Bugzilla ID: 451298
Bugzilla Summary: Enable EV and code signing for StartCom Root

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.

General Information	Data
CA Name	StartCom
Website URL (English version)	https://www.startssl.com/
Organizational type	public corporation
Primary market / customer base. (Which types of customers does the CA serve? Are there particular vertical market segments in which it operates? Does it focus its activities on a particular country or other geographic region?)	StartCom is a commercial corporation with customers worldwide, and is the producer and vendor of the StartCom Linux operating systems, operates the StartSSL™ Certification Authority and MediaHost™.

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 root is already included in NSS. This request is to enable the root for EV and code signing. All of the subordinate CAs issued from this root are operated internally.
The root CA certificate URL	https://www.startssl.com/certs/ca.crt The StartCom Authority Certificates Repository is at https://www.startssl.com/certs/
SHA-1 fingerprint.	3E:2B:F7:F2:03:1B:96:F3:8C:E6:C4:D8:A8:5D:3E:2D:58:47:6A:0F
Valid from	2006-09-17
Valid to	2036-09-17
Cert Version	3
Modulus length	4096
CRL • URL • update frequency for end-entity certificates	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,

	whichever comes first. CRLs are published via Internet download. Each intermediate CA issues its own corresponding CRL for the certificates it issues. The CRL distribution points are included in the certificates. The CRL of root and intermediate CA certificates are updated once a year.
OCSP (if applicable) • OCSP Responder URL • Max time until OCSP responders updated to reflect end-entity revocation	http://ocsp.startcom.org/sub/class2/server/ca In https://www.startssl.com/policy.pdf, section titled "OCSP Responder Service" OCSP responder service is provided and the respective URL location of the service are included in the certificates. The current CRLs are reloaded at least every 60 minutes.
List or description of subordinate CAs operated by the CA organization associated with the root CA. (For example, this might include subordinate CAs created to issue different classes or types of end entity certificates: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on.) For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant CPS, and that any audit covers them as well as the root.	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. Therefore an intermediate CA certificate is responsible for the signing if EV end-user server certificates. From https://www.startssl.com/certs/: StartCom Certification Authority -> 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 All are addressed in https://www.startssl.com/policy.pdf.
For subordinate CAs operated by third parties, if any: General description of the types of third-party subordinates that exist, and what the general legal/technical arrangements are by which those subordinates are authorized, controlled, and audited.	In https://www.startssl.com/policy.pdf, section titled "CA Structure" There is a sub-CA category for external sub-CAs. In https://www.startssl.com/policy.pdf, section titled "StartCom Intermediate CA Program (SICAP)": "Middle to bigger sized organizations may request to run an intermediate certification authority, which allows a limited role as intermediate CA operator…. **The intermediate CA is operated at StartCom's premise** and the organization must accept all conditions and terms as outlined in the StartCom Intermediate Certification Authority Policy Appendix."

List any other root CAs that have issued cross-signing certificates for this root CA	None
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code (Code Signing)	Websites Email Code
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: • Whether or not the domain name referenced in the certificate is verified to be owned/controlled by the certificate subscriber. (This is commonly referred to as a DV certificate.) • Whether or not the value of the Organization attribute is verified to be that associated with the certificate subscriber. (This is commonly referred to as an OV certificate.) • Whether verification of the certificate subscriber conforms to the Extended Validation Certificate Guidelines issued by the CAB Forum. (This is commonly referred to as an EV certificate.)	DV, OV, EV Class 1 are DV Class 2 are IV Class 3 are OV New intermediate CA for EV
EV policy OID	1.3.6.1.4.1.23223.2
Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable.	https://forum.startcom.org
CP/CPS	StartCom Certification Authority Policy and Practice Statements:

	https://www.startssl.com/policy.pdf StartCom Certification Authority Extended Validation Certificates Policy Appendix: https://www.startssl.com/extended.pdf
AUDIT	Audit Type: WebTrust CA Auditor: Ernst & Young Auditor Website: www.ey.com/il Audit Report and Management Assertions: https://bugzilla.mozilla.org/attachment.cgi?id=366567 Audit Type: WebTrust EV Auditor: Ernst & Young Auditor Website: www.ey.com/il Audit Report and Management Assertions: https://bugzilla.mozilla.org/attachment.cgi?id=366568 From: Udi.Gelbort@il.ey.com Subject: Re: Verification of Audit Reports for StartCom To: "Kathleen Wilson" <kathleen95014@yahoo.com> Date: Tuesday, March 10, 2009, 12:52 PM Dear Kathleen, I've checked the reports you've linked bellow and I approve that Ernst & Young Israel has audited StartCom and posted these two reports. Best Regards, Udi.

Review CPS sections dealing with subscriber verification (COMPLETE)

- Verify domain check for SSL
    - Found in https://www.startssl.com/policy.pdf section called “Certification Rules”
        - “Additionally the existence of the domain name is verified by checking the WHOIS records provided by the domain name registrar.”
        - “Extended Validation for organizations are performed according to the validation procedures and requirements of the Extended Validation Guidelines as published by the CA/Browser Forum. Applicants for EV must be at least Class 2 Identity validated prior to engagement for Extended validation.”

        - Also in https://www.startssl.com/policy.pdf in the section "Certificate Profiles -> Naming conventions" it shows that the domain name is validated for SSL certificates for each class.
- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber's legal identity.
    - Found in https://www.startssl.com/policy.pdf section called "Certification Rules"
        - "Email accounts are validated by sending an electronic mail message with a verification code to the email account in question. The subscriber has to return and submit the verification code as prove of ownership of the email account within a limited period sufficient enough to receive an electronic mail message."
    - Also in https://www.startssl.com/policy.pdf in the section "Certificate Profiles -> Naming conventions" it shows that the email address is validated for each cert type within each class.
- Verify identity info in code signing certs is that of subscriber
    - From Eddy Nigg: Under the StartCom CA Policy -> Certificate Profiles -> Naming conventions, each certificate Class and Type is listed. Object Code Signing is not applicable under Class 1 and not listed and not issued. The minimum validation level for Object Code Signing is Class 2 -> Identity Validation. Also note that no Class 1 Intermediate CA certificate exists for object code signing.
- Make sure it's clear which checks are done for which context (cert usage)

Flag Problematic Practices (COMPLETE)
(http://wiki.mozilla.org/CA:Problematic_Practices)

- Long-Lived Domain-Validated SSL certs
    - The DV SSL certs are good for one year.
- Wildcard DV SSL certs
    - 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).
- Issuing end entity certs directly from root rather than using an offline root and issuing certs through a subordinate CA
    - 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.
- Allowing external entities to operate subordinate CAs
    - All sub-CAs are operated in StartCom premises.
- Distributing generated private keys in PKCS#12 files
    - Not Found
- Certificates referencing hostnames or private IP addresses
    - It looks like IP addresses can be referenced, as per https://www.startssl.com/policy.pdf section called "Certification Rules"

    - Comment #4: The issuing of IP based certificates is maintained (for historical reasons) for the StartCom Intermediate CA Program and conditional. Currently StartCom does not issue certificates for IP addresses from this root but only for fully qualified domain names.
- OCSP Responses signed by a certificate under a different root
    - Able to go to the test https site with OCSP enforced.
- CRL with critical CIDP Extension
    - CRL downloads into Firefox without error.

Verify Audits (COMPLETE)
(Sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/)

- Validate contact info in report, call to verify that they did indeed issue this report.
    - Audit reports have been verified by contacting the auditor via email.
- For EV CA's, verify current WebTrust EV Audit done.
    - Audits are current – December 31, 2008
- Review Audit to flag any issues noted in the report
    - No issues noted in reports