Bugzilla ID: 1092963
Bugzilla Summary: Add Renewed A-Trust-Root-05 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	A-Trust
Website URL	http://www.a-trust.at
Organizational type	Commercial Company
Primark Market / Customer Base	A-Trust's product range comprises user certificates, developer certificates and corporate certificates as well as consultation services and support with the development of e-commerce and signature applications in accordance with the Directive 1999/93/EC
Impact to Mozilla Users	Renewal of root included via Bugzilla Bug #530797. A-Trust's CA hierarchy is used to issue Austrian Citizen Cards and A-Trust SSL certificates.
Inclusion in other browsers	The A-Trust 1, 2, and 3 roots are included in Microsoft's root program.
CA Primary Point of Contact (POC)	Christoph Klein, christoph.klein@a-trust.at Head of Customer Care Management Tel.: +43 1 713 21 51 353 CA Email Alias: Technik@a-trust.at CA Phone Number: +43 (1) 713 21 51 – 0 Title / Department: IT Operation

Technical information about each root certificate

Certificate Name	A-Trust-Root-05
Certificate Issuer Field	CN = A-Trust-Root-05 OU = A-Trust-Root-05 O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT
Certificate Summary	This root has internally-operated subordinate CAs that issue smartCard-based certificates to a natural person after a face-to-face identification (email), software certificates (PKCS#12), and server certificates (SSL and EV SSL). This root will eventually replace the A-Trust-nQual-03 root certificate that was included via Bugzilla Bug #530797.
Mozilla Applied Constraints	None
Root Cert URL	http://www.a-trust.at/certs/A-Trust-Root-05.crt
SHA1 Fingerprint	2E:66:C9:84:11:81:C0:8F:B1:DF:AB:D4:FF:8D:5C:C7:2B:E0:8F:02
Valid From	2013-09-23
Valid To	2023-09-20

Certificate Version	3
Cert Signature Algorithm	SHA-256
Signing key parameters	4096
Test Website URL	https://ca-train.a-trust.at/
CRL URL	http://crl.a-trust.at/crl/A-Trust-Root-05 http://crl.a-trust.at/crl/a-sign-SSL-EV-05 CRL issuing frequency for subordinate end-entity certificates: 2 hours or on change CRL issuing frequency for subordinate CA certificates: 2 hours or on change
OCSP URL	http://ocsp.a-trust.at/ocsp Need maximum expiration time of OCSP responses, as per the CA/Browser Forum's Baseline Requirements (BRs).
Requested Trust Bits	Websites (SSL/TLS)
SSL Validation Type	DV, OV, and EV
EV Policy OID(s)	1.2.40.0.17.1.22 If requesting EV treatment, then need EV test results: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version
Non-sequential serial numbers and entropy in cert	http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html "9. We expect CAs to maintain current best practices to prevent algorithm attacks against certificates. As such, the following steps will be taken: … - all new end-entity certificates must contain at least 20 bits of unpredictable random data (preferably in the serial number)."
Response to Recent CA Communication(s)	https://wiki.mozilla.org/CA:Communications#May_2014_Responses Still need URL to info about publicly disclosed subCA certs. See action #5 of https://wiki.mozilla.org/CA:Communications#May_13.2C_2014

CA Hierarchy information for each root certificate

CA Hierarchy	This root currently has two internally-operated subordinate CAs: -- a-sign-SSL-05 (http://www.a-trust.at/certs/a-sign-ssl-05.crt) -- a-sign-SSL-EV-05 (http://www.a-trust.at/certs/a-sign-ssl-ev-05.crt)
Externally Operated SubCAs	Can this root ever have subCAs that are operated by external third parties? If yes, then provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist
Cross-Signing	List all other root certificates for which this root certificate has issued cross-signing certificates. List all other root certificates that have issued cross-signing certificates for this root certificate. If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.
Technical Constraints on Third-party Issuers	Describe the technical constraints that are in place for all third-parties (CAs and RAs) who can directly cause the issuance of certificates. See #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate

Verification Policies and Practices

Policy Documentation	Document Repository: http://www.a-trust.at/ATrust/Downloads.aspx SSL CP: http://www.a-trust.at/docs/cp/a-sign-ssl/a-sign-ssl.pdf EV SSL CP: http://www.a-trust.at/docs/cp/a-sign-ssl-ev/a-sign-ssl-ev.pdf SSL CPS: http://www.a-trust.at/docs/cp/a-sign-ssl/Certification%20Practice%20Statement_a-sign-ssl.pdf EV SSL CPS: http://www.a-trust.at/docs/cp/a-sign-ssl/a-sign-ssl-ev_cps.pdf
Audits	Audit Type: WebTrust and WebTrust EV Auditor: Ernst & Young (Austria) Auditor Website: http://www.ey.com/ Audit Document URL(s): CA: https://cert.webtrust.org/SealFile?seal=1753&file=pdf (2014.10.03) EV: https://cert.webtrust.org/SealFile?seal=1754&file=pdf (2014.10.23)
Baseline Requirements (SSL)	URL to BR audit statement: Please carefully review: https://wiki.mozilla.org/CA:BaselineRequirements (also have your auditor carefully review this wiki page) The document(s) and section number(s) where the "Commitment to Comply" with the CA/Browser Forum Baseline Requirements may be found, as per BR #8.3.
SSL Verification Procedures	Please translate the relevant sections of the SSL and SSL EV CP or CPS into English, and attach to the bug. If you are requesting to enable the Websites Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs It is not sufficient to simply reference section 11 of the CA/Brower Forum's Baseline Requirements (BR). BR #11.1.1 lists several ways in which the CA may confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. Simply referencing section 11 of the BRs does not specify which of those options the CA uses, and is insufficient for describing how the CA conforms to the BRs. The CA's CP/CPS must include a reasonable description of the ways the CA can verify that the certificate subscriber owns/controls the domain name(s) to be included in the certificate.
Organization Verification Procedures	Please translate the relevant sections of the SSL and SSL EV CP or CPS into English, and attach to the bug.
Email Address Verification Procedures	Not applicable – not requesting the email trust bit.
Code Signing Subscriber Verification Procedures	Not applicable – not requesting the code signing trust bit.
Multi-factor Authentication	Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices

Network Security	Confirm that you have performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices

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	???
Revocation of Compromised Certificates	??? – See BRs section 13.1.5.
Verifying Domain Name Ownership	See above
Verifying Email Address Control	N/A
Verifying Identity of Code Signing Certificate Subscriber	N/A
DNS names go in SAN	??? – See BRs section 9.2.1
Domain owned by a Natural Person	???
OCSP	See above

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

Long-lived DV certificates	??? – See BRs section 9.4.1
Wildcard DV SSL certificates	??? – See BRs section 11.1.3
Email Address Prefixes for DV Certs	If DV SSL certs, then list the acceptable email addresses that are used for verification.
Delegation of Domain / Email validation to third parties	???
Issuing end entity certificates directly from roots	No.
Allowing external entities to operate subordinate CAs	???
Distributing generated private keys in PKCS#12 files	???
Certificates referencing hostnames or private IP addresses	???
Issuing SSL Certificates for Internal Domains	???
OCSP Responses signed by a certificate under a different root	No.
SHA-1 Certificates	???
Generic names for CAs	No
Lack of Communication With End Users	???
Backdating the notBefore date	???