Bugzilla ID: 1011182
Bugzilla Summary: Add "S-TRUST Universal Root CA" root certificate

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	Deutscher Sparkassen Verlag GmbH (DSV Gruppe) S-TRUST is a trademark of Deutscher Sparkassen Verlag GmbH
Website URL	https://www.s-trust.de/
Organizational type	The CA is operated by a public corporation.
Primark 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, 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
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.
Inclusion in other major browsers	Microsoft
CA Primary Point of Contact (POC)	https://wiki.mozilla.org/CA:Information_checklist#CA_Primary_Point_of_Contact_.28POC.29 POC direct email: alexandru.matei@dsv-gruppe.de Email Alias: felix.buermann@dsv-gruppe.de CA Phone Number: +49 711 782 2188

Technical information about each root certificate

Certificate Name	S-TRUST Universal Root CA
Certificate Issuer Field	CN = S-TRUST Universal Root CA OU = S-TRUST Certification Services O = Deutscher Sparkassen Verlag GmbH C = DE
Certificate Summary	Universal Root, issues certificates for E-Mail/SMIME and Authentication&Encryption
Mozilla Applied Constraints	This Root Certificate does not issue SSL certificates
Root Cert URL	https://www.s-trust.de/ablage_download_dokumente/ablage_zertifikate/S-TRUST_Universal_Root_CA1.cer
SHA1 Fingerprint	1B:3D:11:14:EA:7A:0F:95:58:54:41:95:BF:6B:25:82:AB:40:CE:9A
Valid From	2013-10-22
Valid To	2038-10-21
Certificate Version	3
Certificate Signature Algorithm	SHA-256
Signing key parameters	2048
Example Certificate (non-SSL)	Example Cert: https://bugzilla.mozilla.org/attachment.cgi?id=8506014 Intermediate Cert: https://www.s-trust.de/service_support/signaturkarten/download_wurzelzertifikate/qual_angezeigt_akkreditiert/ https://www.s-trust.de/ablage_download_dokumente/ablage_zertifikate/S-TRUST_Authentication_and_Encryption_Class_3_CA1.cer
CRL URL	http://crl.s-trust.de/public/offlineCA/DeutscherSparkassenVerlagGmbHS-TRUSTUniveralRootCA/LatestCRL.crl
OCSP URL	None
Requested Trust Bits	Email (S/MIME)
SSL Validation Type	No issuance of SSL certificates
EV Policy OID(s)	No issuance of SSL certificates
Non-sequential serial numbers and entropy in cert	A 16-Byte Random serial number is used.

CA Hierarchy information for each root certificate

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

Verification Policies and Practices

Policy Documentation	CPS (German): https://www.s-trust.de/stn-cps
Audits	Audit Type: ETSI TS 102 042 V2.4.1 Auditor: TUVIT Audit Report: https://www.tuvit.de/data/content_data/tuevit_en/6744UE_s.pdf (2014.04.11)
Baseline Requirements (SSL)	Will this root be used to issue SSL certs? Currently NO
SSL Verification Procedures	Not applicable. Not requesting Websites trust bit.
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,).
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. "
Code Signing Subscriber Verification Procedures	Not applicable. Not requesting Code Signing trust bit.
Multi-factor Authentication	multi-factor authentication is required for all accounts capable of directly causing certificate issuance.
Network Security	The actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices were performed

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	See above.
CA Hierarchy	See above.
Audit Criteria	See above.
Document Handling of IDNs in CP/CPS	No issuance of SSL certificates
Revocation of Compromised Certificates	

Verifying Domain Name Ownership	See above.
Verifying Email Address Control	See above.
Verifying Identity of Code Signing Certificate Subscriber	See above.
DNS names go in SAN	No issuance of SSL certificates
Domain owned by a Natural Person	No issuance of SSL certificates
OCSP	See above.

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	No issuance of SSL certificates
Wildcard DV SSL certificates	No issuance of SSL certificates
Email Address Prefixes for DV Certs	No issuance of SSL certificates
Delegation of Domain / Email validation to third parties	No Domain Delegation / no E-Mail Validation to third parties
Issuing end entity certificates directly from roots	See above.
Allowing external entities to operate subordinate CAs	No
Distributing generated private keys in PKCS#12 files	No
Certificates referencing hostnames or private IP addresses	No issuance of SSL certificates
Issuing SSL Certificates for Internal Domains	No issuance of SSL certificates
OCSP Responses signed by a certificate under a different root	See above.
CRL with critical CIDP Extension	
Generic names for CAs	See above.
Lack of Communication With End Users	Communication with end-users via E-Mail (see www.s-trust.de)
Backdating the notBefore date	No backdating of notBefore date – Certificates are valid from the issuing day