StartCom Application

V1

July 2017

Contents

[Introduction 3](#_Toc487111622)

[CA information 3](#_Toc487111623)

[Root Certificates 4](#_Toc487111624)

[StartCom Root CA G3 4](#_Toc487111625)

[Summary 4](#_Toc487111626)

[CRL 5](#_Toc487111627)

[OCSP 5](#_Toc487111628)

[Other 5](#_Toc487111629)

[StartCom Root CA ECC 6](#_Toc487111630)

[Summary 6](#_Toc487111631)

[CRL 6](#_Toc487111632)

[OCSP 7](#_Toc487111633)

[Other 7](#_Toc487111634)

# Introduction

## CA information

Name: StartCom

Website URL: [www.startcomca.com](http://www.startcomca.com)

Organizational type: Private organization

Primary market: worldwide

Impact to mozilla users: StartCom is a private organization which provides certificates worlwide and has become the 6th largest CA worldwide due to the number of certificates issued.

StartCom has performed all the tasks requested by Mozilla after being distrusted and now is requesting again for inclussion in the Mozilla products.

**POC**

Name: Iñigo Barreira

Title: CEO

Email: [inigo@startcomca.com](mailto:inigo@startcomca.com)

Phone number: +34 944 007 736

Additional POC

Name: Jane Jiang

Email: [v6@startssl.com](mailto:v6@startssl.com)

# Root Certificates

## StartCom Root CA G3

|  |  |
| --- | --- |
| Friendly Name | StartCom Root CA G3 |
| Version | V3 |
| Signature algorithm | Sha256RSA |
| Subject | CN = StartCom Certification Authority G3  O = StartCom CA  C = ES |
| Issuer | CN = StartCom Certification Authority G3  O = StartCom CA  C = ES |
| Valid | 2017-03-22 to 2042-03-22 |
| Basic Constraints | Critical |

### Summary

This root certificate, G3, is inteded to issue only SSL certificates. It has 2 subCAs, one for SSL EV certificates exclusively and the other one for BR certificates of the DV, IV and OV types.

Root certificate URL: <https://www.startcomca.com/root>

SHA-1 fingerprint: ‎68 9a 12 29 d6 98 d1 72 e9 9e 1b f0 0b 9c 19 85 41 19 c9 fc

Validity period: March 22, 2017 15:19:56 to March 22, 2042 15:17:58

Public key length: 4096 bits (RSA)

Test website: <https://valid.startcomca.com>, <https://revoked.startcomca.com>, and <https://expired.startcomca.com>

### CRL

**End-entity**

<http://crl.startcomca.com/sca-server4.crl> for EV

<http://crl.startcomca.com/sca-server3.crl> for OV

<http://crl.startcomca.com/sca-server2.crl> for IV

<http://crl.startcomca.com/sca-server1.crl> for DV

**Intermediate CAs**

<http://crl.startcomca.com/sfscaev.crl> for EV ICA

<http://crl.startcomca.com/sfscabr.crl> for BR ICA

Next-update value: 48 hours

CPS v3.2 section 4.9.7 CRL issuance frequency

### OCSP

URL: <http://ocsp.startcomca.com>

AIA

<http://aia.startcomca.com/certs/sca.server4.crt> for EV

<http://aia.startcomca.com/certs/sca.server3.crt> for OV

<http://aia.startcomca.com/certs/sca.server2.crt> for IV

<http://aia.startcomca.com/certs/sca.server1.crt> for DV

### Other

Maximum delayed time for publishing revocation: less than an hour

CPS v3.2 section is 4.10.2 OCSP responder service

Validity OCSP response is 2 days

Requested trust bits: Websites (SSL/TLS)

SSL validation type: StartCom provides DV, IV, OV and EV SSL certificate types performing all the validation procedures indicated in the CAB Forum documents

**EV policy**

OID: 1.3.6.1.4.1.23223.1.1.1

OID: 2.23.140.1.1

## StartCom Root CA ECC

|  |  |
| --- | --- |
| Friendly Name | StartCom Root CA ECC |
| Version | V3 |
| Signature algorithm | Ecdsa-with-SHA384 |
| Subject | CN = StartCom Certification Authority ECC  O = StartCom CA  C = ES |
| Issuer | CN = StartCom Certification Authority ECC  O = StartCom CA  C = ES |
| Valid | 2017-03-22 to 2042-03-22 |
| Basic Constraints | Critical |

### Summary

This root certificate, ECC, is inteded to issue only certificates for signing emails or documents, it has 2 subordinate CAs, with different validity times. SubCA CC is for issuing client certificates of what we call class 1, 2 and 3, which basically depends on the validation method, being the class 1 with no validation, just the email, and class 3 with a complete process to validate the identity of the subscriber. The subCA CC2 is a new one, technically constrained, following the Google requirements for S/MIME certificate type and intended to issue only class 1.

Root certificate URL: <https://www.startcomca.com/root>

SHA-1 fingerprint: ‎ ‎b5 10 85 d9 5b 95 da 91 20 12 d2 c3 b0 01 9a 2d c4 6d 26 e3

Validity period: March 22, 2017 15:22:33 to March 22, 2042 15:20:31

Public key length: 384 Bits (ECDSA)

### CRL

**End-entity**

<http://crl.startcomca.com/sca-client3.crl> for class 3 from CC ICA

<http://crl.startcomca.com/sca-client2.crl> for class 2 from CC ICA

<http://crl.startcomca.com/sca-client1.crl> for class 1 from CC ICA

<http://crl.startcomca.com/sca-client22.crl> for class 1 from CC2 ICA

**Intermediate CAs**

<http://crl.startcomca.com/sfscacc.crl> for CC ICA

<http://crl.startcomca.com/sfscacc2.crl> for CC2 ICA

Next-update value: 48 hours

CPS v3.2 section 4.9.7 CRL issuance frequency

### OCSP

URL: <http://ocsp.startcomca.com>

AIA

<http://aia.startcomca.com/certs/sca.client3.crt> for class 3 from CC ICA

<http://aia.startcomca.com/certs/sca.client2.crt> for class 2 from CC ICA

<http://aia.startcomca.com/certs/sca.client1.crt> for class 1 from CC ICA

<http://aia.startcomca.com/certs/sca.client22.crt> for class 1 from CC2 ICA

### Other

Maximum delayed time for publishing revocation: less than an hour

CPS v3.1 section is 4.10.2 OCSP responder service

Validity OCSP response is 2 days

Requested trust bits: Email (S/MIME)