 01  (!..w.O..n.O.b..
0120: 47 07 73 8A 02 75 B5 19   B4 D2 DC 76 80 25 A1 0B  G.s..u.....v.%..
0130: 5C A5 42 53 EA C9 71 B4   71 E5 E5 06 B4 00 86 B6  \.BS..q.q.......
0140: BD 06 95 43 66 45 35 74   21 D6 57 87 BA 25 B5 0A  ...CfE5t!.W..%..
0150: C8 B6 2A F8 73 69 BB 9E   C7 DB 95 92 0D D1 07 5C  ..*.si.........\
0160: 98 E3 B1 FD FE CB 0E BA   E7 E7 D9 7A 55 CC 0A B1  ...........zU...
0170: 35 99 B6 46 91 14 9A 07   09 83 AE 8F 87 0A F2 16  5..F............
0180: D5 EA 3B 9F 6C 52 2B 4E   AA EA 5B 15 E9 84 28 3D  ..;.lR+N..[...(=
0190: DE 62 C2 06 76 DF 03 D5   D3 C7 8C A2 F9 48 34 9D  .b..v........H4.
01A0: 3D 5E AB 05 F1 D1 DB 3F   79 08 2E F1 52 86 A3 77  =^.....?y...R..w
```

```
01B0: 5A 91 4D 12 4C C1 72 CF   5A 5D 90 26 58 15 83 12  Z.M.L.r.Z].&X...
01C0: 51 F5 84 57 8A 5D E3 58   78 8B 15 4A 5C 16 FC 6F  Q..W.].Xx..J\..o
01D0: 50 B1 51 30 DC 76 FA D2   9F 01 9D A0 0B 52 59 1A  P.Q0.v.......RY.
01E0: 36 55 21 02 AD 73 68 05   20 D0 1A 59 9F 55 33 50  6U!..sh. ..Y.U3P
01F0: CD 6D A6 C7 09 E5 CA 51   01 76 E2 8E 59 BE FB 21  .m.....Q.v..Y..!

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIIQjCCBiqgAwIBAgIBADANBgkqhkiG9w0BAQsFADCCAR0xGDAWBgkqhkiG9w0B
CQEWCWNhQGdzZS5jbzEwMC4GA1UEAwwnR2xvYmFsIENlcnRpZmljYXRpb24gQXV0
aG9yaXR5IFJvb3QgRlNFMTQwMgYDVQQKDCtHRVNUSU9OIERFIFNFR1VSSURBRCBF
TEVDVFJPTklDQSBTLkEuIC0gR1NFMRMwEQYDVQQFEwo5MDAyMDQyNzI4MTswOQYD
VQQLDDJJbnRlcm5ldCBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSBodHRwOi8vd3d3
LmdzZS5jbzEiMCAGA1UECQwZaHR0cDovL3d3dy5nc2UuY28vYWRkcmVzczEWMBQG
A1UEBwwNQk9HT1TDgSwgRC5DLjELMAkGA1UEBhMCQ08wHhcNMTYwMTE5MDcwMDAw
WhcNNDYwMTExMDcwMDAwWjCCAR0xGDAWBgkqhkiG9w0BCQEWCWNhQGdzZS5jbzEw
MC4GA1UEAwwnR2xvYmFsIENlcnRpZmljYXRpb24gQXV0aG9yaXR5IFJvb3QgRlNF
MTQwMgYDVQQKDCtHRVNUSU9OIERFIFNFR1VSSURBRCBFTEVDVFJPTklDQSBTLkEu
IC0gR1NFMRMwEQYDVQQFEwo5MDAyMDQyNzI4MTswOQYDVQQLDDJJbnRlcm5ldCBD
ZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSBodHRwOi8vd3d3LmdzZS5jbzEiMCAGA1UE
CQwZaHR0cDovL3d3dy5nc2UuY28vYWRkcmVzczEWMBQGA1UEBwwNQk9HT1TDgSwg
RC5DLjELMAkGA1UEBhMCQ08wggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoIC
AQCx496ylK3xkEbuCNT/97crz6cn18FppxsdHsDYZv39S4jNwf0Yq2KkyqR0W9No
1iDT/P8mF7d8evIsrBDSDXS8ir6w3oOaer5fAv1Nd7ZOLpWzTJn6TsIdUuzfJ+Rt
Eh9vexjk83kIAQnJA5CfJM3w0nFu5pVQHFyKQCu++86KQdFjg37vOK/6TsHQ/oS5
Y34rL7oD3FG4dytSV2Uoku+fO3HEs7WxIm7dZ/5NDkRdKQvV1Gi/2fuO4FIYo3Hg
AvP0TvWq1zkryvNe/07WaOLt5kgBdtunnd3B626XdKkS+ciiO/8U8QpRPwgkpEYF
ytFjk9wzXnqf3S+3OV1dqjBYil16epPIW3JJfDYFFLpgG5kDq8ZVGXa3WOuTGlu5
q/9qbY9Byzg1bKCKRM3Ey4rgS1d39Y50qp9KSNeWfyRE26g8T0vlX+3yqcNwu883
VIxXj34cXzZv23Xtb7CvTEUPAk/2cAF3+ZzLXIQnX3vjqHEnVmABWPwUju1SXjQk
LViy+PDO0WkiHgZIYYkd0/0mtLqpGhrBpTBxxonMFUcUmJhH4ZCVGxGg1h2lD0KE
iMDLMiugoYP0vgzJH9r8KcPx3EZVXzo1HjvkDdeX8M/sTsWYnplBQC7FXSh05z9D
BmGMeJFIsehiiCc4QydokMyluxm8THD5MUyAl53N5PMzDQIDAQABo4IBhzCCAYMw
HQYDVR0OBBYEFEegDAmHj2o4QdO+r3+i5hQ6gb+gMB8GA1UdIwQYMBaAFEegDAmH
j2o4QdO+r3+i5hQ6gb+gMA4GA1UdDwEB/wQEAwIBBjCBmgYDVR0gBIGSMIGPMIGM
BgRVHSAAMIGDMDEGCCsGAQUFBwIBFiVodHRwOi8vY3BzLmdzZS5jby9yb290L2Nw
c19jYV9nc2UucGRmME4GCCsGAQUFBwICMEIaQFRlcm1zIG9mIHVzZSBhdCBDUFMg
Q0EgR1NFIGh0dHA6Ly9jcHMuZ3NlLmNvL3Jvb3QvY3BzX2NhX2dzZS5wZGYwFgYD
VR0RBA8wDYELaW5mb0Bnc2UuY28wHAYDVR0SBBUwE4YRaHR0cDovL3d3dy5nc2Uu
Y28wSgYIKwYBBQUHAQEEPjA8MDoGCCsGAQUFBzAChi5odHRwOi8vY2VydHMuZ3Nl
LmNvL3Jvb3QvY3J0X3Jvb3RfZ3NlX3NoYTIuY3J0MBIGA1UdEwEB/wQIMAYBAf8C
AQMwDQYJKoZIhvcNAQELBQADggIBAF+IeQukR7DFXZM0lYyZGYoQDcxeFTe/jI2P
GMp+35cslFTfqCcqTg9uxuJeVYbF/z8h3P8Nz50ALoZFq4HU5IGlwd4enaHDHdS0
AtaPHMDEoCfeyGi+lXlQkQCSbjYH6iPLWKCUJv11AZq8V1vvON9Lit6gv+/8T0k9
n9WxEs36k3en7ynPHLrm4JPVWMV3IM6O0y9QaYUN87kBSKwqyce8tPRt5iNBwnZD
aCsaWh4Py5MXcnh7Pyx7UMhbcULd0AnHya5jGyEL6o1UG1ZwiDko2LCz2hOHJSTA
JTdu3vp3s8U1hcW8nHy6DBfRsHy+CPw8YSBzMV6fb0gb+aggmnabTvtLZkYOV+Bf
VYn4qeXOKCEGj3f+T9Xkbo9PwGKlAUcHc4oCdbUZtNLcdoAloQtcpUJT6slxtHHl
5Qa0AIa2vQaVQ2ZFNXQh1leHuiW1Csi2Kvhzabuex9uVkg3RB1yY47H9/ssOuufn
2XpVzAqxNZm2RpEUmgcJg66PhwryFtXqO59sUitOqupbFemEKD3eYsIGdt8D1dPH
jKL5SDSdPV6rBfHR2z95CC7xUoajd1qRTRJMwXLPWl2QJlgVgxJR9YRXil3jWHiL
FUpcFvxvULFRMNx2+tKfAZ2gC1JZGjZVIQKtc2gFINAaWZ9VM1DNbabHCeXKUQF2
4o5Zvvsh
-----END CERTIFICATE-----
```

Certificate Service Provider Name (en): ACEPTA PERU S.A.C.

Trade name (en)	ACEPTA PERU S.A.C.
Information URI (en)	WWW.ACEPTA.PE
Service provider street address (es)	CALLE AMADOR MERINO REYNA N° 465, OFICINA 602
Service provider street address (en)	CALLE AMADOR MERINO REYNA N° 465, OFICINA 602
Service provider postal code (es)	15046
Service provider postal code (en)	15046
Service provider locality (es)	SAN ISIDRO
Service provider locality (en)	SAN ISIDRO
Service provider state (es)	LIMA
Service provider state (en)	LIMA
Service provider country (es)	PE

Service provider country (en)	PE

SERIALNUMBER=20562999711, EMAILADDRESS=info@acepta.com, CN=Acepta Peru Autoridad de Sellado de Tiempo - V1, O=ACEPTA PERU S.A.C., C=PE

Type	CA/QC
Status	undersupervision
Status starting time	2019-08-22T21:40:03.000Z

Service digital identity (X509)

Version	3
Serial number	200
Signature algorithm	SHA256withRSA
Issuer	SERIALNUMBER=20562999711, EMAILADDRESS=info@acepta.com, CN=Acepta Peru Autoridad Certificadora Raiz - V1, O=ACEPTA PERU S.A.C., C=PE
Valid from	Wed Apr 18 10:54:31 PET 2018
Valid to	Sun Apr 18 10:54:31 PET 2038
Subject	SERIALNUMBER=20562999711, EMAILADDRESS=info@acepta.com, CN=Acepta Peru Autoridad de Sellado de Tiempo - V1, O=ACEPTA PERU S.A.C., C=PE
Public key	Sun RSA public key, 2048 bits modulus: 20185023918502727146656160722234152252985649714450488583656236183519041 35605629691644861055736056290046484168393194044134565817056936517273193 04656886388198493731496707336280343369074720764788027528019026813104147 17866113581175126735653942176660479373973635057192340527162156177611623 84607210610445259685240266366357004392139421732052095049843385180961858 65719578994316904899092766327474000789413292185427827736716560242634128 53826488861871917395250883403578489889476959795471171265817686977281943 69800614461711095996682029442947281290455872487439151074017305638011740 07937107861379008597655116504782495092396286467 43 public exponent: 65537
Subject key identifier	02c3efebb2425014d1574548b7c74bd7be3a033c
CRL distribution points	https://acpev1.acepta.pe/pev1/crl/PeruRaiz-V1.crl
Authority key identifier	0418301680147da80d687b38269de59b82489c6c73cd30e81d0c
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	e5139f64e09d6f773f4970cdce62443cdb636bc3
SHA256 Thumbprint	aa83fc9e5b2e360fa62fef0677b904aadfe46d6fee66d82a46237127519c33ab

The decoded certificate:

```
[
[
 Version: V3
 Subject: SERIALNUMBER=20562999711, EMAILADDRESS=info@acepta.com, CN=Acepta Peru Autoridad de Sellado de Tiempo - V1, O=ACEPTA PERU S.A.C., C=PE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
20185023918502727146656160722234152252985649714450488583656236183519041356056296916448610557360562900464841683931940441345658170569365172731930465688638819849373149670733628034336907472076478802752801902681310414717866113581175126735653942176660479373973635057192340527162156177611623846072106104452596852402663663570043921394217320520950498433851809618586571957899431690489909276632747400078941329218542782773671656024263412853826488861871917395250883403578489889476959795471171265817686977281943694800614461711095996682029442947281290455872487439151074017305638011740079371078613790085976551165047824950923962864674 3
 public exponent: 65537
 Validity: [From: Wed Apr 18 10:54:31 PET 2018,
             To: Sun Apr 18 10:54:31 PET 2038]
 Issuer: SERIALNUMBER=20562999711, EMAILADDRESS=info@acepta.com, CN=Acepta Peru Autoridad Certificadora Raiz - V1, O=ACEPTA PERU S.A.C., C=PE
 SerialNumber: [    c8]

Certificate Extensions: 8
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 02 C3 EF EB B2 42 50 14   D1 57 45 48 B7 C7 4B D7  .....BP..WEH..K.
0010: BE 3A 03 3C                                        .:.<
]
]
```

```
[2]: ObjectId: 2.5.29.18 Criticality=false
IssuerAlternativeName [
 Other-Name: Unrecognized ObjectIdentifier: 1.3.6.1.4.1.8321.2
 Other-Name: Unrecognized ObjectIdentifier: 1.3.6.1.5.5.7.8.3
 RFC822Name: info@acepta.com
]

[3]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 7D A8 0D 68 7B 38 26 9D   E5 9B 82 48 9C 6C 73 CD  ...h.8&....H.ls.
0010: 30 E8 1D 0C                                        0...
]

]

[4]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: https://acpev1.acepta.pe/pev1/crl/PeruRaiz-V1.crl]
]]

[5]: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
 Other-Name: Unrecognized ObjectIdentifier: 1.3.6.1.4.1.8321.1
 Other-Name: Unrecognized ObjectIdentifier: 1.3.6.1.5.5.7.8.3
 RFC822Name: info@acepta.com
]

[6]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [1.3.6.1.4.1.6891.1]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 2B 68 74 74 70 73 3A   2F 2F 61 63 70 65 76 31  .+https://acpev1
0010: 2E 61 63 65 70 74 61 2E   70 65 2F 43 50 53 2D 50  .acepta.pe/CPS-P
0020: 45 2D 56 31 2D 41 63 65   70 74 61 70 65           E-V1-Aceptape

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 81 D9 30 19 16 12 41   43 45 50 54 41 20 50 45  0..0...ACEPTA PE
0010: 52 55 20 53 2E 41 2E 43   2E 30 03 02 01 01 1A 81  RU S.A.C.0......
0020: BB 4C 61 20 75 74 69 6C   69 7A 61 63 69 6F 6E 20  .La utilizacion
0030: 64 65 20 65 73 74 65 20   63 65 72 74 69 66 69 63  de este certific
0040: 61 64 6F 20 65 73 74 61   20 73 75 6A 65 74 61 20  ado esta sujeta
0050: 61 20 6C 61 73 20 70 6F   6C 69 74 69 63 61 73 20  a las politicas
0060: 64 65 20 63 65 72 74 69   66 69 63 61 64 6F 20 28  de certificado (
0070: 43 50 29 20 79 20 70 72   61 63 74 69 63 61 73 20  CP) y practicas
0080: 64 65 20 63 65 72 74 69   66 69 63 61 63 69 6F 6E  de certificacion
0090: 20 28 43 50 53 29 20 65   73 74 61 62 6C 65 63 69   (CPS) estableci
00A0: 64 61 73 20 70 6F 72 20   41 63 65 70 74 61 2C 20  das por Acepta,
00B0: 79 20 64 69 73 70 6F 6E   69 62 6C 65 73 20 70 75  y disponibles pu
00C0: 62 6C 69 63 61 6D 65 6E   74 65 20 65 6E 20 77 77  blicamente en ww
00D0: 77 2E 61 63 65 70 74 61   2E 70 65 2E              w.acepta.pe.

]]  ]
]

[7]: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[8]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 7A FE A0 E9 CA F4 B3 81   86 F0 89 4C 8D BB 79 E8  z..........L..y.
0010: BA 29 83 3E 8C 56 8E BB   1B 1B 60 5A B5 ED E6 CD  .).>.V....`Z....
0020: FC F9 02 78 DA 3E 23 2E   92 0F 01 79 A2 E9 1F 9C  ...x.>#....y....
0030: 88 35 8B C0 0C 99 10 CF   CE C0 0C 07 FA BE E3 48  .5.............H
0040: 7A B0 2A 2F 3F F6 38 48   99 5B 2C 3D 3D B4 A3 70  z.*/?.8H.[,==..p
0050: B5 BC 11 C4 7B 2F 49 6E   E0 2E CE FC 81 E0 AD 71  ...../In.......q
0060: 71 95 3F 01 90 C7 03 A0   1B 91 9E 0C 17 66 82 BB  q.?.........f..
0070: A4 0D 0B A3 C8 B2 96 39   C2 83 30 0B C5 FB 9C 83  .......9..0.....
0080: 57 78 6C F1 05 B1 66 C2   AA C4 AA 29 C5 0D B8 5A  Wxl...f....)...Z
0090: 0F A0 77 0B 9F 1E 86 0C   4F 79 BF 28 FC 58 17 07  ..w.....Oy.(.X..
00A0: BE 92 71 61 9E B0 4F DD   7A 81 82 93 7D 7C F1 6F  ..qa..O.z......o
00B0: 60 84 17 29 6F 17 B9 77   A4 D7 C8 0F 3F BE 5F 0F  `..)o..w....?._.
00C0: F2 89 A1 C2 CC 21 40 75   02 29 00 DF 6D 17 01 3E  .....!@u.)..m..>
00D0: 3F D1 61 66 13 14 96 21   B7 B1 9B CD CC CE D1 3A  ?.af...!.......:
00E0: C5 DB 85 A0 A9 EA D2 96   C7 94 3E EF C8 70 11 C3  ..........>..p..
00F0: A5 61 B1 A4 7E 74 04 49   91 11 52 BA 6F 84 89 C7  .a...t.I..R.o...

]
```

The certificate in PEM format:


```
-----BEGIN CERTIFICATE-----
MIIGWTCCBUGgAwIBAgICAMgwDQYJKoZIhvcNAQELBQAwgZgxCzAJBgNVBAYTAlBF
MRswGQYDVQQKExJBQ0VQVEEgUEVSVSBTLkEuQy4xNjA0BgNVBAMTLUFjZXB0YSBQ
ZXJ1IEF1dG9yaWRhZCBDZXJ0aWZpY2Fkb3JhIFJhaXogLSBWMTEeMBwGCSqGSIb3
DQEJARYPaW5mb0BhY2VwdGEuY29tMRQwEgYDVQQFEwsyMDU2Mjk5OTcxMTAeFw0x
ODA0MTgxNTU0MzFaFw0zODA0MTgxNTU0MzFaMIGaMQswCQYDVQQGEwJQRTEbMBkG
A1UEChMSQUNFUFRBIFBFUlUgUy5BLkMuMTgwNgYDVQQDEy9BY2VwdGEgUGVydSBB
dXRvcmlkYWQgZGUgU2VsbGFkbyBkZSBUaWVtcG8gLSBWMTEeMBwGCSqGSIb3DQEJ
ARYPaW5mb0BhY2VwdGEuY29tMRQwEgYDVQQFEwsyMDU2Mjk5OTcxMTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ/lbKrj4lxX7k28q6ijQvOon9QyzZq9
vjXSMxqUKtU98SSxb7fVwo7hp86/mMVnag7G3x7RgY0mhwBfgP8Km2yqjQFX6d95
ScTdDAPWh0WEklogV+ONpVhOBkXGNlYk8dNna6Z+uKm9YQdyZm4nR36AyIYrjljl
XqShispKzr91kdageXNFXtlI+P/Ctu7zNJwefSQzSpwkikK41wRcdMWZiJz84VHc
94224SITTh0sgozwAueMlbd0vBmeH3LPsQeCV8u7BE34vJJECvjpL6v3upPaIeAW
3vrip8D6MjXQKHKfmgli6ux+NDehPRCHDv5CO3r7MHmFOdscQRI2SVcCAwEAAaOC
AqcwggKjMA8GA1UdEwEB/wQFMAMBAf8wHwYDVR0jBBgwFoAUfagNaHs4Jp3lm4JI
nGxzzTDoHQwwHQYDVR0OBBYEFALD7+uyQlAU0VdFSLfHS9e+OgM8MAsGA1UdDwQE
AwIBBjCCAUEGA1UdIASCATgwggE0MIIBMAYIKwYBBAG1awEwggEiMDcGCCsGAQUF
BwIBFitodHRwczovL2FjcGV2MS5hY2VwdGEucGUvQ1BTLVBFLVYxLUFjZXB0YXBl
MIHmBggrBgEFBQcCAjCB2TAZFhJBQ0VQVEEgUEVSVSBTLkEuQy4wAwIBARqBu0xh
IHV0aWxpemFjaW9uIGRlIGVzdGUgY2VydGlmaWNhZG8gZXN0YSBzdWpldGEgYSBs
YXMgcG9saXRpY2FzIGRlIGNlcnRpZmljYWRvIChDUCkgeSBwcmFjdGljYXMgZGUg
Y2VydGlmaWNhY2lvbiAoQ1BTKSBlc3RhYmxlY2lkYXMgcG9yIEFjZXB0YSwgeSBk
aXNwb25pYmxlcyBwdWJsaWNhbWVudGUgZW4gd3d3LmFjZXB0YS5wZS4wXAYDVR0S
BFUwU6AZBggrBgEEAcEBAqANFgsyMDU2Mjk5OTcxMaAlBggrBgEFBQcIA6AZMBcM
CzIwNTYyOTk5NzExBggrBgEEAcEBAoEPaW5mb0BhY2VwdGEuY29tMFwGA1UdEQRV
MFOgGQYIKwYBBAHBAQgDRYLMjA1NjI5OTk3MTGgJQYIKwYBBQUHCAOgGTAXDAsy
MDU2Mjk5OTcxMQYIKwYBBAHBAQKBD2luZm9AYWNlcHRhLmNvbTBCBgNVHR8EOzA5
MDegNaAzhjFodHRwczovL2FjcGV2MS5hY2VwdGEucGUvcGV2MS9jcmwvUGVydVJh
aXotVjEuY3JsMA0GCSqGSIb3DQEBCwUAA4IBAQB6/qDpyvSzgYbwiUyNu3nouimD
PoxWjrsbG2Bate3mzfz5AnjaPiMukg8BeaLpH5yINYvADJkQz87ADAf6vuNIerAq
Lz/2OEiZWyw9PbSjcLW8EcR7L0lu4C7O/IHgrXFxlT8BkMcDoBuRngwXZoK7pA0L
o8iyljnCgzALxfucg1d4bPEFsWbCqsSqKcUNuFoPoHcLnx6GDE95vyj8WBcHvpJx
YZ6wT916gYKTfXzxb2CEFylvF7l3pNfIDz++Xw/yiaHCzCFAdQIpAN9tFwE+P9Fh
ZhMUliG3sZvNzM7ROsXbhaCp6tKWx5Q+78hwEcOlYbGkfnQESZERUrpvhInH
-----END CERTIFICATE-----
```


SERIALNUMBER=20562999711, EMAILADDRESS=info@acepta.com, CN=Acepta Peru Autoridad Certificadora Digital - V1, O=ACEPTA PERU S.A.C., C=PE

Type	CA/QC
Status	undersupervision
Status starting time	2018-08-01T17:27:16.000Z

Service digital identity (X509)

Version	3
Serial number	3
Signature algorithm	SHA256withRSA
Issuer	SERIALNUMBER=20562999711, EMAILADDRESS=info@acepta.com, CN=Acepta Peru Autoridad Certificadora Raiz - V1, O=ACEPTA PERU S.A.C., C=PE
Valid from	Wed Apr 18 10:54:31 PET 2018
Valid to	Sun Apr 18 10:54:31 PET 2038
Subject	SERIALNUMBER=20562999711, EMAILADDRESS=info@acepta.com, CN=Acepta Peru Autoridad Certificadora Digital - V1, O=ACEPTA PERU S.A.C., C=PE
Public key	Sun RSA public key, 2048 bits modulus: 27060710516406163684509599022390553214999726795320603730344522040861084198651195327569534016957497766743078366713767516460910868232450666042057758023485540430146631523766356005062365622532065042166537370692882885498406869142817508701385306863713330787351431311086884219662492646670810867000495323341420353868892500198193284117966204888375006767838840624281488742312530269537559025450135178447080047698659789924686585827657045292967523951599313634040064058175250320816664775846892320689092179394977410157586889170683521769379694070408863643136998836179319510416504794030051222900099358123009452817055477530094255864171 public exponent: 65537
Subject key identifier	e5ea517d8f5e00f4de965ee4aae0325408b49d6f
CRL distribution points	https://acpev1.acepta.pe/pev1/crl/PeruRaiz-V1.crl
Authority key identifier	0418301680147da80d687b38269de59b82489c6c73cd30e81d0c
Key usage	keyCertSign cRLSign

Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	119539eecd5b177b57794fb63cead30ccceb656a
SHA256 Thumbprint	d6abd1ec32b2c6bef475e960af527c952128b3e7cb29b6dfb65c1a14203df38f

The decoded certificate:

```
[
[
 Version: V3
 Subject: SERIALNUMBER=20562999711, EMAILADDRESS=info@acepta.com, CN=Acepta Peru Autoridad Certificadora Digital - V1, O=ACEPTA PERU S.A.C., C=PE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
270607105164061636845095990223905532149997267953206037303445220408610841986511953275695340169574977667430783667137675164609108682324506660420577580234855404301466315237663560050623656225320650421665373706928828854984068691428175087013853068637133307873514313110868842196624926466708108670004953233414203538688925001981932841179662048883750067678388406242814887423125302695375590254501351784470800476986597899246865858276570452929675239515993136340400640581752503208166647758468923206890921793949774101575868891706835217693796940704088636431369988361793195104165047940300512229000993581230094528170554775300942558641715
 public exponent: 65537
 Validity: [From: Wed Apr 18 10:54:31 PET 2018,
             To: Sun Apr 18 10:54:31 PET 2038]
 Issuer: SERIALNUMBER=20562999711, EMAILADDRESS=info@acepta.com, CN=Acepta Peru Autoridad Certificadora Raiz - V1, O=ACEPTA PERU S.A.C., C=PE
 SerialNumber: [    03]

Certificate Extensions: 8
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: E5 EA 51 7D 8F 5E 00 F4   DE 96 5E E4 AA E0 32 54  ..Q..^....^...2T
0010: 08 B4 9D 6F                                        ...o
]
]

[2]: ObjectId: 2.5.29.18 Criticality=false
IssuerAlternativeName [
 Other-Name: Unrecognized ObjectIdentifier: 1.3.6.1.4.1.8321.2
 Other-Name: Unrecognized ObjectIdentifier: 1.3.6.1.5.5.7.8.3
 RFC822Name: info@acepta.com
]

[3]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 7D A8 0D 68 7B 38 26 9D   E5 9B 82 48 9C 6C 73 CD  ...h.8&....H.ls.
0010: 30 E8 1D 0C                                        0...
]

]

[4]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: https://acpev1.acepta.pe/pev1/crl/PeruRaiz-V1.crl]
]]

[5]: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
 Other-Name: Unrecognized ObjectIdentifier: 1.3.6.1.4.1.8321.1
 Other-Name: Unrecognized ObjectIdentifier: 1.3.6.1.5.5.7.8.3
 RFC822Name: info@acepta.com
]

[6]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [1.3.6.1.4.1.6891.1]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 2B 68 74 74 70 73 3A   2F 2F 61 63 70 65 76 31  .+https://acpev1
0010: 2E 61 63 65 70 74 61 2E   70 65 2F 43 50 53 2D 50  .acepta.pe/CPS-P
0020: 45 2D 56 31 2D 41 63 65   70 74 61 70 65           E-V1-Aceptape

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 81 D9 30 19 16 12 41   43 45 50 54 41 20 50 45  0..0...ACEPTA PE
0010: 52 55 20 53 2E 41 2E 43   2E 30 03 02 01 01 1A 81  RU S.A.C.0......
0020: BB 4C 61 20 75 74 69 6C   69 7A 61 63 69 6F 6E 20  .La utilizacion
0030: 64 65 20 65 73 74 65 20   63 65 72 74 69 66 69 63  de este certific
0040: 61 64 6F 20 65 73 74 61   20 73 75 6A 65 74 61 20  ado esta sujeta
0050: 61 20 6C 61 73 20 70 6F   6C 69 74 69 63 61 73 20  a las politicas
0060: 64 65 20 63 65 72 74 69   66 69 63 61 64 6F 20 28  de certificado (
0070: 43 50 29 20 79 20 70 72   61 63 74 69 63 61 73 20  CP) y practicas
0080: 64 65 20 63 65 72 74 69   66 69 63 61 63 69 6F 6E  de certificacion
0090: 20 28 43 50 53 29 20 65   73 74 61 62 6C 65 63 69   (CPS) estableci
00A0: 64 61 73 20 70 6F 72 20   41 63 65 70 74 61 2C 20  das por Acepta,
00B0: 79 20 64 69 73 70 6F 6E   69 62 6C 65 73 20 70 75  y disponibles pu
00C0: 62 6C 69 63 61 6D 65 6E   74 65 20 65 6E 20 77 77  blicamente en ww
00D0: 77 2E 61 63 65 70 74 61   2E 70 65 2E              w.acepta.pe.

]]  ]
]

[7]: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
```

```
 Key_CertSign
 Crl_Sign
]

[8]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 39 44 0D B3 B4 AC DA 11   CA BA E1 54 D8 9A D5 62  9D.........T...b
0010: 80 F8 07 24 9D 0D 2B 36   E5 82 D1 0A C0 1B 76 AF  ...$..+6......v.
0020: 4A E6 9E 07 78 1B 05 DF   87 C6 A7 78 C3 10 45 E0  J...x......x..E.
0030: B2 44 87 0E 17 5F FC 10   5E CA EB E8 2F 72 52 6F  .D..._..^.../rRo
0040: 1E 04 D8 17 AA 29 A5 BC   76 F0 B9 FC 25 64 F7 23  .....)..v...%d.#
0050: 99 7C 61 F5 50 F0 94 35   B7 2B 90 8E 3B 2B 89 EC  ..a.P..5.+..;+..
0060: CF AB 94 C7 25 1A 5A 09   5D 47 33 FF 9A 8A FA EB  ....%.Z.]G3.....
0070: 94 CB 53 17 21 78 5E 58   5C 16 F4 7C 04 BC 6B BC  ..S.!x^X\.....k.
0080: 63 BE 05 09 B3 38 6C 15   0D B4 25 EB 5E DE 52 31  c....8l...%.^.R1
0090: 28 87 DE 62 18 69 BC 73   69 36 A5 C0 49 5A 4A 26  (..b.i.si6..IZJ&
00A0: 4E FB 70 42 A0 17 AA 16   58 AC 23 A6 53 80 1D B1  N.pB....X.#.S...
00B0: 9D D2 B5 09 55 C2 9E 34   DC C9 4E 56 2E 97 4B 95  ....U..4..NV..K.
00C0: 58 C2 B1 68 68 3A 01 B1   7A 7B 70 73 3B 96 C1 61  X..hh:..z.ps;..a
00D0: AE 5C FF E1 4A AC 44 A5   1E 87 39 5C 6A 56 A7 7D  .\..J.D...9\jV..
00E0: A7 0D 9E C3 F4 BD 8A 3F   F1 C7 E1 AD B9 92 50 F4  .......?......P.
00F0: 6B 9B 06 0B DE 01 95 C2   85 0D 53 BD 95 A0 80 5C  k.........S....\

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGWTCCBUGgAwIBAgIBAzANBgkqhkiG9w0BAQsFADCBmDELMAkGA1UEBhMCUEUx
GzAZBgNVBAoTEkFDRVBUQSBQRVJVIFMuQS5DLjE2MDQGA1UEAxMtQWNlcHRhIFBl
cnUgQXV0b3JpZGFkIENlcnRpZmljYWRvcmEgUmFpeiAtIFYxMR4wHAYJKoZIhvcN
AQkBFg9pbmZvQGFjZXB0YS5jb20xFDASBgNVBAUTCzIwNTYyOTk5NzExMB4XDTE4
MDQxODE1NTQzMVoXDTM4MDQxODE1NTQzMVowgZsxCzAJBgNVBAYTAlBFMRswGQYD
VQQKExJBQ0VQVEEgUEVSVSBTLkEuQy4xOTA3BgNVBAMTMEFjZXB0YSBQZXJ1IEF1
dG9yaWRhZCBDZXJ0aWZpY2Fkb3JhIERpZ2l0YWwgLSBWMTEeMBwGCSqGSIb3DQEJ
ARYPaW5mb0BhY2VwdGEuY29tMRQwEgYDVQQFEwsyMDU2Mjk5OTcxMTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBANZcs9AEht7/Dl/Cxi8GkHylyPEE0LIq
FbtvlMb765GfNrwC2+bnNCxp2w0eGFyOmNZ6S5mOl7Nu9ZxcQ9vphGCLXVEWBeg4
JBJPUOMx2xH+npzNGyJOUpDMF/0W7f5bss6b8aoW62LzVLITX0o1hpHzh9Jl0OZ5
s7ZJlD0FrkMDJTXNEol6zJ9Q2+ZZusrwD+bWWE6AXyC4RpRoRGtpmNzF8mqqnlWl
IcTy3H69lnn9f34oY73+rfiAj+fIXGxT04TwrgSHj7qclROegQ9MGoBGAtF8qYfG
Hrl6W9X/fnS3l4U7noCCZHdrFwHy4voSQWP0JuEDeF8JCR+GmNTJ+WsCAwEAAaOC
AqcwggKjMA8GA1UdEwEB/wQFMAMBAf8wHwYDVR0jBBgwFoAUfagNaHs4Jp3lm4JI
nGxzzTDoHQwwHQYDVR0OBBYEFOXqUX2PXgD03pZe5KrgMlQItJ1vMAsGA1UdDwQE
AwIBBjCCAUEGA1UdIASCATgwggE0MIIBMAYIKwYBBAG1awEwggEiMDcGCCsGAQUF
BwIBFitodHRwczovL2FjcGV2MS5hY2VwdGEucGUvQ1BTLVBFLVYxLUFjZXB0YXBl
MIHmBggrBgEFBQcCAjCB2TAZFhJBQ0VQVEEgUEVSVSBTLkEuQy4wAwIBARqBu0xh
IHV0aWxpemFjaW9uIGRlIGVzdGUgY2VydGlmaWNhZG8gZXN0YSBzdWpldGEgYSBs
YXMgcG9saXRpY2FzIGRlIGNlcnRpZmljYWRvIChDUCkgeSBwcmFjdGljYXMgZGUg
Y2VydGlmaWNhY2lvbiAoQ1BTKSBlc3RhYmxlY2lkYXMgcG9yIEFjZXB0YSwgeSBk
aXNwb25pYmxlcyBwdWJsaWNhbWVudGUgZW4gd3d3LmFjZXB0YS5wZS4wXAYDVR0S
BFUwU6AZBggrBgEEAcEBAqANFgsyMDU2Mjk5OTcxMaAlBggrBgEFBQcIA6AZMBcM
CzIwNTYyOTk5NzExBggrBgEEAcEBAoEPaW5mb0BhY2VwdGEuY29tMFwGA1UdEQRV
MFOgGQYIKwYBBAHBAQGgDRYLMjA1NjI5OTk3MTGgJQYIKwYBBQUHCAOgGTAXDAsy
MDU2Mjk5OTcxMQYIKwYBBAHBAQKBD2luZm9AYWNlcHRhLmNvbTBCBgNVHR8EOzA5
MDegNaAzhjFodHRwczovL2FjcGV2MS5hY2VwdGEucGUvcGV2MS9jcmwvUGVydVJh
aXotVjEuY3JsMA0GCSqGSIb3DQEBCwUAA4IBAQA5RA2ztKzaEcq64VTYmtVigPgH
JJ0NKzblgtEKwBt2r0rmngd4GwXfh8aneMMQReCyRIcOF1/8EF7K6+gvclJvHgTY
F6oppbx28Ln8JWT3I5l8YfVQ8JQ1tyuQjjsriezPq5THJRpaCV1HM/+aivrrlMtT
FyF4XlhcFvR8BLxrvGO+BQmzOGwVDbQl617eUjEoh95iGGm8c2k2pcBJWkomTvtw
QqAXqhZYrCOmU4AdsZ3StQlVwp403MlOVi6XS5VYwrFoaDoBsXp7cHM7lsFhrlz/
4UqsRKUehzlcalanfacNnsP0vYo/8cfhrbmSUPRrmwYL3gGVwoUNU72VoIBc
-----END CERTIFICATE-----
```

SERIALNUMBER=20562999711, EMAILADDRESS=info@acepta.com, CN=Acepta Peru Autoridad Certificadora Electronica - V1, O=ACEPTA PERU S.A.C., C=PE

Type	CA/QC
Status	undersupervision
Status starting time	2018-08-01T16:47:28.000Z

Service digital identity (X509)

Version	3
Serial number	9
Signature algorithm	SHA256withRSA
Issuer	SERIALNUMBER=20562999711, EMAILADDRESS=info@acepta.com, CN=Acepta Peru Autoridad Certificadora Raiz - V1, O=ACEPTA PERU S.A.C., C=PE
Valid from	Wed Apr 18 10:54:31 PET 2018

Valid to	Sun Apr 18 10:54:31 PET 2038
Subject	SERIALNUMBER=20562999711, EMAILADDRESS=info@acepta.com, CN=Acepta Peru Autoridad Certificadora Electronica - V1, O=ACEPTA PERU S.A.C., C=PE
Public key	Sun RSA public key, 2048 bits modulus: 184930534051121592231416831406498226470454307810715412078964645021294056924003091235834928978077416588945879125925671024841369460327693596154025880057040616486553243899896428705193964091980283102784920695537713345660530780414590226184884881172683813130614806036452513194137525899180385777056946348298666918777676186881431742265232859983809269002336538844619466521660010956817127220618635897907739999095450623481684699324439605860772185378008759696238037587447374713266846119087035909611984930123485007581772831410652342674841407469754271796423212420041475739039947490884509955444897113420622528163960501797398999778701; public exponent: 65537
Subject key identifier	812552bdb3aa8da1fcaf59463ac9e3ac36ce6ef3
CRL distribution points	https://acpev1.acepta.pe/pev1/crl/PeruRaiz-V1.crl
Authority key identifier	0418301680147da80d687b38269de59b82489c6c73cd30e81d0c
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	30e63acc60a3f622ed7323145384ff905c5c6837
SHA256 Thumbprint	b53381a208e6eafb9f0207d4b75e352dfc1851c13dc72435fb93f0a2b0c5c008

The decoded certificate:

```
[
[
 Version: V3
 Subject: SERIALNUMBER=20562999711, EMAILADDRESS=info@acepta.com, CN=Acepta Peru Autoridad Certificadora Electronica - V1, O=ACEPTA PERU S.A.C., C=PE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
184930534051121592231416831406498226470454307810715412078964645021294056924003091235834928978077416588945879125925671024841369460327693596154025880057040616486553243899896428705193964091980283102784920695537713345660530780414590226184884881172683813130614806036452513194137525899180385777056946348298666918777676186881431742265232859983809269002336538844619466521660010956817127220618635897907739999095450623481684699324439605860772185378008759696238037587447374713266846119087035909611984930123485007581772831410652342674841407469754271796423212420041475739039947490884509955444897113420622528163960501797398999778701
 public exponent: 65537
 Validity: [From: Wed Apr 18 10:54:31 PET 2018,
             To: Sun Apr 18 10:54:31 PET 2038]
 Issuer: SERIALNUMBER=20562999711, EMAILADDRESS=info@acepta.com, CN=Acepta Peru Autoridad Certificadora Raiz - V1, O=ACEPTA PERU S.A.C., C=PE
 SerialNumber: [    09]

Certificate Extensions: 8
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 81 25 52 BD B3 AA 8D A1   FC AF 59 46 3A C9 E3 AC  .%R.......YF:...
0010: 36 CE 6E F3                                        6.n.
]
]

[2]: ObjectId: 2.5.29.18 Criticality=false
IssuerAlternativeName [
 Other-Name: Unrecognized ObjectIdentifier: 1.3.6.1.4.1.8321.2
 Other-Name: Unrecognized ObjectIdentifier: 1.3.6.1.5.5.7.8.3
 RFC822Name: info@acepta.com
]

[3]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 7D A8 0D 68 7B 38 26 9D   E5 9B 82 48 9C 6C 73 CD  ...h.8&....H.ls.
0010: 30 E8 1D 0C                                        0...
]

]

[4]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: https://acpev1.acepta.pe/pev1/crl/PeruRaiz-V1.crl]
]]

[5]: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
 Other-Name: Unrecognized ObjectIdentifier: 1.3.6.1.4.1.8321.1
 Other-Name: Unrecognized ObjectIdentifier: 1.3.6.1.5.5.7.8.3
 RFC822Name: info@acepta.com
```

```
]

[6]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [1.3.6.1.4.1.6891.1]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 2B 68 74 74 70 73 3A   2F 2F 61 63 70 65 76 31  .+https://acpev1
0010: 2E 61 63 65 70 74 61 2E   70 65 2F 43 50 53 2D 50  .acepta.pe/CPS-P
0020: 45 2D 56 31 2D 41 63 65   70 74 61 70 65           E-V1-Aceptape

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 81 D9 30 19 16 12 41   43 45 50 54 41 20 50 45  0..0...ACEPTA PE
0010: 52 55 20 53 2E 41 2E 43   2E 30 03 02 01 01 1A 81  RU S.A.C.0......
0020: BB 4C 61 20 75 74 69 6C   69 7A 61 63 69 6F 6E 20  .La utilizacion
0030: 64 65 20 65 73 74 65 20   63 65 72 74 69 66 69 63  de este certific
0040: 61 64 6F 20 65 73 74 61   20 73 75 6A 65 74 61 20  ado esta sujeta
0050: 61 20 6C 61 73 20 70 6F   6C 69 74 69 63 61 73 20  a las politicas
0060: 64 65 20 63 65 72 74 69   66 69 63 61 64 6F 20 28  de certificado (
0070: 43 50 29 20 79 20 70 72   61 63 74 69 63 61 73 20  CP) y practicas
0080: 64 65 20 63 65 72 74 69   66 69 63 61 63 69 6F 6E  de certificacion
0090: 20 28 43 50 53 29 20 65   73 74 61 62 6C 65 63 69   (CPS) estableci
00A0: 64 61 73 20 70 6F 72 20   41 63 65 70 74 61 2C 20  das por Acepta,
00B0: 79 20 64 69 73 70 6F 6E   69 62 6C 65 73 20 70 75  y disponibles pu
00C0: 62 6C 69 63 61 6D 65 6E   74 65 20 65 6E 20 77 77  blicamente en ww
00D0: 77 2E 61 63 65 70 74 61   2E 70 65 2E              w.acepta.pe.

]]  ]
]

[7]: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[8]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: A7 3A 2E 82 46 D0 A4 B0   0F 0E 09 DE ED DB 32 28  .:..F.........2(
0010: 94 FA CA 67 2D 03 ED BD   4C B6 25 9C 48 70 94 F4  ...g-...L.%.Hp..
0020: 3F F4 12 5D 82 90 18 6C   EB E9 4B BB 6E 97 00 8A  ?..]...l..K.n...
0030: 7F 1D D7 14 B8 16 1C 3D   DD B4 83 A6 A5 9D DC 31  .......=.......1
0040: D7 32 D6 D3 91 EB 44 8C   E7 AD 7B 0F D6 62 45 1E  .2....D......bE.
0050: 81 37 C5 C5 2C 4E 81 82   B1 D6 DF 4B 1C 68 69 91  .7..,N.....K.hi.
0060: 4D AC 2C F6 6B 71 BF A8   15 5D 9E 47 29 8E 66 43  M.,.kq...].G).fC
0070: FE 91 D9 5B 75 64 51 DB   73 4B 17 F9 3B C9 E2 4A  ...[udQ.sK..;..J
0080: 43 92 39 F6 3C 1E 4A A0   14 DC 53 08 E9 91 22 A6  C.9.<.J...S...".
0090: 47 B6 AC D3 23 52 0B 49   BF FB 89 E4 5E 41 A6 4B  G...#R.I....^A.K
00A0: 1A 5C C5 C7 02 7C AA 66   DC 75 E1 AC CE 91 34 78  .\.....f.u....4x
00B0: 99 6A 0E 9F 00 60 BF 82   76 CA 8B 00 5B CD F5 52  .j...`..v...[..R
00C0: E6 B9 42 D9 C0 30 E1 32   F5 A2 3D 0E 0E 42 94 28  ..B..0.2..=..B.(
00D0: 84 B3 8F BC 16 5F 4A AA   A2 E7 E7 52 BE 7A 51 72  ....._J....R.zQr
00E0: 23 27 A7 A7 36 89 1B B6   76 9C 77 47 62 C1 EE C9  #'..6...v.wGb...
00F0: E0 DE B8 C0 EB E4 CD D2   34 3C BC A7 43 0A B4 07  ........4<..C...

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGXTCCBUWgAwIBAgIBCTANBgkqhkiG9w0BAQsFADCBmDELMAkGA1UEBhMCUEUx
GzAZBgNVBAoTEkFDRVBUQSBQRVJVIFMuQS5DLjE2MDQGA1UEAxMtQWNlcHRhIFBl
cnUgQXV0b3JpZGFkIENlcnRpZmljYWRvcmEgUmFpeiAtIFYxMR4wHAYJKoZIhvcN
AQkBFg9pbmZvQGFjZXB0YS5jb20xFDASBgNVBAUTCzIwNTYyOTk5NzExMB4XDTE4
MDQxODE1NTQzMVoXDTM4MDQxODE1NTQzMVowgZ8xCzAJBgNVBAYTAlBFMRswGQYD
VQQKExJBQ0VQVEEgUEVSVSBTLkEuQy4xPTA7BgNVBAMTNEFjZXB0YSBQZXJ1IEF1
dG9yaWRhZCBDZXJ0aWZpY2Fkb3JhIEVsZWN0cm9uaWNhIC0gVjExHjAcBgkqhkiG
9w0BCQEWD2luZm9AYWNlcHRhLmNvbTEUMBIGA1UEBRMLMjA1NjI5OTk3MTEwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCSfkJum7sbyuOB0lvnwrjtpzlO
SjxY0xoCYpjwsq6KBagBbUYQYZFbrtWTQXMFHPASREC+lHu2mdNcAgTFQbl4oMmX
0lwaT65H8Vu/7oiwHiVh9lc9uExz/fAjP1mto+J8Sfmt6iqCnpU5rdTWTHiIOtMQ
apTTd2P9t4d0v7/M/30fBiaLXR1DM+JJ1iYbOhEqIMKHBQh6VZZH8wWRSFiAMiZI
EIrblXgtuuoEFigICU6PyTyMtOgZeVclLGD7ULNxjNK1EJ9A7Kren1ZdUy7/0PPn
zBJ5O/Od6hbgNBPJUbTDedMP7t07RVcWNHLwcUbTtnFddftadyPcO60vonzbAgMB
AAGjggKnMIICozAPBgNVHRMBAf8EBTADAQH/MB8GA1UdIwQYMBaAFH2oDWh7OCad
5ZuCSJxsc80w6B0MMB0GA1UdDgQWBBSBJVK9s6qNofyvWUY6yeOsNs5u8zALBgNV
HQ8EBAMCAQYwggFBBgNVHSAEggE4MIIBNDCCATAGCCsGAQQBtWsBMIIBIjA3Bggr
BgEFBQcCARYraHR0cHM6Ly9hY3BldjEuYWNlcHRhLnBlL0NQUy1QRS1WMS1BY2Vw
dGFwZTCB5gYIKwYBBQUHAgIwgdkwGRYSQUNFUFRBIFBFUlUgUy5BLkMuMAMCAQEa
gbtMYSB1dGlsaXphY2lvbiBkZSBlc3RlIGNlcnRpZmljYWRvIGVzdGEgc3VqZXRh
IGEgbGFzIHBvbGl0aWNhcyBkZSBjZXJ0aWZpY2FkbyAoQ1ApIHkgcHJhY3RpY2Fz
IGRlIGNlcnRpZmljYWNpb24gKENQUykgZXN0YWJsZWNpZGFzIHBvciBBY2VwdGEs
IHkgZGlzcG9uaWJsZXMgcHVibGljYW1lbnRlIGVuIHd3dy5hY2VwdGEucGUuMFwG
A1UdEgRVMFOgGQYIKwYBBAHBAQKgDRYLMjA1NjI5OTk3MTGgJQYIKwYBBQUHCAOg
GTAXDAsyMDU2Mjk5OTcxMQYIKwYBBAHBAQKBD2luZm9AYWNlcHRhLmNvbTBcBgNV
HREEVTBToBkGCCsGAQQBwQEBoA0WCzIwNTYyOTk5NzExoCUGCCsGAQUFBwgDoBkw
FwwLMjA1NjI5OTk3MTEGCCsGAQQBwQECgQ9pbmZvQGFjZXB0YS5jb20wQgYDVR0f
```

BDswOTA3oDWgM4YxaHR0cHM6Ly9hY3BldjEuYWNlcHRhLnBlL3BldjEvY3JsL1Bl
cnVSYWl6LVYxLmNybDANBgkqhkiG9w0BAQsFAAOCAQEApzougkbQpLAPDgne7dsy
KJT6ymctA+29TLYlnEhwlPQ/9BJdgpAYbOvpS7tulwCKfx3XFLgWHD3dtIOmpZ3c
Mdcy1tOR60SM5617D9ZiRR6BN8XFLE6BgrHW30scaGmRTaws9mtxv6gVXZ5HKY5m
Q/6R2Vt1ZFHbc0sX+TvJ4kpDkjn2PB5KoBTcUwjpkSKmR7as0yNSC0m/+4nkXkGm
SxpcxccCfKpm3HXhrM6RNHiZag6fAGC/gnbKiwBbzfVS5rlC2cAw4TL1oj0ODkKU
KISzj7wWX0qqoufnUr56UXIjJ6enNokbtnacd0diwe7J4N64wOvkzdI0PLynQwq0
Bw==
-----END CERTIFICATE-----

SERIALNUMBER=20562999711, EMAILADDRESS=info@acepta.com, CN=Acepta Peru Autoridad Certificadora Raiz - V1, O=ACEPTA PERU S.A.C., C=PE

Type	CA/QC
Status	undersupervision
Status starting time	2018-06-15T21:39:40.000Z

Service digital identity (X509)

Version	3
Serial number	1
Signature algorithm	SHA256withRSA
Issuer	SERIALNUMBER=20562999711, EMAILADDRESS=info@acepta.com, CN=Acepta Peru Autoridad Certificadora Raiz - V1, O=ACEPTA PERU S.A.C., C=PE
Valid from	Wed Apr 18 10:54:31 PET 2018
Valid to	Sun Apr 18 10:54:31 PET 2038
Subject	SERIALNUMBER=20562999711, EMAILADDRESS=info@acepta.com, CN=Acepta Peru Autoridad Certificadora Raiz - V1, O=ACEPTA PERU S.A.C., C=PE
Public key	Sun RSA public key, 2048 bits modulus: 22674885644285035646123794701449581437349587151647546292805853283769739 89603929078139656941655943685546504100191871056771315700633655062383515 21952553965340384022962892617759619168139615691148076411456637182955818 91966566590457575801055172032094936158643730545987980309028354924965466 86829488396613673860258851060659874596616196533443095049866952406522722 08950536850689996872109470728742158470554872003821260660313637995635989 32190593739290424007829443831476217936281550083471593961314784218803680 92103296517608334363056430700499945584747630349396292777671359365240512 71643013494119170460333526194738270841509116889 33 public exponent: 65537
Subject key identifier	7da80d687b38269de59b82489c6c73cd30e81d0c
Authority key identifier	0418301680147da80d687b38269de59b82489c6c73cd30e81d0c
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	48dbd2eb7e631652dac4e01c2cfd85d5ad3dc10a
SHA256 Thumbprint	1565ec78a6fac8eb25be95b1d9887711cfb861206e3b52f781a5708d47656e7e

The decoded certificate:

```
[
[
 Version: V3
 Subject: SERIALNUMBER=20562999711, EMAILADDRESS=info@acepta.com, CN=Acepta Peru Autoridad Certificadora Raiz - V1, O=ACEPTA PERU S.A.C., C=PE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
22674885644285035646123794701449581437349587151647546292805853283769739896039290781396569416559436855465041001918710567713157006336550623835152195255396534038402296289261775961916813961569114807641145663718295581891966566590457575801055172032094936158643730545987980309028354924965466864829488396613673860258851060659874596616196533443095049866952406522722089505368506899968721094707287421584705548720038212606603136379956359893219059373929042400782944383147621793628155008347159396131478421880368092103296517608334363056430700499945584747630349396292777671359365240512716430134941191704603335261947382708415091168893340765227220895053685068999687210947072874215847055487200382126066031363799563598932190593739290424007829443831476217936281550083471593961314784218803680921032965176083343630564307004999455847476303493962927776713593652405127164301349411917046033352619473827084150911688933
 public exponent: 65537
 Validity: [From: Wed Apr 18 10:54:31 PET 2018,
             To: Sun Apr 18 10:54:31 PET 2038]
 Issuer: SERIALNUMBER=20562999711, EMAILADDRESS=info@acepta.com, CN=Acepta Peru Autoridad Certificadora Raiz - V1, O=ACEPTA PERU S.A.C., C=PE
 SerialNumber: [    01]

Certificate Extensions: 7
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 7D A8 0D 68 7B 38 26 9D   E5 9B 82 48 9C 6C 73 CD  ...h.8&....H.ls.
0010: 30 E8 1D 0C                                        0...
```

```
]
]

[2]: ObjectId: 2.5.29.18 Criticality=false
IssuerAlternativeName [
 Other-Name: Unrecognized ObjectIdentifier: 1.3.6.1.4.1.8321.2
 Other-Name: Unrecognized ObjectIdentifier: 1.3.6.1.5.5.7.8.3
 RFC822Name: info@acepta.com
]

[3]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 7D A8 0D 68 7B 38 26 9D   E5 9B 82 48 9C 6C 73 CD  ...h.8&....H.ls.
0010: 30 E8 1D 0C                                        0...
]

]

[4]: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
 Other-Name: Unrecognized ObjectIdentifier: 1.3.6.1.4.1.8321.1
 Other-Name: Unrecognized ObjectIdentifier: 1.3.6.1.5.5.7.8.3
 RFC822Name: info@acepta.com
]

[5]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [1.3.6.1.4.1.6891.1]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 2B 68 74 74 70 73 3A   2F 2F 61 63 70 65 76 31  .+https://acpev1
0010: 2E 61 63 65 70 74 61 2E   70 65 2F 43 50 53 2D 50  .acepta.pe/CPS-P
0020: 45 2D 56 31 2D 41 63 65   70 74 61 70 65           E-V1-Aceptape

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 81 D9 30 19 16 12 41   43 45 50 54 41 20 50 45  0..0...ACEPTA PE
0010: 52 55 20 53 2E 41 2E 43   2E 30 03 02 01 01 1A 81  RU S.A.C.0......
0020: BB 4C 61 20 75 74 69 6C   69 7A 61 63 69 6F 6E 20  .La utilizacion
0030: 64 65 20 65 73 74 65 20   63 65 72 74 69 66 69 63  de este certific
0040: 61 64 6F 20 65 73 74 61   20 73 75 6A 65 74 61 20  ado esta sujeta
0050: 61 20 6C 61 73 20 70 6F   6C 69 74 69 63 61 73 20  a las politicas
0060: 64 65 20 63 65 72 74 69   66 69 63 61 64 6F 20 28  de certificado (
0070: 43 50 29 20 79 20 70 72   61 63 74 69 63 61 73 20  CP) y practicas
0080: 64 65 20 63 65 72 74 69   66 69 63 61 63 69 6F 6E  de certificacion
0090: 20 28 43 50 53 29 20 65   73 74 61 62 6C 65 63 69   (CPS) estableci
00A0: 64 61 73 20 70 6F 72 20   41 63 65 70 74 61 2C 20  das por Acepta,
00B0: 79 20 64 69 73 70 6F 6E   69 62 6C 65 73 20 70 75  y disponibles pu
00C0: 62 6C 69 63 61 6D 65 6E   74 65 20 65 6E 20 77 77  blicamente en ww
00D0: 77 2E 61 63 65 70 74 61   2E 70 65 2E              w.acepta.pe.

]]  ]
]

[6]: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[7]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 8F B4 D3 D9 69 A7 C5 0F   7B 35 4A 49 71 7A 03 99  ....i....5JIqz..
0010: 78 7F 60 4F FF E9 3A 5A   07 2E 9A 11 95 D4 C9 74  x.`O..:Z.......t
0020: 05 76 A6 0B D7 3A 16 16   B4 90 E6 CD 27 C1 6F 59  .v...:......'.oY
0030: D5 A5 46 11 23 9C B2 4F   C0 2B D6 50 A0 C1 EF 9B  ..F.#..O.+.P....
0040: C5 13 72 7F 8D B5 E9 C7   3C 8A 9C 4B 6B 48 F1 A0  ..r.....<..KkH..
0050: EB 6D CD 0E 64 CA EA 1B   44 39 FC F6 7E DF 98 03  .m..d...D9......
0060: F2 93 0F 6D 6C A6 1B B4   B7 84 F7 B9 1B 73 33 90  ...ml........s3.
0070: A2 97 58 84 88 68 AF F9   3F 46 1F 7F 92 8B 56 33  ..X..h..?F....V3
0080: E0 96 22 C6 94 01 C2 8B   D7 AC B4 88 B7 0A 14 52  .."............R
0090: DD 3D 22 DB 49 E5 F6 21   2C 9E 39 16 CC 01 8F CA  .="."I..!,.9.....
00A0: B5 C2 42 A1 0A F2 DF 06   A2 0C 89 86 C9 FA 4F 42  ..B..........OB
00B0: 21 A3 D2 01 3F E2 1E 3E   8C 05 7F C6 39 7E C6 98  !...?..>....9...
00C0: 2A F2 56 AC 6D D7 06 03   6D F9 D4 D9 08 E0 29 71  *.V.m...m.....)q
00D0: 8F 06 30 A5 E3 39 36 17   F0 56 81 C5 C6 90 A5 34  ..0..96..V.....4
00E0: 2E FC C6 33 26 14 24 52   73 C8 6E 46 12 22 DB 3C  ...3&.$Rs.nF.".<
00F0: DD 04 CD DD 47 53 8A 77   07 91 47 1B B5 3A 21 5C  ....GS.w..G..:!\

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGEjCCBPqgAwIBAgIBATANBgkqhkiG9w0BAQsFADCBmDELMAkGA1UEBhMCUEUx
GzAZBgNVBAoTEkFDRVBUQSBQRVJVIFMuQS5DLjE2MDQGA1UEAxMtQWNlcHRhIFBl
cnUgQXV0b3JpZGFkIENlcnRpZmljYWRvcmEgUmFpeiAtIFYxMR4wHAYJKoZIhvcN
```

AQkBFg9pbmZvQGFjZXB0YS5jb20xFDASBgNVBAUTCzIwNTYyOTk5NzExMB4XDTE4
MDQxODE1NTQzMVoXDTM4MDQxODE1NTQzMVowgZgxCzAJBgNVBAYTAlBFMRswGQYD
VQQKExJBQ0VQVEEgUEVSVSBTLkEuQy4xNjA0BgNVBAMTLUFjZXB0YSBQZXJ1IEF1
dG9yaWRhZCBDZXJ0aWZpY2Fkb3JhIFJhaXogLSBWMTEeMBwGCSqGSIb3DQEJARYP
aW5mb0BhY2VwdGEuY29tMRQwEgYDVQQFEwsyMDU2Mjk5OTcxMTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBALOepDt69KarS0vKlKpv08eMmuhedC8P9cr0
/1fcZWwTw7ODNRI06MZc6JgeVAwLeXdtelwvQyls6Nkc0jeNX5IK2dQXM///rs+D
5X2iqHkrn2QupUr5ljnJdmog8FSIiKgeQkccvFimg7Wmv/AwBzM8vlxRrgXz9nEL
gfUcErHPZN+pkxt51OXB1R3cn52KlCO0vkw4l6Rjz9n//RsYQVUvjm9Xmc9z3svF
r300FC67TG21/HrUEEWQd66uU1+A+H+hbFCv5H+XPun9u9a8TtP8QKnpcD/Igy7M
PNU9SMnSnBda46yiFGJAc6rSUqoHF1/43hKXi07keWEsuZMWYOUCAwEAAaOCAmMw
ggJfMA8GA1UdEwEB/wQFMAMBAf8wHwYDVR0jBBgwFoAUfagNaHs4Jp3lm4JInGxz
zTDoHQwwHQYDVR0OBBYEFH2oDWh7OCad5ZuCSJxsc80w6B0MMAsGA1UdDwQEAwIB
BjCCAUEGA1UdIASCATgwggE0MIIBMAYIKwYBBAG1awEwggEiMDcGCCsGAQUFBwIB
FitodHRwczovL2FjcGV2MS5hY2VwdGEucGUvQ1BTLVBFLVYxLUFjZXB0YXBlMIHm
BggrBgEFBQcCAjCB2TAZFhJBQ0VQVEEgUEVSVSBTLkEuQy4wAwIBARqBu0xhIHV0
aWxpemFjaW9uIGRlIGVzdGUgY2VydGlmaWNhZG8gZXN0YSBzdWpldGEgYSBsYXMg
cG9saXRpY2FzIGRlIGNlcnRpZmljYWRvIChDUCkgeSBwcmFjdGljYXMgZGUgY2Vy
dGlmaWNhY2lvbiAoQ1BTKSBlc3RhYmxlY2lkYXMgcG9yIEFjZXB0YSwgeSBkaXNw
b25pYmxlcyBwdWJsaWNhbWVudGUgZW4gd3d3LmFjZXB0YS5wZS4wXAYDVR0SBFUw
U6AZBggrBgEEAcEBAqANFgsyMDU2Mjk5OTcxMaAlBggrBgEFBQcIA6AZMBcMCzIw
NTYyOTk5NzExBggrBgEEAcEBAoEPaW5mb0BhY2VwdGEuY29tMFwGA1UdEQRVMFOg
GQYIKwYBBAHBAQGgDRYLMjA1NjI5OTk3MTGgJQYIKwYBBQUHCAOgGTAXDAsyMDU2
Mjk5OTcxMQYIKwYBBAHBAQKBD2luZm9AYWNlcHRhLmNvbTANBgkqhkiG9w0BAQsF
AAOCAQEAj7TT2WmnxQ97NUpJcXoDmXh/YE//6TpaBy6aEZXUyXQFdqYL1zoWFrSQ
5s0nwW9Z1aVGESOcsk/AK9ZQoMHvm8UTcn+NtenHPIqcS2tI8aDrbc0OZMrqG0Q5
/PZ+35gD8pMPbWymG7S3hPe5G3MzkKKXWISIaK/5P0Yff5KLVjPgliLGlAHCi9es
tIi3ChRS3T0i20nl9iEsnjkWzAGPyrXCQqEK8t8GogyJhsn6T0Iho9IBP+IePowF
f8Y5fsaYKvJWrG3XBgNt+dTZCOApcY8GMKXjOTYX8FaBxcaQpTQu/MYzJhQkUnPI
bkYSIts83QTN3UdTincHkUcbtTohXA==
-----END CERTIFICATE-----

Certificate Service Provider Name (en): CORE ANDINA GROUP S.A.C.

Trade name (en)	CORE ANDINA GROUP S.A.C.
Information URI (en)	HTTPS://COREDOPERU.CERTISIGN.COM.PE
Service provider street address (es)	JR. NARCISO DE LA COLINA NRO. 421 INT. 1201
Service provider street address (en)	JR. NARCISO DE LA COLINA NRO. 421 INT. 1201
Service provider postal code (es)	15074
Service provider postal code (en)	15074
Service provider locality (es)	MIRAFLORES
Service provider locality (en)	MIRAFLORES
Service provider state (es)	LIMA
Service provider state (en)	LIMA
Service provider country (es)	PE
Service provider country (en)	PE

CN=Certisign Application CA, O=Certisign Certificadora Digital S.A., C=BR

Type	CA/QC
Status	undersupervision
Status starting time	2018-06-27T14:56:46.000Z

Service digital identity (X509)

Version	3
Serial number	6216629776151424254
Signature algorithm	SHA512withRSA
Issuer	CN=Certisign Root CA, O=Certisign Certificadora Digital S.A., C=BR
Valid from	Tue Apr 14 22:00:00 PET 2015
Valid to	Sat Apr 13 22:00:00 PET 2030

Subject	CN=Certisign Application CA, O=Certisign Certificadora Digital S.A., C=BR
Public key	Sun RSA public key, 4096 bits modulus: 78907298955084947665559750637111680047273484546847393864407044576147541 29793985306683520615200129355415533942015383729879414179231608916721009 78038981909646003110266184009658834161110638245801201459492227952584309 37009853285741511273469227395387233933402847285629727064028364554469568 83008261540988949746833318362081052093444983003966169284433806288318792 57504127643615153100970822933326008708787194361239880858656215399898070 62078802648474747825067566488308084257720740392069003447672893592752622 80509693560287676105347529235327648968241798484964872839245208358739755 68823221491470991312408174513062517974776641017321598995911773754508949 93372942429411494169176969753513012420204607051793450183585866423371441 80351140176042082602038636616847259246196677126977063610319290610892121 33484490466482072836205990675614512222518500489222911293319477422878048 22491646653959637404570329715733972792330109970178519938112364977577414 44133400587551206869215235579969135048500220981966973784153005292370555 80018220752255057626969340991473403823393268152095789870285904811786045 12334901089347926492651024529873183399634371294321778738696297667981363 73298649872527598164072452139943630883717248982984307573473756101542613 1125983033858263738231901 public exponent: 65537
Subject key identifier	b8751e3144670322e68b689518ab822956fd8be7
CRL distribution points	http://certisign-ca.certisign.com.br/repositorio/lcr/CertisignRootCA/LatestCRL.crl
Authority key identifier	0418301680148ba6cea547d11b8c8b9d1959725cab3bb534141f
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	8beba16e51889b029f14ccfa03cb33c1f70e4477
SHA256 Thumbprint	55f1b5af8b10b135394f3372fc8e81d862484fa6d481e6b0ac77c16d420e8759

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=Certisign Application CA, O=Certisign Certificadora Digital S.A., C=BR
 Signature Algorithm: SHA512withRSA, OID = 1.2.840.113549.1.1.13

 Key:  Sun RSA public key, 4096 bits
 modulus:
78907298955084947665559750637111680047273484546847393864407044576147541297939853066835206152001293554155339420153837298794141792316089167210097803898190964600311026618400965
88341611106382458012014594922279525843093700985328574151127346922739538723393340284728562972706402836455446956883008261540988949746833318362081052093444983003966169284433806
28831879257504127643615153100970822933326008708787194361239880858656215399898070620788026484747478250675664883080842577207403920690034476728935927526228050969356028767610534
75292353276489682417984849648728392452083587397556882322149147099131240817451306251797477664101732159899591177375450894993372942429411494169176969753513012420204607051793450
18358586642337144180351140176042082602038636616847259246196677126977063610319290610892121334844904664820728362059906756145122225185004892229112933194774228780482249164665395
96374045703297157339727923301099701785199381123649775774144413340058755120686921523557996913504850022098196697378415300529237055580018220752255057626969340991473403823393268
15209578987028590481178604512334901089347926492651024529873183399634371294321778738696297667981363732986498725275981640724521399436308837172489829843075734737561015426131125
9830338582637382311901
 public exponent: 65537
 Validity: [From: Tue Apr 14 22:00:00 PET 2015,
             To: Sat Apr 13 22:00:00 PET 2030]
 Issuer: CN=Certisign Root CA, O=Certisign Certificadora Digital S.A., C=BR
 SerialNumber: [    5645e7d8 239f2cfe]

Certificate Extensions: 7
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: B8 75 1E 31 44 67 03 22   E6 8B 68 95 18 AB 82 29  .u.1Dg."..h....)
0010: 56 FD 8B E7                                        V...
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 8B A6 CE A5 47 D1 1B 8C   8B 9D 19 59 72 5C AB 3B  ....G......Yr\.;
0010: B5 34 14 1F                                        .4..
]

]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://certisign-ca.certisign.com.br/repositorio/lcr/CertisignRootCA/LatestCRL.crl]
]]
```

```
[4]: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
 OCSPSigning
 clientAuth
 codeSigning
 timeStamping
]

[5]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[6]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [1.3.6.1.4.1.30253.7]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 34 68 74 74 70 3A 2F   2F 63 65 72 74 69 73 69  .4http://certisi
0010: 67 6E 2D 63 61 2E 63 65   72 74 69 73 69 67 6E 2E  gn-ca.certisign.
0020: 63 6F 6D 2E 62 72 2F 72   65 70 6F 73 69 74 6F 72  com.br/repositor
0030: 69 6F 2F 63 70 73                                  io/cps

]]  ]
]

[7]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA512withRSA]
 Signature:
0000: B7 8C 4C AF 11 5A CB 05   A9 75 E5 1A 0F 38 4C 25  ..L..Z...u...8L%
0010: C6 4A 09 2E 05 3D FD D2   86 1C CA C9 C1 EB 81 24  .J...=.........$
0020: 8E 29 6E CE 44 CC 0C 58   5F 43 A6 CD C7 3D 8D D1  .)n.D..X_C...=..
0030: A5 20 73 3D 6D CD 41 74   A4 11 1E 6F 1E F0 C5 E8  . s=m.At...o....
0040: B2 08 25 38 9E 21 CC 30   C3 82 BE 4E 9C 48 A2 77  ..%8.!.0...N.H.w
0050: C2 55 46 80 8F E4 7B 56   7B AC F1 4D 44 F9 11 E1  .UF....V...MD...
0060: FB 13 F7 39 A9 71 5D F2   1F 4A CC F2 85 52 A6 2F  ...9.q]..J...R./
0070: D4 C5 F6 02 10 19 EC 47   1A 6A D8 DA DE 88 19 4C  .......G.j.....L
0080: C7 71 9C E2 BD EE 6E D9   52 63 EF DC 5A 02 76 2F  .q....n.Rc..Z.v/
0090: 69 43 AE 79 4E F7 CC 10   62 05 68 2E F9 88 65 60  iC.yN...b.h...e`
00A0: E1 03 23 F7 C0 84 46 DB   79 C0 EB 0B 0F 08 7A 41  ..#...F.y.....zA
00B0: 84 B9 D4 0D 83 DB BA 9E   C7 8F EE DF 98 3A F7 D6  .............:..
00C0: 8B A4 FF FD 30 A6 5C 72   A8 92 35 D5 85 DD 90 3B  ....0.\r..5....;
00D0: FA 2E EB E5 AC 97 E9 C9   BE 0E 81 E4 02 BE C7 14  ................
00E0: 82 6A 90 1A EF DC FF 56   C7 A6 E1 38 49 DB 83 77  .j.....V...8I..w
00F0: C2 C4 79 9B 87 87 E2 2C   6B 81 69 9C B4 08 54 0B  ..y....,k.i...T.
0100: 1A E5 1A 29 4E B8 EF 57   87 A0 E7 B7 21 85 56 32  ...)N..W....!.V2
0110: C6 29 0C 22 8D 58 EF EE   65 DF 82 23 0E B5 29 33  .).".X..e..#..)3
0120: 92 03 61 6E D2 E4 48 5E   F4 1A F0 88 5C BE 8C D5  ..an..H^....\...
0130: 0B EA 65 29 8A A8 67 2E   76 00 BF EA 88 6E A6 A4  ..e)..g.v....n..
0140: 2A 16 0A 4E 07 54 E5 7C   2C 22 EE 78 7B BB CC F3  *..N.T..,".x....
0150: 4C AD 50 9E 40 D1 3E 80   4F 6A 4F DF BA 3F 61 49  L.P.@.>.OjO..?aI
0160: AD 3A 1A 6E 00 51 89 96   37 F9 C1 4B EA 34 37 D3  .:.n.Q..7..K.47.
0170: 9B 58 DE 1A 11 C1 59 E7   9A 63 76 09 1D 55 6B 39  .X....Y..cv..Uk9
0180: FF 46 46 10 E0 1C C6 3F   4A 21 F5 58 94 C8 E4 42  .FF....?J!.X...B
0190: DC 8D B5 2F 3E 6C EF 70   A7 2A 59 F2 A6 5C 65 C8  .../>l.p.*Y..\e.
01A0: 2C C2 2C FE A4 E7 D8 17   4C A9 13 A2 73 E6 A9 C5  ,.,.....L...s...
01B0: 84 7E CD 06 39 ED 4B 76   16 BF D1 3B 02 90 9E 5A  ....9.Kv...;...Z
01C0: 32 85 8E 5A 5C 41 BA C6   96 7B 82 37 10 51 C4 07  2..Z\A.....7.Q..
01D0: 25 7A 03 64 31 47 27 61   1C F9 60 4C 41 06 B5 17  %z.d1G'a..`LA...
01E0: DF 6C 3F C3 CE E3 0B E5   15 CD C2 E5 82 B3 14 29  .l?............)
01F0: F2 10 01 BB 88 39 C7 29   15 F0 BB BB BC 0A 83 E9  .....9.).........

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGlDCCBHygAwIBAgIIVkXn2COfLP4wDQYJKoZIhvcNAQENBQAwWDELMAkGA1UE
BhMCQlIxLTArBgNVBAoTJENlcnRpc2lnbiBDZXJ0aWZpY2Fkb3JhIERpZ2l0YWwg
Uy5BLjEaMBgGA1UEAxMRQ2VydGlzaWduIFJvb3QgQ0EwHhcNMTUwNDE1MDMwMDAw
WhcNMzAwNDE0MDMwMDAwWjBfMQswCQYDVQQGEwJCUjEtMCsGA1UEChMkQ2VydGlz
aWduIENlcnRpZmljYWRvcmEgRGlnaXRhbCBTLkEuMSEwHwYDVQQDExhDZXJ0aXNp
Z24gQXBwbGljYXRpb24gQ0EwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoIC
AQDBasgbndTYOZ05QhPh8swH0Uo1gHQwuQvM7HnKhEwmAwAoQApvyEfi5RNb1/z0
iuU9QPhmJhuLy9+C2ubf4Zw5P9UFvewN42Yx+g/vKoZH9t5Z+cfTvg5NrOrPobCz
2CSSuSpepjwlLT56mxpt9v3dHdL0JtsXt/pxfWYJS5qmKYdmhmyS+HKrtXIOuC5b
qLtdGHMSBnidLVL23N07FKJ8HQ2KbkMQSzK7xFb6U9tpj/c5xrPcj0bWa3xiIqXR
v6zhmhrLDpv/FVpfjpjbGSrrJZ21PcDuxtfGeIwZBe96tfs4z1plBljZcYU1+T9U
b6ti6T24ghNXzjvuy4//ZsOWnSstz4RV36g4+k7Md2w6zznIM9mkpKvm0poT0kj4
fcD5f9vJiXKt9tKBxWjcQCyyzDYtMr5jC/tzJIeLUR3pwFKqgyVeWdl2Pn3tNJee
QtZh+7OSWHquIPuVzi/fMEDFcN+Iqy/xv4DCpRs9jKrFUqIqBb4pntCe0Cn/qNNm
2iuIX8xUKbpZU+Q+IKbT8tfJIybTussxce7Tiusym31jTr1R6aru0jRBzw98VyTq
9VvyQHNRfPLerrEbqbWfRY6lFKT9KxLFYcN+JzvReNO2+G6zQc66/ck8p7LWi6bS
LFkRoXblGsidrKZn7f2vJ5hiBGNUq+Fb+BHDQgA79WGf3QIDAQABo4IBWTCCAVUw
DwYDVR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBSLps6lR9EbjIudGVlyXKs7tTQU
HzAdBgNVHQ4EFgQUuHUeMURnAyLmi2iVGKuCKVb9i+cwWgYDVR0gBFMwUTBPBgkr
BgEEAYHsLQcwQjBABggrBgEFBQcCARY0aHR0cDovL2NlcnRpc2lnbi1jYS5jZXJ0
```

aXNpZ24uY29tLmJyL3JlcG9zaXRvcmlvL2NwczBjBgNVHR8EXDBaMFigVqBUhlJo
dHRwOi8vY2VydGlzaWduLWNhLmNlcnRpc2lnbi5jb20uYnIvcmVwb3NpdG9yaW8v
bGNyL0NlcnRpc2lnblJvb3RDQS9MYXRlc3RDUkwuY3JsMA4GA1UdDwEB/wQEAwIB
BjAxBgNVHSUEKjAoBggrBgEFBQcDCQYIKwYBBQUHAwIGCCsGAQUFBwMDBggrBgEF
BQcDCDANBgkqhkiG9w0BAQ0FAAOCAgEAt4xMrxFaywWpdeUaDzhMJcZKCS4FPf3S
hhzKycHrgSSOKW7ORMwMWF9Dps3HPY3RpSBzPW3NQXSkER5vHvDF6LIIJTieIcww
w4K+TpxIonfCVUaAj+R7Vnus8U1E+RHh+xP3OalxXfIfSszyhVKmL9TF9gIQGexH
GmrY2t6IGUzHcZzive5u2VJj79xaAnYvaUOueU73zBBiBWgu+YhlYOEDI/fAhEbb
ecDrCw8IekGEudQNg9u6nseP7t+YOvfWi6T//TCmXHKokjXVhd2QO/ou6+Wsl+nJ
vg6B5AK+xxSCapAa79z/Vsem4ThJ24N3wsR5m4eH4ixrgWmctAhUCxrlGilOuO9X
h6DntyGFVjLGKQwijVjv7mXfgiMOtSkzkgNhbtLkSF70GvCIXL6M1QvqZSmKqGcu
dgC/6ohupqQqFgpOB1TlfCwi7nh7u8zzTK1QnkDRPoBPak/fuj9hSa06Gm4AUYmW
N/nBS+o0N9ObWN4aEcFZ55pjdgkdVWs5/0ZGEOAcxj9KIfVYlMjkQtyNtS8+bO9w
pypZ8qZcZcgswiz+pOfYF0ypE6Jz5qnFhH7NBjntS3YWv9E7ApCeWjKFjlpcQbrG
lnuCNxBRxAclegNkMUcnYRz5YExBBrUX32w/w87jC+UVzcLlgrMUKfIQAbuIOccp
FfC7u7wKg+k=
-----END CERTIFICATE-----

CN=Certisign Root CA, O=Certisign Certificadora Digital S.A., C=BR

Type	CA/QC
Status	undersupervision
Status starting time	2018-06-26T20:54:33.000Z

Service digital identity (X509)

Version	3
Serial number	8496730048626051985
Signature algorithm	SHA512withRSA
Issuer	CN=Certisign Root CA, O=Certisign Certificadora Digital S.A., C=BR
Valid from	Tue Apr 14 22:00:00 PET 2015
Valid to	Sun Apr 14 22:00:00 PET 2030
Subject	CN=Certisign Root CA, O=Certisign Certificadora Digital S.A., C=BR
Public key	Sun RSA public key, 4096 bits modulus: 838581495727241538791479293555239809897343214758597498890250772134382012652488417060641400394683897528297344133916636665969425472487828769033674619340229210019038411557207353988428020514146059990415173356285194019897255430297354813503205682934644048136379610031647285811138251150679415446400087425463638353870508433217003601893787901159569082836654688379442238984855385231401082187574319605112793969098253082696258163595003930445061950654069738669798344653576001863172995311200598895649547781379060799393531790322593111555129456150836683209648138553001874886823375897094509231461436751145038654845132484221730531887066468315315900133713176878495087742466068582159983716526844510815691937296039489667370036617311657486903475207500048185705560313300472051511818534083028759148911121731446254498831643125678570838959058891513879770747968424374849154186072949379467148026357106147636558915764658360798432495985381452975120829238150529696652139150186218075610218147641903003491674572883765315997662348670149550479538217376609894907505134206162584771350820191765432142729586009581569966939449508702375617081931621572274290186400962622738506471676193149936968223696357741356225487891807728322738157803728856435994837185278097707227421 public exponent: 65537
Subject key identifier	8ba6cea547d11b8c8b9d1959725cab3bb534141f
CRL distribution points	http://certisign-ca.certisign.com.br/repositorio/lcr/CertisignRootCA/LatestCRL.crl
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	fea8693e1f236ea1fe915b7da13211db4d48454c
SHA256 Thumbprint	c5056b845d6cbdcb02deff1add921533d956f253954c76fa5fe6f0fbe516e7f2

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=Certisign Root CA, O=Certisign Certificadora Digital S.A., C=BR
 Signature Algorithm: SHA512withRSA, OID = 1.2.840.113549.1.1.13

 Key:  Sun RSA public key, 4096 bits
 modulus:
```

```
838581495727241538791479293555239809897343214758597498890250772134382012652488417060641400394683897528297344133916636665969425472487828769033674619340229210019038411557207353988428020514146059990415173356285194019897255430297354813503205682934644048136379610031647285811138251150679415446400087425463638353870508433217003601893787901159569082836654688379442238984855385231401082187574319605112793969098253082696258163595003930445061950654069738669798344653576001863172995311200598956495477845054713790607993935317903225931115551294561508366832096481385530018748868233758970945092314614367511450386548451324842217305318870664683153159001337131768784950877424660685821599837165268445108156919372960394896673700366173116574869034752075000481857055603133004720515118185340830287591489111217314462544988316431256785708389590588915138797707479684243748491541860729493794671480263571061476365589157646583607984324959853814529751208292381505296966521391501862180756102181476419030034916745728837653159976623486701495504795382173766098949075051342061625847713508201917654321427295860095815699669394495087023756170819316215722742901864009626227385064716761931499369682236963577413562254878918077283227381578037288564359948371852780977072274 21
 public exponent: 65537
 Validity: [From: Tue Apr 14 22:00:00 PET 2015,
             To: Sun Apr 14 22:00:00 PET 2030]
 Issuer: CN=Certisign Root CA, O=Certisign Certificadora Digital S.A., C=BR
 SerialNumber: [    75ea72f6 2cbe4b91]

Certificate Extensions: 5
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 8B A6 CE A5 47 D1 1B 8C   8B 9D 19 59 72 5C AB 3B  ....G......Yr\.;
0010: B5 34 14 1F                                        .4..
]
]

[2]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://certisign-ca.certisign.com.br/repositorio/lcr/CertisignRootCA/LatestCRL.crl]
]]

[3]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [1.3.6.1.4.1.30253.4]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 34 68 74 74 70 3A 2F   2F 63 65 72 74 69 73 69  .4http://certisi
0010: 67 6E 2D 63 61 2E 63 65   72 74 69 73 69 67 6E 2E  gn-ca.certisign.
0020: 63 6F 6D 2E 62 72 2F 72   65 70 6F 73 69 74 6F 72  com.br/repositor
0030: 69 6F 2F 63 70 73                                  io/cps

]]  ]
]

[5]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA512withRSA]
 Signature:
0000: 7C B3 5C 98 80 D8 B2 6F   13 78 5A 85 48 9D D2 D1  ..\....o.xZ.H...
0010: 0C 41 39 A9 05 23 35 3A   53 8C C8 8D EB CA 90 A2  .A9..#5:S.......
0020: 61 2F 6F 73 25 59 9A DC   44 D8 30 E4 35 1B 4D FB  a/os%Y..D.0.5.M.
0030: 1E 41 BE 2E D3 F1 92 21   06 0B AB D9 18 6A 85 59  .A.....!.....j.Y
0040: B7 E3 64 5D 51 D9 02 5A   2F 3A 9E 5E 8B D4 A3 69  ..d]Q..Z/:.^...i
0050: C5 C4 20 A9 95 47 B4 63   62 57 70 F2 CA E3 18 1F  .. ..G.cbWp.....
0060: 6F 18 50 13 3F 5C 39 30   5D 38 E2 67 BA C9 E4 84  o.P.?\90]8.g....
0070: A1 ED AE 7F E3 F1 C0 0B   F7 58 49 4F 19 30 2C EF  .........XIO.0,.
0080: 27 94 7A 82 7B 7A 05 C4   F8 40 92 2C B9 EF E9 DA  '.z..z...@.,....
0090: 46 6B 5C D5 DD B6 91 25   55 ED 79 A1 01 C2 F8 5A  Fk\....%U.y....Z
00A0: 83 A3 85 B9 20 63 BF 2E   9B E9 19 C3 A8 B6 9C AC  .... c..........
00B0: 37 18 DA 69 42 A6 85 69   2E 3D F2 D4 E5 76 12 7E  7..iB..i.=...v..
00C0: BB DF 89 1A 2B 17 5A C2   39 64 28 E1 51 5C BF 01  ....+.Z.9d(.Q\..
00D0: B9 A0 08 97 AE 32 9E A3   96 F8 9F E0 3C E2 36 2F  .....2......<.6/
00E0: 15 CC FB 0F 67 4A 69 72   80 B3 71 BC B9 D6 FE E7  ....gJir..q.....
00F0: 7B DE 37 46 16 5C 2C C3   A1 83 3D BE BE FB D5 88  ..7F.\,...=.....
0100: C5 5A 59 4F 8E 50 C2 12   EE C0 BE 72 B0 47 1D A5  .ZYO.P.....r.G..
0110: 75 35 0D 9D DC FE 1B A4   63 09 91 C6 64 A3 2A D2  u5......c...d.*.
0120: D0 F5 BA B7 C8 BC B7 B3   86 39 3D D1 45 AE C1 0D  .........9=.E...
0130: 07 9E 8B F0 F5 2B EC 64   F7 1F 96 CB 4F FE 9C 75  .....+.d....O..u
0140: 03 41 F1 FA 97 DD ED 6D   D1 16 F8 AA 05 51 DB 26  .A.....m.....Q.&
0150: E0 0E A3 EB 2A A0 8D A3   66 36 7A 79 93 CC E2 B9  ....*...f6zy....
0160: 28 01 C7 FE 71 DF 61 CC   1A 63 99 8A 36 52 FC 3A  (...q.a..c..6R.:
0170: 53 6B B9 87 5A AC 4B 3F   D1 EB 44 20 8F 3B D4 33  Sk..Z.K?..D .;.3
0180: 5A 06 A6 0E 2C 71 84 75   90 8A 66 D7 D0 C4 7E 5D  Z...,q.u..f....]
0190: 11 64 5D C4 5B EF D8 6F   34 90 AF 8D C1 2A 10 86  .d].[..o4....*..
01A0: C1 73 C0 62 1A B1 E8 D9   83 77 F9 C7 58 75 25 34  .s.b.....w..Xu%4
01B0: 63 A0 3A 90 64 37 60 AB   22 6A 31 3B 18 FF 7E A8  c.:.d7`."j1;....
01C0: F1 95 C7 C4 82 2B 24 03   5E B7 68 D2 69 C1 91 C0  .....+$.^.h.i...
01D0: 6A 88 27 2A EE FA 3A 2C   09 A2 9B 3A 22 90 23 29  j.'*..:,...:".#)
01E0: 6B 29 76 30 0D B5 EC 3D   C5 85 B9 06 FF F6 BF 53  k)v0...=.......S
01F0: CA 33 C6 B2 9F 6A 0B 87   31 83 F7 56 BF 31 44 96  .3...j..1..V.1D.

]
```

The certificate in PEM format:


```
-----BEGIN CERTIFICATE-----
MIIGOTCCBCGgAwIBAgIIdepy9iy+S5EwDQYJKoZIhvcNAQENBQAwWDELMAkGA1UE
BhMCQlIxLTArBgNVBAoTJENlcnRpc2lnbiBDZXJ0aWZpY2Fkb3JhIERpZ2l0YWwg
Uy5BLjEaMBgGA1UEAxMRQ2VydGlzaWduIFJvb3QgQ0EwHhcNMTUwNDE1MDMwMDAw
WhcNMzAwNDE1MDMwMDAwWjBYMQswCQYDVQQGEwJCUjEtMCsGA1UEChMkQ2VydGlz
aWduIENlcnRpZmljYWRvcmEgRGlnaXRhbCBTLkEuMRowGAYDVQQDExFDZXJ0aXNp
Z24gUm9vdCBDQTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAM2NeAEe
wi63b5vLD+awgtRT8AjMkNDA8VFUy/kRdHvy7YakqtiW7tSp54YNsg+82Ti8B5aS
1BqlSmBnQCpKIiofzkhcmEK3fsXocdI3sllXIo5nBE9EI/RCOrv+OBpT8szZphVG
ZXGsrbhXVbTLDpVIT6OEyHFjb26SjVT+oSURb7CBffs6RJT2XpU3lD0dU5t3VvEq
fB+FQyyfoDcg7s4N1M7khbdYycN0Bg+ogwhkNr5pS6pCOBz+3jI2RwnwbJJIRnKH
JC/I+Y/z/lzRu3RM6BBeiHObOSLyKW1rYX/Z0e5UPf5HbIREr7f8A3xnh9Couifz
LUmZ2XfjjcBIg7/P6GKlGu5PVGjw1nBC/ZiLhRgBYokX4zUhvAMMXZe4873VnBdo
LeNhWV175EsESNM1dZoV3R6FPR8PbV9XKLl66RB5LvOHRui2AlxrjpKK/60Jy/Cn
N81nmuyst97sLtjhTOwoYkHL5tjZY2E3U7Zx1+B/CxLx1sKvbZwxDrgiJ745XodX
nX3OVqE1Y7ynIdm1Q4Em8089d6mHDIaEXaHqJhq7VCMz+IiZvc0MmcUIPGwWWlz0
XK3ymhVV70XNhnU7j88qrt02TJfl6CHJM1bn8rz+SfJZ6tofrY7x6PvJB26Y88Xt
iuGsrkDFRkgQYyKa/jLJZYuk6mAfKOPEs9kdAgMBAAGjggEFMIIBATAPBgNVHRMB
Af8EBTADAQH/MB0GA1UdDgQWBBSLps6lR9EbjIudGVlyXKs7tTQUHzBaBgNVHSAE
UzBRME8GCSsGAQQBgewtBDBCMEAGCCsGAQUFBwIBFjRodHRwOi8vY2VydGlzaWdu
LWNhLmNlcnRpc2lnbi5jb20uYnIvcmVwb3NpdG9yaW8vY3BzMGMGA1UdHwRcMFow
WKBWoFSGUmh0dHA6Ly9jZXJ0aXNpZ24tY2EuY2VydGlzaWduLmNvbS5ici9yZXBv
c2l0b3Jpby9sY3IvQ2VydGlzaWduUm9vdENBL0xhdGVzdENSTC5jcmwwDgYDVR0P
AQH/BAQDAgEGMA0GCSqGSIb3DQEBDQUAA4ICAQB8s1yYgNiybxN4WoVIndLRDEE5
qQUjNTpTjMiN68qQomEvb3MlWZrcRNgw5DUbTfseQb4u0/GSIQYLq9kYaoVZt+Nk
XVHZAlovOp5ei9SjacXEIKmVR7RjYldw8srjGB9vGFATP1w5MF044me6yeSEoe2u
f+PxwAv3WElPGTAs7yeUeoJ7egXE+ECSLLnv6dpGa1zV3baRJVXteaEBwvhag6OF
uSBjvy6b6RnDqLacrDcY2mlCpoVpLj3y1OV2En6734kaKxdawjlkKOFRXL8BuaAI
l64ynqOW+J/gPOI2LxXM+w9nSmlygLNxvLnW/ud73jdGFlwsw6GDPb6++9WIxVpZ
T45QwhLuwL5ysEcdpXU1DZ3c/hukYwmRxmSjKtLQ9bq3yLy3s4Y5PdFFrsENB56L
8PUr7GT3H5bLT/6cdQNB8fqX3e1t0Rb4qgVR2ybgDqPrKqCNo2Y2enmTzOK5KAHH
/nHfYcwaY5mKNlL8OlNruYdarEs/0etEII871DNaBqYOLHGEdZCKZtfQxH5dEWRd
xFvv2G80kK+NwSoQhsFzwGIasejZg3f5x1h1JTRjoDqQZDdgqyJqMTsY/36o8ZXH
xIIrJANet2jSacGRwGqIJyru+josCaKbOiKQIylrKXYwDbXsPcWFuQb/9r9TyjPG
sp9qC4cxg/dWvzFElg==
-----END CERTIFICATE-----
```


Certificate Service Provider Name (en): BIT4ID S.A.C.

Trade name (en)	BIT4ID S.A.C.
Information URI (en)	HTTPS://WWW.BIT4ID.COM
Service provider street address (es)	CALLE MARTIR JOSE OLAYA NRO. 129 OFICINA 1204, MIRAFLORES
Service provider street address (en)	CALLE MARTIR JOSE OLAYA NRO. 129 OFICINA 1204, MIRAFLORES
Service provider postal code (es)	15074
Service provider postal code (en)	15074
Service provider locality (es)	MIRAFLORES
Service provider locality (en)	MIRAFLORES
Service provider state (es)	LIMA
Service provider state (en)	LIMA
Service provider country (es)	PE
Service provider country (en)	PE

OID.2.5.4.97=VATES-A66721499, CN=UANATACA CA2 2016, OU=TSP-UANATACA, O=UANATACA S.A., L=Barcelona (see current address at www.uanataca.com/address), C=ES

Type	CA/QC
Status	undersupervision
Status starting time	2018-08-28T21:58:09.000Z

Service digital identity (X509)

Version	3
Serial number	2317042835735686419
Signature algorithm	SHA256withRSA
Issuer	OID.2.5.4.97=VATES-A66721499, CN=UANATACA ROOT 2016, OU=TSP-UANATACA, O=UANATACA S.A., L=Barcelona (see current address at www.uanataca.com/address), C=ES
Valid from	Fri Mar 11 05:37:31 PET 2016
Valid to	Sun Mar 11 05:37:31 PET 2029
Subject	OID.2.5.4.97=VATES-A66721499, CN=UANATACA CA2 2016, OU=TSP-UANATACA, O=UANATACA S.A., L=Barcelona (see current address at www.uanataca.com/address), C=ES
Public key	Sun RSA public key, 4096 bits modulus: 84609201759709241477504090634564013869822813127294222229682166099085633 65373543206677979791446723899724857018234905808600953788462147930919466 36711810510143602935614448969052976569460191344340411085278864480397551 13928848168259548886042999410681700965459097916985266598794470652209392 73591912844169369934733226533226485445464903747137029119306308267181774 93478384013463616572466695103685157701006946012762949509273382917462547 87462160403839417941439449488026559284704494247178338819015761652554161 92517515850886868212203776701656097437048673335218042357268145153942376 06684342206020857315868853226372860689522748419197604789918543589374052 78304097405134469286117208885155772687177065698793406053439577539323415 91681926533607994971541574786412858592991476103353528974198484683270770 11255384029376433001982296658878991024512554611481520933743417241066654 44856661504717223128490253555968862186950573834319765587702038515095835 74928618709547937806064909677942357433930147239962229150708418698933897 80477909787821319057498544842663672676740377222756626575154296238425341 15884861908158732634146703480166601216863579412152417845597010953886387 64945484941606109495899963944573730124741135490198108054489773447586353 75156307556203228143384409 public exponent: 65537
Subject key identifier	7d57e76073ce0746a9e2a368f0e111b2749273fd
CRL distribution points	http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl
Authority key identifier	041830168014552cf1bca15eb9eea02f8857105bfc96f7919a2c
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=0
SHA1 Thumbprint	0ece527803c9db6e63bcea5536b93ae8284e8d2d
SHA256 Thumbprint	00ff2ff2efba98c6b023ad1035559a606dd9fc48a39d3407cc07a678379a7909

The decoded certificate:

```
[
[
 Version: V3
 Subject: OID.2.5.4.97=VATES-A66721499, CN=UANATACA CA2 2016, OU=TSP-UANATACA, O=UANATACA S.A., L=Barcelona (see current address at www.uanataca.com/address), C=ES
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
84609201759709241477504090634564013869822813127294222229682166099085633653735432066779797914467238997248570182349058086009537884621479309194663671181051014360293561444896905297656946019134434041108527886448039755113928848168259548886042999410681700965459097916985266598794470652209392735919128441693699347332265332264854454649037471370291193063082671817749347838401346361657246669510368515770100694601276294950927338291746254787462160403839417941439449488026559284704494247178338819015761652554161925175158508868682122037767016560974370486733352180423572681451539423760668434220602085731586885322637286068952274841919760478991854358937405278304097405134469286117208885155772687177065698793406053439577539323415916819265336079949715415747864128585929914761033535289741984846832707701125538402937643300019822966588789910245125546114815209337434172410666544856661504717223128490253555968862186950573834319765587702038515095835749286187095479378060649096779423574339301472399622291507084186989338978047790978782131905749854484266367267674037722275662657515429623842534115848861908158732634146703480166601216863579412152417845597010953886387649454849416061094958999639445737301247411354901981080544897734475863537515630755620322814338440 9
 public exponent: 65537
 Validity: [From: Fri Mar 11 05:37:31 PET 2016,
              To: Sun Mar 11 05:37:31 PET 2029]
 Issuer: OID.2.5.4.97=VATES-A66721499, CN=UANATACA ROOT 2016, OU=TSP-UANATACA, O=UANATACA S.A., L=Barcelona (see current address at www.uanataca.com/address), C=ES
 SerialNumber: [    2027ca2e d163ad13]

Certificate Extensions: 8
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 7D 57 E7 60 73 CE 07 46   A9 E2 A3 68 F0 E1 11 B2  .W.`s..F...h....
```

```
0010: 74 92 73 FD                                        t.s.
]
]

[2]: ObjectId: 2.5.29.18 Criticality=false
IssuerAlternativeName [
 RFC822Name: info@uanataca.com
]

[3]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 55 2C F1 BC A1 5E B9 EE   A0 2F 88 57 10 5B FC 96  U,...^.../.W.[..
0010: F7 91 9A 2C                                        ...,
]

]

[4]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl]
, DistributionPoint:
    [URIName: http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl]
]]

[5]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[6]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 27 68 74 74 70 3A 2F   2F 77 77 77 2E 75 61 6E  .'http://www.uan
0010: 61 74 61 63 61 2E 63 6F   6D 2F 70 75 62 6C 69 63  ataca.com/public
0020: 2F 70 6B 69 2F 64 70 63   2F                      /pki/dpc/

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 72 0C 70 43 65 72 74   69 66 69 63 61 64 6F 20  0r.pCertificado
0010: 64 65 20 6C 61 20 45 6E   74 69 64 61 64 20 64 65  de la Entidad de
0020: 20 43 65 72 74 69 66 69   63 61 63 69 C3 B3 6E 20   Certificaci..n
0030: 73 75 62 6F 72 64 69 6E   61 64 61 20 64 65 20 55  subordinada de U
0040: 41 4E 41 54 41 43 41 2E   20 56 65 72 20 68 74 74  ANATACA. Ver htt
0050: 70 3A 2F 2F 77 77 77 2E   75 61 6E 61 74 61 63 61  p://www.uanataca
0060: 2E 63 6F 6D 2F 70 75 62   6C 69 63 2F 70 6B 69 2F  .com/public/pki/
0070: 64 70 63 2F                                        dpc/

]]  ]
]

[7]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:0
]

[8]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://ocsp1.uanataca.com/public/pki/ocsp/,
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://ocsp2.uanataca.com/public/pki/ocsp/]
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 07 18 D1 D3 31 53 A5 BB   93 A4 CA A0 02 1F 3B 8D  ....1S........;.
0010: 56 19 88 FF 74 87 81 15   B3 7B 63 A7 FB D8 A8 4F  V...t.....c....O
0020: E6 8E 9C 75 19 AF 2D AB   80 35 D1 27 E4 73 B9 3F  ...u..-..5.'.s.?
0030: 4E 26 91 FE D3 23 8D 1B   47 9E EF C9 B3 35 87 83  N&...#..G....5..
0040: 53 4C 69 DD 06 AA 20 5E   B8 E6 64 B0 BC 0C ED C5  SLi... ^..d.....
0050: 9B A5 E1 5E 8E 10 C1 D6   DE F5 CF B4 3F 77 A2 5A  ...^........?w.Z
0060: F8 32 AE EB F4 9E 2B 09   19 64 16 E7 F9 95 88 AF  .2....+..d......
0070: E1 27 66 F0 E9 19 D4 F7   6E 52 4E 51 78 ED 7B 6A  .'f.....nRNQx..j
0080: 0E A7 92 D7 05 C9 22 64   B2 53 AE 61 54 29 E2 7F  ......"d.S.aT)..
0090: 08 09 03 60 7F A2 58 8F   D1 59 1B 55 1A D0 7D 98  ...`..X..Y.U....
00A0: 53 32 50 BC 7D 05 BE 7F   71 89 D7 E4 C3 79 F7 09  S2P.....q....y..
00B0: 88 AC 5A 76 A5 06 08 2B   C6 B7 52 9E 80 4D 0B 89  ..Zv...+..R..M..
00C0: A7 15 D5 3E F3 F7 08 DF   28 ED B5 3C 57 13 B9 91  ...>....(..<W...
00D0: 62 54 F5 B5 EB B3 52 2A   C2 29 C0 68 46 F0 0E 15  bT....R*.).hF...
00E0: AE 3A C9 25 2E 08 94 F0   33 1C B9 41 88 6E 61 A3  .:.%....3..A.na.
00F0: F8 9B 70 AE D0 0C 05 CE   1B 63 CC 24 1A F7 F1 3B  ..p......c.$...;
0100: F5 4F 3B 16 65 38 A6 E1   75 53 6E C2 F3 CC 76 97  .O;.e8..uSn...v.
0110: 46 59 A3 E5 92 D7 6A 0C   95 AE 22 5A 75 92 18 41  FY....j..."Zu..A
0120: DA C9 6D D3 1D 20 9F A0   7E 14 00 AA 6B 7B 99 CB  ..m.. ......k...
0130: 55 16 33 01 16 13 72 6D   0C EF 7F 17 C9 C1 8A D8  U.3...rm........
0140: 9C E0 84 EC 17 56 69 A8   8A 2C 74 F7 0D 1F A0 41  .....Vi..,t....A
```

```
0150: 88 A7 73 00 F9 A7 81 AA   F5 8D C6 14 B1 8E D6 AF  ..s.............
0160: 4B 42 24 9D 63 30 8A AD   1C 78 B8 D9 CC 41 B6 40  KB$.c0...x...A.@
0170: 00 A9 C5 1A EB 92 72 2D   34 DB D6 E6 7B ED 43 48  ......r-4.....CH
0180: DF A0 61 DD 6F 0C B5 E4   4C B7 89 17 2C 6C EF A0  ..a.o...L...,l..
0190: DB 65 99 99 5D A7 2B 1B   22 A3 FF E1 3E 81 2C 25  .e..].+."...>.,%
01A0: F7 4A 48 9D 77 D9 F8 84   1C 3E 7F FD AA F7 52 38  .JH.w....>....R8
01B0: F8 2B 2D 01 A6 EC 05 90   4A 16 C8 28 8F F2 5A 75  .+-.....J..(..Zu
01C0: C7 CF B6 B4 59 57 CA DE   B1 0B 49 2B D5 6E D7 79  ....YW....I+.n.y
01D0: 99 D7 FC 40 5D AD 82 AE   7D FE E3 33 27 40 93 9F  ...@].....3'@..
01E0: 13 15 2B ED 1F C7 CD E5   B8 23 7C D5 82 EC 52 97  ..+......#....R.
01F0: 69 73 77 B4 51 11 BB 78   33 0A 34 6E 78 5A FB 56  isw.Q..x3.4nxZ.V

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIIWjCCBkKgAwIBAgIIICfKLtFjrRMwDQYJKoZIhvcNAQELBQAwgbkxCzAJBgNV
BAYTAkVTMUQwQgYDVQQHDDtCYXJjZWxvbmEgKHNlZSBjdXJyZW50IGFkZHJlc3Mg
YXQgd3d3LnVhbmF0YWNhLmNvbS9hZGRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0Eg
Uy5BLjEVMBMGA1UECwwMVFNQLVVBTkFUQUNBMRswGQYDVQQDDBJVQU5BVEFDQSBS
T09UIDIwMTYxGDAWBgNVBGEMD1ZBVEVTLUE2NjcyMTQ5OTAeFw0xNjAzMTExMDM3
MzFaFw0yOTAzMTExMDM3MzFaMIG4MQswCQYDVQQGEwJFUzFEMEIGA1UEBww7QmFy
Y2Vsb25hIChzZWUgY3VycmVudCBhZGRyZXNzIGF0IHd3dy51YW5hdGFjYS5jb20v
YWRkcmVzcykxFjAUBgNVBAoMDVVBTkFUQUNBIFMuQS4xFTATBgNVBAsMDFRTUC1V
QU5BVEFDQTEaMBgGA1UEAwwRVUFOQVRBQ0EgQ0EyIDIwMTYxGDAWBgNVBGEMD1ZB
VEVTLUE2NjcyMTQ5OTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAM9k
wiDGaY0Sgs8VgEawfJ+YBhye+CX3RH9S+MOdgDGRNqpNUzEDEwChjTBMV6cx+1u8
gvn+H41lTaCGkea6nLIAN6EIaVV5SPmBt9KApR6wTlbCljx5yJPNZ55Sg/FGYHru
QLZ3D3st1tr4Kh/Tum82/sGkWGruPzylUtyOeBOTc0A92Yv3GdA00SRJy9Fjslbb
oeqtWTVI5Rk8Txfyn5BDC7gp27stfCP9K/WECxjFIMqdHtm+bdSyyYTm+seSC4ra
zZ+9fSSEBmRvbpPdEtZug38UoSr/Yp3bo9c09qLO6N35JO0pcSjG5/UEZyC9wXSz
RFpq7FY2lX2l0yZpbc553QyTbRulTGzQENjy3J5YaAd6BiV0oEa/ITRjtBsbbIr3
e7LFcrHNCx9A0n+LoTUyj04B7A7tzAMkwfM5VFNFInnkWJgUbQLz/VZtwqmm/Fmf
40LynMV5XmdBq85v0dmdDrleuNpV8m4AQOEdgzTaGwLityMWMepNEKN1Paw0I1P4
HanSRhkl5K56sAeFVseuA6QVJGHQ+rdSv8nCFAF+pLd3rI7VmaQna0wkJvSEIa5h
2CDGesXr39VvBuQONDb/nM/acBQjpOtmwsVCi8hRmPKvRvzcqpUmJlWhUMBtHr0R
cw7+bOP92sNAtEeIQOdxD+3WNuAufGaEtizR1XdZAgMBAAGjggJjMIICXzB+Bggr
BgEFBQcBAQRyMHAwNgYIKwYBBQUHMAGGKmh0dHA6Ly9vY3NwMS51YW5hdGFjYS5j
b20vcHVibGljL3BraS9vY3NwLzA2BggrBgEFBQcwAYYqaHR0cDovL29jc3AyLnVh
bmF0YWNhLmNvbS9wdWJsaWMvcGtpL29jc3AvMB0GA1UdDgQWBBR9V+dgc84HRqni
o2jw4RGydJJz/TASBgNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaAFFUs8byh
XrnuoC+IVxBb/Jb3kZosMBwGA1UdEgQVMBOBEWluZm9AdWFuYXRhY2EuY29tMIHM
BgNVHSAEgcQwgcEwgb4GBFUdIAAwgbUwMwYIKwYBBQUHAgEWJ2h0dHA6Ly93d3cu
dWFuYXRhY2EuY29tL3B1YmxpYy9wa2kvZHBjLzB+BggrBgEFBQcCAjByDHBDZXJ0
aWZpY2FkbyBkZSBsYSBFbnRpZGFkIGRlIENlcnRpZmljYWNpw7NuIHN1Ym9yZGlu
YWRhIGRlIFVBTkFUQUNBLiBWZXIgaHR0cDovL3d3dy51YW5hdGFjYS5jb20vcHVi
bGljL3BraS9kcGMvMIGLBgNVHR8EgYMwgYAwPqA8oDqGOGh0dHA6Ly9jcmwxLnVh
bmF0YWNhLmNvbS9wdWJsaWMvcGtpL2NybC9hcmxfdWFuYXRhY2EuY3JsMD6gPKA6
hjhodHRwOi8vY3JsMi51YW5hdGFjYS5jb20vcHVibGljL3BraS9jcmwvYXJsX3Vh
bmF0YWNhLmNybDAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQELBQADggIBAAcY
0dMxU6W7k6TKoAIfO41WGYj/dIeBFbN7Y6f72KhP5o6cdRmvLauANdEn5HO5P04m
kf7TI40bR57vybM1h4NTTGndBqogXrjmZLC8DO3Fm6XhXo4Qwdbe9c+0P3eiWvgy
ruv0nisJGWQW5/mViK/hJ2bw6RnU925STlF47XtqDqeS1wXJImSyU65hVCnifwgJ
A2B/oliP0VkbVRrQfZhTMlC8fQW+f3GJ1+TDefcJiKxadqUGCCvGt1KegE0LiacV
1T7z9wjfKO21PFcTuZFiVPW167NSKsIpwGhG8A4VrjrJJS4IlPAzHLlBiG5ho/ib
cK7QDAXOG2PMJBr38Tv1TzsWZTim4XVTbsLzzHaXRlmj5ZLXagyVriJadZIYQdrJ
bdMdIJ+gfhQAqmt7mctVFjMBFhNybQzvfxfJwYrYnOCE7BdWaaiKLHT3DR+gQYin
cwD5p4Gq9Y3GFLGO1q9LQiSdYzCKrRx4uNnMQbZAAKnFGuuSci0029bme+1DSN+g
Yd1vDLXkTLeJFyxs76DbZZmZXacrGyKj/+E+gSwl90pInXfZ+IQcPn/9qvdSOPgr
LQGm7AWQShbIKI/yWnXHz7a0WVfK3rELSSvVbtd5mdf8QF2tgq59/uMzJ0CTnxMV
K+0fx83luCN81YLsUpdpc3e0URG7eDMKNG54WvtW
-----END CERTIFICATE-----
```

OID.2.5.4.97=VATES-A66721499, CN=UANATACA CA1 2016, OU=TSP-UANATACA, O=UANATACA S.A., L=Barcelona (see current address at www.uanataca.com/address), C=ES

Type	CA/QC
Status	undersupervision
Status starting time	2018-08-25T00:09:59.000Z

Service digital identity (X509)

Version	3
Serial number	6611671282825056795
Signature algorithm	SHA256withRSA
Issuer	OID.2.5.4.97=VATES-A66721499, CN=UANATACA ROOT 2016, OU=TSP-UANATACA, O=UANATACA S.A., L=Barcelona (see current address at www.uanataca.com/address), C=ES
Valid from	Fri Mar 11 05:35:33 PET 2016
Valid to	Sun Mar 11 05:35:33 PET 2029
Subject	OID.2.5.4.97=VATES-A66721499, CN=UANATACA CA1 2016, OU=TSP-UANATACA, O=UANATACA S.A., L=Barcelona (see current address at www.uanataca.com/address), C=ES

Public key	Sun RSA public key, 4096 bits modulus: 913805944940121185734945814247196343929480703472229580919824147053770991734548360184183044197302190857752864888772731706928719902130156942881236105728583989490929999864394605612919876699480804702767118285221167710041535548648393691077136190924184807433997779448020813578490256168515227319410020611326473599615789834813014708753804193433703172957579379856671746663404320417623621693765954851985792792362426001720931971117464095685626977124716406637963993925632038413236793781314423958835469923454719770761006441100302288612074737287331424232362843520151859031545737544362005519669372343757281524692913778309158593468491898945103977668411710426447167501130520663963494808271197978988749037454219178653231296362507981869994918061505327238571749497904584667821327703238912258990244967305178450424839912718864684982532222709071195810069729226644535885513096705859991508767665813841729283580427314815137526189513892357085600222596172339919459881018507334311087755662655063244569367429546588253068259089985817646683036851775983489410140874326989239429120391433703499640901664430054808560768653529637781262750211039518241070295814894481487579352902369022327219623042319716135560654456480672326142078758916385962839989703586622757073238662270358662275707323866227
public exponent: 65537
Subject key identifier	2d71efb0637ff5fde08322447f441030814f4de5
CRL distribution points	http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl
Authority key identifier	04183016801455 2cf1bca15eb9eea02f8857105bfc96f7919a2c
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=0
SHA1 Thumbprint	7f2cb4f769224cb0cf8b692751cbd4cc64a2c450
SHA256 Thumbprint	35a99284a220789ba0e062eeff1b5f2f74be43754469977cb318c7c86ad48f9f

The decoded certificate:

```
[
[
 Version: V3
 Subject: OID.2.5.4.97=VATES-A66721499, CN=UANATACA CA1 2016, OU=TSP-UANATACA, O=UANATACA S.A., L=Barcelona (see current address at www.uanataca.com/address), C=ES
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
913805944940121185734945814247196343929480703472229580919824147053770991734548360184183044197302190857752864888772731706928719902130156942881236105728583989490929999864394605612919876699480804702767118285221167710041535548648393691077136190924184807433997779448020813578490256168515227319410020611326473599615789834813014708753804193433703172957579379856671746663404320417623621693765954851985792792362426001720931971117464095685626977124716406637963993925632038413236793781314423958835469923454719770761006441103022886120747372873314242323628435201518590315457375443620055196693723437572815246929137783091585934684918989451039776684117104264471675011305206639634948082711979789887490374542191786532319863625798186999491806150532723857174949790458466782132770323891225899024496730517845042483991271886468498253222270907119581006972922664453588551309670585999150878766581384172928358042731481513752618951389235708566022259617233991945988101850733431108775566265506324456936742954658825306825908998581764668303685177598348941014087432698923942912039143370349964090166443005480856076865352963778126275021103951824107029581489448148757935290236902232721962304231971613556065445648067232614207875891638596283298997035866227575073238662270
 public exponent: 65537
 Validity: [From: Fri Mar 11 05:35:33 PET 2016,
             To: Sun Mar 11 05:35:33 PET 2029]
 Issuer: OID.2.5.4.97=VATES-A66721499, CN=UANATACA ROOT 2016, OU=TSP-UANATACA, O=UANATACA S.A., L=Barcelona (see current address at www.uanataca.com/address), C=ES
 SerialNumber: [    5bc16000 6870521b]

Certificate Extensions: 8
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 2D 71 EF B0 63 7F F5 FD   E0 83 22 44 7F 44 10 30  -q..c....."D.D.0
0010: 81 4F 4D E5                                        .OM.
]
]

[2]: ObjectId: 2.5.29.18 Criticality=false
IssuerAlternativeName [
 RFC822Name: info@uanataca.com
]

[3]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 55 2C F1 BC A1 5E B9 EE   A0 2F 88 57 10 5B FC 96  U,...^.../.W.[..
0010: F7 91 9A 2C                                        ...,
]

]
```

```
[4]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl]
, DistributionPoint:
    [URIName: http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl]
]]

[5]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[6]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 27 68 74 74 70 3A 2F   2F 77 77 77 2E 75 61 6E  .'http://www.uan
0010: 61 74 61 63 61 2E 63 6F   6D 2F 70 75 62 6C 69 63  ataca.com/public
0020: 2F 70 6B 69 2F 64 70 63   2F                       /pki/dpc/

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 72 0C 70 43 65 72 74   69 66 69 63 61 64 6F 20  0r.pCertificado
0010: 64 65 20 6C 61 20 45 6E   74 69 64 61 64 20 64 65  de la Entidad de
0020: 20 43 65 72 74 69 66 69   63 61 63 69 C3 B3 6E 20   Certificaci..n
0030: 73 75 62 6F 72 64 69 6E   61 64 61 20 64 65 20 55  subordinada de U
0040: 41 4E 41 54 41 43 41 2E   20 56 65 72 20 68 74 74  ANATACA. Ver htt
0050: 70 3A 2F 2F 77 77 77 2E   75 61 6E 61 74 61 63 61  p://www.uanataca
0060: 2E 63 6F 6D 2F 70 75 62   6C 69 63 2F 70 6B 69 2F  .com/public/pki/
0070: 64 70 63 2F                                        dpc/

]]  ]
]

[7]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:0
]

[8]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://ocsp1.uanataca.com/public/pki/ocsp/,
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://ocsp2.uanataca.com/public/pki/ocsp/]
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 0A 23 C6 0D DA 32 0D 3D   51 6B 67 A6 9F D6 5E 78  .#...2.=Qkg...^x
0010: A7 00 E5 A7 F9 97 EB 78   7C 73 EE 4A 75 BA E2 34  .......x.s.Ju..4
0020: DB 19 EA 6E AC CB 29 EC   09 27 6C 62 20 7A E5 02  ...n..)..'lb z..
0030: 01 B1 4B 6A 4B 8D 74 1F   EC F7 96 71 40 17 23 CE  ..KjK.t....q@.#.
0040: CA 24 A5 3B 1C EC 15 C8   36 A9 2D 37 86 70 EB 35  .$.;....6.-7.p.5
0050: CB 19 32 23 62 C7 EA 4A   F2 8C 6E 9F FD FF EA AE  ..2#b..J..n.....
0060: A9 3D 9C F4 31 8C 18 52   98 01 8E 3C 27 E6 22 D4  .=..1..R...<'.".
0070: 58 47 66 D3 18 98 CD F4   94 94 55 3F FF 65 B6 C5  XGf.......U?.e..
0080: EC 18 50 80 FB BE 8C 28   56 E3 A5 6B 47 BC ED 09  ..P....(V..kG...
0090: 21 50 11 D1 F0 4B AE 4C   51 CF 22 99 71 B1 4F 24  !P...K.LQ.".q.O$
00A0: 90 D6 0A DE 72 72 B4 E8   C9 57 DE 5F 6C AC 5B 69  ....rr...W._l.[i
00B0: 5A 81 AE 5D 5B 39 AF 82   45 12 76 63 01 14 C2 0E  Z..][9..E.vc....
00C0: 24 47 0F 3C 63 33 D0 7B   39 EC AF 84 6B D5 55 FA  $G.<c3..9...k.U.
00D0: 0C 83 16 A3 D1 33 F0 33   72 01 E9 FE 45 36 BC 1E  .....3.3r...E6..
00E0: 83 E5 D0 78 63 5C 69 7B   FA 95 12 EF 26 57 74 77  ...xc\i.....&Wtw
00F0: 1F B7 28 A5 F4 0E D8 6A   2E 2A B1 CF FB 46 F7 D3  ..(....j.*...F..
0100: 2C 6A E7 1F 23 59 7F F1   0D 41 A5 6B 8A 76 B0 AC  ,j..#Y...A.k.v..
0110: 11 6C 3F E0 F6 40 15 98   5D 58 1E 18 B5 11 70 5F  .l?..@..]X....p_
0120: 62 42 21 DD 49 D7 7B E7   5A 14 DF 33 94 89 F7 8F  bB!.I...Z..3....
0130: 01 78 E3 34 E9 D4 B2 64   14 CF 5E A2 71 DC 0B 85  .x.4...d..^.q...
0140: 4D 86 6D 01 6C E9 C1 26   77 8C 01 14 E6 E8 1D 4E  M.m.l..&w......N
0150: 7C 9A A6 F2 77 95 7B 4A   34 4B 15 E6 87 E6 04 0A  ....w..J4K......
0160: A6 83 38 93 63 34 88 9F   B1 FE 53 E4 22 FF 99 9E  ..8.c4....S."...
0170: 86 06 95 86 8D F9 C6 24   A2 B8 CB 0E EB FF 1E 63  .......$.......c
0180: 5D A2 C1 D7 A1 7F E1 8B   F8 6F 4A AD CE 9E 51 15  ]........oJ...Q.
0190: C0 6E D5 0F 02 C2 34 9C   80 8A 36 EA 96 64 22 8C  .n....4...6..d".
01A0: D4 AB 79 F6 8C BA C6 D2   45 6B E9 DF 18 37 A3 73  ..y.....Ek...7.s
01B0: BA 0E 93 18 B7 F6 D1 F6   66 19 36 F2 CC C4 81 00  ........f.6.....
01C0: A8 42 1C CF CF 5C 2C D2   05 1C 21 55 E9 C7 83 7C  .B...\,...!U....
01D0: A3 B1 AC AC 04 91 CA DE   CC 65 6D 67 9B 8D AC E5  .........emg....
01E0: 2F 48 D6 02 89 BE 85 D6   EB 75 8C 20 59 72 E9 C4  /H.......u. Yr..
01F0: D7 CC 75 02 20 E0 B5 42   32 4A 3B 25 8E F7 3F 56  ..u. ..B2J;%..?V

]
```

The certificate in PEM format:

-----BEGIN CERTIFICATE-----
MIIIWjCCBkKgAwIBAgIIW8FgAGhwUhswDQYJKoZIhvcNAQELBQAwgbkxCzAJBgNV
BAYTAkVTMUQwQgYDVQQHDDtCYXJjZWxvbmEgKHNlZSBjdXJyZW50IGFkZHJlc3Mg
YXQgd3d3LnVhbmF0YWNhLmNvbS9hZGRyZXNzTEWMBQGA1UECgwNVUFOQVRBQ0Eg
Uy5BLjEVMBMGA1UECwwMVFNQLVVBTkFUQUNBMRswGQYDVQQDDBJVQU5BVEFDQSBS
T09UIDIwMTYxGDAWBgNVBGEMD1ZBVEVTLUE2NjcyMTQ5OTAeFw0xNjAzMTExMDM1
MzNaFw0yOTAzMTExMDM1MzNaMIG4MQswCQYDVQQGEwJFUzFEMEIGA1UEBww7QmFy
Y2Vsb25hIChzZWUgY3VycmVudCBhZGRyZXNzIGF0IHd3dy51YW5hdGFjYS5jb20v
YWRkcmVzcykxFjAUBgNVBAoMDVVBTkFUQUNBIFMuQS4xFTATBgNVBAsMDFRTUC1V
QU5BVEFDQTEaMBgGA1UEAwwRVUFOQVRBQ0EgQ0ExIDIwMTYxGDAWBgNVBGEMD1ZB
VEVTLUE2NjcyMTQ5OTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAN/9
2JPM78ixJtnnGkLZ8xG7CEHN9OirwbFxzD/wBGaWBW4bwloJHw9vgEBdY4a/yLnI
33kgh+mJIry8DcYmbkUx+/9m9AbINR/W4QW90LOvCf168R5v3Bf8IkKRjLNbzG81
Vo4AuUI2NkWTvBq/8vNUReK8H4/TexxqstDVA7aNzRoj2zmTLPQ0Ct0OTIur/zZb
+vfliZ/vQUUbCsAB2x5udnp0awml/DutwUoas+28cGHi1zpT2OFOuAg5HTjrjeqC
8Dif5x4h5+r99oIf+V34TAIO0aCiCRGS2/uTdI0bcXdurauV0/Q6K7Rivwk2NEyX
5CS3fML9VXYH49UhqRB+36uPNDdJcQUkBP+G/t0XMVDNIwOZHGiA0yfUSogPScdF
yWYJlCt58JJkJXp2ANWYmdZvQKIQ8aUdeeEoc60GA0763jD+q4hZAVww7J41Dsu9
DNN4ziPurz0kZx3f8fjO0Io+uYPcty/BbHjRytWZ0DoIIj9I5Xw1glqHYZFBcLH9
BOhVGebmeaaGZy/hwbTfTSoaRGIHge3lZws/kys0yDZW4ETdNWR4DnKm9gNM0PGm
5v6nUtqA8Ygpowyow3LWYIa1Gl9GTHtLvj/usZcbI7NWIGNgS9Rw9tmDyi/gtbzu
Vy9HuNXtVLklVfhYJbDOev7kSsNJJ8Fct8BTgNxzAgMBAAGjggJjMIICXzB+Bggr
BgEFBQcBAQRyMHAwNgYIKwYBBQUHMAGGKmh0dHA6Ly9vY3NwMS51YW5hdGFjYS5j
b20vcHVibGljL3BraS9vY3NwLzA2BggrBgEFBQcwAYYqaHR0cDovL29jc3AyLnVh
bmF0YWNhLmNvbS9wdWJsaWMvcGtpL29jc3AvMB0GA1UdDgQWBBQtce+wY3/1/eCD
IkR/RBAwgU9N5TASBgNVHRMBAf8ECDAGAQH/AgEAMB8GA1UdIwQYMBaAFFUs8byh
XrnuoC+IVxBb/Jb3kZosMBwGA1UdEgQVMBOBEWluZm9AdWFuYXRhY2EuY29tMIHM
BgNVHSAEgcQwgcEwgb4GBFUdIAAwgbUwMwYIKwYBBQUHAgEWJ2h0dHA6Ly93d3cu
dWFuYXRhY2EuY29tL3B1YmxpYy9wa2kvZHBjLzB+BggrBgEFBQcCAjByDHBDZXJ0
aWZpY2FkbyBkZSBsYSBFbnRpZGFkIGRlIENlcnRpZmljYWNpw7NuIHN1Ym9yZGlu
YWRhIGRlIFVBTkFUQUNBLiBWZXIgaHR0cDovL3d3dy51YW5hdGFjYS5jb20vcHVi
bGljL3BraS9kcGMvMIGLBgNVHR8EgYMwgYAwPqA8oDqGOGh0dHA6Ly9jcmwxLnVh
bmF0YWNhLmNvbS9wdWJsaWMvcGtpL2NybC9hcmxfdWFuYXRhY2EuY3JsMD6gPKA6
hjhodHRwOi8vY3JsMi51YW5hdGFjYS5jb20vcHVibGljL3BraS9jcmwvYXJsX3Vh
bmF0YWNhLmNybDAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQELBQADggIBAAoj
xg3aMg09UWtnpp/WXninAOWn+ZfreHxz7kp1uuI02xnqbqzLKewJJ2xiIHrlAgGx
S2pLjXQf7PeWcUAXI87KJKU7HOwVyDapLTeGcOs1yxkyI2LH6kryjG6f/f/qrqk9
nPQxjBhSmAGOPCfmItRYR2bTGJjN9JSUVT//ZbbF7BhQgPu+jChW46VrR7ztCSFQ
EdHwS65MUc8imXGxTySQ1grecnK06MlX3l9srFtpWoGuXVs5r4JFEnZjARTCDiRH
DzxjM9B7OeyvhGvVVfoMgxaj0TPwM3IB6f5FNrweg+XQeGNcaXv6lRLvJld0dx+3
KKX0DthqLiqxz/tG99MsaucfI1l/8Q1BpWuKdrCsEWw/4PZAFZhdWB4YtRFwX2JC
Id1J13vnWhTfM5SJ948BeOM06dSyZBTPXqJx3AuFTYZtAWzpwSZ3jAEU5ugdTnya
pvJ3lXtKNEsV5ofmBAqmgziTYzSIn7H+U+Qi/5mehgaVho35xiSiuMsO6/8eY12i
wdehf+GL+G9Krc6eURXAbtUPAsI0nICKNuqWZCKM1Kt59oy6xtJFa+nfGDejc7oO
kxi39tH2Zhk28szEgQCoQhzPz1ws0gUcIVXpx4N8o7GsrASRyt7MZW1nm42s5S9I
1gKJvoXW63WMIFly6cTXzHUCIOC1QjJKOyWO9z9W
-----END CERTIFICATE-----

OID.2.5.4.97=VATES-A66721499, CN=UANATACA ROOT 2016, OU=TSP-UANATACA, O=UANATACA S.A., L=Barcelona (see current address at www.uanataca.com/address), C=ES

Type	CA/QC
Status	undersupervision
Status starting time	2018-08-24T23:49:46.000Z

Service digital identity (X509)

Version	3
Serial number	5576462295436354964
Signature algorithm	SHA256withRSA
Issuer	OID.2.5.4.97=VATES-A66721499, CN=UANATACA ROOT 2016, OU=TSP-UANATACA, O=UANATACA S.A., L=Barcelona (see current address at www.uanataca.com/address), C=ES
Valid from	Fri Mar 11 04:13:53 PET 2016
Valid to	Mon Mar 11 04:13:53 PET 2041
Subject	OID.2.5.4.97=VATES-A66721499, CN=UANATACA ROOT 2016, OU=TSP-UANATACA, O=UANATACA S.A., L=Barcelona (see current address at www.uanataca.com/address), C=ES

Public key	Sun RSA public key, 4096 bits modulus: 630171227781198011478956676509343979463287197711508717349592296636933511758166691880780224008606602803520716160163811642230709214769884490778268662573890902240140705811088928170408875136611415781042232384531036885263111988768980085910041331788207275027720525562946972746516079196617207873269329791574109276308794038876881898394788638682704152880742950556196442679466363917714856256186278852840804925812393431398874641496000981470925254897081856430169410905923331287098493534114770307581123210667752719745438345262616008331171978422535914792004126653260623863503316290306040082152206717930617611180006733988790512386581680075208468968034755266889934879679900047115115593836851799633089100018914004270614129841152652687367036587685932721598916746145777613976268242177283672148852935667330307115212299111818695094121674817269164416217298316095171555634572199454745594374521823810569788814784730908764499342973489045664106800815220671793061761118000673398879051238658168007520846896803475266889934879679900047115115593836851799633089100018914004270614129841129526873670365876859327215989167461457776139762682421772836721488529356673300711521229911181869509412167481726916441621729831609517155563457219945474559437452182381056978881478473090876449934297348904566348680861687027472554087648788853827117823918086995788811872389253123757756030827771228798401725619390521987195423030567660830229214362788532400886559386182499146544818440981519658964108036851995854187478607339456101708724947997286191094996739218056745858690790930659795628688398572844946024835005611750507252913977345471
public exponent: 65537
Subject key identifier	552cf1bca15eb9eea02f8857105bfc96f7919a2c
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	6dc08450a95cd32662c0910f8c2dce230d7466ad
SHA256 Thumbprint	44607b3d0ebd0d2bf181cb62f3cea9766dbb6718743f55b153a320ea99dfb5a6

The decoded certificate:

```
[
[
 Version: V3
 Subject: OID.2.5.4.97=VATES-A66721499, CN=UANATACA ROOT 2016, OU=TSP-UANATACA, O=UANATACA S.A., L=Barcelona (see current address at www.uanataca.com/address), C=ES
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
630171227781198011478956676509343979463287197711508717349592296636933511758166691880780224008606602803520716160163811642230709214769884490778268662573890902240140705811089281704088751366114157810422323845310368852631119887689800859100413317882072750277205255629469727465160791966172078732693297915741092763087940388768818983947886386827041528807494295055619644267946363917714856256186278852840804925812393431398874641496000981437925254897081856430169410905923333128709849353411477030758112321066775271974543834526261600833117197842253591479200141266532606238635033162903060400821522067179306176111800067339887905123865816800752084689680347552668899348796799000471151155938368517996330891000189140042706141298411295268736703658768593272159891674614577761397626824217728367214885293566733030711521229911181869509412167481726916441621729831609517155563457219945474559437452182381056978881478473090876449934297348904566348680861687027472554087648788853827117823918086995788811872389253123757756030827771228798401725619390521987195423030567660830229214362788532400886559386182499146544818440981519658964108036851995854187478607339456101708724947997286191094996739218056745858690790930659795628688398572844946024835005611750507252913977345471
 public exponent: 65537
 Validity: [From: Fri Mar 11 04:13:53 PET 2016,
             To: Mon Mar 11 04:13:53 PET 2041]
 Issuer: OID.2.5.4.97=VATES-A66721499, CN=UANATACA ROOT 2016, OU=TSP-UANATACA, O=UANATACA S.A., L=Barcelona (see current address at www.uanataca.com/address), C=ES
 SerialNumber: [    4d6392e9 8ed7e594]

Certificate Extensions: 5
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 55 2C F1 BC A1 5E B9 EE   A0 2F 88 57 10 5B FC 96  U,...^.../.W.[..
0010: F7 91 9A 2C                                        ...,
]
]

[2]: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
 RFC822Name: info@uanataca.com
]

[3]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 27 68 74 74 70 3A 2F   2F 77 77 77 2E 75 61 6E  .'http://www.uan
0010: 61 74 61 63 61 2E 63 6F   6D 2F 70 75 62 6C 69 63  ataca.com/public
0020: 2F 70 6B 69 2F 64 70 63   2F                      /pki/dpc/

], PolicyQualifierInfo: [
```

```
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 4C 0C 4A 43 65 72 74   69 66 69 63 61 64 6F 20  0L.JCertificado
0010: 72 61 C3 AD 7A 20 64 65   20 55 41 4E 41 54 41 43  ra..z de UANATAC
0020: 41 2E 20 56 65 72 20 68   74 74 70 3A 2F 2F 77 77  A. Ver http://ww
0030: 77 2E 75 61 6E 61 74 61   63 61 2E 63 6F 6D 2F 70  w.uanataca.com/p
0040: 75 62 6C 69 63 2F 70 6B   69 2F 64 70 63 2F        ublic/pki/dpc/

]]  ]
]

[5]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 4C 0C 8E 48 A9 8A FF 28   FA 24 56 FF 45 A1 CC 9A  L..H...(.$V.E...
0010: 8A FC 92 79 30 41 65 62   DE 51 40 48 AC 9F 2D 07  ...y0Aeb.Q@H..-.
0020: 3A 15 F1 E8 56 31 20 8A   1B BA 1D E9 08 94 C4 BB  :...V1 .........
0030: 58 1C DE B5 05 68 99 A4   D1 4C 3B BA 78 97 B2 A3  X....h...L;.x...
0040: FF BB 08 1F 95 18 61 CE   61 88 D2 75 CF 05 F1 62  ......a.a..u...b
0050: 35 1C 53 77 7F AC ED 2A   E3 3A CE 55 73 DD 7C A3  5.Sw...*.:.Us...
0060: F4 11 E1 83 51 F8 82 A3   4B 63 17 BD F6 4A B5 E3  ....Q...Kc...J..
0070: 14 04 39 1F DF 9B 4A 7B   AD 58 15 79 E1 E1 1B C9  ..9...J..X.y....
0080: B5 4B 95 06 CB 22 75 BA   47 A2 07 47 74 3E AC 15  .K..."u.G..Gt>..
0090: 5A 51 B5 9E 9F A2 FE 78   5F 9E BC 46 49 39 DB 44  ZQ.....x_..FI9.D
00A0: 9C 87 CF 1E AD B9 A2 EE   43 21 D0 53 E0 E0 D1 34  ........C!.S...4
00B0: BC 93 AE 5A F1 44 62 A1   59 10 D0 25 9B EF 22 32  ...Z.Db.Y..%.."2
00C0: 27 96 C4 06 63 D1 DB 2A   97 3B 0B 7A 9D 84 7C FF  '...c..*.;.z....
00D0: 76 E5 AD 4F 7D FB 0A 7A   EE 99 90 B6 D4 A0 81 7D  v..O...z........
00E0: EC 07 66 BD 59 F6 3D E1   8E 6E 20 F0 7B 26 2B 0E  ..f.Y.=..n ..&+.
00F0: 50 19 AA 1F 6D D1 8D A9   04 73 E5 0C 2C C8 E7 BC  P...m....s..,...
0100: 94 3C DB ED 4C EE 81 9E   6E 76 95 77 54 55 2B EA  .<..L...nv.wTU+.
0110: 24 7A 64 39 CF 1E 7B 07   39 33 4A 5F E2 E0 6F 99  $zd9....93J_..o.
0120: C7 26 BC A1 06 F6 70 8A   85 1E 7B F2 09 55 C3 39  .&....p.....U.9
0130: DE 3F 09 63 41 2D 94 02   4F 21 91 50 A3 A8 72 FB  .?.cA-..O!.P..r.
0140: B5 90 A5 E0 99 56 3A 85   34 06 84 CF 13 AF 9C A0  .....V:.4.......
0150: FD 74 F6 D6 06 80 BF 7F   FB B6 1E 62 6F 68 86 82  .t.........boh..
0160: AF 10 F0 4D C0 5B 73 43   FB C3 7F A8 C8 D9 D9 A2  ...M.[sC........
0170: 24 04 A4 18 50 59 8B 5A   26 6D EA 7E A7 8B BD C4  $...PY.Z&m......
0180: D8 B4 10 12 CF B4 BA 1F   7E D7 14 CF 70 8E C0 7C  ............p...
0190: 3B FE A7 49 BA 1C 33 F4   A6 AD 2D EC 15 F4 0D 06  ;..I..3...-.....
01A0: E1 E5 0C 0F A6 21 C1 90   1F 1A B7 31 39 82 64 31  .....!.....19.d1
01B0: 9E 4B 78 FE 0D 12 D9 AB   F9 2D CF 94 EE E7 D9 E7  .Kx......-......
01C0: F6 A8 EE D2 CB D6 A9 13   5F 6A FC EE 33 7B 4F CF  ........_j..3.O.
01D0: A5 64 E4 87 05 B4 1A 9F   64 28 B3 20 5F 65 65 E0  .d......d(. _ee.
01E0: C5 A1 58 4E CA 68 CB 9B   4F 9F 84 4C 70 28 17 A8  ..XN.h..O..Lp(..
01F0: 74 98 94 0A D4 29 A4 3C   39 69 93 E3 60 0A 2D D6  t....).<9i..`.-.

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIHAzCCBOugAwIBAgIITWOS6Y7X5ZQwDQYJKoZIhvcNAQELBQAwgbkxCzAJBgNV
BAYTAkVTMUQwQgYDVQQHDDtCYXJjZWxvbmEgKHNlZSBjdXJyZW50IGFkZHJlc3Mg
YXQgd3d3LnVhbmF0YWNhLmNvbS9hZGRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0Eg
Uy5BLjEVMBMGA1UECwwMVFNQLVVBTkFUQUNBMRswGQYDVQQDDBJVQU5BVEFDQSBS
T09UIDIwMTYxGDAWBgNVBGEMD1ZBVEVTLUE2NjcyMTQ5OTAeFw0xNjAzMTEwOTEz
NTNaFw00MTAzMTEwOTEzNTNaMIG5MQswCQYDVQQGEwJFUzFEMEIGA1UEBww7QmFy
Y2Vsb25hIChzZWUgY3VycmVudCBhZGRyZXNzIGF0IHd3dy51YW5hdGFjYS5jb20v
YWRkcmVzcykxFjAUBgNVBAoMDVVBTkFUQUNBIFMuQS4xFTATBgNVBAsMDFRTUC1V
QU5BVEFDQTEbMBkGA1UEAwwSVUFOQVRBQ0EgUk9PVCAyMDE2MRgwFgYDVQRhDA9W
QVRFUy1BNjY3MjE0OTkwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
d5rtQey704cMzz7A1vuB4HLs0Y8YlH7BXKFAuxwzst1GOl7TzZzOeDEjGZMSjI00
JRUdmZ/lmG927tES5dDlrfDrNvKu3mof9j6Wjch4HmNqT6I30TXnhBNbtKEYHWxC
cIvQ0OKaFUUBEt+NzS6smyDAzbwyFUPSPid8JoGaGUMy7hhah38cLN408ffigCFT
ehZIsRvDnsU1WU34vcAYLLmgjsvBNmq2V+Ts8+vtrLcRbpQ8usMbwJSO1aoi71Lu
ISeBGJjqaszMPOty923PGHemImxHl5mHT13k5ha98EK4ZXMFfjxSVrypvpHgjThU
V3s4ZeaSpSbWkFxl6Tl++OTciMLOp66jwZV3I4DqeRmNXJkiRebs5u8bDDZxxeSP
RusoFI1cLm9cqCNy51hd2LNv8QECUNQ/RPon0sh+BSoSedppYXq6TFqpabE/FTnt
JBU7CMJV3EFJ/jSvXf6qj7JjInUQXajSxDdt0WrmDW8aQCRKCZ0Ml/Iwb8yk83/y
ZDt6E+Ez63V/x7sA2ZygG61zf4wOT95FNA4Z1atfOEcp/2uc5HXKrUTXTMDJJZfD
WMo30Ae1Rei94TRd/9XRqPdEk0B/VL5/991SlEX6Ol0NwKRPm6HNNZoWbdnmLEc+
CGnX1yj01R51Y4UTOalJ/W7oiNxmpZQAdAc9NN/gkwIDAQABo4IBCzCCAQcwHQYD
VR0OBBYEFFUs8byhXrnuoC+IVxBb/Jb3kZosMA8GA1UdEwEB/wQFMAMBAf8wgaYG
A1UdIASBnjCBmzCBmAYEVR0gADCBjzAzBggrBgEFBQcCARYnaHR0cDovL3d3dy51
YW5hdGFjYS5jb20vcHVibGljL3BraS9kcGMvMFgGCCsGAQUFBwICMEwMSkNlcnRp
ZmljYWRvIHJhw616IGRlIFVBTkFUQUNBLiBWZXIgaHR0cDovL3d3dy51YW5hdGFj
YS5jb20vcHVibGljL3BraS9kcGMvMA4GA1UdDwEB/wQEAwIBBjAcBgNVHREEFTAT
gRFpbmZvQHVhbmF0YWNhLmNvbTANBgkqhkiG9w0BAQsFAAOCAgEATAyOSKmK/yj6
JFb/RaHMmor8knkwQWVi3lFASKyfLQc6FfHoVjEgihu6HekIlMS7WBzetQVomaTR
TDu6eJeyo/+7CB+VGGHOYYjSdc8F8WI1HFN3f6ztKuM6zlVz3Xyj9BHhg1H4gqNL
Yxe99kq14xQEOR/fm0p7rVgVeeHhG8m1S5UGyyJ1ukeiB0d0PqwVWlG1np+i/nhf
nrxGSTnbRJyHzx6tuaLuQyHQU+Dg0TS8k65a8URioVkQ0CWb7yIyJ5bEBmPR2yqX
Owt6nYR8/3blrU99+wp67pmQttSggX3sB2a9WfY94Y5uIPB7JisOUBmqH23RjakE
c+UMLMjnvJQ82+1M7oGebnaVd1RVK+okemQ5zx57BzkzSl/i4G+Zxya8oQb2cIqF
HnvyCVXDOd4/CWNBLZQCTyGRUKOocvu1kKXgmVY6hTQGhM8Tr5yg/XT21gaAv3/7
th5ib2iGgq8Q8E3AW3ND+8N/qMjZ2aIkBKQYUFmLWiZt6n6ni73E2LQQEs+0uh9+
1xTPcI7AfDv+p0m6HDP0pq0t7BX0DQbh5QwPpiHBkB8atzE5gmQxnkt4/g0S2av5
Lc+U7ufZ5/ao7tLL1qkTX2r87jN7T8+lZOSHBbQan2QosyBfZWXgxaFYTspoy5tP
n4RMcCgXqHSYlArUKaQ8OWmT42AKLdY=
```

-----END CERTIFICATE-----

Certificate Service Provider Name (en): LLAMA.PE S.A.

Trade name (en)	LLAMA.PE S.A.
Information URI (en)	HTTP://LLAMA.PE
Service provider street address (es)	CAL.MARTIR JOSE OLAYA NRO. 129 INT. 902 LIMA - LIMA - MIRAFLORES
Service provider street address (en)	CAL.MARTIR JOSE OLAYA NRO. 129 INT. 902 LIMA - LIMA - MIRAFLORES
Service provider postal code (es)	15074
Service provider postal code (en)	15074
Service provider locality (es)	MIRAFLORES
Service provider locality (en)	MIRAFLORES
Service provider state (es)	LIMA
Service provider state (en)	LIMA
Service provider country (es)	PE
Service provider country (en)	PE

C=PE, O=LLAMA.PE, CN=Llama.pe SHA256 Standard CA

Type	CA/QC
Status	undersupervision
Status starting time	2018-10-26T19:51:03.000Z

Service digital identity (X509)

Version	3
Serial number	4514259705906360530
Signature algorithm	SHA256withRSA
Issuer	C=PE, O=LLAMA.PE, CN=Llama.pe Root CA
Valid from	Wed Jul 18 18:05:18 PET 2018
Valid to	Tue Jul 13 17:54:21 PET 2038
Subject	C=PE, O=LLAMA.PE, CN=Llama.pe SHA256 Standard CA
Public key	Sun RSA public key, 2048 bits modulus: 23709370699278415828643942147580377836369563071166627002786048859694992 04106201557398216535076187959768485144243154562204213240072929466575992 39686972999998774849465955653973161961418728386880110934668903106281027 65237836160564475177890255307598436088907054278027937466165531691697821 26564820140324254727346776900927500828677788929396586500772231489747830 78694118192481769273105866393158837503627314412328399337372816128936375 03690153391201011166461442952620725679649006946597589557007014070260931 56459162538184795022865038457003083685876624788330786152743539705997 57 51440402026920478593290955470883473868045727316 03 public exponent: 65537
Subject key identifier	5d885badeb65fbfe68a2e4d96f3d5772a2ef2b99
CRL distribution points	http://crl.llama.pe/llamaperootca.crl
Authority key identifier	041830168014a68344cd5597841f8809e1ad75e7295a5f98f7a4
Key usage	digitalSignature keyCertSign cRLSign

Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	3fd3e5385ddafee1216dca3c0739c871d7019122
SHA256 Thumbprint	0412eb962cbe52aa80d262b4555d3c7407ffeda28ffd0c7df36807b4d30a6c72

The decoded certificate:

```
[
[
 Version: V3
 Subject: C=PE, O=LLAMA.PE, CN=Llama.pe SHA256 Standard CA
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
23709370699278415828643942147580377836369563071166627002786048859694992041062015573982165350761879597684851442431545622042132400729294665759923968697299999877484946595565397
31619614187283868801109346689031062810276523783616056447517789025530759843608890705427802793746616553169169782126564820140324254727346776900927500828677788929396586500772231
48974783078694118192481769273105866393158837503627314412328399337372816128936375036901533912010111664614429526207256796490069465975895570070140702609315645916253818479502286
50384570030836858766247883330786152743539705997575144040202692047859329095547088347386804572731603
 public exponent: 65537
 Validity: [From: Wed Jul 18 18:05:18 PET 2018,
             To: Tue Jul 13 17:54:21 PET 2038]
 Issuer: C=PE, O=LLAMA.PE, CN=Llama.pe Root CA
 SerialNumber: [    3ea5df48 f26870d2]

Certificate Extensions: 5
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 5D 88 5B AD EB 65 FB FE   68 A2 E4 D9 6F 3D 57 72  ].[..e..h...o=Wr
0010: A2 EF 2B 99                                        ..+.
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: A6 83 44 CD 55 97 84 1F   88 09 E1 AD 75 E7 29 5A  ..D.U.......u.)Z
0010: 5F 98 F7 A4                                        _...
]

]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.llama.pe/llamaperootca.crl]
]]

[4]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 DigitalSignature
 Key_CertSign
 Crl_Sign
]

[5]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 69 ED BB E3 F8 AF 5F 93   3A 35 96 2F 4C 26 19 2F  i....._.:5./L&./
0010: 69 BD 09 AA 95 E2 93 C3   25 DA 28 27 81 77 1E 89  i.......%.('.w..
0020: 92 0F 89 CE F1 27 BD EB   71 67 7A AF 67 9E 11 3D  .....'..qgz.g..=
0030: 41 F9 6C 0A 3F 1E 2E 74   E3 0B A7 81 A0 EB 17 2B  A.l.?..t.......+
0040: 3A 0F 8F 5B F0 D6 1A CB   C5 FB BC 2A 58 FD 44 14  :..[.......*X.D.
0050: F1 AB 29 53 82 51 17 A7   0D 2F 24 2B E2 D7 F0 17  ..)S.Q.../$+....
0060: 7A DA A1 19 F5 DA C3 AE   39 DD F8 D9 B1 9D 9A 0B  z.......9.......
0070: 2A C7 31 97 CE 2A 13 DE   6E FF C5 7E D7 A3 E9 A7  *.1..*..n.......
0080: 3D AD E7 3F A1 76 D7 5A   4E 67 F2 36 DA CD BE 15  =..?.v.ZNg.6....
0090: A7 24 A9 77 32 1D 7E 7D   27 10 6F 67 41 D7 67 B1  .$.w2...'.ogA.g.
00A0: 56 3E 59 8E 59 B5 6A FE   F1 D3 91 5A 5A 68 6F BE  V>Y.Y.j....ZZho.
00B0: 28 B0 9B AF AE 1C 3F 73   3D 0F DF 2D 6B 08 23 A7  (.....?s=..-k.#.
00C0: 84 FA B2 7B 36 CA B0 70   F0 9A F8 40 CC A6 17 EF  ....6..p...@....
00D0: 09 04 99 14 64 93 F9 71   6A EF 26 EE 76 D8 18 43  ....d..qj.&.v..C
00E0: C0 C2 68 8F B2 C5 B6 5A   BE E0 09 DB DA 3C B7 2F  ..h....Z.....<./
00F0: E2 95 94 4B D4 CE CC 54   38 00 D0 12 97 9B F6 17  ...K...T8.......

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIDoDCCAoigAwIBAgIIPqXfSPJocNIwDQYJKoZIhvcNAQELBQAwOzEZMBcGA1UE
AwwQTGxhbWEucGUgUm9vdCBDQTERMA8GA1UECgwITExBTUEuUEUxCzAJBgNVBAYT
AlBFMB4XDTE4MDcxODIzMDUxOFoXDTM4MDcxMzIyNTQyMVowRjEkMCIGA1UEAwwb
TGxhbWEucGUgU0hBMjU2IFN0YW5kYXJkIENBMREwDwYDVQQKDAhMTEFNQS5QRTEL
MAkGA1UEBhMCUEUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC70HwZ
u6wAQIYR7TMNbYm3KJxv60Ax0FpARIt+4hGOrK6LN0OBPQA1BUJqg27zrPx2PG5J
lC4aqvd6QgyeQJC3hdcsThYMQbq62aPjQaVWlY5dPWNtWRhi/3YCXNyLlMs16TZf
Rx5N/KvgJSBrAYRzPMqRhontKmrxKzjZTl29EfyBdLu5WwGv5Z2sKmoArp0Te/Np
```

/9+ND4mopl7wsgBWfv8TxCrWhkAxvLm2R4psRO6eJgCJYWN7AyzkRH3YR68yrfz2
bg3VFPiVVydgSrEYUFwKXCuKZfx2jOCDIPjf8L11nuhDL0U0b4ko5HgQ4SSPqlWY
tKMbXjI5AJEvdzjTAgMBAAGjgZwwgZkwDwYDVR0TAQH/BAUwAwEB/zAfBgNVHSME
GDAWgBSmg0TNVZeEH4gJ4a115ylaX5j3pDA2BgNVHR8ELzAtMCugKaAnhiVodHRw
Oi8vY3JsLmxsYW1hLnBlL2xsYW1hcGVyb290Y2EuY3JsMB0GA1UdDgQWBBRdiFut
62X7/mii5NlvPVdyou8rmTAOBgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQAD
ggEBAGntu+P4r1+TOjWWL0wmGS9pvQmqleKTwyXaKCeBdx6Jkg+JzvEnvetxZ3qv
Z54RPUH5bAo/Hi504wungaDrFys6D49b8NYay8X7vCpY/UQU8aspU4JRF6cNLyQr
4tfwF3raoRn12sOuOd342bGdmgsqxzGXzioT3m7/xX7Xo+mnPa3nP6F211pOZ/I2
2s2+FackqXcyHX59JxBvZ0HXZ7FWPlmOWbVq/vHTkVpaaG++KLCbr64cP3M9D98t
awgjp4T6sns2yrBw8Jr4QMymF+8JBJkUZJP5cWrvJu522BhDwMJoj7LFtlq+4Anb
2jy3L+KVlEvUzsxUOADQEpeb9hc=
-----END CERTIFICATE-----

C=PE, O=LLAMA.PE, CN=Llama.pe Root CA

Type	CA/QC
Status	undersupervision
Status starting time	2018-10-25T15:24:14.000Z

Service digital identity (X509)

Version	3
Serial number	4191800503798586627
Signature algorithm	SHA256withRSA
Issuer	C=PE, O=LLAMA.PE, CN=Llama.pe Root CA
Valid from	Wed Jul 18 17:54:21 PET 2018
Valid to	Tue Jul 13 17:54:21 PET 2038
Subject	C=PE, O=LLAMA.PE, CN=Llama.pe Root CA
Public key	Sun RSA public key, 2048 bits modulus: 22379900198102108658489878949118817575116657322040383888609673007180142 82979588614726534175841890493320940464890137193319750374100829878813401 24005358593323747074356965215714689618711622734240042212113441144020579 29674020300653284654989380155003158754334229067359683890031148452713588 70206232334338102657093085531279792046125433499346126527831321742416273 20461957137939368800060534457121821184879855109854661470037772061733311 30921387439743015438586215273763505302581718281342343663523733969794911 47075279454902739195692429760228804808520824759556081621379087118665473 62571633673764803055125539550954775415010306029 19 public exponent: 65537
Subject key identifier	a68344cd5597841f8809e1ad75e7295a5f98f7a4
Authority key identifier	041830168014a68344cd5597841f8809e1ad75e7295a5f98f7a4
Key usage	digitalSignature keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	282bf316e004fdad6ab547a6cc9cd3c50e616f12
SHA256 Thumbprint	228ca84d00687d20dfe5434a7ac982e75532a8146601896edcd9146e54a289fe

The decoded certificate:

```
[
[
 Version: V3
 Subject: C=PE, O=LLAMA.PE, CN=Llama.pe Root CA
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
22379900198102108658489878949118817575116657322040383888609673007180142829795886147265341758418904933209404648901371933197503741008298788134012400535859332374707435696521571
46896187116227342400422121134411440205792967402030065328465498938015500315875433422906735968389003114845271358870206232334338102657093085531279792046125433499346126527831321
74241627320461957137939368800060534457121821184879855109854661470037772061733311309213874397430154385862152737635053025817182813423436635237339697949114707527945490273919569
24297602288048085208247595560816213790871186654736257163367376480305512553955095477541501030602919
 public exponent: 65537
 Validity: [From: Wed Jul 18 17:54:21 PET 2018,
             To: Tue Jul 13 17:54:21 PET 2038]
 Issuer: C=PE, O=LLAMA.PE, CN=Llama.pe Root CA
 SerialNumber: [    3a2c4459 5e37dd03]

Certificate Extensions: 4
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
```

```
0000: A6 83 44 CD 55 97 84 1F   88 09 E1 AD 75 E7 29 5A  ..D.U.......u.)Z
0010: 5F 98 F7 A4                                        _...
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: A6 83 44 CD 55 97 84 1F   88 09 E1 AD 75 E7 29 5A  ..D.U.......u.)Z
0010: 5F 98 F7 A4                                        _...
]

]

[3]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 DigitalSignature
 Key_CertSign
 Crl_Sign
]

[4]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 70 26 D4 59 DE EA D3 8B   FE E2 F2 7E 64 FF 83 70  p&.Y........d..p
0010: F5 AE 7A 7D 89 3D 26 14   F4 C0 CB F1 42 FF 36 0B  ..z..=&.....B.6.
0020: 08 56 9C A5 E6 58 83 19   C7 E7 31 64 25 74 52 0A  .V...X....1d%tR.
0030: 61 40 7F 4E 4C DA D6 D4   BA 52 06 4D 90 AC FB 3E  a@.NL....R.M...>
0040: 4B 6B 45 5D 62 7C 00 A7   B0 E8 BC AB 8A 53 CD 6B  KkE]b........S.k
0050: 50 7A 79 41 79 85 73 85   BA AC CA 99 5E D2 E0 DE  PzyAy.s.....^...
0060: 4C DF 8B 6C BD 29 F4 DE   89 98 C4 FC C8 83 58 F3  L..l.).........X.
0070: FA E5 79 45 EF 18 42 DE   F1 0E CE 1D F2 3F C9 11  ..yE..B......?..
0080: 91 26 F8 49 46 D1 45 E5   7E 64 16 F6 BA 7E 1E 33  .&.IF.E..d.....3
0090: 77 B1 15 87 3E 45 C9 08   8C 0F 4F C8 C0 4A EF 95  w...>E....O..J..
00A0: CF 8B 45 5E 26 6E 2A 5A   86 18 B9 0A FF E1 CA E8  ..E^&n*Z........
00B0: EF A0 32 C8 82 53 A7 D2   2C 51 63 F9 DC 6C EA 6E  ..2..S..,Qc..l.n
00C0: 5E 19 74 1B 85 3C 9A 05   E8 59 13 B3 55 9B 83 7F  ^.t..<...Y..U...
00D0: 48 10 30 62 2A D9 27 EA   95 2D 0A AE 9B 22 FB B2  H.0b*.'..-...".. 
00E0: 81 8B 0F 09 0A 03 91 E1   51 29 87 32 50 2B AF A0  ........Q).2P+..
00F0: 0F F7 6A 48 6B DE EF 25   ED A4 EA 4E 7F 00 E8 6D  ..jHk..%...N...m

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIIOixEWV433QMwDQYJKoZIhvcNAQELBQAwOzEZMBcGA1UE
AwwQTGxhbWEucGUgUm9vdCBDQTERMA8GA1UECgwITExBTUEuUEUxCzAJBgNVBAYT
AlBFMB4XDTE4MDcxODIyNTQyMVoXDTM4MDcxMzIyNTQyMVowOzEZMBcGA1UEAwwQ
TGxhbWEucGUgUm9vdCBDQTERMA8GA1UECgwITExBTUEuUEUxCzAJBgNVBAYTAlBF
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsUhv+jmfYMop5RUOZUZY
aDwJtREVNMrpFu8Wu1ybT94LFGO8h11bwnOy92R+ARPSm/JF8jzBu/M7/JKQqe1d
UEOaleWvNRMko2CTvAdkkmWdaAQloR+D5N8DgoAz/XStGwOUInuKCj3NDfdmN81j
88hicK1/jsf0Cm6e8eIBdtpkwwwJPuQQMU4sFK1sAFC453etEVCoXVYjELUVdlm6
ZaB0otpqYG7xiKRL2iaxGOxX7U7jUoYMKQMKfD5foiNyJojNq3wFpkZiifvqf6oY
xw41w8OJ0tPvEDVCJKn0bouOF2fctVsrvB6uiURvIuiVJpHOwggcjQA32lo+tGuY
pwIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MB8GA1UdIwQYMBaAFKaDRM1Vl4Qf
iAnhrXXnKVpfmPekMB0GA1UdDgQWBBSmg0TNVZeEH4gJ4a115ylaX5j3pDAOBgNV
HQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggEBAHAm1Fne6tOL/uLyfmT/g3D1
rnp9iT0mFPTAy/FC/zYLCFacpeZYgxnH5zFkJXRSCmFAf05M2tbUulIGTZCs+z5L
a0VdYnwAp7DovKuKU81rUHp5QXmFc4W6rMqZXtLg3kzfi2y9KfTeiZjE/MiDWPP6
5XlF7xhC3vEOzh3yP8kRkSb4SUbRReV+ZBb2un4eM3exFYc+RckIjA9PyMBK75XP
i0VeJm4qWoYYuQr/4cro76AyyIJTp9IsUWP53Gzqbl4ZdBuFPJoF6FkTs1Wbg39I
EDBiKtkn6pUtCq6bIvuygYsPCQoDkeFRKYcyUCuvoA/3akhr3u8l7aTqTn8A6G0=
-----END CERTIFICATE-----
```

Certificate Service Provider Name (en): THOMAS SIGNE DE PERU S.A.

Trade name (en)	THOMAS SIGNE DE PERU S.A.
Information URI (en)	HTTPS://THOMAS-SIGNE.PE
Service provider street address (es)	CAL.C MZA. A LOTE. 15 OTR. CENTRO INDUSTRIAL LAS PRADERAS DE LURIN (KM 35.5 DE LA PANAMERICANA SUR) LIMA - LIMA - LURIN
Service provider street address (en)	CAL.C MZA. A LOTE. 15 OTR. CENTRO INDUSTRIAL LAS PRADERAS DE LURIN (KM 35.5 DE LA PANAMERICANA SUR) LIMA - LIMA - LURIN
Service provider postal code (es)	LIMA16
Service provider postal code (en)	LIMA16
Service provider locality (es)	LURIN

Service provider locality (en)	LURIN
Service provider state (es)	LIMA
Service provider state (en)	LIMA
Service provider country (es)	PE
Service provider country (en)	PE

CN=SIGNE Autoridad de Certificacion, SERIALNUMBER=A11029279, O=SIGNE S.A., L=Avenida de la Industria 18. Tres Cantos 28760-Madrid, C=ES

Type	CA/QC
Status	undersupervision
Status starting time	2019-07-17T20:50:56.000Z

Service digital identity (X509)

Version	3
Serial number	2445720188065766261
Signature algorithm	SHA256withRSA
Issuer	CN=Autoridad de Certificacion Firmaprofesional CIF A62634068, C=ES
Valid from	Wed Jul 29 06:22:23 PET 2015
Valid to	Mon Dec 30 23:02:55 PET 2030
Subject	CN=SIGNE Autoridad de Certificacion, SERIALNUMBER=A11029279, O=SIGNE S.A., L=Avenida de la Industria 18. Tres Cantos 28760-Madrid, C=ES
Public key	Sun RSA public key, 2048 bits modulus: 25953646932771384799125486082044833995584509178602282676461069866790406 86669712733459923075443274240876335762403409004840161780799198497717574 27666286948610610077269993082533182203682191179777610890815678025967591 74934379437237265954519891508783237835970126703022813934562318645550332 08393346021574390571032786851307665350564022609923175214543125140803731 72566488137368067705242923382591405640291595277407381572586923587549995 88471222360414961359987442052988620146799102554233051887886544607858489 78031828289482649391153243350377665262870846510103085132779156812563722 37465673720147712738291559887653861919680542737 97 public exponent: 65537
Subject key identifier	90ad1a31fd47456d32444318859764c738ae6da8
CRL distribution points	http://crl.firmaprofesional.com/fproot.crl
Authority key identifier	04183016801465cdebab351e003e7ed574c01cb473470e1a642f
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=0
SHA1 Thumbprint	e6b52b5d52e5cde9862ac1de668ec953ad3659bd
SHA256 Thumbprint	1cb470728cf56f302003bb0e4eb062414fa11d4f97e3f061170c96c88071d711

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=SIGNE Autoridad de Certificacion, SERIALNUMBER=A11029279, O=SIGNE S.A., L=Avenida de la Industria 18. Tres Cantos 28760-Madrid, C=ES
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
25953646932771384799125486082044833995584509178602282676461069866790406866697127334599230754432742408763357624034090048401617807991984977175742766628694861061007726999308253318220368219117977761089081567802596759174934379437237265954519891508783237835970126703022813934562318645550332083933460215743905710327868513076653505640226099231752145431251408037317256648813736806770524292338259140564029159527740738157258692358754999588471222360414961359987442052988620146799102554233051887886544607858489780318282894826493911532433503776652628708465101030851327791568125637223746567372014771273829155988765386191968054273797
 public exponent: 65537
 Validity: [From: Wed Jul 29 06:22:23 PET 2015,
             To: Mon Dec 30 23:02:55 PET 2030]
```

```
 Issuer: CN=Autoridad de Certificacion Firmaprofesional CIF A62634068, C=ES
 SerialNumber: [    21f0f18d 95a95b75]

Certificate Extensions: 8
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 90 AD 1A 31 FD 47 45 6D   32 44 43 18 85 97 64 C7  ...1.GEm2DC...d.
0010: 38 AE 6D A8                                        8.m.
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 65 CD EB AB 35 1E 00 3E   7E D5 74 C0 1C B4 73 47  e...5..>..t...sG
0010: 0E 1A 64 2F                                        ..d/
]

]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.firmaprofesional.com/fproot.crl]
]]

[4]: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
 clientAuth
 emailProtection
 OCSPSigning
 1.3.6.1.4.1.311.20.2.2
]

[5]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[6]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 81 E5 1E 81 E2 00 43   00 65 00 72 00 74 00 69  0......C.e.r.t.i
0010: 00 66 00 69 00 63 00 61   00 64 00 6F 00 20 00 64  .f.i.c.a.d.o. .d
0020: 00 65 00 20 00 41 00 75   00 74 00 6F 00 72 00 69  .e. .A.u.t.o.r.i
0030: 00 64 00 61 00 64 00 20   00 64 00 65 00 20 00 43  .d.a.d. .d.e. .C
0040: 00 65 00 72 00 74 00 69   00 66 00 69 00 63 00 61  .e.r.t.i.f.i.c.a
0050: 00 63 00 69 00 F3 00 6E   00 2E 00 20 00 43 00 6F  .c.i...n... .C.o
0060: 00 6E 00 73 00 75 00 6C   00 74 00 65 00 20 00 6C  .n.s.u.l.t.e. .l
0070: 00 61 00 73 00 20 00 63   00 6F 00 6E 00 64 00 69  .a.s. .c.o.n.d.i
0080: 00 63 00 69 00 6F 00 6E   00 65 00 73 00 20 00 64  .c.i.o.n.e.s. .d
0090: 00 65 00 20 00 75 00 73   00 6F 00 20 00 65 00 6E  .e. .u.s.o. .e.n
00A0: 00 20 00 68 00 74 00 74   00 70 00 3A 00 2F 00 2F  . .h.t.t.p.:././
00B0: 00 77 00 77 00 77 00 2E   00 66 00 69 00 72 00 6D  .w.w.w...f.i.r.m
00C0: 00 61 00 70 00 72 00 6F   00 66 00 65 00 73 00 69  .a.p.r.o.f.e.s.i
00D0: 00 6F 00 6E 00 61 00 6C   00 2E 00 63 00 6F 00 6D  .o.n.a.l...c.o.m
00E0: 00 2F 00 63 00 70 00 73                            ./.c.p.s

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 23 68 74 74 70 3A 2F   2F 77 77 77 2E 66 69 72  .#http://www.fir
0010: 6D 61 70 72 6F 66 65 73   69 6F 6E 61 6C 2E 63 6F  maprofesional.co
0020: 6D 2F 63 70 73                                     m/cps

]]  ]
]

[7]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:0
]

[8]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://crl.firmaprofesional.com/caroot.crt,
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://ocsp.firmaprofesional.com]
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: C9 51 6C 02 F7 7B 4B 40   FB 88 02 AE BD 0C 0D E4  .Ql...K@........
0010: 35 CE 49 C9 39 9E 53 D0   D5 09 F4 A8 B1 92 E5 DA  5.I.9.S.........
0020: A1 FA D7 7A 95 3E DF 16   D0 F2 68 9C 46 73 58 8A  ...z.>....h.FsX.
0030: 1B 2E 6E 10 04 B9 CA 73   34 EB 98 2C 3A A4 50 13  ..n....s4..,:.P.
0040: 2F 8D 7E 63 F7 37 65 F1   E9 54 50 6C 5C F1 E4 63  /..c.7e..TPl\..c
```

```
0050: AC C2 42 CC C6 A2 FB 27   5C A8 DD D8 9B 33 CE BB  ..B....'\....3..
0060: CC 06 FF 61 85 D8 C5 6A   C0 58 EE 0F 1E 96 FA 74  ...a...j.X.....t
0070: 3C 09 D7 63 99 44 68 30   C4 B4 79 50 50 2C B1 E1  <..c.Dh0..yPP,..
0080: C7 52 33 0D EF D5 45 68   6D 2E 06 3D C4 AE 1F 48  .R3...Ehm..=...H
0090: 2D EA 4A 5A B4 4E C9 86   29 21 2E 28 37 5D B4 D6  -.JZ.N..)!.(7]..
00A0: C5 81 A9 52 97 B9 00 85   C1 7D 01 45 FC 45 25 8E  ...R.......E.E%.
00B0: 00 5B 20 29 B4 21 8C 0E   5F 07 77 93 58 CF 1C 53  .[ ).!.._.w.X..S
00C0: 5A 36 2E 69 CB 8A 9E EA   DB 5A 7B 5F 1B A0 60 0D  Z6.i.....Z._..`.
00D0: 08 45 F3 FE B9 6C 85 E5   EA 30 00 56 3D C4 2A 12  .E...l...0.V=.*.
00E0: E8 1F DC BD 95 5D 12 6C   15 B8 E2 F8 BF D3 B6 1E  .....].l........
00F0: 52 47 D1 66 C4 B5 30 41   3C E6 36 77 2B 08 E5 AE  RG.f..0A<.6w+...
0100: 4B 81 6A 1A C6 DC 58 84   82 EF 23 C4 7B 2C 60 2B  K.j...X...#..,`+
0110: 75 2C 19 A4 97 28 F1 EC   6D 4D 86 B0 0E D5 76 4C  u,...(..mM....vL
0120: 2E AB B2 A3 59 50 DA F0   0E B0 43 CF 70 05 67 18  ....YP....C.p.g.
0130: CB 3F 87 3E E3 3E DC C1   E4 BC 6B 48 50 9C 92 6C  .?.>.>....kHP..l
0140: C1 73 C8 B4 A3 33 33 01   CA F2 2D 55 88 19 26 17  .s...33...-U..&.
0150: 67 D7 FE F3 94 0D B8 AB   76 29 66 B5 65 6A 04 BD  g.......v)f.ej..
0160: 28 A5 46 87 C9 57 68 43   61 C2 D7 8F A6 F3 90 5C  (.F..WhCa......\
0170: 5E 6D EA 19 89 63 19 F7   12 5B 89 80 2F FA 87 77  ^m...c...[../..w
0180: 5E 96 14 62 51 D4 50 9E   6C 8C EB BD ED F6 FA 4C  ^..bQ.P.l......L
0190: F2 F0 46 7F 40 C9 C5 1F   47 52 BB 0A 0F 78 75 43  ..F.@...GR...xuC
01A0: 8C 89 94 01 85 26 63 4D   7E 08 5F CC F5 BE 51 BF  .....&cM..~_...Q.
01B0: 5F 61 2C C7 5B D8 3B 41   F6 8C D5 5D DF 43 3F 32  _a,.[.;A...].C?2
01C0: 90 54 52 D8 CC 3C 2E AB   AA F5 E0 6E 5E 54 DA 84  .TR..<.....n^T..
01D0: 76 60 7C 6E CF C7 F6 99   24 FE 85 40 50 38 AC 6A  v`.n....$..@P8.j
01E0: D8 5A 06 2C DA 58 34 08   90 23 64 C9 7B 60 03 80  .Z.,.X4..#d..`..
01F0: 97 6F 0E E3 C7 6A 45 8B   3F B6 C8 40 E6 4F 72 89  .o...jE.?..@.Or.

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIHCzCCBPOgAwIBAgIIIfDxjZWpW3UwDQYJKoZIhvcNAQELBQAwUTELMAkGA1UE
BhMCRVMxQjBABgNVBAMMOUF1dG9yaWRhZCBkZSBDZXJ0aWZpY2FjaW9uIEZpcm1h
cHJvZmVzaW9uYWwgQ0lGIEE2MjYzNDA2ODAeFw0xNTA3MjkxMTIyMjNaFw0zMDEy
MzEwNDAyNTVaMIGgMQswCQYDVQQGEwJFUzE9MDsGA1UEBww0QXZlbmlkYSBkZSBs
YSBJbmR1c3RyaWEgMTguIFRyZXMgQ2FudG9zIDI4NzYwLU1hZHJpZDETMBEGA1UE
CgwKU0lHTkUgUy5BLjESMBAGA1UEBRMJQTExMDI5Mjc5MSkwJwYDVQQDDCBTSUdO
RSBBdXRvcmlkYWQgZGUgQ2VydGlmaWNhY2lvbjCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAM2XrSfJuBB206FoW+I/I9HbW4VTois+IqlkOZhY5zFqu2Sx
YH/GLFsI3aVwzbt6XYk/ukhJgA+W7OunjNOmHDW+0EGaueWdTdHNzguEB6SPmKqM
enodGrPWABJpI9Jdy864O+riOqD/6DiZYA4HL2+xfoMCESixeNuO67Xw/7Ymcdwq
rkcibJmfQGUUBKbE48yyghrkehDXfvgBeF2COqsMdXsvYdAxXD13wZqMBkmZIYTY
STxF788LK3Hs2H1q3nIrI+bzO2tfUTv3C0X9A6ke7Q6mev1hZ9IDepW2DPa7om0m
dnsgzXSXBQP/Qul/CcGFmxf5Ko8gLq6F9ulP5wUCAwEAAaOCApUwggKRMHQGCCsG
AQUFBwEBBGgwZjA2BggrBgEFBQcwAoYqaHR0cDovL2NybC5maXJtYXByb2Zlc2lv
bmFsLmNvbS9jYXJvb3QuY3J0MCwGCCsGAQUFBzABhiBodHRwOi8vb2NzcC5maXJt
YXByb2Zlc2lvbmFsLmNvbTAdBgNVHQ4EFgQUkK0aMf1HRW0yREMYhZdkxziubagw
EgYDVR0TAQH/BAgwBgEB/wIBADAfBgNVHSMEGDAWgBRlzeurNR4APn7VdMActHNH
DhpkLzCCAUEGA1UdIASCATgwggE0MIIBMAYEVR0gADCCASYwgfIGCCsGAQUFBwIC
MIHlHoHiAEMAZQByAHQAaQBmAGkAYwBhAGQAbwAgAGQAZQAgAEEAdQB0AG8AcgBp
AGQAYQBkACAAZABlACAAQwBlAHIAdABpAGYAaQBjAGEAYwBpAPMAbgAuACAAQwBv
AG4AcwB1AGwAdABlACAAbABhAHMAIABjAG8AbgBkAGkAYwBpAG8AbgBlAHMAIABk
AGUAIAB1AHMAbwAgAGUAbgAgAGgAdAB0AHAAOgAvAC8AdwB3AHcALgBmAGkAcgBt
AGEAcAByAG8AZgBlAHMAaQBvAG4AYQBsAC4AYwBvAG0ALwBjAHAAczAvBggrBgEF
BQcCARYjaHR0cDovL3d3dy5maXJtYXByb2Zlc2lvbmFsLmNvbS9jcHMwOwYDVR0f
BDQwMjAwoC6gLIYqaHR0cDovL2NybC5maXJtYXByb2Zlc2lvbmFsLmNvbS9mcHJv
b3QuY3JsMA4GA1UdDwEB/wQEAwIBBjAzBgNVHSUELDAqBggrBgEFBQcDAgYIKwYB
BQUHAwQGCCsGAQUFBwMJBgorBgEEAYI3FAICMA0GCSqGSIb3DQEBCwUAA4ICAQDJ
UWwC93tLQPuIAq69DA3kNc5JyTmeU9DVCfSosZLl2qH613qVPt8W0PJonEZzWIob
Lm4QBLnKczTrmCw6pFATL41+Y/c3ZfHpVFBsXPHkY6zCQszGovsnXKjd2JszzrvM
Bv9hhdjFasBY7g8elvp0PAnXY5lEaDDEtHlQUCyx4cdSMw3v1UVobS4GPcSuH0gt
6kpatE7JhikhLig3XbTWxYGpUpe5AIXBfQFF/EUljgBbICm0IYwOXwd3kljPHFNa
Ni5py4qe6ttae18boGANCEXz/rlsheXqMABWPcQqEugf3L2VXRJsFbji+L/Tth5S
R9FmxLUwQTzmNncrCOWuS4FqGsbcWISC7yPEeyxgK3UsGaSXKPHsbU2GsA7Vdkwu
q7KjWVDa8A6wQ89wBWcYyz+HPuM+3MHkvGtIUJySbMFzyLSjMzMByvItVYgZJhdn
l/7zlA24q3YpZrVlagS9KKVGh8lXaENhwtePpvOQXF5t6hmJYxn3EluJgC/6h3de
lhRiUdRQnmyM673t9vpM8vBGf0DJxR9HUrsKD3h1Q4yJlAGFJmNNfghfzPW+Ub9f
YSzHW9g7QfaM1V3fQz8ykFRS2Mw8Lquq9eBuXlTahHZgfG7Px/aZJP6FQFA4rGrY
WgYs2lg0CJAjZMl7YAOAl28O48dqRYs/tshA5k9yiQ==
-----END CERTIFICATE-----
```

CN=Autoridad de Certificacion Firmaprofesional CIF A62634068, C=ES

Type	CA/QC
Status	undersupervision
Status starting time	2019-07-17T20:21:18.000Z

Service digital identity (X509)

Version	3
Serial number	1977337328857672817
Signature algorithm	SHA256withRSA
Issuer	CN=Autoridad de Certificacion Firmaprofesional CIF A62634068, C=ES
Valid from	Tue Sep 23 10:22:07 PET 2014
Valid to	Mon May 05 10:22:07 PET 2036

Subject	CN=Autoridad de Certificacion Firmaprofesional CIF A62634068, C=ES
Public key	Sun RSA public key, 4096 bits modulus: 826485213734724534139558653444712595965061511481086908348901524397436444795273211181636335369797141950525036010648473085518670072866035792533856438041221141932966272342283601989810361717157272554224009619645583194 093830431461529088326021959411964542338599854387433413716462611105852866 619770314642703653105149477259409112639028942787990412416188800852507879918495693358130720937085938761022643583552256754358238722400156232299727058216730176976107819075552676166007691186916985917495747848639546660 564707341731404804570010301527604151383832915053501958744732901661320626 742207642568676667151838477644810305883970361955206965395787849068883422579681308731031140259640758682552641766424489596620 257968130873103114025964075868825526417664244895966203270465947840359834617732018207870889340575620144469600414320106663965579768573757519715881056694242029009636835747928676391494060287447286252889712854000732582 194396094409292015244765655882034365300720239543796180220782615691851461 114801447782908780749481781273078630545117160363432796437682716108759321 360917642482762790682579895929590188459560616594190398331217739045414727 827726219996097637649136171644068253593179321342142671851909408765983990 073909514086266014002802019049423200647582854525193384566978115046828734 465422975415533443483035471 public exponent: 65537
Subject key identifier	65cdebab351e003e7ed574c01cb473470e1a642f
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=1
SHA1 Thumbprint	0bbec2272249cb39aadb355c53e38cae78ffb6fe
SHA256 Thumbprint	57de0583efd2b26e0361da99da9df4648def7ee8441c3b728afa9bcde0f9b26a

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=Autoridad de Certificacion Firmaprofesional CIF A62634068, C=ES
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
826485213734724534139558653444712595965061511481086908348901524397436444795273211181636335369797141950525036010648473085518670072866035792533856438041221141932966272342283601989810361717157272554224009619645583194093830431461529088326021959411964542338599854387433413716462611105852866197703146427036531051494772594091126390289427879904124161888008525078799184956933581307209370859387610226435835522567543582387224001562322997270582167301769761078190755526761660076911869169859174957478486395466605647073417314048045700103015276041513838329150535019587447329016613206274220764256867666715183847764481030588397036195520696539578784906888342257968130873103114025964075868825526417664244895966203270465947840359834617732018207870889340575620144469600414320106663965579768573757519715881056694242029009636835747928676391494060287447286252889712854000732582194396094409292015244765655882034365300720239543796180220782615691851461480144778290878074948178127307863054511716036343279643768271610875932360917642482762790682579895929590188459560616594190398331217739045414727827726219996097637649136171644068253593179321342142671851909408765983990730951408626601400280201904942320064758285452519338456697811504682873465422975415533443483035471
 public exponent: 65537
 Validity: [From: Tue Sep 23 10:22:07 PET 2014,
              To: Mon May 05 10:22:07 PET 2036]
 Issuer: CN=Autoridad de Certificacion Firmaprofesional CIF A62634068, C=ES
 SerialNumber: [    1b70e9d2 ffae6c71]

Certificate Extensions: 4
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 65 CD EB AB 35 1E 00 3E   7E D5 74 C0 1C B4 73 47  e...5..>..t...sG
0010: 0E 1A 64 2F                                        ..d/
]
]

[2]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[3]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 23 68 74 74 70 3A 2F   2F 77 77 77 2E 66 69 72  .#http://www.fir
0010: 6D 61 70 72 6F 66 65 73   69 6F 6E 61 6C 2E 63 6F  maprofesional.co
0020: 6D 2F 63 70 73                                     m/cps

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 50 1E 4E 00 50 00 61   00 73 00 65 00 6F 00 20  0P.N.P.a.s.e.o.
0010: 00 64 00 65 00 20 00 6C   00 61 00 20 00 42 00 6F  .d.e. .l.a. .B.o
```

```
0020: 00 6E 00 61 00 6E 00 6F   00 76 00 61 00 20 00 34  .n.a.n.o.v.a. .4
0030: 00 37 00 20 00 42 00 61   00 72 00 63 00 65 00 6C  .7. .B.a.r.c.e.l
0040: 00 6F 00 6E 00 61 00 20   00 30 00 38 00 30 00 31  .o.n.a. .0.8.0.1
0050: 00 37                                              .7

]]  ]
]

[4]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:1
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 74 87 28 02 2B 77 1F 66   89 64 ED 8F 74 2E 46 1C  t.(.+w.f.d..t.F.
0010: BB A8 F8 F8 0B 1D 83 B6   3A A7 E8 45 8A 07 B7 E0  ........:..E....
0020: 3E 20 CB E1 08 DB 13 08   F8 28 A1 35 B2 80 B3 0B  > .......(.5....
0030: 51 C0 D3 56 9A 8D 33 45   49 AF 49 F0 E0 3D 07 7A  Q..V..3EI.I..=.z
0040: 45 13 5A FF C8 97 D8 D3   18 2C 7D 96 F8 DD A2 65  E.Z......,.....e
0050: 43 70 93 90 15 BA 90 DF   E8 19 B0 DB 2C 8A 60 0F  Cp..........,.`.
0060: B7 6F 94 07 1E 1D A6 C9   85 F6 BD 34 F8 40 78 62  .o.........4.@xb
0070: 10 70 3A BE 7D 4B 39 81   A9 10 D4 96 41 BB F8 5F  .p:..K9.....A.._
0080: 1C 0B 1D 08 F2 B1 B0 89   7A F2 F7 A0 E0 C4 8F 8B  ........z.......
0090: 78 B5 3B 58 A5 23 8E 4F   55 FE 36 3B E0 0C B7 CA  x.;X.#.OU.6;....
00A0: 2A 30 41 20 B4 80 CD AE   FC 76 66 73 A8 AE 6E E1  *0A .....vfs..n.
00B0: 7C DA 03 E8 94 20 E6 22   A3 D0 1F 90 5D 20 53 14  ..... ."....] S.
00C0: 26 57 DA 54 97 DF 16 44   10 01 1E 88 66 8F 72 38  &W.T...D....f.r8
00D0: 93 DD 20 B7 34 BE D7 F1   EE 63 8E 47 79 28 06 FC  .. .4....c.Gy(..
00E0: F3 59 45 25 60 22 33 1B   A3 5F A8 BA 2A DA 1A 3D  .YE%`"3._..*..=
00F0: CD 40 EA 8C EE 05 15 95   D5 A5 2C 20 2F A7 98 28  .@........, /..(
0100: EE 45 FC F1 B8 88 00 2C   8F 42 DA 51 D5 9C E5 13  .E.....,.B.Q....
0110: 68 71 45 43 8B 9E 0B 21   3C 4B 5C 05 DC 1A 9F 98  hqEC...!<K\.....
0120: 8E DA BD 22 9E 72 CD AD   0A CB CC A3 67 9B 28 74  ...".r......g.(t
0130: C4 9B D7 1A 3C 04 58 A6   82 9D AD C7 7B 6F FF 80  ....<.X......o..
0140: 96 E9 F8 8D 6A BD 18 90   1D FF 49 1A 90 52 37 93  ....j.....I..R7.
0150: 2F 3C 02 5D 82 76 0B 51   E7 16 C7 57 F8 38 F9 A7  /<.].v.Q...W.8..
0160: CD 9B 22 54 EF 63 B0 15   6D 53 65 03 4A 5E 4A A0  ..".T.c..mSe.J^J.
0170: B2 A7 8E 49 00 59 38 D5   C7 F4 80 64 F5 6E 95 50  ...I.Y8....d.n.P
0180: B8 11 7E 15 70 38 4A B0   7F D0 C4 32 70 C0 19 FF  ....p8J....2p...
0190: C9 38 2D 14 2C 66 F4 42   44 E6 55 76 1B 80 15 57  .8-.,f.BD.Uv...W
01A0: FF C0 A7 A7 AA 39 AA D8   D3 70 D0 2E BA EB 94 6A  .....9...p.....j
01B0: FA 5F 34 86 E7 62 B5 FD   8A F0 30 85 94 C9 AF 24  ._4..b....0....$
01C0: 02 2F 6F D6 DD 67 FE E3   B0 55 4F 04 98 4F A4 41  ./o..g...UO..O.A
01D0: 56 E2 93 D0 6A E8 D6 F3   FB 65 E0 CE 75 C4 31 59  V...j....e..u.1Y
01E0: 0C EE 82 C8 0C 60 33 4A   19 BA 84 67 27 0F BC 42  .....`3J...g'..B
01F0: 5D BD 24 54 0D EC 1D 70   06 5F A4 BC FA 20 7C 55  ].$T...p._... .U

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGFDCCA/ygAwIBAgIIG3Dp0v+ubHEwDQYJKoZIhvcNAQELBQAwUTELMAkGA1UE
BhMCRVMxQjBABgNVBAMMOUF1dG9yaWRhZCBkZSBDZXJ0aWZpY2FjaW9uIEZpcm1h
cHJvZmVzaW9uYWwgQ0lGIEE2MjYzNDA2ODAeFw0xNDA5MjMxNTIyMDdaFw0zNjA1
MDUxNTIyMDdaMFExCzAJBgNVBAYTAkVTMUIwQAYDVQQDDDlBdXRvcmlkYWQgZGUg
Q2VydGlmaWNhY2lvbiBGaXJtYXByb2Zlc2lvbmFsIENJRiBBNjI2MzQwNjgwggIi
MA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDKlmuO6vj78aI14H9M2uDDUtd9
thDIAl6zQyrET2qyyhxdKJp4ERppWVevtSBC5IsP5t9bpgOSL/UR5GLXMnE42QQM
cas9UX4PB99jBVzpv5RvwSmCwLTaUbDBPLutN0pcyvFLNg4kq7/DhHf9qFD0sefG
L9ItWY16Ck6WaVICqjaY7Pz6FIMMNx/Jkjd/14Et5cS54D40/mf0PmbR0/RAz15i
NA9wBj4gGFrO93IbJWyTdBSTo3OxDqqHECNZXyAFGUftaI6SEspd/NYrspI8IM/h
X68gvqB2f3bl7BqGYTM+53u0P6APjqK5am+5hyZvQWyIplD9amML9ZMWGxmPsu2b
m8mQ9QEM3xk9Dz44I8kvjwzRAv4bVdZO0I08r0+k8/6vKtMFnXkIoctXMbScyJCy
Z/QYFpM6/EfY0XiWMR+6KwxfXZmtY4laJCB22N/9q06mIqqdXuYnin1oKaPnirja
EbsXLZmdEyRG98Xi2J+Of8ePdG1asuhy9azuJBCtLxTa/y2aRnFHvkLfuwHb9H/T
KI8xWVvTyQKmtFLKbpf7Q8UIJm+K9Lv9nyiqDdVF8xM6HdjAeI9BZzwelGSuewvF
6NkBiDkal4ZkQdU7hwxu+g/GvUgUvzlN1J5Bto+WHWOWk9mVBngxaJ43BjuAiUVh
OSPHG0SjFeUc+JIwuwIDAQABo4HvMIHsMB0GA1UdDgQWBBRlzeurNR4APn7VdMAc
tHNHDhpkLzASBgNVHRMBAf8ECDAGAQH/AgEBMIGmBgNVHSAEgZ4wgZswgZgGBFUd
IAAwgY8wLwYIKwYBBQUHAgEWI2h0dHA6Ly93d3cuZmlybWFwcm9mZXNpb25hbC5j
b20vY3BzMFwGCCsGAQUFBwICMFAeTgBQAGEAcwBlAG8AIABkAGUAIABsAGEAIABC
AG8AbgBhAG4AbwB2AGEAIAA0ADcAIABCAGEAcgBjAGUAbABvAG4AYQAgADAAOAAw
ADEANzAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQELBQADggIBAHSHKAIrdx9m
iWTtj3QuRhy7qPj4Cx2Dtjqn6EWKB7fgPiDL4QjbEwj4KKE1soCzC1HA01aajTNF
Sa9J8OA9B3pFE1r/yJfY0xgsfZb43aJlQ3CTkBW6kN/oGbDbLIpgD7dvlAceHabJ
hfa9NPhAeGIQcDq+fUs5gakQ1JZBu/hfHAsdCPKxsIl68veg4MSPi3i1O1ilIl45P
Vf42O+AMt8oqMEEgtIDNrvx2ZnOorm7hfNoD6JQg5iKj0B+QXSBTFCZX2lSX3xZE
EAEeiGaPcjiT3SC3NL7X8e5jjkd5KAb881lFJWAiMxujX6i6KtoaPc1A6ozuBRWV
1aUsIC+nmCjuRfzxuIgALI9C2lHVnOUTaHFFQ4ueCyE8S1wF3BqfmI7avSKecs2t
CsvMo2ebKHTEm9caPARYpoKdrcd7b/+Alun4jWq9GJAd/0kakFI3ky88Al2CdgtR
5xbHV/g4+afNmyJU72OwFW1TZQNKXkqgsqeOSQBZONXH9IBk9W6VULgRfhVwOEqw
f9DEMnDAGf/JOC0ULGb0QkTmVXYbgBVX/8Cnp6o5qtjTcNAuuuuUavpfNIbnYrX9
ivAwhZTJryQCL2/W3Wf+47BVTwSYT6RBVuKT0Gro1vP7ZeDOdcQxWQzugsgMYDNK
GbqEZycPvEJdvSRUDewdcAZfpLz6IHxV
-----END CERTIFICATE-----
```

Certificate Service Provider Name (en): INDENOVA SUCURSAL DEL PERÚ

Trade name (en)	INDENOVA SUCURSAL DEL PERÚ
Information URI (en)	WWW.INDENOVA.COM
Service provider street address (es)	AV. ALFREDO BENAVIDES N° 1944, PISO 9 OFICINA 32 MIRAFLORES (LIMA)
Service provider street address (en)	AV. ALFREDO BENAVIDES N° 1944, PISO 9 OFICINA 32 MIRAFLORES (LIMA)
Service provider postal code (es)	15048
Service provider postal code (en)	15048
Service provider locality (es)	LIMA
Service provider locality (en)	LIMA
Service provider state (es)	LIMA
Service provider state (en)	LIMA
Service provider country (es)	PE
Service provider country (en)	PE

C=PE, L=LIMA, STREET=http://www.indenova.com, OU=Internet Certification Authority http://www.indenova.com, T=Subordinate Certificate Perú, O=inDenova Sucursal del Perú, EMAILADDRESS=sub_ca_pe@indenova.com, SERIALNUMBER=20549615709, CN=inDenova SUB001_PE, OID.2.5.4.13=inDenova Subordinate Certificate 001 Perú HW-KUSU

Type	CA/QC
Status	undersupervision
Status starting time	2020-04-07T03:56:26.000Z

Service digital identity (X509)

Version	3
Serial number	6
Signature algorithm	SHA256withRSA
Issuer	C=ES, L=Valencia, STREET=https://www.indenova.com/aviso-legal/, OU=Internet Certification Authority https://www.indenova.com, SERIALNUMBER=B97458996, O=Indenova SL, CN=Global Certification Authority Root Indenova, EMAILADDRESS=ca@indenova.com
Valid from	Thu Mar 12 03:00:00 PET 2020
Valid to	Fri Mar 04 03:00:00 PET 2050
Subject	C=PE, L=LIMA, STREET=http://www.indenova.com, OU=Internet Certification Authority http://www.indenova.com, T=Subordinate Certificate Perú, O=inDenova Sucursal del Perú, EMAILADDRESS=sub_ca_pe@indenova.com, SERIALNUMBER=20549615709, CN=inDenova SUB001_PE, OID.2.5.4.13=inDenova Subordinate Certificate 001 Perú HW-KUSU

Public key	Sun RSA public key, 4096 bits modulus: 7731397979508677564983649393819753601877603194466806714117709968956870 7 9998511077638724900927179652786911183836321486262128117279297825739305 0 5094201705663730223015376615002951418547950404903325465558271568348264 7 2728000330180098781040595075889525992086252142675597607030075073472021 8 6843967326440309671248414406733193329900847937991767598947579993309237 6 2773458308660742514397781094347945528079562656184377934682805784438944 9 5312041710980695632580357653169744194929065277565073106151337830813952 5 0679904592944480050287225539173250029558742934130400703788661002710359 1 2240986125090150466048086938914245306692339456736973216759463070432368 9 8055878384239659473192055613101904398218490540730616795156352877205229 7 6908740489101905179355086201335112109642004210128275053358133080555851 8 7050289993007729191139180899037349553790639483440454961800222458396548 1 8066890257762341935023891428328663700777246424667621465642453231458476 8 6285845408038650792576301328561478042413095763061906128271413792704280 1 2763121146789015211248473754366174005622352374784439504183510379209701 7 2309944134251142508015942185657904984573187389361350436897189305874224 4 1911395276440204495464301874358955001300110246236037658528772235382342 7 1325837072151742847086358 9 public exponent: 65537
Subject key identifier	0024f43d1b886ad9ac51f0229e88b6b96a394e7c
CRL distribution points	http://crl.esigna.es/root/indenova_global_root_ca.crl http://crl1.esigna.es/root/indenova_global_root_ca.crl
Authority key identifier	041830168014f950303750431b1ea6d2bd40dedf8d6242f7ec40
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=0
SHA1 Thumbprint	67269b9d042b53a77b502289a84fea0ba0c7c3cf
SHA256 Thumbprint	547f344fda1d38334622d0e8a9d88ae21f992f49df4dc012484a8461f66992cd

The decoded certificate:

```
[
[
 Version: V3
 Subject: C=PE, L=LIMA, STREET=http://www.indenova.com, OU=Internet Certification Authority http://www.indenova.com, T=Subordinate Certificate Perú, O=inDenova Sucursal del
Perú, EMAILADDRESS=sub_ca_pe@indenova.com, SERIALNUMBER=20549615709, CN=inDenova SUB001_PE, OID.2.5.4.13=inDenova Subordinate Certificate 001 Perú HW-KUSU
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
7731397979508677564983649393819753601877603194466806714117709968956870799985110776387249009271796527869111838363214862621281172792978257393050509420170566373022301537661500 2
95141854795040490332546555827156834826472728000330180098781040595075889525992086252142675597607030075073472021868439673264403096712484144067331933299008479379917675989475799
93309237627734583086607425143977810943479455280795626561843779346828057844389449531204171098069563258035765316974419492906527756507310615133783081395250679904592944480050287
22553917325002955874293413040070378866100271035912240986125090150466048086938914245306692339456736973216759463070432368980558783842396594731920556131019043982184905407306167
95156352877205229769087404891019051793550862013351121096420042101282750533581330805558518705028999300772919113918089903734955379063948344045496180022245839654818066890257762
34193502389142832866370077724642466762146564245323145847686285845408038650792576301328561478042413095763061906128271413792704280127631211467890152112484737543661740056223523
74784439504183510379209701723099441342511425080159421856579049845731873893613504368971893058742244191139527644020449546430187435895500130011024623603765852877223538234271325
8370721517428470863589
 public exponent: 65537
 Validity: [From: Thu Mar 12 03:00:00 PET 2020,
             To: Fri Mar 04 03:00:00 PET 2050]
 Issuer: C=ES, L=Valencia, STREET=https://www.indenova.com/aviso-legal/, OU=Internet Certification Authority https://www.indenova.com, SERIALNUMBER=B97458996, O=Indenova SL,
CN=Global Certification Authority Root Indenova, EMAILADDRESS=ca@indenova.com
 SerialNumber: [    06]

Certificate Extensions: 9
[1]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://certs.esigna.es/root/indenova_global_root_ca.crt]
]

[2]: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
 RFC822Name: info@indenova.com
]

[3]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: F9 50 30 37 50 43 1B 1E   A6 D2 BD 40 DE DF 8D 62  .P07PC.....@...b
0010: 42 F7 EC 40                                        B..@
]

]
```

```
[4]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 00 24 F4 3D 1B 88 6A D9   AC 51 F0 22 9E 88 B6 B9  .$.=..j..Q."....
0010: 6A 39 4E 7C                                        j9N.
]
]

[5]: ObjectId: 2.5.29.18 Criticality=false
IssuerAlternativeName [
 RFC822Name: info@indenova.co
]

[6]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 2C 68 74 74 70 3A 2F   2F 63 70 73 2E 65 73 69  .,http://cps.esi
0010: 67 6E 61 2E 65 73 2F 73   75 62 2F 63 70 73 5F 73  gna.es/sub/cps_s
0020: 75 62 30 30 31 70 65 5F   63 61 2E 70 64 66        ub001pe_ca.pdf

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 42 1A 40 54 65 72 6D   73 20 6F 66 20 75 73 65  0B.@Terms of use
0010: 20 61 74 20 43 50 53 20   68 74 74 70 3A 2F 2F 63   at CPS http://c
0020: 70 73 2E 65 73 69 67 6E   61 2E 65 73 2F 73 75 62  ps.esigna.es/sub
0030: 2F 63 70 73 5F 73 75 62   30 30 31 70 65 5F 63 61  /cps_sub001pe_ca
0040: 2E 70 64 66                                        .pdf

]]  ]
]

[7]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:0
]

[8]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.esigna.es/root/indenova_global_root_ca.crl]
, DistributionPoint:
    [URIName: http://crl1.esigna.es/root/indenova_global_root_ca.crl]
]]

[9]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 58 CD 3A 11 F4 DA 22 9F   F5 56 05 5A A4 92 17 49  X.:...".."..V.Z...I
0010: 93 F8 5B 30 B6 1F 86 B6   56 26 3B 5E 0F 8E 56 EC  ..[0....V&;^..V.
0020: DE 60 D3 C2 09 C2 F8 1D   6B 3D 0B 34 9F C2 F9 67  .`......k=.4...g
0030: 75 4D 83 30 A6 2D 53 BB   E2 CA F1 44 3A 1B A1 1A  uM.0.-S....D:...
0040: 38 EB A2 03 29 BB 31 A9   70 EA 75 79 04 23 A0 4F  8...).1.p.uy.#.O
0050: BB 85 25 86 95 C9 44 8E   73 29 54 3A 17 37 85 0E  ..%...D.s)T:.7..
0060: 04 11 F6 8F CB 55 5C C2   65 1F DE C1 C9 95 6A DB  .....U\.e.....j.
0070: AB B9 FF 3E FB 2D 1A 3F   42 87 0E D5 79 5F 64 E1  ...>.-.?B...y_d.
0080: 8D E4 5C ED C0 D3 A4 8E   37 07 60 F1 A5 36 66 7B  ..\.....7.`..6f.
0090: 4C 98 25 BA A0 84 7C 6C   7A CC D3 EE 9E D1 65 94  L.%....lz.....e.
00A0: 09 AD BF DA 4F 1B EA 6A   F1 58 3D E7 B8 10 BA 48  ....O..j.X=....H
00B0: 5C 0F CB EE CB AA 24 DF   AF 5E 25 95 F7 46 E2 99  \.....$..^%..F..
00C0: B6 A1 25 78 76 4A CB 69   D0 A6 A4 1C DF E5 62 40  ..%xvJ.i......b@
00D0: A5 BE AB 09 2D 45 BD FD   26 6E F0 3B 26 F9 35 B3  ....-E..&n.;&.5.
00E0: 14 62 37 C1 23 E2 D2 F5   34 22 66 67 C7 75 DD BA  .b7.#...4"fg.u..
00F0: 5E 20 C3 AB 56 B1 67 C4   52 6A BE B9 50 6A 99 C0  ^ ..V.g.Rj..Pj..
0100: 42 A6 4D FB 4B B8 E8 B1   3D 1C 3B 79 9E 4F 2D 9D  B.M.K...=.;y.O-.
0110: B7 3C 88 19 BD AB B9 9F   A8 D9 01 F3 31 13 45 2A  .<..........1.E*
0120: 75 A7 8A 08 57 30 09 2B   E0 79 BD 76 4D 53 E8 EE  u...W0.+.y.vMS..
0130: 6B 53 27 B0 DE E8 CA 76   D1 D1 1E 64 12 49 EF 23  kS'....v...d.I.#
0140: FE EF 72 D6 07 08 5E 54   69 86 D9 2F AA 8B 3A 0E  ..r...^Ti../..:.
0150: D0 C8 51 88 3B DB 23 5D   D5 3C 4B 7E E3 0D 28 74  ..Q.;.#].<K...(t
0160: F6 5B 72 F1 3E 29 F8 17   BA 59 80 1A E9 91 05 D0  .[r.>)...Y......
0170: 24 40 32 74 92 1E 50 2C   0F CA 3F D6 AC B0 43 5B  $@2t..P,..?...C[
0180: AB E6 9E 93 9E 9B CD DB   B0 F2 12 DC EA AA C7 18  ................
0190: 08 5A 6B 0B 6D 94 67 FF   7B 39 0A 70 58 FF 7C 48  .Zk.m.g..9.pX..H
01A0: A3 2F 56 D9 27 0B AB 3A   2C E5 56 BF FF 04 30 AD  ./V.'..:,.V...0.
01B0: 8F 7E E2 F4 63 61 4D 9E   5A B0 D3 BB E6 B7 44 02  ....caM.Z.....D.
01C0: 95 06 C5 34 6C ED F3 DA   EA 44 E0 FE CD 2B CE 4D  ...4l....D...+.M
01D0: 18 0C 93 CF DF 7F E5 60   8D BC 83 A3 2A 7E 13 FF  .......`....*...
01E0: 95 F0 10 6E C9 C3 63 DD   EA 45 B4 DC C3 DA D6 6A  ...n..c..E.....j
01F0: 45 67 87 C2 BB 45 8E CC   B8 10 B4 D9 C3 FC 9C 79  Eg...E.........y

]
```

The certificate in PEM format:


```
-----BEGIN CERTIFICATE-----
MIIJITCCBwmgAwIBAgIBBjANBgkqhkiG9w0BAQsFADCCARUxHjAcBgkqhkiG9w0B
CQEWD2NhQGluZGVub3ZhLmNvbTE1MDMGA1UEAwwsR2xvYmFsIENlcnRpZmljYXRp
b24gQXV0aG9yaXR5IFJvb3QgSW5kZW5vdmExFDASBgNVBAoMC0luZGVub3ZhIFNM
MRIwEAYDVQQFEwlCOTc0NTg5OTYxQjBABgNVBAsMOUludGVybmV0IENlcnRpZmlj
YXRpb24gQXV0aG9yaXR5IGh0dHBzOi8vd3d3LmluZGVub3ZhLmNvbTEuMCwGA1UE
CQwlaHR0cHM6Ly93d3cuaW5kZW5vdmEuY29tL2F2aXNvLWxlZ2FsLzERMA8GA1UE
BwwIVmFsZW5jaWExCzAJBgNVBAYTAkVTMCAXDTIwMDMxMjA4MDAwMFoYDzIwNTAw
MzA0MDgwMDAwWjCCAWYxOzA5BgNVBA0MMmluRGVub3ZhIFN1Ym9yZGluYXRlIENl
cnRpZmljYXRlIDAwMSBQZXLDuiBIVy1LVVNVMRswGQYDVQQDDBJpbkRlbm92YSBT
VUIwMDFfUEUxFDASBgNVBAUTCzIwNTQ5NjE1NzA5MSUwIwYJKoZIhvcNAQkBFhZz
dWJfY2FfcGVAaW5kZW5vdmEuY29tMSQwIgYDVQQKDBtpbkRlbm92YSBTdWN1cnNh
bCBkZWwgUGVyw7oxJjAkBgNVBAwMHVN1Ym9yZGluYXRlIENlcnRpZmljYXRlIFBl
csO6MUEwPwYDVQQLDDhJbnRlcm5ldCBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSBo
dHRwOi8vd3d3LmluZGVub3ZhLmNvbTEgMB4GA1UECQwXaHR0cDovL3d3dy5pbmRl
bm92YS5jb20xDTALBgNVBAcMBExJTUExCzAJBgNVBAYTAlBFMIICIjANBgkqhkiG
9w0BAQEFAAOCAg8AMIICCgKCAgEAvYL2+9R3cgJnH3AZYalh9ykvvAfyk8UBzOFf
d+t82DdTZmaDtwEyMa/cRIU/kEmo0aOqjdKvMgmEi1gx0AEoedb4iL8xm+Bclfx7
rwCl01iop62UmH1l/n1W4iLh9S22wHAcGVc+R94Y6QiA96IYRMprE/BjZtLgG2c0
+uL/HaurBjzSC9rY17j0etJGWpgucpNw6QC9K370iJB2YtuZAPhhN52gd9nYer1u
lA6K+zVIdJCKFC50D90NcW3JcCzXS+jliIDFP5Lb4Rf0Gdz1sqyTDaUdw3WCFOtd
zO/QOL4tE9cOmLEeIbAGOmoZOiP1F78/UC6u38IETH9/z4aOJSKOaXUbDMFwg7DH
NXXs6D8PANvARjMac0Kuhyteg99EmmPPSHmECXo9fJsRvp1KzyVTAaWDWy6cKsgK
oLMjt0AjFWfaLPud6CyQRqfDyqbHYqSAq5F4saD1g9lI1XvX7+oCIY+wcPPkIyAq
r1j2MqfOKxFipfb4wHhMWhB/axesCGFnGEkACcB+BgN4fZKMTQzjejV3XpglykEY
ePs1uORDDb6GRrrtirocqOn2bFMZ3n5f4pFGobtZf6ONoH+GMlLqjK1OTeknPvKW
KfwG62BK69MRIegA8v2SacdQKU+GTvSBQHKkctl2RFAU8i0CKyqrR+8peXOaLQFu
hmwKVuUCAwEAAaOCAiMwggIfMB0GA1UdDgQWBBQAJPQ9G4hq2axR8CKeiLa5ajlO
fDAfBgNVHSMEGDAWgBT5UDA3UEMbHqbSvUDe341iQvfsQDAOBgNVHQ8BAf8EBAMC
AQYwgaEGA1UdIASBmTCBljCBkwYEVR0gADCBijA4BggrBgEFBQcCARYsaHR0cDov
L2Nwcy5lc2lnbmEuZXMvc3ViL2Nwc19zdWIwMDFwZV9jYS5wZGYwTgYIKwYBBQUH
AgIwQhpAVGVybXMgb2YgdXNlIGF0IENQUyBodHRwOi8vY3BzLmVzaWduYS5lcy9z
dWIvY3BzX3N1YjAwMXBlX2NhLnBkZjAcBgNVHREEFTATgRFpbmZvQGluZGVub3Zh
LmNvbTAbBgNVHRIEFDASgRBpbmZvQGluZGVub3ZhLmNvMFMGCCsGAQUFBwEBBEcw
RTBDBggrBgEFBQcwAoY3aHR0cDovL2NlcnRzLmVzaWduYS5lcy9yb290L2luZGVu
b3ZhX2dsb2JhbF9yb290X2NhLmNydDASBgNVHRMBAf8ECDAGAQH/AgEAMIGEBgNV
HR8EfTB7MDugOaA3hjVodHRwOi8vY3JsLmVzaWduYS5lcy9yb290L2luZGVub3Zh
X2dsb2JhbF9yb290X2NhLmNybDA8oDqgOIY2aHR0cDovL2NybDEuZXNpZ25hLmVz
L3Jvb3QvaW5kZW5vdmFfZ2xvYmFsX3Jvb3RfY2EuY3JsMA0GCSqGSIb3DQEBCwUA
A4ICAQBYzToR9Noin/VWBVqkkhdJk/hbMLYfhrZWJjteD45W7N5g08IJwvgdaz0L
NJ/C+Wd1TYMwpi1Tu+LK8UQ6G6EaOOuiAym7Malw6nV5BCOgT7uFJYaVyUSOcylU
Ohc3hQ4EEfaPy1VcwmUf3sHJlWrbq7n/PvstGj9Chw7VeV9k4Y3kXO3A06SONwdg
8aU2ZntMmCW6oIR8bHrM0+6e0WWUCa2/2k8b6mrxWD3nuBC6SFwPy+7LqiTfr14l
lfdG4pm2oSV4dkrLadCmpBzf5WJApb6rCS1Fvf0mbvA7Jvk1sxRiN8Ej4tL1NCJm
Z8d13bpeIMOrVrFnxFJqvrlQapnAQqZN+0u46LE9HDt5nk8tnbc8iBm9q7mfqNkB
8zETRSp1p4oIVzAJK+B5vXZNU+jua1MnsN7oynbR0R5kEknvI/7vctYHCF5UaYbZ
L6qLOg7QyFGIO9sjXdU8S37jDSh09lty8T4p+Be6WYAa6ZEF0CRAMnSSHlAsD8o/
1qywQ1ur5p6TnpvN27DyEtzqqscYCFprC22UZ/97OQpwWP98SKMvVtknC6s6LOVW
v/8EMK2PfuL0Y2FNnlqw07vmt0QClQbFNGzt89rqROD+zSvOTRgMk8/ff+VgjbyD
oyp+E/+V8BBuycNj3epFtNzD2tZqRWeHwrtFjsy4ELTZw/yceQ==
-----END CERTIFICATE-----
```


C=ES, L=Valencia, STREET=https://www.indenova.com/aviso-legal/, OU=Internet Certification Authority https://www.indenova.com, SERIALNUMBER=B97458996, O=Indenova SL, CN=Global Certification Authority Root Indenova, EMAILADDRESS=ca@indenova.com

Type	CA/QC
Status	undersupervision
Status starting time	2020-04-07T03:24:24.000Z

Service digital identity (X509)

Version	3
Serial number	0
Signature algorithm	SHA256withRSA
Issuer	C=ES, L=Valencia, STREET=https://www.indenova.com/aviso-legal/, OU=Internet Certification Authority https://www.indenova.com, SERIALNUMBER=B97458996, O=Indenova SL, CN=Global Certification Authority Root Indenova, EMAILADDRESS=ca@indenova.com
Valid from	Thu Mar 12 03:00:00 PET 2020
Valid to	Sat Mar 12 03:00:00 PET 2050
Subject	C=ES, L=Valencia, STREET=https://www.indenova.com/aviso-legal/, OU=Internet Certification Authority https://www.indenova.com, SERIALNUMBER=B97458996, O=Indenova SL, CN=Global Certification Authority Root Indenova, EMAILADDRESS=ca@indenova.com

Public key	Sun RSA public key, 4096 bits modulus: 81951747366827246661568186069780961271791970508943248750800720629201420 19112147530620025828618033506031569117146043454959589219023236392908884 69786526775715461797452150887013992310367210572989331176123684925755968 58220343848619645271744950373229812398334285170560187560620167615887997 96831267182658017809703875185260077918368807590171030138704489557287222 71482592564658947697488850615994671931422915415992455008578115320736944 70729946031751245918637625187855871609621022789336342144020984031651853 77108796275803124693044639200802146246848397096243241470171741559365685 42520441046207466129431840898584803507509797194724066318965420571708719 87987848083677837630855543525478501931436685085959789032083269389550216 95131098624443153785188856022993766836927367787536242517161065041991781 99564645460518616280833299935103873113207070278528055991549933243000498 41384126007613326088065663224969021106060606573128075898151972915746243 99961442189212072191413916486841297717404843870201934926294061258100513 24502744568984065756074693877568695704723863214351374061937748976399721 70223968634785042759426920313245297584313249163601442990447376733460796 71840678415897219477959767156039419402495711026005927078413264859879072 3203094345645398481183809 9 public exponent: 65537
Subject key identifier	f950303750431b1ea6d2bd40dedf8d6242f7ec40
Authority key identifier	041830168014f950303750431b1ea6d2bd40dedf8d6242f7ec40
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=3
SHA1 Thumbprint	554dbd264c9af8101ee1348ae63895ddc79d073e
SHA256 Thumbprint	54d7bede36daaf77aa1b4cea8c7ea4708a94fae80423db211efebacb2350eb90

The decoded certificate:


```
[
[
 Version: V3
 Subject: C=ES, L=Valencia, STREET=https://www.indenova.com/aviso-legal/, OU=Internet Certification Authority https://www.indenova.com, SERIALNUMBER=B97458996, O=Indenova
SL, CN=Global Certification Authority Root Indenova, EMAILADDRESS=ca@indenova.com
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 4096 bits
 modulus:
819517473668272466615681860697809612717919705089432487508007206292014201911214753062002582861803350603156911714604345495958921902323639290888469786526775715461797452150887 01
399231036721057298933117612368492575596858220343848619645271744950373229812398334285170560187560620167615887997968312671826580178097038751852600779183688075901710301387044 89
557287222714825925646589476974888506159946719314229154159924550085781153207369447072994603175124591863762518785587160962102278933634214402098403165185377108796275803124693 04
463920080214624684839709624324147017174155936568542520441046207466129431840898584803507509797194724066318965420571708719879878480836778376308555435254785019314366850859597 89
032083269389550216951310986244431537851888560229937668369273677875362425171610650419917819956464546051861628083329993510387311320707027852805599154993324300049841384126007 61
332608806566322496902110606060657312807589815197291574624399961442189212072191413916486841297717404843870201934926294061258100513245027445689840657560746938775686957047238 63
214351374061937748976399721702239686347850427594269203132452975843132491636014429904473767334607967184067841589721947795976715603941940249571102600592707841326485987907232 03
0943456453984811838099
 public exponent: 65537
 Validity: [From: Thu Mar 12 03:00:00 PET 2020,
             To: Sat Mar 12 03:00:00 PET 2050]
 Issuer: C=ES, L=Valencia, STREET=https://www.indenova.com/aviso-legal/, OU=Internet Certification Authority https://www.indenova.com, SERIALNUMBER=B97458996, O=Indenova SL,
CN=Global Certification Authority Root Indenova, EMAILADDRESS=ca@indenova.com
 SerialNumber: [    00]

Certificate Extensions: 8
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: F9 50 30 37 50 43 1B 1E   A6 D2 BD 40 DE DF 8D 62  .P07PC.....@...b
0010: 42 F7 EC 40                                        B..@
]
]

[2]: ObjectId: 2.5.29.18 Criticality=false
IssuerAlternativeName [
 URIName: https://www.indenova.com
]

[3]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: F9 50 30 37 50 43 1B 1E   A6 D2 BD 40 DE DF 8D 62  .P07PC.....@...b
0010: 42 F7 EC 40                                        B..@
]

]

[4]: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
 RFC822Name: info@indenova.com
```

```
]

[5]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 35 68 74 74 70 73 3A   2F 2F 77 77 77 2E 69 6E  .5https://www.in
0010: 64 65 6E 6F 76 61 2E 63   6F 6D 2F 61 63 72 65 64  denova.com/acred
0020: 69 74 61 63 69 6F 6E 65   73 2F 69 6E 64 65 63 6F  itaciones/indeco
0030: 70 69 2F 73 76 61 2F                               pi/sva/

], PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.2
 qualifier: 0000: 30 4F 1A 4D 54 65 72 6D   73 20 6F 66 20 75 73 65  0O.MTerms of use
0010: 20 61 74 20 43 50 53 20   43 41 20 49 6E 64 65 6E   at CPS CA Inden
0020: 6F 76 61 20 68 74 74 70   3A 2F 2F 63 70 73 2E 65  ova http://cps.e
0030: 73 69 67 6E 61 2E 65 73   2F 72 6F 6F 74 2F 63 70  signa.es/root/cp
0040: 73 5F 63 61 5F 69 6E 64   65 6E 6F 76 61 2E 70 64  s_ca_indenova.pd
0050: 66                                                 f

]]  ]
]

[6]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[7]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:3
]

[8]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://certs.esigna.es/root/indenova_global_root_ca.crt]
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: 35 A2 E9 51 44 0B 4F AA   A7 F7 55 82 D8 6E 3D 01  5..QD.O...U..n=.
0010: 77 51 C1 6B CD 2D CF EC   E6 A3 29 69 29 36 7A 25  wQ.k.-....)i)6z%
0020: 0C 19 D2 86 EC EB BD 83   90 49 2E 1D 90 03 F8 70  .........I.....p
0030: C5 52 19 A8 76 08 1E BC   28 5C 91 11 4E 25 4D 08  .R..v...(\..N%M.
0040: 0E 79 26 75 04 3E 42 29   D3 8F 3D F5 30 8E 0B 78  .y&u.>B)..=.0..x
0050: DF 4A B4 D2 2D 51 49 9F   35 F8 C3 B2 28 02 90 1A  .J..-QI.5...(...
0060: CF B8 D9 75 54 24 BC 61   69 8A CB C8 14 93 D1 52  ...uT$.ai......R
0070: 5F 0A BB 14 D4 C1 1C A9   B8 6E 6E 4A 46 49 F6 9C  _........nnJFI..
0080: CC A2 0A D4 26 2B A5 F5   C9 30 60 0A 61 E1 8A B1  ....&+...0`.a...
0090: D4 3D 9F 9F 37 B5 2A F1   2F 21 73 CC 3E 2F 4B D5  .=..7.*./!s.>/K.
00A0: 0C 75 A2 48 DB 70 6C 2C   59 5B E9 66 24 29 E8 EA  .u.H.pl,Y[.f$)..
00B0: DA 8D BD 66 A2 A7 65 B3   5E 12 94 E3 47 88 0E F0  ...f..e.^...G...
00C0: 35 86 0D 9D C8 D5 01 76   95 44 E2 E7 64 E0 F7 71  5......v.D..d..q
00D0: 1C 94 B4 E1 22 57 53 B5   A8 E4 AC D2 19 72 D9 C6  ....."WS......r..
00E0: 6B E4 94 95 12 51 5A F5   FD D1 0E 43 F5 1B 4C 35  k....QZ....C..L5
00F0: 78 B0 05 EB 89 36 28 C6   F5 8B 11 C5 E0 0C EE 12  x....6(.........
0100: 72 7B 68 5E 42 62 0F D6   D0 B5 95 6E 8D 11 D0 2E  r.h^Bb.....n....
0110: DF 73 8E C9 A8 FB 48 57   1F 2F D3 8E EF 3C 1C DB  .s....HW./...<..
0120: BA AC 31 DA 14 2B 4C 89   72 5B E4 4B 7A FD 38 0F  ..1..+L.r[.Kz.8.
0130: BD 99 DA 9E DF 1D 31 2C   4D 47 7E 71 EC 9E EB C3  ......1,MG.q....
0140: E8 77 B0 2B 04 4B 32 FA   A2 63 43 DF A7 09 EE 8B  .w.+.K2..cC.....
0150: C4 31 3A 07 BA A8 3D A6   FC B1 57 2E 06 6D F0 19  .1:...=...W..m..
0160: 9C BB 8B 37 51 02 33 86   55 D0 D7 AC EA 6F 73 40  ...7Q.3.U....os@
0170: 0C CC 5F 8F 40 EA 39 2C   19 E2 63 6B 77 17 21 BD  .._.@.9,..ckw.!.
0180: 97 A0 A4 AA 78 8C 15 AC   78 C0 3C 8A 7B 6F B5 AB  ....x...x.<..o..
0190: 09 71 48 6A CE 52 92 21   F4 1A 60 13 17 7A 8A 7D  .qHj.R.!..`..z..
01A0: 96 49 1B 07 C3 EE 87 BA   68 05 B6 5E B6 49 79 89  .I......h..^.Iy.
01B0: 9B 57 38 73 06 31 42 D2   19 78 9B E0 AC 05 92 9D  .W8s.1B..x......
01C0: 99 C5 F9 B2 F1 07 D1 4C   F5 79 62 44 DF 3A 81 86  .......L.ybD.:..
01D0: B7 6B 0D CD BA 24 D0 6D   59 AD 99 66 D0 A1 95 96  .k...$.mY..f....
01E0: F9 E3 AE 42 73 50 CF 28   C3 B4 5C FE E0 80 E1 2B  ...BsP.(..\....+
01F0: E9 2B F2 CD F0 43 C9 BA   66 A5 F3 86 11 2C 47 25  .+...C..f....,G%

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIIZzCCBk+gAwIBAgIBADANBgkqhkiG9w0BAQsFADCCARUxHjAcBgkqhkiG9w0B
CQEWD2NhQGluZGVub3ZhLmNvbTE1MDMGA1UEAwwsR2xvYmFsIENlcnRpZmljYXRp
b24gQXV0aG9yaXR5IFJvb3QgSW5kZW5vdmExFDASBgNVBAoMC0luZGVub3ZhIFNM
MRIwEAYDVQQFEwlCOTc0NTg5OTYxQjBABgNVBAsMOUludGVybmV0IENlcnRpZmlj
YXRpb24gQXV0aG9yaXR5IGh0dHBzOi8vd3d3LmluZGVub3ZhLmNvbTEuMCwGA1UE
CQwlaHR0cHM6Ly93d3cuaW5kZW5vdmEuY29tL2F2aXNvLWxlZ2FsLzERMA8GA1UE
BwwIVmFsZW5jaWExCzAJBgNVBAYTAkVTMCAXDTIwMDMxMjA4MDAwMFoYDzIwNTAw
MzEyMDgwMDAwWjCCARUxHjAcBgkqhkiG9w0BCQEWD2NhQGluZGVub3ZhLmNvbTE1
MDMGA1UEAwwsR2xvYmFsIENlcnRpZmljYXRpb24gQXV0aG9yaXR5IFJvb3QgSW5k
ZW5vdmExFDASBgNVBAoMC0luZGVub3ZhIFNMMRIwEAYDVQQFEwlCOTc0NTg5OTYx
QjBABgNVBAsMOUludGVybmV0IENlcnRpZmljYXRpb24gQXV0aG9yaXR5IGh0dHBz
```

Oi8vd3d3LmluZGVub3ZhLmNvbTEuMCwGA1UECQwlaHR0cHM6Ly93d3cuaW5kZW5v
dmEuY29tL2F2aXNvLWxlZ2FsLzERMA8GA1UEBwwIVmFsZW5jaWExCzAJBgNVBAYT
AkVTMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAyOEwwtL0Uz9QAsUz
7fy/QIV2IfCuNks7jINqU5x1BSw0dU+OpSQCsNlczP5O87lB8XOu2UQ8E2rCNkrt
cWZVCliGN4WNr/Agg6Oe9mEQ6Og0+0OCjRxvVcPq3qZjVfF1sriTuDuXMNmZuIdq
0CRthlgJYcLrMYhH/TD+h4l2kf02fapKpZu0ghd98m6+Va3n/Z1z+fijCP4QTOej
EJd6YBUdzCgD2dk2qeT6KySs24X/qUqYvM/FxyHjdL6Mnuw2yJppU0gNsqQwX63J
M9tpzwSwrmecPuvhg0gS0Ztg4D/lYAKlWq/SwTpHv5iVnniZSp/g5qqaeADPGA/1
V5DXZSh3srrN2PEhtVBEEAlFhW1X+yBW2Ji08cxJe7kZMroWJ2BkFphmHQhqNqbB
CFcTr47Miq149dFFww7Bw399CWxp2WK10iJLm8pL6/+mK8YytGE0sw1ntBUZbHas
6Ci8FVEF4mJV9N8+qaWkPQCt9miPp4sMYtowdBDxwgptlWdJDVkAFwnOLh9GPLn/
rWWfcIk1Btf/gZwFBU9Rln4vmUVM7dEvbZhA73yz/0f9/Vauh6P9WD7hwavYGs+j
iETwedbeNtGoPvqzb/1EsL72l8GNlJHmZ9Dqa3CeeptmNfcpsJKWXb0222eZsxgY
vko6aDrJFPkQ6/lVa4w3i2UhapMCAwEAAaOCAbowggG2MB0GA1UdDgQWBBT5UDA3
UEMbHqbSvUDe341iQvfsQDAfBgNVHSMEGDAWgBT5UDA3UEMbHqbSvUDe341iQvfs
QDAOBgNVHQ8BAf8EBAMCAQYwgbcGA1UdIASBrzCBrDCBqQYEVR0gADCBoDBBBggr
BgEFBQcCARY1aHR0cHM6Ly93d3cuaW5kZW5vdmEuY29tL2FjcmVkaXRhY2lvbmVz
L2luZGVjb3BpL3N2YS8wWwYIKwYBBQUHAgIwTxpNVGVybXMgb2YgdXNlIGF0IENQ
UyBDQSBJbmRlbm92YSBodHRwOi8vY3BzLmVzaWduYS5lcy9yb290L2Nwc19jYV9p
bmRlbm92YS5wZGYwHAYDVR0RBBUwE4ERaW5mb0BpbmRlbm92YS5jb20wIwYDVR0S
BBwwGoYYaHR0cHM6Ly93d3cuaW5kZW5vdmEuY29tMFMGCCsGAQUFBwEBBEcwRTBD
BggrBgEFBQcwAoY3aHR0cDovL2NlcnRzLmVzaWduYS5lcy9yb290L2luZGVub3Zh
X2dsb2JhbF9yb290X2NhLmNydDASBgNVHRMBAf8ECDAGAQH/AgEDMA0GCSqGSIb3
DQEBCwUAA4ICAQA1oulRRAtPqqf3VYLYbj0Bd1HBa80tz+zmoylpKTZ6JQwZ0obs
672DkEkuHZAD+HDFUhmodggevChckRFOJU0IDnkmdQQ+QinTjz31MI4LeN9KtNIt
UUmfNfjDsigCkBrPuNl1VCS8YWmKy8gUk9FSXwq7FNTBHKm4bm5KRkn2nMyiCtQm
K6X1yTBgCmHhirHUPZ+fN7Uq8S8hc8w+L0vVDHWiSNtwbCxZW+lmJCno6tqNvWai
p2WzXhKU40eIDvA1hg2dyNUBdpVE4udk4PdxHJS04SJXU7Wo5KzSGXLZxmvklJUS
UVr1/dEOQ/UbTDV4sAXriTYoxvWLEcXgDO4ScntoXkJiD9bQtZVujRHQLt9zjsmo
+0hXHy/Tju88HNu6rDHaFCtMiXJb5Et6/TgPvZnant8dMSxNR35x7J7rw+h3sCsE
SzL6omND36cJ7ovEMToHuqg9pvyxVy4GbfAZnLuLN1ECM4ZV0Nes6m9zQAzMX49A
6jksGeJja3cXIb2XoKSqeIwVrHjAPIp7b7WrCXFIas5SkiH0GmATF3qKfZZJGwfD
7oe6aAW2XrZJeYmbVzhzBjFC0hl4m+CsBZKdmcX5svEH0Uz1eWJE3zqBhrdrDc26
JNBtWa2ZZtChlZb5465Cc1DPKMO0XP7ggOEr6SvyzfBDybpmpfOGESxHJQ==
-----END CERTIFICATE-----

Certificate Service Provider Name (en): SOFT & NET SOLUTIONS S.A.C.

Trade name (en)	SOFT & NET SOLUTIONS S.A.C.
Information URI (en)	WWW.SOFT-NET.COM.PE
Service provider street address (es)	CALLE GERMAN SCHREIBER NRO 184 DPTO 802
Service provider street address (en)	CALLE GERMAN SCHREIBER NRO 184 DPTO 802
Service provider postal code (es)	15027
Service provider postal code (en)	15027
Service provider locality (es)	SAN ISIDRO
Service provider locality (en)	SAN ISIDRO
Service provider state (es)	LIMA
Service provider state (en)	LIMA
Service provider country (es)	PE
Service provider country (en)	PE

CN=Soft-Net Secure Signing CA - C1, O=Soft and Net Solutions SAC, OU=emSign PKI, C=PE

Type	CA/QC
Status	undersupervision
Status starting time	2020-10-27T23:06:06.000Z

Service digital identity (X509)

Version	3
Serial number	364693615674180102926613
Signature algorithm	SHA256withRSA
Issuer	CN=emSign Root CA - C1, O=eMudhra Inc, OU=emSign PKI, C=US

Valid from	Wed Aug 12 13:30:00 PET 2020
Valid to	Sun Aug 12 13:30:00 PET 2035
Subject	CN=Soft-Net Secure Signing CA - C1, O=Soft and Net Solutions SAC, OU=emSign PKI, C=PE
Public key	Sun RSA public key, 2048 bits modulus: 181355980255826170393776473382269657872886364290788710111611383690995698634266302304186685314993765994021505066230078686113615538625164427728359999697432830568746989809181169865924906667060035565876582552509683298363705652510844989581479123499641136336537366262845700489873925126085553625483669664475113034632853301572429929075024009703567113770130775578257624352384652293970370788398011542785924084378774399495960716912120732392007484358288469920676005897222736799766818319558925075228823243118362473504770750819052389598701351191501701202386534887100081224026730680803649406018614752172431616683644905203859084666 3 public exponent: 65537
Subject key identifier	e85e0212e347945b655e072087adb773113d6f77
CRL distribution points	http://crl.emsign.com?RootCAC1.crl
Authority key identifier	041830168014fea1e0701e2a0339525a42be5c91857a18aa4db5
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=0
SHA1 Thumbprint	8b9d93d9550e542aaefabf7d864956485447d267
SHA256 Thumbprint	ccec157da0f0bd58e3e8b584054fe0c44f04b4dd8c97b75b788d9140b05142f7

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=Soft-Net Secure Signing CA - C1, O=Soft and Net Solutions SAC, OU=emSign PKI, C=PE
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
181355980255826170393776473382269657872886364290788710111611383690995698634266302304186685314993765994021505066230078686113615538625164427728359999697432830568746989809181169865924906667060035565876582552509683298363705652510844989581479123499641136336537366262845700489873925126085553625483669664475113034632853301572429929075024009703567113770130775578257624352384652293970370788398011542785924084378774399495960716912120732392007484358288469920676005897222736799766818319558925075228823243118362473504770750819052389598701351191501701202386534887100081224026730680803649406018614752172431616683644905203859084666 3
 public exponent: 65537
 Validity: [From: Wed Aug 12 13:30:00 PET 2020,
             To: Sun Aug 12 13:30:00 PET 2035]
 Issuer: CN=emSign Root CA - C1, O=eMudhra Inc, OU=emSign PKI, C=US
 SerialNumber: [    4d3a149c fa144f9e 3115]

Certificate Extensions: 8
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: E8 5E 02 12 E3 47 94 5B   65 5E 07 20 87 AD B7 73  .^...G.[e^. ...s
0010: 11 3D 6F 77                                        .=ow
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: FE A1 E0 70 1E 2A 03 39   52 5A 42 BE 5C 91 85 7A  ...p.*.9RZB.\..z
0010: 18 AA 4D B5                                        ..M.
]

]

[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
 [DistributionPoint:
    [URIName: http://crl.emsign.com?RootCAC1.crl]
]]

[4]: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
 [CertificatePolicyId: [2.5.29.32.0]
[PolicyQualifierInfo: [
 qualifierID: 1.3.6.1.5.5.7.2.1
 qualifier: 0000: 16 1C 68 74 74 70 3A 2F   2F 72 65 70 6F 73 69 74  ..http://reposit
0010: 6F 72 79 2E 65 6D 73 69   67 6E 2E 63 6F 6D        ory.emsign.com

]]  ]
]
```

```
[5]: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
 clientAuth
 emailProtection
 1.3.6.1.4.1.311.10.3.12
 1.2.840.113583.1.1.5
 1.3.6.1.4.1.311.20.2.2
]

[6]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[7]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
 [
  accessMethod: 1.3.6.1.5.5.7.48.1
  accessLocation: URIName: http://ocsp.emsign.com,
  accessMethod: 1.3.6.1.5.5.7.48.2
  accessLocation: URIName: http://repository.emsign.com/certs/RootCAC1.crt]
]

[8]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:0
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: B5 43 22 FD DE 26 35 36   CD 32 93 4F 0C 85 07 B4  .C"..&56.2.O....
0010: 34 3D F6 F2 8C 84 E0 6F   24 1D BA 83 CD 34 16 DC  4=.....o$....4..
0020: 02 3F DE 4C AD 90 43 B0   E3 BD 34 2B 3D BE 3B 9F  .?.L..C...4+=.;.
0030: 5E DC D5 B6 44 FD A0 49   FE 55 79 40 DA 0D 8D C9  ^...D..I.Uy@....
0040: A2 6F 2C 53 0C 28 66 CB   57 3A 7D 13 A8 65 C6 E8  .o,S.(f.W:...e..
0050: 61 1B B3 16 46 6A E6 B4   F0 4E 48 56 2A AF F0 2B  a...Fj...NHV*..+
0060: 7C 00 C1 5D DF B1 0D B9   4C 1D 7C 5A 97 9D 09 AF  ...]....L..Z....
0070: D4 6B 8F 7B 47 E4 9B 41   0E A4 25 97 0E 8A 19 C2  .k..G..A..%.....
0080: D6 B7 69 8A BE 0D E1 C2   0E 7F C4 3F 49 FF 04 95  ..i........?I...
0090: A3 24 3D FD 68 16 0E CD   3E 1A F6 3C A6 49 E4 BC  .$=.h...>..<.I..
00A0: 6D F9 9E C6 6A 46 83 B2   C6 88 0B 49 3F 39 1F 04  m...jF.....I?9..
00B0: CB 2B 32 8D 10 FE 12 B7   8D 70 9F 50 92 A0 C6 8A  .+2......p.P....
00C0: 11 8A BF 15 B1 44 F7 E8   89 3B 0F CF A4 5B 82 88  .....D...;...[..
00D0: F6 88 53 DB B8 CE B0 4C   93 0D 91 3F FF D0 30 5D  ..S....L...?..0]
00E0: F9 1C A7 54 46 96 42 B8   12 08 B2 82 B6 78 58 D4  ...TF.B......xX.
00F0: 85 9E AF 8A 81 90 37 28   D5 B8 04 5C AE 47 A3 9E  ......7(...\.G..

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIE3DCCA8SgAwIBAgIKTToUnPoUT54xFTANBgkqhkiG9w0BAQsFADBWMQswCQYD
VQQGEwJVUzETMBEGA1UECxMKZW1TaWduIFBLSTEUMBIGA1UEChMLZU11ZGhyYSBJ
bmMxHDAaBgNVBAMTE2VtU2lnbiBSb290IENBIC0gQzEwHhcNMjAwODEyMTgzMDAw
WhcNMzUwODEyMTgzMDAwWjBxMQswCQYDVQQGEwJQRTETMBEGA1UECxMKZW1TaWdu
IFBLSTEjMCEGA1UEChMaU29mdCBhbmQgTmV0IFNvbHV0aW9ucyBTQUMxKDAmBgNV
BAMTH1NvZnQtTmV0IFNlY3VyZSBTaWduaW5nIENBIC0gQzEwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQCPqV83Us0NI2OWsJHYm1Zj4tpSyJIn1NrhcwBy
XiXXsRi24H/GNztAC1KX7b8a4QRdpaxqSbXwMHmf7zUZdAsQygwup4MGYfFx/FC6
zXMwa0aWag+OYBDMOulQf24HIJT6p7suwnzzzex9sX66eUWVP0ziqw5uQv77/Rh5
0q0mrV4h53mfF2byXNuZ+YM2bC9oS55OhWx70Yxd9KbXKUkTa/pxw7tJJVRjbShO
8c0Cyec5fb9Johry4oRZTouT13ISDSP6L6QscXAasJeW2ixAToGZoWzadv1Mckcv
5v0u0iWO5IeZwj2ZcWEJwIuq9yA5NPB3pnXMFwOEFR1IL1bHAgMBAAGjggGPMIIB
izAfBgNVHSMEGDAWgBT+oeBwHioDOVJaQr5ckYV6GKpNtTAdBgNVHQ4EFgQU6F4C
EuNHlFtlXgcgh623cxE9b3cwDgYDVR0PAQH/BAQDAgEGMEAGA1UdJQQ5MDcGCCsG
AQUFBwMCBggrBgEFBQcDBAYKKwYBBAGCNwoDDAYJKoZIhvcvAQEFBgorBgEEAYI3
FAICMD0GA1UdIAQ2MDQwMgYEVR0gADAqMCgGCCsGAQUFBwIBFhxodHRwOi8vcmVw
b3NpdG9yeS5lbXNpZ24uY29tMBIGA1UdEwEB/wQIMAYBAf8CAQAwbwYIKwYBBQUH
AQEEYzBhMCIGCCsGAQUFBzABhhZodHRwOi8vb2NzcC5lbXNpZ24uY29tMDsGCCsG
AQUFBzAChi9odHRwOi8vcmVwb3NpdG9yeS5lbXNpZ24uY29tL2NlcnRzL1Jvb3RD
QUMxLmNydDAzBgNVHR8ELDAqMCigJqAkhiJodHRwOi8vY3JsLmVtc2lnbi5jb20/
Um9vdENBQzEuY3JsMA0GCSqGSIb3DQEBCwUAA4IBAQC1QyL93iY1Ns0yk08MhQe0
ND328oyE4G8kHbqDzTQW3AI/3kytkEOw4700Kz2+O59e3NW2RP2gSf5VeUDaDY3J
om8sUwwoZstXOn0TqGXG6GEbsxZGaua08E5IViqv8Ct8AMFd37ENuUwdfFqXnQmv
1GuPe0fkm0EOpCWXDooZwta3aYq+DeHCDn/EP0n/BJWjJD39aBYOzT4a9jymSeS8
bfmexmpGg7LGiAtJPzkfBMsrMo0Q/hK3jXCfUJKgxooRir8VsUT36Ik7D8+kW4KI
9ohT27jOsEyTDZE//9AwXfkcp1RGlkK4EgiygrZ4WNSFnq+KgZA3KNW4BFyuR6Oe
-----END CERTIFICATE-----
```

CN=emSign Root CA - C1, O=eMudhra Inc, OU=emSign PKI, C=US

Type	CA/QC
Status	undersupervision
Status starting time	2020-10-27T22:44:21.000Z

Service digital identity (X509)

Version	3
Serial number	825510296613316004955058
Signature algorithm	SHA256withRSA
Issuer	CN=emSign Root CA - C1, O=eMudhra Inc, OU=emSign PKI, C=US
Valid from	Sun Feb 18 13:30:00 PET 2018
Valid to	Wed Feb 18 13:30:00 PET 2043
Subject	CN=emSign Root CA - C1, O=eMudhra Inc, OU=emSign PKI, C=US
Public key	Sun RSA public key, 2048 bits modulus: 26247538881278784918887441808900234165057609046147884746676566401197446 44608585861337843267892456396768492986032909376370602635800150964139328 38431388295541464557505440064746033789640055402976299605047976856128379 43410342081328554016178164530923033091856792080173636601612118276928452 29563173986052075157365205654118126713763381410421839372837620691862542 00367005449148315236267951536136110387592088524888371824501137053286575 82933743149177113226306442846318952860205968613675283653192398417133453 35948402101225253503697324129461781764406588455093914785641525025403218 83713553336953218809494258118923635365769770908 31 public exponent: 65537
Subject key identifier	fea1e0701e2a0339525a42be5c91857a18aa4db5
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	e72ef1dffcb20928cf5dd4d56737b151cb864f01
SHA256 Thumbprint	125609aa301da0a249b97a8239cb6a34216f44dcac9f3954b14292f2e8c8608f

The decoded certificate:

```
[
[
 Version: V3
 Subject: CN=emSign Root CA - C1, O=eMudhra Inc, OU=emSign PKI, C=US
 Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

 Key:  Sun RSA public key, 2048 bits
 modulus:
26247538881278784918887441808900234165057609046147884746676566401197446446085858613378432678924563967684929860329093763706026358001509641393283843138829554146455750544006474
60337896400554029762996050479768561283794341034208132855401617816453092303309185679208017363660161211827692845229563173986052075157365205654118126713763381410421839372837620
69186254200367005449148315236267951536136110387592088524888371824501137053286575829337431491771132263064428463189528602059686136752836531923984171334533594840210122525350369
732412946178176440658845509391478564152502540321883713553336953218809494258118923635365769770908 31
 public exponent: 65537
 Validity: [From: Sun Feb 18 13:30:00 PET 2018,
             To: Wed Feb 18 13:30:00 PET 2043]
 Issuer: CN=emSign Root CA - C1, O=eMudhra Inc, OU=emSign PKI, C=US
 SerialNumber: [    aecf00ba c4cf32f8 43b2]

Certificate Extensions: 3
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: FE A1 E0 70 1E 2A 03 39   52 5A 42 BE 5C 91 85 7A  ...p.*.9RZB.\..z
0010: 18 AA 4D B5                                        ..M.
]
]

[2]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[3]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA256withRSA]
 Signature:
0000: C2 4A 56 FA 15 21 7B 28   A2 E9 E5 1D FB F8 2D C4  .JV..!.(......-.
0010: 39 96 41 4C 3B 27 2C C4   6C 18 15 80 C6 AC AF 47  9.AL;',.l......G
0020: 59 2F 26 0B E3 36 B0 EF   3B FE 43 97 49 32 99 12  Y/&..6..;.C.I2..
0030: 15 5B DF 11 29 FF AB 53   F8 BB C1 78 0F AC 9C 53  .[..)..S...x...S
0040: AF 57 BD 68 8C 3D 69 33   F0 A3 A0 23 63 3B 64 67  .W.h.=i3...#c;dg
0050: 22 44 AD D5 71 CB 56 2A   78 92 A3 4F 12 31 36 36  "D..q.V*x..O.166
0060: E2 DE FE 00 C4 A3 60 0F   27 AD A0 B0 8A B5 36 7A  ......`.'.....6z
```

```
0070: 52 A1 BD 27 F4 20 27 62   E8 4D 94 24 13 E4 0A 04  R..'. 'b.M.$....
0080: E9 3C AB 2E C8 43 09 4A   C6 61 04 E5 49 34 7E D3  .<...C.J.a..I4..
0090: C4 C8 F5 0F C0 AA E9 BA   54 5E F3 63 2B 4F 4F 50  ........T^.c+OOP
00A0: D4 FE B9 7B 99 8C 3D C0   2E BC 02 2B D3 C4 40 E4  ......=....+..@.
00B0: 8A 07 31 1E 9B CE 26 99   13 FB 11 EA 9A 22 0C 11  ..1...&......"..
00C0: 19 C7 5E 1B 81 50 30 C8   96 12 6E E7 CB 41 7F 91  ..^..P0...n..A..
00D0: 3B A2 47 B7 54 80 1B DC   00 CC 9A 90 EA C3 C3 50  ;.G.T..........P
00E0: 06 62 0C 30 C0 15 48 A7   A8 59 7C E1 AE 22 A2 E2  .b.0..H..Y..."..
00F0: 0A 7A 0F FA 62 AB 52 4C   E1 F1 DF CA BE 83 0D 42  .z..b.RL.......B

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIDczCCAlugAwIBAgILAK7PALrEzzL4Q7IwDQYJKoZIhvcNAQELBQAwVjELMAkG
A1UEBhMCVVMxEzARBgNVBAsTCmVtU2lnbiBQS0kxFDASBgNVBAoTC2VNdWRocmEg
SW5jMRwwGgYDVQQDExNlbVNpZ24gUm9vdCBDQSAtIEMxMB4XDTE4MDIxODE4MzAw
MFoXDTQzMDIxODE4MzAwMFowVjELMAkGA1UEBhMCVVMxEzARBgNVBAsTCmVtU2ln
biBQS0kxFDASBgNVBAoTC2VNdWRocmEgSW5jMRwwGgYDVQQDExNlbVNpZ24gUm9v
dCBDQSAtIEMxMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAz+upufGZ
BczYKCFK83M0UYRWEPWgTywS4/oTmifQz/l5GnRfHXk5/Fv4cI7gklL35CX5VIPZ
HdPIWoU/Xse2B+4+wM6ar6xWQio5JXDWv7V7Nq2s9nPczdcdioOl+yuQFTdrHCZH
3DspVpNqs8FqOp099cGXOFgFixwR4+S0uF2FHYP+eF8LRWgYSKVGczQ7/g/IdrvH
GPMF0Ybzhe3nudkyrVWIzqa2kbBPrH4VI5b2P/AgNBbeCsbEBEV5f6f9vtKppa+c
xSMq9zwhbL2vj07FOrLzNBL834AaSaTUqZX3noleoomslMuoaJuvimUnzYnu3Yy1
aylwQ6BpC+S5DwIDAQABo0IwQDAdBgNVHQ4EFgQU/qHgcB4qAzlSWkK+XJGFehiq
TbUwDgYDVR0PAQH/BAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQEL
BQADggEBAMJKVvoVIXsoounlHfv4LcQ5lkFMOycsxGwYFYDGrK9HWS8mC+M2sO87
/kOXSTKZEhVb3xEp/6tT+LvBeA+snFOvV71ojD1pM/CjoCNjO2RnIkSt1XHLVip4
kqNPEjE2NuLe/gDEo2APJ62gsIq1NnpSob0n9CAnYuhNlCQT5AoE6TyrLshDCUrG
YQTlSTR+08TI9Q/Aqum6VF7zYytPT1DU/rl7mYw9wC68AivTxEDkigcxHpvOJpkT
+xHqmiIMERnHXhuBUDDIlhJu58tBf5E7oke3VIAb3ADMmpDqw8NQBmIMMMAVSKeo
WXzhriKi4gp6D/piq1JM4fHfyr6DDUI=
-----END CERTIFICATE-----
```

Certificate Service Provider Name (en): TOC PERU SAC

Trade name (en)	TOC PERU SAC
Information URI (en)	HTTP://WWW.TOC.PE
Service provider street address (es)	AV. GRAU 629 BARRANCO
Service provider street address (en)	AV. GRAU 629 BARRANCO
Service provider postal code (es)	15063
Service provider postal code (en)	15063
Service provider locality (es)	LIMA
Service provider locality (en)	LIMA
Service provider state (es)	LIMA
Service provider state (en)	LIMA
Service provider country (es)	PE
Service provider country (en)	PE

C=PE, ST=Lima, L=Lima, O=TOC PERU SAC, SERIALNUMBER=20547367112, CN=TOC PERU RAIZ G1, EMAILADDRESS=soportepki@toc.pe

Type	CA/QC
Status	undersupervision
Status starting time	2020-12-18T17:13:58.000Z

Service digital identity (X509)

Version	3
Serial number	4266143491429758250
Signature algorithm	SHA512withRSA

Issuer	C=PE, ST=Lima, L=Lima, O=TOC PERU SAC, SERIALNUMBER=20547367112, CN=TOC PERU RAIZ G1, EMAILADDRESS=soportepki@toc.pe
Valid from	Thu Jul 12 12:43:56 PET 2018
Valid to	Sun Jul 12 12:43:56 PET 2043
Subject	C=PE, ST=Lima, L=Lima, O=TOC PERU SAC, SERIALNUMBER=20547367112, CN=TOC PERU RAIZ G1, EMAILADDRESS=soportepki@toc.pe
Public key	Sun RSA public key, 4096 bits modulus: 815341689822087926835304612017818671140602301022672573124706674562691130365194287151995647012248849023830174769311984865068708379025995132289876111234710463370299250668229830824034518826099872148721708509723368012211031429759962782289745225944354110865014078795407587340650323178630235454671941499222390366497361653379108204780608539505312512598710229139639083295460160512068313482800506848230077872572432243914492308127682967900944374058223238294576182191198504289969416260863205132951239275225179467110197930169398392259944354110865014078795407587340650323178630235454671941499222390366497361653379108204780608539505312512598710229139639083295460160512068313482800506848230077872572432243914492308127682967909443740582232382945761821911985042899694162608632051329512392752251794671101979301693983922599238287386063275095414035159410883241510039628956910123107798113748810807381533789544590774858639354932639561552952581187571546695830932629982033038924147848942878700641037635951398548712959324641988074633038479902593939012045580199303522407370184041148688149152158167085795601023682774047219951748446942066975463411525059464128090175972563764132392542060038963527243162740690558700783793872456372245633090871952200103726022131535379777670466476694874857184800626901916030582214752843895380319374971999970785025447874456948411464837465945940282102762072544575641130123678473572183228120583839979498732243350578892352380269755621060522493375184803763083229545484981936453584973523110119199318009332690716500522065772.
public exponent: 65537
Subject key identifier	34c060f8d68709ffaa392f5420f61af8566d1203
Authority key identifier	04183016801434c060f8d68709ffaa392f5420f61af8566d1203
Key usage	keyCertSign cRLSign
Basic constraints	CA=true; PathLen=unlimited
SHA1 Thumbprint	0b0dca0d0e0b8025f58d54d373e66ceee13a6e9a
SHA256 Thumbprint	e1b58207f2c4dbbdb41a559c50b24e6aaccd04208bc5ee2942968131b4443398

The decoded certificate:

```
[
[
 Version: V3
 Subject: C=PE, ST=Lima, L=Lima, O=TOC PERU SAC, SERIALNUMBER=20547367112, CN=TOC PERU RAIZ G1, EMAILADDRESS=soportepki@toc.pe
 Signature Algorithm: SHA512withRSA, OID = 1.2.840.113549.1.1.13

 Key:  Sun RSA public key, 4096 bits
 modulus:
815341689822087926835304612017818671140602301022672573124706674562691130365194287151995647012248849023830174769311984865068708379025995132289876111234710463370299250668229830824034518826099872148721708509723368012211031429759962782289745225944354110865014078795407587340650323178630235454671941499222390366497361653379108204780608539505312512598710229139639083295460160512068313482800506848230077872572432243914492308127682967909443740582232382945761821911985042899694162608632051329512392752251794671101979301693983922599238287386063275095414035159410883241510039628956910123107798113748810807381533789544590774858639354932639561552952581187571546695830932629982033038924147848942878700641037635951398548712959324641988074633038479902593939012045580199303522407370184041148688149152158167085795601023682774047219951748446942066975463411525059464128090175972563764132392542060038963527243162740690558700783793872456372245633090871952200103726022131535379777670466476694874857184800626901916030582214752843895380319374971999970785025447874456948411464837465945940282102762072544575641130123678473572183228120583839979498732243350578892352380269755621060522493375184803763083229545484981936453584973523110119199318009332690716500522065772
 public exponent: 65537
 Validity: [From: Thu Jul 12 12:43:56 PET 2018,
             To: Sun Jul 12 12:43:56 PET 2043]
 Issuer: C=PE, ST=Lima, L=Lima, O=TOC PERU SAC, SERIALNUMBER=20547367112, CN=TOC PERU RAIZ G1, EMAILADDRESS=soportepki@toc.pe
 SerialNumber: [    3b3462e7 0783f52a]

Certificate Extensions: 4
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 34 C0 60 F8 D6 87 09 FF   AA 39 2F 54 20 F6 1A F8  4.`......9/T ...
0010: 56 6D 12 03                                        Vm..
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 34 C0 60 F8 D6 87 09 FF   AA 39 2F 54 20 F6 1A F8  4.`......9/T ...
0010: 56 6D 12 03                                        Vm..
]

]
```

```
[3]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 Key_CertSign
 Crl_Sign
]

[4]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CA:true
 PathLen:2147483647
]

]
 Algorithm: [SHA512withRSA]
 Signature:
0000: 02 38 C0 63 F0 CC EF B4   6F 73 28 63 0E 38 D0 14  .8.c....os(c.8..
0010: 33 70 1E 4F 77 BB 4E 4F   5B 86 5E D2 80 8F 25 EF  3p.Ow.NO[.^...%.
0020: 32 F1 19 C2 62 51 1E DB   19 6A 34 32 74 31 1F ED  2...bQ...j42t1..
0030: DA 87 66 37 6D B1 D6 6A   7B 5D 75 1F DA E9 5B BB  ..f7m..j.]u...[.
0040: 37 B3 63 76 F8 8C B3 1F   01 F4 38 3A 46 B1 10 8F  7.cv......8:F...
0050: 33 08 09 01 2F 60 D6 9C   B1 52 F2 8C D3 80 11 11  3.../`...R......
0060: BF 2D CF 73 84 27 6F 96   31 50 05 5F 6A A3 9E C0  .-.s.'o.1P._j...
0070: 67 1E 86 E5 6F 4B 56 CD   45 32 DC 6E 37 A8 10 D5  g...oKV.E2.n7...
0080: D7 BE 82 BD 27 BC 72 28   01 00 33 85 39 04 06 63  ....'.r(..3.9..c
0090: AB 19 BD 87 AE E1 0B 4A   B7 EF 18 83 B0 90 9A 44  .......J.......D
00A0: 6F FD 7F 43 3A 93 C5 BE   CF A3 3A AD 28 CB 6E CD  o..C:.....:.(.n.
00B0: 78 55 F3 99 04 86 42 B1   36 93 BC 17 B4 66 88 BE  xU....B.6....f..
00C0: 11 9F 01 63 73 E2 F4 3F   4B 0C D0 A9 04 25 2D 73  ...cs..?K....%-s
00D0: F1 54 0A BF 18 59 12 CF   65 D4 4D 04 9A 9B 8E 09  .T...Y..e.M.....
00E0: EC 52 52 0B 26 67 60 67   BC 3D 57 62 A3 57 11 05  .RR.&g`g.=Wb.W..
00F0: 73 62 0B AA 4B C5 FB 2D   D9 C0 2F D1 FB 37 67 17  sb..K..-../..7g.
0100: E6 69 4B 4E 09 DA 1C 0B   F8 0A 21 FF 5D 7F 56 7C  .iKN......!.].V.
0110: FB CE B6 66 9C E4 65 83   23 EF 03 4D 05 32 29 65  ...f..e.#..M.2)e
0120: E3 1F B0 AF DF 8B 16 19   09 32 67 5A FC F6 FA 7D  .........2gZ....
0130: 3D A8 BC 44 D2 CC 1E 40   DB BF 2E 8B 7A 91 E1 E7  =..D...@....z...
0140: 3E 1D 9F 15 79 D2 95 6C   3E F6 D4 39 76 30 03 94  >...y..l>..9v0..
0150: B3 40 65 FA D4 10 8A 31   D7 EF CB 1C 8E 9B F3 E8  .@e....1........
0160: D2 90 44 20 A2 42 7D 58   54 B6 6A 94 CD 27 BC CB  ..D .B.XT.j..'..
0170: 41 35 A4 F5 7C 57 A8 31   04 5E BB CC 05 62 D0 01  A5...W.1.^...b..
0180: 53 FB E2 B0 76 35 D4 E4   EE 1B 55 BD 3A BB 9B DE  S...v5....U.:...
0190: 73 C1 5F F5 C9 E5 0F D8   6E 57 D7 B8 F9 81 80 B1  s._.....nW......
01A0: 94 5E B6 8A 44 15 EA 09   19 C6 7B 9D 3E 23 D3 C5  .^..D.......>#..
01B0: BB 36 D9 5E DE 5A 6E 29   7A 4F 35 F4 47 2E 0D A6  .6.^.Zn)zO5.G...
01C0: 7D E0 96 D1 EA 58 D1 01   CB E8 99 65 D1 23 4A FB  .....X.....e.#J.
01D0: 8B 30 D1 A6 26 9E 54 66   6C 22 BA 7E C6 64 2A F5  .0..&.Tfl"...d*.
01E0: C5 06 00 EB 09 3D 11 4B   D3 13 44 EE 06 52 D0 CD  .....=.K..D..R..
01F0: B6 B0 72 28 0B 18 6E 5E   86 25 A3 29 F6 C1 82 49  ..r(..n^.%.)...I

]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGETCCA/mgAwIBAgIIOzRi5weD9SowDQYJKoZIhvcNAQENBQAwgZUxIDAeBgkq
hkiG9w0BCQEWEXNvcG9ydGVwa2lAdG9jLnBlMRkwFwYDVQQDDBBUT0MgUEVSVSBS
QUlaIEcxMRQwEgYDVQQFEwsyMDU0NzM2NzExMjEVMBMGA1UECgwMVE9DIFBFUlUg
U0FDMQ0wCwYDVQQHDARMaW1hMQ0wCwYDVQQIDARMaW1hMQswCQYDVQQGEwJQRTAe
Fw0xODA3MTIxNzQzNTZaFw00MzA3MTIxNzQzNTZaMIGVMSAwHgYJKoZIhvcNAQkB
FhFzb3BvcnRlcGtpQHRvYy5wZTEZMBcGA1UEAwwQVE9DIFBFUlUgUkFJWiBHMTEU
MBIGA1UEBRMLMjA1NDczNjcxMTIxFTATBgNVBAoMDFRPQyBQRVJVIFNBQzENMAsG
A1UEBwwETGltYTENMAsGA1UECAwETGltYTELMAkGA1UEBhMCUEUwggIiMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQDH2yhbiGSoLNmzPISGvO/XYsEKnev3lyXq
2Ql7bfUeboNjqSX1d7UkwnbJORlXpELDznglPeml5LFPjBqNS2Lq+4PVD+BjmaCU
i8v8+233bP9kNRYfxKSapiEKTRGjDRi5xudWUTMG/mHFjYYeWaz9kbg/EeRNPQ8m
pdUVwC9tec10A82Bk9owveC0pdeBBDhx23P2C32hjveo19bD+029NFlAQurB1PoJ
GsxgNR3qGfNjh7lVn2KAQCoU15LPativY9I9J98rS0Q5GntiZJ5GcyqHpe/MMOC3
JMG6jsgHF4brr2gBz+sdMc34tnihc4uH5aWQHdrB1RrQK3skge6WYOIn8H6MkDe/
8xuE3JAX1OU4Wna1skn+Ls2fsS7pSYuft+on6TdhqnFhgFqwra6M88AUbpE/7T9Q
5X+zHSbTVO8CbVL2LzBDczwsF64qcuR/CSDn1F7J9hs8ZFhmK9UbevYYPA8IvQRZ
r4uFN3+Dj4dabоGO5SIcSXE2q8lB6KpBvcyBjDVZRMDlwW7FF2TKNOK+RlKZj22G
8+bWWn9wwnk2PpmmQ8C0Huc1IWrgPeUYeZin1dHCE/TpwsDf8qLKgNc6virPh5ZR
93CmVUoEfzvkW8iM2b6f+U/sxkmTwn5J8TFownAE9OP3slTN1kh3PLVg3atg7p/t
auPiVvFv8QIDAQABo2MwYTAdBgNVHQ4EFgQUNMBg+NaHCf+qOS9UIPYa+FZtEgMw
DwYDVR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBQ0wGD41ocJ/6o5L1Qg9hr4Vm0S
AzAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQENBQADggIBAAI4wGPwzO+0b3Mo
Yw440BQzcB5Pd7tOT1uGXtKAjyXvMvEZwmJRHtsZajQydDEf7dqHZjdtsdZqe111
H9rpW7s3s2N2+IyzHwH0ODpGsRCPMwgJAS9g1pyxUvKM04AREb8tz3OEJ2+WMVAF
X2qjnsBnHoblb0tWzUUy3G43qBDV176CvSe8cigBADOFOQQGY6sZvYeu4QtKt+8Y
g7CQmkRv/X9DOpPFvs+jOq0oy27NeFXzmQSGQrE2k7wXtGaIvhGfAWNz4vQ/SwzQ
qQQLLXPxVAq/GFkSz2XUTQSam44J7FJSCyZnYGe8PVdio1cRBXNiC6pLxfst2cAv
0fs3ZxfmaUtOCdocC/gKIf9df1Z8+862ZpzkZYMj7wNNBTIpZeMfsK/fixYZCTJn
Wvz2+n09qLxE0sweQNu/Lot6keHnPh2fFXnSlWw+9tQ5djADllLNAZfrUEIox1+/L
HI6b8+jSkEQgokJ9WFS2apTNJ7zLQTWk9XxXqDEEXrvMBWLQAVP74rB2NdTk7htV
vTq7m95zwV/1yeUP2G5X17j5gYCxlF62ikQV6gkZxnudPiPTxbs22V7eWm4pek81
9EcuDaZ94JbR6ljRAcvomWXRI0r7izDRpiaeVGZsIrp+xmQq9cUGAOsJPRFL0xNE
7gZS0M22sHIoCxhuXoYloyn2wYJJ
-----END CERTIFICATE-----
```