Bugzilla ID: 530797
Bugzilla Summary: Add Root CA "A-Trust" to trusted list

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, as per http://wiki.mozilla.org/CA:Information_checklist.

CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	**Data**
CA Name	A-Trust
Website URL	http://www.a-trust.at
Organizational type	Commercial Company
Primary market / customer base	A-Trust (founded in February 17, 2000) is the only accredited TrustCenter in Austria issuing smartcard based qualified certificates for Austrian citizen used in eGovernment, etc. In March 11, 2002 A-Trust has been accredited according to § 17 of the Austrian Signature Law by Telekom-Control-Kommission, the Austrian supervisory body. 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.
CA Contact Information	CA Email Alias: Technik@a-trust.at CA Phone Number: +43 (1) 713 21 51 – 0 Title / Department: IT Operation

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

Info Needed	**Data**
Certificate Name	A-Trust-nQual-03
Cert summary / comments	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).
Root Cert URL	http://www.a-trust.at/certs/A-Trust-nQual-03.crt
SHA-1 fingerprint	D3:C0:63:F2:19:ED:07:3E:34:AD:5D:75:0B:32:76:29:FF:D5:9A:F2
Valid from	2005-08-17
Valid to	2015-08-17
Cert Version	3
Modulus length / key length	2048 (SHA1)
Test Website	https://test1.a-trust.at/
CRL URL	CRL Distribution point of SSL cert: URI: ldap://ldap.a-trust.at/ou=a-sign-SSL-03,o=A-Trust,c=AT?certificaterevocationlist?base?objectclass=eidCertificationAuthority
CRL Update Frequency	2 hours
OCSP Responder URL	AIA extension of SSL cert: OCSP: URI: http://ocsp.a-trust.at/ocsp EV SSL CP section 3.3.6, #7: As the current status of the certificate is being newly determined every time the query is performed, the ocsp-response field "nextUpdate" is not set.

CA Hierarchy	A-Trust Certificate Hierarchy: https://www.a-trust.at/docs/CA-Hierarchy_v12.pdf This A-Trust-nQual-03 root has the following subordinate CAs: • a-sign-Token-03 (encryption/decryption certificates for the Citizen Card) • a-sign-corporate-light-03 – (email signing) • a-sign-corporate-03 – (email signing) • a-sign-SSL-03 (SSL certs) • a-sign-SSL-EV-03 (EV SSL certs) • a-sign-light-03 (software Certificates) • a-sign-limited-03 (limited validity Test Certificates, not SSL, and no new test certs are issued)
Sub-CAs operated by 3rd parties	None
Cross-Signing	None
Requested Trust Bits	Websites (SSL/TLS)
SSL Validation Type DV, OV, and/or EV	OV, EV
EV policy OID(s)	1.2.40.0.17.1.22
CP/CPS	All Certification Practice Statements: https://www.a-trust.at/docs/cps All Certificate Policies: https://www.a-trust.at/docs/cp SSL CPS (German): http://www.a-trust.at/docs/cps/a-sign-ssl/a-sign-ssl_cps.pdf SSL CP (German): http://www.a-trust.at/docs/cp/a-sign-ssl/a-sign-ssl.pdf EV SSL CPS (German): http://www.a-trust.at/docs/CPS/a-sign-ssl-ev/a-sign-ssl-ev_cps.pdf EV SSL CP (German): http://www.a-trust.at/docs/CP/a-sign-ssl-ev/a-sign-ssl-ev.pdf Translations of sections of the CP and CPS documents are provided below.
AUDIT	Audit Type: WebTrust CA Auditor: Ernst & Young Audit Report: https://cert.webtrust.org/ViewSeal?id=1016 (2010.11.30) Audit Type: WebTrust EV Readiness Auditor: Ernst & Young Audit Report and Management's Assertions: https://trusties.a-trust.at/ev.pdf (2010.10.22)
Organization Verification	See the translations below of the SSL CPS section 3.1.7 through 3.1.9, and of the SSL CP section 3.3.1.
Domain Name Ownership / Control	SSL CPS section 3.1.8: Registration Authority verifies the validity of the ownership of the requested domain by querying a database like www.nic.at, www.denic.de,... If this is not possible the applicant has to guarantee the possession of the Domain in written form. If a server certificate is issued to an IP Address, a written statement of the provider proving the applicants possession of the IP Address is required. From Comment #9: > How is the information from the database query used to verify the validity of the ownership of the requested domain? As per SSL CPS section 3.1.9, we require a PhotoID from the domain owner and a representative of the company who is signed in the name. The domain owner is the person found in the database information of www.nic.at etc as stated in 3.1.8 > When database query isn't possible, how is the written form and written statement verified? In these rare cases there is still the verification process of a representative as described in SSL CPS section 3.1.9 (company

	registration number/EBR). This trusted person has to guarantee us the validity of the information provided.
EV SSL	A-Trust verifies the existence of the organization, the authority of the subscriber, and the domain name as per the CAB Forum EV Guidelines v 1.2. Details are in sections 3.1.7 to 3.1.9 of the EV SSL CPS. Translations from these sections are provided below.
Email Address Ownership / Control	Not Applicable – Not requesting the Email Trust bit at this time. To request the email trust bit, the CA will need to have information in the appropriate CP/CPS documents that satisfies section 7 of the Mozilla CA Certificate Policy (http://www.mozilla.org/projects/security/certs/policy/). Additionally, there will need to be an audit of the corresponding documented practices that satisfies the Mozilla CA Certificate Policy.
Identity of Code Signing Subscriber	Not Applicable – Not requesting the Code Signing Trust bit at this time. To request the code signing trust bit, the CA will need to have information in the appropriate CP/CPS documents that satisfies section 7 of the Mozilla CA Certificate Policy (http://www.mozilla.org/projects/security/certs/policy/). Additionally, there will need to be an audit of the corresponding documented practices that satisfies the Mozilla CA Certificate Policy.
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices • Long-lived DV certificates o SSL certs are OV. • Wildcard DV SSL certificates o Not allowed. • Delegation of Domain / Email validation to third parties o Not applicable. • Issuing end entity certificates directly from roots o Root signs intermediate certs which sign end-entity certs. • Allowing external entities to operate unconstrained subordinate CAs o Not applicable. • Distributing generated private keys in PKCS#12 files o Signer has to send PKCS#10. • Certificates referencing hostnames or private IP addresses o IP Addresses have been issued, but only after validation of the ownership of the IP Address (SSL CP section 3.3.1, point 5) • Issuing SSL Certificates for Internal Domains o If a cert is issued to a domain, it has to be validated that the signatory owns this domain via Internic request, the protocol of the internic query is archived • OCSP Responses signed by a certificate under a different root o Not applicable. • CRL with critical CIDP Extension o CIDP extension is not critical. • Generic names for CAs o CN, OU, and O all have A-Trust
SSL CPS Translations	SSL CPS (German): http://www.a-trust.at/docs/cps/a-sign-ssl/a-sign-ssl_cps.pdf 3.1.7 Authentification of organisations

	For applying an a.sign. SSL certificate for a domain owned by an organization the organisation will be verified as follows: If the company can be found in the European Business Register (EBR) the verification process performed by the registration authority contains querying the Austrian Company Register or the EBR. The application must include this number. If the company is not registered in this databases the applicant has to provide a document proving the existence of the organisation. This can be a document (not older than three months) of a public department or something comparable. 3.1.8 Verification of Domain or IP Address Registration Authority verifies the validity of the ownership of the requested domain by querying a database like www.nic.at, www.denic.de,... If this is not possible the applicant has to guarantee the possession of the Domain in written form. If a server certificate is issued to an IP Address, a written statement of the provider proving the applicants possession of the IP Address is required. 3.1.9 Authentification of individuals Persons validated during this process are: * Signatory ie the domain owner and if the domain owner is acting for an organisation * a representative of the company who is allowed to sign in the name of the company Both entities have to provide a copy of a valid photo-ID according to the following requirements * Austrian Photo ID (List...) * international Passport in English or German Language If the company representative cannot be found in the company registration number or ERB, then an additional proof of his authority is required
SSL CP Translations	SSL CP (German): http://www.a-trust.at/docs/cp/a-sign-ssl/a-sign-ssl.pdf 3.3.1 Registration of the certificate holder These action for identification and registration of the certificate holder ensure that the application for an a.sign SSL certificate if correct, complete and authorised. 1) Before the contract between certificate holder and a.trust is signed, the business conditions and other applying documents concerning the use of the certificate are made accessible to the certificate holder (3.3.4) 2) the application form and the information are accessible via the a.trust web site 3) the certificate application form contains the following information * full name, phone number and email address of the applicant * Password for verification * Domain name or IP Address * optional email address which will be included in the certificate (RFC 822) * the public key to be signed If the domain is owned by an organisation * full name and contact information of a person allowed to sign for the company * company register or ERB number (if exists) * Name and place of the organisation * optional name of the organisatiuonal unit 4) the contract to be signed with the certificate holder contains

* acceptance of the responsibilites of a certificate holder
* acceptance that a.trust is allowed to record the process of registration and all contained data and accepting that this data in case of the CAs end of operation may be given to a third party
* the certificate holders confirmation that the provided data is correct

5) a.trust verified the following data

* verification of the ownership of the domain or IP Address

If the domain owner is an organisation the following additional verification is performed

* Verification of the organisation (company register databases)
* Verification that the person allowed to sign for the company is mentioned as such in the company register and verification of the photo ID

6) The certificate request and all contained documents (copy of photo ID, info about company, domain/ip,..) are archived for seven years (electronic archiving)

7) The regulations of the Datenschutzkomission DSG (i.e. data privacy protection commission) are assured by the registration authorities following the procedere described by a.trust.

3.3.2 Certificate renewal

The following measures ensure the correctness and completeness of applications for certificates which had already been authorised by a.trust:

1) the data contained in the certificate has to be verified by the registration authority

2) changes in the conditions of a contract are sent to the applicant

3) changes of data used for applying for a certificate are verified and need to be signed by the applicant in accordance to 3.3.1

4) changes of certificate lifecycle before the validTo of the certificate is reached are performned according to §12 of SigV [Austrian Signature Law] The new certificate lifetime must not exceed five years. Renewal is only performed, if the used cryptographic methods are still state of the art and there are no signs of compromise of the private key.

3.3.3 Issuing the certificate

The following measures assure that the issuing and renewal of certificates are performed in a secure manner according to the Austrian Signature law

1) a.sign SSL certificate are X.509 v3 certificates. the following informations are included

* version number
* serial number
* name of the certificate issuer
* validity period
* DN of the signatory
    * CN
    * O (optional)
    * OU (optional)
    * email (optional)
    * CIN (Cardholder IDentification Number) [ie: internal unique number for the customer]
    * Nationality of the domain owner (eg. AT, DE)

	* public key * Algorithm used * signature * Certificate Extensions 2) The certificates are only issued after proper verification of the provided data. Same procedure is used for renewal. 3) The correct assignment of certificate to certificate holder is ensured by: * PKCS #10 delivered by applicant * Issuing of the certificate only after verification of data * All data provided signed by customer if applicable 4) The Data aquired in the registration authority is sent via SSL to the CA 5) Every Registration Officer has to authenticate via a smart card 3.3.4 publishing of Terms a.trust informs its customers about the terms of use on the homepage: https://www.a-trust.at/docs 1) CP 2) CPS 3) terms and conditions 4) other information Changes are also published on the homepage in some cases additionally an emails is sent 3.3.5 Publication of the certificates Certificates issued by a.trust are published in the following manner 1) All a.sign SSL certificates are published in the public LDAP directory 2) terms are published as mentioned in 3.3.4 3) The relevant documents can be found using the product name "a.sign SSL" 4) public LDAP directory is available 24/7 5) LDAP directory is public a.trust reserves the right to block certain IP Addresses in case of abuse (DOS).
EV SSL CPS Translations	EV SSL CPS (German): http://www.a-trust.at/docs/CPS/a-sign-ssl-ev/a-sign-ssl-ev_cps.pdf 3.1.7 Authentication of organisations When ordering an a.sign SSL EV certificate, the domain and organisation has to be verified. If the ordering entity is registered in either the Austrian commercial register or the European Business Register (EBR), A-Trust verifies the existence using the online - database of those registers. The registration number has to be included in the request. The physical address is also verified using the official register. If not applicable, the check is performed using a duplicate of a document that confirms the organisations existence. Examples for such documents are extracts from legal registers or databases of trusted third parties. The checks are performed according to the requirements in EV-GL (guidelines v1.2, CAB Forum), section 10.

In case an a.sign SSL EV certificate is order, additional information has to be gathered:
- confirmation issued by the bank of the ordering organisation, confirming the existance of an account related to the organisation
- annual statement of the organisation, verified by a certified accountant
- if an exchange embargos exist (inqury at responsible entity in the applicants country through A-Trust)
- verification of the physical address. If the address provided in the legal register used for verification of the organisation is also stated in the annual statement gathered in point 2, the physical address is considered correct. If these requirements are not met, verification can only be achieved through a check on location. Possible costs of this check are charged to the applicant.

Further information can be found at EV-GL, section 10.4.1.

If an entire obtaining of all required information is not possible within a reasonable amount of time, the application is rejected and the applicant will be informed.

3.1.8 Check of Domain or IP Address

The holder of a domain is verified using the databases provided by the applicable authority (such as www.nic.at, www.denic.de,...).

The use of IP addresses in EV certficates is not permitted.

3.1.9 Authentication of individuals

The individuals, who are audited in the process of issuing an a.sign SSL EV certificate are
- the domain owner

and, if the domain order is acting in the name of an organisation
- an organisational responsible person, that is allowed to sign in the ogranisations name and confirms the correctness of the application

The people that are mentioned in the application have to provide an identification document (i.e. passport).

If the organisational responsible person is not listed in the used register, additional confirmation of his status has to be provided (i.e. a certificate of authority).