

## ORC ECA 2 CA Certificate Chain

Total number of certificates: 2

## ORC ECA 2 Signing Certificate:

Certificate Subject DN

**CN=ORC ECA 2,OU=Certification Authorities,OU=ECA,O=U.S. Government,C=US**

Certificate in base64 encoded format

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

```
MIIECTCCA3KgAwIBAgIBIjANBgkqhkiG9w0BAQUFADBLMQswCQYDVQQGEwJVUzEY
MBYGA1UEChMPVSt5TLiBhb3Zlcm5tZW50MQwwCgYDVQQLEwNFQ0ExFDASBgNVBAMT
C0VDQSBsb290IENBMB4XDTA3MDYyMTEzMDAyM1oXDTEzMDYyMjEyMDAyM1owbTEL
MAkGA1UEBhMCVVMxGDAWBGNVBAoTD1UuUy4gR292ZXJubWVudDEMMAoGA1UECxMD
RUNBMSIwIAYDVQQLExlDZXJ0aWZpY2F0aW9uIEF1dGhvcml0aWVzMRlwEAYDVQQD
EwIPIUkMgRlUNBIDlwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAPKIPLs+r4Wd
aqXgmVRv2EkXIGvJ7ijvD7uRKHE7mxyINpLcgT6Ks8uRD3j0oYhp228k7ghEsm55
vaWqTrpN8dzodxzZDUm5JF1Enzs5s2/F4RSOW59j2QJko8mK/e2RfsYS3fsSSWpw
prSrlvQyb8afJ6EtDGayxEUoqQep3E6zAgMBAAGjggHZMIIB1TASBgNVHRMBAf8E
CDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBhjAFBgNVHSMEGDAWgBT2uAQnDIYW2blj
2f2hVGVBoAhlLzAdBgNVHQ4EFgQUquTnY3LdXa6B7btRUF3xNXF9/ZwwggEpBgNV
HR8EggEgMIIBHDCBjaCBiqCBh4aBhGxkYXA6Ly9jcmwuY2hhbWluZGlzYS5taWwv
Y24IM0RFQ0EIMjBSb290JTIwQ0EIMkMIMjBvdSUzREVDQSUyQyUyMG8IM0RVLIMu
JTIwR292ZXJubWVudCUyQyUyMG8IM0RUVz9jZXJ0aWZpY2F0ZXJldm9jYXRpb25s
aXN0O2JpbmFyeTCBiaCBh4aBhGxkYXA6Ly9lY2E2ZHMub3JlLmNvbS9jbiUz
REVDQSUyMFJvb3QIMjBDQSUyQyUyMG91JTNERUNBJTJDJTIwbyUzRFUuUy4IMjBH
b3Zlcm5tZW50JTIwJTIwYyUzRFVTP2NlcnRpbm9jYXRlcmV2b2NhdGlvbmxpc3Q7
YmluYXJ5MEIGCCsGAQUFBwEBBDYwNDAYBggrBgEFBQcwAoYmaHR0cDovL2VjYS5v
cmMuY29tL2NlcnRzL2VjYXJvb3RjYS5wN2MwDQYJKoZIhvcNAQEFBQADgYEAfSIX
tnW2IVwBDjoVvQ0nF0XOQ/+P1+ciTc/VbSD4xFICxkSX2/CZGTa4EfCfLQnHITIJ
awD269sf7kWEvtDzA3KSwrRdOb7HkP3zGjQBwll1ZaHQLeNuDdEtrutl3qoYwru
GJJuHVGQljuPEXeBX4NbCpb2ID04oy+AQNKuRVU=
```

-----END CERTIFICATE-----

Certificate Contents

Certificate:

Data:

Version: v3

Serial Number: 0x22

Signature Algorithm: SHA1withRSA - 1.2.840.113549.1.1.5

Issuer: CN=ECA Root CA,OU=ECA,O=U.S. Government,C=US

Validity:

Not Before: Thursday, June 21, 2007 1:00:23 PM GMT

Not After: Saturday, June 22, 2013 12:00:23 PM GMT

Subject: CN=ORC ECA 2,OU=Certification Authorities,OU=ECA,O=U.S. Government,C=US

Subject Public Key Info:

Algorithm: RSA - 1.2.840.113549.1.1.1

Public Key:

Exponent: 65537

Public Key Modulus: (1024 bits) :

F2:88:3C:BB:3E:AF:85:9D:6A:A5:E0:99:54:6F:D8:49:

17:94:6B:C9:EE:28:EF:0F:BB:91:2A:11:3B:9B:1C:88:

36:92:DC:81:3E:8A:B3:CB:91:0F:78:F4:A1:88:69:DB:  
6F:24:EE:08:44:B2:6E:79:BD:A5:AA:4E:BA:4D:F1:DC:  
E8:77:1C:D9:0D:49:B9:24:5D:44:9F:3B:39:B3:6F:C5:  
E1:14:8E:5B:9F:63:D9:02:64:A3:C9:8A:FD:ED:91:7E:  
C6:12:DD:FB:12:49:6A:70:A6:B4:AB:22:F4:32:6F:C6:  
9F:27:A1:2D:0C:66:B2:C4:45:28:A9:07:A9:DC:4E:B3

Extensions:

Identifier: Basic Constraints - 2.5.29.19

Critical: yes

Is CA: yes

Path Length Constraint: 0

Identifier: Key Usage: - 2.5.29.15

Critical: yes

Key Usage:

Digital Signature

Key CertSign

Crl Sign

Identifier: Authority Key Identifier - 2.5.29.35

Critical: no

Key Identifier:

F6:B8:04:27:0E:56:16:D9:B9:63:D9:FD:A1:54:65:41:

A0:08:48:2F

Identifier: Subject Key Identifier - 2.5.29.14

Critical: no

Key Identifier:

AA:E4:E7:63:72:DD:5D:AE:81:ED:BB:51:50:5D:F1:35:

71:7D:FD:9C

Identifier: CRLDistributionPoints - 2.5.29.31

Critical: no

Value:

30:82:01:1C:30:81:8D:A0:81:8A:A0:81:87:86:81:84:

6C:64:61:70:3A:2F:2F:63:72:6C:2E:63:68:61:6D:62:

2E:64:69:73:61:2E:6D:69:6C:2F:63:6E:25:33:44:45:

43:41:25:32:30:52:6F:6F:74:25:32:30:43:41:25:32:

43:25:32:30:6F:75:25:33:44:45:43:41:25:32:43:25:

32:30:6F:25:33:44:55:2E:53:2E:25:32:30:47:6F:76:

65:72:6E:6D:65:6E:74:25:32:43:25:32:30:63:25:33:

44:55:53:3F:63:65:72:74:69:66:69:63:61:74:65:72:

65:76:6F:63:61:74:69:6F:6E:6C:69:73:74:3B:62:69:

6E:61:72:79:30:81:89:A0:81:86:A0:81:83:86:81:80:

6C:64:61:70:3A:2F:2F:65:63:61:2D:64:73:2E:6F:72:

63:2E:63:6F:6D:2F:63:6E:25:33:44:45:43:41:25:32:

30:52:6F:6F:74:25:32:30:43:41:25:32:43:25:32:30:

6F:75:25:33:44:45:43:41:25:32:43:25:32:30:6F:25:

33:44:55:2E:53:2E:25:32:30:47:6F:76:65:72:6E:6D:

65:6E:74:25:32:43:25:32:30:63:25:33:44:55:53:3F:

63:65:72:74:69:66:69:63:61:74:65:72:65:76:6F:63:

61:74:69:6F:6E:6C:69:73:74:3B:62:69:6E:61:72:79

Identifier: Authority Info Access: - 1.3.6.1.5.5.7.1.1

Critical: no

Access Description:

Method #0: 1.3.6.1.5.5.7.48.2

Location #0: URIName: <http://eca.orc.com/certs/ecarootca.p7c>

Signature:

Algorithm: SHA1withRSA - 1.2.840.113549.1.1.5

Signature:

15:29:71:B6:75:B6:95:5C:01:0E:3A:15:BD:0D:27:17:  
45:CE:43:FF:8F:D7:E7:22:4D:CF:D5:6D:20:F8:C4:52:  
02:C6:44:97:DB:F0:99:19:36:B8:11:F0:9F:2D:09:C7:  
21:32:09:6B:00:F6:EB:DB:1F:EE:45:84:BE:D0:F3:03:  
72:92:C2:B4:5D:39:BE:C7:90:FD:F3:1A:34:01:8B:09:  
48:D5:96:87:40:87:8D:B8:37:44:B6:BB:AD:97:7A:A8:  
63:0B:AB:18:92:6E:1D:51:90:22:3B:8F:11:77:81:5F:  
83:5B:0A:96:F6:94:3D:38:A3:2F:80:40:D2:AE:45:55

## ORC ECA 2 Root Certificate:

Certificate Subject DN

**CN=ECA Root CA,OU=ECA,O=U.S. Government,C=US**

Certificate in base64 encoded format

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

```
MIICmDCCAgGgAwIBAgIBDjANBgkqhkiG9w0BAQUFADBLMQswCQYDVQQGEwJVUzEY
MBYGA1UEChMPVS5TLiBHb3Zlcm5tZW50MQwwCgYDVQQLEwNFQ0ExFDASBgNVBAMT
C0VDQSBSb290IENBMB4XDTA0MDYxNDEwMjAwOVoXDTQwMDYxNDEwMjAwOVoXDTQw
MAkGA1UEBhMCVVMxGDAWBgNVBAoTD1UuUy4gR292ZXJubWVudDEMMAoGA1UECxMD
RUNBMRQwEgYDVQQDEwTFQ0EgUm9vdCBDQTCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEArkr2eXIS6oAKIpDkOlcQZdMGdncoyGCEIU+ktqY3of5SVVXU7/it7kJ1
EUzR4ii2vthQtbww9aAnpQxcEmXZk8eEyiGEPy+cCQMIIbY+efOtKgjbQNDZ3IB9
19qzUJwBI2BMxslU1XsJQw9SK10IPbQm4asa8E8e5zTUknZBWNCAwEAAaOBizCB
iDAfBgNVHSMEGDAWgBT2uAQnDIYW2blj2f2hVGVB0AhILzAdBgNVHQ4EFgQU9rgE
Jw5WFtm5Y9n9oVRIQaAISC8wDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMB
Af8wJQYDVR0gBB4wHDAMBgpghkgBZQMCAQwBMAwGCmCGSAFIAwIBDAIwDQYJKoZI
hvcNAQEFBQADgYEAHh0EQY2cZ209aBb5q0wW1ER0dc4OGzsLyqjHfaQ4TEaMmUwL
AJRta/c4KVWLiwbODsvgJk+CaWmSL03gRW/ciVb/qDV7qh9Pyd1cOlanZTAnPog2
i82yL3i2fK9DCC84uoxEQbgqK2jx9bljFTwIAqITk9fGAm5mdT84IEwq1Gw=
```

-----END CERTIFICATE-----

Certificate Contents

Certificate:

Data:

Version: v3

Serial Number: 0xE

Signature Algorithm: SHA1withRSA - 1.2.840.113549.1.1.5

Issuer: CN=ECA Root CA,OU=ECA,O=U.S. Government,C=US

Validity:

Not Before: Monday, June 14, 2004 10:20:09 AM GMT

Not After: Thursday, June 14, 2040 10:20:09 AM GMT

Subject: CN=ECA Root CA,OU=ECA,O=U.S. Government,C=US

Subject Public Key Info:

Algorithm: RSA - 1.2.840.113549.1.1.1

Public Key:

Exponent: 65537

Public Key Modulus: (1024 bits) :

AE:4A:F6:79:72:12:EA:80:0A:22:90:E4:3A:57:10:65:

D3:06:76:77:28:CA:00:84:21:4F:A4:B6:A6:37:A1:FE:

52:55:55:D4:EF:F8:AD:EE:42:75:11:4C:D1:E2:28:B6:

BE:D8:50:B5:BC:30:F5:A0:27:A5:0C:5C:12:65:D9:93:

C7:84:CA:21:84:3F:2F:9C:09:03:25:94:16:3E:79:F3:

AD:2A:08:DB:40:D0:D9:DE:50:7D:D7:DA:B3:50:9C:01:

97:60:4C:C6:C9:54:D5:7B:09:43:0F:52:2B:5D:25:3D:

B4:26:E1:AB:1A:F0:4F:1E:E7:34:D4:92:76:41:5A:71

Extensions:

Identifier: Authority Key Identifier - 2.5.29.35

Critical: no

Key Identifier:

F6:B8:04:27:0E:56:16:D9:B9:63:D9:FD:A1:54:65:41:

A0:08:48:2F

Identifier: Subject Key Identifier - 2.5.29.14

Critical: no

Key Identifier:

F6:B8:04:27:0E:56:16:D9:B9:63:D9:FD:A1:54:65:41:  
A0:08:48:2F

Identifier: Key Usage: - 2.5.29.15

Critical: yes

Key Usage:

Digital Signature

Key CertSign

Crl Sign

Identifier: Basic Constraints - 2.5.29.19

Critical: yes

Is CA: yes

Path Length Constraint: UNLIMITED

Identifier: CertificatePolicies - 2.5.29.32

Critical: no

Value:

30:1C:30:0C:06:0A:60:86:48:01:65:03:02:01:0C:01:  
30:0C:06:0A:60:86:48:01:65:03:02:01:0C:02

Signature:

Algorithm: SHA1withRSA - 1.2.840.113549.1.1.5

Signature:

1E:1D:04:41:8D:9C:67:6D:3D:68:16:F9:AB:4C:16:D4:  
44:74:75:CE:0E:1B:3B:0B:CA:A8:C7:7D:A4:38:4C:46:  
8C:99:4C:0B:00:94:6D:6B:F7:38:29:55:8B:8B:06:CE:  
0E:CB:E0:26:4F:82:69:69:92:2F:4D:E0:45:6F:DC:89:  
56:FF:A8:35:7B:AA:1F:4F:C9:DD:5C:3A:56:A7:65:30:  
27:3E:88:36:8B:CD:B2:2F:78:B6:7C:AF:43:08:2F:38:  
BA:8C:44:41:B8:2A:2B:68:F1:F5:B2:23:15:3C:25:02:  
A2:13:93:D7:C6:02:6E:66:75:3F:38:20:4C:2A:D4:6C