Bugzilla ID: 370627
Bugzilla Summary: Add S-TRUST root certificates

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.

General Information	**Data**
CA Name	Deutscher Sparkassen Verlag GmbH S-TRUST is a trademark of Deutscher Sparkassen Verlag GmbH
Website URL (English version)	https://www.s-trust.de/
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	Deutscher Sparkassen Verlag GmbH is the world's largest smartcard provider and the central certification service provider for all German savings banks. This CA exists to enable up to 40 million German customers (end-users) to use their banking card as a certificate based signature, encryption and authentication device.
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?)	The business purpose of the root certificates is to provide all customers of the German Savings Bank Financial Group with client-certificates for his/her signature enabled debit card (smartcard). The German Financial Group consists of 463 Savings banks with about 17.000 branches, 11 State banks, 11 State home loan banks, 12 Groups of primary insurers, 2 Factoring companies, 6 Leasing companies, 80 Venture capital companies and others. All German citizen are able to get one of these signature cards. These signature cards are used to • secure email communication using Mozilla Thunderbird • enable secure web-access with Mozilla Firefox e.g. for Online Banking/Brokerage (instead of pass-word and login) • sign legally binding transactions e. g. qualified signing of a contract • access more than 170 e-government applications like electronic tax-declaration Certificates will be issued to all Online Banking customers (private and business) of the German Savings Banks. Until the end of 2008 there will be about 45 Million signature enabled debit cards in the German market to be potentially equipped with S-TRUST certificates.

Comment in initial Bugzilla request:

Number of roots Deutscher Sparkassenverlag (DSV) wants to submit:
"…up to 8 roots in the next 5 years. Due to German legal requirements we have to issue one new so called "Qualified Root" every year (root renewal), in order to enable our customers to be consistent with these legal requirements. These "Qualified Roots" have a re-stricted validity time of 5 years and can be removed from the Mozilla-related software products certificate storage right after expiration to reduce the number of S-TRUST roots to a minimum. (German Signature Law: Germany was the first European country to transpose the European Community Signature Directive into national law. This law enables digital signatures created in conjunction with a qualified certificate to be the legal equivalent to hand written signatures. Due to the strict security demands of this law there are only a few PKI Providers which are approved by German authorities to issue qualified certificates. DSV is the first and only officially declared PKI Provider to issue qualified certificates on Bank Cards)."

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

Info Needed	**Data**	**Data**	**Data**	**Data**	**Status / Notes**
Certificate Name	S-TRUST Authentication and Encryption Root CA 2005:PN	S-TRUST Qualified Root CA 2006-001:PN	S-TRUST Qualified Root CA 2007-001:PN	S-TRUST Qualified Root CA 2008-001:PN	COMPLETE
Cert summary / comments	This root will provide all customers of the German Savings Bank Financial Group with client certificates for their signature-enabled debit cards (smartcards).				COMPLETE
The root CA certificate URL Download into FireFox and verify	http://www.s-trust.de/service_support/zertifikatsmanagement/verzeichnisdienste/download_wurzelzertifikate/ordner_crt_dateien/authentication.crt	http://www.s-trust.de/service_support/zertifikatsmanagement/verzeichnisdienste/download_wurzelzertifikate/ordner_crt_dateien/S-TRUST_Qualified_Root_CA_2006-001_PN.crt	http://www.s-trust.de/service_support/zertifikatsmanagement/verzeichnisdienste/download_wurzelzertifikate/ordner_crt_dateien/STRUSTQualifiedRootCA2007-001.crt	http://www.s-trust.de/service_support/zertifikatsmanagement/verzeichnisdienste/download_wurzelzertifikate1/ordner_crt_dateien/S-TRUSTQualifiedRootCA2008-001_v3_509.crt	COMPLETE
SHA-1 fingerprint.	BE:B5:A9:95:74:6B:9E:DF:73:8B:56:E6:DF:43:7A:77:BE:10:6B:81	7D:DC:76:1C:FD:AF:4C:E0:3A:B5:3A:DD:C9:FA:13:35:19:A3:DE:C9	7A:3C:1B:60:2E:BD:A4:A1:E0:EB:AD:7A:BA:4F:D1:43:69:A9:39:FC	C9:2F:E6:50:DB:32:59:E0:CE:65:55:F3:8C:76:E0:B8:A8:FE:A3:CA	COMPLETE
Valid from	2005-06-21	2005-12-31	2006-12-31	2007-12-31	COMPLETE

Valid to	2030-06-21	2010-12-30	2011-12-30	2012-12-30	COMPLETE
Cert Version	3	3	3	3	COMPLETE
Modulus length / key length	2048	2048	2048	2048	COMPLETE
CRL - URL - update frequency for end-entity certificates	http://onsitecrl.s-trust.de/DeutscherSparkassenVerlagGmbHSTRUSTQualifiedRootCA2005001PN/LatestCRL.crl	http://onsitecrl.s-trust.de/DeutscherSparkassenVerlagGmbHSTRUSTQualifiedRootCA2006001PN/LatestCRL.crl	http://onsitecrl.s-trust.de/DeutscherSparkassenVerlagGmbHSTRUSTQualifiedRootCA2007001PN/LatestCRL.crl	http://onsitecrl.s-trust.de/DeutscherSparkassenVerlagGmbHSTRUSTQualifiedRootCA2008001PN/LatestCRL.crl	COMPLETE Comment #24: “CRLs will be updat hours.”
OCSP (if applicable) - OCSP Responder URL	http://ocsp-q.s-trust.de	http://ocsp-q.s-trust.de/	http://ocsp-q.s-trust.de/	http://ocsp-q.s-trust.de/	COMPLETE
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	There are no subordinate CAs for this CA available.	There are up to 10 subordinate CAs which eventually issue end-user certificates which are stored on the banking signature cards. These subordinate CAs are all operated internally by Deutscher Sparkassen Verlag GmbH. A certificate hierachy diagram can be found in section 2.1.1 of the CPS http://www.s-trust.de/stn-cps/stn_cps.pdf “The business purpose of the root certificates is to provide all customers of the German Savings Bank Financial Group with client-certificates for his/her signature enabled debit card (smartcard).”			COMPLETE

that any audit covers them as well as the root.			
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. (For example, contractual arrangements should require third-party subordinates to operate in accordance with some CPS/CP. Technical arrangements might include name constraints, not allowing them to create their own subordinates, etc.)	There are no subordinate CAs for this CA available.	None of the subordinate CAs are operated by third parties. They are all internally operated.	COMPLETE
List any other root CAs that have issued cross-signing certificates for this root CA	None		COMPLETE
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code (Code Signing)	Email Comment #15: We have no SSL-description / product in the CPS yet. So please leave out the flag "ssl cert" until we have established these processes.		COMPLETE

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.)	IV/OV -- Identity-validated Class, personal (face to face) validation is conducted. “The validation of an identity is based on the personal (physical) presence of the certificate applicant in front of an agent of our CA or RA who is following the requirements of the German signature law. The agent shall check the identity of the certificate applicant against a well-recognized form of government-issued photo-graphic identification, such as a passport.”	COMPLETE
If EV certificates are	Not Applicable	N/A

issued within the hierarchy rooted at this root, the EV policy OID(s) associated with those EV certificates.		
Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable. • For SSL certificates this should also include URLs of one or more web servers using the certificate(s). • There should be at least one example certificate for each of the major types of certificates issued, e.g., email vs. SSL vs. code signing, or EV vs. OS vs. DV.	Comment #17: We have not issued any ssl certificates under the root yet. Example cert issued from S-TRUST Authentication and Encryption Root CA 2005:PN https://bugzilla.mozilla.org/attachment.cgi?id=337727 Example cert issued from S-TRUST Qualified Root CA 2008-001:PN https://bugzilla.mozilla.org/attachment.cgi?id=337728	COMPLETE
CP/CPS • Certificate Policy URL • Certificate Practice Statement(s) (CPS) URL (English or available in English translation)	http://www.s-trust.de/stn-cps/stn_cps.pdf Comment #22: We found a solution today. Additionally to the fact that the applicant confirms by his signature that he is the legal owner of the email address we are going to implement a technical verification process: An individuell "E-Mail-Address verification code" will be part of the E-Mail the applicant receives for downloading his certificate. Without this code a certificate issuence will not be possible. Comment #23: That sounds fine. Please let me know when your CP/CPS and your issuance policies have been updated to include this procedure.	COMPLETE

	Comment #29: we will go live with our updated CPS (Ver 1.2) and your issuance policies on Monday the 7th of January 2008. The new CPS can be downloaded from that date on from the following link: http://www.s-trust.de/stn-cps/ Comment #40: I translated the part of that document here for you **Methode to the possession proof of the e-mail address given in the certificate application** **Before the ZDA DSV (Trustcenter Deutscher Sparkassenverlag) issues a certificate for a signature-prepared card with electronic chip, the application plate must prove that e-mail account (e-mail address) – which was given with the order – under the control from the card-owner stands. This proof occurs by means of a personal code which is sent to the application plate on affected e-mail account by the ZDA DSV. The download process – the exhibit of the personal certificates – can be carried out only under information of this e-mail-verification code.**	
. AUDIT: The published document(s) relating to independent audit(s) of the root CA and any CAs within the hierarchy rooted at the root. (For example, for WebTrust for CAs audits this would be the "audit report and management assertions" document available from the webtrust.org site or elsewhere.)	Audits performed by TÜV-IT: http://www.tuvit.de/ Audit: ETSI TS 102.042: http://www.tuvit.de/certuvit/pdf/6702UE.pdf Audit ETSI TS 101.456: http://www.tuvit.de/certuvit/pdf/6701UE.pdf (This one clearly references the CPS at http://www.s-trust.de/stn-cps/stn_cps.pdf)	COMPLETE

Review CPS sections dealing with subscriber verification (COMPLETE)

- Verify domain check for SSL
  - Not applicable
- 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.
  - As per Comment #29 the CPS was updated to address this. Comment #40 includes the translation (see above).

- Verify identity info in code signing certs is that of subscriber
    - Not Applicable
- Make sure it’s clear which checks are done for which context (cert usage)

Flag Problematic Practices (COMPLETE)

- Long-Lived Domain-Validated SSL certs
    - Not Applicable
- Wildcard DV SSL certs
    - Not Applicable
- Issuing end entity certs directly from root rather than using an offline root and issuing certs through a subordinate CA
    - Not Applicable as of the 2006 root
- Allowing external entities to operate subordinate CAs
    - None

Verify Audits (COMPLETE)

- Validate contact info in report, call to verify that they did indeed issue this report.
    - On the Tuvit website
- For EV CA’s, verify current WebTrust EV Audit done.
    - Not Applicable
- Review Audit to flag any issues noted in the report
    - Complete, no issues noted.