Translations into English of a few sections of the A-Trust SSL and EV SSL CP and CPS

SSL CPS: http://www.a-trust.at/docs/cps/a-sign-ssl/a-sign-ssl_cps.pdf
SSL CP: http://www.a-trust.at/docs/cp/a-sign-ssl/a-sign-ssl.pdf

EV SSL CPS: http://www.a-trust.at/docs/CPS/a-sign-ssl-ev/a-sign-ssl-ev_cps.pdf
EV SSL CP: http://www.a-trust.at/docs/CP/a-sign-ssl-ev/a-sign-ssl-ev.pdf

Translations from SSL CPS
--

3.1.7 Authentication of organizations

When ordering an a.sign SSL certificate, the domain and organization 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 by comparing the provided data with data gathered from the corresponding online-database. The registration number has to be included in the request. A.sign SSL certificates can only be issued to organizations, whose head office is located in the EU. The physical address is also verified using the official register. If not applicable (the organization is a legal entity that cannot be found in the given registers, for example a governmental authority or self-employed persons), the check is performed using a duplicate of a document that confirms the organizations existence, acquired from a governmental entity. Examples for such documents are extracts from legal registers or databases of trusted third parties.

All communication with the involved parties (applicant, authorized persons from the organization, trusted third parties like governmental contacts) is carried out through e-mail, fax or telephone.

3.1.8 Check of domain / IP address

A-Trust verifies the validity of the ownership of the requested domain by querying a database like www.nic.at, www.denic.de. If the applicant is not the owner of the domain himself, a written confirmation signed by the owner is required.

If the included address is an IP address and no domain, a written confirmation (that the IP address is only assigned to the applicant) issued by the applicants provider is needed.

A-Trust may verify that the applicant is aware of his exclusive control of the domain name by obtaining a confirmation from the administrative contact listed at the domain record through e-mail or telephone.

3.1.9 Authentication of individuals

Individuals, who are audited in the process of issuing an a.sign SSL certificate are:
• the domain owner and,
if the domain order is acting in the name of an organization
• an organizational responsible person, that is allowed to sign in the organizations name and confirms the correctness of the application

The people that are mentioned in the application have to provide an identification document from the following list:
• a Photo ID, issued in Austria (a list of accepted documents is available at the A-Trust Website)
• an international passport in German or English language

If the organizational responsible person is not listed in the used register, additional confirmation of his status has to be provided (i.e. a certificate of authority from a person allowed to sign for the company – check through business register / EBR).
--
--

Translations from EV SSL CPS
--
3.1.7 Authentication of organizations

When ordering an a.sign SSL EV certificate, the domain and organization 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 by comparing the provided data with data gathered from the corresponding online-database. The registration number has to be included in the request. A.sign SSL EV certificates can only be issued to organizations, whose head office is located in the EU. The physical address is also verified using the official register. If not applicable (the organization is a legal entity that cannot be found in the given registers, for example a governmental authority or self-employed persons) , the check is performed using a duplicate of a document that confirms the organizations existence, acquired from a governmental entity. Examples for such documents are extracts from legal registers or databases of trusted third parties.

All communication with the involved parties (applicant, authorized persons from the organization, trusted third parties like governmental contacts) is carried out through e-mail, fax or telephone.

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 organization, confirming the existence of an account related to the organization
• annual statement of the organization, 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 organization 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 / IP address

A-Trust verifies the validity of the ownership of the requested domain by querying a database like www.nic.at, www.denic.de. If the applicant is not the owner of the domain himself, a written confirmation signed by the owner is required. If the included address is an IP address and no domain, a written confirmation (that the IP address is only assigned to the applicant) issued by the applicants provider is needed.

In case of a.sign SSL EV certificates, the use of IP – addresses is restricted. A-Trust may verify that the applicant is aware of his exclusive control of the domain name by obtaining a confirmation from the administrative contact listed at the domain record through e-mail or telephone.

3.1.9 Authentication of individuals

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 organization
• an organizational responsible person, that is allowed to sign in the organization's name and confirms the correctness of the application

The people that are mentioned in the application have to provide an identification document from the following list:
• a Photo ID, issued in Austria (a list of accepted documents is available at the A-Trust Website)
• an international passport in german or english language

If the organizational responsible person is not listed in the used register, additional confirmation of his status has to be provided (i.e. a certificate of authority from a person allowed to sign for the company – check through business register / EBR).
--
--

Translations from EV SSL CP
--
3.3.2 Extension of validity of a certificate and replace of expired certificates

The following measures make sure, that request from applicants that already use certificates are processed correctly. The rules are applied for renewal as well as replacement of (revoked or expired) certificates.

1. The registration authority has to re-check all data, contained in the certificate (e.g. the name of the organization) according to recent validity
2. Possible changes in contractual terms have to be communicated
3. Possible changes in contents of important documents (CP, CPS,…) have to be provided to the applicant (acceptance is signed in contract)
4. The renewal (extension) of valid certificates is carried out according to the Austrian Signature Law. The validity period of the new certificate may not be longer than 3.25 years. The renewal is only possible, if the cryptographic security provided by the used method (e.g. key lengths, algorithms) is still adequate and no hints for a possible key compromise of the applicants private key exist.

a.sign SSL EV certificates cannot be extended. If a certificate expires, the complete application- and issuing procedure has to be carried out from the beginning.
--
--