Bugzilla ID: 602750
Bugzilla Summary: Add Renewed StartCom root certificate

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	Data
CA Name	StartCom
Website URL	http://www.startssl.com
Organizational type	Public Corporation
Primary market / customer base	StartCom is a commercial corporation with customers worldwide, and is the producer and vendor of the StartCom Linux operating systems, operates the StartCom Certification Authority and MediaHost.
CA Contact Information	CA Email Alias: certmaster@startcom.org CA Phone Number: 972-8634-4170 Title / Department: CA

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	Data
Certificate Name	StartCom Certification Authority
Cert summary / comments	This is the SHA256 version of the root certificate that was approved for inclusion in bug #362304. StartCom operates intermediate CA certificates arranged in 4 different verification levels (classes) and certificate types (server, client, code). Class 1 is used for server and email; Class 2, Class 3, and Class 4 are used for server, email, and code signing.
Root Cert URL	https://www.startssl.com/certs/ca-sha2.pem
SHA-1 fingerprint	A3:F1:33:3F:E2:42:BF:CF:C5:D1:4E:8F:39:42:98:40:68:10:D1:A0
Valid from	2006-09-17
Valid to	2036-09-17
Cert Version	3
Modulus length	4096
Test Website	For testing purposes, please provide a URL to a website whose EV SSL cert chains up to this root. https://www.startssl.com/ chains up to the SHA1 root. I deleted that root and imported this new root, then tried this website. Then I got the Untrusted Connection error.
CRL URL	CRL HTTP URL: According to CRL distribution points in intermediate and end-user certificates (varies according to class level and certificates type).

	http://cert.startcom.org/sfsca-crl.crl In https://www.startssl.com/policy.pdf, section titled "Distribution of Certificate Revocation List" CRLs of subscriber certificates are updated at least every 12 hours or every time a certificate is revoked
OCSP Responder URL	OCSP URL: According to AIA OCSP URI set in the certificates (varies according to class level and certificates type). http://ocsp.startcom.org/sub/class2/server/ca In https://www.startssl.com/policy.pdf, section titled "OCSP Responder Service": The OCSP responder provides results about the status of a certificate instantly. The current CRLs are reloaded at least every 60 minutes.
CA Hierarchy	The StartCom PKI is structured by different Class levels (1 - 3, EV) and different purposes (SSL/TLS Server, Client S/MIME, Object Code) and every Class and purpose is handled by a different intermediate CA. https://www.startssl.com/certs/ StartCom Certification Authority sub-CAs: -> StartCom Class 1 Primary Intermediate Client CA -> StartCom Class 1 Primary Intermediate Domain Controller CA -> StartCom Class 1 Primary Intermediate Server CA -> StartCom Class 2 Primary Intermediate Client CA -> StartCom Class 2 Primary Intermediate Object CA -> StartCom Class 2 Primary Intermediate Server CA -> StartCom Class 3 Primary Intermediate Client CA -> StartCom Class 3 Primary Intermediate Object CA -> StartCom Class 3 Primary Intermediate Server CA -> StartCom Extended Validation Client CA -> StartCom Extended Validation Server CA
Externally operated subCAs	Does this root have any subordinate CAs that are operated by external third parties? If yes, please see https://wiki.mozilla.org/CA:SubordinateCA_checklist The https://www.startssl.com/policy.pdf has provisions for externally operated subCAs: Organizations wishing to operate an external intermediate CA enter into a contractual relationship with the StartCom CA and must commit to all requirements of the StartCom CA policies, including the lowest validation levels, physical and operational standards and practices.
Cross-Signing	List any other root CAs that have issued cross-signing certificates for this root CA.
Requested Trust Bits	Websites Email Code Signing
SSL Validation Type	DV, OV, and EV Class 1 are DV, Class 2 are IV, Class 3 are OV, and there is a separate intermediate CA for EV.

If DV – email addresses used for verification	In https://www.startssl.com/policy.pdf, section titled "Ceritification Rules", Class 1: ● webmaster@domain.com ● hostmaster@domain.com ● postmaster@domain.com
EV policy OID(s)	1.3.6.1.4.1.23223.2
CP/CPS	Document Repository: https://www.startssl.com/?app=26 CP and CPS: https://www.startssl.com/policy.pdf EV CP: https://www.startssl.com/extended.pdf
AUDIT	Auditor: Ernst & Young Auditor Website: www.ey.com/il Audit Type: WebTrust CA Audit Report and Management Assertions: https://www.startssl.com/ey-webtrust.pdf (2009.12.31) Audit Type: WebTrust EV Audit Report and Management Assertions: https://www.startssl.com/ey-webtrust-ev.pdf (2009.12.31) Audit Type: Witness of Key Ceremony for new EV Root Audit Report and Management Assertions: https://bugzilla.mozilla.org/attachment.cgi?id=481737 (2010.08.11) I'll send email to the auditor to confirm the authenticity of the documents.
Organization Identity Verification	See https://www.startssl.com/policy.pdf, section titled "Ceritification Rules", Class 2, Class 3, and Extended Validation.
Domain Name Ownership / Control	DV: Challenge-response via email is used, existence of domain name is verified by checking WHOIS records provided by the registrar, and additional checks are performed as needed. See https://www.startssl.com/policy.pdf, section titled "Ceritification Rules", Class 1. Does it say somewhere in the CP/CPS that all certs must at least meet the requirements of Class 1? E.g. all certs must meet the requirements of its Class, as well as all of the lower Classes? In particular, are the verification steps that are taken for Class 1 SSL certs also taken for Class 2 and Class 3 SSl certs?
Email Address Ownership / Control	Challenge-response via email is used to conform ownership of the email account. See https://www.startssl.com/policy.pdf, section titled "Ceritification Rules", Class 1. Is the challenge-response mechanism used for all S/MIME certs regardless of Class level? It's only described in Class 1.
Identity of Code Signing Subscriber	According to the "Certificate Profiles" section of https://www.startssl.com/policy.pdf, Code Signing certificates are issued under Class 2 and Class 3. The steps taken to verify the identity and authorization of the individual and the identity and existence of the organization are described in the section titled "Ceritification Rules", in Class 2 and Class 3.

Potentially Problematic Practices	Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). Identify the ones that are and are not applicable. For the ones that are applicable, please provide further information.
	• 1.1 Long-lived DV certificates
	  ○ The DV SSL certs are valid for one year.
	• 1.2 Wildcard DV SSL certificates
	  ○ Found in https://www.startssl.com/policy.pdf section called "Certification Rules": "Wild card domain names like *.domain.com are only issued to Class 2 or higher validated subscribers. Likewise multiple domain names within the same certificate are not supported in the Class 1 settings."
	  ○ Wild cards and multiple domain names (SNI) require at least Class 2 validation. Class 2 is identity validated for individuals, organization validation is optional. However OV always implies prior IV validation of the subscriber (and therefore responsible person).
	• 1.3 Email Address Prefixes for DV Certs
	  ○ See https://www.startssl.com/policy.pdf, section titled "Ceritification Rules", Class 1.
	  ▪ webmaster@domain.com
	  ▪ hostmaster@domain.com
	  ▪ postmaster@domain.com
	• 1.4 Delegation of Domain / Email validation to third parties
	  ○ ?
	• 1.5 Issuing end entity certificates directly from roots
	  ○ From https://www.startssl.com/policy.pdf: "The StartCom CA root is an off-line CA and shall be used only for the signing of Intermediate CA certificates and the relevant Certificate Revocation Lists.
	• 1.6 Allowing external entities to operate subordinate CAs
	  ○ All sub-CAs are operated in StartCom premises.
	• 1.7 Distributing generated private keys in PKCS#12 files
	  ○
	• 1.8 Certificates referencing hostnames or private IP addresses
	  ○ IP addresses are validated as per https://www.startssl.com/policy.pdf, section titled "Ceritification Rules", Class 1, IP Addresses.
	• 1.9 Issuing SSL Certificates for Internal Domains
	  ○
	• 1.10 OCSP Responses signed by a certificate under a different root
	  ○
	• 1.11 CRL with critical CIDP Extension
	  ○
	• 1.12 Generic names for CAs
	  ○ CN includes StartCom