A-Trust Gesellschaft für Sicherheitssysteme
im elektronischen Datenverkehr GmbH
Landstraßer Hauptstraße 1b
A-1030 Vienna
Tel: +43 (1) 713 21 51 - 0
Fax: +43 (1) 713 21 51 - 350
https://www.a-trust.at

A-Trust Certificate Practice Statement for a.sign SSL and a.sign SSL EV certificates

Version: 2.1
Date: 2019-04-08

Contents

List of Tables

List of Figures

1 Overview

1.1 Overview

The target of this CPS is to determine the exact implementation of processes defining the issue and administration of a.sign SSL and a.sign SSL EV certificates to ensure a secure and reliable execution of offered certificate services and their application.

A certificate practice statement informs the relying parties about the methods exercised in issuing certificates that are defined by the Trust Center. This definition is used to commit to internal practices and helps relying parties to gain an understanding about the approach implemented by the Trust Center and the existing security standards.

A-Trust follows the requirements outlined by AICPA/CICA, WebTrust 2.1 Program for Certification Authorities, AICPA/CICA, WebTrust for Certification Authorities Extended Validation Audit Criteria, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/B Forum Guidelines for the Issuance and Management of Extended Validation Certificates and CA/B Forum Network and Certificate System Security Requirements. A-Trust services are in line with the regulation 2014/910/EU on electronic identification (eID) and trusted services for electronic transactions in the internal market (eIDAS).

This is the first version of this policy in English language. A Changelog will be implmented for consequent versions.

1.2 Document Name and Identification

Policy Name: A-Trust Certificate Policy for a.sign SSL and a.sign SSL EV certificates
Version: 2.1 / 2019-04-08

Object Identifier: 1.2.40.0.17 (A-Trust) .2 (CPS) .22 (a.sign SSL EV)

1.3 Certificate infrastructure and applicability

1.3.1 Certification authorities

A-Trust is a Certification Authority issuing Certificates according to [eIDAS] and in accordance with this CPS. As a Certification Authority, A-Trust performs functions related to Certificate lifecycle management such as Subscriber registration, Certificate issuance, Certificate renewal, Certificate distribution and Certificate revocation. A-Trust also provides Certificate status information using a Repository in the form of a Certificate Revocation List (CRL) distribution point and/or Online Certificate Status Protocol (OCSP) responder. There is only one central a-trust Certification Authority signing the public keys of the certificate owners, and the revocation information of certificates.

1.3.2 Registration authorities

In addition to identifying and authenticating applicants for certificates, a registration authority (RA) may also initiate or pass along revocation requests for certificates and requests for reissuance and renewal (sometimes referred to as re-key) of certificates. The issuance of a.sign SSL and a.sign SSL EV certificates is solely performed by A-Trust.

1.3.3 Revocation service

For certificate revocation, subscribers are able to contact the revocation service directly via telephone or fax (for details, see chapter 2.5.2).

1.3.4 Subscribers

Subscribers in this context are considered as individuals, who receive SSL or a.sign SSL EV certificates from A-Trust, whereas, those who trust/rely on the certificate details are relying parties/users. Subscribers of a.sign SSL EV certificates are always corporate bodies; this is verified by A-Trust.

1.3.5 Applicability

This document applies for all certificate authorities and the associated registration authorities, as well as the services of these authorities and their subscribers. According to definition, the a.sign SSL (EV) policy is applicable for advanced (a.sign SSL) and qualified (a.sign SSL EV) certificates, which are issued for signature, secrecy and authentication operations. The certificate owners' private keys are stored on their computers. A.sign SSL EV certificates are governed by the regulations of [EV-GL]. EV certificates are identifiable by the corresponding EV-policy OID. The content of qualified a.sign SSL EV certificates is based on Appendix IV [eIDAS]. The subscriber keys have to be generated only by the certificate subscriber in a secure way and never by A-Trust. The subscriber key generation and storage is not bound to certain hardware, but the generation process has to be performed using techniques that guarantee a sufficient level of randomness. A-Trust acts in accordance to the current versions of the relevant CA/Browser Forum Guidelines, published at http://www.cabforum.org. In case of inconsistencies between the CPS / CP of A-Trust and the Guidelines, the policies of the CA/Browser Forum guidelines/requirements shall prevail.

1.3.6 A-Trust Directory Tree

A schema of the directory tree is displayed in figure 1. The certificate of the A-Trust-nQual-nn key is the root certificate, where nn states the version of the root CA, which

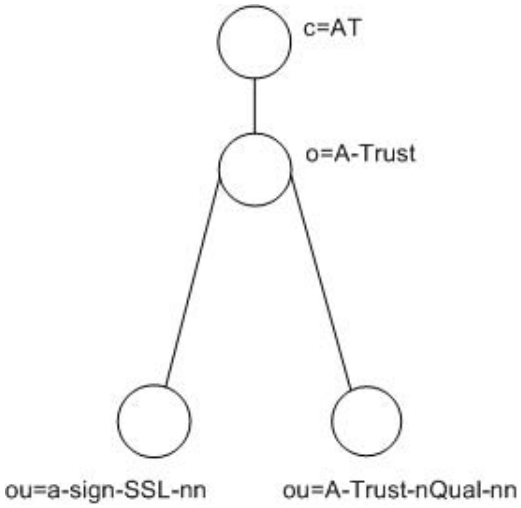

Figure 1: a.trust Directory Tree

generates the signature with the corresponding private key. A-Trust-nQual-nn is used to sign all CA certificates and the corresponding CRLs. The certificates of the a.sign SSL and a.sign SSL EV certificate owners and the corresponding CRLs are signed with the CA keys

- a-sign-SSL-nn
- a-sign-SSL-EV-nn,

where 'nn' states the version of the CA certificate, which uses the matching private key to create digital signatures.

1.3.7 Certificate hierarchy

Figure 2 displays the scheme of the certificate hierarchy.

1.4 Contact Information

1.4.1 Organization Administering the Document

A-Trust Gesellschaft für Sicherheitssysteme
im elektronischen Datenverkehr GmbH
Landstraße Hauptstraße 1b
1030 Vienna
AUSTRIA

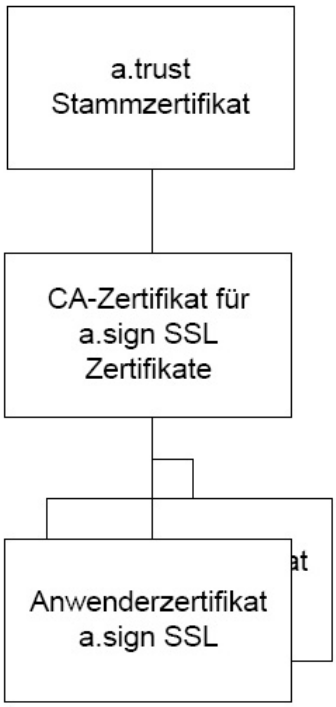

Figure 2: Certificate hierarchy

1.4.2 Channels of Communication

Up to Date contact Information can be found:

- On the A-Trust website https://www.a-trust.at/
- Through the A-Trust Hotline https://www.a-trust.at/support
- In A-Trust Registration Authorities https://www.a-trust.at/registrierungsstellen
- Written by letter

1.4.3 Approving Policies

A-Trust handles the approval process of other Policies.

2 General Terms and Conditions

2.1 Obligations

2.1.1 Certificate Authority Obligations

The Certificate Authority A-Trust acts in accordance with this certification policy, which especially covers the following aspects:

- The certificate owners' certificates are issued revoked and renewed in accordance to this certificate policy.
- The certificate authority acts in accordance to the security and certification concept, presented to the regulatory authority.
- The certificate authority only employs personnel that are sufficiently qualified.
- The certificate authority fulfills its obligations to provide required information to the subscribers and the regulatory authority.
- The certificate authority has appropriate measures in place (technical, organizational, infrastructural and personnel) to provide protection for its private key.
- The private key of the certificate authority is exclusively used to sign the certificates of the subscribers and the revocation information. Remark: Private keys also exist for other purposes. This policy solely covers private keys to sign certificates and revocation lists.
- The certificate authority publishes all issued certificates and revocation lists.

2.1.2 Registration Authorities Obligations

The registration authorities of A-Trust act in accordance with this certification policy, which especially covers the following aspects:

- The registration authority acts in accordance to the security and certification concept, presented to the regulatory authority.
- The registration authorities assure the adherence to the identification and authentication mechanisms described within this policy.
- The registration authorities' employees are qualified adequately.
- The registration authorities submit the a.sign SSL (EV) certificates electronically to the subscriber. A-Trust provides following documents to the subscriber electronically:

- general terms and conditions
- payment terms
- certificate policy, certification practice statement

2.1.3 Subscribers Obligations

The subscribers have to adhere to this certificate policy, which especially covers following aspects:

- The subscribers commit themselves to adhere to the general terms and conditions and the certificate policy for a.sign SSL and a.sign SSL EV, as well as the certification practice statement and payment terms of A-Trust, which are the basis of the concluded agreement.
- The subscriber is responsible for the correctness of the information stated during the registration and makes use of the procedures for identification and authentication described in this policy.
- The subscriber is obliged to protect his private key appropriately. This comprises especially the encrypted storage, which prevents unauthorized access to the private key, as well as the secrecy of the activation data (PIN), if applicable.
- If necessary, the subscriber initiates immediately the revocation of his certificate.
- The subscriber uses the certificate only for the purpose, defined within the certificate (see chapter *Key Usage (X.509 v3 key usage field)*). Applicable for this are the certificate policy and the certification practice statement, valid at the issuance of the certificate.
- The subscriber is obliged to adhere to the national export restrictions as well as the national use restrictions, when using the private key abroad.

2.1.4 Certificate User Obligations

The user of a.sign SSL and a.sign SSL EV certificates is obligated to perform following verification prior to the acceptance:

- The certificate user verifies the validity of the certificate
- The certificate user verifies, whether the certificate has been used as designated (e.g. for generating a digital signature).

2.1.5 Directory Service Obligations

The directory service publishes regularly

- issued certificates and
- lists of revoked certificates

The directory service is obligated to update these lists on a regular basis and to guarantee their availability. The current update frequency of the list of revoked certificates can be found on the website of A-Trust.

2.2 Liability

The general terms and conditions ([AGB]) combined with the certificate policy, the certification practice statement and the payment terms of A-Trust in their current version is the basis of the agreed contract.

2.2.1 Liability of the Certificate Authority

A-Trust is liable towards third parties, which trust in the correctness of the certificate with regard to

- the certificate being revoked immediately under circumstances described in Chapter 4.3.1 and a revocation service being available,
- fulfillment of the requirements of the signature law for providers of certification services,
- adherence to the X.509-standard,
- adherence to the procedures described in this certificate policy.

A-Trust is able to define a limited liability within the certificates. In case such a transaction limit is included in the certificate, A-Trust can only be held liable up to this amount. When there is no amount stated in the certificate, a limitation of the liability is not given.

2.2.2 Liability of the Registration Authority

The certificate authority is liable for the registration authority.

2.3 Financial Responsibility

2.3.1 Damage Compensation for involved Parties

No terms defined.

2.3.2 Fiduciary Relationship

No terms defined.

2.3.3 Administrative Processes

No terms defined.

2.4 Interpretation and (Legal) Enforcement

2.4.1 Legal Basis

The contractual agreement between A-Trust and the subscriber is subject to Austrian law. In a contractual relationship with a foreign certificate owner, the application of the United Nations Convention on Contracts for the International Sale of Goods is explicitly excluded.

2.4.2 Separability of Terms, Persistence of Claims, Fusion, Termination

A-Trust is entitled to transfer rights and obligations from the existing contract to a third party. A special termination right does not arise herewith to the subscriber, as long as the third party exercises the rights and obligations of the contract. Changes to the general terms and conditions, like the certificate policy, will be announced to the subscriber on certificate renewal. In case A-Trust makes amendments to the terms and conditions, the subscriber has the possibility to terminate the contract anytime. Should the subscriber not disagree within one month to the amended general terms and conditions, they are regarded as agreed up on.

2.4.3 Arbitration

No terms defined.

2.5 Fees

The current applicable fees can be found in the payment terms. All fees, which are not included in the base fee, will be charged upon consumption of the service.

2.5.1 Retrieval of Certificates

The retrieval of a.sign SSL and a.sign SSL EV certificates via the directory service is free of charge.

2.5.2 Revocation of Certificates

The revocation of a certificate is free of charge.

2.5.3 Retrieval of Status Information

The access to the revocation lists and the status information is free of charge.

2.5.4 Guideline for the Refund of Fees

The subscriber is not entitled to the refund of fees. In case of a contract termination, the certificate owner has to pay the fees until the end of the payment period.

2.6 Repository

2.6.1 A-Trust Root certificates

The current root certificate can be found at https://www.a-trust.at/certs/A-Trust-Root-nn.crt or through LDAP via ldap://ldap.a-trust.at/ou=A-Trust-Root-nn,o=A-Trust,c=AT. Older versions of the root certificate can be found in the LDAP directory.

Additional Explanation: nn states the Root-CAs generation and is incremented when a new key is generated. A link to the current Root certificate is also published on the A-Trust Website.

2.6.2 A-Trust Intermediate CA certificates

The deployed intermediate certificate for a.sign SSL and a.sign SSL EV certificates can also be accessed through the A-Trust Website or the A-Trust LDAP:

- https://www.a-trust.at/certs/a-sign-SSL-nn.crt or ldap://ldap.a-trust.at/ou=a-sign-SSL-nn,o=A-Trust,c=AT
- https://www.a-trust.at/certs/a-sign-SSL-EV-nn.crt or ldap://ldap.a-trust.at/ou=a-sign-SSL-EV-nn,o=A-Trust,c=AT Additional Explanation: nn states the Intermediate-CAs generation and is incremented when a new key is generated.

2.6.3 Publication of Revocation

Distribution Points for CRLs for a.sign SSL and a.sign SSL EV:

- ldap://ldap.a-trust.at/ou=a-sign-SSL-nn,o=A-Trust,c=AT?certificaterevocationlist?base?objectc
- ldap://ldap.a-trust.at/ou=a-sign-SSL-EV-nn,o=A-Trust,c=AT?certificaterevocationlist?base?obj

The current CRL can be downloaded from the A-Trust Homepage (https://www.a-trust.at/directory) additionally.

2.6.4 Repositories

A-Trust publishes following documents on its Website https://www.a-trust.at:

- The current CPS for a.sign SSL and a.sign SSL EV
- The current CP for a.sign SSL and a.sign SSL EV
- A-Trust General Terms and Conditions
- audit reports
- the A-Trust Root certificates
- current price-lists
- a list of points of contacts and registration authorities

Following Information is published in case of an incident:

- revocation of A-Trust Root or Intermediate CA keys
- suspicion of compromise of A-Trust keys
- long interval outages
- major changes in CP or CPS

- CA or RA termination

The Information is provided via following channels:

- A-Trust Website
- optional: Newsletter via E-Mail
- optional: through mail for subscribers
- optional: Austrian Media (TV, newspapers)

Information that is only relevant for single subscribers is delivered directly.

2.6.5 Frequency of Publication

Updates of the CPS are outlined in section 8.

2.6.6 Access control on Repositories

Reading access to the repositories is publicly available to anyone. Access controls are in place to assure that only cleared employees are able to perform changes to the documents and are able to oversee CRLs.

2.7 Audits

2.7.1 Frequency

Internal revisions and audits are performed annually. a.sign SSL EV certificates are monitored monthly. Three percent of all certificates issued since the last audit are reviewed with a focus on the integrity of the process. This audit is documented. External audits for SSL certificates are performed in the outlined intervals. Additionally A-Trust is monitored by the Austrian Regulatory Authority for Broadcasting and Telecommunications.

2.7.2 Identity and Qualifications of Assessor

Internal audits are carried out by Security Officers according to the A-Trust role concept.1 External audits are performed by public accounting firms that are independent of A-Trust.

2.7.3 Topics covered by audits

The auditor reviews the compliance of A-Trust with the underlying CP and CPS. Internal audits also cover confidential documents like internal risk and security policies. The auditor confirms the proper adherence to those principles. External audits also cover principles layed out by specific requirements as stated in section 1.1.

2.7.4 Actions taken as a result of Deficiency

Following consequences are taken if an audit returns an insufficient outcome:

- Revocation of the affected certificate
- Cessation of service for a specific product if the affected certificate is an Intermediate or Root certificate
- A deadline is given to correct the existing problem so the certificate life cycle can be returned to a safe state

2.7.5 Communication of Results

A-Trust publishes external audit result. Internal audits are available to external auditors and the Austrian Regulatory Authority for Broadcasting and Telecommunications.

2.8 Confidentiality

2.8.1 Confidential Information

A-Trust ensures, that the data provided by the subscriber is handled confidential according to Austrian and European Data Privacy Laws. Data provided throughout the registration process is solely used to provide the services ordered by the customer. Every information related to personal data that is not included in the certificate is is deemed confidential.

2.8.2 Non confidential Information

Information included in certificates, status information and revocation lists are not deemed confidential.

2.8.3 Publication of Information regarding revocations

Reasons that trigger a revocation are expressed in the A-Trust directory.

2.8.4 Relaying of Information

A-Trust obtains the subscribers agreement before relaying confidential data related to the subscriber to public entities and for reasons subject to private law if the relaying is not required by Austrian or European law.

2.8.5 Intellectual Property Rights

Intellecutal property rights for following documents and keys belong to A-Trust:

- Certificate Practice Statement
- Certificate Policy
- A-Trust private keys
- A-Trust public keys

Intellecutal property rights for following documents and keys belong to the subscriber:

- Subscribers private key
- Subscribers public key

2.9 Publishing and Acceptance of Certificates

The created certificate can be provided to the subscriber digitally in two different ways:

- Via e-mail.
- Via search on the A-Trust website (the URL will be send to the subscriber via e-mail) for the individual common name. The search result is the download link of the certificate.

2.10 Revocation of Certificates

For all types of a.sign SSL Certificates an immediate and permanent revocation of the certificate is possible. The retrieval of the revocation list via directory service (LDAP) or OCSP is possible at any time; the availability is guaranteed by the redundant setup of the data centers and the corresponding contracts with their providers.

2.10.1 Reasons for Revocation

The revocation of a certificate is necessary, when

- essential information of the certificate are no longer correct,
- the private key to an a.sign SSL or SSL (EV) certificate cannot be used anymore (e.g. defect storage and no backup is available),
- suspicion of compromise exists (e.g. unauthorized access to the computer where the private key is stored), respectively a compromise occurred,
- the certificate authority becomes aware of a relevant breach of this policy or the general terms and conditions by the subscriber,
- the contractual relationship ends,
- the person of the subscriber changes,
- the used algorisms are no longer sufficient to match the security expectations,
- the certificate authority goes out of businesscertificate.

The requirements of [EV-GL] 13 are applicable for a.sign SSL EV certificates.

2.10.2 Who can Request Revocation

A revocation of the certificate can be requested by:

- the subscriber,
- the certificate authority and
- everyone, who knows the password for revocation.

2.10.3 Procedure for Revocation Request

The revocation of an a.sign SSL (EV) certificates is made via phone or fax at the corresponding revocation service. The current telephone number of the revocation service can be found on the homepage (http://www.a-trust.at/widerruf). The revocation service is available 24x7 and has a direct contact to the A-Trust support hotline.

There exist the following requirements for the procedure:

- The revocation password has to be given in order to revoke the certificate.

- The reason for the revocation (e.g. compromise of the private key, termination of contract) has to be stated to the employee of the revocation service.

The required information for the revocation can be broken down into following:

- Password for the revocation: obligatory
- Domain name or certificate number: obligatory

In case the password cannot be provided for the revocation of an a.sign SSL or a.sign SSL EV certificate, the revocation process can be initiated by a registered letter (including corporate signature). Alternatively the subscriber can arrange a suspension of the certificate after a successful identification.

2.10.4 Suspension of a Certificate

A.sign SSL and a.sign SSL EV certificates can only be revoked, suspension ist not available.

2.10.5 Procedure for the Suspension Request

A.sign SSL and a.sign SSL EV certificates can only be revoked, suspension ist not available.

2.10.6 Time within Which CA Must Process the Revocation Request

According to the Austrian signature law, the update of the revocation service has to be performed within three hours after stating the reason for revocation.

The revocation service is available 24x7 and has a direct contact to the A-Trust support hotline or online (http://www.a-trust.at/widerruf).

2.10.7 Update Frequency of the Revocation List

The update frequency of the revocation list can be found in the CRL.

In case a revocation is issued the entry stays in the CRL even after the 'valid to' date of the certificate.

2.10.8 Revocation Checking Requirements for Relying Parties

Prior to relying upon a certificate, relying parties must validate the suitability of the certificate to the purpose intended and ensure the certificate is valid. Relying parties

will need to consult the CRL or OCSP information for each Certificate in the chain as well as validating that the certificate chain itself is complete. This may include the validation of Authority Key Identifier (AKI) and Subject Key Identifier (SKI).

2.10.9 Online Revocation/Status Checking Availability

A-Trust established an OCSP service (http://ocsp.a-trust.at/ocsp) for an online revocation/status check.

2.10.10 Revocation Checking Requirements

Relying Parties must confirm revocation information otherwise all warranties becomes void. The validation of the revocation information comprises the check of the signature of the corresponding information from the directory service, as well as a match of the verification date and the status date of the requested status information.

2.10.11 Other Forms of Revocation Advertisements Available

No stipulation.

2.10.12 Requirements for Other Forms of Revocation Advertisements

No stipulation.

2.10.13 Special Requirements Related to Key Compromise

In case of any suspicion for an a.sign SSL respectively an a.sign SSL EV certificate being compromised, the subscriber has to request revocation.

3 Identification and Authentication

3.1 Initial Registration

3.1.1 Naming

Subscriber data is divided into two categories - required and optional Information. A.sign SSL EV requires additional data as outlined in [EV-GL]. Following data has to be submitted:

- Common Name: Domain that the SSL certificate is issued for. IP Addresses are not permitted.
- Organization Name: full Organization name as registered in the inspected registers (eg. the Austrian Commercial Register). Required for SSL EV certificates. The Distinguished Name has to be distinct and always assigned to the same subscriber.
- Nationality
- Name of the Organizational Unit
- E-Mail Address
- Additional Fields for SSL EV certificates: Business Category, Jurisdiction of Incorporation or Registration, Company Registration Number, physical Address, see[EV-GL]

3.1.2 Rules regarding the Interpretion of different name forms

No Regulation

3.1.3 Need for Names to be Meaningful

The subject of a.sign SSL and a.sign SSL EV certificates is distinct due to the combination of Common Name, Organization, Organizational Unit and other fields.

3.1.4 Claim to Names and settlement of Dispute

No Regulation

3.1.5 Recognition, Authentication and Role of Trademarks

Certificate Applicants are responsible for the use of the submitted names and are therefore liable for legal action.

3.1.6 Method to Prove the Possession of the Private Key

The subscriber has to generate the key pair using appropriate Software or Hardware Devices (Smartcard, HSM) while creating the certificate request. This request is sent to A-Trust and therefore used to issue the certificate. This ensures that the private key belonging to the public key included in the certificate request is under exclusive control of the applicant.

3.1.7 Authentication of organisations

When ordering an a.sign SSL EV certficate, 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 inlcuded in the request.

The physical address is also verified using the offical 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] and [eIDAS].

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 in [EV-GL].

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 adresses 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).

3.2 Returning Customers / Re-Key

a.sign SSL and a.sign SSL EV certificates are not renewed, orders by returning customers are treated like initial requests. Subscribers receive a notification prior to the end of the validity of the certificate and is invited to provide a new PKCS#10 Request using a new private key. All controls from section 3.1 are carried out as if the request was an initial request.

3.3 Renew after Revocation

See 3.2

3.4 Authentication for Revocation

The process for revocation is outlined in section 4.3.

4 Operational Requirements

4.1 Request for Certificate Issuance

The application is done via the form provided at the A-Trust homepage.

Passport copies and confirmations are sent to the registration authority by the subscriber.

In case the affiliation to a government agency should be stated within the certificate, the correctness of this information has to be confirmed in writing by an official representative to the registration authority.

The procedures of the application for the issuance of an a.sign SSL EV certificate are subject to the requirements from [EV-GL] section 10 and 11. The identification of the

natural person named in the application, has to be done in person with an official passport. Copies of the used passport will be deposited. Alternatively, the identity can be verified by a qualified signature (based on a certificate issued by A-Trust).

In case several applications for a.sign SSL (EV) certificates are submitted by the same applicant at the same time, the applications have to be submitted individually. Documents submitted for this purpose will be taken into account for all applications, as long as the applications have been submitted at the same time.

4.2 Publication of certificates

The issued certificate is made available to the applicant via

- E-Mail
- the A-Trust Website

4.3 Log Procedures

4.3.1 Events Recorded

- Changes in the role concept
- Changes in the software configuration (Updates or new Software)

Additional type, time, success and event owner for every transaction is logged, that affects core systems. Following transaction types are logged:

- Certifcate Requests
- Key Generation
- Issuing of certificates
- Publishing of CRLs and certificates
- Revocation Requests
- Performed revocations
- Key changes

Events that are stored throughout the registration process include following data:

- Acceptance of A-Trust Terms and Conditions
- Subscriber Data changes (eg. Home Address)

4.3.2 Frequency of Processing Log

The Eventlog is checked for suspicious occurrences on a daily basis, live monitoring alerts employees in case of critical Events.

4.3.3 Retention of Logs

Security relveant logs are retained for an unlimited amount of time. Logs that are needed to allow A-Trust to make detailed statements regarding to the validity of single certificates are archived. This includes information on the issuing of the certificate and CRLs. The exact retention time of archived log files is covered in section 4.5.2.

4.3.4 Protection of Audit Logs

Logs are created and stored in different locations and are only accessible for authorized employees. Every archived log file is signed to prevent modification.

4.3.5 Audit Collection System

Audit Logs are generated internally using the A-Trust core systems.

4.3.6 Notifcation to event causing Subject

A-Trust decides on a case basis if a security related event has to be related to the causing party.

4.3.7 Vulnerability Assessments

No Regulations.

4.4 Archiving

4.4.1 Archived data

Following data is archived:

- Data of the subscriber that has been used for the certificate request
- Certification Application

- All certificates issued by the Certification authority (Certificates of the Certification Authority, Cross-Certificates and Certificates of Certificate Holder)
- Cancellation Requests with time and date of arrival (including relevant protocol data)
- All issued revocation lists
- Date and time of the publication of certificate and revocation lists (including relevant protocol data)
- Date and time of the key change of the Certification authority and
- Data about procedures and policies (CP, CPS)

4.4.2 Retention periods

Retention period is at least 7 years. Following aspects must be considered:

- Data must be stored at least as long as they could be needed in case of recovery of system components during the application period.
- Especially in the case of usage of digital signatures, data must be stored at least as long as digitally signed documents could be inspected.
- Technical compatibility must be considered as well. This is particularly relevant for Soft- and Hardware that, in case they are altered in any way, makes an inspection of the documents impossible.

Provisions from [EV-GL] are relevant for a.sign SSL EV certificates.

4.4.3 Protective Measures

Archive is located in safe rooms. Access is permitted only to authorized personnel and an exact regulation is determined inside a role concept. Electronic documents are protected from modifications through digital signatures of the archived unit. Access and admission control enables only two persons from a particular area of responsibility access and alteration rights at the same time.

4.4.4 Data Time stamp Requirement

All certification requests must be time-stamped. This is particularly relevant for cancellation requests and changes on cancellation lists.

4.4.5 System of collection of archived data (internal/external)

The Certificate management system is responsible for the process of archiving of all data that have to be archived in the A-Trust system.

4.4.6 Procedures for data retrieval and check

When archiving electronic data over a long period of time, incompatibility of the data with the new systems must be taken into account. Due to this fact, the Approved Certification authority holds these systems active so that these data can be processed over the whole archiving period. Measures are taken so that, in case of service interruption or cessation of the Approved Certification authority, the archive remains intact.

4.5 CA key changes

A key change of CA and root keys may be related to the Failure of a hardware security module and is necessary in any case, if the key lengths or algorithms used no longer meet the safety expectations or in the case of compromise of keys. In the latter case, a revocation of the affected certificates is absolutely necessary.

The CAs regularly renew their certificates before the expiration of the period of validity specified in the certificate. The validity period of the certificates can be found in the respective certificate profile. The reviewer of a certificate receives the new certificate through the directory service. He can check the validity of the certificate via the certification chain.

With a key change, the old key loses its active validity and the private key is no longer used for certification. Only the new key is used to sign certificates. The certificate for the old key will only be revoked if necessary (e.g. compromised). If the old key has not been revoked, it may be used to validate certificates until the validity period ends.

If existing technical standards are unchanged and the algorithm used still meets the security expectations and legal requirements, no new key is generated but the period of validity of the certificate is renewed at regular intervals.

4.6 Compromise and emergency plan

4.6.1 Hardware, Software and/or Data are corrupted

If faulty or manipulated hardware, software or data that could affect the security of the system and its services have been discovered, the corresponding components are immediately removed from service.

In the case of certificates, the signatories concerned must be informed. Affected certificates will be revoked, if the certificate contains incorrect information.

In case of errors in a revocation list, a correct revocation list will be issued immediately. If a secure and immediate issue of the revocation list is not possible and the errors are critical to security, the directory services are shut down to prevent the publication of incorrect data. The resumption of the service is associated with the publication of the new revocation list. Depending on the errors and the downtime of the directory services, the users are informed. Once the identified deficiencies have been eliminated, the components that may have been switched off are put back into service.

4.6.2 Revoking Certificates of Certification Authority Keys

Certification Authority certificates are revoked:

- in case of compromise or suspicion of compromise of the corresponding Key,
- if the algorithms used no longer meet the safety expectations and thus a safe application would no longer exist,
- upon cessation of the activity of the CA, if the revocation list or Status information services are no longer maintained.

Depending on the reason of the revocation of the certificate, the according sections of this CPS apply.

If a revocation is planned in advance, the signatories will be informed in time. An unplanned revocation requires immediate information of the certificate holder. The information is provided via the web page. Private keys of the CA that have their associated certificates revoked are no longer used by the CA. These private keys are destroyed according to the CPS.

Revoking Certificates of CA Services

If certificates of services of the CA are revoked, the services without a valid key are immediately removed. This prevents users from using services whose signatures are invalid. The revoked keys are replaced by new keys. The services will not start up until the new, valid keys have been installed.

Revoking CA Certificates

If a certificate of the CA is revoked, all certificates issued under this certificate have to be revoked as well. The status information service will generally respond with an invalid status to requests for all certificates issued under the CA or its subunits. Signatories whose certificates are affected by the revocation will receive a new certificate according to the specified procedures. The certification is carried out with a new CA key.

Key Change

After the revocation of the certificate, the associated private key will no longer be used. In order to maintain the certification services, the CA has to use a new key. If the CA already has such a new key because of a key change that has been carried out, the key can be used. However, this is only possible on the condition that the key is still valid. If this is no longer the case, then a key change according to the guidelines from this CPS is carried out, that, however, differs from the regular change in following ways:

- A timely information for Signatories regarding the key change is not possible in case of immediate revocation. In this case, the information regarding the revocation also includes information on the key change.
- Cross-certification with the invalid certificate is not used to verify the authenticity of the new certificates. Information about the new keys will include new Certificates issued by the CA, with which the authenticity of the new Certificates can be checked.
- Revoked keys are invalid and will not be used any more.

Revocation of Cross-Certificates

If a certificate of the CA is revoked, all cross certificates created for it are also revoked. This also applies to cross certificates issued for other CAs. This is especially true if the security requirements are no longer met by this CA.

4.6.3 Key compromise or suspected key compromise

If the compromise of keys is suspected in a CA, a Security Officer is immediately informed. The SO enforces the revocation of affected certficates. Important actions after the compromise of keys:

- Subscribers are informed immediately
- Directory and status services are taken offline if needed
- Distribution of new, valid certificates inluding new keys if needed

The SO has to perform checks, if other keys have been compromised and what keys can be considered safe after the incident.

4.6.4 Security measures after incidents

The SO has to decide if the safety of the CAs' services is endangered by the incident and to implement safety measures accordingly. Subscribers are informed if integral parts of the CAs' services such as revocation or web services are unavailable due to the incident.

This information will be distributed through mail if electronic options (Website, E-Mail) are not available.

Devices containing critical data are stored in a secure environment if the pyhsical security of the CA is in danger.

4.7 Cessation of any acticities

Access to archived records is guaranteed even in case the CA ceases its activities.

A cessation of the CAs' activities will be announced to every affected entitiy at least three months prior. All remaining certificates will be revoked after this period and the subscribers receive written confirmation of the revocation. Relevant data concerning the subscribers is stored and CRLs are made available publicly even afert the cessation.

4.7.1 Insurance

A-Trust GmbH is insurance holder according to the [eIDAS] regulation. The insurance policy fulfills the requirement from [EV-GL] by having an A rating.

5 Physical, Process and Personnel related Safety Precautions

5.1 Physical Safety Precautions

5.1.1 Location and regional considerations

A-Trust services are performed on following locations:

	Address
Head Office	**A-Trust** Gesellschaft fuer Sicherheitssysteme im elektronischen Datenverkehr GmbH Landstrasser Haupstrasse 1b A-1030 Wien
Registration, cancellation service	Registration office and cancellation service can be found at: https://www.a-trust.at/.

Table 1: Service Locations

5.1.2 Access Control

Access to all technical components in the computer center is only possible through the A-Trust authorization system.

Access controls are adjusted to the pursued security levels of particular areas which contain different critical security components.

Access to the high-level security area of the computer center is restricted and requires two persons with appropriate authorization cards and requires the correct entry of PIN-codes. All admittances are logged and can be traced at any time. Additionally, Video-Surveillance-Systems as well as Intrusion Alarm Systems are installed.

5.1.3 Power Supply and air conditioning system

Power supply on site is in accordance with international standards and is designed, excluding registration offices, in a redundant fashion. Additionally, there is an emergency power supply for the data center.

Sites that contain A-Trust technical components are equipped with an appropriately sized air conditioning system.

5.1.4 Water damage

Sites that contain A-Trust technical components are properly protected against water damage.

5.1.5 Fire

All sites that host technical components are equipped with an appropriate fire alarm system.

In the high-level security areas of the computer center, fire alarm systems conforms the local regulations regarding fire protection in high-level security computer centers.

5.1.6 Data media

There are following data media:

- Paper
- Magnetic tapes
- Hard-disks

- DVDs
- WORMs

Data media with sensitive or highly security relevant data are access protected and kept in locked rooms or vaults.

5.1.7 Waste disposal

Data on the electronic data media are destroyed and transferred to a specialized company for a proper disposal afterwards. Paper data media are destroyed using shredders and transferred to a specialized company for a proper disposal afterwards.

5.1.8 Redundant design

All services in the computer center are, as far as technically possible, designed in a redundant way so that high availability (7x24 hours) of the services of the data center is ensured.

5.2 Procedure-oriented Precautions

This chapter outlines the roles defined at A-Trust. The roles are explained and classified by their security impact.

5.2.1 A-Trust Tasks

Tabelle

5.2.2 Security related tasks

Tabelle

5.2.3 Other tasks

Tabelle

5.2.4 People needed for security related tasks

Tabelle

5.2.5 Authentication of roles

The access control limits the acces to premises holding security relevant components to persons that are allowed to enter due to the role concept.

5.2.6 Risk analysis

Risk analysis are carried out while developing a new process for certificate issuance. A-Trust conducts a yearly review of these risk analysis to detect if any risks habe changed in their impact or the probalitity, that the risk will occur.

5.3 Staff precautions

5.3.1 Staff requirements

Staff employed by A-Trust fulfills all requirements regarding reliability, integrity, and technical qualifications in the following sectors:

- IT education,
- Security technology, cryptography, digital signature and Public Key Infrastructure,
- technical standards,
- Hard- and Software.

5.3.2 Staff Reliability

Employees hired to partake in security relevant tasks have to provide certificate of conduct issued by the Austrian government. This certificate may not be older than two years and has to be renewed accordingly.

5.3.3 Training

Trainings concerning security and functional issued held by capable staff are conducted regularly. Some roles required specific trainings and can only be assigned after completion.

5.3.4 Training intervals

Trainings are conducted for new employees and after significant changes in the internal system or after major developments occur in the market.

5.3.5 Job Rotation

No regulations.

5.3.6 Sanctions for unauthorized actions

Grave violations of security measures are handled through disciplinary measures.

5.3.7 Staff contracts

Employees are bound to confidentiality through their work contract.

5.3.8 Documents made available to the staff

Employees have access to the following documents:

- Betriebskonzept (Operation Manual),
- Certificate Practice Statement and
- Training materials.

6 Technical Safety Precautions

6.1 Key generation and installation

6.1.1 Key generation

Key of the Approved Certification Authority

The key of the Certification authority for signature of the a.sign SSL und a.sign SSL EV certificates is generated in Hardware Security Module of the Certification authority. For the secret key of the Certification authority there is an export or alternatively back-up to another Security Module, which is held active in case of service interruption.

Key of the Subscriber

Keys are generated by Certificate Holder in a Software or Hardware module, with respect to mechanisms that guarantee an appropriate quality of coincidence. A-Trust has no insight into the private keys. Certificates are generated by Certification authority based on PKCS# 10-Requests, produced by the requester.

6.1.2 Delivery of Private Keys to Subscriber

Delivery of private keys is not permitted because only the subscriber can control private keys and A-Trust has never access to private keys of the subscriber.

6.1.3 Delivery of public keys to Subscriber

Public Keys of the Certification Authority

Certificates of the Root-CA key as well as certificates of all certification bodies are published in a directory on Internet so that access remains public and all Certificate users can inspect certificates.

Public keys of a.sign SSL (EV) Certificate

The key pair is generated by subscriber himself and he is in possession of the public key.

6.1.4 Key Lenghts

The key length of root and all intermediate CAs is at least 2048bit (RSA). SHA-256 is used as Hash-Algorithm for all certificates. Subscriber certificates are also required to have a key lenght of at least 2048 Bit (RSA).

Minimum key lenghts can be changed due to changes in laws or underlying guidelines and policies.

6.1.5 Key generation

CA keys are generated using a random number generator based on a physical noise source.

6.1.6 Quality Testing

The person responsible for IT Security ensures the adherence to effective laws regarding the paramaters of key generation and guarantees that the physical random number generator is used correctly.

6.1.7 Hardware/Software key generation

The root and interemdiate CA keys for a.sign SSL and a.sign SSL EV are genereated and used in a purpose-built Hardware module.

The subscriber keys are generated by the applicant (see chapter *Key generation*) using Software or Hardware tools. The CA has no knowledge about the subscribers' private key.

6.1.8 Key Usage (X.509 v3 key usage field)

The key usage is defined in the X.509 v3 extension 'keyUsage'.

Key usage of root CA keys

The root CA is self signed with following key usages set in the extension 'keyUsage':

- keyCertSign (certificate signing)
- cRLSign (CRL signing)

Key usage of intermediate CAs

The intermediate CA has following key usages set in the extension 'keyUsage':

- keyCertSign (certificate signing)
- cRLSign (CRL signing)

Key usage of subscriber certificates

Following key usage extensions are set for subscriber certificates:

- digitalSignature
- keyEncipherment

The

6.2 Protection of private keys

6.2.1 Protection of private CA keys

The private key of the Root CA is only used to sign Intermediate CAs. The private keys of Intermediate CAs are used to sign subscriber certificates and CRLs. Both key types are only used in a safe environment.

Root and Intermediate CA keys for a.sign SSL and a.sign SSL EV certificates are generated and kept in Hardware Security Modules that offer adequate physical access control.

6.2.2 Protection of subscriber private keys

Subscriber private keys are generated and secured by the subscriber.

6.2.3 Key escrow

Key escrow is not possible for Root, Intermediate or subscriber private keys.

6.2.4 Backup of private keys

Private keys of Roote and Intermediate CAs for a.sign SSL and a.sign SSL EV certificates are migrated to a backup Hardware Security Module for redundancy.

6.2.5 Archiving private keys

Private keys of Root and Intermediate CAs are not archived.

6.2.6 Insertion of private keys into the cryptographic module

The private key of Root and Intermediate CAs can only be generated in Hardware Security Modules. Generated keys can be exported and inserted into another HSM to generater redundancy.

All signing procedures using the keys are carried out on the cryptographic hardware module and is secured by user authentication and four-eyes principle.

6.2.7 Deactivation of private keys

Private CA keys that are not in use any more are disabled using the apporpriate function of the Hardware Security Module.

6.2.8 Deletion of private keys

Private CA keys that are not in use any more are deleted using the apporpriate function of the Hardware Security Module if needed.

The subsciber is responsible for the deleteon of subscriber keys.

6.3 Further aspects of Key Management

6.3.1 Archiving public keys

see Chapter *Repository*

6.3.2 Validty periods public and private keys

The Shell Model is used for a.sign SSL and a.sign SSL EV. The Intermediate CA has to be valid at the point of time, the subscriber certificate has been issued.

Maximum validity periods of certificates (in years):

- Root CA: 20 years
- Intermediate CA: 20 years
- Subscriber (a.sign SSL): 2 years
- Subscriber (a.sign SSL EV): 2 years

6.4 Activation data

6.4.1 Creation and installation of the activation data (PINs) for the keys of Certification Authority

Keys of the ROOT-CA and Certification Authorities for a.sign SSL and a.sign SSL EV certificates can only be activated within the "four-eye" principle of two officers using chip cards and PIN. Activation data are directly created in a Hardware Security module of the CA-System. Created activation data are not recorded. There is a sufficient number of chip cards so that, in case of damaged or missing chip cards, keys of the Certification Authority are not endangered.

6.4.2 Protection of the activation data

Activation data for the keys of Certification authority

Employees possessing activation data for the keys of the Certification Authority are obliged to keep them secret (PIN) and safe (chip card).

Activation data for the keys of signatories

Signatories are, if in possession of activation data for the secret key (PIN), obliged not to pass them on or keep them on locations accessible to unauthorized individuals.

6.5 Computer security regulations

6.5.1 System computer security requirements

No regulations.

6.5.2 Assessment of computer security

No regulations.

6.6 Life cycle of the security measures

6.6.1 System development

System development policies are aligned with the security regulations of A-Trust.

6.6.2 Security management

Security management policies are aligned with the security regulations of A-Trust.

6.6.3 Assessment

Assessment policies are aligned with the security regulations of A-Trust.

6.7 Network security provisions

Transfer of the critical data is conducted through appropriately secured communication channels. All security-related components that can be accessed over Internet, must be secured through a firewall solutions.

6.8 Provisions regarding maintenance (analysis) of the cryptographic module

Maintenance is conducted strictly by respecting the four-eye principle.

7 Certificate and CRL Profile

Certificates issued under this CPS are X.509 v3 certificates.

7.1 Certificate Profile

7.1.1 CA certificates

Attribute	Content	Description
Version	v3(2)	Version number '2' denotes an X.509 Version 3 certificate
Serial number	Certificate serial number	distinct in A-Trust certificate infrastructure
Algorithm	≥ SHA-256	Algorithm used to sign the certificate
Certificate Issuer	CN = CommonName OU = OrganizationalUnit O = Organization C = AT	CommonName, OrganizationalUnit: A-Trust-nQual-nn Organization: A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH
Valid from Valid To	Begin and end of the certificates validity period	Maximum validity is ten years
Certificate Owner (subject)	CN = CommonName OU = OrganizationalUnit O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	CommonName, OrganizationalUnit: a-sign-SSL-nn or a-sign-SSl-EV-nn -nn CA root certificate generation
Public Key	≥ RSA 2048 Bit	CA public key

Table 2: CA certificate profile

7.1.2 Subscriber certificates

Attribute	Content	Description
Version	v3(2)	Version number '2' denotes an X.509 Version 3 certificate
Serial number	Certificate serial number	distinct in A-Trust certificate infrastructure
Algorithm	≥ SHA-256	Algorithm used to sign the certificate
Certificate Issuer	CN = CommonName OU = OrganizationalUnit O = Organization C = AT	CommonName, OrganizationalUnit: A-Trust-nQual-nn Organization: A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH
Valid from Valid To	Begin and end of the certificates validity period	Maximum validity is 24 months
Certificate Owner (subject)	CN = CommonName OU = OrganizationalUnit O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	CommonName, OrganizationalUnit: a-sign-SSL-nn or a-sign-SSl-EV-nn -nn CA root certificate generation
Public Key	≥ RSA 2048 Bit	Subscriber public key

Table 3: a.sign SSL profile

Attribute	Content	Description
Version	v3(2)	Version number '2' denotes an X.509 Version 3 certificate
Serial number	Certificate serial number	distinct in A-Trust certificate infrastructure
Algorithm	≥ SHA-256	Algorithm used to sign the certificate
Certificate Issuer	CN = CommonName OU = OrganizationalUnit O = Organization C = AT	CommonName, OrganizationalUnit: A-Trust-nQual-nn Organization: A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH
Valid from Valid To	Begin and end of the certificates validity period	Maximum validity is 24 months
Certificate Owner (subject)	C = CountryName CN = CommonName O = Organization OU = OrganizationalUnit E = E-Mail address SerialNumber = SerialNumber	CountryName: AT, DE, ... CommonName: Domain Organization: Organisation name as listed in public register (or abbreviation) OrganizationalUnit: eg. department, optional E-Mail address: optional SerialNumber: unique serial number identifying the subscriber
Public Key	≥ RSA 2048 Bit	Subscriber public key
BusinessCategory	OID	see [EV-GL] section 8
Jurisdiction of Incorporation Locality	OID	Organisations place of jurisdiction (see [EV-GL] section 8)
Registration Number	OID	eg. Firmenbuchnummer [EV-GL] section 8
physical address of the subscribing organsation	OID	[EV-GL] section 8

Table 4: a.sign SSL EV profile

7.1.3 Certificate Extensions

Following X.509 v3 and PKIX extensions are used:

Extension	Type of Certificate		Classification	
	Root	CA	critical	non critical
Standard extensions				
authorityKeyIdentifier	no	yes		X
subjectKeyIdentifier	yes	yes		X
keyUsage	yes	yes	X	
subjectAltName	optional	optional		X
basicConstraints	yes	yes	X	
CRLDistributionPoints	no	yes		X
Private Extensions				
authorityInfoAccess	no	yes		X

Table 5: Extensions (CA certificates)

The usage of Extensions used in certificates issued by the CA are displayed in the following tables:

Extension	present in certificate	Classification	
		critical	non critical
Standard extension			
authorityKeyIdentifier	yes		X
subjectKeyIdentifier	yes		X
keyUsage	yes	X	
extkeyUsage	optional		X
certificatePolicies	yes		X
basicConstraints	yes		X
cRLDistributionPoints	yes		X
subjectAltName	optional		X
Private Extensions			
authorityInfoAccess	yes		X
qc-Statement	yes		X
1.2.40.0.10.1.1.1	optional		X
1.2.40.0.10.1.1.2	optional		X
1.3.36.8.3.4	optional		X

Table 6: Extensions (a.sign SSL and a.sign SSL EV certificates)

The extension keyusage is definied in section "Key usage (X.509 v3 key usage field)".

SSL certfifcates can contain an OID, that identifies the organisation as a or affiliated to a governmental entity ("Behördenkennzeichen" - OID 1.2.40.0.10.1.1.1, "Dienstleistereigenschaft" - OID 1.2.40.0.10.1.1.2).

The extensions definied in [ETSI TS 119 495] are used In case of a certificate according to section 34 [PSD2].

7.1.4 Identification of this Policy

The extension certificatePolicies in the certificate is encoded as follows:

- OID 0.4.0.194112.1.4 gem. [ETSI 319 411]
  itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-web (4)
- OID 0.4.0.194112.1.2 gem. [ETSI 319 411]

and

- OID 1.2.040.0.17.1.22
  1.2.040.0.17 (A-Trust).1 (Policy).22 (a.sign SSL EV)

7.2 CRL Profile

7.2.1 Versionsnummern

CRLs issued under this CPS are X.509 v3 certificates.

7.2.2 CRL and CRL Entry Extensions

The non critical extensions authorityKeyIdentifier und CRLNumber are usesd for full CRLs.

Additionally, the critical extension deltaCRLIndicator is used for Delta-CRLs.

The non critial extension reasonCode is used in case of CRL Entry Extensions.

8 Administration of this Document

8.1 Procedures for hanging this Document

Changes to this certification practice statement are conducted strictly by A-Trust and must be approved by the board of directors. Changes that are connected with security-related aspects or require alteration in the processes on the side of subscribers need a change in OID of the Security Policies and in the URI of the Certification practice statement and in that way a general announcement to the subscribers. These changes relate in particular to:

- Obligations, liabilities, financial responsibility
- Registration
- Personalization
- Internet addresses and contact information
- Key and certificate management
- Directory and revocation service.

If changes to this certification regulation do not relate to any of the abovementioned criteria, they can be introduced without any announcement. This especially applies to changes related to typography and layout as well as to mailing address information or working hours of the offices.

8.2 Process of Publication and Announcement

Current certification practice statement and certificate policy as well as all previous versions can be accessed publicly after a change is introduced.

8.3 Approval and Eligibility of a Certification Regulation

This certification practice statement applies to a.sign SSL products. A-Trust is making sure that this certification regulation complies with the Certificate Policies.

9 Appendix / Referenced Documents

A Appendix

A.1 Abbreviations

CA Certification Authority

CPS Certification Practice Statement

CRL Certificate Revocation List

LDAP Lightweight Directory Access Protocol

OCSP Online Certificate Status Protocol

OID Object Identifier

PIN Personal Identification Number

PKI Public Key Infrastructure

PUK Personal Unblocking Key

RA Registration Authority

RCA Revocation Center Agent

RFC Request for Comments

RO Registration Officer

RSA Encryption Algorithm

SO Security Officer

URI Uniform Resource Identifier

EV-GL Guidelines For The Issuance And Management Of Extended Validation Certificates (recent version: http://www.cabforum.org)

eIDAS EU regulation (https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014)

PSD2 DELEGIERTE VERORDNUNG (EU) 2018/389 DER KOMMISSION vom 27. November 2017

A.2 Referenced documents

References

[RFC3647] RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003

[EV-GL] Guidelines For The Issuance And Management of Extended Validation Certificates 1.6.2, 2017

[eIDAS] EU regulation (https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014)

[AGB] Allgemeine Geschäftsbedingungen (AGB) A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH (A-Trust) für qualifizierte und fortgeschrittene Zertifikate Version 7.3

[PSD2] DELEGIERTE VERORDNUNG (EU) 2018/389 DER KOMMISSION vom 27. November 2017

[ETSI TS 119 495] Electronic Signatures and Infrastructures (ESI)

[ETSI 319 411] Policy and security requirements for Trust Service Providers issuing certificates - ETSI EN 319 411-2 v2.2.2 (April 2018)