Print this page

Mozilla - CA Program

Case Information

Case Number	00000003	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	A-Trust	**Request Status**	Need Information from CA

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=1092963

General information about CA's associated organization

CA Email Alias 1	technik@a-trust.at		
CA Email Alias 2			
Company Website	http://www.a-trust.at	**Verified?**	Verified
Organizational Type	Commercial Organization	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Austria, Central Europe	**Verified?**	Verified
Primary Market / Customer Base	Used to issue Austrian Citizen Cards and A-Trust SSL (EV) certificates, customers from Central Europe.	**Verified?**	Verified
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. 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	**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	* Document Handling of IDNs in CP/CPS - Manual handling, addressed in next WebTrust Audit * Issuing SSL Certificates for Internal Domains - only domains successfully verified through a NIC-database are accepted * DNS names go in SAN - every DNS name in SAN, additionaly one DNS name in Subject * Domain owned by a Natural Person - SSL certificates are only issued to organizations (SSL and SSL EV)	**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	* Long-lived DV - Non EV certificates issued by the new root certificate will have a maximum validity of 36 months (3 years) * Wildcard DV SSL certificates - Every issued SSL certificate is validated using OV * Email Address Prefixes for DV Certs - no email challenge-response mechanism to verify domain control is used domains are validated by identifying individual domain owners who are mentioned in trustworthy whois-databases * Delegation of Domain / Email validation to third parties - no third parties / RAs are involved in issuing SSL and SSL EV certificates * Allowing external entities to operate subordinate CAs - not used with SSL certificate roots * Distributing generated private keys in PKCS#12 files - keys are always generated by the subscriber * Certificates referencing hostnames or private IP addresses - certificates are only issued for external hostnames that can be verified - no IP adresses, no internal hostnames * Issuing SSL Certificates for Internal Domains - certificates are only issued for external hostnames that can be verified - no IP adresses, no internal hostnamesold certificates have been audited, every used domain name in our certificates has been verified against the database or our national registration service * SHA-1 Certificates - the new root certificate will only be used to issue SHA-256 certificatesexisting certificates (using another root) will be migrated, once the new root certificate has been deployed	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	A-Trust-Root-05	**Root Case No**	R00000002
Request Status	Need Information from CA	**Case Number**	00000003

Additional Root Case Information

Subject	Include A-Trust-Root-05

Technical Information about Root Certificate

O From Issuer Field	A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	**Verified?**	Verified
OU From Issuer Field	A-Trust-Root-05	**Verified?**	Verified
Certificate Summary	This root will eventually replace the A-Trust-nQual-03 root certificate that was included via Bugzilla Bug #530797. This root has internally-operated subordinate CAs.	**Verified?**	Verified
Root Certificate Download URL	http://www.a-trust.at/certs/A-Trust-Root-05.crt	**Verified?**	Verified
Valid From	2013 Sep 23	**Verified?**	Verified
Valid To	2023 Sep 20	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	4096	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://ca-train.a-trust.at/	**Verified?**	Verified
CRL URL(s)	http://crl.a-trust.at/crl/A-Trust-Root-05 http://crl.a-trust.at/crl/a-sign-SSL-EV-05	**Verified?**	Verified
OCSP URL(s)	http://ocsp.a-trust.at/ocsp Max expiration time of OCSP responses: 10 minutes	**Verified?**	Verified
Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	DV; OV; EV	**Verified?**	Verified
EV Policy OID(s)	1.2.40.0.17.1.22	**Verified?**	Verified
EV Tested	// CN=A-Trust-Root-05,OU=A-Trust-Root-05,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT "1.2.40.0.17.1.22", "A-Trust EV OID", SEC_OID_UNKNOWN, { 0x2D, 0xDE, 0x9D, 0x0C, 0x0A, 0x90, 0xE7, 0xB3, 0x2B, 0x5A, 0xBC, 0x01, 0xF4, 0x17, 0x99, 0xD4, 0x2E, 0x95, 0xA1, 0xE3, 0xC3, 0x1C, 0x3B, 0x39, 0x37, 0x3B, 0xB8, 0x14, 0x1E, 0xA5, 0x44, 0x71 }, "MIGLMQswCQYDVQQGEwJBVDFIMEYGA1UECgw/QS1UcnVzdCBHZXMuIGYuIFNpY2hl" "cmhlaXRzc3lzdGVtZSBpbSBlbGVrdHIuIERhdGVudmVya2VociBHbWJIMRgwFgYD" "VQQLDA9BLVRydXN0LVJvb3QtMDUxGDAWBgNVBAMMD0EtVHJ1c3QtUm9vdC0wNQ==" "", "D820", Success!	**Verified?**	Verified
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	2E:66:C9:84:11:81:C0:8F:B1:DF:AB:D4:FF:8D:5C:C7:2B:E0:8F:02	**Verified?**	Verified
SHA-256 Fingerprint	2D:DE:9D:0C:0A:90:E7:B3:2B:5A:BC:01:F4:17:99:D4:2E:95:A1:E3:C3:1C:3B:39:37:3B:B8:14:1E:A5:44:71	**Verified?**	Verified

CA Hierarchy Information

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)	**Verified?**	Verified
Externally Operated SubCAs	None. None planned.	**Verified?**	Verified
Cross Signing	None. None planned.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	No third parties / RAs are involved in issuing SSL and SSL EV certificates	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in German Translations of some sections of the documents have been attached to the bug.	**Verified?**	Verified
CA Document Repository	http://www.a-trust.at/ATrust/Downloads.aspx	**Verified?**	Verified
CP Doc Language	German		
CP	http://www.a-trust.at/docs/cp/a-sign-ssl/a-sign-ssl.pdf	**Verified?**	Verified
CP Doc Language	German		
CPS	http://www.a-trust.at/docs/cp/a-sign-ssl/Certification%20Practice%20Statement_a-sign-ssl.pdf	**Verified?**	Verified
Other Relevant Documents	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	**Verified?**	Verified
Auditor Name	Ernst & Young	**Verified?**	Verified
Auditor Website	http://www.ey.com/	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1753&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	10/3/2014	**Verified?**	Verified

BR Audit	NEED See https://wiki.mozilla.org /CA:BaselineRequirements#Extended_Validation Please have your auditor review the entire wiki page: https://wiki.mozilla.org/CA:BaselineRequirements	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit	https://cert.webtrust.org/SealFile?seal=1754&file=pdf	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	10/3/2014	**Verified?**	Verified
BR Commitment to Comply	NEED https://wiki.mozilla.org /CA:BaselineRequirements#CA_Conformance_to_the_BRs "The CA's CP or CPS documents must include a commitment to comply with the BRs, as described in BR section 8.3."	**Verified?**	Need Response From CA
SSL Verification Procedures	NEED Translation of the sections of the CP or CPS that document how non-EV SSL certs are verified, according to https://wiki.mozilla.org /CA:BaselineRequirements#CA_Conformance_to_the_BRs and https://wiki.mozilla.org /CA:Recommended_Practices#Verifying_Domain_Name_Ownership	**Verified?**	Need Response From CA
EV SSL Verification Procedures	Translation of EV SSL CPS sections 3.1.7, 3.1.8, and 3.1.9: https://bug1092963.bugzilla.mozilla.org/attachment.cgi?id=8584406	**Verified?**	Verified
Organization Verification Procedures	Translation of EV SSL CPS sections 3.1.7, 3.1.8, and 3.1.9: https://bug1092963.bugzilla.mozilla.org/attachment.cgi?id=8584406	**Verified?**	Verified
Email Address Verification Procedures	Not requesting the Email trust bit	**Verified?**	Not Applicable
Code Signing Subscriber Verification Pro	Not requesting the Code Signing trust bit	**Verified?**	Not Applicable
Multi-Factor Authentication	Issuance is only possible using a smart card with PIN	**Verified?**	Verified
Network Security	Regular Network security checks are performed and monitored by Austrian Authorities since the Austrian citizen card, which is used for E-Government is also issued by A-Trust.	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://bugzilla.mozilla.org /show_bug.cgi?id=1092963	**Verified?**	Verified