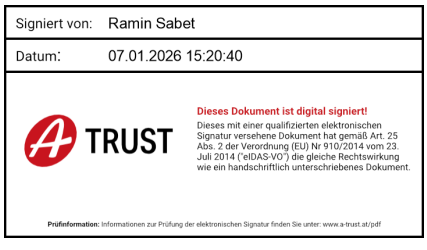
A-Trust GmbH
Landstraßer Hauptstraße 1b E02,
A-1030 Wien
Tel: +43 (1) 713 21 51 - 0
Fax: +43 (1) 713 21 51 - 350
https://www.a-trust.at

A-Trust
Certificate Practice Statement for a.sign Mail certificates



Version: 1.1
Datum: 2025-10-23

Contents

List of Tables

List of Figures

Rev	Date	Author	Changes
1.0	2025-10-06	KS, RS	initial version
1.1	2025-10-23	KS, RS	7.1.6 a.sign Mail CPS object identifier

Table 1: Document History

1 Introduction

1.1 Overview

The target of this CPS is to determine the exact implementation of processes defining the issuing and administration of a.sign Mail (S/MIME) 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.

This document is based on the RFC 3647 (RFC 3647 - Internet X.509 Public Key Infrastructures, Certificate Policy and Certification Practices Framework).

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).

1.2 Document Name and Identification

Policy Name A-Trust Certificate Policy for a.sign Mail (S/MIME) certificates

Version 1.1 / 2025-10-23

Object Identifier 1.2.40.0.17 (A-Trust) .2 (CPS) .27 (a.sign Mail)

1.3 PKI Participants

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.

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 is 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.

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 Mail (S/MIME) certificates is solely performed by A-Trust.

This certification policy especially covers the following aspects:

- The registration authority acts in accordance to the security and certification concept, presented to the regulatory authority.
- The registration authority assures the adherence to the identification and authentication mechanisms described within this policy.
- The registration authority's employees are qualified adequately.
- The registration authority submits the a.sign Mail (S/MIME) 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

1.3.3 Subscribers

Subscribers in this context are considered as individuals, who receive a.sign Mail (S/MIME) certificates from A-Trust, whereas, those who trust/rely on the certificate details are relying parties/users.

1.3.4 Relying parties

Anyone who receives an email signed with an S/MIME certificate is to be considered a relying party.

The user of a.sign Mail (S/MIME) 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).

1.3.5 Other participants

Other participants include the Regulatory Authority.

1.4 Certificate Usage

1.4.1 Appropriate certificate uses

S/MIME certificates are used for encrypting and/or signing email. Furthermore the identity of the individual and/or the organization can be validated.

1.4.2 Prohibited certificate uses

A-Trust strongly discourages uses that exceed the scope of this policy.

1.5 Policy Administration

This document applies to all certificate authorities, as well as the services of these authorities and their subscribers. According to definition, the a.sign Mail (S/MIME) policy

is applicable for a.sign Mail (S/MIME) certificates.
A-Trust acts in accordance to the current versions of the relevant CA/Browser Forum Guidelines, published at http://www.cabforum.org.

1.5.1 Organization Administering the Document

A-Trust is responsible for administering this document. It is located at:

A-Trust GmbH
Landstraße Hauptstraße 1b
1030 Vienna
AUSTRIA
office@a-trust.at

1.5.2 Contact person

Attn: Product Management
A-Trust GmbH
Landstraße Hauptstraße 1b
1030 Vienna
AUSTRIA
office@a-trust.at

1.5.3 Person determining CPS suitability for the policy

Attn: CEOs
A-Trust GmbH
Landstraße Hauptstraße 1b
1030 Vienna
AUSTRIA

1.5.4 CPS approval procedures

The A-Trust CEOs approve every CP and CPS using a qulaified signature. The date of the signature indicates effective date.

1.6 Definitions and Acronyms

CA Certification Authority

CAA Certification Authority Authorization

CPS Certification Practice Statement

CRL Certificate Revocation List

LDAP Lightweight Directory Access Protocol

MPIC Multi-perspective issuance corroboration

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

S/MIME Secure MIME (Multipurpose Internet Mail Extensions, Mailbox Address)

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

WORM Write once read many

2 Publication and Repository Responsibilities

2.1 Repositories

A-Trust publishes its root certificates on its own website. Documentation can be found at www.a-trust.at/docs.

2.2 Publication of certification information

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

- The current CPS for a.sign Mail (S/MIME)
- 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 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.

2.3 Time or Frequency of Publication

CRL updates are published according to 4.9. The CPS are updated upon changes but at least on an annual basis. These are published within five days after approval.

2.4 Access controls on Repositories

Read 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.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of names

All a.sign Mail (S/MIME) certificates are issued with a Subject Distinguished Name that must not be null.

3.1.2 Need for names to be meaningful

The subject of a.sign Mail (S/MIME) end entity certificates is distinct due to the combination of Common Name, Organization, Organizational Unit and other fields.

3.1.3 Anonymity or pseudonymity of subscribers

No stipulation.

3.1.4 Rules for interpreting various name forms

A-Trust complies with the X.500 and ASN.1 standards.

3.1.5 Uniqueness of names

As the email address is included in the S/MIME certificate uniqueness is ensured.

3.1.6 Recognition, authentification, and role of trademarks

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

3.2 Initial identity validation

For S/MIME certificates the following authentication methods apply:

- organization-validated (3.2.2)
- individual-validated (3.2.3)
- mailbox-validated (3.2.3)

3.2.1 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.

3.2.2 Authentication of organisation identity

The authentication of organization identity for S/MIME certificates is carried out according to S/MIME Baseline Requirements [S/MIME Baseline Requirements].

3.2.3 Authentication of individual identity

The individuals, who are audited in the process of issuing a certificate are e-mail domain owner

organization validated:

individual validated:

mailbox validated: It is confirmed that the applicant or applicant organization either controls the email account(s) or has been authorized by the account holders to act on their behalf. Only methods specified in the S/MIME Baseline requirements [S/MIME Baseline Requirements] are used.

3.2.4 Non-verified subscriber information

All subscriber information are verified.

3.2.5 Validation of authority

The authorization of a certificate request is described in 4.1. For S/MIME certificates this is carried out in accordance with section 3 of the S/MIME Baseline Requirements [S/MIME Baseline Requirements].

3.2.6 Criteria for interoperation

No stipulation.

3.3 Identification and Authentification for Re-key Requests

3.3.1 Identification and authentication for routine re-key

Not applicable. Initial validation must be undertaken.

3.3.2 Identification and authentication for re-key after revocation

Not applicable. Initial validation must be undertaken.

3.4 Identification and Authentication for Revocation Requests

The process for revocation is outlined in section 4.9.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

See chapter 3. 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.

4.1.2 Enrollment process and responsibilities

The application is done via the form provided at the A-Trust homepage. The public key as well as a revocation password must be submitted during the application and the General Terms must be agreed to.

Any required documents and confirmations are sent to the registration authority by the subscriber.

In case several applications for a.sign Mail (S/MIME) 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 Certificate Application Processing

4.2.1 Performing identification and authentication functions

A-Trust verifies the information provided in the application in accordance with section 3.2. Any missing, necessary information is requested either from the applicant or obtained from a reliable third-party source. All data is verified. The limits for validity laid out in the [S/MIME Baseline Requirements] apply. No certificate is issued outside these validation limits. As required by [S/MIME Baseline Requirements] 3.2.2.9 CAA records are checked prior to creation of a Certificate Transparency pre-certificate using multiple remote network perspectives.

4.2.2 Approval or rejection of certificate applications

If the application complies with all requirements, a certificate is issued by A-Trust. All applications that cannot be validated are rejected but can re-apply.

4.2.3 Time to process certificate applications

Under regular circumstances certificates are issued within a business week.

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

The officer is authenticated by their officer smart card using an A-Trust software to issue the certificate.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The issued certificate is made available to the applicant via

- E-Mail

- the A-Trust Website

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

After installation or initial use.

4.4.2 Publication of the certificate by the CA

All certificates are published in the repositories unless subscribers requests otherwise.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

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

- The subscriber is obliged to protect their 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. The certificate policy and the certification practice statement, valid at the issuance of the certificate, are applicable.
- The subscriber is obliged to adhere to the national export restrictions as well as the national use restrictions, when using the private key abroad.

4.5.2 Relying party public key and certificate usage

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

4.6 Certificate Renewal

4.6.1 Circumstance for certificate renewal

Not applicable. Initial validation must be undertaken.

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing certificate renewal requests

No stipulation.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate Re-key

4.7.1 Circumstance for certificate re-key

Not applicable. Initial validation must be undertaken.

4.7.2 Who may request certification of a new public key

No stipulation.

4.7.3 Processing certificate re-keying requests

No stipulation.

4.7.4 Notification of new certificate issuance to subscriber

No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

No stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate Modification

4.8.1 Circumstance for certificate modification

Not applicable. Initial validation must be undertaken.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate Revocation and Suspension

For all types of a.sign Mail (S/MIME) certificates an immediate and permanent revocation of the certificate is possible.

4.9.1 Circumstances for revocation

The revocation of a certificate is necessary:

- upon request of the subscriber,
- if essential information of the certificate are no longer correct,
- if the private a.sign Mail (S/MIME) certificate key cannot be used anymore (e.g. defect storage and no backup is available),
- if suspicion of compromise exists (e.g. unauthorized access to the computer where the private key is stored), respectively a compromise occurred,
- if the certificate authority becomes aware of a relevant breach of this policy or the general terms and conditions by the subscriber,
- if the contractual relationship ends,
- if the used algorithms are no longer sufficient to match the security expectations,
- if the certificate authority goes out of business.

4.9.2 Who can request revocation

A revocation of the certificate can be requested by:

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

4.9.3 Procedure for revocation request

The revocation of an a.sign Mail (S/MIME) certificates is carried out 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.

The procedure entails the following requirements:

- The revocation password has to be submitted in order to revoke the certificate.
- Optional: The reason for the revocation (e.g. compromise of the private key, termination of contract) can be stated to the revocation service.

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

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

4.9.4 Revocation request grace period

Subscribers should immediately request revocation but are required within one day after a loss of the private key.

4.9.5 Time within which CA must process the revocation request

A-Trust adheres to the Austrian signature law, specifying the update frequency of the revocation service after requesting the 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).

4.9.6 Revocation checking requirement for relying parties

Prior to relying on a certificate, relying parties must validate the suitability of the certificate for 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).

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 date of the requested status information.

4.9.7 CRL issuance frequency

CRLs are regularly updated as stated in the nextUpdate field in the current CRL. The update frequency of the revocation list is at least once every six hours. These frequencies are identical for CA and subscriber certificate revocation lists.

4.9.8 Maximum latency for CRLs

A-Trust takes all measures to minimize the latency of CRL updates. Regularly, the publication of a CRL happens before the previous CRL expires.

4.9.9 On-line revocation/status checking availability

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

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.

4.9.10 On-line revocation checking requirements

Relying Parties must confirm revocation information. 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.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re key compromise

No stipulation.

4.9.13 Circumstances for suspension

a.sign Mail (S/MIME) certificates can only be revoked, suspension is not available.

4.9.14 Who can request suspension

No stipulation.

4.9.15 Procedure for suspension request

No stipulation.

4.9.16 Limits on suspension period

No stipulation.

4.10 Certificate Status Services

4.10.1 Operational characteristics

Certificate status information can be obtained via CRL and OCSP. Expired certificates remain on the CRL, by the extension ExpiredCertsOnCRL.

CRLs are archived for thirty years after expiration.

4.10.2 Service availability

Certificate status services via CRL and OCSP are available 24x7.

4.10.3 Optional features

No stipulation.

4.11 End of Subscription

The subscription ends if the certificate expires or is revoked.

4.12 Key Escrow and Recovery

4.12.1 Key escrow and recovery policy and practices

Key Escrow is not offered for a.sign Mail (S/MIME) end user certificates. CA private keys are never escrowed.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 Management, Operational, and Physical Controls

5.1 Physical Security Controls

5.1.1 Site location and construction

A-Trust registration and revocation personnel is located at the head offices at:

- Landstrasser Haupstrasse 1b, A-1030 Wien

Furthermore, the CA services are situated in the high security data center.

5.1.2 Physical Access

Access to all technical components in the data center is only possible through the A-Trust authorization system. Unauthorized access is restricted according to physical access.

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 data 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.

Registration offices, being located at the A-Trust headquarter, are secured through access control systems for A-Trust employees as well as an alarm system.

5.1.3 Power and air conditioning

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 exposures

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

5.1.5 Fire prevention and protection

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

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

5.1.6 Media storage

Data media with sensitive or 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 documents are destroyed using shredders and transferred to a specialized company for a proper disposal afterwards.

5.1.8 Off-site backup

All services in the data 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 Procedural Controls

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

5.2.1 Trusted roles

Security Officer is responsible for administrating the CA. They are authenticated by personal smartcard

Registration Officer is responsible for validating the application, certificate issuance, and revocation services. They are authenticated by a personal smartcard.

System Administrator is responsible for maintaining and configuring the hardware and software in the data center as well as the headquarters.

Internal Auditor is responsible for performing internal checks to ensure the compliance with policies.

5.2.2 Number of persons required per task

All tasks performed in the data center require two Security officers. Application processing is carried out by one registration officer. Verification and issuance of the certificate requires two registration officers.

5.2.3 Identification and authentication for each role

Identification and authentification is performed through usage of a personal smartcard.

5.2.4 Roles requiring separation of duties

Internal Auditors must not assume any other role.

5.3 Personnel Controls

5.3.1 Qualifications, experience, and clearance requirements

Personell employed by A-Trust fulfill all requirements regarding reliability, integrity, and technical qualifications in the following sectors according to their roles:

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

5.3.2 Background check procedures

Employees hired to conduct security relevant tasks have to provide certificate of good 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 requirements

Training concerning security and functional issues are held by capable staff and conducted regularly. The roles of security relevant personell and administrator require specific training and can only be assigned after completion.

5.3.4 Retraining frequency and requirements

Trainings are conducted for new employees as well as for all employees on a regular basis and after relevant changes in the internal system or after major developments occur in the market.

5.3.5 Job Rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

Employees are bound to confidentiality through their work contract. Violations of security measures are handled through disciplinary measures up to termination.

5.3.7 Independent contractor requirements

Independent contractors are assigned the same roles as stated in section 5.2.1.

5.3.8 Documents supplied to personnel

Employees have access to the following documents:

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

5.4 Audit Logging Procedures

5.4.1 Types of events recorded

- Changes in the role assignment
- Changes in the software configuration (Updates or new software)
- Firewall and router configuration changes
- System crashes
- Changes in certificate profiles
- Physical access to data center

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

- Each successful and unsuccesful login attempt
- Certifcate requests
- Key generation
- Issuing of certificates
- Publishing of CRLs and certificates
- Revocation requests
- Performed revocations
- Key changes
- Verification and rejection of certificate applications

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

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

5.4.2 Frequency of processing log

The eventlog is checked for suspicious occurrences on a bimonthly basis, live monitoring alerts employees in case of critical events.

5.4.3 Retention period for audit log

Logs relveant to the lifecycle of the certificates are retained for thrity years after expiration. Logs that are needed to allow A-Trust to make detailed statements regarding the validity of single certificates are archived. This includes information on the issuing of the certificate and CRLs.

5.4.4 Protection of audit log

Logs are created and stored in different locations and are only accessible to authorized employees. Relevant archived log files are signed to prevent modification and stored on a WORM storage.

5.4.5 Audit log backup procedures

A-Trust creates incremental backups of audit logs on an hourly and full backups on a daily basis. Backups are transferred to another data center.

5.4.6 Audit collection system (internal vs. external)

All security relevant systems create logs on the local system. In case logs can not be created, the system will shut down.

5.4.7 Notification to event-causing subject

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

5.4.8 Vulnerability assessments

A-Trust carries out external and internal PEN testing on a yearly basis. Risk assessment is performed twice a year. Policies are assessed and updated at least yearly.

5.5 Records Archival

5.5.1 Types of records archived

Following data is archived:

- Data of the subscriber that has been used for the verification of the certificate request
- Certification application and accepted validation
- All certificates issued by the certification authority (certificates of the certification authority and certificates of certificate holder)
- Cancellation and revocation 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
- CP and CPS versions
- Terms and conditions versions of services by the CA
- Acceptance of A-Trust Terms and Conditions
- Changes of roles

5.5.2 Retention period for archive

Retention period is at least 7 years. Provisions from [S/MIME Baseline Requirements] are relevant for a.sign Mail certificates.

5.5.3 Protection of archive

The A-Trust archive is located in a safe location. Access is permitted only to authorized personnel. Electronic documents are protected from modifications through digital signatures of the archived data. Archives are only released on a legal basis.

5.5.4 Archive backup procedures

Security relevant data are stored in two different data centers on a WORM. Other data is backuped on a daily basis and transferred to an off-site location once a year.

5.5.5 Requirements for time-stamping of records

All certification requests must be time-stamped with system time. The system time is synchonized with at least two different recognized time servers (see section 6.8)

5.5.6 Archive collection system (internal or external)

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

5.5.7 Procedures to obtain and verify archive information

As the security relevant archive is stored on a WORM and digitally signed, retrieving data from this source, guarantees integrity and authenticity of the archived data.

5.6 Key Changeover

A key changeover 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 length 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.

A-Trust 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 and A-Trust website. The validity of the CA certificate can be compared to a provided fingerprint.

With a key changeover, the old key loses its active validity and the private key is no longer used for signing. Only the new key is used to sign certificates and CRL. 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.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and compromise handling procedures

Internal documentation and guidelines describe the procedure and recipients of information in case of incidents and compromises. These documents are reviewed and updated at least on a yearly basis.

5.7.2 Computing resources, software, and/or data are corrupted

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

In case of certificates, the signatories affected 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.

All other systems are redundant and therefore not affected.

5.7.3 Entity private key compromise procedures

The crisis response team will assess the situation and determine an appropriate action plan. If necessary all affected subscriber certificates are revoked. If necessary, government agencies are informed. Affected parties are informed about the compromise.

5.7.4 Business continuity capabilities after a disaster

As approved by the conformity assessment body, a method to transfer all private CA keys in an encrypted form to another HSM on a different location is in use. Hence the private key never exists in plain form.

All other relevant data is also transferred to the other data center in order to ensure continuity in case of disaster.

5.8 CA or RA Termination

A-Trust is entitled to transfer rights and obligations from the existing contract to a third party. Subscribers are informed. 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. Access to archived records is guaranteed even in case the CA ceases its activities.

A cessation of the CA's 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.

RA termination is not applicable.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Key of the Approved Certification Authority The key of the Certification authority for signature of the a.sign Mail (S/MIME) certificates is generated in a Hardware Security Module (meets and exceeds FIPS 140-2 Level 2) of the Certification authority. CA keys are generated using a hardware random number generator according to guidelines of the HSM.

For the private key of the Certification authority see section 5.7.4.

Key of the Subscriber The subscriber keys are generated by the applicant using software or hardware tools. 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 Private key delivery 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 Public key delivery to certificate issuer

No stipulation.

6.1.4 CA public key delivery to relying parties

All CA certificates are published in an LDAP directory on the Internet as well as the A-Trust website so that access remains public and all certificate users can acquire certificates.

6.1.5 Key sizes

The key length of root and all intermediate CAs is at least 4096 Bit (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.

6.1.6 Public key parameters generation and quality checking

CA keys are generated in an HSM (see section 6.1.1) using the onboard random number generator. 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 Key usage purposes (as per 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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

Subscriber private keys are generated and secured by the subscriber.

For CA key generation see section 6.1.1.

6.2.2 Private key (n out of m) multi-person control

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

6.2.3 Private key escrow

Key escrow is not possible for root, intermediate or subscriber private keys.

6.2.4 Private key backup

See section 5.7.4.

6.2.5 Private key archival

Private keys of root and intermediate CAs are not archived.

6.2.6 Private key transfer into or from a 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 generate redundancy (see 5.7.4).

6.2.7 Private key storage on cryptographic module

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. All these keys are generated and stored in an HSM (see 6.1.1).

6.2.8 Method of activating private key

CA private keys are activated according to the specifications of the HSM manufacturer. Subscriber are responsible for their private keys.

6.2.9 Method of deactivating private key

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

6.2.10 Method of destroying private key

Private CA keys that are not in use anymore are destroyed using the apporpriate function of the Hardware Security Module.

The subsciber is responsible for the deletion of subscriber keys.

6.2.11 Cryptographic Module Rating

See section 6.1.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

See chapter 2.1

6.3.2 Certificate operational periods and key pair usage periods

The Shell Model is used for a.sign Mail (S/MIME). The Intermediate CA has to be valid at the point of time, the subscriber certificate has been signed.

Maximum validity periods of certificates:

- Root CA: 20 years
- Intermediate CA: 20 years
- Subscriber (S/MIME): 820 days

6.4 Activation Data

6.4.1 Activation data generation and installation

Keys of the Root-CA and Certification Authorities for a.sign Mail (S/MIME) certificates can only be activated obeying the "four-eye" principle of two Security Officers using smartcards and PIN. Activation data are directly created in a Hardware Security module of the CA-System (see 6.1.1). Created activation data are not recorded.

Subscriber activation data is solely generated by the subscriber and not sent to A-Trust.

6.4.2 Activation data protection

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 (smartcard). There is a sufficient number of smartcards so that, in case of damaged or missing smartcards, the keys of the Certification Authority are not endangered.

Activation data for the keys of subscribers Subscribers 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.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

A-Trust encrypts all communication between its CA, involved clients, and systems. All hardware is protected according to industry best practices, including user authentification, virus protection, local firewall, and regular security updates.

All access to client software used for certificate issuance is restricted through multi-factor authentication via smartcard.

Physical access control to the data center where all the front facing servers are located, is described in section 5.1.2.

6.5.2 Computer security rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

System development is solely performed in-house and using secure coding guidelines, based on best practice industry standards. Before deploying the system in the data center, rigorous testing is performed on the test system.

6.6.2 Security management controls

Security management controls are aligned with the security regulations of A-Trust. In line but not limited to the security management regulations, deployment of updates to the CA systems can only be performed by two Security officers.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network Security Controls

Adhering to the insustry standards, transfer of the critical data is conducted through appropriately autheticated and encrypted communication channels.

All systems are located in a private network and can only connect to the Internet via a firewall. Furthermore, all HSMs containing the private keys are located in a separate network and are only accessible via firewall.

The firewalls are configured using a deny all policy, thus only needed ports are opened.

6.8 Time-stamping

Time-stamping is used to indicate the accurate time in certificates, revocation lists, and log files.

Server time is updated at least once an hour using the Network Time Protocol, using trusted time servers, including the official time provided by the Austrian Federal Office of Metrology and Surveying.

7 Certificate, CRL, and OCSP Profiles

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

7.1 Certificate Profile

Non-sequential certificate serial numbers, having at least 64 bit entropy.

7.1.1 Version number(s)

v3(2): Version number '2' denotes an X.509, Version 3 certifcate

7.1.2 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
extkeyUsage	no	yes		X
Private Extensions				
authorityInfoAccess	no	yes		X

Table 2: Extensions (CA certificates)

The subordinate CA is using id-kp-serverAuth and id-kp-clientAuth as extkeyUsage.

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			
authorityInformationAccess	yes		X
smimeCapabilities	optional		X

Table 3: Extensions (a.sign Mail (S/MIME) certificates)

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

7.1.3 Algorithm object identifiers

CA certificates $\geq$ SHA-256RSA: Algorithm used to sign the certifcate

Subscriber certificates $\geq$ SHA-256RSA: Algorithm used to sign the certifcate

SHA-256 OID: 1.2.840.113549.1.1.10

7.1.4 Name forms

For CA Root certificates:

- CN = A-Trust-Root-SMIME-nn
- OU = A-Trust-Root-SMIME-nn
- O = A-Trust GmbH
- C = AT

For CA Intermediate certificates:

- CN = a-sign-Mail-nn

- OU = a-sign-Mail-nn
- O = A-Trust GmbH
- C = AT

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate policy object identifier

The extension certificatePolicies in the certificate is encoded as follows:

- OID 1.2.40.0.17.2.27
  1.2.40.0.17 (A-Trust).2 (CPS).27 (a.sign Mail)
- 2.23.140.1.2.1 (domain-validated) or
- 2.23.140.1.2.2 (organization-validated) or
- 2.23.140.1.2.3 (individual-validated) or
- 2.23.140.1.1 (extended-validation)

Based on [S/MIME Baseline Requirements]:

- Mailbox-validated Multipurpose 2.23.140.1.5.1.2
- Mailbox-validated Strict 2.23.140.1.5.1.3
- Organization-validated Multipurpose 2.23.140.1.5.2.2
- Organization-validated Strict 2.23.140.1.5.2.3
- Sponsor-validated Multipurpose 2.23.140.1.5.3.2
- Sponsor-validated Strict 2.23.140.1.5.3.3
- Individual-validated Multipurpose 2.23.140.1.5.4.2
- Individual-validated Strict 2.23.140.1.5.4.3

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL Profile

7.2.1 Version number(s)

v2(1): Version number '1' denotes an X.509, Version 2 revocation list

CRLs are signed using the algorithm SHA-256 (1.2.840.113549.1.1.10).

7.2.2 CRL and CRL Entry Extensions

The non critical extensions authorityKeyIdentifier and 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.

A-Trust specifies the following reason codes:

- unspecified (0),
- keyCompromise (1),
- cACompromise (2),
- affiliationChanged (3),
- superseded (4),
- cessationOfOperation (5),
- certificateHold (6),
- removeFromCRL (8).

7.3 OCSP Profile

7.3.1 Version number(s)

OCSP responders conform to version 1 of RFC 6960 [RFC6960].

7.3.2 OCSP extensions

No stipulation.

8 Compliance and Other Assessment

8.1 Frequency or circumstances of assessment

External audits are performed at least annually by an independant auditor.

8.2 Identity/qualifications of assessor

Webtrust auditors must meet the requirements of section 8.2 of the CA/Browser Baseline Requirements [S/MIME Baseline Requirements] and section 3.1 of the Mozilla Root Store Policy [Mozilla Root Store Policy] where applicable.

8.3 Assessor's relationship to assessed entity

The conformity assessment entity is independent from A-Trust in any way, including but not limited to financial or business relations.

8.4 Topics covered by assessment

The auditor reviews the compliance of A-Trust with the underlying CPS. Internal audits also cover confidential documents like internal risk and security policies. The auditor confirms the proper adherence to those principles.

The audits are performed according to the following scheme: ETSI EN 319 411-1 v1.2.2 [ETSI 319 411].

Internal audits cover random samples of at least three percent of all certificates issued since the last audit. They are reviewed with a focus on the integrity of the process. This audit is documented. a.sign Mail (S/MIME) certificates are monitored quarterly.

8.5 Actions taken as a result of deficiency

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

- The reported discrepancy is analyzed

- A plan to rectify the discrepancy is drafted
- The plan is double-checked with the auditor
- and followed step by step, which may include:
  - Contacting the affected parties
  - Revocation of the affected certificate

8.6 Communication of results

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

Audit Attestation Letters are uploaded to the relevant websites or sent directly to the relevant entities [CA/Browser Baseline Requirements] [Mozilla Root Store Policy].

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

Charges are due when a certificate is issued or renewed. Said charges are subject to change under the applicable customer agreement.

9.1.2 Certificate access fees

A-Trust may charge for access to its certificate databases.

9.1.3 Revocation or status information access fees

A-Trust will not charge for checking the validity status of an issued Certificate using a CRL. A-Trust may charge for services related to customization of CRLs and/or OCSP services. Third parties that provide products or services related to certificate status information are not permitted to access revocation information, certificate status information or time stamping without the explicit consent of A-Trust.

9.1.4 Fees for other services

Accessing this A-Trust CPS is free. Any other use of this CPS must be coordinated with A-Trust.

9.1.5 Refund policy

Customer aknowledges that refunds are not provided for.

9.2 Financial Responsibility

9.2.1 Insurance coverage

A-Trust holds an IT liability insurance with a coverage of 5 million euros.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

A-Trust provides warranty to subscribers according to Austrian law.

9.3 Confidentiality of Business Information

9.3.1 Scope of confidential information

Private keys and activation data shall be treated as confidential.

9.3.2 Information not within the scope of confidential information

Any information that is not marked as confidential is regarded as public knowledge. Public information includes information about issued certificates and their revocation.

9.3.3 Responsibility to protect confidential information

Contractually, employees, agents, and contractors of A-Trust are obligated to safeguard confidential information. Employees are trained in information security.

9.4 Privacy of Personal Information

9.4.1 Privacy plan

Personal information is only disclosed when required by law or when requested by the subject of the personal information.

9.4.2 Information treated as private

A-Trust considers all personal information about a person in a Certificate or CRL that is not made public as private. A-Trust uses appropriate information security measures to safeguard private information.

9.4.3 Information not deemed private

Private information does not include Certificates, CRLs, or their contents subject to Austrian ond/or European Law.

9.4.4 Responsibility to protect private information

Data protection laws in Europe mandate that A-Trust contractors and employees handle personal information highly confidential. All relevant data is stored safely and shielded from accidental disclosure.

9.4.5 Notice and consent to use private information

If the information is not included in a Certificate, personal information obtained from an applicant during the application or identity verification process is considered private information. Any personal information contained in a Certificate may be globally transferred and published only with the consent of all Subscribers. A-Trust will only make use of private information with the persons permission or as required by law or regulation.

9.4.6 Disclosure pursuant to judicial or administrative process

If A-Trust believes that disclosure is required by law or regulation, it may do so without prior notice.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual Property Rights

The intellectual property rights to A-Trust's services are owned by A-Trust. Customers shall grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, insofar it is necessary for the provision of the services in question. A-Trust and customers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable CRL usage agreement, Relying Party Agreement, or any other applicable agreements. Any trademark, service mark, or trade name on any Certificate, as well as any distinguished name on any Certificate issued to a Subscriber or an Applicant, remain the property of those parties.

9.6 Representations and Warranties

9.6.1 CA representations and warranties

A-Trust does not make any claims about its products or services unless specifically stated in this CPS or in a separate agreement with a Subscriber. To the extent specified in this CPS, A-Trust represents that it will regularly publish and update CRLs and OCSP responses and maintain a repository of public information on its website. Furthermore, A-Trust assures that it will comply with present CPS and all applicable laws and regulations in any material aspects as well as that all Certificates issued under this CPS will meet the minimum requirements outlined in this section and in the baseline requirements. A-Trust can not be held responsible for quality of any software and/or hardware device. Neither does A-Trust stand for the validity of any unverified information (name verification for certificates included) nor is A-Trust responsible for failing to comply with the present CPS due to circumstances accredited to acts of Force Majeur. Finally, A-Trust can not be held resposible for information contained in a Certificate, except as stated in this CPS.

9.6.2 RA representations and warranties

RAs are to make sure that information given to A-Trust by the RA is neither false nor misleading and that all translations performed by the RA are accurate in perspective to the original information. Furthermore, RAs stand for that the present CPS is met by each certificate the RA requests as well as that the certificate management and issuance services provided by the RA cohere with this CPS.

9.6.3 Subscriber representations and warranties

Regardless of whether the use of the subscriber's Private Key was authorized, subscribers are exclusively responsible for any false statements they make to third parties prior to receiving a Certificate. Should a change occur that could affect the status of the

certificate, the subscriber must inform A-Trust. The applicant is required by A-Trust to fulfill the promises and warranties outlined in this section for the benefit of A-Trust and the certificate beneficiaries as part of the subscriber agreement. Before issuing a certificate, the subscriber has to either accept the subscriber agreement or the terms of use stipulated by A-Trust. Subscribers may only use S/MIME certificates for email addresses for which the certificate was issued. If Subscribers become aware of or suspect any compromise of the security of the private key associated with the public key of the relevant certificate, they must immediately request revocation of the Certificate, suspend the use of the certificate and any associated private keys. The certificate must also be revoked if the information contained in the certificate is false or unclear; before using the certificate, subscribers must verify that the data contained in the certificate is correct. Upon expiry of the certificate and the associated private key, use must be discontinued immediately. The certificate may only be used for authorised and legal means in compliance with this CPS. When communicating with A-Trust, the subscriber agrees to provide complete, truthful and accurate information. Additional representations and warranties may be incorporated in subscriber agreements.

9.6.4 Relying party representations and warranties

Relying parties shall ascertain that they are familiar with the use of digital certificates and the PKI. They have understood the provisions set out in this CPS and the applicable restrictions associated with the use of certificates as well as the liability restrictions of A-Trust related to the use of certificates. The relying parties have verified the A-Trust certificate and the certificates in the certificate chain through the corresponding CRL or OCSP. They are aware that the use of a digital signature can be associated with risks and take all measures to prevent these risks. Any unauthorised reliance on a certificate is at their sole risk. Agreements with contractors may contain additional representations and warranties.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of Warranties

Except as stated above, certificates, software and services are provided "as they are" and only "as available". A-trust does not warrant that any service or product will meet any expectations or that access to certificates will be timely or error-free. A-Trust does not guarantee the availability of Certificates, Software ans Services and may modify or discontinue any certificate, software or service offering at any time.

9.8 Limitations of Liability

Nothing in this disclaimer limits liabilty related to death or personal injury resulting from A-Trust's negligence or fraud committed by A-Trust officers. Except as stated above, any entity using an A-Trust certificate, software or service waives all liability of A-Trust related to such use, provided that A-Trust has materially complied with this CPS in providing the certificate, software or service. A-Trust's liability for certificates, software and services that do not materially comply with this CPS is limited with € 5.000,- per claim. Liability does not extend to indirect or consequential damages or loss of opportunity. A-Trust is not liable for any damages due to intentional misconduct or fraud by the applicant, nor for damages related to use of certificates that is not in accordance with this CPS. The limitations in this section apply to the maximum extent permitted by law. The disclaimers and limitations on liabilities in this CPS are fundamental terms to the use of A-Trust's Certificates, Software and services.

9.9 Indemnities

Generally, A-Trust indemnifies providers of application software against damages of any kind arising in connection with an EV certificate issued by A-Trust. Excluded from this are cases in which the provider's software has presented a trustworthy certificate as untrustworthy and damage has occurred directly as a result or if the provider's software has presented a certificate as trustworthy that had actually expired or been revoked. Subscribers shall hold A-Trust, its employees and affiliates harmless from and against any and all claims based on misrepresentation or concealment of material facts, breach of contract or failure to comply with applicable laws or the provisions set forth in this CPS, or misuse of the Certificate or Private Key by Subscribers.Relying parties shall hold A-Trust, ist employees and affiliates harmless from claims based on the breach of the relying party agreement, this CPS, applicable law or an end user license agreement. Furthermore A-Trust shall be indemnified of damages due to unreasonable reliance on a certificate or failure to check the certificats status prior to use.

9.10 Term and Termination

9.10.1 Term

This CPS is effective when distributed to A-Trust's online repository. This shall also apply to updates of this CPS.

9.10.2 Termination

This CPSwill stay in force until a newer version replaces it.

9.10.3 Effect of termination and survival

A-Trust will communicate the result of this CPS's termination in the A-Trust Repository. The responsibilities related to protecting confidential information will survive termination in any case. All customer agreements remain effective until the certificate is revoked or expired, even if this CPS is terminated.

9.11 Individual notices and communications with participants

A-Trust will accept notices related to this CPS at its head office.

9.12 Amendments

9.12.1 Procedure for amendment

This CPS is reviewed once a year. Amendments are made effective by publishing the latest version to the online repository. Updates supersede any designated or conflicting provisions of the referenced version of the CPS.

9.12.2 Notification mechanism and period

Revisions of this CPS will be published on the A-Trust Website.

9.12.3 Circumstances under which OID must be changed

A-Trust is solely responsible for deciding if an amendment to this CPS shall effect an OID change.

9.13 Dispute Resolution Procedures

Disputes shall be settled by the ordinary courts of the Republic of Austria.

9.14 Governing Law

Austrian law shall apply exclusively. The application of the UN Convention on Contracts for the International Sale of Goods is explicitly excluded.

9.15 Compliance with Applicable Law

This CPS is subject to the laws of the Republic of Austria.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement

A-Trust is obligated to comply with this CPS and applicable industry guidelines. A-Trust requires each party using its products and services to enter into an agreement before the beginning of use. If an agreement differs from this CPS, the agreement with the respective party shall apply primarily without prejudice to third parties.

9.16.2 Assignment

Companies operating under this CPS may not assign their rights and obligations without the prior written consent of A-Trust.

9.16.3 Severability

If any provision of these CPS becomes invalid, the other provisions shall not be affected.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

If A-Trust waives enforcement of any right arising under this CPS, this will not result in a general waiver of enforcement of that or any other right arising under this CPS. To be effective, waivers must be in writing and signed by A-Trust. If A-Trust incurs damages, expenses or losses due to the conduct of a party, it may claim compensation from that party as well as any legal fees.

9.16.5 Force Majeure

If the non-fulfilment or delay in the fulfilment of an obligation set out in this CPS is due to an event outside the control of A-Trust, A-Trust shall not be liable for it. Such events include, but are not limited to, natural disasters, war, strikes, and the like.

9.17 Other Provisions

No stipulation.

A Appendix

A.1 Referenced documents

References

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

[RFC6960] RFC 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

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

[AGB] Allgemeine Geschäftsbedingungen (AGB) A-Trust GmbH (A-Trust) für qualifizierte und fortgeschrittene Zertifikate Version 7.6

[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)

[Mozilla Root Store Policy] Mozilla Root Store Policy - v2.8 (June 2022)

[CA/Browser Baseline Requirements] Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates - v1.8.4 (April 2022)

[S/MIME Baseline Requirements] Baseline Requirements for the Issuance and Management of Publicl - Trusted S/MIME Certificates - v1.0.8 (December 2024)