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	Will be needed before starting discussion.
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 From policy.pdf: CRLs are updated at least every 12 hours or upon adding of a new entry, e.g. every time a certificate is revoked. However the next update entry in the CRL is set to 48 hours.
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 EV: http://ocsp.startssl.com/sub/class4/server/ca From policy.pdf: 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	Comment #5: The StartCom CA policy operates all CA certificates, being it for "internal" use or being it for third parties. There are no CA certificates that are controlled by any third party.
Cross-Signing	Comment #5: There will be a third party cross-signed CA root and I'll publish this information prior to the public discussion. Also here the same rule applies and the CA keys and roots are exclusively controlled by StartCom. In the same manner, StartCom has overall responsibility, oversight and rights.
Requested Trust Bits	Websites Email Code Signing
SSL Validation Type	DV, OV, and EV Class 1 are DV, Class 2 are IV/OV, 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 Addendum to CP and CPS: https://www.startssl.com/policy-addendum-2010.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)

	-------- Original Message -------- Subject: Re: Confirming Authenticity of Audit Reports from StartCom Date: Sun, 17 Oct 2010 15:48:30 +0300 From: Udi.Gelbort@il.ey.com … This is to confirm that Ernst & Young (Israel) has issued those audit reports. Best regards, Udi
Organization Identity Verification	From policy.pdf: Certification Rules Validations The StartCom CA performs the following validations and verifications according to the following rules: Class 1 ● Email Addresses 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. The validation may be valid for 30 days for the generation of digital certificates. ● Domain Names Fully qualified domain names, typically “www.domain.com” or “domain.com” are validated by sending an electronic mail message with a verification code to one of the following administrative electronic mail accounts: ● webmaster@domain.com ● hostmaster@domain.com ● postmaster@domain.com The subscriber has to return and submit the verification code as prove of ownership of the domain name within a limited period sufficient enough to receive an electronic mail message. Additionally the existence of the domain name is verified by checking the WHOIS records provided by the domain name registrar. If the WHOIS data contain additional email addresses, they may be offered as additional choices to the above mentioned electronic mail accounts. The StartCom CA performs additional sanity and fraud prevention checks in order to limit accidental issuing of certificates whose domain names might be misleading and/or might be used to perform an act of fraud, identity theft or infringement of trademarks. 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. The validation may be valid for 30 days for the generation of certificates. ● IP Addresses IP Addresses representing a dotted IPv4 address, typically “10.0.0.1” (*) are validated by sending a electronic mail message with a verification code to one of the following administrative mail accounts: ● webmaster@10.0.0.1 ● hostmaster@10.0.0.1 ● postmaster@10.0.0.1 The subscriber has to return and submit the verification code as prove of ownership of the domain name within a limited period sufficient enough to receive an electronic mail message. The validation may be valid for 30 days for the generation of digital certificates. (*) The IP 10.0.0.1 is an illustrative example. Class 2

	● Personal Identity The verification process of personal identities of subscribers are performed manually. The StartCom CA validates without any reasonable doubt that the following details are correct: ● First and last name ● Residence, Address ● State or Region ● Country The subscriber has to provide in a secure and reliable fashion two scanned or photographed identification papers in high quality and resolution. The documents must be valid in every respect and not be expired. If the accuracy of the documents are in doubt as to the correctness of the details provided, the StartCom CA may request the original documents and/or a copy of the original document confirmed, signed and stamped by the issuing authority or Latin notary via postal mail. Any document obtained physically may be scanned or photographed for archiving purpose at the premise of the StartCom CA and shall be returned to the sender via registered postal mail. StartCom verifies the correctness of the identity through confirmation procedures of the submitted documents with third party sources and cross-verification of the claimed identity. In the absence of third party sources or listing thereof, a registered postal mail is sent to the claimed address and identity. The validation may be valid for 350 days for the generation of digital certificates. ● Organization The verification process of organizations implies same level identity validation of the subscriber (responsible person) and are performed manually. The StartCom CA validates without any reasonable doubt that the following details are correct: ● Registered organization name ● Address ● State or Region ● Country The subscriber has to provide in a secure and reliable fashion supporting documentation. The documents must be valid in every respect and not be expired. If the accuracy of the documents are in doubt as to the correctness of the details provided, the StartCom CA may request the original documents and/or a copy of the original document confirmed, signed and stamped by the issuing authority via postal mail. Any document obtained physically may be scanned or photographed for archiving purpose at the premise of the StartCom CA and shall be returned to the sender via registered postal mail. StartCom verifies the correctness of the organization details through confirmation procedures of the submitted documents with third party sources and cross-verification of the claimed organization. In the absence of third party sources or listing thereof, a registered postal mail is sent to the claimed address and organization name. The validation may be valid for 350 days for the generation of digital certificates. Class 3 ● Personal Identity and Organization Class 3 validation is reserved for specially trusted entities to which the StartCom CA has usually a relationship like business partnership which includes employees, investors, business partners and operators of intermediate CAs. The StartCom CA management knows without any doubt the entity in question. The StartCom CA is in the possession or has reviewed original documents during face-to-face meetings about the entity in question. The validation may be valid for 365 days for the generation of digital certificates. From policy-addendum-2010.pdf [Insert at Security - Validations – Class 2 - Organization:]

	The subscriber has to provide in a secure and reliable fashion supporting documentation which must be either from a Qualified Government Information Source, Qualified Government Tax Information Source or Qualified Independent Information Source. [Add at Security - Validations – Class 2 - Organization:] StartCom confirms and verifies that the subscriber is duly authorized to represent the organization and obtain the certificates on their behalf by obtaining an authorization statement and by contacting the authorizer. The obtained and confirmed organization documents should state the authorizer and position, but StartCom may rely on other means and sources to obtain the necessary authority if necessary. StartCom may assume proper authorization in case the validated subscriber is either the appointed CEO, Director, President or owner and sole proprietor. [Add at Certificate Profiles – Naming conventions:] Class 1 Client Authentication and S/MIME certificates The fields common name (CN), organization (O) and country (C) MAY be omitted until the 30th of June 2011. Starting at the 1st of July 2011 these fields MUST be omitted. SSL/TLS server certificates The fields organization (O), organizational unit (OU) and country (C) MAY be omitted until the 30th of June 2011. Starting at the 1st of July 2011 these fields MUST be omitted. Class 1 + Web-of-Trust Community Validated Client Authentication and S/MIME certificates The organization (O) MAY be omitted until the 30th of June 2011. Starting at the 1st of July 2011 this field MUST be omitted. SSL/TLS server certificates The organization unit (OU) MAY be omitted until the 30th of June 2011. Starting at the 1st of July 2011 this field MUST be omitted. From https://www.startssl.com/extended.pdf 4.1.1.2. Certificate Request Requirements Applicants for EV certificates must be at least Class 2 validated prior to engagements for extended validation. The applicant shall serve as the “Contract Signer”, “Certificate Approver”, and “Certificate Requester” as defined by the Extended Validation Guidelines. The applicants must make the request by the designated utility at the from the StartCom CA operated web site and sign the “StartCom Extended Validation Subscriber Agreement”. 4.1.2. Enrollment process and responsibilities The StartCom CA verifies the applicants authorization for signing the “StartCom Extended Validation Subscriber Agreement” and authorization for approving and requesting EV certificates on behalf of the subscriber according to the requirements of the Extended Validation Guidelines. 4.2 Certificate application processing 4.2.1. Performing identification and authentication functions The StartCom CA verifies the applicants legal existence and identity according to the “Verification Requirements” and “Methods of Verification” specified in the Extended Validation Guidelines as published by the CA/Browser Forum.
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. It is not clear to me if the DV validation that is described for Class 1 certs must also be performed for Class 2, Class 3, and EV certs. If this is the case, then I think this should be made clear in the CP/CPS documents. Comment #5: we'll add this to our current addendum and eventually to the new policy.

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. It is not clear to me if the email challenge-response mechanism that is described for Class 1 email address verification must also be performed for Class 2 and Class 3 certs. If this is the case, then I think this should be made clear in the CP/CPS documents. Comment #5: we'll add this to our current addendum and eventually to the new policy. The current addendum is at https://www.startssl.com/policy-addendum-2010.pdf
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	http://wiki.mozilla.org/CA:Problematic_Practices
	• 1.1 Long-lived DV certificates
	  ○ The DV SSL certs are valid for one year.
	• 1.2 Wildcard DV SSL certificates
	  ○ From 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
	  ○ Comment #5: There are no CA certificates that are controlled by any third party.
	  ○ From policy.pdf: The StartCom CA does not maintain registration authorities.
	• 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
	  ○ From policy.pdf Subscriber Obligations: Never share the private key with any other party
	• 1.8 Certificates referencing hostnames or private IP addresses
	  ○ From policy.pdf, section titled "Ceritification Rules", Class 1, IP Addresses: IP Addresses representing a dotted IPv4 address, typically "10.0.0.1" (*) are validated by sending a electronic mail message with a verification code to one of the following administrative mail accounts:
	  ▪ webmaster@10.0.0.1
	  ▪ hostmaster@10.0.0.1
	  ▪ postmaster@10.0.0.1
	  ○ The subscriber has to return and submit the verification code as prove of ownership of the domain name

	within a limited period sufficient enough to receive an electronic mail message. The validation may be valid for 30 days for the generation of digital certificates. (*) The IP 10.0.0.1 is an illustrative example.
	• 1.9 Issuing SSL Certificates for Internal Domains
	  ○ Not found.
	• 1.10 OCSP Responses signed by a certificate under a different root
	  ○ No.
	• 1.11 CRL with critical CIDP Extension
	  ○ No.
	• 1.12 Generic names for CAs
	  ○ CN includes StartCom