

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 Guías de Acreditación.

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 amended by Supreme Decree 070-2011-PCM, and the Accreditation Guidelines.

<i>Scheme territory</i>	PE
<i>Scheme status determination approach</i>	appropriate
<i>Issue date</i>	2018-11-29T21:00:18.325Z
<i>Next update</i>	2019-05-29T16:00:18.326Z
<i>Historical information period</i>	3653 days
<i>Sequence number</i>	25
<i>Scheme information URIs</i>	http://www.iofe.gob.pe/ http://www.iofe.gob.pe/en/

Scheme Operator

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

81840250607529923946313763098980784333900879154578808727714083680357843
64345879548767445200282566378711148940768917407358633453139140391569500
6032520276907079315615226531801772660363656546656156139250475577764233
54967748700878972678222256596932289277384594974841086946665946612185842
66334955512342611037939699329888902671200121025037302713613130526180602
92457067600325046187572471020460481743913815400714652320432989584053225
91304035180888164936705658113651449317062571167953687831746289088315087
39810608805542178786400877626069176820781260645478990825957262810667870
71475832935115588709859760056782398552643294404533086560312975439252436
82249519974613774764012972314912458163979156972705451310085375220657750
98052534488798747647186162567637970033421493519086499976106802238837133
11287833824460286278174765392386562908577270531724723663795072825282576
52597515411540033515199926327389348387601247656450377361985453739096645
05050101667246721482228725458892749811800214564832563113604138616014320
4190580039823166150077093219196458478862956514566588996993303493808370
91845043922288645794806074792931564212551488935522668876882537857607789
37757637161222769636516043369803858901672191073904751668163123975810855
74487321264714261513760879

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:
81840250607529923946313763098980784333900879154578808727714083680357843643458795487674452002825663787111489407689174073586334531391403915695006032520276907079315615226531801
7726603636564665615613925047557776423354967748700878972678222565969322892773845949748410869466659466121858426633495551234261103793969932988902671200121025037302713613130
52618060292457067600325046187572471020460481743913815400714652320432989584053225913040351808881649367056581136514493170625711679536878317462890883150873981060880554217878640
08776260691768207812606454789908259572628106678707147583293511558870985976005678239855264329440453308656031297543925243682249519974613774764012972314912458163979156972705451
31008537522065775098052534488798747647186162567637970033421493519086499976106802238837133112878338244602862781747653923865629085772705317247236637950728252825765259751541154
0033515199926327389348387601247656450377361985453739096645050501016672467214822287254588927498118002145648325631136041386160143204190580039823166150077093219196458478862956
51456658899699330349380837091845043922288645794806074792931564212551488935522668876882537857607789377576371612227696365160433698038589016721910739047516681631239758108557448
7321264714261513760879
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

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

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 12 406.....0D<.@
0020: 71 5B 9C B6 B9 36 91 4D 28 E1 D2 65 DA 8B 8A F5 q[...6.M(.e.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 FFg(...0UoB..
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 7Do...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.r.D.8..
00F0: 83 D0 D0 C9 BD 25 BF 50 04 C2 D6 1F B4 0B 08 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 58nw.....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 D0 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 E8 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 59F.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 70 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 5CI..E.....\
01E0: 04 E7 A0 A6 F1 95 35 A0 EA 0F 95 FE 48 23 4E DD5.....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-----
MIIGizCCBHOgAwIBAgIUxPERaNB4nMA3pFZyNFZxI3ZV0wDQYJKoZIhvcNAQEF
BQAwDELMakGA1UEBHMCEUxPDA6BgNVBAAoMML1Z2LzdHJvIE5hY2lvbmFsIGRl
IElkZW50aWZpY2Fjac0zbiB5IEVzdGFKbYBDAxZpb2EnMCGUA1UEAwUkVOSUVD
IENlcnRpb2glYXRpb24gQXV0aG9yYXR5MBA4XDTpZWMDcyMTIyNDUzMTloXDTIwMDcx
ODUyNDUzMl9wga0xczAjBgNVBAYTA1BFMTtww0YDVQKDDNSZWdp3RybyB0YWNp
b25hbCBkZSBZJGVVdGlmMWhNY2N0S24geSBFC3RhZG8gQ2L2aWwzJzA1BgNVBAsM
hUJFTkLFQyBDZXRjOaWZpY2F0aW9uIEF1dGhvcml0eTECMBoGA1UEAwTUkVOSUVD
IENsYXNzIElJSSBDQTEZMBCGA1UEB0wOUlVD0iAyMDI5NTYxMzYyMDCCaiIwDQYJ
KoZIhvcNAQEBBQADgglIPADCCAgocGgIBAMiB0cId5htddebM/cc+X7b4M2F1Iy2o
1mdID8uk3vzgsiU4jAUQCAgqZZ1+bSgaBkaWBLamXRM0LiccjijCTpTyRe98WEJ
bLKRim9pQvGzNqHkclHKwzPTCz7u65Be8tF2f5kbECn00yx0SqwR7v900CahSuH
4zBDBDRfyGNguzKq0LqgUzXJq+mXhqu43ecy0n84tWh0sRmBp2iJDzvYvCBct/u
at6q90Y02NW0B0hcMwrn15q7jjFIKtbtIKX46AYR+H8Dx0au/LRug0w5iLTwBIMv
i60KrdG0J031i+w9F//8eMc6zIb00IK+FXdzeEjqlFAfTntjK0owrLENFYika/
Big5J5vJksrHvMvMzLVe8GCIX0LrKlOjC8LYfIA0I8mPg+Uagd5/6qQEYJjaPhVn
Bt6N35pxV7mvuKUZTK6dvEagI0Pnm2dz5SxzG5zq+0akMKWSNEwXeytYIK0p6/
dv6elZqAzo9iDeg50x23j7Gwsm8LtghaeRfL0FGl92VD1IEjRedGNrpT6i72NbPg
o/a/SE7FJfTcMIkQV4dCnftgmYjuYvvtIAzWQL/m51YxwhRUcxF50x0D0lbKXX+1
xJCSN6ADpp6/cImuAhsB/7bDqM1Yc2USKvGl/n1rLpR7leXjqf4ZxcJgxeU1JAC
HxmznpSRRfbvAgMBAAGjgDowgdGdwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQU
CW7S2T/VyE67HGngT1r1ZPtB8/0whWYDVR0jBBgwFoAUsjLQIap6/79+qgsT5r/z
tSfAymMwPgyDVR0fBDcwNTAzoDGGL4YtaHR0cDovL2NybC5yZ5pZmWuZ29iLnB1
L2FybC9jYXNlcnZpY2ZvMDEuY3JSMGUA1UdIAQ9MSw00YEVROGADAxMC8GCCSg
AQUFBwIBFiNodHRw0i8vd3d3LnJlbnllYy5nb2IucGUvcnV3b3NpdG9yeTANBgkq
hkiG9w0BAQUFAAOCAgEAdSrd3Yy/9YH++zW0rVYb5ka2B/0NgKDC9b8T08EkBx
W5y2uTaRTSjh0mXai4r18hGxvwdg4YTo3iRDgthLuICIg7fGga2+iaQw0kCBFv
q62B+mcor0sIT1VvQhr/Po3MtaMP1nG6+v7PGgz0HmYINFAmYt0P1NDQdiWE8Zf
Hm0F6iKkgZ04YwksW3CxpPB7j2/2jHJ++DCBew/XfXo7VjfgkKbKv5bHx0B0jm2
aeVht/F9s0UvnzYQ+BKggqMVFIKtckr0GyAzanPwA1ZzKc3jtw3k4n4u5qfEpbQk
IJy90JNxmFDhckSK0K0Wg9D0yB0L1AEwtYftAuwP9g3eGuEjMw36FLMGED+0DH
xtPB9hy3bnfv+qvw7LYNG2C3+bnueE5iucn/CsU8r+jer6MDLEEXNsZo9adj/MQ
Mh/mfW9wQukHV3gsgy9Mt2f+BKWSVCEC5iPA47ENnzDyS1QWV015o0hPY5FUAF
CsnGdLw2N6/hD/dLzqPtpw/akoxGhzLub6B3iZJCWavAdn0aBz0oIG2IPRR0aEs
k31EXoqsakHq/WYYPHhaS6SptQhendVotuBAGEJe+FeLoSs/nCLsxWfQ+Xtr6rr
ygbKzRJu1FARmtmN9cB0GepvGVNaDqD5X+SCN03W5V0vCgHsj823E5M98NmY=
-----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
769049142885762476827032827
public exponent: 65537

Subject key identifier 12343c6172d19d8acc455c001d970dcaa8c91f4f
CRL distribution points http://crl.reniec.gov.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:
10322105508640716486498782637964411902040075877659293686819537442119967901985594693634339481190265571315642172640381142366544651099844487010665732773998926515504813789471782
49234890001167950018234713297768631158937919120744294372288011590660836415120591085643889903981943367949815006858541410731378550930809959545791252362061612810349018782500176
17243950865888401351192133299482515524450876533706809094507055182112858278666647501679130714995204143343177054067775323522335636099576377163530218131283919208316406371042211
45902109249703159551516734088239331855097081999776495416734569522569973400989607976096570955199310475669915479166540145698590796704968270876708899456859948320992522365292317
41488930321451375451169347909073013427235469462201077019577054716666251994245762335652933271685163653768704077495710317039906794211618539262350452830538387815937713408911825
13678374579971834115773167459487980591743636596175663533252885040589456516760588615129814117704718912725379429383083689074849514837543364788482892884714902516889886748087484
54825119558204999740593224506877804163692977420904986783799379682138975642551669568655163020248815919374514598392206285055412184159347217418682841385241833614399270437157690
49142885762476827032827
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 a367f6f89 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\.....

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

```
0010: A8 C9 1F 4F ...0
]
]

[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.B].
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 84 D1 70 7D F0 43 FF @^..N...=...p..C.
0030: D9 D4 01 8E F0 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 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 67 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 39 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.....oS.W.
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..FSJ]-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 89 25 A8 4A 8B 56 23 17 2F AA D2 42 ..(8.%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.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-----
MIIGozCCB1UgAwIBAgIU5xPERaNNb4nMA3pFZyNFZXi3ZV4wDQYJKoZIhvcNAQEL
BQAwfzELMAkGA1UEBhMCUExPDQ6BGNVBAoMM1JLZ2ZzdHJzIE5hY2lVbWFsIGRl
IElkZW50aWZpY2Fjac0zb1B5IEVzdGFkbW9kYXZpbnE5MDA1UEAwVjV0SUVD
IEhpZ2ggR3JhZGUgQ2VydGlmYWVhdG9kb3BDbXZpbnE5MDA1UEAwVjV0SUVD
IEM1WHcNMjAwNzE4MjI1MzI1YjCBuDELMAkGA1UEBhMCUExPDQ6BGNVBAoMM1JL
Z2ZzdHJzIE5hY2lVbWFsIGRlIElkZW50aWZpY2Fjac0zb1B5IEVzdGFkbW9kYXZp
bDEnMCA1UECweUKVOSUVDIENlcnRzZm1jYXRpb24gQXV0aG9yaXR5MScwJQYD
VQDDB5SRU5JRUMgQ2xhc3MgSULJIEMhZ2ggR3JhZGUgQ0ExGTAxBGNVBAUMFJVV
Qz0gMjAyOTUzMTMzMjAwNzE4MjI1MzI1YjAwGCSqGSIb3DQEBAQUAA4CDAWggIAoI
CAQD9A82DjJiZVgZJaCyeFBnyxkM4p6Rt061Bo6bLhrziFg09acGbjD6q7vpNfnLVPJM/
vwNhmvwBLdP0u3zsIpg9mAB/5ebPdA0JFH5VbKEDjGL9kgyC/Pw0otzHuY+HDJ8
5SK0LhcbeRqXREZaRnQdY9qN9cZpJ0+vPcL5LYu1UUGw6u+wFMDHXE3047T33A5
7VG3mVcZjIqXehaIbPnP3KX4BH6UFL7KB5Mcoy2TSTRZKpQd63ecse1R00Plj+7
f2eRuwCeb0MJKYhPtYwJf0EADSiLG0xa1p7V/0DsgIlrZF8Sk9xp6hBY5f/EJT
33ZcISFMBDDjdnxayhLPO3ftdNvnmM8WiIrm55NBL4Tg4t32ZSf6F00FrfDI2c7hw
YE62JyqTg28ebolgpCwRrVK5tI2fr0mFIUo0ohvKdCFyZUSrVpzuDw7VhSLzqqNSs
e0X31tXFJ/CCekQoJfMePqfD/Ux3neY4wZrLLiSer032dNqestAL3XzsH3D5Z
-----
```

TaxpX0Itj lCnIu4uphuZDH4j34LN3s40LEK6WtKsqPagDA0i89vB+XQu0HXIP0n
C0S1cyCUTukt2J0eB05E7ax3o3Ccs/N4c5LRrsusB3mZd7UMEsRE4xRFvd06xjZv
7165FM9uEEMyCj6GDRK5o65JJDWAUtg5gxESab08+wIDAQABo4HcMIH2MA8GA1Ud
EwEB/wQFMAMBAF8wHQYDVIR00BBYEFB10PGFY0Z2KzEVcAB2XDcqoyR9PMB8GA1Ud
IwQYMBaAFea16FtnmR0CjQYMBv9CSp4JjZwmMEAGA1UdHwQ5MDcwNaAzoDGL2h0
dHA6Ly9jcmwucmVuaWVjLmdvYi5wZS9hcmwvaGdjYXNlcnZpY2VzMDEuY3JsMEQG
A1UdIAQ9MDsw0QYEVROgADAxMCRGCGsGAUQFBwIBF1NodHRwOi8vd3d3LnJlbnMl
Yy5nb2IucDUCVcmVwb3NpdG9yeTANBgkqhkiG9w0BAQsFAA0CAgEAB82tnYzUUA0
ooMhyXI9xyvX08rLxR1y13oAvG5dZ+pAXhHUTrHWPdu00XB98EP/2d0Bjv1NteNS
L/wJj8M/Bhyc0mJUgRwy0b5Z5TtjUMZ9A9k5jGHcnDeceKIqc34cc4S/n+qv6AEB
KCX/Apg6Rt0d1E25FS616uzZ0oIzxFbSoZKKjDr4PfoKUFbChcT1M+jZW49zV1j
oge3jEP7nUMadGP6y/2c9xn5wK4a91v04IxtducruZp611f7R6CBhkwpqBHa03i8
2rAvF6mm2Lcf4DLyL8FXmCZnqJJoERmdpfVKfNaJy54DJWI5DMdLgywY7Y9GoGiv
EgT823aRkXI6SEgwrBzIq1XdFBG08ELNaCL0SVKxVuE8MAQt50qEzV7V7G9rsij
KG9Mg4PmqgT64hvqkK75eaiW9Td719oUQA2iawbcTMnqPQMnuFwbisRLNdyUYt
VZqE4oysIsetmjSEz22njEL5zIQEn0reLEuqIMiL1z2FZdfiP2KgeH4RtLVlpJse
j0x7vYoFIPwoMT15JahK11YjFy+q0kKRnWgnYr0k/oP/9rDpoBgVp2QdRCJmm2d
aPfiHd1+3kesL4LcTdZ0KHb6FT0xRuCBiLogQMnyantI4/vD20CRQrSvCe/Ze4P
5mc05Mmdt7RIsxTCJFzFfYDF50VovY=
-----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:
66530449338922445472305525839440217278274410524465983445852205298698590
80756260943945495710405079660020378520959903942124213059222541708527991
13151448879155014256345541410785909426710180892901794298810705848775648
46263577598691423538839300030692161348626780079589202439268135739040151
70698553667191579627100308836350783225953309187161820785072591983726838
96046394809347008080997237745455462182986068574368145469552618466880034
08406824432067444984309066343139318238474738647731630372472137477766691
33471156987522748833187387854461539994517415031451704193494356040446862
40559977829723727855421850538998027237169917437849204106293777132340367
31766998266041425699306973661031894488093814750213604656202468809710681
07586696660465191227871975035641697942265257401118431137586148108961144
26952209439386083547076503847181894028010260350034686261696148452245109
44725376456150180495996777841873182271647716986269346467307749108780135
54416503231680324751538291288114231559950311561770180344311213821409232
17012897485736425056523806025665876613749693008422026785889949358565156
62174578818618460112970375341171509350497216463840574776181750105854141
01605521488719311480892706868003328896637982956124519572961631610394243
65351153851505845285012639
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=RENEIC Class II High Grade CA, OU=RENEIC 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:
66530449338922445472305525839440217278274410524465983445852205298698590807562609439454957104050796600203785209599039421242130592225417085279911315144887915501425634554141078
59094267101800929017942988107058487756484626357759869142353883930003069216134862678007958920243926013573904015170698553667191579627100308836350783225953309107161820785072591
9837268389604639480934700808099723774545462182986068574368145469552618466880034008406824432067444984309066343139318238474738647731630372472137477666913347115698752274883318
73878544615399945174150314517041934943560404468624055997782972372785542185053899802723716991743784920410629377713234036731766998266041425699306973661031894488093814750213604
65620246880971068107586696660465191227871975035641697942265257401118431137586148108961144269522094393860835470765038471818940280102603500346862616961484522451094472537645615
0180495996778418731822716477169862693464673077491087801355441650323168032475153829128811423155995031156177018034431121382140923217012897485736425056523806025665876613749693
00842202678588994935856515662174578818618460112970375341171509350497216463840574776181750105854141016055214887193114808927068680033288966379829561245195729616316103942436535
1153851505845285012639
public exponent: 65537
Validity: [From: Wed Jul 21 17:36:51 PET 2010,
To: Sat Jul 18 17:36:51 PET 2020]
Issuer: CN=RENEIC 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.B].
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./..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 08 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 B6 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 ..^?...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 ACt.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 09 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

1

The certificate in PEM format:

-----BEGIN CERTIFICATE-----
MIIGojCCB1IqgAwIBAgIU5xPERaNnb4nMA3pFZYNFZxI3ZVwvDQYJKoZIhvcNAQEL
BQAwfzELMAKGA1UEBHMCEUExPDA6BgNVBAAoMm1JL2ZldHJvIE5hY2lvbmFsIGRl
IElKZW50aWZpY2Fja0Zib5IEVzdGFkbyB0aXZpbdEYMDAGA1UEAwpuKvOSUVD
IEhpZ2g2R3JhZGUGQ2YyZGlmYWVhdGlvb1BBdXRob3JpdHkxHhcnMTAwNzIxMjIz
NjUxwHcnMjAwNzE4MjIzNjUxwHcnMjAwNzE4MjIzNjUxwHcnMjAwNzE4MjIzNjUx
Z2ZldHJvIE5hY2lvbmFsIGRlIElKZW50aWZpY2Fja0Zib5IEVzdGFkbyB0aXZp
bDEncmVudGUA1UECwweUkVOSUVDIENlcnRpbmZlYXRpb24qOXV0aG9yaXR5MSYwJAYD
VQ0DD1SRU5JRUMgQ2xhc3MgSUkgSGlnaCBhcnRkZSB0QTEZMBCGA1UEBQwQUlVLD
O1AyMD15NTYxMzYyMDCCAIW0QYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAKMu
PNpNK90j5AUGYLiZ5VFFUYIXxNA/6FXeqiYL2H0L306FR5ABaC00NRRQEvAFf70
NUX80NLRyfnbxy4I9YA+HZfOHGSPSYf8uGJYp9BugsTS1P1qGweYBkmUHXOTZb4Lw
WC4h3/kmG5MCfpJEshyYwThP13L0NzQC1w0KxMyEMAK/84vmU8L0D017FyBIJC
Ts0J2aso5oDIbgLksW4i2Ao0r8rNw15YtzCg2H3H7j0Dv0qnjcabc4HV51LF8cyU
Apej/+bHb4LUIqzXXhgBtbK7cgr7gWnSstEjJfQ/Ji7ZUswz0zIHx0GgXLiSGK0
YXZbjGhHE7N6VI0t6zIaIh/suy684I79+NykKfNDfG+sefUboeQNFQIRdB63d0jZ
LJ3ME1znwDYpAR3Nrlq0noUZH4yS03W6Ht5uMNSncapb+1kxRxy9vhglctnJK1Bf
fhGhVBB+/DHSUAtWt5BdQzSIETZtHV0mp//jbiZTN3VA98qudTumPt32tQ7HV/0
HtmM+/e3L8ph24pt70D7kxK+Pov77VdyK/GQWkbrA1wbJ2/qS2b9D/JfrIn7wwD+
XyrGy80jpkuz2qZUy5Ia7n6YU/LdV9zClj9tCF9G5G6dyA8rzepDlk0dXYEthxTL
gAN5Apjvuh++c1a0aRTK2L0WqhoE0QRULPHdhsCfAgMBAAGjgdwgdkwDwYDVR0T
AQH/BAUwAwEB/zAdBgNVHQ4EFgQU7d585zJ0HjxYgrIgvqW+L1VgIYwHwYDVR0T
BBgwFoAURrXoW2eZ4KNBqXu/0JKngmNLaYwQAYDVR0fBDkwNzA1OD0gMYyaHR0
cDovL2NybC5yZW5pZmMuZ291LnBlL2FybC9oZ2Nhc2VydmljZXMmMS5jcmwvRAYD
VR0gBD0wOzA5BGRVHSAAMDEwLWYIKwYBBQUHAgEWI2h0dHA6Ly93d3cuVuaWVj
LmdvY15wZS9yZXBvc2l0b3J5MA0GC5qGSIs3DQEBCCUAA4ICAQBVC/OM0geSLLj
tcqFBW0N9/dg93TLb0d67hCQLLJVULNAkyPp3J4Qj9gSaEE/gCmDGUBQPveNt6a9
6H8XeUduUXFFZrv/OdiHF4Bx1b00dcMtOueJca9+WUS8IPdtjWwtgBuyfqk10m
zBrt1q0xDtVurPw2LYKco//RDjBp0LJh2DaWteACLylTctbGxofM2Mta4iuSW0
8jwbbh887EqRxAtoUdnPH7U/CsYjvh/FnBqoW2LYY0uNFC+1j5t5aK8LrgIxm7Q
C0Ji3AoeqK06BactG/374qa16YnV6/peN+SCHXU5hnxZCubat2pieTwp77oDxpLG
7fuVlUY2c+a1wqWjQdKL+JwxYiqmYvBtH1rS07ajyDp0LT6yf85Ip+jwocRUcoy7
nsd2LLeIUbfLpph30eXMD2M391Luk81xLA672NkhLte5G86x7yYcp+0u0aPrtMx/
A3TIOUysTuvJV1wufgjrohi+VgZY1aMyKPCISZlemqT37AJs9hddWu1Vua0atFi
j03sS323ByFRpT2I8qZcmhM6Q14AAewS4bKPKDkmwV2EKhoj6s+2bQeS5w3Y3Lid
h17f2Wxqr4oKM00n1QJNVW6idiXsPDV4PucWveK+o8T/NwtSwGDu0HhC11Kj+FUB
9VEHU2Y8G56ia0iK3JL/MNDPKGnW==
-----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
82015730737672617855525165179816619245200353175688964691801615138898398319799331858376896535640574561568973140105578747223667092461859135799002767416620141682074498081148815
05689967043498332734369125871359798597410743895948799693115534873779230450867352599953028065247027589468314656001986242249719988928466115960774709259607088770296511763295925
74237908819465892757075454432297417070992201733946173946241509299711210465000931292351574938610562714058293359904306275518607683383977212913375734842372778346807895308587570
58179614697819311164193352429298975597332184054216477105264763663327333866651939369745246189514935597036156752509933844104651943794407615773016247296164144992023073498760300
54063303399829365241693643393143010299782442214647357631217199285035769145463239016514553613133542002838079860403815763699766412619483222826738495029468061617799697470191176
87733887948333645679416444571025082796336262888438917625589086585339778649952056240442986272365216455183466802611222930714267947327781861149786137628479306745150647899890390
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
```


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:
97482974381192860297271599748529075145603706561626700901374970936411086
98960727345439221916268193878294010926032687728144063024771398122323654
75510345311393682826757219683954382745620418640602220960850400689849406
95460757846237072874770308423282009547608575772329842325713666717728392
89408696148793810737892207941636755805947169302965149320188921075346706
42232169811896300178005011493714040485029492607037102045780004231857647
88869514017616800585906426543055893698057793964143727401756108818342849
57405534332110087774785879306063055849676983791356726856914845944152408
42210152165529135423824479346653658011823207946038311797440592600720292
13656488437546836006608441657239918084556759161335235284635209119516124
27032036314836450447360836925764149281654978297933151883016654232776611
24158169459181090110662234290538960139604102798234191399360444235622149
22226240616383079234617974988735375127501067259393746629273604519017971
36259130581372796671169800336733377071277438258656157300069802250990540
54797433780720204638842942073565409116090225276246848062024443213442386
61734233822269654714798034207313305340984195958814047607756293745440361
70325573264764395886364465667788385493600068725646427729184987154620130
00037014211405288233037651
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:
97482974381192860297271599748529075145603706561626700901374970936411086898607273454392219162681938782940109260326877281440630247713981223236547551034531139368282675721968395
4382745620418640602209608504006898494069546075784623707287477030842328200954760857577232984232571366671772839289408696148793810737892207941636755805947169302965149320188921
0753467064223216981189630017800501149371404048502949260703710204578000423185764788869514017616800585906426543055893698057793964143727401756108818342849574055343321108877478
58793060630558496769837913567268569148459441524084221015216552913542382447934665365801182320794603831179744059260072029213656488437546836006608441657239918084556759161335235
2846352091195161242703203631483645044736083692576414928165497829793315188301665423277661124158169459181090110662234290538960139604102798234191399360444235622149222624061638
30792346179749887353751275010672593937466292736045190179713625913058137279667116980033673337707127743825865615730006980225099054054797433780720204638842942073565409116090225
2762468480620244321344238661734233822269654714798034207313305340984195958814047607756293745440361703255732647643958863644656677883854936000687256464277291849871546201300083
7014211405288233037651
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.

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

```
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.B].
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.....
0010: 0C C1 64 A0 AF 28 72 40  3A 33 E0 DC 60 23 00 40  .d..(r@:3..#.a
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  ...$..ro.X.v
0060: BA 20 58 64 F5 C3 76 2D  FF 1D EC ED D1 BE 80 F9  .Xd.v.....
0070: F9 E6 68 DD F5 98 AD 56  E8 D1 CC 2D A6 B8 02 E8  .h...V.....
0080: 31 F5 30 97 95 DD D2 5F  A1 BA 0B 5F AB FE 23 F1  1.0.....#.
0090: D2 16 7C 26 D8 B2 DC 63  ED 34 34 D6 70 F8 B4 1E  ...&...c.44.p...
00A0: 0D 69 92 96 75 EB F6 65  24 6E E5 E9 63 9D 2F C7  .i...u..e$nc./..
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 50 D4  ..R..b:.....].
00F0: 5B 24 09 3A 00 BF 61 EA  E1 13 99 A7 9C 29 E7 B0  [$.::a.....)..
0100: 2F D8 D8 86 1E 51 98 B7  BB BE 87 35 19 67 97 1F  /...Q.....5.g..
0110: 70 4A 9F 85 53 F3 1C FB  FE B4 A8 D3 DE 4B 4C 9C  pJ..S.....KL.
0120: 5B 45 03 3E 42 E2 75 81  B9 F0 45 97 55 DA E2 AA  [E.>B.u...E.U...
0130: 64 79 C3 F4 51 79 7C 54  76 8D CE 90 AC 15 ED 23  dy..Qy.Tv.....#
0140: 5A E1 19 AC 08 5E 2A 21  E0 40 10 1A 38 70 0C 4E  Z...^*!@..8p.N
0150: D4 F4 00 15 D4 4A EB 00  54 4F 54 2E 52 33 67 03  ....J..TOT.R3g.
0160: C9 0F 47 24 73 EC 0E 9D  2C 67 77 C1 14 F8 B1 8D  ..G$.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..x...h.o...\.
]
]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGoTCCBImGAWIBAgIU5xPERaNNb4nMA3pFZyNFZxI3ZVowDQYJKoZIhvcNAQEL
BQAwfzELMAkGA1UEBHMCEUxPDA6BgNVBAoMM1JLZ2ZzdHJvIE5hY2l2bWFSIGRl
IElkZW50aWZpY2Fjac0zbiB5IEVzdGFkbyB0aXZpbDEyMDA1UEAwVWV0SUVD
IEhpZ2ggrR3JhZGUGQ2VydGlmawNhdGlvbiBBdXRob3JpdHkwHhcnMTAwNzIxMjIx
ODM2WhcNMjAwNzE4MjIxODM2WjCBtjELMAkGA1UEBHMCEUxPDA6BgNVBAoMM1JL
Z2ZzdHJvIE5hY2l2bWFSIGRlIElkZW50aWZpY2Fjac0zbiB5IEVzdGFkbyB0aXZp
bDEnMCA1UECwweUkV0SUVDIENlcnRpmZm1jYXRpb24gQXV0aG9yaXR5MSUwIiwYD
VQDDbXSRU5JRUMgQ2xhc3MgSSBlaWdoIEdyYWRLEIENBRkFwFwYDQVQVQVQVQVQVQV
ID1wMjkiNjEzZjEzZjEzZjEzANBgkqhkiG9w0BAQEFAAOCBgAMIICCAgEA7vmf
0qBoc89Y4awVv8M+oQAPGCUhs5zVJTeBojvJ3Hp/uxanh1um8C4xdu72S5AqDgg
nntxkEKnixiWopr0pYNOVcR1Z1Hxv5x0Ydz/rBBZfintUM97bJrbm+1M/2R4I9i
jGDLWhv0sNdCwMb/KoyDJzsHCL6p0kth1LiWgwDzywiXDTJTR2bx0G/NztmIQLS
Cvu9Lq/HDVsxJkpk5sVYNUQz8bajwLrv310gXLhcL555/gG+CzHh0kwdxbW8Vgso
ufStB9zk8DW2pccv/9iKYl3L7VPg+X8/JUGnPtv/W9DK5vd6tzzLK9z5VsQJ8Lrby
PogfjTD8cYFZdNydzn9mKe2UwAhvEetiE136nj3YzJL7DCu8y0Rt2i0WwqVG/bi
pKqzFYDLv1ws4kAw0vDLAeGzR16HbIMiGKB3AK03R1COVtbHTRWjrrqqquW4t6K
UDA2YEXbAn2vmRozjdxrK+j3o+AiNmBZB8fLuR3taIEAwEQKL7I05DI9f2zqzjR
```

iSs+B5/eR575NVWfSgZwt1o4lk5j73UmPHamtF7vcXNWF0uoUKmyc1aMjuzJEx
xSHfcJ8fFM0HCjJYa+khKdro5upJk7E0fk+XKms7v0Ah6vj3bpaDDE0zjRXbjGdA
CuG3nFAwXljU81YgFcsx00ms0FX/A2C8TvfC71MCAwEAA0B3DCB2TAPBgNVHRMB
Af8EBTADAQH/MB0GA1UdDgQWBRRenfVWGYVNmSrvUvqbxDEp80onqmTAFBgNVHSM
GDAWgBRGtehbZ5kTgo0GDG7/QkqeCY2VpjBAbgNVHR8E0TA3MDWgM6Axi9odHRw
0i8vY3JslNjlbmlLYy5nb2IucGUvYXJsL2hnY2FzXkZ2aWNLczAxLmNybDEBEGNV
HSAEPTA7MDkGFUDIAAMTAvBggR/BgEFB0cCARYjaHR0cDovL3d3dy5yZW5pZWMu
Z29iLnBlL3JlcG9zaXRvcnkW0QYJKoZIhvcNAQELBQADggIBAF4etoxHj7v9vHcd
6hKLy38MwSgryhyQDoz4NxxgIwBAK0IMUV5CYEeoPLCOTgEu0epLX817uuFYP1kb
VUPNxnwTH2VcapQtUQblUxrgYffUutTJXJEXiDkktXJvH1jjVrogWGTlw3Yt/x3s
7d+gPn55mjd9ZitVujRzC2muALoMfUwL5Xd0L+hugtFq/4j8dIWfCbYstxj7T00
1nd4tB4NaZkWdevZ2SRu5eLjns/H80385jSPy3ie0ceWLEl28GfZz2V2cicoHIT7
PvppPPwt4B01UGcvI6Wn4q2KyQNgjM1SBU1i0qGmfL9Mzd1FskToAv2Hq4R0Z
p5wp57Av/diGHLGYt7u+hZUZZ5cfcEqfhVPzHPv+tkjT3ktMnFtFAz5C4nWBufBF
1LXa4qpkcP0UXl8VHaNzpcFe0jWuEzrAheK1Hg0BAa0HAMTtT0ABXUSusAVE9U
LLIzZwPJd0ckc+w0nSxnd8EU+LGNFR53mqG2BEbqTe0J20I80I fMLtRmd2c1FS03
ZAZRkwn7Pq+FnyE50udwnxrBu8Lsu95SC3/Kv/J2ofNh0KXmkoZiTHNnuqzHTcTI
ks4AnxWA+FDdiTDmNo0gTnuNDoy+v/jhv4w3YmXMI6bLnXKWFusc14Ubjxim9z
Ofp+E4xwTJ2od6CI+W1Mb7aT8VwG
-----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:
10230884787858298599154185212641505473010571530325109987958544864074766
94076378025143202468077263446546603289575073369098066255030027359674356
67622943122894942127062585384730975749809417363802831725985621078986029
73407478474179595715207799135908913218128933138306682536344062682692189
39401484548680748837141060653941321363556770750387299724013396767347981
90884248799041102931492410749619453756259041367422108118758122588127700
89667698652072368965481908266620971666090069168651919749743637667995777
36374759309197587066094960362713476896409364641697062540625669020075126
70119661072965071668592544242321151950038351741530540846779126538595022
85642115373793623933281514615324943042864180686085514139476109265971734
46307672351412312003273495405233250482063289145119940915318631501198804
48459681620638850300877049318512322046193873648044385771467236570714109
19214728581083915399203455930307774761139330651364778517746797345838222
53996155375540472055558802633319316279491597792290228109255364421200834
25185441052590850146520782062155712568849489563590219550515942656926781
79377660078788658796875947856104674525930054187155207103158119841754120
7639797790845050615641190434559307317477790786338434351329831964465182
506720736272197442973800523
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:

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

```
[
[
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:
10230884787858298599154185212641505473010571530325109987958544864074766940763780251432024680772634465466032895750733690980662550300273596743566762294312289494212706258538473
0975749809417363802831725985621078986029734074784741795957152077991359089132181289331383066825363440626826921893940148454868074883714106065394132136356770750387299724013396
76734798190884248799041102931492410749619453756259041367422108118758122588127708096676986520723689654819882666209716660900691686519197497436376679957773637475930919758706609
49603627134760964093646416970625406256690200751267011966107296507166859254424232115195003835174153054004677912653859502285642115373793623933281514615324943042864180680085514
13947610926597173446307672351412312003273495405233250482063289145119940915318631501198804484596816206388503008770493185123220461938736480443857714672365707141091921472858108
391539920345593030774761139330651364778517746797345838222539961553755404720555588026331931627949159779229022810925536442120083425185441052590850146520782062155712568849489
5635902195505159426569267817937766007878865879687594785610467452593005418715520710315811984175412076397977908450506156411904345593073174777907863384343513298319644651825067
20736272197442973800523
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/ar1/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 ...[..I0...U..$/
0020: D7 17 A2 7E A1 62 DF 2B F6 6C 52 C6 B3 8A 1C D1 ....b.+lR.....
0030: 9E 54 D3 D8 04 0F 90 34 46 E3 48 93 3A D2 F9 A1 .T.....4F.K:....
0040: 93 E9 8A E0 AD 3B 12 08 A0 81 D1 45 9D F0 19 B2 .....E....
0050: 1A 6C 40 4F BF 51 68 73 F4 E3 19 34 D4 25 24 00 .l@0.Qhs...4.%.
0060: 7A 08 24 F5 67 13 64 A6 17 2F 00 52 B6 17 A5 1A z.$g.d../R...
0070: 7E CF 96 4F 20 1C 6E 98 FD 6E 65 CA 59 00 8C 29 ...0 .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 88 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 9E 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 18 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..8sM.....
01A0: 6E C5 6D 1B D7 03 D6 2D C0 23 DF BA 0B CE 14 C2 n.m.....-#.....
```

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

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 BFY8.....
01E0: E6 AF FB 45 2D 34 A9 BA BA 82 31 6D C1 BD 53 1A ...E-4....Im..S.
01F0: D5 FA EC 99 15 96 77 D7 C7 2E 6A 13 1B 93 27 15w...j...'

]

The certificate in PEM format:

-----BEGIN CERTIFICATE-----
MIIGiTCBHGgAwIBAgIU5xPERaNHb4nMA3pFzYNFzXt3ZVkwDQYJKoZIhvcNAQEF
BQAwdDELMAKGA1UEBHMCEUxvPDA6BgNVBAoMM1JLZ2lzdHJvIEShY2lvbmF5IGRL
IElkcW50aWZpY2Fjac0zbiB5IEVzdGFGkbyBDbAxpbnB0EnMCUGA1UEAwUkV0SUVD
IENlcnRpbZmljYXRpb24gQXV0aG9yaXR5MjB4XDEwMDcyMTIyMDc0M1oXDTIwMDcx
ODIyMDc0M1owgasXc2AjBgNVBAYTAUFMTWw0gYDQVODkDNzZwdpc3RybyB0YWNp
b25hbCBkZSBZJGVudGlmawWhY2N2s24geSBF3RhZG8gQ2l2aWwXJzAlBgNVBAASM
HUJFTKlF0yBDXj0aWZpY2F0aW9uIEF1dGhvcml0eTEaMBGGA1UEAwRUkV0SUVD
IENsYXNzIEkqOQExGTAxBGNVBAUMEFJvQzoqMjAyOTU2MTM2MjAwgGIiMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAAD6x2M2K0ECvNJCFEDr3erfUKKlGgorfTmX
zXm6lNlV7oroDXTemajXy837yNPr882M2E+og2duU30QRn1F/1U6xotJVA8gHmqw
jkaxIvdtSkBAjt7bEdVeL6u0A/tK2kFqwMYnnItwXLwLhU9b1t2Z3Ad8adTY1
UZha+p3GUikdAtRH4+bZ4TJA6sQ5S90YpH9fQk57vtasydy7ccxR6wQ59smGV21
A05iBJU/z0x0YgAV4YX95imv4Yxz1z1CHOA3LNMHNPnsdfACUSGmnTX+BjZ55FY
k5S7DR2VEkp034Ny/iMLbnH913PZzMEajZaYOYDLAgZz6+BPJjiFmAL9aXQXjm4C0
ggfD5jtYrYw9M+14fJeiR/LrRIW+9Na0d4hdmZN2Xaw9Q17/5RJIowV7fJM9bhY4
063d40FmaAXPHTSn2j9qs85LSAGJk3SHNsyepe00oupvWZLEjJmN9a0yyJspehu0
4lCa//Iy0hxBI0877zbtAKs41Lm6Dkk0Kpvtcs1xJTYLT/sEvkRSIO3G+yMU0L4n
dy2GuGqtkBuv7lS2e+d4ytHJLC7U4I2tns92fFHT6Z8CWk9t5Xa2MjwzaxXi23p
tg3N3J255Xl0d59xTM0uPrzz8FCoIp7erQt/dcQjKKB9cFMIKMJoH0vNSyVRwU
Upe4pLkYSwIDAQABo4HaMIHMA8GA1UdEwEB/wQFMAMBAf8wHQYDR00BBYEFGB
j/r3/MONpeA3eEL4gpW+IhsDIMB8GA1UdIwQYMBaAFIY0Cgqev+/fqoLE+a/87Un
3AMjMD4GA1UdHwQ3MUDWMA6AocC+GLWh0dHA6Ly9jcmwucmVuaWVjLmdvY15wZS9h
cmvY2FzZXJ2aWNLczAxLmNyDBEBGwVHSAEPTA7MDkGFUdIAAwMTAvBggRbGf
BQcCARyjaHR0cDovL3d3dy5yZW5pZWMuZ29iLnBlL3JlCG9zaXRvcnkWQYJKoZI
hvcNAQEFBQADggIBACB7UyfbXnH5Ua2V/jB5Iu04tBhb6IHT6074VWdzI0v1xei
fqfI3yv2bFLGs4oc0Z5U09gED5A0RuNLkzr5+aGT6YrggrTsSCKCB0UWd/RmyGmx
A79RaHP04x0IcUKAHO1JPVneZ5mFy8AUrYXpRp+z5ZPIBxumP1uZcpZAIwpXNHw
zTNGkXnk4/R21xdKHJfWk0E9s9epJsy4vprAtpaVehLWjZB/MLX8BsBu8NHUW
TeHhLsRHxotxBYeVcQgZG+8ghjUaiaXCgJL3cWa+b0vwxqyS1CXcb9auz7Buyf5
3eB5Pwe5LuJiy83Q8cDhgbs5/1NmhyPn55sa7688Vko6nfr4/DdhBWMp7E+En/1
yRw3HPP11ZnkPMKEIhwHlBASwg0A77Ebzw3HwrJzYduJF2e2fKogG+qU9jN4yJ0n
wdw8YajbrnV3ZMPK8By6kuE9JRswRj43LdMH/PnywB20oVNBGjs03D8X0Yxr8i0h
xCiYxok6l54jdXa9AL/GCoVinM08nyID7klVDDfpmMkTgkTzHdu+IC/6WXBsVt
G9cD1i3AI9+6C84UwoZeQMdyGLYDFhpa5X0wrKMKs76G9tU80tUbfrcwSjxUGx3b
p1k4ipGcftsZn87ov+av+0UtNKmGuoIxbCg9Uxrv+uyZFZ318cuahMbkycV
-----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:

80253179521295581167799513006800979607479798254917778002061453034823146
98425342050650998126473341946932107278444556630715186496242184307603071
90550689366985528371513507700099136358820869714295100901669591558226646
55269205001393129828618399217348632021371086744246801501807537793871739
30807956946234226124962827984262022749886110746259579944621332105247188
14821408853950783019868251860820531351854771860717933097482017163169625
53563639513847991943577789365955639943351228428527282130639785382714158
67518230090574191578644700515694150720515671751241868248391709135089662
66380286116136566899968452821258993809342624556368886044255285936094105
83517494362494454000590986415683167457065717888025807875060004863010104
13811002142547877691874257592171128596090240009085696258394819601165704
05602314156886232160119387879852262774952868683795014821067018096221823
20349217116333650595291773813762807465671195164733051810051349893947142
37457648872813371982294215685674794618789363312788663541512352900673186
41844949039950029463800190660271139580994459326995768727786979160296300
58591598748351762642937016704468197734001330564892471360057146128482768
08401722002443786833124621986932901726971532101927418283185513881641998
99347325572857722212726423

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:
80253179521295581167799513006800979607479798254917778002061453034823146984253420506509981264733419469321072784445566307151864962421843076030719055068936698552837151350770009
91363588208697142951009016695915582266465526920500139312982861839921734863202137108674424680150180753779387173930807956946234226124962827984262022749886110746259579944621332
10524718814821408853950783019868251860820531351854771860717933097482017163169625535636395138479919435777893659556399433512284285272821306397853827141586751823009057419157864
47005156941507205156717512418682483917091350896626638028611613656689996845282125899380934262455636888604425528593609410583517494362494454000590986415683167457065717888025807
875060004863010104138110021425478776918742575921711285960902400090856962583948196011657040560231601193878798522627749528686837950148210670180962218232034921711633
36505952917738137628074656711951647330518100513498939471423745764887281337198229421568567479461878936331278866354151235290067318641844949039950029463800190660271139580994459
32699576872778697916029630058591598748351762642937016704468197734001330564892471360057146128482768884017220024437868331246219869329017269715321019274182831855138816419989934
7325572857722212726423
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..\\.

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

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 8BkL.>.....
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 0Cc...L....2L.
00E0: 49 AD 85 62 42 62 78 AD 77 DF 18 7E 80 75 3A 6B I...bBx.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 08 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 2Ff=.../
0140: A1 59 A5 20 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 Ur7V[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.z.z..p.l.'t...
01B0: F2 91 B3 BA FC 66 95 20 21 BB 66 7F 08 34 75 F2f. !.f..4u.
01C0: A9 CB B3 D2 72 9E F1 24 F1 2B CC FE D8 CB 54 9Fr.\$+....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 F0y.....
01F0: BC E2 0C 74 37 F9 83 37 C9 5B B6 89 15 0D 6D DF ...t.7..7.[....m.

1
The certificate in PEM format:

-----BEGIN CERTIFICATE-----
MIIFF3zCCA8egAwIBAgIU5xPERaNbn4nMA3pFZYNFZxI3ZVgWdQYJKoZIhvcNAQEL
BQAwfzELMAkGA1UEBHMCEUxwPDABGgNBVAoMM1JLZ2ZhdHJvIE5hS2lvbmfSIGRL
IElkZW50aWZpY2Fjac0zbiB5IEVzdGFkbYBDAxZpbDEyMDA0MDEyMDEyMDEyMDEy
IEhpZ2ggR3JhZGUgQ2VydGlmYWwHdGlvb1BBdXRob3JpdHkwHhcnMTAwNzIxMjEj
MjAxXwhcNmZAwNzE2MjEjEYmJAxwJb/MQswCQYDVQGEwJQRTE8MDoGA1UECgwzUmVn
aXN0cm8tMjFjYW9uYm9uYm9uYm9uYm9uYm9uYm9uYm9uYm9uYm9uYm9uYm9uYm9u
MTIwMAYDVQQDDClSRU5JRUMgSGlnaCBHcmFkZSB0ZXJ0aWZpY2F0aW9uIEFIdGhv
cm0leTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgocGgIBAMS3VfV1mCmYroK
RWIz3fth6awRo4LVHMJMjwPR43FN0DErnOq2qzbCjP3BLR1bCsRjC53Yr6qKU4f6
cPMXF4NAKTN0LTX0zviuvqLtk3iWQXijSweHA60yXtrZhsImnIXTpuC9nTOjB9vml
+cGuilrXASqZ2UGaJ7INPFnqhtFRHJPD12LD1Mb0si/vol++EgWPb+3YBSpIDJ5
58siUa9vcIgjWBU/Ha48yjKma/vGkBI502nG+QzECQVK2iowVgKDKsv7gJ6Irrlg
fLQjWohjDL4MXptRTh+4HuhfCZHtdXtc04jV0WaGw0i5CfoK1VMgs0jZ+a2kLld
/L81TznLuq4tKNVctDnYxQ1QHxerIjUG/X92T0V5ND0ibvj2Gt4puY92Iw5QJ4d7
YNX/9PtB0bAP8noHxkKwQ6UiXoF0ART0jOCQRE9ed167MtD+ppSrhac4zphE5
IMTE5KEhtG58R6apxmL4SKJTHvX489G2Z04uniWPHd1XGpxDzunv1vbcnttIue
Hdm10Yd/YfgAhIgxEBvIqsquMcwDbr0eLJ8klte80Hv3TiulzAmtc4SoJx94GR5mT
rGvQrKJXdYeEQzHIw1/TSg2kU0r6V+dCLljE9PkaRdgcNv80b1rPoq2bhNKLk
bQVMD5bc7MrELkaPRTvYdYvKdAXAgMBAAGjUzBRM8GA1UdEwEB/wQFMAMBAf8w
HQYDVR0BBYEFaE16FtnmR0CjQYmV9CSp4jZwmMB8GA1UdIwQYMBAAFE16Ftn
mR0CjQYmV9CSp4jZwmMA0GCSqGSIb3DQEBCwUAA4ICAQBwiFVQrXVe9sxzNmxxz
aUSzb0jmwMRJL2/vx0S39fjS+Spn+6nq2cfn9LoFcZY8x61k1s9Um5zGH95rFL83
E4Mni2c8f74jZx1qEr5c+r9cBGU2h7c/wn6K3JRu1HMkD2adibxcFAIMh3DHVMa
bHgnWuWubN03hj0jn0T5Kw5bbDdqf+3ZB4w1NbfVagrpqDZ06I9m2xzgn9l0jr
XASLnABFjJprb00+80nbzIQd1wyVkiVM36U90uHM/UbpEyhtS0Em+o6Lw08Dkn44
K/KomHvsLmPb531M/4rHAzJmDEmthWJCynitd98YfoB10muKtrVeiH9bj0RPPwA
f1QYUixYtuZGRSuyRedZuptZ0cAggPU2U0necijzJdFw04ytBbtmHwZeUtdNC4iY
BjVWkfgK8B0AwQ/zZj32c/d/L6FzP5202tE9bXVUbyCYPVzDac4N5BLS6LHckfZ
/vw8C244vbrEA9YBkm6C5HuicLVyP1ZbaB/9o945KLFo3mZVMGgyZKXuFlpkzoA6
EaPcgmRLCARY5su06koB0pDYwvR43jK6eg22cKAX1Cd0ywrYkb06/GaVICG7Zn8I
NHXyqcuz0nKe85TXK8z+2MtUn1d/vkwZw0MwF3dSqa82LcM1r3omrmjXnkfXvG
e5Dw0IMdDf5gzfJW7aJfDbt3w==
-----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:
71162538624742581163159203713803781354467293474045239650255378454937180
29957652612977264618826015390989243914546542664015416859966207365836565
60283323503306982397685985141078450139967363670256889913475311275841141
3154995420256464912189613995457005804525320919199826430627237180795308
05543816712315607638085615864011232857709504986526501727755865333413628
62644256015853851421756269421779766564715872495761393402301043017012745
10025989639819355208012031002473522067536355140584624719055002138625329
55673226654905696343486661779371823937223695994122029899436969001479917
10983843546917433391153675585317478265029656483762050141286740694792324
25630569102960315253145276010504468941562855485194908859066235956020764
97709566623678590495686002784683823587733718129969788836285766363287957
76924633143060999385961318750417551705212132654716175258706266780065143
02604077899804514141057745389347145666047358344921489506816797469083236
62945279409057218861872008860421675953993006530276489790258040901645447
83301936945405305858519885493489593000533207009256268353678884221105238
53117988489543000178543292425201473490672762286118998117896736866320148
65145268994015219316921483693002368182113224428979127866578494381624813
71623436156230215774607971
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:
7116253862474258116315920371380378135446729347404523965025537845493718029957652612977264618826015390989243914546542664015416859966207365836565028332350330698239768598514107
84501399673636702568899134753112758411413154999542025646491218961399545700580452532091919982643062723718079530805543816712315607638085615864011232857709504986526501727755865
3334136286264425601585385142175626942177976656471587249576139340230104301701274510025989639819355208012031002473522067536355140584624719055002138625329567322665490569634348
66617793718239372236959941220298994369690014799171098384354691743339115367558531747826502965648376205014128674069479232425630569102960315253145276010504468941562855485194908
85906623595602076497709566623678590495686002784683823587733718129969788836285766363287957769246331430609993859613187504175517052121326547161752587062667800651430260407789980
45141410577453893471456660473583449214895068167974690832366294527940905721886187200886042167595399300653027648979025804090164544783301936945405305858519885493489593000533207
00925626835367888422110523853117988489543000178543292425201473490672762286118998117896736866320148651452689940152193169214836930023681821132244289791278665784943816248137162
3436156230215774607971
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 620Kb
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.Jq.....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 40 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.i.R.)..o.5.j...
00E0: DA 4A 38 EE 53 0A 0E 67 BA 25 8A 4E 08 0F 18 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.....E4M5Q
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...04a....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!..
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*.9dH!
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-00BP.8....

1
The certificate in PEM format:

-----BEGIN CERTIFICATE-----
MIIFFyTCCA7GgAwIBAgIU5xPERaNnb4nMA3pFZYNFZxI3ZVcWdQYJKoZIhvcNAQEF
BQAwDELMAkGA1UEBHMCEUExPDA6BgNVBAAoMmM1JzZzZDhJvIE5hY2l2bWVfS1GR1
IElkZW50aWZpY2Fjac0zbiB5IEVzdGFkbyBDbAaXZpbDk0ZDk0ZDk0ZDk0ZDk0ZDk0
IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MjEzZDhJvIE5hY2l2bWVfS1GR1IElkZW50aWZpY2Fjac0zbiB5IEVzdGFkbyBDbAaXZpbDk0ZDk0ZDk0ZDk0ZDk0ZDk0
IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MjEzZDhJvIE5hY2l2bWVfS1GR1IElkZW50aWZpY2Fjac0zbiB5IEVzdGFkbyBDbAaXZpbDk0ZDk0ZDk0ZDk0ZDk0ZDk0
AA0CAg8AMIIICGKCAgEArm7mdj6EvmHqzCIZuL9qIDYzj7wYq4hjDFJM5o+yDu6I
36pn46Go3BBaDeFndRR9uFFyKcZbLuAc7TdWRYbqcn74qYfjKEorzmaC2+5pH8q
NX6A0rjVGNMmHRZEWCa1A8Q1a0Q6vx4XhSdNi4ps7eaV52H0QNeaRMHnG0n+kpD
Cwuz4i3rmrJ7YNN0oEc+RhiHMIdz2ceZ8Njhm49QhFIh5rCR1zMBnExhHjlixkjj
DaMtnaV8ZNA7+xBsdVEUEaeQeTvNaA5FZVNAyhE8WeyLDmRuzfKmiI7Ng4Mej3L0
cnOPH+hE5mspY0hcCjYZwVaBp54cSErtkK8V58R0tLm4GPPba9K4uq7erThYgGN
0Sg8NDkac0o88ITVMgakyVwaX12XfSdK9v/FK1/4GUsMURQImSgMe9gP3zKqb60G
n+9WYznf+w3Q98s10145f2MdPLk5mm7hd3CtUz4kfrGtZd2YqT0QZwahnLf49Da
ppLm8Hksju8LHdVh+tiJtiuuNGk1hvEJZxoQoJfIwDSUDKHUYiBI7LYCZazGsZ8
Zdgn5bIZ0aMe/EoJYM8sKmPuFwa+AhnzU6dzULxHovtbOpdMiveMIg+fGuo9tP0
YqW5jALtP1KKEKPLuSn6oG9gc8nhd8uic9PBjRjxumUhsMbhE0RFxfRjyEsdmMC
AwEAaNTMFEwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUUSjLQIap6/79+qgsT
5r/zT5fcAyMwHwYDVR0rjBBgwFoAUSjLQIap6/79+qgsT5r/zT5fcAyMwDQYJKoZI
hvcNAQEFBQADggIBAFMHESJ8ev5+e57CWT09j2um9mnnbb3WpbmEkL3n81LU1eWv
/pcpt5oNFwv+FTBLNm376n1ry2HUjQbtXzhhDn810XKXhrDnN3FawSewaVgE7v
u66VvS2l1lqhx/v3Ynq3WShYm2g5305k9E5v5064sWiSti1TT726Rh7+uLxbnoao2
2K0Lu4CEbuH8f8kQfYewiCglZ5c0KncYwe91YtRE493JmZ/xHyAUihpNmXm9AeKP
PxSk0Epb3f1/StPwjVTVRg0YpqJegBZogjMP6mccct9pUgwp1G/8NdFqLgXK2ko4
7LMkdme6jYp0CA8b118Lb/jKN/dL2+b/0WdDvAofKAs05i7b1cUSLU0TSRRMnCU
I+JXq5Q5b+6aXadZ:IhLs1/GEPLQ00qLNVqyURXXP7CkxGQJPNNGN5bKQVQXoJZnu
pUNRshKml0Lk1i0MrneIhZh28HnwPIRMLC9EFhT6nwD8Pm0g0UeIHeBYuF69LBF
juPLrJ5QxajjU8HKovDs6LZrc7ho1Rhzb1ROIFz2XCjWrcs4Kq0rDPQIZM7kuPe
rzvS1hyFW4no8XsyVuAT6mqspySg/dJC7r9ThzVuH9zcxLcV0QdCKsCs5EhsDkiC
sZdZefjF7kd7MZvMay6LEFT28QSE5fwi9tJkz6PSVU1cS1EMEJQxziyGy7M
-----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
3722510680529605497478751656927884273316159491149
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:
30337547528942006267353543430178699897514218074033697247936474690038342990680507244540891693339684538933839092722338869245347043731428441933862212065847583478137157522135576
08558696522661027271216627152723787312170757488970857585992407208364397123782114519960030934622041459973057104937613127223195776527840685808772815793796035756419165647035983
16511460864630553598949007755463127135415413336751950302418700965620521525982583173671688091596924886172574758261147892268311188427746173841928827847762889225140261082919515
86624047524189894965577342561769319592278459469483722510680529605497478751656927884273316159491149
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...

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

```
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/wcidpgbcal.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 7F 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/wcidpgbcal.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....>6K
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.7mM.j6o..
0040: 28 56 3D FC 6A 3C D3 DB 9E E5 E3 2D 52 DD C0 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 J0U...`f+[.....
00F0: D4 17 99 73 51 D1 05 5B CC AA EA 4F CA 8B CA 4F ...sQ...[...0...0]
```

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIeGtCCA2mgAwIBAgIICyut7LnH+rkwDQYJKoZIhvcNAQELBQAwSjELMAKGA1UE
BhMC09gxEADA0BgnVBA0TB1dJU2VlZXkxKTAnBgNVBAMTIFdJU2VlZXkgQ2VydGlm
eUUEiFBvbG1jeSBHQiBDQSAxMB4XDTE1MDUyZjE1MjIwNFoXDTM5MTIwMTE1MTA5
MwovTDElMAKGA1UEBhMC09gxEADA0BgnVBA0MB1dJU2VlZXkxKTAnBgNVBAMTIFdJU2Vl
ZXkgQ2VydGlmUUEiEFkdmFuY2VkIEEiEiENBIDIwggEiMA0GCSCqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQDwUdXB1k9z1Zo0+cuD72DSfubC02ybUHYvmX2Uo2aF
cGkpbHt1v3CTE7E8iCkPjFV9TdAnFuQM4sKaY2XiERG9/TEsxzcqSsnPzcz5/S
lj8MtqV1biTUN9d7jtVZQrSpxXAGzfKRaIwR0B0EBCQbkwMo0bXwDpkvJ8Yyqvp/
D3Cw9vX/3cuqBs2L7Mdu0thRB97+HEE26H+zobQ0USfUwL0TFXQHYg+gc/dpXdA+
mtq1yFgW1LQurrLDIdodZsIszwbGx98brm7cENP7e/68wyZCndpzTDVg0B88LiA
VHVH12b8b0mA5uAghsRtQkrJppMv1QT+9w1RBse6JwxNagMBAAGjggFnMIIByzBv
BggrBgEFBQcBAQRjMGEwOAYIKwYBBQUHMAKGLGH0dHA6Ly9wdWJsawMud2l2ZwTl
eS5jb20vY3J0L3djaWRwZ2ZjYUeY3J0MCCGCCsGAQUFBzABhh1odHRwOi8vb2Nz
cDUud2l2ZwTleS5jb20vY3J0L3djaWRwZ2ZjYUeY3J0MCCGCCsGAQUFBzABh1odHRw
BgNVHRMBAF8ECDAGAQH/AgEAMB8GA1UdIwQYMBaFAFNHmC4I1dCUsvZHVAxh7v8Hu
```

```
rx2AME0GA1UdIARGMQw0gYHYIV0BQ4HAzAvMC0GCCsGAQUFBwIBFIFodHRwOi8v
d3d3Lndpc2VrZXkuY29tL3JlLm9zZXkuY29tL2NybC93Y2lkGdiY2ExLmNy
MKAUhixodHRwOi8vcHVibG1jLndpc2VrZXkuY29tL2NybC93Y2lkGdiY2ExLmNy
bDA0BGNVHQ8BAF8EBAMCAYYwDQYJKoZIhvcNAQELBQADggEBAEu7V5Ijacp3unZ9
5qs+JktPDPjrUeQLNfidApMntwWITCYqQndQbulGuuOLFizSZPJZH90a+I3bk3Q
ajZvLhAoVj38ajzT25714y1S3dwJwxfcH0gSsa7+kCvCsOTI00BxydEamoyajh9
N35jzPzXlXKSwdUMitS/nwgbTVkv19K/Gjhi2zvbsivYHqi40Lrwg0NHb03Gx+A
FKCSxa3TG6QMozTjaCXFaB7c/yuSQLfwJm99Q1tjKzqB+HhZLoK6bwYUz1qyLU
Xhq6Lna0Q1FhGKFF1Q/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
3268614117498340521035744826143191446276694961161
public exponent: 65537

Subject key identifier f4e49b57d2aec29e884d00ba2baf65c963a9879b
CRL distribution points http://public.wisekey.com/crl/owrggaca.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:
22998960246314316614078373118493787911621436538469497722422881644910586294734124398115144153940706407692456638802072785203364072662407565285466837841235654358940952643584857
67708422033796446874513532645901735851550813182005306101215239161980530078651212014153700944199691310617173391614325596304477884726988185991654970457104161303022408796903823
45461329885588968448680719908527209845980625731237879035473503970231639929277231979496835177592521971792358563218084421336577681844782938361284853870016086614640653275371839
85926072363901893135323861528084639982008055060493268614117498340521035744826143191446276694961161
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

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

```
[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/owrgaca.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/owrgaca.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...#[.f0.....
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 \)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 B0 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:

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

```
-----BEGIN CERTIFICATE-----
MIIFNDCCBBYgAwIBAgIKOfs4FwAAAAADTANBgkqhkiG9w0BAQsFADCBijELMAKGA
A1UEBHMCOBgxEDA0BgNVBAoTB1dJU2VLZkxkGzAZBgNVBAsTEkNvcHlyaWdodCAo
YykgMjAwNTE1MCAgA1UECXMZT0LTVEUgRm91bmRhdGlvb1BFbmcvbnNLZDE0MUYG
A1UEAAMT0LTVEUgV0LTZUtlESBHBG91Ym91bW90Ym90Ym90Ym90Ym90Ym90Ym90
NjUzZjRlZjRlZjRlZjRlZjRlZjRlZjRlZjRlZjRlZjRlZjRlZjRlZjRlZjRlZjRl
V0LTZUtlEEmCQGA1UECjM2Q29wZXJpZ2h0IChjKSAyMDE2IFdJU2VLZkxkG9Ex
FjAUBGNVBA5TDU1udG9ybmF0aW9uYm90Ym90Ym90Ym90Ym90Ym90Ym90Ym90Ym90
eULEIEFkdmlFyZVklFNlcnZpY2VzIENBIDQwggEiMA0GCsqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQC2L9X7Ban4aQ6ilphaaAFK5SCf+bnLfsdJdJzOYGexsY7ZiDiU
SyU6bx8u7AZ9InzYm/0AQ2+Ufxht0+hRPMYF60zbIEEz8jF7+RFiZauM8Tu6GR+
t2+MEDVfzCRCiBvM61CLusHQ60bJbtzqNweezKpXBW5f8e0Gwfmf05HtLw0m0050I
mk7I6+XYhRUruVwS1U8kQom1qXp860o5S+eRqZAFiXB2h10A94wdrosHwL3vCLBX
RF7pa+gK5j7bB5F9w4bWVX/a41J+Y8WihlanLVASRkzht5Jf+cRBC0hppjt57uBv
OnpX9ITHdV6KpwiB27ycmYORXDJEab6FFWwJAqMBAAGjggGQMIIBjDA0BgNVHQ8B
Af8EBAMCAQYwEAYJKwYBAGCjNBAMCAQAwHQYDVR00BBYEFPTkm1f5rsKeiE0A
uuivZcljqYeBME4GA1UdIARHMEUwOwYIYV0BQ4EAwEwLzAtBggrBgEFBQcCARYh
aHR0cDovL3d3dy53aXNLa2V5LmNvbS5yZXVzL2l0b3J3MAYGBGFUeIAAwGQYJKwYB
BAGCjNBAMCAQYwEAYJKwYBAGCjNBAMCAQAwHQYDVR00BAQwBAGwBgEB/wIBADAfBgNVHSMC
GDAGBSzA36uNrywedHclCa2Eb4hsmmGLDA7BgNVHR8ENDAYMDClqAshipodHRw
O18vcHViLjLndpc2VrZXkuY292L2Nybc9vd2dyZ2FjY5YjcmwBAYIKwYBBQUH
AQEEYDBEMCQGCSsGAQUFBzABhhodHRwO18vb2Nzcc53aXNLa2V5LmNvbS5wNgYI
KwYBBQUHMAKGkqhkiG9w0BAQsFAA0CAQEAZCcx6V5Bw+3JeiwtMINKtmzjHomn8jw5xm
TxydkPzpxbhlqx4bc3pbT7oxQ0ZSYRQbCLpu0713id9yy/fuFPT8jYnLU3GA2
jKiDISQ30LvnIdMxstUz/nWzH4M9iW6p27qN+RWB5ypLQT rvCFyUNg5P1vwTMP
34Ri1yvw8XvVdr3o5FjOm+pNeJgx9+iuwQbPvp7gKYVURLDKp/+qTrclWtRHx01y
HP7B+0QyKcZ+0BBkgHfT+3L1Jb0SaQzZa3+mNJdD0dEQauFwuHQ0M8D5ytxQ70Y
ISHgrJwe50m1deYpK61if6c3dTzpb0nhZtDBsrEGxbDjvquSYYPU2g==
-----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
<i>Service digital identity (X509)</i>	
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 3279475487464259551106530560220272067630486843259 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:
24288478345426820300170647212650028183209172240700549408406936117107702748038509701626393019879313050641203308775566378367707614411599448000580006742234127564729157806272833
87892577498376295817882602457423385571104485143075295810767512205054756703355012080263290884190851633060555966707107256996505788105039037018831615858096998713437400310144168
97973542516413296476970768525294161764162278363174487117866772958700346310703729205374924949840804717547954739831453388178138501238141493937506601607971993728615571421253331
08142183012604557930417470818667026814359533805253279475487464259551106530560220272067630486843259
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/wcidaglca.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 68 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/wcidaglca.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 \.....x.....
```

```

0030: 6C CC C1 14 D6 75 6C DC 0C 43 B8 2E A9 7B 37 7D 1....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 58 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 68 51 62 09 66 99 ....b.....k0b.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;..
    
```

1

The certificate in PEM format:

```

-----BEGIN CERTIFICATE-----
MIIFCTCCA/GgAwIBAgIKNBgY9wAAAAAAGjANBgkqhkiG9w0BAQUFADCBijELMAKGA
A1UEBHMCM09xEDA0BgNVBAoTB1dJU2VLZkxkXjAKBgNVBAsTHUNvchlyaWdodCAo
YkkgMjAwNSBXSVNLS2V5IFNBMRyYwFAYDQVQLW1dnR1c2V5LWVmbmF5MSkYwJWY
VQ0EYXBXSVNLS2V5IENlcnRpbzNlJRCBBZHhbmNlZCBHM5BDQTAeFw0xMjAyMjE
NTMzMzJaFw0yMDEyMTEwMDAwNDdaMIGOMQswCQYDVQQGEJDSDEQMA4GA1UEChMH
V0lTZUtleTEtMCAGA1UECwwMZQ029weXJpZ2h0IDVhMTEgV0lTZUtleSBTQTEwMBQ
A1UECwwNSW50ZkxkXjYXRpb25hbDExMCA1UEAxMoV0lTZUtleSBBDXJ0awZ5SU0g
QWR2Ym5jZW0gU2VydmlkZkxMg0EgMjYwMjYwMjYwMjYwMjYwMjYwMjYwMjYwMjY
A0CGgEBAMBm3QJR+dIYJ/RKHG5W1vmOKYihHp6dcCLZ26FjcnTx/gArnGaJfB3/
JbC6wbT1pcD5eyeVAgp8Xss00C0Xr6EAhFe+M47JLgNRessR31PV05EaalBIuM55
Z1fcEZ/AhtwtZ+KtJdp59F10PL9uYcZSsIFB5eLJy5TLK6rJM6cD8QBeDw98rH
2gY0Q0X1JKGAn2LRV1Tr00PAkZ51fLQ8y9Eb7XaWRc4cywjkB0Tw1840DQH8bQ
ToIE3+U62bsUSFg4pKIaouxhyozNyBKHVpXz0MKiB+/QVpBwykEIRe/Mb7C/rATw
VsMqNKQFdw1bafxKFNUz7eJSX/873sCAwEAAoCAWkggFLMBIGA1UdEwEB/wQI
MAYBAf8CAQAwHQYDVRR0BBEYFNcVl/MJ8VYHUX3nTC5IRErahv2YMAsgA1UdDwQE
AwIBhjAQBgrkBgEEAYI3FQEEAwIBADBOBgNVHSAERzBFMDsGCCFDAAUOBAMBMC8w
LQYIKwYBBQUHAgEWIWh0dHA6Ly93d3cuZm90Lm9uZC51d2l2ZWtLeS5jb20vcmluZ3NpdG9yeTAG
BgRVHSAAMBkGCSsGAQQBjZjUAgQMHgoAUwB1AGIAQwBBMB8GA1UdIwQYMBaAFFAf
MMTKo1XiZg0XLK9tMr64FFMDwGA1UdHwQIMDMwMmAvO2C2Gk2h0dHA6Ly9wdWJs
aWwud2l2ZWtLeS5jb20vcmluZ3NpdG9yeS5jcmwRwYIKwYBBQUHAQE0zA5
MDcGCCsGAQUFBzACCh1tdHRw0i8vchVibGljLndpc2VrZXkuY29tL2Nydc93Y2lk
YwcyY2EuY3J0MA0GCsGqS1b3DQEBBQAA4IBAQUdQd60MkqXFLyCsBR414TqBzm
wwIm+3mhKtuqqF35tWwYggu563j4BsudghXH9sVsZMEU1nVs3AxDuC6pezd9MhB0
2NPjLlv3S5Es8EghjfuCwskc5ykeXNZWRkAZDUBGmVeo79d75gZpjLjCG8qFLou
bTC3YKSMa0nhGfgIGATjAN8fLQA1tF611twFJX1gdioDoup95cp5PwRJhg4j1Q
gU7SKYPmB0zSUVtXMRPv8ZiE028FONrUWIJZpnpHs+tuQdcr8qjnlqnhN7FpEF0
LaoayrFrWVM0aMgcEjW1Gy7AbAdmkSx17ejnG6fW1KX9v1U2Q2oE1poLdDsK
-----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 86718877871133159090080555911823548314
 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:
 25665677062212238926425337868672790984523975826397568772898393679835223
 79215361472476274067860436714640896498866776555724303333217881199443031
 82192680137227811038941771642754716527908915047671263165545439491678726
 58969863516618824989331325931780164035733540663902032602128347596286518
 56658415161131716185399495955856037164448949398527620054287213549952490
 62661015705941843504398253766005943340412105516353562678765502195260798
 84846250242014323238477351950638683648063570726696890119634093256994831
 49551493065058583484332173198815090149983980763171935736798366921816346
 1065125420004275703859743682152491140031902515461
 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
21731988150901499839807631719357367983669218163461065125420004275703859743682152491140031902515461
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.....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.....60.....
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 90 74 C5 47 :AO[G.....t.G
0050: C6 3B 6A 0F AC 14 DB 3C F4 73 9C A9 05 DF 00 DC .;]....<.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-----
MIID8TCCAvmgAwIBAgIQQT1yx/RrH4FDffHsKFTfmjANBgkqhkiG9w0BAQUFADCB
ijELMAKGA1UEBHMCC0gxeDA0BgNVBAoTB1dJU2VLZkxkGzAZBgNVBAStEKVncHly
awdodCAoYyYkMjAwNTEiMCAgA1UECXMZT0lTVEUgRm91bmlRhdGlvbiBFbmlRvcnNl
ZDEoMCMYGA1UEAxMFT0lTVEUgV0lTZUtEzSBHbG91YWwgUm9vdCBHQSBDOQAeFw0w
NTEyMTEyMjUyMTEyMTEyMTEyMTEyMTEyMTEyMTEyMTEyMTEyMTEyMTEyMTEyMTEy
A1UECmHV0lTZUtLEtEbmBkGA1UECXMzQ29weXJpZ2h0IChjKSAyMDA1MSIwIAAY
VQQLExlPSVNURSBDb3VzZGF0aW9uIEVlVzG9yZ2VkM5GwJgYDVQDEx9PSVNURSBx
SVNLS2V5IEdsb2JhbCBSc290IEdlbIElENBmlIIBIjANBgkqhkiG9w0BAQFAAQ8A
MIIBCgKCAQEAy0+zAJ59Nt350U1qaxB3H+zYK7LG+DKBKU0VTJoZiYEVrd7jyBxR
Vvuuk+g3/ytr6dTqvi.rdqFEr12bDYVxgAsj1znJ707jyTmUms2kahnBAbtzptf2
w93NvKSLtZlhuAGi9RN1AU9ka34tAhxZK9R8RxfvDbD50kc3vkDIzh2TbhmYsF
```

mQvtRTEJysIA2/dyoJaqLYfQjse2YXmNdmaM3Bu0Y6Kff5MTMPGhJ9vZ/yxViJGg
4EBHsChWjBgb16S0id3gF27nKu+P0QoxhILYQBRJLnpB5Kf+42TMwVlxSywhp1t9
4B3RLoGbw9ho972W6GxwsRYUC9tguSYBBQIDAQABo1EwTzALBgNVHQ8EBAMCAYYw
DwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUsWn+rja8sHnR3JQmthG+IbJphpQw
EAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEFBQADggEBAEuh/wuHbrP5wU0x
SPMowB0uyQ1B+pQAHKSkq0LPjz0e701vvbyk9vImMMkQyh2I+3QZH4FvbBsUfk2
ftv1TDI6QU9bR8/oCy22xBmdMVHxjtd6wU2zz0c5ypBd8A3HR4+vg1YFkCEXh8
vPtNsCBtQ7tgMhpnM1zFmdH4LTLSc/uMqpcLXHLZCB6rTjzjgTGFa6b7wP4piFXa
hNVQA7bihK0mNqoR0gHhGEvWRGizPFLTDISzRpFGLgC3gCy24eMQ4tu5yiPAZZi
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
5080353582058387016955678231307621269112715452961
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:
173819564184728976939695085821626360240716593460322692633829207398421504692785258372162917714106758571166981520598101663018631820931731409654107720087605003458793700292047194169818313172767256880241716377274896565132685789623174772135269624628148347999166048564205641884831477293260126888705031728993336341321083681414458890830680761955133206859315193891324046887022413555455855897507018984996629041020918774445528628794543541140874770243390812773050671663698501311923756685240238851034620721633799334153281921718809769061541848791636830356107529222528478476284885635080353582058387016955678231307621269112715452961
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.....0.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 ....[j r...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.....B#.K.
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 ..0.4n.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-----
MIIErzCCA5egAwIBAgIRA0AjyxUSg10JrWfueLRnayeWdQYJKoZIhvcNAQELBQAw
bzELMAkGA1UEBhMCU0uFDASBgNVBAoTC0FkZFRydXN0IEFMSYwJAYDVOQLEx1B
ZGRUcnVzdCBFeHRlcm5hbnCBUVFAGTmV0d29yazE1MCAgA1UEAxMZQRkVHJlL3Qg
RXh0ZXJyYUwqO0EgUm9vdDhEw0xNDEyMjYwMDAwMDA1MzAxMDQ0Mzha
MIGBMQswCQYDVQQGEwJH0jEjEBAQgA1UECBMSR3JlYXRlciBhYXN0eG9yZGVyMRAw
DgYDVQQHEwdTYWxmb3JkMR0wGAYDVQQKExF0T01PRE8gO0EgTG1taXRlZDFBMD8G
A1UEAxM0Q09NTR0RPFNIQSOyNTYgO2xpZW50IEF1dGh1bnRyP2F0aW9uIGFvZCBT
ZW50IENyZXR1b3V0EwggEiMA0GCSCqGSIs3DQEBAAQAA1BDwAwggEKAoIBAQCJ
S03aeLMZTnBShBxWpgYmt7hJ4JbnUavx8FoTSRwjT1wYlX6UUKneYykIt8XYU6R
1XyJChTTSGj/th0JgG61BD3ZursW/qGhG55DUKMFk8YUMimT1rpCNjPkyWce4jo
MGTMpPhWgP0qJBQzF5msR0Vpi6NGBkvCM9Tp0J8GSgk0C5t0iToPwqU6MQ2z0g
YTxVA47ZTnYLAiEp+qN8cXZP7ufgen7VIDbw3s1UreE3iI9LDAtMX9ZvVI3sDNp
LUPr+ta18Zd3Z1GM2e4n67yLBzh2jKSpOP/fjPUDrEm+yvdzmToPMquclToTPQ5G
01d0YVC+xA/y+Ti6InHAgMBAAGjggEXMIIIEBEzAFBgNVHSMGDAwG8BStvZh6NLQm
9/rEJlTvA73gJMtUGjAdBgnVHQ4EFgQUkMFRguG1oKpP7fXwqP3tIAAwewWdgYD
VR0PAQH/BAQDAggGMBIGA1UdEwEB/wIIMAYBAf8CAQAwH0YDVRR0LBBYwFAYIKwYB
BQUHAWIGCCsGAQUFBwMEMBECA1UdIAQKMAgwBgYEVR0gADBEAgNVHR8EPTA7MDmg
N6A1hjNodHRwO18vY3JsLnVzZXJ0cnVzdC5jb20vQRkVHJlL3QgRFRkZDFBMD8G
Um9vdC5jcmwvNQYIKwYBBQUHAQEKAAnMCUGCCsGAQUFBzABhhLodHRwOi8vb2Nz
cS51c2VydHJlL3QgYUwqO0EgUm9vdDhEw0xNDEyMjYwMDAwMDA1MzAxMDQ0Mzha
Vf0qa2ErwAKQI5kPxwZqB7H1tLV3Xg8CYQDffQX+Er0kgIAA/Psdw2pyAgpBvAW6
wVjVjS1u2E+/6CmM9YG+M1Y5xS+LsFNqt9WKxeqztj5drVc+/s4Pt74qP/8Eij
nMq2jU0+5EYA7KoLdTYu0JLkGmFNumNToe+ABEKwcyjrHn0+ING6KZdAairup
3MrkNtH0/MJkKtWv1rGncRHSA00xjz6a7J4yU/R2ksqGNAe5LmrmHerYmQ3BhuKQ
kvtaQmojIRDPzCf11bt+6oyFIAJi6tE6ByxZxZkz8ji55bbpFnoFeRT2ShAaJvp8
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
<i>Service digital identity (X509)</i>	
Version	3
Serial number	43390818032842818540635488309124489234
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
3815810044366927828104368429473637812056461354743
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:
26289395806318381231692261863750242292037560230101026221289605413810223123911371296433478418980467635690027557786662605587500663810030355156860038214524665629429491183904761
65980434059578530740350846597719524414645025834261978506232725617226958412711772065601599345090517683404610010953270431696513519356433527274923661810035291369082738108001201526306613
52630661339792683744834685477466252935847104367829705960299566072962573971128784882967787982428230779760446716641280620338315837331971847648098659786131359724660931636746496
04238245904200630728151797566966978950876822107093815810044366927828104368429473637812056461354743
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 dddfelc7 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 62V.
]
]

[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.....!0ur
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 1A3.7...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 7AF....4"...z
00C0: AD B7 B2 A4 9A 33 88 71 02 3C 2E D6 7A B2 1F A23.q.<..z...
00D0: CA C0 DD 2F 10 94 FD B3 8C 84 20 79 46 05 05 D4 .../..... yF...
00E0: 10 E4 D2 DB 64 4F B8 5B EE 1B C5 20 47 5B 94 ABd0.[... 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-----
MIID0DCCArigAwIBAgIQIKTEf93f4cdTYwciHdgEjANBgkqhkiG9w0BAQUFADCB
gTELMakGA1UEBHMCR0IxGzAZBgNVBAGTEkdyZWZ0ZXIgdWVWY2hlc3RlcjEQMA4G
A1UEBxMHU2FzZm9yZDEaMBGGA1UEChMRQ09NT0RPIENBIExpbWl0ZW0xJzALBgNV
BAMTHkNPTU9ETyBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAeFw0xMTA5MDUwMDAw
MDEBaFw0zMDUyMzE1MzU5NTU1aMIGBMQswCQYDVQ0EJHJ0EjEbmBkGA1UECmSR3Jl
YXRlcjBNYW5jaGVzZdGVyYRAwDgYDVQ0HEwdTYWxmb3JkMR0wGAYDVQQKExFDT01P
RE8gQ0EgTG1taXRlZDEncmUGA1UEAxMeQ09NT0RPIENlcnRpZmZlYXRpb24gQ0XV0
aG9yaXR5MIIIBIjANBgkqhkiG9w0BAQEFAAQCAQ8AMIIBCgKAQEA0ECLi3LjkRv3
UcEbvASy06m/weakXtUuH+7uIzg3jLz8GLvC1KVCZrts7oVewdFFxe1CkU1B/qnI
2GqGd0S7WwaXUF601CxmRM/aN5VCaTwwxHGzUvAhTaHYujl8HJ6jJJ3ygaYqhZ8
Q5sVw7euNjH+1GImGEaaP+vB+fgQV+useg2L23IwambV4EajcNxo2f8ESI133rXp
+2dtQem80b0y2WIC8bG0Pw43n0Iv4t0iJovGuFVDi0EjPqXSJD1qR6sA1KGzqSX+
DT+nHbrTUcELpNqs009VUCQFZUaTNE8tj a3G1CEZ0o7KBWFxB3NH5YoZEr0ETc50
nKVIrLsm9wIDAQAB0IwQDAAdBgNVHQ4EFgQUCljli8ZMFTekQKkw5G+RzZaVv8w
DgYDV0R0PAQH/BAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQEFBQAD
ggEBAC/Jx8wH089hAgCx25FRdXIDMLDEFh9sAIs0rK/xR95uEdwMGvjUk2ysEdd8
t6aDZK3N3w6HM503sMZ70HKx8xo0o/LVem0DZgMXLUrXsXrfvIEG0o+x06iF3u6X
HMLrp+cxEmbDD6ZLLKGC9/3JG6gbr+48zu0craigHoSybJMIPiYaDMouGDx8rEKYl
Fo92kANr3ryqImhrjKGSKx5pttwn1y6TPn/CbxdfR5p2ErPioBhLG5qfpqj0i
pKGFeg23sqSaM4hxAjwu1nqyH6Lkwn0vEJT9s4yEIH1G10XUE0TS22RPuFvuG8UG
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/](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:
74550301454764894858436895359988151894690624301296360185771452280477781
39006227097627829418403707802184818353303040900226716949744297685434071
14010421320638577157215826721076491384610221868785174509514660662491662
61850590720747085539831035663356093826348439119819714826301278624142478
44029200116795663914330316020556259133796534127177915042071171068491356
81742154584117552829200504285439260372022597732694280107090146259016072
04757064263754788586662863659250353777981398741383692736813035233187376
32620546138901617101372104103521617321438518395842716766444276775835684
64175752738509024375642083789099934602535327668452735602199757783829503
05139720907320282040293102698831734949274666296641393283602834119244831
60294116148304689305890450291664813753369968689349015931415424674308622
57017134563417222706548377769543484439105105922405283338706016073360199
58463216200572008934881591994507927248897987250083167041408847219172411
21768776700515031676378192693067874449638243618188054778976245788221673
75961385557831602267390212785616275712203561701890180232010492667691455
92655962061277567019556313065142238688850848699228124566758595593957427
07648958243784711503527359823682376929652358055164794388297320694177715
84792804821875147837083137
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:
  74550301454764894858436895359988151894690624301296360185771452280477781390062270976278294184037078021848183533030409002267169497442976854340711401042132063857715721582672107
  64913846102218687851745095146606624916626185059072074708553983103566335609382634843911981971482630127862414247844029200116795663914330316020556259133796534127177915042071171
  06849135681742154584117552829200504285439260372022597732694280107090146259016072047570642637547885866628636592503537779813987413836927368130352331873763262054613890161710137
  2104103521617321438518395842716766444276775835684641757273850902437564208378909993460253532766845273560219975778382950305139720907320282040293102698831734949274666296641393
  28360283411924483160294116148304689305890450291664813753369968689349015931415424674308622570171345634172227065483777695434844391051059224052833387060160733601995846321620057
  20089348815919945079272488979872500831670414088472191724112176877670051503167637819269306787444963824361818805477897624578822167375961385557831602267390212785616275712203561
  70189018023201049266769145592655962061277567019556313065142238688850848699228124566758595593957427076489582437847115035273598236823769296523580551647943882973206941777158479
  2804821875147837083137
  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]
] ]
```

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

```
[
[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 2C 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.....0
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 EA 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.c0...:....=...0
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/yNYNbkK8wDQYJKoZIhvcNAQENBQAwcjlELMAKGA1UE
BHMCEUExOjBAbG9uVBAoM0UUVudGkYkYwQgZGUgQ2VydGlmawNnY2Ns24gTmFjaW9u
YWwgCGFyYSB1bCBFC3RhZG8gUGVydWVubzEzFMB0GA1UEAwWRUNFUK5FUCBQRVJAJ
IENBIFJPT1QgMzAeFw0NzA4MTAxNzIxMjE1aWw0MjE1aWw0MjE1aWw0MjE1aWw0MjE1
BGNVBAITA1BFMUUwQAYDQKDD1FbnRpZGFkIGRlIENlcnRpZmlkYXN0cmlzZW50IE5h
Y2lVbWVfSiHhcmEgZWw9RXN0YWRvIFB1cnVhbm8xH2AdBgNVBAMMFkVDRVJ0RVAv
IEVSVSB0QSB0S090U0U0U0U0U0U0U0U0U0U0U0U0U0U0U0U0U0U0U0U0U0U0U0U0U0
vL2La6NiGtUwwoyA7Cdnqju1VLYrp5/MX01RCXrns5DvuobS/Afb2unu0oVRSw6jY
cpDP0bNnaPuBhLa0FKhjB0VJvA3US+b+9Ek2cKekCzJyQLNwB6r/m2ggTGGGGITO
GayNkLsrM0vNPP8F/T48bx0nUDupGVmpuKLMzz9xASBF0DhofK0xC/eEU/i r r6d
nmbFDtFFdrJr/4c6lNyiYerwPw4knu4br6uJ6KfKXE1P5r7eol4n3JxBhU10NK/
mMc8CypJkZXC+LZ2bv7nGgZpVkv04yen/uX5VkuIevMPyNi2EengxwI0SexZP
BMITH37RqiG02NDsN1EopFqXpddwyMIJMcLr4ZsVn0Zhd0KlxZmPt1P/GPy8VM7
63LkkWnHueq84ZG02CwrUa0U8R8Y41JRUn/q0lyJYdveDNfLuGf/SYML5UrcXjg
+j6r54je02nY6dgZ3oI8CP9HaNRvsrFbRt9bnRlWlXQr8/iFoyAbnClhs0KpxG
Ay0v4pBB60tL0yTp7NeBY1FMY8tFAQNP5HKZ3V684j2kJ/T3wPwFCQuQuLY1bztb
p/bfxjZGkkrznqSLb00/+tJUBeAediTx8H3d61RpAo1QnPxHLKIXIz6k5/bpYT4n
QuDkH20vv68j9SVeyd771fMt0qWHV/yp3uEY200A0IDAQABO4HFMIHCBMIGA1Ud
EwEB/wQIMAYBAf8CAQIwHwYDVR0jBBgwFoAUH+kpIGHSUMUK13f1SIr7dDs/yR4c
S0YIKwYBBQUHAQEPTA7MDkGCCsGAQUFBzACh1lodHRw018vd3l3LnJlbnLLYy5n
b2IucGUvY3J0L3NoYTIvZW50cm51c2c5jcn0wEQYDR0R0BAowCDAGBgRVHSAAMB0G
A1UdDgQWBQf6SkgYdIxRxd/VI1vt00z/JHhzA0BGNVHQ8BAF8EBAMCAQYwDQYJ
KoZIhvcNAQENBQADggIBAEP8rU4dSIY9Zts3a6/vFvb1hNvETmVxhx/DhI7GkW
AuiXANVBL/x1jeDjNkMka0ThQWazBCVbuyrD1LB+ptv0G6BLti6MG1heGv0mFMgz
prqH9J4AF8w2IffyfbgzCaTTOGp88L5959h3mq0Lmfq3xR+MFAN7JGvWPCsbaLj
8sfY1t1JN/hoZ3+x0Ll3Xw9Q0MmdFG5Tlz/yqAE9n9QMBwSob5uvXBgvU6CI
zYjzqnn0308V4eYgY1WL3iK0V7eYeumKQ1LnNm5N27zids1oPkBeLhvTh8Kq0
765UHKHVMC3YdHH2z/LD6ZuVlGxZLgAmx6EGzbz4PmqX6iDen3azI8ps5CnKYPP
q0vqSYCLGTTZosfaHhbgqCCPNXU3xHn/5j+jnqVntoUXVJKVK0/mTrn9+LOYw
o/LEvpNxpWkK5KfobAuXa4Y86/0Whb4jNLczb//4VkrZ+/3Hu7X2QthAv42ALR6
3xgFY3T/GVfLw8V0RLU+leg4sNfgaFFH1qSPofN/28NhP6pm0aytIL+2g44xJ5J
0BSAUxv6IPITh065Y6sL91QRNF419N3XfvdZQeyA5GNw1GeFtcwMQUzTzqoYSN6
Dipmd06Lny9Zj+eactfjGj0Y0/k0oCGPaaTn7rkH0/ppG1XkiYi6GxecT9MU0QS
-----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:
67154680094615224171494412742951981673461687731648096332530187632107159
66133097984412055213762024720208136674648471169650009236044003755416893
80727244060023530337987062449703399170879547186940392709114729226771716
00030752463722047005786705818866122850765741491414882621645926136871521
10181926164372296695928544740736195438089686493146546263063209755625511
34403130387719395733631148618357639367007751742033806558140267461699582
09116648596356165474140749059408048873147584933918054725324694536423269
25669602651519057354045373058073294978103243344361189548398525013760980
81576745125670097735852304114514054633890841149731562614295860272936686
77253433040148199482428357051308808978711112352180234727367673211131499
72362690745231779724425216903235649538364497433126119840045839325902569
89889770921038154778019804568184349991107662916773408902982480299668782
16916987278799300027026226215375526600428306096216611020840683054879871
42396913750124269740155477588697665097127916476575139473390145205940454
32161334758306697960409277270920998544074839503531748567722869174771557
36716448767307454744162795193428460627361044052090228179802705140744473
42026162101043948052811063809165839038508734324636812965137573268548595
50921665465184552319151877
public exponent: 65537
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:

```
[
  [
    Version: V3
    Subject: CN=ECEP-RENIEC, O=Registro Nacional de Identificación y Estado Civil, C=PE
    Signature Algorithm: SHA512withRSA, OID = 1.2.840.113549.1.1.13

    Key: Sun RSA public key, 4096 bits
    modulus:
    67154680094615224171494412742951981673461687731648096332530187632107159661330979844120552137620247202081366746484711696500092360440037554168938072724406002353033798706244970
    33991708795471869403927091147292267717160003075246372204700578670581886612285076574149141488262164592613687152101881926164372296695928544740736195438089686493146546263063209
    75562551134403130387719395733631148618357639367007751742033806558140267461699582091166485963561654741407490594080488731475849339180547253246945364232692566960265151905735404
    53730580732949781032433443611895483985250137609808157674512567009773585230411451405463389084114973156261429586027293668677253433040148199482428357051308808978711112352180234
    72736767321113149972362690745231779724425216903235649538364497433126119840045839325902569898897709210381547780198045681843499911076629167734089029824802996687821691698727879
    93000270262262153755266004283060962166110208406830548798714239691375012426974015547758869766509712791647657513947339014520594045432161334758306697960409277270920998544074839
    50353174856772286917477155736716448767307454744162795193428460627361044052090228179802705140744473420261621010439480528110638091658390385087343246368129651375732685485955092
    1665465184552319151877
    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

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

```
[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 18 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 .....UM^
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...'..TdCF0
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/07T0wDQYJKoZIhvcNAQENBQAwc24gTmFjYj9wYyYwGCFYySB1bCBF3RhZG8gUGVydWVubzEhMB0GA1UEAwWRUNFUK5FUCBQRVJV
IENBIFJPT1QgMzAeFw0xNzA4MjA4MDMxNTlaFw0zMDA4MjA4MDMxNTlaMGExCzA1BGNVBA
YTA1BFMTw0gYDVQKDDNSZwpc3RybyB0YVNBp25hbCBkZSBZSGVudGlm
aWhhY2N0s24geSBF3RhZG8gQ212aWwxFDASBgNVBAMMOVDRVatUkVOSUVDMiIC
IjANBgkqhkiG9w0BAQFAA0CAg8AMiICCGKAgEApJvYm1RwB1B00KMKFH9tkjCq
nyF9ZkTMkQg3S1k+qxFwq8Bv4K1Ma00aWe4/5vdaRI2NW/E61C+q76BAaAr/nwFP
```

TBPStBw6KerwZ4w+20FCF0UaioCJ6P15RETsRYesNDFeU/FJD7+o7MTt1s3nxPz
sqc0gi0RX07Zs8RmhRdLmhi+L0ZHxx6xNngd7bpk/ustCb3XKHkHJfJSLEd5EInA
Z+JhTzS18qvMqE5nV0+cBNcpvAazFp4R9J2vH4W1AbR8pIXoxXhQXIxtjoJWDX0
RgANBbv10NqHf6x0wCtJgALc2bzUzNZd6QhsiVe18kDJGjD34KvqT080yk98gwKo
mzrKEavXA3LrP8aCxtxX9URugt5KdH9GRgu4zm8632A9X76MjkhApvy0a7iA+s4
JZWhNS0bGYTTDBWeYjktcbEnGyfx/olze0qnYsPqn8n5001b52pV60YwYuKhw1b
D/flk0Z28CQ120sJm1LBXhgXtALE8n59/m/yELk7u17QZgQdCY2e2wi6H+7L7V9C
7e0eJnf/5WD1oUa6F/yswj47Le1p4peVXZg7P3JIGugCbBHtl42j04Jee+/+8E2DJ
omVJ16oFLZk38d1F00QaWgP6dv4L1PFVDRG5XkIIdF7GmLcb05iY01/sRbhBrue
jx+VmtA2zWg0UlpfbwUCAwEAa0CAR0wggEZMBIGAUdEwEB/wQIMAYBAf8CAQEW
HwYDVROjBBgwFoAUH+kpIGHSMUK13f1SIr7d0s/yR4cwPQYDVR0LBDYwNAYIKwYB
BQUHAWIGCCsGAQUFBwMEBgorBgEEAYI3FAICBggrrBgEFBQCDCQYIKwYBBQUHAWew
dAYDVROFBG0wazAz0dGgLL4YtaHR0cDovL2Nybc5yZW5pZWZ29iLnBL2FybC9z
aGEyL2VjZjZuZXUyY3sMDSgMqAwh15odHRw018vY3JSMi5yZW5pZWZ29iLnBL
L2FybC9zaGEyL2VjZjZuZXUyY3sMB0GAUdQgQwBBQIer/Nf7uFFfUzvfuf0LJ8
y857dTA0BgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQENBQADggIBAGqyEziEtBM/
ZuQ/2UBxXhticPgnRmrW0p3KD+7JbiGrSTKvRU0czeqm40wRP4j2+wFYALTGIUtB
z2F4rcYlNvycDXRw+Q7DXf6PopIbncP1YaziZuqw0DH0DL5cFxoQ+AZhWJh+vmi
2RLK2pJLHd7gAEYUGjmiAWXK5RN6b9rb6KA+N9bNvekA9QGNm7KnhZo5Fu4XNbp7
FdlQE3IVBxZH3J6eiWt0a111SpZAP7eYBjDtay2jUWLa0XrTE62WKhj6n+yBiowP
LPSP/Ew+DgAUw0fPDW8BkoXUids0VU1ewNC3FgwchuAM+a+E7+60oLOmN0lpTqT
8QM7Xtq1Rw1c+x5fxLGNEnJ14UAC2nz1KWF6cDkXreh6C5jpoV9ZVQ9/nI05tyAW
vENz01KVNareI0TPbQACmNGYay1wLcZIXsY7bBL0EhdRhL8k4hrdSeonS8+o
JwHVVRDR1GPF4aM61HDCxd15Pon/XmIwqC6DMV/j97LVqjV0Xe0mvrGPiWqBZu4
jVmWkt1Jw1oaPPTM2BA+j/KJLN/xlm301ApEVrtbG1UgHDXeur0BGvGz0J5ULKG
POzyM1gB71U2pCJwn93W/gxVxXcpIhtCoVz/KdPSxz2ppIx/bYYWo6u9Fd+E8c6G
UXH877/VRKvrm0pf2ntWn5jRjh5/6gY+
-----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:
22049080826349849073929231571857745080792825156349745752321416196524981
85171693862985715366517176420702065677048330265354620100178926752219652
26169549224793071180489301140306460877036034148458921106339386643281824
46878612069446305708519913011036088299485134949224193666648550579483141
99236120320145925422527612210656452315462262012327824392630122866761230
31784518127783466179475164334081913117609774411270824992172657645285354
49271193543991418454538809735726697736528764121555324149222711071520223
76173824141393461417250552357005942073158878512849822365628643925942627
2115291325851607773789958873344237570509543769563
public exponent: 65537
Subject key identifier d44b9a04348187b1f38ebcafad8a1efa6d48c35
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
public exponent: 65537

Public key

Sun RSA public key, 2048 bits

modulus:
22049080826349849073929231571857745080792825156349745752321416196524981
85171693862985715366517176420702065677048330265354620100178926752219652
26169549224793071180489301140306460877036034148458921106339386643281824
46878612069446305708519913011036088299485134949224193666648550579483141
99236120320145925422527612210656452315462262012327824392630122866761230
317845181277834661794751643340819131176097744112708249921726576452853449271193543991418454538809735726697736528764121555324149222711071520223
76173824141393461417250552357005942073158878512849822365628643925942627
2115291325851607773789958873344237570509543769563
public exponent: 65537

Subject key identifier

d44b9a04348187bf1f38ebcafad8a1efa6d48c35

Basic constraints

CA=false

SHA1 Thumbprint

d6e40831185c8dbf8b103a2a83d01ce6eef73774

SHA256 Thumbprint

ce6408bd05a240c9d9832edb1549e86a00d9d72f2b9ccb6cb1cc15921255f12b

The decoded certificate:

[
[
Version: V3
Subject: CN=RENEIC EREP Persona Natural DNIE, OU=RENEIC 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:
220490808263498490739292315718577450807928251563497457523214161965249818517169386298571536651717642070206567704833026535462010017892675221965226169549224793071180489301140306460877036034148458921106339386643281824
64608770360341484589211063393866432818244687861206944630570851991301103608829948513494922419366664855057948314199236120320145925422527612210656452315462262012327824392630122
8667612303178451812778346617947516433408191311760977441127082499217265764528535449271193543991418454538809735726697736528764121555324149222711071520223761738241413934614172505523570059420731588785128498223656286439259426272115291325851607773789958873344237570509543769563
public exponent: 65537
Validity: [From: Tue Mar 19 06:55:00 PET 2013,
To: Sun Mar 19 06:55:00 PET 2023]
Issuer: CN=RENEIC EREP Persona Natural DNIE, OU=RENEIC 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 FFi.....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 7Bw29...[.
0050: 48 5D 94 40 52 16 68 7C F6 64 77 FD A3 64 AA B4 HJ;.@.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-----
MIID2jCCAsKgAwIBAgIBATANBgkqhkiG9w0BAQUFAwEBAQIEMAKG1UEBHMCEUx
PDA6BNVBAoMM1JL2ZlzdHJvIE5hY2lvbmF5IGRlIElKZW50aWZpY2Fjac0zbiB5
IEVzdGFkbyB0aXZpbDEmMCQGA1UECxMduKvOSUVDIFJL2ZlzdHJhdGlvbiBBdXR0
b3JpdHkxKTANBgVBAMTIFjFTkLFQyBFUKVQIFB1cnNvbEgTmF0dXJhbCBETkll
MB4XDTExMjM0MTEyMjM0MTEyMjM0MTEyMjM0MTEyMjM0MTEyMjM0MTEyMjM0MTEy
MTwvOgYDVQKDDNSZndpc3RybyB0YWNpb25hbCBKZSBKZGVudGlmahNhY2Ns24g
eSBFfC3RhZG8gQ2l2aWwzJjAKBgNVBAsTHVJFTkLFQyBSZndpc3RyYXRpb24gQXV0
aG9yaXR5MSkwJWYDVQ0EYsBRU5JRUMgRVJFUCBQZjZb25hIE5hdHVyYWwgRE5J
ZTCCAS1w0YjKozZlhcNAQEBAQAgEPADCCAQoCggEBAK6pkLcGhLwLPTbGD0S
PZAYGvp4x1wnk9AV4tdQ3vgv77RwpggFXCF4E+2MxSz1P1GjVn0Wg1EPpKRULSA0
pL3yZzec9jLvtVbZIZHAV/90pYsHKHPUR/qs8+jZr9dkYGwyiaylbjYcCTgzHD
cfpL3ME/N460JhUf83ceNnIp6w0iyIu6k2zucZBANUmfbkxADnajZcsNjXj7UHM7
JRCRp203reMclC1IayQAAxt3virX5mC3tULs7261dp+ZCPBdy97azKXNghINj r
6ufV81bn54QTgm7a1cMfIqHbJgYVLOEmqQ1I0U237AVogNHUwJMjGE24zC8a/Ip3
BdsCAwEAAMhMB8HQYDVR0BBYEFNRLmg00gYe/HzjryvrYoe+mIw1MA0GCSGq
S1b3DQEBBQUAA4IBAQBz+DTxUX01pp3g33hJ177+4YD5q76qaZUtHqHK0tu/2eQ
4/PnyZ4kbNALNyEhtB45qfAr+kC2SX7thwHx+EJ7pEbTgBap3MjnmNbe0hd

LEBSFmh89mR3/aNkqrSgoUE9lqdUup03sQLGz1Ufa8JWPj9mN3M738+0cMX8RCh/
MVgs/JtaM6f5ICjy2Y50ymFM5K0f0I0WucAwR6bYvv0sIR8LZRdjIJQLRZI7+rB
2dde0RYADi reg5mBhrdqH2mDloqmHmbA7ZdmhP5eE2U20bJqVPG88VGE4kouXzq
Rn40r4gQtIBmbZ4pe06XFV+DEtBoCGpdUSXu12g
-----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 6188659425723429735036633399849591730
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:
17919184782495014516458115511710766250990319541591515170122817264841793
63022309679355056016428356484335617902108796173618803484564015972882564
67298805675225400383669828648565566371144915451122420710246198187631005
50486793202622047840555144926483753464365720616817514646914303869361760
03659923632989719140535106666179076634498143318507545903045182875218447
97269086008492164500389319997100012344837618919019831038131743755551941
61371322576853439721603499752472091693466966627541440239615134661874995
21814915222913904937346787839877295607468652788242200778407118283231878
8764713105191100934576134122922071034225272977773
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:
17919184782495014516458115511710766250990319541591515170122817264841793630223096793550560164283564843356179021087961736188034845640159728825646729880567522540038366982864856
55663711449154511224207102461981876310055048679320262204784055514492648375346436572061681751464691430386936176003659923632989719140535106666179076634498143318507545903045182
87521844797269086008492164500389319997100012344837618919019831038131743755551941613713225768534397216034997524720916934669666275414402396151346618749952181491522291390493734
67878398772956074686527882422007784071182832318788764713105191100934576134122922071034225272977773
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..

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

```
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..00.
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 08 77 6A ..EB..lEm..(.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...l.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 10 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...
```

1

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIHDzCCBfeGAWIBAgIQBkfk6B7+Z8WnZg7V18jsjANBqgkqkiG9w0BAQUFAADBv
M0swcQYDVQ0GEWJVVzEVMBMGA1UECHMmRGLnaUNLcnQgSW5jMRkwFwYDQQLExB3
d3cuZGlnaWNLcnQyY29tMS4wLAYDVQ0DEYVeAwDpQ2VydcCBBc3N1cmVkaEIEIENv
ZGUgU2lnbmLuZyBDQ50xMB4XDTEyMTA0MDAwMFAwDQZTEzMTAyMzEyMDAwMFow
dGx0CzAJBgNVBAYTA1BFMQ0wCwYDQVQIEWRMaW1hMQ0wCwYDQVQHEWRMaW1hMQ0w
CwYDQVQKDDtS2WdpC3RybyBOYWNpb25hbCBkZSBjZGVudGlnbmhY2Nds24geSBF
c3RhZG8gQ212awwsIFJFTkLFQzEhMB8GA1UECwYR2VyZw5jagEwEUGUgUgUw5m3Jt
w6F0aWNLHUQ0gYDQVQDDtS2WdpC3RybyBOYWNpb25hbCBkZSBjZGVudGlnbmhY
2Nds24geSBF3RhZG8gQ212awwsIFJFTkLFQzCCASIdW0JKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAl3ygvVZHTAT+HBTv1X8t1RXr0H7GM1h9tgLwh8URmATSF2xpy
WICPEwtG7s3lc81Na55SLHEu80FTQ0AQ0Tiqb5jMgtNKZGyWLe0pBHvzvp8q4Yk2
YdU7MqY9vt/KNC5L7gNoX0KDuwDgow5xrecmstbPmdX60B7i8tdW6AS9u+2x0
r8o7zrrMQafp208j j cRMYq11fMv5WBPj qIX4LcRNLt8SD0kFevv5NdOWZATdFDbh
cYD+po0EqU309dPuK04n5B1Jt3y0hJnniJ93aV3xT8yXHSQEUY+qN0TnJ6kIup4
ALx7a6X3899H5X2mgzeHuzCLy0C8vWA9/yCyew0CAwEAA0CAzkwggM1MB8GA1Ud
IwQYMBAFHtoz1mqwBe+5Xrh5T/Wp/dFjzUyMB0GA1UdDgQWBRRvoRjb4585E80e
8aI3Nmj80TSPzzA0BgNVHQ8BAf8EBAMCB4AwEwYDVR0LBAAwCgYIKwYBBQUHAWMw
cwYDVR0FBGwWajAzodGgL4YtaHR0CDovL2NybDMLnaWNLcnQyY29tL2Fz3Vv
ZW0tY3MtHjAXMwEuY3J5MD0gMaAvh11odHRw0i8VY3J3N5kaWdpY2Vydc5jb20v
YXNzdXJlZC1jcy0yMDEyY3J5cmwggHEBGNVHSAEggG7MIIBtzCCAbMGwGSAAG
/WwDATTCAAQ0gYIKwYBBQUHAgEwLmh0HA6Ly93d3cuZGlnaWNLcnQyY29tL3Nz
bc1j cHMTcmVwb3NpdG9yeS5odG0wgGFKBggRBgEFBQCAjCCAVYegGFSAEAAAgB5
ACAAdQBzAGUAIABvAGYAIAB0AGGAAQzACAAQwBLAHIAdABpAGYAABjAGEAdABL
ACAAYwBvAG4AcwB0AGkAdAB1AHQAZQBzACAAYQBJAGMAZQBwAHQAYQBUAGMAZQAg
AG8AZGAgAHQAaABALCAARABpAGcAaQBDAAGUAAGGAAQwBQAC8AQBQAFMAIABh
AG4AZAGAHQAaABALCAAUgBLAGwAeOBpAG4AZwAgAFAYQBYAHQAEQAEEAZwBy
AGUAZQBtAGUAAbG0ACAAdwBoAGkAYwBoACAABABpAG0AAQwBQACAAABABpAGEAyGp
AGwAaQB0AHkAIABhAG4AZAGAGGAEAgB1ACAaAQBwAGMAbwByAHAAbwByAGEAdABL
AGQAIAB0AGUAAGBLAGkAbgAgAGIAeQAQAHIAZQBmAGUAAGBLAG4AYwBLAC4wgYIG
CCsGAQUFBwEBBHYwdDAKBggRBgEFBQcwAYYyHR0CDovL29j3AuZGlnaWNLcnQy
Y29tMEwGCCsGAQUFBzAChkBoDHRw0i8VY2FjZlJ0cy5kaWdpY2Vydc5jb20vRGln
aUNLcnRBc3N1cmVKSURDb2RlU2lnbmLuZ0NBLTEuY3J0MwAwGA1UdEwEB/wQCMAAw
DQYJKoZIhvcNAQEFBQADggEBAAd8Z7eD34qIZL9Isr8wUYrQAMSEcm0L3up9iGzs
066WU/fz3JTA1L9Wu6Haw20V/6AicCbdkbN4ZnAIQDmjKkwsKVC4tQxRW2CrSiq
C3dqq3QdIGIy4715/TPyPjXe8zdb+nQ8+81+z5wu1whfKwhwWMtARS6dNN6CHos
zS0ZL2Kw+v5p+5wx4HnvFJDqfcXzhXTzgCJ7KtMvN05Jx5H/5xPbm5/RWJpHEeqn
0yDvq+1ejmJAWvZuKUszr9yW1YBJR27CEbK2m69vuuvwzGgYLRs16kCx/ieIiK
sR551M2Z0nuHwWj12KU5q+7ALSppwLYbGRqsBnm7KkbGh5E=
-----END CERTIFICATE-----
```

Certificate Service Provider Name (en): GSD

- Trade name (en)* GSD
- Information URI (en)* HTTP://WWW.GMD.COM.PE
- Service provider street address (es)* AVE. PASEO DE LA REPUBLICA 4675
- Service provider street address (en)* AVE. PASEO DE LA REPUBLICA 4675
- Service provider postal code (es)* LIMA 34
- Service provider postal code (en)* LIMA34
- 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=Certificado TSU GSD, O=GSD SAC, L=Lima, EMAILADDRESS=consultastsa@gmd-gsd.com.pe, C=PE

Type unspecified
Status undersupervision
Status starting time 2013-01-11T17:20:13.000Z
Service digital identity (X509)
Version 3
Serial number 114608067467920
Signature algorithm SHA1withRSA
Issuer CN=AC Camerfirma TSA CA, O=AC Camerfirma SA, SERIALNUMBER=A82743287, L=Madrid (see current address at www.camerfirma.com/address), EMAILADDRESS=ac_camerfirma_tsa_ca@camerfirma.com, C=ES
Valid from Thu Sep 20 05:29:12 PET 2012
Valid to Tue Sep 19 05:29:12 PET 2017
Subject CN=Certificado TSU GSD, O=GSD SAC, L=Lima, EMAILADDRESS=consultastsa@gmd-gsd.com.pe, C=PE
Public key Sun RSA public key, 2048 bits
modulus:
24363163391036060950491207371436188091159528520696832373904907235738573
03406086202134595479819274024248484907033528984664558293537582044658294
51379726160627633134314004028441257292467152647280339661238633044867042
14418983141593306365847648217014728652954665721777473454390026357304464
60170970188424144922853970317327376728206190385439281917019969418731591
03609400690583506683695093737375656715560835625147143101189586942626326
94078082731408537288567669615971822556103567480364235283450162953564033
30445813377676716779354248691311135690732883945353811319848301055748440
1179343459387635561827518167060171499822119692271
public exponent: 3
Subject key identifier cd6b5053a6fcfa84de7c4ad3741d5cb9ebd599fe
CRL distribution points http://crl.camerfirma.com/tsa_camerfirma.crl
http://crl1.camerfirma.com/tsa_camerfirma.crl
Authority key identifier 0481a33081a08014bffa7eae99daa656972c632168de0102ea59b22a18184a48181307f3
10b300906035504061302455531273025060355040a131e41432043616d65726669726d
61205341204349462041383237343332383731233021060355040b131a687474703a2f2f
7777772e6368616d6265727369676e2e6f726731223020060355040313194368616d626
57273206f6620436f6d6d6572636520526f6f74820112
Key usage digitalSignature
nonRepudiation
Basic constraints CA=false
SHA1 Thumbprint 2f2dc09bc70b5c09bfac22c7c487c273e9489993
SHA256 Thumbprint 26d6a74ff04b403c6275b2d2d1dee4b248e16c601e0aa38f20acb53bace93530

The decoded certificate:

```
[
[
Version: V3
Subject: CN=Certificado TSU GSD, O=GSD SAC, L=Lima, EMAILADDRESS=consultastsa@gmd-gsd.com.pe, C=PE
Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

Key: Sun RSA public key, 2048 bits
modulus:
24363163391036060950491207371436188091159528520696832373904907235738573034060862021345954798192740242484849070335289846645582935375820446582945137972616062763313431400402844
12572924671526472803396612386330448670421441898314159330636584764821701472865295466572177747345439002635730446460170970188424144922853970317327376728206190385439281917019969
4187315910360940069058350668369509373737565671556083562514714310118958694262632694078082731408537288567669615971822556103567480364235283450162953564033044581337767671677935
42486913111356907328839453538113198483010557484401179343459387635561827518167060171499822119692271
public exponent: 3
Validity: [From: Thu Sep 20 05:29:12 PET 2012,
To: Tue Sep 19 05:29:12 PET 2017]
Issuer: CN=AC Camerfirma TSA CA, O=AC Camerfirma SA, SERIALNUMBER=A82743287, L=Madrid (see current address at www.camerfirma.com/address),
EMAILADDRESS=ac_camerfirma_tsa_ca@camerfirma.com, C=ES
SerialNumber: [ 683c4526 5a90]

Certificate Extensions: 10
[1]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
[
```

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

```
accessMethod: 1.3.6.1.5.5.7.48.2
accessLocation: URIName: http://www.camerfirma.com/certs/ac_camerfirma_tsa_ca.crt]
]

[2]: ObjectID: 2.5.29.17 Criticality=false
SubjectAlternativeName [
  RFC822Name: consultatsa@gmd-gsd.com.pe
]

[3]: ObjectID: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
  KeyIdentifier [
    0000: BF FA 7E AE B9 9D AA 65 69 72 C6 32 16 8D E0 10 .....eir.2....
    0010: 2E A5 9B 22 ...."
  ]
]

[CN=Chambers of Commerce Root, OU=http://www.chambersign.org, O=AC Camerfirma SA CIF A82743287, C=EU]
SerialNumber: [ 12]
]

[4]: ObjectID: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
  KeyIdentifier [
    0000: CD 6B 50 53 A6 FC FA 84 DE 7C 4A D3 74 1D 5C B9 .kPS.....J.t.\.
    0010: EB D5 99 FE ....
  ]
]

[5]: ObjectID: 2.5.29.18 Criticality=false
IssuerAlternativeName [
  RFC822Name: ac_camerfirma_tsa_ca@camerfirma.com
]

[6]: ObjectID: 2.5.29.32 Criticality=false
CertificatePolicies [
  [CertificatePolicyId: [1.3.6.1.4.1.17326.10.13.1.4]
  [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
  ]], PolicyQualifierInfo: [
    qualifierID: 1.3.6.1.5.5.7.2.2
    qualifier: 0000: 30 4A 1A 48 47 45 53 54 49 4F 4E 20 44 45 20 53 0J.HGESTION DE S
    0010: 4F 4C 55 43 49 4F 4E 45 53 20 44 49 47 49 54 41 0LUCIONES DIGITA
    0020: 4C 45 53 20 53 2E 41 2E 43 2E 20 54 69 6D 65 73 LES S.A.C. Times
    0030: 74 61 6D 70 20 55 6E 69 74 20 2D 20 52 55 43 3A tamp Unit - RUC:
    0040: 20 32 30 34 36 38 33 34 30 39 37 37 20468340977
  ]] ]
]

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

[8]: ObjectID: 2.5.29.37 Criticality=true
ExtendedKeyUsages [
  timeStamping
]

[9]: ObjectID: 2.5.29.31 Criticality=false
CRLDistributionPoints [
  [DistributionPoint:
    [URIName: http://crl.camerfirma.com/tsa_camerfirma.crl]
  ], DistributionPoint:
    [URIName: http://crl1.camerfirma.com/tsa_camerfirma.crl]
]

[10]: ObjectID: 2.5.29.15 Criticality=true
KeyUsage [
  DigitalSignature
  Non_repudiation
]

]
Algorithm: [SHA1withRSA]
Signature:
0000: 67 28 B4 48 E6 D3 3B 55 CF 16 90 76 72 47 41 47 g(.H.;U...vrGAG
0010: 64 E6 AF 9F 3E 34 7C DC D5 00 7A 03 7B 96 26 30 d...>4....z...60
0020: 5A 31 2E 51 2B 38 AB 5E DC 2E 50 3E 3F 73 27 F6 ZL.Q+8.^..P?>?>'.
0030: 0A E8 BF FB 89 E3 29 42 F9 B6 60 13 77 F9 39 11 .....)B..`w.9.
0040: 4D 84 7B 2D 1B BD 80 81 FD A6 37 B8 44 B2 87 F6 M.....7.D...
0050: C5 F0 01 2B 1F 32 1B 28 4A 70 EE 44 E9 81 4C 79 ...+.2.(Jp.D..Ly
0060: 29 4A 74 D0 49 B6 D9 48 B4 D0 3E 04 74 BF E7 3C )Jt.I..H..>t...<
0070: 90 3D 72 30 BE 7B 59 89 4A EF CD 38 E8 5A CF F9 .r0..Y.J..8.Z..
0080: 58 72 3F DA 87 C5 16 54 60 FA CF 00 5E 29 52 F9 Xr?....T...^)R.
0090: C9 43 64 04 03 27 8B 39 9D 83 E8 DC AC DD 68 0B .Cd..'.9.....h.
00A0: 03 80 1A 02 58 7C 8F F8 7E 09 EE 8B 88 9B F5 DE ....X.....
00B0: 18 33 C9 82 AD 7B 0C 6B 03 88 B2 85 77 45 B6 93 .3....k....wE..
00C0: 85 28 BA 46 EC E7 5C A2 C1 B9 3C F9 6A 5F 11 3A .(.F..\.<..]_..
00D0: A0 A3 9A C4 D8 B7 2C B5 67 91 6C FC 5A E8 F4 56 .....;g.l.Z..V
```

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

00E0: EC EF 53 24 63 B6 9F 10 4C 57 EE 60 E1 EA 07 BB ..S\$c...LW.`....
00F0: 44 36 54 25 FE F0 3D C6 DB 17 7A B2 86 CC C9 B8 D6T%..=...z.....

]
1

The certificate in PEM format:

-----BEGIN CERTIFICATE-----
MIIGmzCCBY0gAwIBAgIGadxFJlqQMA0GCsGSIb3DQEBBQUAMIHUMQswCQYDVQQG
EwJFUzEyMDAGCSGSIb3DQEBBQUAMIHUMQswCQYDVQQG...
-----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:
12275773751243453819770946154555407610013499176168145849177654625640125
03767239895572403812587628793047309698513831599335691444465356120807670
26887482900599667102367709729124760758849708042854475220596254813184297
41587207469873202054328867118621768107054031350871622211578461907848811
0509485917528478089788769
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 0481a33081a08014691a9472a0d196ff3d562ad8fe2b4718159db0eea18184a48181307f3
10b300906035504061302455531273025060355040a131e41432043616d65726669726d
61205341204349462041383237343332383731233021060355040b131a687474703a2f2f
7777772e6368616d6265727369676e2e6f726731223020060355040313194368616d626
57273206f6620436f6d6d6572636520526f6f7482010c

Key usage digitalSignature
nonRepudiation

Basic constraints CA=false

SHA1 Thumbprint 7981a7952f5a8446195a2eed54bb686d40160208

SHA256 Thumbprint 32757c5025fcd67c4440c70fbf0925af320c5c84717fefc7fb14fb9941f8dc22

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 08 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]
```

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

]

```
[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 pertenecei
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.....o....
```

]

The certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGTKCCBRGgAwIBAgICAMEwDQYJKoZIhvcNAQEFBQAwge0xCzAJBgNVBAYTAkVT
MSIwIAYJKoZIhvcNAQkBFhNpbmZvQGhnbWVyZmlybWUyZ29tMUMwQQYDVQHEzPn
WYryawQgKHNLZSBjdXJyZW50IGFkZHZJL3MgYXQgd3d3LmNhbWVyZmlybWUyZ29t
L2FkZHZJL3MgMmRIwEAYDVQQFEwLBODI3NDMyODcxIjAgBgNVBAStGWh0dHA6Ly93
d3cuY2FtZXJmaXJtYS5jb20xGTAXBgNVBAQTEEFDIENhbWVyZmlybWUyZ29tIjAg
BgNVBAMTGUFDIENhbWVyZmlybWUyZ29tZXNpZ24gdjIwHhcNMTAxMTEzMTI1INjI0
WhcNMTMxMTEzMTI1INjI0WjB7MQswCQYDVQQGEwJFUzERMA8GA1UECBMlVFRU5D
SUEXETAPBgNVBAcTCFZBTEV0Q00lBMREwDwYDVQQKEWhJkRFRk9WOTUeUMBIAGA1UE
CxMLREVTVQVJST0xMTlMxHTAbBgNVBAMTFFLOREVOTLZBIERFU0FSUK9MTE9TMlGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCu0BUH8GwJMPwBJqIq2dHS46kwE44v
rLfrwQpE92Rgsmae57AEGRS5BeLQRDS0Gdt/o6L6wbZo0d+NTtYm5UmygxLmKdRm
```


iLMZ9dt8/30HzLwKD+0fW0+V1yT2KhmpfAJ/eP9IQAYVe1X6GpIv6/MPLWi4bpCM
 FGXbeLFU0my9YQIDAQABo4ICxjCCAsIwCQYDR0TBAIwADA0BgNVHQ8BAf8EBAMC
 BsAwHQYDR00BBEYFPfRQJ05XnmBTLMKTFH2MMLvrbZAMIGrBgNVHSMegaMwgaCA
 FGkaLHKg02b/PVYq2P4rRxgVnbDuoYGEpIGBMH8xCzAJBgNVBAYTAKVMSwJQYD
 VQKEEx5BQyBDYW1lcmZpcmlhIFNBIENJRiBBODI3NDMyODcxIzAhBgNVBAsTGmh0
 dHA6Ly93d3cuY2hhbWJlcnNpZ24ub3JnMSIwIAAYDQ0DExLDAGFtYmVycyBvZiBD
 b21tZXJjZSBSb290ggEMMB8GA1UdJQ0YMBYGCCsGAQUFBwMDBGorBgEEAYI3AgEW
 MHMGCCsGAQUFBwEBBgcwZTA7BggrrBgEFBQcwoAovvHR0cDovL3d3dy5jYW1lcmZp
 cm1hLmNvbS9jZXJ0cy90TORFU0HT192M15jcnQwJgYIKwYBBQUHMAGGmh0dHA6
 Ly9vY3NwLnNhbmVybWZmY29tMGwGA1UdHwR1LGMwL6AtoCuGKWh0dHA6Ly9j
 cmuY2FtZXJmaXJtYS5jb29vY29kZXNpZ25fdjIuY3JsMDCGqLqAshipodHRw0i8v
 Y3JsMS5jYW1lcmZpcmlhLmNvbS9jZ2Rlc2lnb192M15jcmwgdMGA1UdIASByzCB
 yDCBxQYLKwYBBAGBhy4KDAIwgbUwKAYIKwYBBQUHAgEWHGh0dHA6Ly9wb2xpY3ku
 Y2FtZXJmaXJtYS5jb29wYgGCCsGAQUFBwIChwaekNlcnRmZm1jYWRvIGR1IEZp
 cm1hIGR1IEPzZGlnbyBDYW1lcmZpcmlhIENVGZvaWduIHBlcnRlbnVjajVudGUG
 YSBsY3Bvcmdhbm16YWNp824gY29uIGlkZW50aWZpZ2FjaFNUIGZpZ2NhbCBDSUY9
 Qjk3NDU4OTk2MA0GC5qG51b3DQEBBQUAA4IBAQC1W7ZcHgs3UnaPk1EbbL+kqyk
 E3qyhCJaY7kStMD9EwYqsemAIYBaMk5TUEau/X42Q3xVXoEeg6iFevrLz4v1rmHd
 LeBX1ohe3JAqwgjXLk7Z06CK3s0+pvoYUIIpn54V0tfeE9/8QKAUu8+77JE/1Yc7
 N9EHkBMW5e3q4nBWBz1YgR1R8/9Q1r8E/17Wae9s0BaMh6kiwLzui837rFV3+9m9
 svTnzaKtOILCLyQ0KF5j5MXZnrnCACA2uxSooLNB+vv8cCFAsDq6wy3X0UH2b96H
 xwv+74t1rPMXjGyhKwWhLzh767yJA053p52Xs0fXwSQiLLZxPHQvW+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 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:
14406702391305106140142766295100576213492235373448846805360353022345240
83223269173693476126789305007937084587470927629433827620180470240139384
14215872028527163969125655573945488614401571467677066488315957153441759
85857577648484861115785092156343809129655752484288533594447905385702519
3408242979060399539152451
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 62f240278c564c4dd8bf7d9d4f6f366ea894d22f5f34d989a983acec2fffd50

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:
    14406702391305106140142766295100576213492235373448846805360353022345240832232691736934761267893050079370845874709276294338276201804702401393841421587202852716396912565557394
    5488614401571467677066488315957153441759858575776484848611157850921563438091296557524842885335944479053857025193408242979060399539152451
    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
```


Key usage

keyCertSign

cRLSign

Basic constraints

CA=true; PathLen=unlimited

SHA1 Thumbprint

99a69be61afe886b4d2b82007cb854fc317e1539

SHA256 Thumbprint

62f240278c564c4dd8bf7d9d4f6f366ea894d22f5f34d989a983acec2fffd50

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:
14406702391305106140142766295100576213492235373448846805360353022345240832232691736934761267893050079370845874709276294338276201804702401393841421587202852716396912565557394
5488614401571467677066488315957153441759858575776484848611157850921563438091296557524842885335944479053857025193408242979060399539152451
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 68 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 68 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: F0 C5 10 0D F7 92 BE F1 C3 D5 D5 95 6A 04 BB 2C .....]...
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.....
```


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 Wed Jan 18 11:36:06 PET 2012

Valid to Fri Jan 17 11:36:06 PET 2014

Subject SERIALNUMBER=B63622252, EMAILADDRESS=ggm@bit4id.com, CN=Bit4id, OU=Desarrollo, O="Bit4id Ibérica", L=Barcelona, ST=Barcelona, C=ES

Public key Sun RSA public key, 2048 bits
modulus:
26825426367756787598787102470995417337393088008304649804712714198784879
92617095461974533153782528173960417108354338450837596554973953735802298
04050033833086767980972408664295171587718250916348178248871591178910014
08705224729832002934286381529160916062383357900337380121915213788553943
39180535597286540753675873217708228634922806118576431307230790591601711
78941413800512849962361103579834855982961811823808049122970657700597461
45080633300121928641064330386555895502834894723797602334030765446166764
04155867475103621060701257367277192305930825326990742167427076041115436
6632715068894221820856034119709685430421415747471
public exponent: 65537

Subject key identifier f4d76066c02fa26db094230cf3665ebff3448671

CRL distribution points http://crl.camerfirma.com/codesign.crl
http://crl1.camerfirma.com/codesign.crl

Authority key identifier 0481a33081a08014691a9472a0d196ff3d562ad8fe2b4718159db0eea18184a48181307f3
10b300906035504061302455531273025060355040a131e41432043616d65726669726d
61205341204349462041383237343332383731233021060355040b131a687474703a2f2f
7777777e6368616d6265727369676e2e6f726731223020060355040313194368616d626
57273206f6620436f6d6d6572636520526f6f7482010c

Key usage digitalSignature
nonRepudiation

Basic constraints CA=false

SHA1 Thumbprint c41540211c090206c2a4607695ab0c43281f9d40

SHA256 Thumbprint a62793a55e4e7aedb6dc5a7120e3e917f461dc5df7e995f6e4c41940d42e12b2

The decoded certificate:

```
[
[
Version: V3
Subject: SERIALNUMBER=B63622252, EMAILADDRESS=ggm@bit4id.com, CN=Bit4id, OU=Desarrollo, O="Bit4id Ibérica", L=Barcelona, ST=Barcelona, C=ES
Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

Key: Sun RSA public key, 2048 bits
modulus:
26825426367756787598787102470995417337393088008304649804712714198784879926170954619745331537825281739604171083543384508375965549739537358022980405003383308676798097240866429
51715877182509163481782488715911789100140870522472983200293428638152916091606238335790033738012191521378855394339180535597286540753675873217708228634922806118576431307230790
59160171178941413800512849962361103579834855982961811823808049122970657700597461450806333001219286410643303865558955028348947237976023340307654461667640415586747510362106070
12573672771923059308253269907421674270760411154366632715068894221820856034119709685430421415747471
public exponent: 65537
Validity: [From: Wed Jan 18 11:36:06 PET 2012,
To: Fri Jan 17 11:36:06 PET 2014]
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: [ 889a1905 f346559f]

Certificate Extensions: 8
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: F4 D7 60 66 C0 2F A2 6D B0 94 23 0C F3 66 5E BF ..`f./..m..#..f^..
0010: F3 44 86 71 ..D.q
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 69 1A 94 72 A0 D1 96 FF 3D 56 2A 08 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]
]
```


Subject

CN=Global Chambersign Root - 2008, O=AC Camerfirma S.A., SERIALNUMBER=A82743287, L=Madrid (see current address at www.camerfirma.com/address), C=EU

Public key

Sun RSA public key, 4096 bits
modulus:
78685081857133083903186647788850502649500978545394737562216742372766117
84768509247698425557191765354903922418171698509292138103318788869289128
36079856447291755305866688080385138501320875714780249271468452120070890
29067450113785464762055270811430262762601630371273959102358149663485740
19314602023183208785474680865099087301217934646139117223035001537502776
54856693972761733774800246130479732372658631361809781953478235060205538
34188503360908928270935504396308128370929120136691909526204858368939918
20479221889804074621938632771421358464610162962562393203580803658290252
41056085879632115826349412664968294359531633897900788497361259111385176
27324896331660550741842360812832352680349344152855501332296935227916747
95283852481863652884015674142231691204176151018455910666342258984941865
32891144590531427390407262114351833841614732372673897237674790988856346
95232379061550962346270780024427351675073148273257431373346449464702600
72460648629421045067464779018249008467702470756253143779377406365306173
97852641815367082936787381059728275234031843352313461687906123495524197
06801104620677419323061373533926839288636940537806250290144299629242759
31767024047534288681552336343567855623461072014254075280295857712920213
91363723886202970109585679
public exponent: 65537

Subject key identifier

b909ca9c1edbd36c3a6baeed54f15b9306352e5e

Authority key identifier

0481d93081d68014b909ca9c1edbd36c3a6baeed54f15b9306352e5ea181b2a481af3081a
c310b3009060355040613024555314330410603550407133a4d61647269642028736565
2063757272656e74206164647265737320617420777772e63616d65726669726d612e6
36f6d2f61646472657373293112301006035504051309413832373433323837311b30190
60355040a131241432043616d65726669726d6120532e412e312730250603550403131e
476c6f62616c204368616d6265727369676e20526f6f74202d2032303038820900ae82190
53f5e8271

Key usage

keyCertSign

cRLSign

Basic constraints

CA=true; PathLen=12

SHA1 Thumbprint

d647d9ea994a1bd5d8c3cfff78d69a99bd45cad4

SHA256 Thumbprint

f01c1aca392882af152e9f01eccc0afddd8aa35bf895b003198b1e8c752ddb8

The decoded certificate:

[
[
Version: V3
Subject: CN=Global Chambersign Root - 2008, O=AC Camerfirma S.A., SERIALNUMBER=A82743287, L=Madrid (see current address at www.camerfirma.com/address), C=EU
Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

Key: Sun RSA public key, 4096 bits
modulus:
78685081857133083903186647788850502649500978545394737562216742372766117847685092476984255571917653549039224181716985092921381033187888692891283607985644729175530586668808038
51385013208757147802492714684521200708902906745011378546476205527081143026276260163037127395910235814966348574019314602023183208785474680865099087301217934646139117223035001
53750277654856693972761733774800246130479732372658631361809781953478235060205538341885033609089282709355043963081283709291201366919095262048583689399182047922188980407462193
86327714213584646101629625623932035808036582902524105608587963211582634941266496829435953163389790078849736125911138517627324896331660550741842360812832352680349344152855501
33229693522791674795283852481863652884015674142231691204176151018455910666342258984941865328911445905314273904072621143518338416147323726738972376747909888563469523237906155
09623462707800244273516750731482732574313733464494647026007246064862942104506746477901824900846770247075625314377937740636530617397852641815367082936787381059728275234031843
35231346168790612349552419706801104620677419323061373533926839288636940537806250290144299629242759317670240475342886815523363435678556234610720142540752802958577129202139136
3723886202970109585679
public exponent: 65537
Validity: [From: Wed Dec 07 06:29:21 PET 2011,
To: Sat Jul 31 06:29:21 PET 2038]
Issuer: CN=Global Chambersign Root - 2008, O=AC Camerfirma S.A., SERIALNUMBER=A82743287, L=Madrid (see current address at www.camerfirma.com/address), C=EU
SerialNumber: [ae821905 3f5e8271]

Certificate Extensions: 5

[1]: ObjectID: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: B9 09 CA 9C 1E DB D3 6C 3A 6B AE ED 54 F1 5B 93l:k..T.[
0010: 06 35 2E 5E5.^
]
]

[2]: ObjectID: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: B9 09 CA 9C 1E DB D3 6C 3A 6B AE ED 54 F1 5B 93l:k..T.[
0010: 06 35 2E 5E5.^
]
]

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

[CN=Global Chambersign Root - 2008, O=AC Camerfirma S.A., SERIALNUMBER=A82743287, L=Madrid (see current address at www.camerfirma.com/address), C=EU]

SerialNumber: [ae821905 3f5e8271]

[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 1C 68 74 74 70 3A 2F 2F 70 6F 6C 69 63 79 2E ..http://policy.
0010: 63 61 60 65 72 66 69 72 6D 61 2E 63 6F 6D camerfirma.com

]]]

[4]: ObjectID: 2.5.29.15 Criticality=true

KeyUsage [

Key_CertSign

Crl_Sign

]

[5]: ObjectID: 2.5.29.19 Criticality=true

BasicConstraints:[

CA:true

PathLen:12

]

Algorithm: [SHA256withRSA]

Signature:

0000: 05 58 76 8C 33 37 91 1D 5F CA 0F D0 47 97 BF 5D ..Xv.37...G...]
0010: 90 89 DE 5A 86 DD 79 2C 82 9D CA 3C 24 CE 8D 39 ...Z.y,...<\$..9
0020: 6C 90 2B 14 F3 08 DD FD 3D 5D E8 25 F5 72 63 48 l.+.....]=%.rCH
0030: B5 0F 97 01 5C 01 49 40 6D 45 04 E2 D1 CD 46 D0\I@E...F.
0040: 86 25 98 6A 03 F9 BB C6 BE EE D0 F3 61 CF 98 F9 .%.j.....a...
0050: 8F ED FC E6 15 0A 35 8A 28 A1 90 66 D7 1C 99 9AS.(.f....
0060: 36 23 EE 6C 20 D6 AD 97 51 55 2A B0 56 28 8E 7F 6#.l...QU*.V(...
0070: 4A E6 07 5E D5 CA F8 5E F3 11 A4 8C 13 4A F2 CD J..^.....J..
0080: F0 B5 B7 66 63 41 50 02 0C 2C 47 6E AC 38 00 7D ...fcAP...Gn.8..
0090: 8C 60 A8 8A 7E 96 27 A3 B7 F1 BD 13 3D 2A EF 03 '.....'.....=*..
00A0: D8 70 FB DD 64 2B E8 C7 5C AF 0C 9C 20 8B 6C D0 .p.d+... \... l.
00B0: 26 40 92 FE F4 09 87 72 53 BE F6 6D E9 18 F5 76 &@.....rS..m...v
00C0: 24 B8 6A 17 E7 E3 3D D8 A6 DB 90 7C 61 D8 4F 93 \$.j...=.....a.0..
00D0: 41 08 F3 65 CA D7 DE AB 93 0A BA 3B ED 5F A5 DC A..e.....;..._..
00E0: CA 18 7C AF 02 F8 CA E0 7B 1C 7C EF 9E C9 93 300
00F0: 1A EE 48 1C 79 F8 50 77 A9 6C 9E 5D FC 6B 0E DE ..H.y.Pw.l.].k..
0100: 93 9A CB 24 F7 80 9D 55 D2 78 CD D9 66 0F 59 81 ...\$.U.x..f.Y..
0110: CB AC A2 37 CA 91 CA AC 57 CD 8D 81 03 AB BC 1F ...7...W.....
0120: CD 92 FE A5 94 DD D6 E7 6A AC 5D DC 25 FE 2B 4Fj.].%.+0
0130: 79 D9 72 3A 20 8C 14 A8 C4 72 30 58 08 9B 53 16 y.r:....r0X..S..
0140: 71 A6 B8 F1 F2 BC 9F BF F9 EB 43 61 B3 2C 68 BA q.....Ca.,h..
0150: 70 E4 6B 08 53 15 84 0F 40 12 54 24 99 10 92 3A p.k.S...@.T\$.:..
0160: 93 CA 82 1D 8A AE B4 88 89 45 2E EF 77 AC C0 0AE..w...
0170: 07 29 3B 8F CB 2D 29 61 45 07 0E 3A F6 04 E1 2A .);...-jaE.....*
0180: BF CF 13 7B 4B 7A A3 6C 23 1A 66 B1 28 0A E1 D1Kz.l#.f.(...
0190: FF D5 2B C8 46 54 81 17 4B E1 E7 10 67 A5 8B BA ...+.FT..K...g...
01A0: 2C 41 C7 37 A2 09 F1 A5 87 29 EE 87 97 6A A9 B2 ,A.7.....)j...
01B0: 4E A8 A8 9F 61 0D AA 34 C4 1F 78 43 95 99 D7 C3 N...a..4..xC...
01C0: BD CA 77 76 52 DC 10 0C 7C 95 25 D8 05 C5 84 30 ..wvR.....%.....0
01D0: 55 DA 78 4C E2 6B 11 F0 BC C3 42 0C 7C 99 DB 30 U.x.l.k...B...#0
01E0: 60 DA 76 E5 14 55 99 56 E6 41 4B 34 5C 7A 48 49 `..v..U.V.AK4zHI
01F0: 6D 05 69 F9 31 71 07 D6 5A 92 85 50 34 74 68 74 m.i.lq...Z..P4tHt

]

The certificate in PEM format:

-----BEGIN CERTIFICATE-----

```
MIIHSTCCBTGgAwIBAgIJAK6CGQU/XoJxMA0GCSqGSIb3DQEBCwUAMIGsMQswCQYD
VQGEWjFVTFTDMEEGA1UEBxM6TWFkcmkIChZlWUgY3VycmVudCBhZGRyZXNzIGF0
IHd3dy5jYW1lcmZpcmlhLmNvbS9hZGRyZXNzKTESMBAGA1UEBRMJOTgYz0zZm9j
MRswGQYDVQKEXJBOyBDYW1lcmZpcmlhIFMuQ54xJzAlBgNVBAMTHkdsb2JhbCBD
aGFtYmVyc2lnb1BSb290IC0gMjAwODAEFw0xMTEyMjYyMjYyMjYyMjYyMjYyMjYy
MTI5MjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYy
cmVudCBhZGRyZXNzIGF0IHd3dy5jYW1lcmZpcmlhLmNvbS9hZGRyZXNzKTESMBAG
A1UEBRMJOTgYz0zZm9jMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYy
BgNVBAMTHkdsb2JhbCBDaGFtYmVyc2lnb1BSb290IC0gMjAwODCAiIwDQYJKoZI
hvcNAQEBBQADggIPADCCAggIBAMDFVtPkOpt2RbQT2//BthmLN0EYLVJH6xEd
KYi0NwGMi5HYvNjBL99RDaxccy9Wglz1dmFRP+RVYXfXja0CNfCUMd2drvXNL7
G706tcut0x8Epu2uIRU/uXpbknYpBI4iRmkt4DS4jJvVpyR1ogQC7N0ZJJ0YPP2
zxhPYLIj0Mc7zmFLmY/CDNBAspjcdDah0o7kKrmCgrUVSY7pmvWjg+b4aqIG7hkF4
dDPB/gBVs1dU6CeQNR1M62X/JcumIS/LMmjv9GYERTyY/jKmIhY5ntRQ0XfjyG
HoiMvvKRhI91NngATH23MRdaKXoKGCwoze1eqkBFsbW+Q60wFH9Gz01KtsX00G2
Id3UwD2ln58fQ1Dju7xsepeY7s2MH/ucUa6LcL0nn3HAa6x9K6bo1106dbDVwo3V
yJ2dwB3Q0L9R50P4wz2rteandeahvENdk5IMagfe0x2Y1taswTXbo6AL/3K1dh3e
beksZixShNBFks4c5eUzHdwHULSjqoI7mjcv3N2gZ0nm3b2u/GSFHTynyQbehP9r
6GsaPMwiS0L7iWk+XwhSx2LE1AVxv8Rk5Pihg+gEpuoHt02T59x90a0900pE9Jh
wZG7SMA0j0GMS0zbaRL/UJ5cIINZc+18ofLx/d335dNDWKBHY809PeU1VlndpSog
zCtLkykPAGMBAAGjggFqMIIBZjASBgNVHRMBAF8ECDAQAQH/AgEMBB0GA1UdDgQW
BB55CccqHtvTbdPrUuU8VuTBjUuXjCB4QYDVR0jBIH2MIHwB55CccqHtvTbdPr
UuU8VuTBjUuXqGbsqSBrczCBrdELMAkGA1UEBhMCVUuXjBBBgNVBAcTOK1hZHZj
ZCAoc2VlIGlnIcnJlbnQgYWRkcmVzcyBhdCB3d3cuY2FtZXJmaXJtY55jb20vYWRk
cmVzcykxXjAQBGNVBAUTCUe4HjcmZz14NzEzBmBkGA1UEChMSUUMgQ2FtZXJmaXJt
YSBTLkEUMScwJQYDVQQDEX5HbG91YmVwQ2hhbWJlcnNpZ24gUm9vdCA2IDIwMDI0
```

CQCughkFP16CcTAOBgnVH08BAf8EBAMCAQYwPQYDVR0gBDYwNDAYBgRVHSAAMCOW
KAYIKwYBBQUHAgEWHGh0dHA6Ly9wb2xpY3kuY2FtZXJmaXJtY55jb20wDQYJKoZI
hvcNAQELBQADggIBAAYVdowzN5EdX8oP0EeXv12Qid5aht15LIKdyjwkzo55bJAr
FPMI3f09Xeg19XJjSLUPLwFcAULAbUUE4tHNRtCGJZhqA/m7xr7u0PNhz5j5j+38
5hUKNYoooZBm1xzJmjYj7mwg1q2XUVUqsFYojn9K5gde1cr4XvMRpIwTSvLN8LW3
ZmNBUIML Edu rDgAfYxgqIp+Liejt/G9Ez0q7wPYcPvdZCvox1yvDjwgi2zQjkCS
/vQjh3JTvvZt6Rj1diS4ahfn4z3YptuQfGHYTSNBPCPNlytfeq5MKujvtX6Xcyhh8
rWL4yub7HHzvnsMTMBruSBx5+FB3qWyeXfXrBt6Tmsk94CdVdJ4zdLmDImBy6y1
N8qRyqxXzY2BA6u8H82S/qWU3dbnaqxd3CX+K0952XI6IiwUqMRyMfgIm1MWcaa4
8fK8n7/560NhsyxounDkawhTFYQPQBjUJkQkjqTxiIdiq60iILFLu93rMAKByk7
j8stKwFFBw469gThKr/PE3tLeqNsIxpsSgk4dH/1SvIR1SBF0vh5xBnpYu6LEHH
N6IJ8aWHKe6H1Zqpsk6oqJ9hDao0xB94Q5WZ1809ynd2UtwQDHyVJdgFxyQwVdp4
TOJrEFC8w0IMfJnbMGDUduUUVZLW5kFLNFx6SEltBwn5MXEH1LqShVA0dGh0
-----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
7212854535471571888024184939778283804918288633703
public exponent: 65537

Subject key identifier 91b38ae87e166ff9121c3f29a45010440bd97776

CRL distribution points http://crl.usertrust.com/UTN-USERFirst-ClientAuthenticationandEmail.crl

Authority key identifier 0418301680148982677dc49d2670004bb450487cde3dae046e7d

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:
26926110584125833537545895214890737273777428404404833368187117345006353822066388549072556394026312688581090272187605227160930241053097823016926548184658427698395267813010100
58554422773474257808012698424667295144068874116630260625159971947121139225186700471562265125711159258072212166076612259199373641977697325865559113275998785588195551750877764
47768607372211213578864171253109087411666203612809460357649088867687580847748313831684286051138159286217917353067996887968888105667439642314340143314039970133023431797453375
27923853845270704002624286370005656500506063260087212854535471571888024184939778283804918288633703
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 .....0...?).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
]]
]]
```


Service provider locality PATERNA
(es)

Service provider locality PATERNA
(en)

Service provider state VALENCIA
(es)

Service provider state VALENCIA
(en)

Service provider country ES
(es)

Service provider country PE
(en)

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
73461886511029985881788281
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:
5675119111807288098961008805558059482326666796622847491532820776689324085248832370515078578240603680634239006146099934381739106442693153315879537217052700587088425324963840
35602532121809573811002399149291819404786555548195418786839967898334051509861479923241857647047551382060328666380139562259906710770546776164153950713621513836181994892225447
7087361506596067860287514262435245595856513835837887652174053626284085640324217766238134127839734655675827704279935639039278445947829732306605581154885940304077630491026500
40991018324487687837957213719376018073389567978040005193253955755061928451500335462868719938814471851334132783913508748854695850176698982445939895734599295127454425193423
8234467328896758654140675819677327783301035623635108332079933344839377486796417980810344642856236592102445939981808719888072920423467157590529643119412812863263522637842958
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://acedicom
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 00 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 4907.....I
0070: 8B F9 27 82 DC C6 91 85 0B EB 3A F0 B1 76 52 FAvR.
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....0.....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 40 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 ...".....0.....
0150: AA ED 6B 9E 88 C7 A3 74 DC F7 D8 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 C7N...
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 24k.....D.g4.\$
01D0: 20 A7 85 59 DF 14 3E E6 8B 00 D7 8F 92 3A C3 E3 ..Y..>.....<.
01E0: AE E4 32 42 38 5B 11 C9 82 33 B3 D6 87 57 57 06 ..2B8[...3...W.
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-----
MIIHQDCCBSigAwIBAgIIJ4m662xZS1owDQYJKoZIhvcNAQELBQAwNjEwMDQGA1UE
AwwNQ0FFRElDT09gUm9vdDEPMA0GA1UECgwGRURJRjQ0M0M0SQYDQVQ0GwJFUzAe
Fw0xNDA3MjIxMTA0NDNaFw0yNDA1MjIxMDIwMDBaMIGBMRMEQYDVQQDDApDQUVE
SUNPPTTAAxMRiWEAYDQVQ0FwLCT0Y00TA4NjcxZDzANBgNBVAoMBKVESUNPTTE4MDYh
A1UEBwwvQ2FsbGUGQ2h0cmxLcyB5b2JlcnQgRGFyd2luIDdggLSA0NjE0MCAIIFBh
dG9ybmE4CzA2BGNVBAVTAkVtMIIICjANBgkqhkiG9w0BAQEFAAOCAg8AMIICcGKC
AgEAIxuyfCbKiXqKaCIv1C50+xy3/RkC8TJ6EF/l8cr5HK6N53eYGGrHcG/B6L43
jgbC8/CVp6py7VlDaLaaIm56dL9WqHqq6Bvg2DFssYYKcmzRT2gIHYE74/x92m1d
n6j0408MXi8mVfhyx4L70LlnwqtH1mAMPSPB8X8bE9+6azf8zGtKiU8vh836uWY2
3p3VlwpofSMF5STtqU45nUk7aXrRt9wRfmVZQF13/Rc47VhNuPtAggQZ1zfLBGc0
350h9sk7yQXPm9Tf1+x0rK251vgfInLUpnDomFpawfy9t7cnuCbnbZXIE3beKXW
I9hy+J0dqHVI9mTjFt89vmAYRZcvSHF7RmsTkRnbuSA8Mpe+++aU5j6cPUR8IhbJ
aWkJWSzZv2p9S38FP7CkL54d0+FixL0HiQzQ5PG7z6oEFZL+YFE3IcwwXrsUllYw
ohyJEqwz2rEhTW39YkLQ5X2N02ciHL0M50JAN/JH/zHusUbtzPmGEHIdccevIc
U6N8wBKR+9rF8UblV98E0Wry+qgXr7VLtnzhQEbJ82xfoWcVqnLJDS062E8Ydu+
VesB42eLywQtceR+JKtj2swDG0s0P6v5t5nsqI98CkacjUaLwroT77CJqCWlJ5j4
Rwk2A15fmgITDK8L3b8d1+Y5zczz/ba5KNtq8oa0mFGj3kAwEAa0CAgQwggIA
MIGTBgggBGEFB0cBAQSBhjCBgZCBgggBGEFB0cBAQSBhjCBgZCBgggBGEFB0cBAQSB
LmVkaWVbWdyb3VwLmNvbS9jZXJ0cy9jYWVkaWVbXJvb3QuY2VyMD0GCCsGAQUF
BzABhjFodHRwOi8vb2Nzc5hY2VkaWVbS5ZG1j2b21ncm91cC5jb20vY2F2L2ZG1j
b21yb290M0GA1UddGQWBBRtaoj4Lup/L83A9HZ3k+ZFMu+LBTASBgNVHRMBAf8E
CDAGQH/AgEAMB8GA1UdIwQYMBAfBTKNKL4Y6thGei4PaHgw5B15/nLMIIGbBgNV
HSAEgZMwgZAwgY0GDcsGA0QBgpejAgMBATB9ME4GCCsGAOUFBwICMEIeQABDAGUA
cgB0AGkAZgBpAGMAY0B0AGkAbwBuCAUAUABYAGEAYwB0AGkAYwBLACAALwB0AGEA
dABLAGA0Z0BuAHQwKwYIKwYBBQUHAgEWH2h0dHA6Ly9hY2VkaWVbS5ZG1j2b21n
cm91cC5jb20wQ0YDVR0fBD0wODA2oDSgMoYwaHR0cDovL2FjZW9jZ29tLmVkaWVb
bWdyb3VwLmNvbS9jYWVkaWVbXJvb3QuY2VyMD0GCCsGAQUFBzABhjFodHRwOi8vb2
Nzc5hY2VkaWVbS5ZG1j2b21ncm91cC5jb20wDQYJKoZIhvcNAQELBQAD
ggIBAD+qPUsRtj1Nf0mP14v2GX9bAhGdD0acG7AhU5WFIXa3Jo31LWdXjkJ6/e
9dTtJNqvzGCIGVrxkpWqFegVbqJTnPkCma+YmiLZLTWao52q84+EggP4cvPVF
40Eweh2q8M0XAQqsTz+DYyLwUmL+SeC3MarHqVr0vCxdLL6L8omucnyscfVfQ5C
0BwGgFCm8KlKPGeG1Uwsb7s3NqF5Q37hWdN2Ney2q8XRTkmyv/quGQjH7yAw552a
oHgLc/KyYrEBpqBptar64B/vyXi/eCdgg1hRvqpG9EuD2UdVdo9sXRHDuTKj/m
XN0N4ETw5vF1j3DXijAmFsd/0zJgcORN8XVjVbxJiDtdy38WNPg8I7AHI1n0X3
uvlf9zuHjLgN1PuW+UBGDyEAGEKrxZuagIFRlFkvhZ5CArnlEigK6hxrVgt0G
oXwM3qrta561x6N03Pfbnhd1pYTrqJXI6icJ8g3PKer8aLeINzLgm/nLlp/4Y/1
Tve0x2bcrv7D007LzJkTXcTzFJlNvfe0Fjuy9ACQR/jigHcdzlkCPSV7LJ12mR5A
PFMZAUaepl+/jDpRi0W3H009T3iWwHEZa5MCy+1+RJRNrNPYkIkeFwd8UPuaLAnEP
kjo8467kMKI4WxHJgj0z1odXVzhMnCKPpfd0hRuFC5MQsk
-----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
728449947008513473597489418783452762228522694143919394165432251630627
02928787967454588425466652790682946539520344846402953024104799389670982
14951614219181419820902977617011939709596294775467170793869134967674269
40147716745519033717744736525356004907395855809731001165063613408132585
41129894520430137200505994855946734104117608732109237174470625484217119
33231244189714158643370058724238642629311557994713609984863044774499154
61063832669514206474394636080826032512898129520050668180056206471892181
2079867635267755510749107
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:
89549450400115540560970202287952704516491243874493294738279582900604072425158453121553732237364711470348620517861724759186136597514025569333958264575264205801018082186298297
12902161311798700842100004861882125508971380892037589429413308274006315323722290056367820712938320765569805302921271536887318869979619942872243522713411666587306009714680046
76530227355386302027521790543889759312651222374115828267523307825409872128113486781432998642916925046105137481617623026845729332025436806128113782887328994152508606875482882
51144627373469276314316142013265915819553290421681584367954439130583157564838524869137361825364695571856604972012972488247327407827047221472233721838606944438004624815416072
704203653341168999728449947008513473597489418783452762228522694143919394165432251630627029287879674545884254666527906829465395203448464029530241047993896709821495161421918
14198209029776170119397095962947754671707938691349676742694014771674551903371774473652535600490739585580973100116506361340813258541129894520430137200505994855946734104117608
73210923717447062548421711933231244189714158643370058724238642629311557994713609984863044774499154610638326695142064743946360808260325128981295200506681800562064718921812079
867635267755510749107
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: [ 58fclabc 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.

```

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

```
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 05 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.U0.....o.<.
0050: 28 5F 54 72 25 73 43 FC   08 D1 08 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 70 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 40 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?2MX0.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 30 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.la..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-----
MIIFUTCzCAzmGAWIBAgIIWpWavKFKLkMwDQYJKoZIhvcNAQELBQAwNjEwM0GA1UE
AwNQ0FFRELDt00gUm9vdDEPMA0GA1UECgwGRURJQ09NMQswCQYDVQQGEwJFUzAe
Fw0xNDA1MTkxMjA4MjBaFw0xNDA1MTkxMTIyMDBaMDYxYjA4BgNVBAMMDUNBRURJ
Q09NIjVb3QxDzANBgNVBAoMBkVesUNPTTElMAkGA1UEBHMCRVwggIiMA0GCsGQ
SIb3DQEBAQUAA4ICDwAwggIKAoICAQD0bgMroSXTH0zgu8CujYv2jC8efjkl6Qb0
VZuLmCmU7YzHMpZxZj6BdcpA4jWwyh/NWQpenm7oeIeYRSN5wDQ3KJUZYrfabLx
R3840BZGp2kxETVM4Sp//Z1P1T3jXuhNGVMIMwsh1RIwaZeQry3B9X9BX0k2j024
HhQVX9oPblwNcQRvF+Fm72t01Veu9/Ou69cmWDh2ka5Ugh+QkKz3Kn8PLe5XgZ
vhLdzYd5Qc4Vrdcl.kRARBB4SnfI4A18Waa6gCtRA+eugDRgPeV6RneQFFJw0ExkC
RLpRw+55smAUo6+85C0o0GgBQ2TKDoaDYtCKGAYn8St7SykhW5rMaEIQyEtPDy0y
iHzEXG4xcMv3r5XAJaQ1cTn8+dhyyNATvafo0i2LTKFvCvy00D07mmv8p0rJ/ua0
iEPMxrw/ddKlqa/6l7k+t85UoE3AXS7BKnhjVHK4rFr10vsgYQY69KAR0KvMgwXJ
1G4+b08+cy825vNPsBAAUUVJw4z2o5gdhH+ZCsPqCjzD0YR4SGf1GzsOHQ5DsQR1
wa5dov22QKlHeGehwe7NlDKIU35iWm0BA/Xr6AVJjnn+NdTL0wSv6S11+3ujjV3
d9ymfyBUktZj1nKeTSqzj3PzGaHEsB/mNKMLAD6XSdhqqoEQTM4tVBRzDYV2x//
vcPIg0iinswIDAQABo2MwYTAdbGNVHQ4EFgQUFM0qWxhjQ2E26Lg9oeBawHXn+csw
DwYDVR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBQUzSpZeG0rYRnouD2h4FAdef5
yzA0BgNVHQ8BAf8EBAMCAYwDQYJKoZIhvcNAQELBQADggIBAE1Rbmc5bqX4UgJ
g9EPGRtYA8n3dn9yIfCXSc13v/f9op15319xLCUuyAWCwdbVH8D6JA33v9rGnHx3
r2hiTsI1fdK2VVEaEBX8L68WxzWCKF9UciVzQ/wI0QvkAdzsFrCX4EoDq4ahVDnT
Rxf60cYA+15cFXSocjvFinA0gtudjLcbjntKsJb1xLc/8VSAINGxmdPctfBmSJTV
IvMiUE7wXHG1Ch4aZlpK0E/H3iV0fBDK8o5SP9V2KCDglqN1ar2+a73edKlMxn
dIoHTQC4hEacH18riFbqk/L4+KEoD1Zw9rTTQWuZ5BUuLaWqu898c+MsawjW+WVI
LtfVvA4pY8KB7sLPMHX5Nwc5CYc6gu/hIw43VYvrtR7w+Y79vcgF7y+toIv0aohK
ypT+1oNBqPo7TewpK/k8ySv0BhXBZ0UyZ2K4z9Be9x1GJ2zud5bgMpus22ry50
1RCXerbZz10bK1+k0A1RM2/j9ZcAwL5/fhH19xBctGyHdc16uaoFFQy5F679SMbc
JqB35zx1Yj8yTVhPqnl1L1Pte8VE9Mvm64xk1ZSHY0XtGk0a0+s9L4fMbAuEyj90
1hENPzA3qzFhDoBnyLk691hz1f5W2Kvr3zk3tdJGDjtMS01fhxT1K5Hs2+GeLmrT
tb/kHUYSayrtRq1qesyVl7pX2Kau
-----END CERTIFICATE-----
```

Certificate 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
8953240621103040483218914574859232366566432512997
public exponent: 65537
Subject key identifier 8c71cc93076fd1d586687d823a41d94c02f8965d
CRL distribution points http://crl.firmaprofesional.com/fpoot.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:
23535818509823618888152413102470237449998648353116926521981512524876912347057781868138053914189777158647722427203589024049670611799019500505420835059571299702868019416930086
49612491734248632999408480467929952831511519616857624286178772394890833736874846638520867498217994107231469568612373180653597168756143683955794759354362231520259463560780129
9023689124646554646614098167083618045298397291582810819706878957615954476375554997338928343229015165771315881695939577119099917053049664358723076644801962240287162940661272
71532347917973237538191691794395019899103323067968953240621103040483218914574859232366566432512997
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/fpoot.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

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

```
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: 8C E1 27 C9 41 87 B1 D5 82 CC 24 8C FD 74 1D 8B ...A.....$.t..
0060: 5F 9F AA E2 E7 CB E0 ED EE AF 58 92 AC C7 35 CC .....X...5.
0070: CE 54 81 A0 F4 33 8F BD 71 D7 51 6B 12 73 ED 3A .T...3..q.0k.s..
0080: 23 78 4C ED 83 43 B0 90 F8 86 5B E8 EB C3 44 60 #xL...C....[...D`
0090: F5 65 A3 8F AE 37 89 3E DD E7 5F 10 0F 72 44 21 .e...7.>...rd!
00A0: A8 0E 13 65 CE 1D 45 2D 00 47 67 75 A2 B3 D3 95 ...e..E..Ggu....
00B0: 1F EF 71 97 AA 18 85 81 8D CC 44 86 60 E2 1E C2 ..q.....D.`...
00C0: 9C 4B 7E 56 C5 E8 B7 72 00 28 A9 9B CC B0 01 98 .K.V...r.(.....
00D0: 3E 35 18 1D 0D 4E 2D CB FF 9D 74 FF A8 06 E8 91 >5...N...t.....
00E0: 9E EC CB 65 92 3D CD FC A5 0B 40 D0 60 49 5C 0B ...e.....@.`I\..
00F0: AF 4B 29 0E 63 73 7D A8 00 DF E4 D2 6E 55 DF 95 .K).cs.....nU..
0100: 4A A9 D1 1C D8 95 0B 9F 4C E5 4C 3C E7 A7 56 A7 J.....L.L<..V..
0110: AF FB A5 4E EE AC 38 B0 A1 6F B2 CE 84 66 63 23 ...N..8...o...fc#
0120: 50 5A C2 43 00 99 94 7E D9 DA F5 85 D5 51 34 9F PZ.C.....04..
0130: E1 9C 18 65 9A CA 5B FE 8E F0 23 DA F3 A0 16 25 ...e..[...#...%
0140: 32 9A 86 23 11 C1 CE 95 55 26 18 4E E6 00 58 5E 2...#.?.UG..N..X`
0150: AA B7 5F 5D A8 48 BD BB C5 8E 8B 4B 5F FC 7E AC ..._].H....K...
0160: 1F 60 BA 2F 54 EC DE 7A 0A FE 4A 00 4D 0E 4E CC `./T..z..J.M.N..
0170: A0 88 D3 24 9C 68 08 D1 B7 F5 DF A1 B6 34 C7 55 ...$.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 A8 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-----
MIIGyDCBLcGAgIBAgIIOQNmRV5uKdQwDQYJKoZIhvcNAQELBQAwUTELMAKGA1UE
BHMCRmVxOjBBAgNVBAMTUF1dG9yaWRhZCBKZSB0ZDZjOAwZpY2FjYW9uIEZpcmlh
cHJvZmVzaW9uYm90LGEIEEZmJyZnDA2ODAEFw0NDAMTg0MDAwNTRaFw0ZMDEY
MzEwNDYNTVAMIGSMQSwCQYDQVQGEWJFUzEeMmBwGA1UEChVrYm90ZmVxOjBBAg
N1BhZCBKZkEuMSIwIAAYDQVQLExLDZjOAwZpY2Fkb3MgO3VhbG1maW9uZG9yMRIw
EAYDQVQFEwLBNjI2MzQwMjg0Mjg0Mjg0Mjg0Mjg0Mjg0Mjg0Mjg0Mjg0Mjg0Mjg0
LSB0VUMFUMSUZjOQFETlMwggE1MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQ
C6cIUUCaCe12gMnFsVFePe9Z52zvebP/J30UrhNH0H4vny6VS7oV0d+aM0vqW9JmT
rYIA1i72jp8TnWnhQ0RNLQmZjd+uQkeVSI0rohSHMejAh0yx+yUsoWDSX0dhKV+
CCjN+nvCDUxJw+jm1N/UVZkH2QRK3M0cbQGRNADeKPsRrUB00280hbGyP0xM6S
x3BIxXz8r2mXt1FkktVY0tU8zyT40M+c6mPEmmWL+uHpuL4MLzvZ/1Rr0+ynyu
a54hGkh4i1jt1a3PecgdY7269FfhLsIWMSnXkV0eY6u6+F+CkxwqiR04xvCEVXY
10bIHPgXON3VYWiZLxvLAgMBAAGjggJmIICXB0B0BgggBgfEBQcBAQRoMGYwNgYI
KwYBQUHMAKGMh0dHA6Ly9jcm90ZmVxOjBBAgNVBAMT25hbC5jb20vY2FyY290
LmNmYDAsBggrBgEFBQcwAYYgaHR0cDovL29j3AuZmlybW90ZmVxOjBBAgNVBAMT25hbC5j
b20wHQYDR00BBYEF1xxzJMHb9HvHmh9gjpB2UwC+JZDMB1GAIUdEwEB/wQIMAYB
Af8CAQAwHwYDR0jBBgwFoAUZc3rqzUeAD5+1XTAHLRzRw4aZC8wggFBBgNVHSAE
ggE4MIIBNDCCATAGBFUdIAAwggEmIHhYBgggBgfEBQcCAjCB5R6B4gBDAGUAcgB0
AGkAZgBpAGMAyQBKAG8AIAABkAGUAIAABBAHUAdABvAHIAAQBKAGEAZAAGAGQAZQAG
AEMAZQByAHQAaQBmAGkAYwBhAGMAA0DzAG4ALGAgAEMAwbBuAHMAdQBsAHQAZQAG
AGwAYQBsACAAYwBvAG4AZABpAGMAA0BvAG4AZQBzACAAdQBsACAAdQBsAG8AIABl
AG4AIABoAHQAdABwA0AlwAvAHCAdwB3AC4AZgBpAHIAAbQBhAHAACgBvAGYAZQBz
AGkAbwBuAGEAbAAUAGMAwbBtAC8AYwBwAHMwLWYIKwYBBQUHAgEwI2h0dHA6Ly93
d3cuZmlybW90ZmVxOjBBAgNVBAMT25hbC5jb20vY3BzMD5GAIUdHwQ0MDIwMKAuoC
yGKmh0dHA6Ly9jcm90ZmVxOjBBAgNVBAMT25hbC5jb20vZnBzY290LmNmYDAsBggr
BgEFBQcwAQYwDQYJKoZIhvcNAQELBQADggIBAAs6836yufcn0XnMxxa80W03iN
T0/xiF1sQH3GfUhnKK9x7QA12MLTM0FvZ8Z23RLLkCnSryCVI5AJCbvAoE3fxqd
V7Q0a45DH7/DNyzTv0EnyUGHsdwCzSM/XQdi1+fQuLny+Dt7q9YkqzHNcz0VIGG
9DDPvXHXUWsSc+06I3hMYNDsJD4hLv068NEYPVLo4+uN4k+3edfEA9yRCGoDhNl
zh1FLQBHZ3wiS90VH+9x16oYhYGNzESGyOIEwpXLFbF6LdyA1pm8yWAZg+NRgd
DU4ty/+ddP+oBuiRnuZLZZI9zfyLc0DQYELcC69LkQ5j32oAN/k0m5V35VKqdEc
2JULn0zLTDznp1anr/u1Tu6s0LChb7L0hGZjI1BawkMmZR+2dr1hdVRNJ/hnBhL
mspb/o7wI9rzoBYlMpqGIXHBzpvVJh05g1YXqq3X12oSL27xY6LS1/8fqwFYLov
V0zeegr2SgBNDk7Mo1jTJx0cNG39d+htjTHVeeEzpz3+0c8HU0Gf98+0nfj09T
zGAz1Pj1qXa77m3Iu982gsaJH8qK5dyxGfYMN5CaNq23p/5g/ATzFrT0f++jP85+
MBAQeDT/zC0r44ewVc2TcxCN6GbieepMDk67n51SHSKZJE/e29hKuGjP3kd1P01
WHLC29X0aKRjmyDC
-----END CERTIFICATE-----
```

Certificate Service Provider Name (en): CERTISIGN

Trade name (en) CERTISIGN

Information URI (en) [HTTPS://WWW.CERTISIGN.COM.BR/](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 21999836477145942709391465284060324680

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
57662688880449366933826184204351631401110102748608483448320449092867978
53298969527055553330202398286589695489642858577694803416337698521274058
47281216174248082539208956559946309055859152012169401579755172994056663
67033770108581155110153750951972985948202976879283731693914356206985814
9212562650217464256942062124500010692075541559821

public exponent: 65537

Subject key identifier 333090627298587376566d3e5ba25408bfd2c797

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:
```

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

```
25680538283525265187038795187562153405958393862848369453954941920316686924369382060119331294604678198889180929714400294650948320107495828582677455235013613048211857729309242
0477168742419732995918665755868027706433207650964755077040772371064485259583830000649321572538844993219786192857662688880449366933826184204351631401110102748608483448320449
092867978532989695270555333020239828658969548964285857769480341633769852127405847281216174248082539208956599463090558591520121694015797551729940566636703377010858115511015
37509519729859482029768792837316939143562069858149212562650217464256942062124500010692075541559821
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 60 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.Z0_.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
MQswCQYDVQQGEwJCUjEtMCsGA1UEChMKQ2VydGZaWduIENlcnRpZmZlYWRvcmlE
RGlnaXRhbCBTLkEuMR4wHAYDVQ0DExVBOyBDXj0aXNpZ24gUGFyY2VyaWEwHhcN
MTEwODE5MDAwMDAwMjE1OTU5WjBcMQswCQYDVQQGEwJCUjEtMCsGA1UEChMKQ2VydGZaWduIENlcnRpZmZlYWRvcmlE
RGlnaXRhbCBTLkEuMR4wHAYDVQ0DExVBOyBDXj0aXNpZ24gUGFyY2VyaWEwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwgEKAoIBAQDLbdYiBUZjEAJ0qn473hdcxshGdHxvzFKsmoecLZhsqxdF0f9D
RcMwzLHb1JbV2Ly3ChoyakEXNXKaK10Kfvd1eE7ZB4C86nvwXARfDRk8c0LDAdI
c9F5fu6sN0ot5M1mKcaMZntIKVq9n4UV0X7Daedo/XzYuyWjPj9j9r9LzCkzbWgLh
mRDsjDI4ZzWYkcr4HQ/mo5mEWg20i/+nWcyv3Ac53RdaB8FMxTOI4nSExe1sA
LRTzVFeFm04Gueuu2VTcaZtWks0bZypknT2fHNQdpOT/SHGhpvNKwrgxmK5QIT
VkZ6r8Hnc2kHqvqfAsCXAWckvRjR66rHHYPoNAGMBAAGjgeQwgeEwDwYDVR0TBAGw
BgEB/wIBADBKBgnVHR8EXTBbMFmgV6BVhLNoDHRw018vb25zaXRlY3JsLmNlcnRp
c2lnbi5jb20uYnIvcmlw3NpdG9yaW8vbGlyL0FDQ2VydGZaWduUGFyY2VyaWEV
TGf0ZXR0Q1JMLNMybDARBgblghkgBhVCAQEBAQCAQYDKQYDVR0RBCIwIKQEMBwx
GjAYBgNVBAMTEUNlcnRpZmZlbn1lYyYxLTUyMjM0MjUyMjUyMjUyMjUyMjUyMjUy
bT5boLQIv9LHLzALBgnVH08EBAMCAQYwDQYJKoZIhvcNAQEFBQADggEBAFP7GP5x
d0HViznFLX5cLX5LreFN6Zi+S/Lp1L+BeGf4irYCK9V00H3CemQ3Tvj27o1z8S
LXSFYt1J54Pzb85Ewf0X4UyI6eV2d0fG667dVoJtd/xLhqWhB+cUsEstV9buKs
Gdd6zCINPUSDQpJq3Fj4Mluam8BxUxcRjmxdiPy/v0miYbiK7PTXoX0mY0J0du
u1nc5eq40yI4Tch6bTYfc+H3L0ZuXU2zYLeT60eX0moP9/meVJh6rw/dgF05PPrVf
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:

85936788191977224731224669339476190588854700556553471417862426631680093
78042969152520094571163439124043639064878132332792014219533375605822770
39405242058279688403482414263122393459329943195479838975657997256471569
94985998569115094619465557838823013011864123974339990015366662513529963
88808101223834619173928987908065514568370463191661651261413211885773998
97035475635318605039478697680647580174163868800818010134953620128890883
94657127060803515435892109519665764783440365969540224157797827981745197
69973255018716853815567486466236984654438261349792239459354636770195541
45948886450136031437768713209612381697796901537264656432881523955998027
36758217268540729712089732124351179090402366820810364728579656620626963
01578187739927461459952029848279482891209927370984923591686382525628277
81109814140471531152421335674321960403435555897081669508536892130381187
26588733739254049468195377058644882660885436272526911132868132726312681
57930979285999757970173788666109725795898024430367706148688594095264278
97597470129053655805013269642393747473841703813248860850792258295369159
50639515542252668928123125268230699807947318672947888882837562251298253
62606738357947332245292470444669949400960410829390493478495177934782200
0273224918432842338222681

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
19301706035504030c10524f4f542041432047534520532e412e312e302c060355040a0c
2547455354494f4e2044452053454755524944414420454c454354524f4e49434120532e
412e311730150603550405130e4e49542039303032303432373238311e301c060355040
b0c15687474703a2f2f777772e6773652e636f6d2e636f314f304d06035504090c464361
72726572612032312041204e6f20313234202d203535204f666963696e61203330332e20
68747470733a2f2f777772e6773652e636f6d2e636f2f646972656363696f6e3116301406
035504070c0d424f474f54c3812c20442e432e310b300906035504061302434f3181ae308
1ab060c2b0601040181f32001010a020c819a456e7469646164206465204365727469666
963616369c3b36e204469676974616c2041626965727461204175746f72697a616461207
0f72206c61205375706572696e74656e64656e63696120646520496e647573747269612
07920436f6d657263696f20646520436f6c6f6d6269612e2068747470733a2f2f777772e6
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:
85936788191977224731224669339476190588854700556553471417862426631680093780429691525200945711634391240436390648781323327920142195333756058227703940524205827968840348241426312
23934593299431954798389756579972564715699498599856911509461946555783882301301186412397433999001536666251352996388808101223834619173928987908065514568370463191661651261413211
88577399897035475635318605039478697680647580174163868800818010134953620128890883946571270608035154358921095196657647834403659695402241577978279817451976997325501871685381556
74864662369846544382613497922394593546367701955414594888645013603143776871320961238169779690153726465643288152395599802736758217268540729712089732124351179090402366820810364
72857965662062696301578187739927461459952029848279482891209927370984923591686382525628277811098141404715311524213356743219604034355558970816695085368921303811872658873373925
40494681953770586448826608854362725269111328681327263126815793097928599975797017378866610972579589802443036770614868859409526427897597470129053655805013269642393747473841703
81324886085079225829536915950639515542252668928123125268230699807947318672947888882837562251298253626067383579473322452924704446699494009604108293904934784951779347822000273
224918432842338222681
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

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

```
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 0.;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 0.;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.gse
    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[ .
```


-----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 38908203973182606954752843738508300
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:
69933286738728365358290221753567885492298399483988454801141936841153446
52131543490132823217421557630091876442049973361504956901948079105765089
92020568075150541515432818884960717734109703474444075161302740294266154
02189152756354453993031235107487462278780242623449331595999239471355252
43522625804507107954460753625063505723355127005334845331319260448889892
00002928446875035742142976009424103697783993717366253243707662105662819
89238034074806556511061841938125595345430452236968077052462159228418265
00322979943259136642203749765319401980252205999627182730113666529497150
49164486891256851847249509639816693929718169639430315235005749289426454
2345125376077921826147380161655599157722185812736521809799053962763760
45254524120084606459927783442518293842140228404247916784902307351106343
52001430606675892308251329803225011800233869941351103862533149083875767
56889268542497109905880632914239331654256138879871005778316385374518704
08305662484227385160185829042200288177880254380417675591827568366730814
29132022541779976649392245749554370138554192760633227167902586210216565
88265862115955298959831344837714018879342047270924767449261700455419168
88396202214080778186145668363329751132152548359699086759801128778831099
15276289123444737363175923
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 Certificadora S.A., O=Sociedad Cameral de Certificación Digital - Certificadora S.A., C=CO
Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

Key: Sun RSA public key, 4096 bits
modulus:
69933286738728365358290221753567885492298399483988454801141936841153446521315434901328232174215576300918764420499733615049569019480791057650899202056807515054151543281888496
07177341097034744440751613027402942661540218915275635445399303123510748746227878024262344933159599923947135525243522625804507107954460753625063505723355127005334845331319260
44888989200002928446875035742142976009424103697783993717366253243707662105662819892380340748065565110618419381255953454304522369680770524621592284182650032297994325913664220
37497653194019802522059996271827301136665294971504916448689125685184724950963981669392971816963943031523500574928942645423451253760779218261473801616555991577221858127365218
097990539627637604525424120084606459927783442518293842140228404247916784902307351106343520014306066758923082513298032250118002338699413511038625331490838757675688926854249
71099058806329142393316542561388798710057783163853745187040830566248422738516018582904220028817788025438041767559182756836673081429132022541779976649392245749554370138554192
76063322716790258621021656588265862115955298959831344837714018879342047270924767449261700455419168083962022140807781861456683633297511321525483596990867598011287788310991527
6289123444737363175923
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 Certificadora S.A., O=Sociedad Cameral de Certificación Digital - Certificadora 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 2CyT.: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 certifiad
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

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

```
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.l..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 A1 DE 77 88 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.Sy.V7...)..
0130: 0F F1 29 39 EF 7E 5C 28 32 70 35 AC DA B8 C8 75 ..)9...L(2p5...u.
0140: 66 FC 9B 4C 39 47 8E 1B 6F 9B 40 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....0d..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 89 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-----
MIIGZjCCBE6gAwIBAgIPB35S3vgFeNX8GmMy+wMMA0GCSqGSIb3DQEBBQUAMHsx
CzAJBgNVBAYTAKNPMUcwRQYDVQVDD5Tb2NpZWRRhZCB0YWI1cmFsIGRlIENcnRz
ZmljYWNpw7NuIERpZ210YXVwL3B0Z0E0B0IMfuuZ0nj8LSWkdF/WU340jC2I+GdV75LaeHM/J4
Ny+LvB2GNzmxLPLyVeqcgxhaBvzz1NS6jBUJJfD5to0EfhcSM2tXSEXP2yYe68yQ
54v5aHxwD6mq0D043zeX4LvegGHTgNiRg0JaTASJaBE8rF9ogEHMYELODVoqDA+b
MMcm81bbq0nXl211i/kDwFJnmXL3wvIumGVC2daa49AZM0yth9VXAnow6IYm+48j
iLSH5L887uvDdUhfHjLvgWJsxS3EF1QZtzeNnDeRyPYL1epjb40s0MLzP96a++Ej
YFDIJs2yKHZMI+ko6Kh3V0z3vCaMh+DkXkwakFU5tTohVTP92dsxA7SH2JD/zt
A/X7JWR1DhcZDY8AFmd5ekD8LVkH2ZD6mq093ICK5Lw1omdMEWux+IBkAC1vImHF
rEsm5VoQgpgk3s0956JkSCXjrdCx2bD00mk1vUgjcTDlaxECp1bczwmPS9KvqfJ
pxAe+59QafMCAwEAa0B5jCB4zAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/w0E
AwIBBjAdBgNVHQ4EFgQU00N06df0eXRU+Tows/RtLAMDG2gwagaGA1UdIASBmDCB
LTCBkgEVR0gADCBI TARBggrBgEFBQcCARYfaHR0cDovL3d3dy5jZXJ0aW50aW50
Y5YjB20vZHBjLzBaBgggrBgEFBQcCAjB0GkxMaW1pdGFjaW9uZXMGZGUgZ2FYW50
7WFzIGRlIGVzdgUgY2VydGlmawNWhZG8gc2UgcHVLZGVuIGVuY29udHJhcilBliBs
YSBEUEMMA0GCSqGSIb3DQEBBQUAA4ICAQBcLLW4RZFNjmEYAgPU3zmpFmps4p6
xbD/Chwso3EcIRNnoZUSQDWDg4902zNc8E12CoF53UnUmjIz75uny3XLesuXEpBc
unvFm9+70SPI/5j0CK01AUghforA1SBCLETvv3e1iWdIG0ADBaGJ7M9i4z0ldma/
Jre7IR5v/zLxdlp6yQGVwZVR6Kss+LGGIOk/yzVb0hfpKv6DExdA7ohiZVvV02Dp
ezy4ydv/NgIlqmjCMRW3MGXrfx1IEbHP0eJCGBbT9ZMj/EyXyVo3Bhwi2ErN0o42
gcmRkBDI8ck1f+404HGIG0atLDCIaR43NAv025TDPCWkPHv+wLaNEC8DY5waN0
jJN+Qd53i+yG2dIPPy3RzEC1iWZIH1CznCNz6cE6r7wkeZBWN7PGKX6jd/Ep0e9+
XCgycDws2rjIdwb8m0w5R44bb5tNA1LQ1M+9hup4ph0905zNHdpdq35f/RWmnkJD
W2ZaioG9xa5P1FLK2Zq19E4UqLWRhH6/JocdJ6PLwsCT2TG9WjTSy3/pDceiz+/
RL5hRqGEPQgnTIEgd4kI6mdAXmwIUV80WoyWaM3X94nCHNMyAK95y9NgWyo6R35r
MD0hY1l/SrnHLeclUw40GEfhewVvdCx/CVxY3UzHcmrr1zZ7Ud3YA47Dx75WnXk
BYn8eNZLcZDzQq==
-----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) PORTSMOUTH
Service provider locality (en) PORTSMOUTH
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 4835703278459707669005204
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
3143463213972159925612976006433949563180335468751
public exponent: 65537
Subject key identifier 607b661a450d97ca89502f7d04cd34a8ffcf4b
Key usage keyCertSign
cRLSign
Basic constraints CA=true; PathLen=unlimited
SHA1 Thumbprint b1bc968bd4f49d622aa89a81f2150152a41d829c
SHA256 Thumbprint ebd41040e4bb3ec742c9e381d31ef2a41a48b6685c96e7cef3c1df6cd4331c99
The decoded certificate:

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=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:
66595160664750516665888947079812222542893744041883076853089856464540621
67443458645344777333381078920760083006502850927451782294842162284078777
869462642087892756828885161002187727135260301491027747250520919461113
51123197795636638844433578815639196795675168495042117310595809896551280
86129951251326234384614503573230652719453708601258964043446685224213986
59528540421178534719175649512308344686598631256869196614575598925005623
04973886078190255908615720132017623851058153662485845782027976850791345
17369427970620243935399882403865979817090561523207098974938446022626118
43097903992992098918191590141440065600923170529386617709606174446518729
74229187661331136494843269518647141346909839934798624443843636192177387
61772508828734391571673577011536590261589625585065879942714125471501042
35200703510299179358504950419526984783589267124226363639483440989631868
41301145057022707141794804317696063105059971910121408353233237271746565
92916612356504683280801081667643672076169301720710830129608447199397198
28601161706646323762114419168587889417102312393586631553886045566728887
10881234013387082544024604615853147788810179000186399245523425836653883
80842031742442925088440791410583474516811132953276777843023094972373257
20423832773651010149331371
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 04820138308201348014e89bcd7e86629b7a4d8c00973985cf1c7890703aa1820110a482010c30820108310b3009060355040613024553310f300d06035504080c064d4144524944310f300d06035504070c064d4144524944313a3038060355040b0c317365652063757272656e742061646472657373206174207777772e63616d65726669726d612e636f6d2f6164647265737331273025060355040b0c1e474c4f42414c204348414d4245525349474e20524f4f54202d203230313631123010060355040513094138323734333238373118301606035504610c0f56415445532d413832373433323837311b3019060355040a0c1241432043414d45524649524d4120532e412e3127302506035504030c1e474c4f42414c204348414d4245525349474e20524f4f54202d203230313682082dd22e5030a65e13
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:
66595160664750516665888947098122254289374404188307685308985646454062167443458645344777333810789207600830065028509274517822948421622840787778694626420878927568288885161000
2187727135260301491027747250520919461113511231977956366388443357881563919679567516849504211731059580989655128086129951251326234384614503573230652719453708601258964043446685
22421398659528540421178534719175649512308344686598631256869196614575598925005623049738860781902559086157201320176238510581536624858457820279768507913451736942797862024393539
98824038659798170905615232070989749384460226261184309790399299209891819159014144006560092317052938661770960617446451872974229187661331136494843269518647141346909839934798624
44384363619217738761772508828734391571673577011536590261589625580658799427141254715010423520070351029917935850495041952698478358926712422636394834409896318684130114505702
2707141794804317696063105059971910121408353233272717465659291661235650468328080108166764367207616930172071083012960844719939719828601161706646323762114419168587889417102312
3935866315538860455667288871088123401338708254402460461585314778881017900018639924523425836653883808420317424429250884407914105834745168111329532767778430230949723732572042
3832773651010149331371
    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 8E 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
]] ]
]
]
```


MKZeZcBggYIKwYBBOUHAQEEdjB0MEoGCCsGAQUFBzAChj5odHRwOi8vd3d3LmNh...
-----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:
85028554818131771606984751484542866367797642544418673337005802720184322
92710791087926751618092569662327268032524279173400622376579666700276179
15568186854741401641272923666868388642211652421444905893521949303671676
15470109757643277175659581685712407264904976535479252324932718022612854
45850996001795706961663620912635572903286788233280697024972884304301443
34143355708400142358893408751830929680745420134947534487455039588528630
80961669688668764194047469284207541938356396473562367037083323363384965
27055109780991433741766982084286120115881754424031959717332618271322729
22823819168664881389748729780914665609345010942922994673889085021510899
27554617946763497012040472250327820209087408722859455597828052712653104
54237546716905573176296543324781659300489720426846078453130186703806233
333280531772842595216812443599715781199574005017229270661863107440254138
68877823259879804352244623294391749225231809528665716690917769518228565
53317225976072376538699004286389725812479294937009231104767127839161597
84170217068137018713683530750998162017677792002785055030917250157976662
38580761996381866275173134496438244444919098029651399335750270101567328
08661732276378744574973579661657536262685474601898821313464435123681310
24760940330634777134117781
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:
85028554818131771606984751484542866367797642544418673337005802720184322927107910879267516180925696623272680325242791734006223765796667002761791556818685474140164127292366686
8388642211652421444905893521949303671676154701097564327717565958168571240726490497653547925232493271802261285445850996001795706961663620912635572903286788233280697024972884
30430144334143355708400142358893408751830929680745420134947534487455039588528630809616696886687641940474692842075419383563964735623670370833233633849652705510978009143374176
69820842861201158817544240319597173326182713227292282381916866488138974872978091466560934501094292299467388908502151089927554617946763497012040472250327820209087408722859455
597828052712653104542375467169055731762965433247816593004897204268460784531301867038062333328053177284259521681244359971578199574005017229270661863107440254138688782325987
9804352244623294391749225231809528665716690917769518228565531722597607237653869900428638972581247929493700923110476712783916159784170217068137018713683530750998162017677792
00278505503091725015797666238580761996381866275173134496438244444919089029651399335750270101567328086617322763787445749735796616575362626854746018988213134644351236813102476
0940330634777134117781
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 1Cb.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 EAj-.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 E6B..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('....x]
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 68 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 40 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 ..2].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.l..=....;
0190: 12 C7 7F F1 F8 46 2F 09 78 97 C0 27 3D B1 3F 71F/.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 AB B2 r@...U./v..v9..
01E0: F4 7D A4 DB 00 42 7A A0 7B 8E 19 06 E4 97 CD 5BBz.....[
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-----
MIG2DCCBMCgAwIBAgIIldIuUDcMhMwDQYJKoZIhvcNAQELBQAwggEIMQswCQYD
VQQGEwJFUzEPMaGGA1UECAwGTUeUkLEMQ8wDQYVQQHDAQZNRURSSUQxOjA4BqNV
BASMXXNLZSBJdXJlZW50IGFkZHUJLc3MgYXQgd3d3LnNhbnVwYmlybWUyZ29tL2Fk

ZHJ1c3MxJzA1BgNVBAsMHkdMT0JBTCDSEFNkVVSU0LHT1BST09UIC0gMjAxNjES
MBAGA1UEBRMJ0TgYnZ0ZmJg3MRGwFgYDVQRhDA9wQVRVUy1B0DI3NDMyODcxGzAZ
BgNVBaoMEKFDIENBTUVSRk1STUEgUy5BLjEnMCUGA1UEAwweR0xPQkFMiENIQU1C
RVJTSUd0IFJPT1QgLSAYMDE2MzB4XDE2MDQxNDA3NTAwNLoXDTQwMDQw0DA3NTAw
N1owggEITM0swCQYDVQGEwJFUzEPMA0GA1UECAwGTUFEUK1EMQ8wDQYDVQVHDAZN
QURSSUQX0jA4BgNVBAsMMXN1ZSBJdXJyZW50IGFkZHI1c3MgYXQgd3d3LmNhbWVW
ZmlybWUy29tLzFkZHI1c3MxJzA1BgNVBAsMHkdMT0JBTCDSEFNkVVSU0LHT1BS
T09UIC0gMjAxNjESMBAGA1UEBRMJ0TgYnZ0ZmJg3MRGwFgYDVQRhDA9wQVRVUy1B
ODI3NDMyODcxGzAZBgNVBaoMEKFDIENBTUVSRk1STUEgUy5BLjEnMCUGA1UEAwwe
R0xPQkFMiENIQU1CRVJTSUd0IFJPT1QgLSAYMDE2MzIiCiJANBgkqhkiG9w0BAQEF
AAOCAg8AMIICGkCAgEA0GvnniIrU3YVVA9MSsBta/v5hEQFoX1gzXsnphz+LuE
BzH3/z1rx35WbMkLXJaw0/FeWx7rMRy/d1cwV08excEsurb5or09CiEyLBILSyW
bfsiqDw0vt5wFRD5ZKFGfQBDZD+NSv0AMc+TgH6a26Wvj2ws/07vHHncD6JuhFwi
iQ5ELKio1HPs0TKRH0IUVX1L5nL+W+dUdS99DuLgymkuXqIO1eiF3j9rf6WCsEz9
XZ5xuhS06+3HwhRkDFhuT5U2YTZFYDZnGeUvGj5YrIsmHiXm+pUA+60SnoSYb4a
3qZ86av/155JckL8u0UR7D9w/BnEmuqXbqzK0AQ74T8BKHGj4q5DZHgWmQJav9Fe
77w31cNYgUGG5LkMAKwImJjrcedYmWgx3u3iSTXz0rNX3MRcn/0879D1KzLuYa56
4cd6Pw0XMGwCrInWw0ScKcCEI64IDYzyoAraH82dWUv+MPa/3Gi/02bd9wZ+vHI
tgX85XCSqcdjLuAaVvU3LjLmrUDwK22rvGZe0u1i07eZatkfL1up80KmbnF/DwT
CEU+35/7x32x0II2FD3AYwABZStk8Jk7HLf4XbkXPFiTFa+o9SUGy0jPRI8Qusv
XUK08jCoJvrm+vdpbb4mWPwPp/ek+LNUwxyMYU2cY7909bMDXLJY1LiVeoM5UC
AwEAAACMEAwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFQUG6JvNfoZim3pNjACX
OYXPHHiQcDowDgYDVR0PAQH/BAQDAgEGMA0GCSqGSIb3DQEBwUAAICAQ87/SrD
yxspAhAJresusytt2Uug2zWY9Y8Cp9NCC00rg7V3R4hGhd3Rth59mBuMcb6qyPDv
xmotVphS6Ja3+9XqAN/+5iLkP7k+ZUR1w4q/i3eJw2pX+rzI4RDe8dqFJ/HtB//V
wkLUomEv34hx4zTmZ25bxnoZ6znv8+oEqHRpTIC1/K29Dj0y08oJ4LK3eJzuldN
uoopwZnhdbm59nhnd7w9s+hGTT8TzwoCyCMrZI44M+d79nlcGimXhCQ/cDTRNX
b91x3Rbz+3k4G2KapM1eUNARIJCKIpir2kZ6TDTRSN3ZzNmV1VAXZdJlndFex0i4Y
sK6snz8u6x+ynM20+Nt4jtQzG60TMwt/7VJy4vPKG/J+VRPA06hugu+uHQJYTj
FvyMjSTjZMwqjLJgU59ZkkUJlFuoEIIuy3fyjpwKRHLPhbfelR0Krv0mtj15Zj1N
vH4yQ13b4Gw1KGm6fJ4ySo/qerA9F139PvobBPgQNXjM7cH2Lb9r0u/pn8Bb+q+
etEx5wY9rYSr7DvxEsd/8fhGLwL4l8AnPbE/c50LGqdc5hYLDiZNU05Wp1Kk0Amv
5QX+f84/vvzm5EqUJ+VTxI906wJXvM60K613U3JAU4UwVRkvg3aVo3Y5qLL0faTb
AEJ6oHu0G0bbk181bPTq0XMBPhzJmwiFhJsiZQ==
-----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:
66233813355793209508805012111802303500444221251315963860144226472236482
38515862776832273621181213258343271393126504662516958467793728566159000
44134647016604824853754408671056099205270425954594898365088019396681928
07250330135988270509141015177838083452095853799410959759953975720976976
86019020160558925391152517947537597189685751139829656831664883753424177
43984736398122768058765393633470875869480169449650697759505389606455491
55410644200938097288915793112866047967822857596336726703358834798286132
35776043278901617806302682206547270628311240953864656032032037659654913
91582936745966492664474737082892979481732445448303967475390384717533457
96298803219387129100029382166731999926670418074391353923672781309379052
84681666886073572895181044611699674821454753350908041356299439597861571
48942949404879416722036983889317932583772584309907503636866438949090572
75633989303815501761888823424907298086548148333615739348258214788123827
53455999145611981828537876391242755502440812339210301606382514791125567
24428493037981100192885424939797457659686090864488811619957009850923816
17339831467580557702065444338286647595714795449342657670242547018976013
37195835625748319870706793560253041145444514645171234325627029591709535
48868653099760080469697611
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

04820138308201348014b76a026d2cd9b036b32b6c05aa345e06edb2b99ba1820110a48
2010c30820108310b3009060355040613024553310f300d06035504080c064d41445249
44310f300d06035504070c064d4144524944313a3038060355040b0c3173656520637572
72656e742061646472657373206174207777772e63616d65726669726d612e636f6d2f61
64647265737331273025060355040b0c1e474c4f42414c204348414d4245525349474e20
524f4f54202d203230313631123010060355040513094138323734333238373118301606
035504610c0f56415445532d413832373433323837311b3019060355040a0c1241432043
414d45524649524d4120532e412e3127302506035504030c1e474c4f42414c204348414d
4245525349474e20524f4f54202d2032303136820826f4aa13f0560872

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:
66233813355793209508805012111802303500444221251315963860144226472236482385158627768322736211812132583432713931265046625169584677937285661590004413464701660482485375440867105
60992052704259545948983650880193966819280725033013598827050914101517783808345209585379941095975995397572097697686019020160558925391152517947537597189685751139829656831664883
75342417743984736398122768058765393633470875869480169449650697759505389606455491554106442009380972889157931128660479678228575963367267033588347982861323577604327890161780630
26822065472706283112409538646560320320376596549139158293674596649266447473708289297948173244544830396747539038471753345796298803219387129100029382166731999926670418074391353
92367278130937905284681666886073572895181044611699674821454753350908041356299439597861571489429494048794167220369838893179325837725843099075036368664389490905727563398930381
55017618888234249072980865481483336157393482582147881238275345599914561198182853787639124275550244081233921030160638251479112556724428493037981100192885424939797457659686090
86448881161995700985092381617339831467580557702065444338286647595714795449342657670242547018976013371958356257483198707067935602530411454445146451712343256270295917095354886
8653099760080469697611
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 [

Public key Sun RSA public key, 2047 bits
modulus:
15565749306815017290572910947913251485658394816871391150519718224752092
68062858659048834366990073975612048779674255897336661658525739042980763
96962976353445306837806698655728708292472338989005934885983563402612261
83154176055624147148998129032292188368010388116242523363115157164130163
43176123522599137408629429484799643338581635645863414670014191985157325
86393279366017314962554998063803944333549469215466510981194042445206770
51782788353164428264902673736604837858615396404885079624196345816148593
32812610429024079594383730463692359849025706062513980948184969165681176
2786684599386086620094356515750413986592521031619
public exponent: 3

Subject key identifier bebc08d42eba004c80dc2667b4a5d8ddc34a1af9

CRL distribution points http://crl.camerfirma.com/racer.crl

Authority key identifier 0481a030819d801470c195fa5da516be62e8a47de3d4645fc4e13e9da18181a47f307d310
b300906035504061302455531273025060355040a131e41432043616d65726669726d61
205341204349462041383237343332383731233021060355040b131a687474703a2f2f77
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:
    15565749306815017290572910947913251485658394816871391150519718224752092680628586590488343669900739756120487796742558973366616585257390429807639696297635344530683780669865572
    87082924723389890059348859835634026122618315417605562414714899812903229218836801038811624252336311515716413016343176123522599137408629429484799643338581635645863414670014191
    98515732586393279366017314962554998063803944333549469215466510981194042445206770517827883531644282649026737366048378586153964048850796241963458161485933281261042902407959438
    37304636923598490257060625139809481849691656811762786684599386086620094356515750413986592521031619
    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
```


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:
81284016177492937202320232025436159637081994026606318711127070241253905
04084461364349133993237238036152518962612715445428815793613146380840620
84365494748422357768833502551514246563892881865862767293219279536553187
59960476792490398293700392904112577326137518314833351094324711025952389
31706006101858776661989243595995350818771109060091268835611938653864311
13344968966492944286772952245359708016130344884052808736697184175916484
68431928332660103085811501195086662786618900268175126553015636724393939
71547161474745940211878830704155163500155642854228499704923621912620547
91493328331683798249293385428900382717825303703888456351014803341347480
08788865762832624148466063682815814716638875023681782789523842034367645
21525268419774793878311750837832894984701323565463743911977123083857951
66156770905780176436573036685538170554554245844954411691170876494787381
71993921649802111234232925139137446675796841256636185949238148711372254
01634432613901431934131968198214062046647827712560273526591040983745668
01900391190760312860735946806991841638115636577630509406264370541940480
56726969236881596001442492154885059881329841653295334867946607008713427
58322613311675455507630211003007965277044950083254285712026467455760716
34116071969511066445575011
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 e0afb2c0ee95a68cd9a3c590b2d3fe07c0a6d0be796ae5291e424d47792178e

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:
81284016177492937202320232025436159637081994026606318711127070241253905040844613643491339932372380361525189626127154454288157936131463808406208436549474842235776883350255151
42465638928818658627672932192795365531875996047679249039829370039290411257732613751831483335109432471102595238931706006101858776661989243595995350818771109060091268835611938
6538643113344968966492944286772952245359708016130344884052808736697184175916484684319283326601030858115011950866627866189002681751265530156367243939397154716147474594021187
88307041551635001556428542284997049236219126205479149332833168379824929338542890038271782530370388845635101480334134748008788865762832624148466063682815814716638875023681782
78952384203436764521525268419774793878311750837832894984701323565463743911977123083857951661567709057801764365730366855381705545542458449544116911708764947873817199392164980
21112342329251391374466757968412566361859492381487113722540163443261390143193413196819821406204664782771256027352659104098374566801900391190760312860735946806991841638115636
57763050940626437054194048056726969236881596001442492154885059881329841653295334867946607008713427583226133116754555076302110030079652770449500832542857120264674557607163411
6071969511066445575011
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 8FRvu.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 8FRvu.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

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

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:
75310184052750510706735433484210147071584424475948754552995700299529711
64845105416519833197852497654307285787624233888137661295438003597451032
86110634819233766872289298164900372687825828827831445369456816283569648
62110510927676547615729161669630919649851175675297256727463692957850331
96331126500335066974745814142902682643269078172703759499850282526536529
00791893701928790453666290708708059265615029231671707180844958746989897
80380522580646135798080363964154007038320861975644561772145390072945255
94276473411597127730766583528397260701138212410008577206486054276905689
24794945635975937418316324384761717599145720943399406972457988391349815
88852214389561441386062826168397170545774163844674737396559899034390572
03142313941164187484030100814671690299901449807290851434155358348909127
46247044673032664609824760155577046414296044054203106506369884626119908
79222687410533332824408275071208256965610956986697528820582378690629174
48445512570781555796127663306927036915923996652297574480233632754031075
16708657410037603202806326407243044087845992430610769753162537771252303
45569800213351675331931942625338094502666433041389310512783116972573879
59029778405190293627705120973943047777160963418144588529734365781729066
82383307958725792986473563
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 464bbeebc557b5eaae5ddb01dd1c816cec471256553da73f604be09c476067e8

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:
75310184052750510706735433484210147071584424475948754552995700299529711648451054165198331978524976543072857876242338881376612954380035974510328611063481923376687228929816490
03726878258288278314453694568162835696486211051092767654761572916166963091964985117567529725672746369295785033196331126500335066974745814142902682643269078172703759499850282
52653652900791893701928790453666290708708059265615029231671707180844958746989897803805225806461357980803639641540070383208619756445617721453900729452559427647341159712773076
65835283972607011382124100085772064860542769056892479494563597593741831632438476171759914572094339940697245798839134981588852214389561441386062826168397170545774163844674737
39655989903439057203142313941164187484030100814671690299901449807290851434155358348909127462470446730326646098247601555770464142960440542031065063698846261199087922268741053
3328244082750712082569656109569866975288205823786906291744844551257078155579612766330692703691592399665229757448023363275403107516708657410037603202806326407243044087845992
43061076975316253777125230345569800213351675331931942625338094502666433041389310512783116972573879590297784051902936277051209739430477771609634181445885297343657817290668238
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 9E 8F ....Rvu.IJ o[p..
]
```

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

```
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..6#...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 ..0..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.%w0...*'.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 00 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
```


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
3706691568906294360163347575652841328374320165467
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:
26168245373349582101216451831842430467040508106906591062594362181961089866544047356607386503984170151271111849561019273165849598781730137218709085057337552468422859171944067
44771115793395547754260870335562673333691529610889880948284741500937726426307342775429770119561692648230366727273384555166046201536162261294646114414424552984781652869757584
55396845488581301363532004406998187793220022540657369120212192431274090846096892261077523954208225402291426488591241275654659289710773093508150865584148160822317863218345099
85483665798528336906343913499355264079013544379873706691568906294360163347575652841328374320165467
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.0c.
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 .<0.
]
]
]
```

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

```
[3]: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
  [DistributionPoint:
    [URIName: http://bmcertcr1.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://bmcertcr1.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$....=u.7w(
0040: 93 56 35 42 DD F2 FF B1 78 90 0A B7 4F BC 9B 42 .V5B....x...0..B
0050: AE B8 CA FD A4 0A F4 05 B3 B5 2C 51 F0 02 96 15 .....0....Q....
0060: 1F 4C ED 23 F6 4C 39 54 32 92 24 A7 0E F6 8B 3E .L.#.L9T2.$....>
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-----
MIIFPTCCBwAwIBAgIEV0cWzZANBgkqhkiG9w0BAQsFADBBMQswCQYDVQQGEwJK
RTEPMA0GA1UEChMGQk1DRVJUMSIwIAYDVQQLEwLDXJ0aWZpY2F0aW9uIEF1dGhv
cm10aWZpMRcwFQYDVQQDEw5CTUNFUlQgUm9vZCBDQTAEFw0xMjYxODI0NDJh
Fw0yMjYxODI0NDJhMF4xCzAJBgNVBAYTALBFRMQ8wDQYDVQQKEwZCTUNFUlQx
IjAgBgNVBA5TGUlnRmZlYXRpb24gQXV0aG9yaXRpZXNkGjAYBgNVBAUTEUJN
Q0VSVCBjc3N1aW5nIENBMIIIBIjANBgkqhkiG9w0BAQEFAAQCAQ8AMIIBCgKCAQE
z0rc43389Em/+TXSASV2ydpJvqj3A3dy2UMEA2n7LTAT50nkAZr4/vxQWZZD/Sbp
MPU+Hh061W/REx+4/uvqx755KrP0dy8vrs5BmHI+HLvFWLntEo9AFQU01RA/
8Mn5ANMY+FQUhdnXjH76iw36PWER3Lb9nI7EuVao0oqhH/Jwe2FaEVE8iSR15
TXCbcxfXZC4ixaILLud+JfFl7pzc1LnHt0RgnJNL+UwLoFnDSQ5jsjUF+/EZGn5
mGwLAtOI+A/ebY56eAKasVaBe1PqPOUyLtGq9FNpIU7mQosZcn6dHY/zpLi f6PJE
7NnNxAS5Mgkzzw7MX0d9yWwIDAQAB04ICBDCCAgAwDgYDVR0PAQH/BAQDAgEGMBIG
A1UdEwEB/wQIMAYBAf8CAQAwPAYDVR0gBDUwMzAPBg1ghkgBhvprUgDCiCBMA8G
DWCGSAGG+muBSAMKJwIwDwYNYIZIAYb6a4FAwonAzCBwYIKwYBBQUHAQEgEYow
gYcwUgYIKwYBBQUHMAKGRmh0dHA6Ly91bWlnLnRjcmwubWfuYwdLZC5lbnRydXN0
LmNvbS9BSUeVQ2VydhNjC3N1ZWR0b0NjQ2VydhFjY3b3RDQ5SvN2MmMQYIKwYBBQUH
MAGGJWh0dHA6Ly91bWlnLnRjcmwubWfuYwdLZC5lbnRydXN0LmNvbS9BSUeVQ2Vydh
Hw5BuTCBtjBAoD6gPIY6aHR0cDovLzJtY2VydgNybc5tYw5hZ2VkLmVudHJlc3Qu
Y29tL0NSThMvQk1DZj0Um9vZnENLmNybDByoHCgbqRSMGoxCzAJBgNVBAYTALBFR
MQ8wDQYDVQQKEwZCTUNFUlQxIjAgBgNVBA5TGUlnRmZlYXRpb24gQXV0aG9yaXRp
ZXNkGjAYBgNVBAUTEUJNMQ0VSVB5SVCBz290IENBM0QswCwYDVQQDEwRDUkxwMB8G
A1UdIwQYMBaAFBKa2aqF6UHtvtZ8InuiXy0pG+VMB0GA1UdDgQWBBDrr//T/EIR
dYjorXhPT2P8IY/4SDANBgkqhkiG9w0BAQsFAAQCAQEABoBovGw/Lc6ktMOYw87z
NcJcvsNh/VUz0n4ozPLGkD8Pe5DRk/oAPx6fLnMwCewDKQMItdpdQUXVc9Td3
KJNWNLd8v+xeJAKt0+8m0KuuMr9paR0BbD1LFHwApYVh0ztI/ZMOV0ykiSndVal
PhHkiCrFk4ZLDUglnM4Hntmt7gyn8tqTm3BfReW9FbCv5wp5xaJnt+hcWZMu/os
Xa1er+Yfdw0d2aM2IV0HTMS14M+srZbWp69nW2kYRMBkym0bpJGAC2BbsNke
Roo05hhbh7xR8GB7XbRaFF67leK0nLXrDpufcnkyWACb9CAH91WCSY76RojE3N3
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
3138876463282355155511394404171976609915145925937
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 .....<0.
]
]

[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 98q.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 1bc.....
00a0: 1f 7c 8c b5 88 b6 09 f7 89 84 61 52 d8 dd 35 f0aR..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 d1l.!.....\....
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-----
MIIDdjCCA16gAwIBAgIEV0cWLDANBgkqhkiG9w0BAQsFADBBMQswCQYDVQGEwJQ
RTEPMA0GA1UEChMGQk1DRVJUMSIwIAYDVQQLEjLDZlZ0AwZyZ2F0aW9uIEF1dGhv
cm10aWVzMRcwFQYDQ0QDEw5CTUNFU1QgUm9vdCBDQTAEFw0xNjA1MjYxNTAwMjla
Fw0zMDEyMjYxNTAwMjlaMFsxCzAJBgNVBAYTALBGMQ8wDQYDVQQKEwZCTUNFU1Qx
IjAgBgNVBAStGUNLcnRpbm1jYXRpb24gQXV0aG9yaXpZMmFzAVBgNVBAMTDkJKN
Q0VSVCSb290IENBMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApy80
SAFzMGYPVWU1s+ybv7L0nBgXAbQ+SKDbuGj2o4orW+VysGbdgXjWhZcVkweeQjb1
HYBd1vEgqCgK0WYfKPFb6nyt6JX4J+edqtcFHFNn6z2sQUumzwb9ZwC7QF+NxQNO
ca007w3tinoHcZffTnLCByJQf68k0unztimLQHU+tmTc8HF/DKvb0uThCTqghez
PZFTuA3d1EcdE+9eN6KKtgumtj74i45+k3/FE6padP9yhrksUpGBkljxg/Wj77BT
GMPEZBbQ7MtnJ0TJu6e1hRxhAR+yz6L8JZH2mdV2/vgLDLPeIUqPhe77bcok14bU
jPzq91nMAqfu6rG1MQIDAQABo0IwQDA0BgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/
BAUwAwEB/zAdBgNVHQ4EFgQUePrZqoXp0e2+1m3wie6JfLQ8b5UwDQYJKoZIhvcN
AQELBQADggEBAIFDDIWEiRXCJ5KNBW45YCiCADQeQZ51PTpboDu+HtkIqUFU59qf
oen5qWg5LZ3+JGc49BoTVwsbEvos8WFX8V9Nh2y51v/b9Q6aKa0ldoYIReoUL2Ry
azfbqJ2ZCAvL1CzULrBxuw0Wv604GhzIZh6bqb8LI/MTk0MSy4Ly7/LecVJYXhx
P0d01dnL8yrNXX3y4M4ULHtjxtbf5qYJERSffIy1iLYJ94mEYVLY3TXwKqFD/que
J2yqeM0ow8zKqQx9yhF3iH1AqubXP2gG9F/iFbdG5tzBNTRvq90gN15vy10B7ti
ExqEgjbZkpGoU92gNsFjUUoU/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:
86081472563693180999345410541014761661204443670584317242235052258266857
35073551167114886917925116463171611686531507489943653191609174672790241
12706760658395806619009237844324461480547667749686040406283452557728069
13432834752114339164271109016826017684659756921721726362377046522422706
71759644360683976163427178303165123271240082568266485125667779962194741
53589483926945247509023767760903711417784607185612852621547032158194375
36977213714149792817680799103705141971225372128994418667723502361955579
24088497716488428342062960538346191883206439116051570557295577047337699
44524841701464491318369058789003250622646476591932046735627151011868823
47778757715819801749502454178790971736602711498610005656410926214484719
73511792788370385209433224502973180716389135788172190168224983672333241
76940502743363633717889882925059543705323321433347106457068575173377347
19114195423899301716637043755184283453528982900471282769980361055140997
81523224066442394255190326055169014882557689635910597022183345590147365
9873657564719053945325181809844266677192214743070218878507776568472410
70492365505284103379231569119800053875456755957848629240689999599295604
17398564953557583967174394733549408849031713875728327558580389421577423
82445878547444263756509591
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:
8608147256369318099934541054101476166120444367058431724223505225826685735073551167114886917925116463171611686531507489943653191609174672790241270676065839580661900923784432
44614805476677496860406283452557728069134328347521143391642711090168260176846597569217217263623770465224227067175964436068397616342717830316512327124008256826648512566779
96219474153589483926945247509023767760903711417784607185612852621547032158194375369772137141497928176807991037051419712253721289944186677235023619555792408849771648842834206
2960538346191883206439116051570557295577047337699445248417014644913183690587890032506226464765919320467356271510118688234778757715819801749502454178790971736602711498610005
65641092621448471973511792788370385209433224502973180716389135788172190168224983672333241769405027433636337178898829250595437053233214333471064570685751733773471911419542389
93017166370437551842834535289829004712827699803610551409978152322406644239425519032605516901488255768963591059702218334559014736598736575647190539453251818098442666771922147
```

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

430702188785077765684724107049236550528410337923156911980005387545675595784862924068999599295604173985649535575839671743947335494088490317138757283275585803894215774238244
5878547444263756509591
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 80 91 9D 75 90 0D0f....
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...=.k5...
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!...0@.
0060: FF 78 99 93 E7 B9 27 7B 77 89 E0 5B 9A 53 39 46 .x.....'w..[.S9F

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

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.

The certificate in PEM format:

-----BEGIN CERTIFICATE-----
MIIBjBCCBu6gAwIBAgIBBjANBgkqhkiG9w0BAQsFADCCAR0xGDAWBgkqhkiG9w0B
CQEWcWVhOQdZSS5jBzEwMCA4A1UEAwNrR2xvYmFsIENlcnRpZmZlYXRpbi24gQXV0

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 04183016801447a00c09878f6a3841d3beaf7fa2e6143a81bfa0
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
9555779043009623245457108586157810404281017634307209615547571234828538952321152605257523752263392643319453578313851858639994466486933082405912652602925304500166841338409659
31954419498756829065806392203680239126800266036716767407595758072636041149554000435853709442393723751760315567207800264035457220159580970301962726298300098498752185286614577
5995027056218417169350725318160884871317671000784008583495273202691394403365445539333649563859348478380287803355516627239116725091216859313381312649014620377814849966952622
09553189689637888165150363561047646158370062584548327817642544825103635595013018381733213559958582207727269864026438706723572245215472753466935689948625003612384518568787842
71497930371006268452613461393118899418221555617312332241918777159662806068093396013797842914847905179811158339038742046641298975012237417859428757763660121112346320189786847
928865698716888911224327426183856696105937197878521616304164346786605630564654449174654159341234326474080036038465562936762043879526285396090615692782542873365656295922398077824716955641695122189
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 [

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

```
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.....0I=.....
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 (...%.%$%n..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 18 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.0..n.0.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 D9 D7 9A 55 CC 0A B1 .....zU...
0170: 35 99 B6 46 91 14 9A 07 09 83 AE 8F 87 0A F2 16 S..F.....
0180: D5 EA 3B 9F 6C 52 2B 4E AA EA 5B 15 E9 84 2B 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
```


Service provider PE
country (en)

**SERIALNUMBER=20562999711, EMAILADDRESS=info@accepta.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@accepta.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@accepta.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:
27060710516406163684509599022390553214999726795320603730344522040861084
19865119532756953401695749776674307836671376751646091086823245066604205
77580234855404301466315237663560050623656225320650421665373706928828854
98406869142817508701385306863713330787351431311086884219662492646670810
86700049532334142035386889250019819328411796620488837500676783884062428
14887423125302695375590254501351784470800476986597899246865858276570452
92967523951599313634040064058175250320816664775846892320689092179394977
41015758688917068352176937969407040886364313699883617931951041650479403
0051222900099358123009452817055477530094255864171
public exponent: 65537
Subject key identifier e5ea517d8f5e00f4de965ee4aae0325408b49d6f
CRL distribution points https://acpev1.accepta.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@accepta.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:
27060710516406163684509599022390553214999726795320603730344522040861084198651195327569534016957497766743078366713767516460910868232450666042057758023485540430146631523766356005062365622532065042166537370692882885498406869142817508701385306863713330787351431311086884219662492646670810867000495323341420353868892500198193284117966204888375006767838840624281488742312530269537559025450135178447080047698659789924686585827657045292967523951599313634040064058175250320816664775846892320689092179394977410157586889170683521769379694070408863643136998836179319510416504794030051222900099358123009452817055477530094255864171
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@accepta.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 .....
]
]
```

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

```
[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@accepta.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.accepta.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@accepta.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 .accepta.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...ACCEPTA 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.accepta.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..+...;+..
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.s.i6..IZ]&
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]V..
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-----
MIIGWTCBUBGgAwIBAgIBAZANBgkqhkiG9w0BAQsFADCBmDELMAKGA1UEBHMCEUEX
GzAZBgNVBAoTEkFDRVBUQSBQVjVIFMuQ5S5LjE2MDQGA1UEAxtQWNLcHRhIFB1
cnUgQXV0b3JpZGFKIENLcnRpbmZlYWRvcnEgUmFpe1AtIFYxMR4wYAYJKoZIhvcN
AQkBFg9pbmZvQGJfZXB0YS55j2b20xZDASBGNVBAUTcIwNTYyOTk5NzExMjE0TE4
MDQxODEINTQzMV0xODM4MDQxODEINTQzMV0wZSx0CzAJBgNVBAYTAEJmRswGQYD
V0QKEzBQ0VQVEEgUEVSVSBTLkEuQy4xOTA3BGNVBAWMEFjZXB0YSBQZj1IEF1
dG9yaWRhZCBZDZj0aWZpY2Fkb3JhIERpZ210YVwglSBWMTEmBwGCSG5Ib3DQEJ
ARYPaW5mb0BhY2VwdGEuY29tMRQwEgYDVQFEwysMDU2Mjk5OTcxMTCASIAwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBANZcs9AEht7/DL/Cx18GkHyLyPEE0LIq
FbtvLmb765GfNrwC2+bnNCxp2w0eGfY0mNZ655m0L7Nu9Zxc09vphGCLXVEW0eg4
JBJPUOMx2Xh+npzNGyJ0UpDMF/0W7f5b5s6b8a0w62LzLITX0e1hpHzh9JL00Z5
s7Z1D0FfrKMDJTXNEo16zJ9Q2+ZZusrwD+bW6E6AXyC4RpRoRGtpmNzF8mqnLWL
IcTy3H69lnn9f340y73+rfaAj+fIXGxT04TwrgSHj7qcLR0eg09MGoBGATF8qYfG
HrL6w9X/fnS314U7noCCZhdRfWHy4voSQWPOJuEdeF8JCR+GmNTJ+WsCAwEAAoC
AqwgGkjmA8GA1UdEwEB/wQFMAMBAf8wHwYDVR0jBBgwFoAUFagNaHs4Jp3Lm4JI
ngzZTD0H0wHQYDVR00BBEYEF0XqUX2PXqD03pZe5KrgMLQIT11vMasGA1UdDw0E
AwIBBjCCAUEGA1UdIASCATgwgGE0MIIBMAyIKwYBBAG1awEwggEiMDcGCCsGAQUF
BwIBF1todHRwczovL2FjZGV2MS5hY2VwdGEucGUVj1BTLVBFVYxLUFjZXB0YXB1
MIHMBGgrBgEFBQcCAjCB2TAZFHJBQ0VQVEEgUEVSVSBTLkEuQy4wAwIBARqBu0xh
IhV0aWxpemFjaW9uIGRlIGVzZGUgY2VydG1maWNoZG8gZXR0YSBzdWp1dGEgYSBs
YXMGcG9saXRpY2FzIGRlIGVlcnRpbmZlYWRvcnEhChDUCKgeSBwcmFjZGljYXMGZGUg
Y2VydG1maWNoZ2Vub3JpZGFKIENLc3RhYmxLY2LkYXMGcG9yIEFjZXB0YSwgeSBk
aXNwb25pYmx1cyBwdWJzsaWNoWVudGUgZW4gd3d3LmFjZXB0YS5wZS4wXAYDVR0S
BFUuU6AZBgggrBgEEAcEBAQANFgsyMDU2Mjk5OTcxMaALBgggrBgEFBQcIA6AZMBCM
CzIwNTYyOTk5NzExMjE0TE4wYDVR0jBBgwFoAUFagNaHs4Jp3Lm4JI
MF0GQYIKwYBBABAgGgDRYLmJ1A1NjI5OTk3MTGgJQYIKwYBBQUHCA0GTAxDA5
MDU2Mjk5OTcxMQYIKwYBBABAgKBD2LuZm9AYWNLcHRhLmNvbTBBCBGNVHR8E0zA5
MdegNaAzHjFodHRwczovL2FjZGV2MS5hY2VwdGEucGUVj2MS5jcmVwUGVydVJh
aX0tVjEuY3JsMA0GCsG5Ib3DQEBCEUAA4IBAQA5RA2ztKzaEcq64VTYmtVigPgh
JJ0NKzblgtEKwBt2r0rmngd4GwFh8aneMMQRcyRiOC1/8EF7K6+gvcLjVhgTY
F6oppbx28Ln8JWt3I5L8YfVQ8J1tyuQjjsriezPq5THJRpaCV1HM/+aivrLmTt
YfY41hcFVR8BLxrvG0+BQmz0GwVDbQ1L617eUjEoh951Gm8c2k2pcBJWkomTvtw
QqAXqhZYrC0mU4AdsZ3StQ1Vwp403MLOV16X55VYrFoaDoBsXp7cHM7lsFhrLz/
4UqsRkUehzLcaLanfacNnsP0vYo/8cfhrbmSUPRrmV3LgGwv0UNU72VoIBc
-----END CERTIFICATE-----

SERIALNUMBER=20562999711, EMAILADDRESS=info@accepta.com, CN=Accepta 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@accepta.com, CN=Accepta 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@accepta.com, CN=Accepta Peru
Autoridad Certificadora Electronica - V1, O=ACEPTA PERU S.A.C., C=PE
Public key Sun RSA public key, 2048 bits
modulus:
18493053405112159223141683140649822647045430781071541207896464502129405
69240030912358349289780774165889458791259256710248413694603276935961540
25880057040616486553243899896428705193964091980283102784920695537713345
66053078041459022618488488117268381313061480603645251319413752589918038
57770569463482986669187776761868814317422652328599838092690023365388446
19466521660010956817127220618635897907739999095450623481684699324439605
86077218537800875969623803758744737471326684611908703590961198493012348
50075817728314106523422674841407469754271796423212420041475739039947490
8845099554448971134206225281639605017973989997787
public exponent: 65537
Subject key identifier 812552bdb3aa8da1fc59463ac9e3ac36ce6ef3
CRL distribution points https://acpev1.accepta.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@accepta.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:
18493053405112159223141683140649822647045430781071541207896464502129405692400309123583492897807741658894587912592567102484136946032769359615402588005704061648655324389989642
8705193964091980283102784920695537713345660530780414590226184884881172683813130614806036452513194137525899180385777056946348298669187776761868814317422652328599838092690023
36538844619466521660010956817127220618635897907739999095450623481684699324439605860772185378008759696238037587447374713266846119087035909611984930123485007581772831410652342
26748414074697542717964232124200414757390399474908845099554448971134206225281639605017973989997787
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@accepta.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@accepta.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.accepta.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@accepta.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 .accepta.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...ACCEPTA 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.accepta.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 78 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_].R.z0r
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 E8 E4 CD D2 34 3C BC A7 43 0A B4 074<..C...

The certificate in PEM format:

-----BEGIN CERTIFICATE-----
MIGTCCBUBwAwIBAgIBCTANBgkqhkiG9w0BAQsFADCBMDELMAGAKA1UEBHMCEUeUx
GzAZBgNVBAoTEKFDVRBUQSBQRVJVFIMuQ5S5DLjE2MDQGA1UEAxMTCWNNLcHRhIFB1
cnUgQXV0b3JpZGFKIENLcnRpZmZlYWRvcmluZmFpeAAtIFYxMR4wHAYJKoZIhvcN
AQkBFg9pbmZvQGZjZXB0YS5jb20xZDAsBgNVBAUzIwNTYyOTk5NzExMjE4MDQx
MDQxODQxMjE4MDQxMjE4MDQxMjE4MDQxMjE4MDQxMjE4MDQxMjE4MDQxMjE4MDQx
VQQKEjB0b3V0VEEgUEVSVSBTLKEuQy4xPTA7BgnVBAAMTNEFjZXB0YSBQZXJ1IEF1
dG9yaWRhZCB0ZXJ0aWZpY2Fkb3JhIEVsZWNOcm9uaW9hIEN0VjExHjAcBgkqhkiG
9w0BCQEDW2luZm9AYWNNLcHRhLmNvbTEUMBIQA1UEBRLMjA1NjE5OTk3MTEwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCSfjkmJ7sbyu0B0Lvnwrjtpz10
SjxY0xoCYpjwsq6KBagBBUyQY2FbrtWTQXMFHPASREC+LHu2mdNcAgTFQbl4oMmX
0LwaT65H8VU/7oiwh1Vh9lC9uExz/FAJp1mto+J85fnt6iqCnpU5rdTWTHiI0tMq
apTTd2P9t4d0v7/M/30fBialXR1DM+JJ1iYb0hEqIMKHBQh6VZHZ8wRSFIAMIzi
ETrblXgtuuoEFigICU6PyTyMt0gZevCLG07ULNjNK1EJ9A7Kren1ZdUy7/0PPn
zBJ50/0d6hbgNBPJUbdDedMP7t07RVcWNLwcbUtnFddftadyPc060vonzbAgMB
AAGjggKnMIICoZAPBgNVHRMBAF8EBTADAQH/MB8GA1UdIwYMBaAFH2oDWh70Cad
5ZuCSxsc80w6B0MB0GA1UdDgQWBBSBjK9s6qNoFyWUY6ye0Ns5u8zALBgNV
HQ8EBAMCAQYwggFBGqNVHSAEggE4MIIBNDCCATAGCCsGAQQ0BtwSBMIIBIjA3BggR
BgEFBQcCARYraHR0cHM6Ly9hY3BldjEuYWNlchRrLnB1L0N0Uy1QR51WMS1BY2Vw
dGFWZTCB5gYIKwYBBQUHAgIwgdkwGRYSQUFUFBFUUGUy5BLkMuMAMCAQEa
gbtMYSB1dG1saXphY2Lvb1BkZSB1c3RlIGNlcnRpZmZlYWRvcmluZmFpeAAtIFYx
IGFg6GFzIHBvbG10aW9hYkZSBjZXJ0aWZpY2Fkb3JhIEhkgcHJhY3Ry2Fz
IGRlIGNlcnRpZmZlYWNpb24gKENUQykgZXN0YjZsZWNPZGFzIHBvc1BBY2VwdGEs
IHKgZG1zcG9uaWJsZXN0YyY1bG1jYw1LbnRlIGVvIHd3dy5hY2VwdGEucGUuMFwG
A1UdEgRVMF0gQ0YIKwYBBABBAQgDRYLMjA1NjE5OTk3MTEwggEiKwYBBQUHCA0g
GTAXDAsyMDU2MjE4MDQxMjE4MDQxMjE4MDQxMjE4MDQxMjE4MDQxMjE4MDQxMjE4
HREVBTV0BkGCCsGAQQ0BwQBoA0wCzIwNTYyOTk5NzExMjE4MDQxMjE4MDQxMjE4
FwwLMjA1NjE5OTk3MTEwggEiKwYBBQ0BwQEG9pbmZvQGZjZXB0YS5jb20wQgYDVR0f
BDSwOTA3oDwGm4YxahR0cHM6Ly9hY3BldjEuYWNlchRrLnB1L0N0Uy1QR51WMS1BY2Vw
cnVSYWl6LlYxLmNvbDANBgkqhkiG9w0BAQsFAA0CAQEAzougk0pLAPDgne7dsy
KJT6ymctA+29TLyLnEhwLPQ/9BJdgpAYb0vpS7tuLwCkfx3XFLghHD3dtI0mpZ3c
Mdcy1t0R605M5617D9Z1RR6BN8XFL6BgrHW30scaGmRTaws9mtxv6gVXZ5HKY5m
Q/6R2Vt1ZFHbc0sX+TvJ4kpDkj2PB5KoBTcUwjpkSkmR7as0yNSC0m/+4nkXkGm
SxpcxcckFkpm3HXhrM6RNHiZag6FAGC/gnbKiwBbzFV5rLC2cAw4TL0j00DKKQ
KISzj7wX0qqoufnUr56UXIJJ6enNokbtnacd0d1we7J4N64w0vkdI0PLynQwQ
Bw==
-----END CERTIFICATE-----

SERIALNUMBER=20562999711, EMAILADDRESS=info@accepta.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@accepta.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

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
22491646653959637404570329715733972792330109970178519938112364977577414
44133400587551206869215235579969135048500220981966973784153005292370555
80018220752255057626969340991473403823393268152095789870285904811786045
12334901089347926492651024529873183399634371294321778738696297667981363
73298649872527598164072452139943630883717248982984307573473756101542613
11259830338582637382311901
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
8834161110638245801201459492227952584309370098532857415112734692273953872339334028472856297270640283645544695688308261540988949746833318362081052093444983003966169284433806
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: 8B 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
]
```


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:
83858149572724153879147929355523980989734321475859749889025077213438201
26524884170606414003946838975282973441339166366659694254724878287690336
74619340229210019038411557207353988428020514146059990415173356285194019
8972554302973548135032056829346440481363796100316472858111382511506794154464000874254636383538705084332170036018937879011595690828366546883794
54464000874254636383538705084332170036018937879011595690828366546883794
42238984855385231401082187574319605112793969098253082696258163595003930
44506195065406973866979834465357600186317299531120059889564954778450547
13790607993935317903225931115551294561508366832096481385530018748868233
75897094509231461436751145038654845132484221730531887066468315315900133
71317687849508774246606858215998371652684451081569193729603948966737003
66173116574869034752075000481857055603133004720515118185340830287591489
11121731446254498831643125678570838959058891513879770747968424374849154
18607294937946714802635710614763655891576465836079843249598538145297512
08292381505296966521391501862180756102181476419030034916745728837653159
97662348670149550479538217376609894907505134206162584771350820191765432
14272958600958156996693944950870237561708193162157227429018640096262273
85064716761931499369682236963577413562254878918077283227381578037288564
35994837185278097707227421
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:
83858149572724153879147929355523980989734321475859749889025077213438201265248841706064140039468389752829734413391663666596942547248782876903367461934022921001903841155720735
39884280205141460599904151733562851940198972554302973548135032056829346440481363796100316472858111382511506794154464000874254636383538705084332170036018937879011595690828366
546883794422389848553852314010821875743196051127939690982530826962581635950039304450619506540669738669798344653576001863172995311200598895649547784505471379060799393531790322
59311155512945615083668320964813855300187488682337589709450923146143675114503865484513248422173053188706646831531590013371317687849508774246606858215998371652684451081569193
72960394896673700366173116574869034752075000481857055603133004720515118185340830287591489111217314462544988316431256785708389590588915138797707479684243748491541860729493794
67148026357106147636558915764658360798432495985381452975120829238150529696652139150186218075610218147641903003491674572883765315997662348670149550479538217376609894907505134
2061625847135082019176543214272958600958156996693944950870237561708193162157227429018640096262273850647167619314993696822369635774135622548789180772832273815780372885643599
4837185278097707227421
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 3BG.....Yr.;
0010: B5 34 14 1F4..
]
]

[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

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

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://certisign.
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 EFXIO.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 ACc.....
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 2F2.....<.6/
00E0: 15 CC FB 0F 67 4A 69 72 80 B3 71 BC B9 06 FE E7gJir..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 .ZY0.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 0D9=.E...
0130: 07 9E 8B F0 F5 2B EC 64 F7 1F 96 CB 4F FE 9C 75+d...0..
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].[...04....*.
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`. "j];...
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..l..V.1D.

The certificate in PEM format:

-----BEGIN CERTIFICATE-----
MIIGOTCCBgAwIBAgIIdEpy9Iy+S5EwDQYJKoZIhvcNAQENBQAwMDEMAkGA1UE
BhMjQ1LlRarBgNVBAoTJENlcnc2LnbiBDZjX0aWZpY2Fkb3JhIERpZ2l0YVwv
YU5BLjEaMDEMAkGA1UEAxMQRQZVydGZaWduIFJvb3Q0EWhHcnMTUwNDEIMDMwMDEw
WWhCNmZAwNDEIMDMwMDEwWjBYMQswCQYDQVQGEWJCUjEtMCsGA1UEChMkQ2VydGZl
awduIENlcncRpmZmljYWRvcmeGRGlnaXRhbCBTLkEuMR0wGAYDQDQDEhFDZjX0aXNp
Z24gUm9vdCBDQTCiAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAg0CggIBAM2NeAeE
wi63b5vLD+awgtrT8AjMkNDA8VFUy/kRdHvy7Yakqt1W7tSp54YNsg+82T18B5aS
1BqLSmBnQcpKIiofzkcmEK3fsXocdI3s1LXI0s5nBE9E1/RC0rv+0BpT8szZphVg
ZGsrhXVbTLdpVIT60EYHFjyb26SjVT+oSURb7C8ffs6RJ2XpU3L0d0dU5t3VvEq
fb+F0yYfoDcg7s4N1M7khdYycN0Bg+ogwhkNr5p56pCBZ+3jI2RwnwbJJIRnKH
JC/I+Y/z/LzRu3RM6BBeih0b0SLyKW1rYX/Z0e5UPf5HbIRer7f8A3xnh9CouiFz
LumZ2XfjzcbI97/P6GKLGu5PVGjwInBc/ZiLhRgBYokX4zUHVAMMXZe4873VnBdo
LeNhwV175EsESNM1dZov3R6FPR8PbV9XKL66RBSLV0HRui2ALxrpjKK/60Jy/Cn
N81nmuySt97sLtjhT0woYkHL5tjZY2E3U7Zx1+B/CxLz1sKvbZwxDrGiJ745XodX
nX30VqE1Y7ynIdm1Q4Em8089d6mHDIAEXaHqJhQ7VCMz+IiZvc0MmcUIPgWwLz0
XK3ymhV70XNhtU7j88qrT02TJfL6CHJM1bn8rz+SfJZ6toFrY7x6PvJB26Y88Xt
iuGsRkDFRkgQYyKa/jLJZYuk6mAFKOPEs9k8AgMBAAGjggEgFMIIBATAPBgNVHRMB
Af8EBTADAQH/MB0GA1UdDgQWBBSLps6LR9EbjIudGVlYXxs7tTQUHzBaBgNVHSAE
UzBRMEBGCsGAQQBgewtBDBCEAGCCsGAQUFBwIBFjRodHRwO18vY2VydGZlZaWdu
LWlnLmNlcncRpmZmljYWRvcmeGRGlnaXRhbCBTLkEuMR0wGAYDQDQDEhFDZjX0aXNp
Z24gUm9vdCBDQTCiAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAg0CggIBAM2NeAeE
wi63b5vLD+awgtrT8AjMkNDA8VFUy/kRdHvy7Yakqt1W7tSp54YNsg+82T18B5aS
1BqLSmBnQcpKIiofzkcmEK3fsXocdI3s1LXI0s5nBE9E1/RC0rv+0BpT8szZphVg
ZGsrhXVbTLdpVIT60EYHFjyb26SjVT+oSURb7C8ffs6RJ2XpU3L0d0dU5t3VvEq
fb+F0yYfoDcg7s4N1M7khdYycN0Bg+ogwhkNr5p56pCBZ+3jI2RwnwbJJIRnKH
JC/I+Y/z/LzRu3RM6BBeih0b0SLyKW1rYX/Z0e5UPf5HbIRer7f8A3xnh9CouiFz
LumZ2XfjzcbI97/P6GKLGu5PVGjwInBc/ZiLhRgBYokX4zUHVAMMXZe4873VnBdo
LeNhwV175EsESNM1dZov3R6FPR8PbV9XKL66RBSLV0HRui2ALxrpjKK/60Jy/Cn
N81nmuySt97sLtjhT0woYkHL5tjZY2E3U7Zx1+B/CxLz1sKvbZwxDrGiJ745XodX
nX30VqE1Y7ynIdm1Q4Em8089d6mHDIAEXaHqJhQ7VCMz+IiZvc0MmcUIPgWwLz0
XK3ymhV70XNhtU7j88qrT02TJfL6CHJM1bn8rz+SfJZ6toFrY7x6PvJB26Y88Xt
iuGsRkDFRkgQYyKa/jLJZYuk6mAFKOPEs9k8AgMBAAGjggEgFMIIBATAPBgNVHRMB
Af8EBTADAQH/MB0GA1UdDgQWBBSLps6LR9EbjIudGVlYXxs7tTQUHzBaBgNVHSAE
UzBRMEBGCsGAQQBgewtBDBCEAGCCsGAQUFBwIBFjRodHRwO18vY2VydGZlZaWdu
LWlnLmNlcncRpmZmljYWRvcmeGRGlnaXRhbCBTLkEuMR0wGAYDQDQDEhFDZjX0aXNp
Z24gUm9vdCBDQTCiAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAg0CggIBAM2NeAeE
wi63b5vLD+awgtrT8AjMkNDA8VFUy/kRdHvy7Yakqt1W7tSp54YNsg+82T18B5aS
1BqLSmBnQcpKIiofzkcmEK3fsXocdI3s1LXI0s5nBE9E1/RC0rv+0BpT8szZphVg
ZGsrhXVbTLdpVIT60EYHFjyb26SjVT+oSURb7C8ffs6RJ2XpU3L0d0dU5t3VvEq
fb+F0yYfoDcg7s4N1M7khdYycN0Bg+ogwhkNr5p56pCBZ+3jI2RwnwbJJIRnKH
JC/I+Y/z/LzRu3RM6BBeih0b0SLyKW1rYX/Z0e5UPf5HbIRer7f8A3xnh9CouiFz
LumZ2XfjzcbI97/P6GKLGu5PVGjwInBc/ZiLhRgBYokX4zUHVAMMXZe4873VnBdo
LeNhwV175EsESNM1dZov3R6FPR8PbV9XKL66RBSLV0HRui2ALxrpjKK/60Jy/Cn
N81nmuySt97sLtjhT0woYkHL5tjZY2E3U7Zx1+B/CxLz1sKvbZwxDrGiJ745XodX
nX30VqE1Y7ynIdm1Q4Em8089d6mHDIAEXaHqJhQ7VCMz+IiZvc0MmcUIPgWwLz0
XK3ymhV70XNhtU7j88qrT02TJfL6CHJM1bn8rz+SfJZ6toFrY7x6PvJB26Y88Xt
iuGsRkDFRkgQYyKa/jLJZYuk6mAFKOPEs9k8AgMBAAGjggEgFMIIBATAPBgNVHRMB
Af8EBTADAQH/MB0GA1UdDgQWBBSLps6LR9EbjIudGVlYXxs7tTQUHzBaBgNVHSAE
UzBRMEBGCsGAQQBgewtBDBCEAGCCsGAQUFBwIBFjRodHRwO18vY2VydGZlZaWdu
LWlnLmNlcncRpmZmljYWRvcmeGRGlnaXRhbCBTLkEuMR0wGAYDQDQDEhFDZjX0aXNp
Z24gUm9vdCBDQTCiAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAg0CggIBAM2NeAeE
wi63b5vLD+awgtrT8AjMkNDA8VFUy/kRdHvy7Yakqt1W7tSp54YNsg+82T18B5aS
1BqLSmBnQcpKIiofzkcmEK3fsXocdI3s1LXI0s5nBE9E1/RC0rv+0BpT8szZphVg
ZGsrhXVbTLdpVIT60EYHFjyb26SjVT+oSURb7C8ffs6RJ2XpU3L0d0dU5t3VvEq
fb+F0yYfoDcg7s4N1M7khdYycN0Bg+ogwhkNr5p56pCBZ+3jI2RwnwbJJIRnKH
JC/I+Y/z/LzRu3RM6BBeih0b0SLyKW1rYX/Z0e5UPf5HbIRer7f8A3xnh9CouiFz
LumZ2XfjzcbI97/P6GKLGu5PVGjwInBc/ZiLhRgBYokX4zUHVAMMXZe4873VnBdo
LeNhwV175EsESNM1dZov3R6FPR8PbV9XKL66RBSLV0HRui2ALxrpjKK/60Jy/Cn
N81nmuySt97sLtjhT0woYkHL5tjZY2E3U7Zx1+B/CxLz1sKvbZwxDrGiJ745XodX
nX30VqE1Y7ynIdm1Q4Em8089d6mHDIAEXaHqJhQ7VCMz+IiZvc0MmcUIPgWwLz0
XK3ymhV70XNhtU7j88qrT02TJfL6CHJM1bn8rz+SfJZ6toFrY7x6PvJB26Y88Xt
iuGsRkDFRkgQYyKa/jLJZYuk6mAFKOPEs9k8AgMBAAGjggEgFMIIBATAPBgNVHRMB
Af8EBTADAQH/MB0GA1UdDgQWBBSLps6LR9EbjIudGVlYXxs7tTQUHzBaBgNVHSAE
UzBRMEBGCsGAQQBgewtBDBCEAGCCsGAQUFBwIBFjRodHRwO18vY2VydGZlZaWdu
LWlnLmNlcncRpmZmljYWRvcmeGRGlnaXRhbCBTLkEuMR0wGAYDQDQDEhFDZjX0aXNp
Z24gUm9vdCBDQTCiAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAg0CggIBAM2NeAeE
wi63b5vLD+awgtrT8AjMkNDA8VFUy/kRdHvy7Yakqt1W7tSp54YNsg+82T18B5aS
1BqLSmBnQcpKIiofzkcmEK3fsXocdI3s1LXI0s5nBE9E1/RC0rv+0BpT8szZphVg
ZGsrhXVbTLdpVIT60EYHFjyb26SjVT+oSURb7C8ffs6RJ2XpU3L0d0dU5t3VvEq
fb+F0yYfoDcg7s4N1M7khdYycN0Bg+ogwhkNr5p56pCBZ+3jI2RwnwbJJIRnKH
JC/I+Y/z/LzRu3RM6BBeih0b0SLyKW1rYX/Z0e5UPf5HbIRer7f8A3xnh9CouiFz
LumZ2XfjzcbI97/P6GKLGu5PVGjwInBc/ZiLhRgBYokX4zUHVAMMXZe4873VnBdo
LeNhwV175EsESNM1dZov3R6FPR8PbV9XKL66RBSLV0HRui2ALxrpjKK/60Jy/Cn
N81nmuySt97sLtjhT0woYkHL5tjZY2E3U7Zx1+B/CxLz1sKvbZwxDrGiJ745XodX
nX30VqE1Y7ynIdm1Q4Em8089d6mHDIAEXaHqJhQ7VCMz+IiZvc0MmcUIPgWwLz0
XK3ymhV70XNhtU7j88qrT02TJfL6CHJM1bn8rz+SfJZ6toFrY7x6PvJB26Y88Xt
iuGsRkDFRkgQYyKa/jLJZYuk6mAFKOPEs9k8AgMBAAGjggEgFMIIBATAPBgNVHRMB
Af8EBTADAQH/MB0GA1UdDgQWBBSLps6LR9EbjIudGVlYXxs7tTQUHzBaBgNVHSAE
UzBRMEBGCsGAQQBgewtBDBCEAGCCsGAQUFBwIBFjRodHRwO18vY2VydGZlZaWdu
LWlnLmNlcncRpmZmljYWRvcmeGRGlnaXRhbCBTLkEuMR0wGAYDQDQDEhFDZjX0aXNp
Z24gUm9vdCBDQTCiAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAg0CggIBAM2NeAeE
wi63b5vLD+awgtrT8AjMkNDA8VFUy/kRdHvy7Yakqt1W7tSp54YNsg+82T18B5aS
1BqLSmBnQcpKIiofzkcmEK3fsXocdI3s1LXI0s5nBE9E1/RC0rv+0BpT8szZphVg
ZGsrhXVbTLdpVIT60EYHFjyb26SjVT+oSURb7C8ffs6RJ2XpU3L0d0dU5t3VvEq
fb+F0yYfoDcg7s4N1M7khdYycN0Bg+ogwhkNr5p56pCBZ+3jI2RwnwbJJIRnKH
JC/I+Y/z/LzRu3RM6BBeih0b0SLyKW1rYX/Z0e5UPf5HbIRer7f8A3xnh9CouiFz
LumZ2XfjzcbI97/P6GKLGu5PVGjwInBc/ZiLhRgBYokX4zUHVAMMXZe4873VnBdo
LeNhwV175EsESNM1dZov3R6FPR8PbV9XKL66RBSLV0HRui2ALxrpjKK/60Jy/Cn
N81nmuySt97sLtjhT0woYkHL5tjZY2E3U7Zx1+B/CxLz1sKvbZwxDrGiJ745XodX
nX30VqE1Y7ynIdm1Q4Em8089d6mHDIAEXaHqJhQ7VCMz+IiZvc0MmcUIPgWwLz0
XK3ymhV70XNhtU7j88qrT02TJfL6CHJM1bn8rz+SfJZ6toFrY7x6PvJB26Y88Xt
iuGsRkDFRkgQYyKa/jLJZYuk6mAFKOPEs9k8AgMBAAGjggEgFMIIBATAPBgNVHRMB
Af8EBTADAQH/MB0GA1UdDgQWBBSLps6LR9EbjIudGVlYXxs7tTQUHzBaBgNVHSAE
UzBRMEBGCsGAQQBgewtBDBCEAGCCsGAQUFBwIBFjRodHRwO18vY2VydGZlZaWdu
LWlnLmNlcncRpmZmljYWRvcmeGRGlnaXRhbCBTLkEuMR0wGAYDQDQDEhFDZjX0aXNp
Z24gUm9vdCBDQTCiAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAg0CggIBAM2NeAeE
wi63b5vLD+awgtrT8AjMkNDA8VFUy/kRdHvy7Yakqt1W7tSp54YNsg+82T18B5aS
1BqLSmBnQcpKIiofzkcmEK3fsXocdI3s1LXI0s5nBE9E1/RC0rv+0BpT8szZphVg
ZGsrhXVbTLdpVIT60EYHFjyb26SjVT+oSURb7C8ffs6RJ2XpU3L0d0dU5t3VvEq
fb+F0yYfoDcg7s4N1M7khdYycN0Bg+ogwhkNr5p56pCBZ+3jI2RwnwbJJIRnKH
JC/I+Y/z/LzRu3RM6BBeih0b0SLyKW1rYX/Z0e5UPf5HbIRer7f8A3xnh9CouiFz
LumZ2XfjzcbI97/P6GKLGu5PVGjwInBc/ZiLhRgBYokX4zUHVAMMXZe4873VnBdo
LeNhwV175EsESNM1dZov3R6FPR8PbV9XKL66RBSLV0HRui2ALxrpjKK/60Jy/Cn
N81nmuySt97sLtjhT0woYkHL5tjZY2E3U7Zx1+B/CxLz1sKvbZwxDrGiJ745XodX
nX30VqE1Y7ynIdm1Q4Em8089d6mHDIAEXaHqJhQ7VCMz+IiZvc0MmcUIPgWwLz0
XK3ymhV70XNhtU7j88qrT02TJfL6CHJM1bn8rz+SfJZ6toFrY7x6PvJB26Y88Xt
iuGsRkDFRkgQYyKa/jLJZYuk6mAFKOPEs9k8AgMBAAGjggEgFMIIBATAPBgNVHRMB
Af8EBTADAQH/MB0GA1UdDgQWBBSLps6LR9EbjIudGVlYXxs7tTQUHzBaBgNVHSAE
UzBRMEBGCsGAQQBgewtBDBCEAGCCsGAQUFBwIBFjRodHRwO18vY2VydGZlZaWdu
LWlnLmNlcncRpmZmljYWRvcmeGRGlnaXRhbCBTLkEuMR0wGAYDQDQDEhFDZjX0aXNp
Z24gUm9vdCBDQTCiAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAg0CggIBAM2NeAeE
wi63b5vLD+awgtrT8AjMkNDA8VFUy/kRdHvy7Yakqt1W7tSp54YNsg+82T18B5aS
1BqLSmBnQcpKIiofzkcmEK3fsXocdI3s1LXI0s5nBE9E1/RC0rv+0BpT8szZphVg
ZGsrhXVbTLdpVIT60EYHFjyb26SjVT+oSURb7C8ffs6RJ2XpU3L0d0dU5t3VvEq
fb+F0yYfoDcg7s4N1M7khdYycN0Bg+ogwhkNr5p56pCBZ+3jI2RwnwbJJIRnKH
JC/I+Y/z/LzRu3RM6BBeih0b0SLyKW1rYX/Z0e5UPf5HbIRer7f8A3xnh9CouiFz
LumZ2XfjzcbI97/P6GKLGu5PVGjwInBc/ZiLhRgBYokX4zUHVAMMXZe4873VnBdo
LeNhwV175EsESNM1dZov3R6FPR8PbV9XKL66RBSLV0HRui2ALxrpjKK/60Jy/Cn
N81nmuySt97sLtjhT0woYkHL5tjZY2E3U7Zx1+B/CxLz1sKvbZwxDrGiJ745XodX
nX30VqE1Y7ynIdm1Q4Em8089d6mHDIAEXaHqJhQ7VCMz+IiZvc0MmcUIPgWwLz0
XK3ymhV70XNhtU7j88qrT02TJfL6CHJM1bn8rz+SfJZ6toFrY7x6PvJB26Y88Xt
iuGsRkDFRkgQYyKa/jLJZYuk6mAFKOPEs9k8AgMBAAGjggEgFMIIBATAPBgNVHRMB
Af8EBTADAQH/MB0GA1UdDgQWBBSLps6LR9EbjIudGVlYXxs7tTQUHzBaBgNVHSAE
UzBRMEBGCsGAQQBgewtBDBCEAGCCsGAQUFBwIBFjRodHRwO18vY2VydGZlZaWdu
LWlnLmNlcncRpmZmljYWRvcmeGRGlnaXRhbCBTLkEuMR0wGAYDQDQDEhFDZjX0aXNp
Z24gUm9vdCBDQTCiAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAg0CggIBAM2NeAeE
wi63b5vLD+awgtrT8AjMkNDA8VFUy/kRdHvy7Yakqt1W7tSp54YNsg+82T18B5aS
1BqLSmBnQcpKIiofzkcmEK3fsXocdI3s1LXI0s5nBE9E1/RC0rv+0BpT8szZphVg
ZGsrhXVbTLdpVIT60EYHFjyb26SjVT+oSURb7C8ffs6RJ2XpU3L0d0dU5t3VvEq
fb+F0yYfoDcg7s4N1M7khdYycN0Bg+ogwhkNr5p56pCBZ+3jI2RwnwbJJIRnKH
JC/I+Y/z/LzRu3RM6BBeih0b0SLyKW1rYX/Z0e5UPf5HbIRer7f8A3xnh9CouiFz
LumZ2XfjzcbI97/P6GKLGu5PVGjwInBc/ZiLhRgBYokX4zUHVAMMXZe4873VnBdo
LeNhwV175EsESNM1dZov3R6FPR8PbV9XKL66RBSLV0HRui2ALxrpjKK/60Jy/Cn
N81nmuySt97sLtjhT0woYkHL5tjZY2E3U7Zx1+B/CxLz1sKvbZwxDrGiJ745XodX
nX30VqE1Y7ynIdm1Q4Em8089d6mHDIAEXaHqJhQ7VCMz+IiZvc0MmcUIPgWwLz0
XK3ymhV70XNhtU7j88qrT02TJfL6CHJM1bn8rz+SfJZ6toFrY7x6PvJB26Y88Xt
iuGsRkDFRkgQYyKa/jLJZYuk6mAFKOPEs9k8AgMBAAGjggEgFMIIBATAPBgNVHRMB
Af8EBTADAQH/MB0GA1UdDgQWBBSLps6LR9EbjIudGVlYXxs7tTQUHzBaBgNVHSAE
UzBRMEBGCsGAQQBgewtBDBCEAGCCsGAQUFBwIBFjRodHRwO18vY2VydGZlZaWdu
LWlnLmNlcncRpmZmljYWRvcmeGRGlnaXRhbCBTLkEuMR0wGAYDQDQDEhFDZjX0aXNp
Z24gUm9vdCBDQTCiAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAg0CggIBAM2NeAeE
wi63b5vLD+awgtrT8AjMkNDA8VFUy/kRdHvy7Yakqt1W7tSp54YNsg+82T18B5aS
1BqLSmBnQcpKIiofzkcmEK3fsXocdI3s1LXI0s5nBE9E1/RC0rv+0BpT8szZphVg
ZGsrhXVbTLdpVIT60EYHFjyb26SjVT+oSURb7C8ffs6RJ2XpU3L0d0dU5t3VvEq
fb+F0yYfoDcg7s4N1M7khdYycN0Bg+ogwhkNr5p56pCBZ+3jI2RwnwbJJIRnKH
JC/I+Y/z/LzRu3RM6BBeih0b0SLyKW1rYX/Z0e5UPf5HbIRer7f8A3xnh9CouiFz
LumZ2XfjzcbI97/P6GKLGu5PVGjwInBc/ZiLhRgBYokX4zUHVAMMXZe4873VnBdo
LeNhwV175EsESNM1dZov3R6FPR8PbV9XKL66RBSLV0HRui2ALxrpjKK/60Jy/Cn
N81nmuySt97sLtjhT0woYkHL5tjZY2E3U7Zx1+B/CxLz1sKvbZwxDrGiJ745XodX
nX30VqE1Y7ynIdm1Q4Em8089d6mHDIAEXaHqJhQ7VCMz+IiZvc0MmcUIPgWwLz0
XK3ymhV70XNhtU7j88qrT02TJfL6CHJM1bn8rz+SfJZ6toFrY7x6PvJB26Y88Xt
iuGsRkDFRkgQYyKa/jLJZYuk6mAFKOPEs9k8AgMBAAGjggEgFMIIBATAPBgNVHRMB
Af8EBTADAQH/MB0GA1UdDgQWBBSLps6LR9EbjIudGVlYXxs7tTQUHzBaBgNVHSAE
UzBRMEBGCsGAQQBgewtBDBCEAGCCsGAQUFBwIBFjRodHRwO18vY2VydGZlZaWdu
LWlnLmNlcncRpmZmljYWRvcmeGRGlnaXRhbCBTLkEuMR0wGAYDQDQDEhFDZjX0aXNp
Z24gUm9vdCBDQTCiAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAg0CggIBAM2NeAeE
wi63b5vLD+awgtrT8AjMkNDA8VFUy/kRdHvy7Yakqt1W7tSp54YNsg+82T18B5aS
1BqLSmBnQcpKIiofzkcmEK3fsXocdI3s1LXI0s5nBE9E1/RC0rv+0BpT8szZphVg
ZGsrhXVbTLdpVIT60EYHFjyb26SjVT+oSURb7C8ffs6RJ2XpU3L0d0dU5t3VvEq
fb+F0yYfoDcg7s4N1M7khdYycN0Bg+ogwhkNr5p56pCBZ+3jI2RwnwbJJIRnKH
JC/I+Y/z/LzRu3RM6BBeih0b0SLyKW1rYX/Z0e5UPf5HbIRer7f8A3xnh9CouiFz
LumZ2XfjzcbI97/P6GKLGu5PVGjwInBc/ZiLhRgBYokX4zUHVAMMXZe4873VnBdo
LeNhwV175EsESNM1dZov3R6FPR8PbV9XKL66RBSLV0HRui2ALxrpjKK/60Jy/Cn
N81nmuySt97sLtjhT0woYkHL5tjZY2E3U7Zx1+B/CxLz1sKvbZwxDrGiJ745XodX
nX30VqE1Y7ynIdm1Q4Em8089d6mHDIAEXaHqJhQ7VCMz+IiZvc0MmcUIPgWwLz0
XK3ymhV70XNhtU7j88qrT02TJfL6CHJM1bn8rz+SfJZ6toFrY7x6PvJB26Y88Xt
iuGsRkDFRkgQYyKa/jLJZYuk6mAFKOPEs9k8AgMBAAGjggEgFMIIBATAPBgNVHRMB
Af8EBTADAQH/MB0GA1UdDgQWBBSLps6LR9EbjIudGVlYXxs7tTQUHzBaBgNVHSAE
UzBRMEBGCsGAQQBgewtBDBCEAGCCsGAQUFBwIBFjRodHRwO18vY2VydGZlZaWdu
LWlnLmNlcncRpmZmljYWRvcmeGRGlnaXRhbCBTLkEuMR0wGAYDQDQDEhFDZjX0aXNp
Z24gUm9vdCBDQTCiAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAg0CggIBAM2NeAeE
wi63b5vLD+awgtrT8AjMkNDA8VFUy/kRdHvy7Yakqt1W7tSp54YNsg+82T18B5aS
1BqLSmBnQcpKIiofzkcmEK3fsXocdI3s1LXI0s5nBE9E1/RC0rv+0BpT8szZphVg
ZGsrhXVbTLdpVIT60EYHFjyb26SjVT+oSURb7C8ffs6RJ2XpU3L0d0dU5t3VvEq
fb+F0yYfoDcg7s4N1M7khdYycN0Bg+ogwhkNr5p56pCBZ+3jI2RwnwbJJIRnKH
JC/I+Y/z/LzRu3RM6BBeih0b0SLyKW1rYX/Z0e5UPf5HbIRer7f8A3xnh9CouiFz
LumZ2XfjzcbI97/P6GKLGu5PVGjwInBc/ZiLhRgBYokX4zUHVAMMXZe4873VnBdo
LeNhwV175EsESNM1dZov3R6FPR8PbV9XKL66RBSLV0HRui2ALxrpjKK/60Jy/Cn
N81nmuySt97sLtjhT0woYkHL5tjZY2E3U7Zx1+B/CxLz1sKvbZwxDrGiJ745XodX
nX30VqE1Y7ynIdm1Q4Em8089d6mHDIAEXaHqJhQ7VCMz+IiZvc0MmcUIPgWwLz0
XK3ymhV70XNhtU7j88qrT02TJfL6CHJM1bn8rz+SfJZ6toFrY7x6PvJB26Y88Xt
iuGsRkDFRkgQYyKa/jLJZYuk6mAFKOPEs9k8AgMBAAGjggEgFMIIBATAPBgNVHRMB
Af8EBTADAQH/MB0GA1UdDgQWBBSLps6LR9EbjIudGVlYXxs7tTQUHzBaBgNVHSAE
UzBRMEBGCsGAQQBgewtBDBCEAGCCsGAQUFBwIBFjRodHRwO18vY2VydGZlZaWdu
LWlnLmNlcncRpmZmljYWRvcmeGRGlnaXRhbCBTLkEuMR0wGAYDQDQDEhFDZjX0aXNp
Z24gUm9vdCBDQTCiAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAg0CggIBAM2NeAeE
wi63b5vLD+awgtrT8AjMkNDA8VFUy/kRdHvy7Yakqt1W7tSp54YNsg+82T18B5aS
1BqLSmBnQcpKIiofzkcmEK3fsXocdI3s1LXI0s5nBE9E1/RC0rv+0BpT8szZphVg
ZGsrhXVbTLdpVIT60EYHFjyb26SjVT+oSURb7C8ffs6RJ2XpU3L0d0dU5t3VvEq
fb+F0yYfoDcg7s4N1M7khdYycN0Bg+ogwhkNr5p56pCBZ+3jI2RwnwbJJIRnKH
JC/I+Y/z/LzRu3RM6BBeih0b0SLyKW1rYX/Z0e5UPf5HbIRer7f8A3xnh9CouiFz
LumZ2XfjzcbI97/P6GKLGu5PVGjwInBc/ZiLhRgBYokX4zUHVAMMXZe4873VnBdo
LeNhwV175EsESNM1dZov3R6FPR8PbV9XKL66RBSLV0HRui2ALxrpjKK/60Jy/Cn
N81nmuySt97sLtjhT0woYkHL5tjZY2E3U7Zx1+B/CxLz1sKvbZwxDrGiJ745XodX
nX30VqE1Y7ynIdm1Q4Em8089d6mHDIAEXaHqJhQ7VCMz+IiZvc0MmcUIPgWwLz0
XK3ymhV70XNhtU7j88qrT02TJfL6CHJM1bn8rz+SfJZ6toFrY7x6PvJB26Y88Xt
iuGsRkDFRkgQYyKa/jLJZYuk6mAFKOPEs9k8AgMBAAGjggEgFMIIBATAPBgNVHRMB
Af8EBTADAQH/MB0GA1UdDgQWBBSLps6LR9EbjIudGVlYXxs7tTQUHzBaBgNVHSAE
UzBRMEBGCsGAQQBgewtBDBCEAGCCsGAQUFBwIBFjRodHRwO18vY2VydGZlZaWdu
LWlnLmNlcncRpmZmljYWRvcmeGRGlnaXRhbCBTLkEuMR0wGAYDQDQDEhFDZjX0aXNp
Z24gUm9vdCBDQTCiAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAg0CggIBAM2NeAeE
wi63b5vLD+awgtrT8AjMkNDA8VFUy/kRdHvy7Yakqt1W7tSp54YNsg+82T18B5aS
1BqLSmBnQcpKIiofzkcmEK3fsXocdI3s1LXI0s5nBE9E1/RC0rv+0BpT8szZphVg
ZGsrhXVbTLdpVIT60EYHFjyb26SjVT+oSURb7C8ffs6RJ2XpU3L0d0dU5t3VvEq
fb+F0yYfoDcg7s4N1M7khdYycN0Bg+ogwhkNr5p56pCBZ+3jI2RwnwbJJIRnKH
JC/I+Y/z/LzRu3RM6BBeih0b0SLyKW1rYX/Z0e5UPf5HbIRer7f8A3xnh9CouiFz
LumZ2XfjzcbI97/P6GKLGu5PVGjwInBc/ZiLhRgBYokX4zUHVAMMXZe4873VnBdo
LeNhwV175EsESNM1dZov3R6FPR8PbV9XKL66RBSLV0HRui2ALxrpjKK/60Jy/Cn
N81nmuySt97sLtjhT0woYkHL5tjZY2E3U7Zx1+B/CxLz1sKvbZwxDrGiJ745XodX
nX30VqE1Y7ynIdm1Q4Em8089d6mHDIAEXa

xIIRJANet2jSacGRwGqIJyru+josCaKb0iKQIyLrKXYwDbXsPcWFuQb/9r9TyjPG
sp9qC4cxg/dWvzFE1g==
-----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:
8460920175970924147750409063456401386982281312729422229682166099085633
65373543206677979791446723899724857018234905808600953788462147930919466
36711810510143602935614448969052976569460191344340411085278864480397551
13928848168259548886042999410681700965459097916985266598794470652209392
73591912844169369934733226533226485445464903747137029119306308267181774
93478384013463616572466695103685157701006946012762949509273382917462547
87462160403839417941439449488026559284704494247178338819015761652554161
92517515850886868212203776701656097437048673335218042357268145153942376
06684342206020857315868853226372860689522748419197604789918543589374052
78304097405134469286117208885155772687177065698793406053439577539323415
91681926533607994971541574786412858592991476103353528974198484683270770
11255384029376433000198229665887899102451255461148152093374341724106665
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:
8460920175970924147750409063456401386982281312729422229682166099085633653735432066779797914467238997248570182349058086009537884621479309194663671181051014360293561444896905
29765694601913443404110852788644803975511392884816825954888604299941068170096545909791698526659879447065220939273591912844169369934733226533226485445464903747137029119306308
26718177493478384013463616572466695103685157701006946012762949509273382917462547874621604038394179414394494880265592847044942471783388190157616525541619251751585088686821220
37767016560974370486733352180423572681451539423760668434220602085731586885322637286068952274841919760478991854358937405278304097405134469286117208885155772687177065698793406
05343957753932341591681926533607994971541574786412858592991476103353528974198484683270770112553840293764330001982296658878991024512554611481520933743417241066654485666150471
72231284902535559688621869505738343197655877020385150958357492861870954793780606490967794235743393014723996222915070841869893389780477909787821319057498544842663672676740377
22275662657515429623842534115884861908158732634146703480166601216863579412152417845597010953886387649454849416061094958999639445737301247411354901981080544897734475863537515
6307556203228143384409
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
]

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

```
[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....0
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 B3 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.....nRNOx..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.$...;
0100: F5 4F 3B 16 65 38 A6 E1 75 53 6E C2 F3 CC 76 97 .0;e8..uSn...v.
0110: 46 59 A3 E5 92 D7 6A 0C 95 AE 22 5A 75 92 18 41 FY....j....Zu..A
0120: DA C9 6D D3 1D 20 9F A0 7E 14 00 AA 6B 7B 99 CB ...m...k...
0130: 55 16 33 01 16 13 72 6D 0C EF 7F 17 C9 C1 8A D8 U.3...rm.....
0140: 9C E0 84 EC 17 56 69 A8 8A 2C 74 F7 0D 1F A0 41 ....Vi...t...A
0150: 88 A7 73 00 F9 A7 81 AA F5 8D C6 14 B1 8E D6 AF ...s.....
0160: 4B 42 24 9D 63 30 8A AD 1C 78 B8 D9 CC 41 B6 40 KB$.c0...x...A.@
0170: 00 A9 C5 1A EB 92 72 2D 34 D6 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:

Public key Sun RSA public key, 4096 bits
modulus:
91380594494012118573494581424719634392948070347222958091982414705377099
17345483601841830441973021908577528648887727317069287199021301569428812
36105728583989490929999864394605612919876699480804702767118285221167710
04153554864839369107713619092418480743399777944802081357849025616851522
73194100206111326473599615789834813014708753804193433703172957579379856
67174666340432041762362169376595485198579279236242600172093197111746409
56856269771247164066379639939256320384132367937813144239588354699234547
19770761006441103022886120747372873314242323628435201518590315457375443
62005519669372343757281524692913778309158593468491898945103977668411710
42644716750113052066396349480827119797898874903745421917865323129863625
79818699949180615053272385717494979045846678213277032389122589902449673
05178450424839912718864684982532222709071195810069729226644535885513096
70585999150876766581384172928358042731481513752618951389235708566022259
61723399194598810185073343110877556626550632445693674295465882530682590
89985817646683036851775983489410140874326989239429120391433703499640901
66443005480856076865352963778126275021103951824107029581489448148757935
29023690223272196230423197161355606544564806723261420787589163859628329
89970358662275707323866227
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 041830168014552cf1bca15eb9eea02f8857105bfc96f7919a2c

Key usage keyCertSign
cRLSign

Basic constraints CA=true; PathLen=0

SHA1 Thumbprint 7f2cb4f769224cb0cf8b692751cbd4cc64a2c450

SHA256 Thumbprint 35a99284a220789ba0e062eef1b5f2f74be43754469977cb318c7c86ad48f9f

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:
91380594494012118573494581424719634392948070347222958091982414705377099173454836018418304419730219085775286488877273170692871990213015694288123610572858398949092999986439460
56129198766994808047027671182852211677100415355486483936910771361909241848074339977794480208135784902561685152273194100206111326473599615789834813014708753804193433703172957
5793798566717466634043204176236216937659548519857927923624260017209319711174640956856269712471640663796399392563203841323679378131442395883546992345471977076100644110302288
61207473728733142423236284352015185903154573754436200551966937234375728152469291377830915859346849189894510397766841171042644716750113052066396349480827119797898874903745421
9178653231298636257981869994918061505327238571749497904584667821327703238912258990244967305178450424839912718864684982532227090711958100697292266445358855130967058599915087
67665813841729283580427314815137526189513892357085660222596172339919459881018507334311087755662655063244569367429546588253068259089985817646683036851775983489410140874326989
23942912039143370349964090166443005480856076865352963778126275021103951824107029581489448148757935290236902232721962304231971613556065445648067232614207875891638596283298997
0358662275707323866227
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 ....
]
]
]
```


Public key

Sun RSA public key, 4096 bits

modulus:
63017122778119801147895667650934397946328719771150871734959229663693351
17581666918807802240086066028035207161601638116422307092147698844907782
68662573890902240140705811089281704088751366114157810422323845310368852
63111988768980085910041331788207275027720525562946972746516079196617207
87326932979157410927630879403887688189839478863868270415288074295055619
64426794663639177148562561862788528408049258123934313988746414960009814
37925254897081856430169410905923333128709849353411477030758112321066775
27197454383452626160083311719784225359147920014126653260623863503316290
30604008215220671793061761118000673398879051238658168007520846896803475
52668899348796799000471151155938368517996330891000189140042706141298411
29526873670365876859327215989167461457776139762682421772836721488529356
67330307115212299111818695094121674817269164416217298316095171555634572
19945474559437452182381056978881478473090876449934297348904566348680861
68702747255408764878885382711782391808699578881187238925312375775603082
77712287984017256193905219871954230305676608302292143627885324008865938
61824991465448184409815196589641080368519958541874786073394561017087249
47997286191094996739218056745858690790930659795628688398572844946024835
00561175050725291397734547
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:
63017122778119801147895667650934397946328719771150871734959229663693351175816669188078022400860660280352071616016381164223070921476988449077826866257389090224014070581108928
17040887513661141578104223238453103688526311198876898008591004133178820727502772052556294697274651607919661720787326932979157410927630879403887688189839478863868270415288074
29505561964426794663639177148562561862788528408049258123934313988746414960009814379252548970818564301694109059233331287098493534114770307581123210667752719745438345262616008
33117197842253591479200141266532606238635033162903060400821522067179306176111800067339887905123865816800752084689680347552668899348796799000471151155938368517996330891000189
14004270614129841129526873670365876859327215989167461457776139762682421772836721488529356673303071152122991118186950941216748172691644162172983160951715556345721994547455943
74521823810569788814784730908764499342973489045663486808616870274725540876487888538271178239180869957888118723892531237577560308277712287984017256193905219871954230305676608
30229214362788532400886593861824991465448184409815196589641080368519958541874786073394561017087249479972861910949967392180567458586907909306597956286883985728449460248350056
1175050725291397734547
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: [

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

```
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 0LJCertificado
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.uanatata.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 18 BA 1D E9 08 94 C4 BB ...V1 .....
0030: 58 1C DE B5 05 68 99 A4 D1 4C 3B 8A 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 98 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..0...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...!..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.ZSm.....
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 00 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...3.0.
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..0..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-----

```
MIIHZAzCCB0uGAW1BAgIITW0S6Y7X5ZQwDQYJKoZIhvcNAQELBQAwgBkxChAJBgNV
BAYTAKVMTUwqDQYVQVQ0HDDtCYXJjZWxvbmEgKHNLZSBJdXJyZW50IGFkZHZHJlLmMg
YXQgd3d3LnVhbmF0YWNhLmNvbS9hZGRyZXNzKTEwM0Q0Q0EgUUECgwwNVU0F0VRB0E0Eg
Uy5BLjEwM0Q0Q0EgUUECgwwNVU0F0VRB0E0EgUUECgwwNVU0F0VRB0E0EgUUECgwwNVU0F0VRB0E0Eg
T09UdWUwMTYxGDAwBGNVBEVMD1ZBVEVTLUE2NjcyMTQ5OTAEwF0xNjAzMTUwE0TEz
NTNaFw0MTAzMTUwE0TEzNTNaMIGSMQswCQYDVQGEwFJFzFEMEIGA1UEBww7QmFz
Y2Vsb25hIChzZWUyY3VycmludCBhZGRyZXNzIGF0IHRhd3dy51Yw5hdGFjY55jb2V0
YWRkcmVzcykxFjAUBGNVBAOwMDVBTkFUQUQUNBFuQ5A4FTATBGNVBAwMDFRFTUC1V
QU5BVEF0TEBMBkGA1UEAwVsUUF0QVRB0EgUk9PVCAYMDE2MRgwFgYDVQRhDA9W
QVRFRU1BNjY3E00TKwggI1MA0GCSCqGSIb3DQEBAQUAA4IDCwAwggIKAoICAQCa
dRtr0ey704cMzz7A1vUB4HLs0Y8Y1H7BKFAuxwzst1G0L7TzZz0eDjGZMSjI00
JRUdmZ/LmG927tES5dLrfdRNVku3moF9j6Wjch4HmNqT6I30TnxhBNbtKEYHwxC
c1vQ00KaFUUBEt+NzS6smyDAzbywFUPS1d8JoGaGUMy7hhah38cLN408ff1gCFT
ehZIsRvDnsU1WU34vcAYLLmgjsvBNmq2V+Ts8+vtRlRcbpQ08usMbwJ501aoi71LU
tSeBGJqqaszMP0ty923PGHemImxHLSmHT13k5ha98EK4ZXFfjxSVryvpHgjThU
V3s4Zea5p5BwKfX16TL++0TciMLOp66jwZV3I4DqeRmNXk1Rebs5u8bDDZxxeSP
RusoF11clm9cqCNy51hd2LNV8QECUNQ/RPon0sh+BS0SedppYxq6TFqabE/FTnt
JBU7CMJ3EFJ/j5vxf6qj7JjInUQXajSxDdt0WrmDW8a0CRKCZ0ML/Iwb8yk83/y
Zdt6E+Ez63V/x7sA2ZygG61z f4w0T95FN4Z1atf0Ecp/2uc5HXKrUTXTMDJJZfD
WMO30Ae1Rei94TRd/9XRqPdEk0B/VL5/99151EX6010NwKRPM6HNNZowbdnmLEc+
CGX1yj01RS1Y4UT0aLj/W7oiNxmpZQAdAc9NN/gkwIDAQAB4IBCzCCAQcwHQYD
VR0BBYEFFU8byhXrnuoC+IVxBb/Jb3kZosMA8GA1UdEwEB/wQFMAMBAf8wgaYG
A1UdIASBnjCBmzCBMAyEVR0gADCbjzAzBggfBgEFPBcCARYnaHR0cDovL3d3dy51
Yw5hdGFjY55jb2V0chVibG1jL3BraS9kGMvMFgGCCsGAOUFBwICMEwMskNlcnRp
ZmljYWRwIHRhZD16IGRlIFVBTkFUQUQUNBL1BwZlIgaHR0cDovL3d3dy51Yw5hdGFj
Y55jb2V0chVibG1jL3BraS9kGMvMA4GA1UdEwEB/wQEAwIBBjAUBGNVHREFTAT
gRFpbmZVhbmF0YWNhLmNvbTANBgkqhkiG9w0BAQsFAAOCAQEAATAyOSKMK/yj6
JFb/RahMmor8knkQWv131FASKyFLQc6FHoVjEgihu6HekILMS7WBzetqVomaTR
DU6eJeyo/+7CB+VGGHOYYjSdc8F8W1IHFN3f6ztKuM6zLvz3Xy9BHhg1H4ggNL
Yxe99kq14QEOR/fm0p7rVgVeeHhG8m1S5UGyyJlUke1B0d0PqwVWLGINp+i/nhf
nrXGStnBrJyHzx6tuaLUyHQU+Dg0tS8k65a8UR1oVkoQ0Cb7yIyJ5EBmPR2yqX
Owt6nYR8/3blrU99+wp67pm0tt5ggX3sB2a9WfY94Y5uIPB7JisOUBmqH23Rjake
c+UMLMjnvJQ82+1M7oGebnaVd1RVK+okemQ5zx57BzKzSL/14G+Zxya80Bz2cIQF
HnyCVXD0d4/CWNBZLQCTYGRUK0ocvu1kKXgmVY6hTQGHM8TR5yg/XT21gaAv3/7
th51b2iGgg08E3AW3ND+8N/qMjZ2aIKBKQYUfMLw1z26n6ni73E2LQ0Es+0uh9+
1xTPc17Afdv+p0m6HDP0p0t7BX0D0bh5QwPp1HBk88atzE5gmQxnkt4/g0S2av5
Lc+U7ufZ5/ao7tLL1qkTXzR87jN7T8+LZ0SHBb0an2QosyBfZWxgaFYTspoy5tP
n4RMcCgXqHSYLAUKaQ80WmT42AKLDY=
```


-----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
56459162538184795022865038457003083685876624788333078615274353970599757
5144040202692047859329095547088347386804572731603
public exponent: 65537
Subject key identifier 5d885bad6b65fbfe68a2e4d96f3d5772a2ef2b99
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
316196141872838680110934668903106281027652378361605644751778902553075984360889070542780279374661655316916978212656482014032425472734677690092750082867788929396586500772231
48974783078694118192481769273105866393158837503627314412328399337372816128936375036901533912010111664614429526207256796490069465975895570070140702609315645916253818479502286
5038457003083685876624788330786152743539705997575144040202692047859329095547088347386804572731603
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.....:./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 *.l..*..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 EF6..p...@....
00D0: 09 04 99 14 64 93 F9 71 6A EF 26 EE 76 D8 18 43d..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-----
MIIDoDCCAoigAwIBAgIIPqXFSPJocNIwDQYJKoZIhvcNAQELBQAwOzEZMBCGAlUE
AwwQTGxhbWUcGUGUm9vdCBDQTERMA8GA1UECgwITExBTUEUeUxZAJBgNVBAYT
A1UFBMB4XDTExMDcxODIzMDUxOFoXDTM0MDCxMzIyNTQyMjYwVjEKMCIgAlUEAwwb
TGxhbWUcGUGU0hBMjUzIFN0YW5kYXJkIENBMREwDyVQKDAhMTEFNQ5S0RTEL
MAKGA1UEBHMCEUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC70HwZ
u6wAQIYR7TMNbyM3Kjxv60Ax0FpARIt+4hG0rK6LN00BPQAIUJqg27zrPx2PG5J
1C4aqvd60gyeQJC3hdcsThYMQbq62aPjQaVWLY5dPWNtWRhY/3YCNyLLMs16TZf
Rx5N/KvgJ5BRAYRzPMqRhontKmrXkZjZTL29EfyBdLu5WwGv5Z2sKmoArp0Te/Np

/9+ND4mop17wsgBwfv8TxCrWhkAxvLm2R4psR06eJgCJYWN7AyzkRH3YR68yrfz2
bg3VFPiVvYdgSrEYUfWkXcKzfx2j0CDIPj f8L11nuhdL0U0b4ko5HgQ45SPqLWY
tKMBxjISAJEvdzjTAqMBAAGjZwvgZkwDwYDVR0TAQH/BAUwAwEB/zAFBgNVHSM
GDAWgB5mg0TNVZeEH4gJ4a115yLaX5j3pDA2BgNVHR8ELzAtMCugKaAnhiVodHRw
0i8vY3JsLmXsYw1hLnBL2xsYw1hcGlyb290Y2EuY3JsMB0GA1UdDgQWBRRdiFut
62X7/mi5NLvPVdyou8rmTA0BgNVHQ8BAF8EBAMCAyYwDQJKoZIhvcNAQELBQAD
ggEBAntu+P4r1+T0jWFL0wmGS9pv0mqLeKtvyXaKCeBdx6Jkg+JzvEnvetxZ3qv
Z54RPUH5bAo/Hi504wungaDrFys6D49b8NYay8X7vCpY/UQU8aspU4JRF6cNly0r
4tFwF3raoRn12s0u0d342bGdmsqzGXz1oT3m7/xX7Xo+mnPa3nP6F211p0Z/I2
2s2+FackQXcYHX59JxBvZ0HXZ7FWPLm0WbVq/vHTKvPaaG+KLCbr64cP3M9D98t
awgjp4T6sns2YrBw8Jr4QMymF+8JB3KUZJPS5cWrvJu5228hdWmJoJ7LFtLq+4Anb
2jy3L+KVLvUzszxU0ADQEp9hc=
-----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
6257163367376480305512553955095477541501030602919
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
7424162732046195713793936880006053445712182118487985510985466147003772061733311309213874397430154385862152737635053025817182813423436635237339697949114707527945490273919569
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 [

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

```
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.....Id%tR.
0030: 61 40 7F 4E 4C DA D6 D4 BA 52 06 4D 90 AC FB 3E @@.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....0..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-----
MIIDWzCCAk0gAwIBAgII0ixEWV4330MwDQYJKoZIhvcNAQELBQAwOzEZMBCGA1UE
AwwQTGxhbWUucGUGUm9vdCBDQTERMA8GA1UECgwITExBTUEuUEUxCzAJBgNVBAYT
A1BFMB4XDTE4MDcxODIyNTQyMVoXDTM4MDcxMzIyNTQyMVoOzEZMBCGA1UEAwwQ
TGxhbWUucGUGUm9vdCBDQTERMA8GA1UECgwITExBTUEuUEUxCzAJBgNVBAYTALBF
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsUhhv+jmFYMop5RU0ZUY
adWJtREvNmRpfFu8Wu1ybt94LFG08h11bwn0y92R+ARPSm/JF8jzBu/M7/JKQe1d
UEOalewvNRmko2CTvAdkkmWdaAQLoR+D5N8DgoAz/XStGw0UInuKcJ3NDfmdN81j
88hicK1/jsf0Cm6e8eIBdtpkwwjPuuQMU4sFK1sAFC453etEVCoXVYjELUvLm6
ZaB0otpqYG7xiKRL2iaxG0xX7U7jUoYMKQMKfD5foiNyJojNq3wFpkZiifvqf6oY
xw4lw80J0tPVEDVCJKn0bou0F2fctVsrvB6uiURvIuiVjPH0wgccjQA32Lo+tGuY
pwIDAQABo2MwYTAzPBGVHRMBAf8EBTADAQH/MB8GA1UdIwQYMBaAFKADRM1V140f
iAnhrXXnKvPpfmPekMB0GA1UdDgQWBBSmg0TNVZeEH4gJ4a115yLaX5j3pDA0BgNV
HQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggEBAHAm1Fne6t0L/uLyfmT/g3D1
rnp9iT0mFPTAy/FC/zYLCFapceZygnH5zFkJXRScmFAf05M2tbUuLIGTZCs+z5L
a0VYnwAp7DovKukU81rUHp5QXmF4W6rMqZxtLg3kzfi2y9KfTeiZjE/MiDWP6
5XLf7xhC3VE0zh3yP8RkRkSb4SUbRRReV+ZBb2un4eM3exFyc+RckIjA9PyMBK75XP
i0VeJm4qWoYyuQr/4cro76AyyIJTp9IeUWP53Gzqb14ZdBuFPJof6FkTs1Wbg39I
EDBiKtkn6pUtCq6bIvuygYsPCQoDkeFRKYcUcuvoA/3akhr3u8l7aTqTn8A6G0=
-----END CERTIFICATE-----
```