Print this page

Mozilla - CA Program

Case Information

Case Number	00000010	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owners/Certificate Name	Deutscher Sparkassen Verlag GmbH (S-TRUST, DSV-Gruppe)	**Request Status**	In Public Discussion

Additional Case Information

Subject	Include renewed root	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1011182

General information about CA's associated organization

Company Website	https://www.s-trust.de/	**Verified?**	Verified
Organizational Type	Public Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Germany	**Verified?**	Verified
Primary Market / Customer Base	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.	**Verified?**	Verified
Impact to Mozilla Users	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.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.

CA's Response to Recommended Practices	No issuance of SSL certificates.	**Verified?**	Verified

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org /CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	No issuance of SSL certificates. No Domain Delegation / no E-Mail Validation to third parties.	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Case No	R00000015	**Case Number**	00000010
Request Status	In Public Discussion	**Root Certificate Name**	S-TRUST Universal Root CA

Additional Root Case Information

Subject	Include S-TRUST Universal Root CA

Technical Information about Root Certificate

O From Issuer Field	Deutscher Sparkassen Verlag GmbH	**Verified?**	Verified
OU From Issuer Field	S-TRUST Certification Services	**Verified?**	Verified
Certificate Summary	This SHA-256 root will eventually replace DSV Gruppe's SHA-1 "S-TRUST Authentication and Encryption Root CA 2005:PN" root certificate was included in NSS via Bugzilla Bug #370627.	**Verified?**	Verified
Root Certificate Download URL	https://www.s-trust.de /ablage_download_dokumente /ablage_zertifikate /S-TRUST_Universal_Root_CA1.cer	**Verified?**	Verified
Valid From	2013 Oct 22	**Verified?**	Verified
Valid To	2038 Oct 21	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	Example Cert: https://bugzilla.mozilla.org /attachment.cgi?id=8506014	**Verified?**	Verified

CRL URL(s)	http://crl.s-trust.de/public/offlineCA/DeutscherSparkassenVerlagGmbHS-TRUSTUniveralRootCA/LatestCRL.crl	**Verified?**	Verified
OCSP URL(s)	None	**Verified?**	Verified
Trust Bits	Email	**Verified?**	Verified
SSL Validation Type		**Verified?**	Not Applicable
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
EV Tested		**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None -- only email trust bit enabled.	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	1B:3D:11:14:EA:7A:0F:95:58:54:41:95:BF:6B:25:82:AB:40:CE:9A	**Verified?**	Verified
SHA-256 Fingerprint	D8:0F:EF:91:0A:E3:F1:04:72:3B:04:5C:EC:2D:01:9F:44:1C:E6:21:3A:DF:15:67:91:E7:0C:17:90:11:0A:31	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	1 subCA is internally operated: S-TRUST Authentication and Encryption Class 3 CA	**Verified?**	Verified
Externally Operated SubCAs	No externally operated CAs.	**Verified?**	Verified
Cross Signing	No issuance of Cross-Signing certificates	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Class 3 certificates, personal identification based on the identity card of the enduser.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in German. Translations of some sections provided.	**Verified?**	Verified
CA Document Repository	https://www.s-trust.de/stn-cps	**Verified?**	Verified
CP Doc Language	German		
CP	https://www.s-trust.de/stn-cps	**Verified?**	Verified
CP Doc Language	German		
CPS	https://www.s-trust.de/stn-cps	**Verified?**	Verified
Other Relevant Documents		**Verified?**	Not Applicable
Auditor Name	TUVIT	**Verified?**	Verified
Auditor Website	https://www.tuvit.de/de	**Verified?**	Verified

Auditor Qualifications	https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx	**Verified?**	Verified
Standard Audit	https://www.tuvit.de/data/content_data/tuevit_en/6744UE_s.pdf	**Verified?**	Verified
Standard Audit Type	ETSI TS 102 042	**Verified?**	Verified
Standard Audit Statement Date	4/11/2014	**Verified?**	Verified
BR Audit	Not requesting websites trust bit.	**Verified?**	Not Applicable
BR Audit Type		**Verified?**	Not Applicable
BR Audit Statement Date		**Verified?**	Not Applicable
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply		**Verified?**	Not Applicable
SSL Verification Procedures	Not requesting Websites trust bit.	**Verified?**	Not Applicable
EV SSL Verification Procedures		**Verified?**	Not Applicable
Organization Verification Procedures	Google Translate of CPS section 2.5.2.2: If a company or organization name be included in the certificate, so this company or organizational affiliation must be proven. This is the "consent to receive company or organization information in the qualified personal certificate and advanced authentication / encryption certificate" fill in the application form and confirmed by an authorized representative (manager / representative). The right of representation is confirmed by signature and company stamp, the case of legal entities of public law (Chambers, authorities) Signature and seal. As proof of authorization to represent the company a current certificate of registration is also attached. If the company is not registered in the commercial register, the company must be reliably detected using current documents (proof of chamber membership / business registration, etc. eg extract from the Handicrafts,).	**Verified?**	Verified
Email Address Verification Procedures	According to section 2.4.2.2 of the CPS the proof of email ownership occurs by means of a personal code, which is sent to the applicant via the email address specified in the certificate. The download process can only be completed using this email verification code. CPS section 2.4.2.2, Method to proof the ownership of the e-mail address entered in the certificate-application “Before the ZDA DSV approves a certificate for a signature-prepared chip card, the applicant has to prove that the e-mail address –he entered during the application process - is under his control. This verification happens whilst a personal code is sent to the applicants related e-mail account by the ZDA DSV. The download process -the delivery of the personal certificates- can only be executed by entering this e-mail verification-code. “	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Not requesting Code Signing trust bit.	**Verified?**	Not Applicable

Multi-Factor Authentication	multi-factor authentication is required for all accounts capable of directly causing certificate issuance.	**Verified?**	Verified
Network Security	The actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices are performed	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	See #4 of https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**Verified?**	Verified