A-Trust Gesellschaft für Sicherheitssysteme
im elektronischen Datenverkehr GmbH
Landstraßer Hauptstraße 5
Tel: +43 (1) 713 21 51 - 0
Fax: +43 (1) 713 21 51 - 350
https://www.a-trust.at

a.trust
Certification Practice Statement for simple certificates
a.sign corporate

Version: 1.0.9
Datum: 21.05.2008

Contents

List of Tables

List of Figures

1 Introduction

1.1 Overview

The aim of this A-Trust Certification Practice Statement is to define the issuance, administration and application of a.sign corporate certificates in order to ensure a secure and reliable execution of the offered certification services and application of the issued certificates.

A Certification Practice Statement provides information on the methods of a certification authority concerning the issuance of a.sign corporate certificates. Its purpose is to internally define the methods and to explain the proceeding of the certification authority to the users. Thus the user is informed about the existing security standards.

This document is structured according to the international standard for Certification Practice Statements (RFC 2527 - Internet X.509 Public Key Infrastructures, Certificate Policy and Certification Practices Framework) of the Internet Society.

1.2 Document Identification

Name of the CPS:	a.trust Certification Practice Statement for simple certificates a.sign corporate
Version:	1.0.9 / 21.05.2008
Object Identifier:	1.2.040.0.17 (a.trust) .2 (CPS) .7 (a.sign corporate) .1.0.9 (version)

1.3 Certification Infrastructure and Applicability

1.3.1 Certification Authorities

There is a central certification authority, which signs the keys of the server certificate holders as well as the revocation lists for those certificates.

1.3.2 Registration Authorities

At the registration authorities registration officers are carrying out user-related tasks. Besides identification these tasks comprise the processing of user data and the transmission of information to the superior certification authority.

1.3.3 Revocation Service

The user may contact the revocation service by phone or fax in order to arrange a suspension of the certificate, to reinstate a certificate or to revoke his certificate (for more details see **??**).

1.3.4 Users

'Users' are on the one hand persons obtaining a a.sign corporate certificate (signatories) and on the other hand persons using a.sign corporate certificates or trusting in the information contained in the certificate.

1.3.5 Applicability

This document is relevant to the certification authority and the affiliated registration authorities as well as to services of the certification and registration authorities and to the users.

The following user certificates are subject to this Certification Practice Statement: a.sign corporate certificates, which are stored on the computer and used for

- signature applications of signature servers or
- secrecy applications of signature servers.

The a.sign corporate certificates are divided into the following three classes depending upon kind and security of its generation and storage of keys:

- a.sign corporate light:
  The certificate applicantsâ keys are generated in a secure way. The keys do not have to be generated and stored in special hardware, however, the production must follow procedures that ensures sufficient quality of the key material.
- a.sign corporate medium:
  The signatoryâs key must be generated in a secure way in dedicated hardware, e.g. in a smart card or in a hardware security module. The hardware unit must be described in the submitted certificate application. The signatory commits itself to use no other hardware for the generation and storage of the keys than communicated to the registration authority.
- a.sign corporate strong:
  The signatoryâs keys are genereted in a secure way in a hardware security module which is certified according to ITSEC E3 or to at least an equivalent criteria. The possession of the hardware security module must be proven to a.trust in the

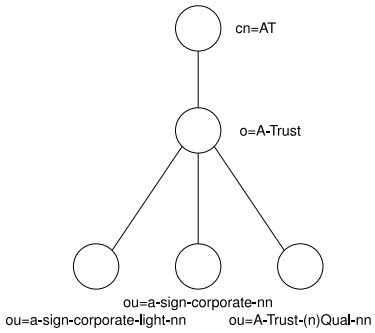

Figure 1: a.trust directory tree

certificate order by presenting contracts or proof-of-possession calculations. The certification documents must be submitted to the registration authority, and the signatory must on A-Trustâs demands allow a local inspection of the use hardware security module.

All certificate classes are also intended for creation of signatures according to the regulations of § 2 Z 3 [SigG]. The signatory is identified during the registration and can bei either a natural person or a legal body.

1.3.6 a.trust Directory Tree

A schematic drawing of the a.trust directory tree can be foun in Picture 1. The certificate of the A-Trust-nQual-nn key is the root certificate of AâTrust for non qualified certificates, -nn specifying the version of the A-Trust Root-CA, which generates digital signatures with the matching secret key.

All CA certificates for a.sign corporate and the appropriate CRLs are signed with A-Trust-nQual-nn. Exception: for certificates, which were issued by CA version 02, root CA A-Trust-Qual-02 is used instead.

Depending on the type of certificate, the certificates of certificate holders of a.sign corporate certificates and the appropriate CRLs are signed with the CA keys

- a-sign-corporate-nn, a.sign corporate medium and strong certificates of CA version 03

- a-sign-corporate-light-nn, a.sign corporate light certificates
- a-sign-corporate-strong-nn, a.sign corporate strong certificates of CA version 02
- a-sign-corporate-medium-nn, a.sign corporate medium certificates of CA version 02

-nn specifying the version of the AâTrust certification authority, which generates digital signatures with the matching secret key.

1.3.7 Certification Hierarchy

In Picture 2 you find a schematic drawing of the certificate hierarchy.

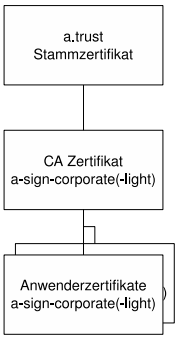

Figure 2: Certification Hierarchy

1.4 Contacts

1.4.1 Administration of this Document

a.trust is responsible for the organization and administration of the Certification Practice Statement.

1.4.2 Contact Information

Contact information on a.sign corporate certificates by A-Trust is available as follows:

- on the a.trust webpage:
  https://www.a-trust.at/
- at the call center:
  the telephone number and accessibility can be found on a.trustâs homepage.
- at selected a.trust registration authority and
- upon written request.

1.4.3 Responsibility for the Acceptance of other Policies

a.trust decides on the acceptance of other policies.

2 General Provisions

2.1 Obligations

2.1.1 Obligations of the Certification Authorities

The certification authority of a.trust follows the regulations of this Certification Practice Statement, which includes in particular the following aspects:

- The certificates for certificate holders are generated in accordance with this Certification Practice Statement and may be suspended, revoked or renewed (i.e. extended validity period).
- The certification authority acts in accordance with the security and certification concept submitted to the supervisory authority.
- The certification authority employs only qualified personnel.
- The certification authority fulfills its obligation to provide information regarding signatories and supervisory authority.
- The certification authority takes appropriate measures (technical, organizational, infrastructural and concerning the personnel) in order to protect the private key of the certification authority.
- The private key of the certification authority is exclusively used for signing the certificates of the signatories and for signing the revocation lists.
  Please note: There are also private A-Trust keys for other purposes. This Practice Statement only deals with the private keys for the issuance of certificates and revocation lists.
- The certification authority publishes all issued certificates as well as all revoked certificates certificates.

2.1.2 Obligations of the Registration Authorities

The a.trust registration authorities follow the regulations of this Certification Practice Statement, including in particular the following aspects:

- The registration authorities act in accordance with the security and certification concept submitted to the supervisory authority.
- The registration authorities guarantee the compliance with the identification and authentication mechanisms described in this Certification Practice Statement.

- The certification authorities employ only qualified personnel.
- The registration authorities transmit the a.sign corporate certificates in electronic form to the signatory. a.trust places in particular the following documents electronically at the disposal of the signatory:
  - terms of contract,
  - terms of payment and
  - Certificate Policy, Certification Practice Statement.

2.1.3 Subscriber Obligations

The signatories have to observe the regulations stipulated in this document. This applies in particular to the following:

- The signatories commit themselves to accepting the general terms and conditions which are applicable in each case with the Certificate Policy for a.sign corporate light, a.sign corporate medium or a.sign corporate strong, this Certification Practice Statement and the terms of payment of a.trust as a basis for the concluded contract.
- In the case of a.sign corporate medium and a.sign corporate strong certificates the signatory is obliged to use only the hardware, which was communicated to a.trust when the application was filed and/or the use was proven, for generation and storage of the private key. If the signatory intends to make relevant changes, he must inform a.trust immediately.
- The signatory is responsible for the correctness of the information provided for registration and cooperates in the identification and authentication procedures as defined in this Certification Practice Statement.
- The signatory has to protect his private key. In particular, he is obliged to prevent the access of unauthorized persons to his private key, be it stored in a coded storage and to keep the activation data (PIN) â if existent - of his private key secret and not share this information.
- If necessary the signatory immediately arranges for the revocation of his certificate.
- The signatory uses his certificate exclusively for the purpose specified in the certificate (refer to chapter 7.1.3). The provisions of the Certification Practice Statement and associated Policy valid at the time of issuance of the certificate are always binding.
- The signatory is obliged to observe the relevant national export regulations and possible national restrictions concerning the application in other countries.

2.1.4 Certificate User Obligations

Prior to accepting, the certificate holder of a.sign corporate certificates is obliged to check the following details:

- In the case of a signature certificate the certificate user checks the digital signature.
- The certificate user checks the validity of the certificate.
- The certificate user checks if the certificate has been used in accordance with the pre-defined purpose (e.g. for the generation of a digital signature).

2.1.5 Repository Obligations

The directory service publishes lists in regular intervals including

- issued certificates and,
- revoked certificates.

The directory service is obliged to update these lists in regular intervals and keep them highly available. The current update frequency of the revocation list may be called up on the Internet via the a.trust web site.

2.2 Liability

The valid versions of the Certification Practice Statement, the Certificate Policy, the terms of payment of a.trust and the general terms and conditions form the basis for the concluded contract.

2.2.1 Liability of the Certification Authority

a.trust is liable against third parties, who trusted in the correctness of the certificate and guarantees that

- if the preconditions are met (refer to chapter 4.3.1), the certificate is immediately revoked and a revocation service is available,
- it meets the requirements of the âFederal Law on Electronic Signaturesâ (Signaturgesetz) on providers of certification services,
- it complies with the X.509 standards,

- it complies with the procedures described in this Certification Practice Statement.

a.trust can define an upper limit of liability in the certificates. In case such a transaction limit has been defined in the certificate, a.trust is only to be held liable up to the specified amount. If no amount has been specified, there is no limitation of liability.

If an injured party can prove that a.trust has ignored obligations and legal provisions, it is assumed that the damage was caused thereby. In case A-Trust can prove that A-Trust and its employees are not responsible for the violation of the above listed obligations, a.trust is not to be held liable. a.trust is not to be held liable for lost profits, consequential damages or non-material damages of the user.

The certification authority is liable for the registration authorities.

2.2.2 Liability of the Registration Authority

The certification authority is liable for the registration authorities.

2.3 Financial Responsibility

2.3.1 Compensation of the Parties Involved

No provisions.

2.3.2 Fiduciary Relations

No provisions.

2.3.3 Administrative Processes

No provisions.

2.4 Interpretation and (Judicial) Enforcement

2.4.1 Underlying Legal Provisions

The contract signed between a.trust and the signatory is subject to Austrian law, and in case of signature certificates the provisions of [SigG] and [SigV] are applied. As far as foreign certificate holders are concerned the United Nations Convention on Contracts for the International Sale of Goods (CISG) is explicitly not applicable.

2.4.2 Separability of the Provisions, Persistence of Claims, Merger, Canceling

a.trust is entitled to confer all rights and obligations arising from the existing contract to third parties, which, however, does not provide the signatory with a particular right to give notice, as long as the third party observes the rights and duties defined in the contract.

The signatory is informed in writing on any changes of the general terms and conditions and of the Certification Practice Statement prior to the renewal of the certificate. If a.trust changes the general terms and conditions the signatory has at any time the possibility to cancel the contract. If the signatory does not oppose the changes of the general terms and conditions within one month, they are considered accepted.

2.4.3 Dispute Resolution Procedures

No provisions.

2.5 Fees

The currently valid fees are specified in the payment regulations. Any payments not included in the basic fee are due and payable upon the use of the relevant service.

2.6 Issuance and Renewal of Certificates

The agreed utilization fee has to be paid annually on the first day of each year. The obligation to pay arises on the first day the services rendered are available; the fee has to be paid in advance.

2.6.1 Certificate Access

a.sign corporate certificates may be called up via the directory service of A-Trust free of charge.

2.6.2 Suspension or Revocation of Certificates

Certificates may be revoked free of charge.

2.6.3 Status Information Access

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

2.6.4 Refund Policy

The signatory is not entitled to reimbursement of fees. In case the contract is canceled the certificate holder has to pay the fees until the end of the accounting period (end of the calendar year).

2.7 Publication and Repositories

2.7.1 a.trust Root Certificate

The a.trust root certificate may be found at

- https://www.a-trust.at/certs/A-Trust-nQual-nn.crt
- ldap://ldap.a-trust.at/ou=A-Trust-nQual-nn,o=A-Trust,c=AT

Explanation: -nn is the version number of the root CA: it is increased when a new key is generated or when the distinguished name is changed; -x denotes the version of the certificate: it is increased when a new certificate is issued with unchanged DN, nevertheless, when a new key is generated the new CA version (nn + 1) will always begin with -a; example: A-Trust-nQual-03a.crt.

The root certificate A-Trust-Qual-02 is used only for validation/CRL production of certificates issued by CA version 02. The root certificate may be downloaded from the corresponding menu on the a.trust homepage or directly by clicking on the above mentioned link.

2.7.2 a.trust CA Certificate

The relevant required CA certificate may be found at

- https://www.a-trust.at/certs/a-sign-corporate-light-nn.crt
- https://www.a-trust.at/certs/a-sign-corporate-nn.crt

Older Version (befor Genaration 03):

- https://www.a-trust.at/certs/a-sign-corporate-light-nn.crt
- https://www.a-trust.at/certs/a-sign-corporate-medium-nn.crt
- https://www.a-trust.at/certs/a-sign-corporate-stong-nn.crt

CA certificates may be downloaded from the A-Trust homepage.

2.7.3 Revocation Information

Certificate revocation lists (CRLs) can be downloaded at:

- ldap://ldap.a-trust.at/ou=a-sign-corporate-light-nn,o=A-Trust,c=AT?certificaterevocationlist?base?objectclass=eidcertificationauthority
- ldap://ldap.a-trust.at/ou=a-sign-corporate-nn,o=A-Trust,c=AT?certificaterevocationlist?base?objectclass=eidcertificationauthority

In addition to that the current CRL can be downloaded from the homepage.

2.7.4 Publication of Information of the Certification Authority

The certification authority publishes

- the relevant valid Certification Practice Statement (CPS),
- the relevant valid Certificate Policy,
- the valid payment conditions,
- internal audit information, provided that the security of a.trust is not at risk,
- the certificate of the certification authority,
- the general terms and conditions as well as
- a list with points of contact and registration authorities

on its homepage http://www.a-trust.at.

This information is kept highly available. Down times caused by system failure are kept at a minimum.

The signatory are also informed in case of:

- revocation of the key of the certification authority,
- compromise or suspected compromise of the key of the certification authority,
- extended down times of services (e.g. after a catastrophe at the certification authority),
- substantial changes of the Certification Practice Statement and
- cessation of the activities of the certification authority.

a.trust provides all information as follows:

- on the web site www.a-trust.at
- optional: in an electronic newsletter per e-mail
- optional: per mail
- optional: print media or television

Information concerning only individual signatory is directly submitted to them. In case a vast number of receivers is concerned one of the above listed alternatives is chosen. In particular in case of emergency print media or television are an appropriate means of publication e.g. to inform on the compromise of the a.trust CA-key.

2.7.5 Update Frequency

The Certification Practice Statement is updated in compliance with chapter **??**.

2.7.6 Access Control

Access control guarantees that the user has only reading access to the publications of a.trust. Only authorized employees of a.trust are entitled to change documents and administer the directories for certificates and the revocation lists.

2.7.7 Repositories

The following directories are maintained by the certification authority: A publicly accessible directory containing the certificates of the certification authorities and revocation lists as well as the certificates of the signatories.

A public web site from which these Certification Practice Statements may be called up and which provides the user with further general information.

2.8 Internal Audit

2.8.1 Frequency of the Audits

Internal revisions and audits are carried out on a yearly basis. They are carried out by means of random tests in all a.trust premises and registration authorities.

2.8.2 Identity of and Requirements on the Auditor

Internal audits are carried out in the framework of a revision.

2.8.3 Relations between Auditor and Party to be Examined

a.trust determines an auditor who examines the certification services but takes no security-critical function in addition to that. The registration authorities and other premises are also examined by the auditor determined by a.trust or by internal revision.

2.8.4 Aspects of the Audit

The auditor verifies if the certification authority works in compliance with the stipulations of the Certification Practice Statement as well as of the security and certification concept. The same applies to the premises to be examined. The auditor verifies the proper application and adequacy of the cryptographic components.

2.8.5 Actions to be Taken in Case of Insufficient Results

An audit concluded with insufficient results has the following consequences:

- Revocation of the relevant certificate and/or cessation of the operation of the examined unit of the certification infrastructure,
- the examined unit of the certification structure has to eliminate the weak points within a prescribed period.

2.8.6 Publication of the Results

a.trust publishes the information resulting from the audit, provided that the security is not at risk.

2.9 Confidentiality

2.9.1 Information Classified as Confidential

a.trust guarantees that the data disclosed by the signatory is treated confidentially in compliance with the Data Protection Act. All data required for registration is exclusively used for the services of the certification authority.

Non published certificates and personal data, which is not part of the certificate are classified as confidential data.

2.9.2 Information Classified as non-Confidential

Information contained in issued and published certificates as well as revocation lists are classified as non-confidential data.

2.9.3 Disclosure of Information Concerning the Suspension or Revocation of Certificates

Reasons entailing a blocking or revocation are published in the directory and revocation service.

2.9.4 Policy on release of Information to law enforcement officials

Personal data of the certificate holder is only transmitted by a.trust to legally authorized authorities upon explicit consent of the signatory and upon request.

2.9.5 Duty to Disclose Information under Civil Law

Refer to section 2.9.4.

2.9.6 Further Reasons for Disclosing Confidential Information

Refer to section 2.9.4.

2.10 Copyright and Right of Ownership

a.trust has the copyright and right of ownership of the following documents:

- Certification Practice Statement and
- Certificate Policy.

a.trust has the copyright and right of ownership of the following keys and certificates:

- private keys of the certification service provider,
- public keys of the certification service provider and
- certificate of the certification authority.

The signatory has the copyright and right of ownership of the following keys:

- private key of the signatory and
- public key of the signatory.

3 Identification and Authentication

3.1 Initial Registration

3.1.1 Type of Names

Particulars given by the certificate holder are classified in two categories: mandatory information and optional information.

The following data has to be included:

- The name of the certificate (Common Name):
  Name of the certified key of a.sign corporate. This is derived from the organization and/or its abbreviation, the key usage (e.g. Sig, Enc etc..), and an unambiguous definition of the organization.
- The name of the organization (complete name e.g. according to entry in register of companies or abbreviation) is required.
- The country in which the organization has its headquarters is also included in the distinguished name of the certificate.
- Name of the of the organization unit (optional)
- CIN: the Cardholder Identification Number is the part of the distinguished name of all a.sign corporate server certificates.
- Email address (optional)

3.1.2 Regulations for the Interpretation of Different Types of Names

No provisions.

3.1.3 Unambiguity of the Names

The name (subject) of a a.sign corporate certificate is unambiguous by the combination of the organizationâs name and other names (e.g. domain, name of the department, unmistakable key identifier, eâmail address, and CIN).

3.1.4 Right to Names and Settlement of Differences

No provisions.

3.1.5 Recognition, Confirmation and Significance of Trademarks

No provisions.

3.1.6 Method for Proving the Ownership of the Secret Key

The signatory generates the key-pair with an appropriate software (a.sign corporate light), a hardware device such as smart card or hardware security module (a.sign corporate medium), or a certified hardware security module (a.sign corporate strong) in a work process in conjunction with the creation of the certificate request that is sent to a.trust. Thus it is ensured through the certification of the public key that the private key belongs to the signatory under his sole control.

3.1.7 Authentication of Organizations

The organization of a signatory ordering an a.sign corporate certificate has to be examined. If the requesting organization is a company registered in the Austrian commercial register or in the European Business Register (EBR), the examination is carried out by the registration authority through online inquiry of the Austrian commercial register or EBR. In this case the Company Register number or the EBR number have to be included in the request. If the requesting organization is not a registered company, the copy of a document proving the existence of the organization has to be provided. Extracts (not older than three months) from a competent official register or comparable documents are accepted. The examination can furthermore by effectuated by means of data bases of trustworthy third parties.

3.1.8 Authentication of Individuals

The persons, who are identified when requesting a.sign corporate certificates, are

- the signatory, that is the technical responsible person (system or server administrator), that has exclusive control of preparation of signature data and
- an organizational responsible person, who has a power of attorney and who confirms the legal correctness of the certificate request.

A copy of a valid official identification document with photo must be submitted by both persons specified in the certificate request on a.trust. The following documents of identification are accepted:

- an official identification document with photo issued in Austria (a list of valid Austrian official identification documents with photos, which are accepted by a.trust, is published at the homepage of a.trust) or

- an internationally valid passport in German and/or English language.

If the organizational responsible person is not listed in the commercial register or EBR, then a complementary power of attorney (e.g. an authorization) must be submitted to a.trust.

3.2 Reregistration/Recertification

When the order has been placed the a.sign corporate certificate is subject to an unlimited contract with a.trust. Therefore, before the certificateâs validity period expires, the signatory of the a.sign corporate certificate is contacted and asked to send a new PKCS #10 request to the registration authority. Whether a new key should be generated is left to the signatory to decide, however a.trust recommends to use the possibility of a key change. The existence of the organization and the unchanged affiliation to the organization, are again examined by the registration authority during the renewal.

3.3 New Registration After Revocation

After revocation of a certificate the signatory may apply for a new certificate. This procedure corresponds to the registration procedure.

3.4 Suspension and Revocation Request

Revocation is handled in compliance with section ??

4 Operational Requirements

4.1 Request for the Issuance of Certificates

The request for the issuance of a certificate is submitted by an electronic form at the a.trust homepage.

The signatory must send the identification document copies, and if necessary confirmations, by fax to the registration authority.

If the affiliation to an authority for an a.sign corporate certificate is to be described, then an authorized representative must send a letter with the request to a.trustâs registration authority, which confirms the legal validity of this statement.

In order to verify the authorization of the a.sign corporate certificate order, the officer at the registration authority must contact the organizational responsible person specified in the request by telephone in order to confirm the legal validity of the request. Only then the certificate may be issued.

4.2 Publication and Acceptance of Certificates

The issued certificate can be distributed electronically to the signatory in two ways:

- It is sent by e-mail.
- There is a search function on the a.trust web site (the URL is sent in an e-mail to the signatory), in which the commonname can be entered. The result of the search is a link to where the appropriate certificate can be downloaded.

4.3 Certificate Revocation

All types of a.sign corporate certificates can be revoked immediately and permanently.

4.3.1 Revocation Reasons

The revocation of a certificate is necessary if

- essential details contained in the certificate are no longer correct,
- the private key for an a.sign corporate certificate can't be used anymore (e.g. the storage medium is defective and there is no back-up available),
- a key compromise is suspected (e.g. unauthorized access to the computer on which the private key is stored) or has already occurred,

- a.trust becomes aware of the fact that the signatory admits and/or has proven another hardware unit for generating or storing the private key of an a.sign corporate medium or a.sign corporate strong certificate than announced to a.trust,
- the certification authority detects a violation of this Certification Practice Statement or of the general terms and conditions by the signatory,
- the contractual relationship is terminated,
- the algorithms used no longer comply with the expected security standards,

4.3.2 Who can revoke a certificate

A revocation of a certificate may be submitted by:

- the signatory,
- the certification authority and,
- any person who knows the password for the revocation.

4.3.3 Procedures for a Revocation Request

A revocation may be carried out by telephone. The phone numbers of the revocation services may be obtained from the a.trust homepage.

The following requirements have to be met in the course of a revocation request:

- For revoking an a.sign corporate certificate the password for the revocation is mandatorily required.
- The reason for revocation (compromise of the private key, defect card, change of certificate data, termination of the contract etc.) has to be communicated to the staff of the revocation service.

The information required for a revocation can be summarized as follows:

- password for the revocation: mandatory
- name of the organization and server name or certificate number: mandatory

If in case of the revocation of an a.sign corporate certificate the password cannot be given, the revocation can be requested by registered mail with authorized company signature.

4.4 Certificate Suspension

A a.sign corporate certificate can't be suspended.

4.4.1 Update Frequency of the Revocation List

The current update frequency of the revocation list may be called up on the Internet at the a.trust website.

4.4.2 Requirements for the Checking Against Revocation Lists

The certificate users are responsible for verifying the validity of the certificates. The content of a certificate may only be considered authentic if the user has verified the validity of a certificate. A positive verification of the validity requires that

- the certificate was signed by using the key based on a valid certificate of the certification authority and
- the certificate is not contained in the current revocation list.

When receiving a signature the user has to check if the signature was created within the validity period of the certificate.

The certificate user should verify the authenticity of a revocation list by checking the signature against the revocation list.

Before using locally stored certificates the user should check a current revocation list. In case the validity check was not successful (e.g. for technical reasons) the certificate should not be accepted. The risk of accepting such a certificate is, however, taken by the certificate user.

4.4.3 Online Certificate Status Protocol

An OCSP service is available on the Internet.

4.4.4 Requirements on the Status Protocol

The certificate user should verify the authenticity of the information provided by the directory service by checking the signature contained in the answer. Furthermore the date contained in the status protocol has to be checked against the date in question.

If a successful validity check cannot be carried out (e.g. for technical reasons) the certificate should not be accepted. The risk of accepting such a certificate is, however, taken by the certificate user.

4.4.5 Further Processes for Announcing Revocations

No provisions.

4.4.6 Requirements for Checking Further Processes for the Announcement of Revocations

No provisions.

4.4.7 Specific Processes in Case of Compromise of Private Keys

If a compromise is suspected in the case of an a.sign corporate certificate the signatory has to request a revocation.

4.5 Recording of Security-Relevant Events

4.5.1 Recorded Events

For recording events the date and time and, if necessary, the person responsible are registered. This concerns:

- start-up and shut-down of systems,
- change of the hardware configuration,
- installation or canceling of authorizations,
- changes of the functions (refer to section 5.2),
- change of the software configuration (installation or update of software).

Furthermore all transactions carried out with the systems are recorded including type of transaction, time of the transaction as well as information on the status of the transaction (completed or canceled) and who initiated the transaction. In particular the following types of transactions have to be recorded:

- certification requests,
- generation of keys,
- certification generation,
- publication of certificates and revocation lists,

- blocking and revocation requests,
- revocations that have been carried out as well as
- change of keys.

The different processes entail additional events, which are recorded at the relevant organizations. This concerns for example:

- declaration of acceptance of the general terms and conditions and the payment conditions by the signatory as well as
- changes of the personal data of the signatory.

4.5.2 Checking Frequency of the Protocol Files

The protocols are checked once every workday for suspicious incidents.

4.5.3 Storage Period of the Protocol Files

Security-relevant protocol files are stored beyond the statutory period. Protocol files, which are required for later statements on the validity of certificates are archived. This applies in particular to data required for the publication of certificates and revocation lists as well as for entry und processing of revocation requests. The storage period for archived protocol files is specified in section 4.5.2.

4.5.4 Protection of the Protocol Files

The protocol files are created and stored at different locations. They are to be made accessible to authorized personnel only. The protocol files are protected against modification by means of a digital signature.

4.5.5 Protocol System (Internal/External)

Protocolling is carried out internally by the system at the different locations.

4.5.6 Notification in Case of Security-Critical Events

If a security-critical event is suspected a.trust decides on the notification of the users concerned.

4.5.7 Evaluation of Vulnerability

No provisions.

4.6 Archiving

4.6.1 Archived Data

The following data is archived:

- personal data of the signatory used for the certification,
- certification requests,
- all certificates issued by the certification authority (certificates of the certification authority and services, cross certificates and certificates of the certificate holders),
- revocation requests including date and time of entry (incl. the relevant protocol files),
- all issued revocation lists,
- date and time of the publication of certificates and revocation lists (incl. the relevant protocol files) and
- date and time of the change of keys of the certification authority.

4.6.2 Storage Period

Data is stored for at least seven years. The following aspects have to be taken into account:

- Data has to be stored for at least the period required for restoring in case of the breakdown of system components within the application period.
- When digital signatures are used data has to be stored at least as long as the digitally signed documents can be checked.
- Furthermore the technical compatibility has to be considered. This applies in particular to software and hardware whose modification render a checking of documents impossible.

4.6.3 Safeguard Measures

The archives are located in secured premises. Access is limited to authorized personnel only.

Electronic documents are protected from modification by digital signatures of the archiving unit.

Admission and access control provides that at the same time only two authorized and competent persons have access to the archives and the right to perform changes.

4.6.4 Requirement to Label Data with a Time Stamp

All certificate requests have to be labeled with a time stamp. This applies in particular to revocation requests and to changes in the revocation lists.

4.6.5 System for the Registration of Archiving Data (Internal/External)

The certificate management system is responsible for archiving all data to be archived in the a.trust system.

4.6.6 Procedures for Calling up and Checking Data

Users should have the possibility to call up archived information they are directly concerned with or which they need for verifying signatures. This involves a certain amount of work by the registration authority and is done under specific preconditions that have to be defined.

If electronic data is archived for a long period it has to be expected that outdated data formats are not supported by new systems. The certification authority thus keeps all systems available required for processing this data over the archiving period.

Provisions are being made in order to maintain the archives over the defined archiving period even in case of interruption or cessation of the activities of the certification authority.

4.7 Change of CA-Keys

A change of CA and root keys can occur in connection with the failure of a hardware security module or if the key lengths or algorithms no longer comply with expected security standards or in case of the compromise of keys. The latter case implicitly requires the revocation of the certificates concerned.

In addition the certification authorities regularly renew their certificates, which should be carried out prior to the expiry of the validity period defined in the certificate. For the validity period of the certificates please refer to chapter 6.3.2. The auditor of a certificate receives the new certificate from the directory service. The validity of the certificate can be checked by checking the validity of the certificate chain.

In case of a change of keys the validity of the old key expires, i.e. the private key is no longer used for certification. From this time on only the new key is used for signing certificates. The certificate for the old key is only revoked if necessary (compromise). If the old key is not revoked it may be used for verifying certificates until expiry of the validity period defined in the certificate.

As long as existing technical standards remain unchanged, i.e. the applied algorithm complies with the expected security standards and the legal provisions also remain unchanged there is no new key generated, but the validity period of the certificate is renewed at regular intervals.

4.8 Compromise and Emergency Plan

4.8.1 Computer, Software and/or Data are Compromised

If defective and manipulated computers, software or data are detected, which might influence the security of the system and its services the corresponding components are immediately put out of operation.

Should certificates be concerned the signatories have to be informed. The certificates in question are immediately revoked, in case the certificate contains defective data.

If a revocation list is defective, a correct revocation lists is immediately issued. Should a secure and immediate issuance of the revocation list be impossible and security-critical defects occur the directory services that publish the revocation lists are put out of operation in order to provide against further distribution of revocation lists with incorrect dates. The resumption of the service is linked with the publication of a new revocation list. The information of the users depends on the defect and the down-time of the directory service.

Should components have been put out of operation, they are put into operation again as soon as the defects are repaired.

4.8.2 Revocation of Certificates of Certification Authorities and Keys for Services

Certificates of the certification authority are revoked:

- in case of compromise or suspected compromise of the relevant keys,

- if the algorithms used no longer comply with expected security standards and thus a secure application cannot be guaranteed,
- in case of cessation of the activities of the certification authority; the revocation list or the status information services are not being maintained.

If a compromise or suspected compromise of the matching private key is the reason for revoking the certificate, section 4.7.3 has to be considered. Should the certificate be revoked due to the cessation of the activities of the certification authority, section 4.8 has to be considered.

The signatories are informed about a planned revocation in due time. In case of a unscheduled revocation the certificate holders have to be informed without delay. The information is provided on the website.Private keys of the certification authority whose certificates are revoked, are no longer used by the certification authority. These private keys are destroyed in compliance with section 6.2.9.

4.8.2.1 Revocation of the Certificates of the Services

If certificates of the services of the certification authority are revoked, the services without valid key are immediately put out of operation. The utilization of services with invalid signatures is thus avoided. The revoked keys are replaced by new keys. The services are put into operation again only after the new, valid keys have been installed.

4.8.2.2 Revocation of the Certificate of a Certification Authority

If a certificate of a certification authority is revoked all certificates issued by this certificate have to be revoked. The certificate status checking service will automatically answer inquires concerning all certificates issued by the certification authority or its sub-units by returning the status âinvalidâ.

Signatories whose certificates are concerned by the revocation receive a new key with new certificates in compliance with the relevant guidelines of this document. The certification is carried out with a new key of the certification authority.

4.8.2.3 Change of Keys

After the revocation of a certificate the matching private key is no longer used. However, in order to maintain the certification services and additional services, the certification authority has to use a new key. Should the certification authority already dispose of a new key due to the change of keys, this new key may be applied. This, however, implies that the key is still valid. If this is not the case the change of keys is performed according to the guidelines specified in section 4.6, which differs from a regular change as follows:

- In case of an immediate revocation it is not possible to inform the signatory about the change of key in time. They are immediately informed about the change of key in connection with the revocation information.

- There is no cross certification with an invalid certificate. The signatories may verify the authenticity of the certificates with the help of other procedures. Together with the new keys current certificates of the certification authority are supplied, which may be used for verifying the authenticity of the certificates.
- Revoked keys are invalid and are no longer used.

4.8.2.4 Revocation of Cross Certificates

If a certificate of the certification authority is revoked all cross certificates generated with this certificate are revoked as well. This also applies to cross certificates issued for other certification authorities and is of particular relevance if the security standards can no longer be guaranteed by this certification authority.

4.8.3 Compromise of Keys or Suspected Compromise of Keys

If keys of the certification authority have been compromised or there is reason to believe that a compromise has occurred, the security officer of the certification authority is immediately informed. If necessary he will order the revocation of the certificates concerned. Important measures are:

- The users are immediately informed.
- If necessary, the directory services are put out of operation and the status information is ceased in order to avoid that these services provide incorrect or invalid information.
- Distribution of new, valid certificates and, if necessary, of new keys to the users.

If a compromise is detected or suspected the security officer has to check carefully if other keys are concerned, too, and if the keys may still be considered secure.

4.8.4 Safety Precautions after disaster

The security officer decides whether the security of the services is in danger due to the catastrophe and arranges the necessary actions. Should usual procedures such as revocations or the provision of information by e-mail or the website be impossible as a result of the catastrophe alternative procedures such as the distribution of the necessary information by mail will be used.

If the security of the locality of the certification authority is in danger, media containing security-critical information are immediately transferred to a secured environment. The same applies to data carriers containing important information and archived data. In addition efforts are made to protect the locality from being accessed by unauthorized persons.

4.9 Cessation of the Activities of the Certification Authority

Cessation of activities means that all services of the certification authority (except the access to archived data) are no longer offered. Organizational changes or the change of the keys of the certification authority are not concerned.

The cessation of activities is communicated to the units and persons involved at least three months in advance. This applies in particular to the notification of the supervisory authority and the holder of valid certificates.

Prior to the definitive cessation of activities of the certification authority all valid certificates issued by the certification authority are revoked. All certificate holders concerned by the revocation are informed about the revocation of their certificates.

All relevant data of the certification authority concerned (certificates, CRLs etc.) is backuped. Archives and access to these archives will be held available over the specified archiving period.

a.trust sees to it that the CRLs of the suspended certification authority remain publicly and authentically available for the users after cessation of activities.

5 Physical, Procedure-Oriented and Personnel-Related Security Precautions

5.1 Physical Security Precautions

5.1.1 Location and Local Conditions

The services of a.trust are carried out in the following locations:

Dienstleistung	**Adresse**
Head office	A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH. Landstraßer Hauptstraße 5 A-1030 Wien
Registration, Revocation	A-Trust registration authorities and revocation services are available on the a.trust website http://www.a-trust.at/.

Table 1: Locations

5.1.2 Access Control

Access to all technical components in the data processing center is controlled by an authorization mechanism installed by a.trust.

Access control is adapted to the level of security required for specific areas containing security-critical components.

Access to top-security areas of the data processing center requires the presence of two persons with authorization card and the input of a PIN. Any access is recorded and thus traceable.

In addition video monitoring systems and anti-burglary systems have been installed.

5.1.3 Power Supply and Air Conditioning

The power supply of the location fulfills international standards and is â except for the registration authorities - of redundant design. In addition a emergency power supply exists in the datacenter.

The locations housing technical components of a.trust are equipped with adequate air conditioning.

5.1.4 Water Damages

The locations housing technical components of A-Trust are all equipped with adequate protection against water damages.

5.1.5 Fire

All premises housing technical components are equipped with a fire alarm system suitable for an EDP environment.

5.1.6 Data Carriers

The following data carriers are used:

- paper
- magnetic tapes
- hard disks
- DVDs
- WORMs

Data carrier with sensitive or security-critical data are kept access-protected in locked rooms or safes.

5.1.7 Waste Disposal

Data on electronic data carriers is properly destroyed, the data carriers are then handed over to a specialized company for their proper disposal. Paper data carriers are disposed of in available shredders or handed over to a specialized company for their proper disposal.

5.1.8 Redundant Design

The data processing center is operating redundantly, thus guaranteeing that the data processing center is operating and available 24 hours a day, seven days a week.

5.2 Procedure-Oriented Security Precautions

This chapter is dedicated to the definition of the functions required by a.trust and its premises. The functions are briefly described and classified according to their security-technical relevance.

5.2.1 Functions of a.trust

Function	Responsibilities
Business management	Commercial success of the company Marketing and Sales Operation Interface to the supervisory authority
Sales and Marketing	Sales concepts and their implementation
Project management	Consulting and execution of client projects in connection with a.trust products
Management	Undisturbed operation in compliance with security and certification concept as well as operations concept
Product marketing	Development of products/product families in line with market requirements
Security officer	Definition of and compliance with safety regulations Personnel security check
Revision	Execution of internal audits Must not perform any other security-critical function, unless required for the revision
Data protection	Supervision and observation of the stipulations of the data protection provisions
Training	Execution, development and supervision of training programs according to the security and certification concept

Table 2: Functionen of a.trust

5.2.2 Security-sensitive Responsibilities

Function	Responsibilities
Chief security officer	Refer to Table 2
Revision	Refer to Table 2
Data protection	Refer to Table 2
Security Officer (SO)	Access to the high-security zone Responsibility for the generation and certification of a.trust keys and for the revocation of these certificates Administration of the hardware security modules Granting of RO and RCA authorization Contact person for security-relevant questions Supervision of the compliance with procedures specified in the CPS
Security system administrator	Access to the high-security zone Supervision of system administrator and system operator
Revocation Center Agent (RCA)	Contact person for the signatories concerning revocation requests
Registration Officer (RO)	Receives certificate requests Identification of certificate applicants in the scope of the registration Instruction to the signatories

Table 3: Security-sensitive Responsibilities

5.2.3 Ohter Non-Security-sensitive Responsibilities

Function	Responsibilities
System administrator	Administration, installation, configuration and maintenance of the systems Is supervised by the security system administrator in security-critical areas
System operator	Continuous system administration, back-ups and data restoration for daily processes
Training	Refer to Table 2

Table 4: Other responsebilities

5.2.4 Number of Persons Required for Security-Relevant Activities

In table 5 security-relevant activities are described and assigned to the corresponding functions. It is furthermore indicated if the four-eyes principle is required for this activity and if the activity is performed in the top-security area of the a.trust data processing center.

Activity	Persons	4-eyes-principle	top-security-area
Registration and identification of certificate applicants	RO	No	No
Revocation of user certificates	RCA, RO	No	No
Generation of the keys for Root-CA and certification authorities as well as change of keys	SO, SO	Yes	Yes
Activation of the keys for Root-CA and certification authorities	SO, SO	Yes	Yes
Deletion of the keys for Root-CA and certification authorities	SO, SO	Yes	Yes
Certification for the Root-CA and the certification authorities	SO, SO	Yes	Yes
Revocation of certificates of the CA	SO, SO	Yes	Yes
Granting the authorization for RO and RCA	SO, SO	Yes	Yes
Start-up of a cryptoÂgraphic module (signature creation device of the AâTrust CA	SO, SO	Yes	Yes
Start-up and shut-down of components, in particular directory services	Security system administrator	No	No
Replacement of hardware components	Security system administrator (2x)	Yes	Yes
Replacement of sotfware components	Security system administrator (2x)	Yes	Yes
Checking of protocol files for suspicious incidents	System administrator	No	No
Checking of protocol files for manipulation	System administrator	No	No
Production and storage of a backups of the protocol files	Security system administrator (2x)	Yes	Yes

Activity	Persons	4-eyes-principle	top-security-area
Quality control of key lengths and parameters used for the generation of keys	SO	No	No
Maintenance or replacement of a cryptographic module	SO, SO	Yes	Yes

Table 5: Number of persons required

5.2.5 Identification and Authentication of the Functions

Access control systems limit the access to the premises containing security-critical components to persons authorized to execute the assigned functions.

5.3 Personnel and Security-Related Measures

5.3.1 Requirements for the Personnel

Personnel employed by a.trust fulfills all the necessary requirements concerning trustworthiness, integrity, reliability and know-how and furthermore disposes of expert knowledge in the following fields:

- general computer training,
- security technology, cryptography, electronic signatures and public key infrastructure,
- technical standards, in particular assessment standards as well as
- hardware and software.

5.3.2 Personnel Check

The reliability of personnel dealing with signature and certification services is checked at least every two years by consulting police records.

5.3.3 Training Requirements

Training by competent personnel is regularly organized for all employees. This training has both a technical and a security-relevant background. Authorization to occupy a certain function is only granted after completed training.

5.3.4 Necessity and Frequency of Repeated Training

Training is held in regular intervals, in particular when new technical systems, software or security systems are introduced.

5.3.5 Sequence and Frequency of Job Rotation

No provisions.

5.3.6 Sanctions for Unauthorized Actions

Disciplinary action is taken against persons violating the safety precautions.

5.3.7 Requirements for Contract Agreements with the Personnel

According to the Data Protection Act the personnel is under an obligation of secrecy.

5.3.8 Documents to be Handed Over to the Personnel

Depending on location and function in particular the following documents are handed over to the personnel:

- operations concept,
- Certification Practice Statement and
- training documents.

6 Technical Security Precautions

6.1 Generation of Keys and Installation

6.1.1 Generation of Keys

6.1.1.1 Keys of the Certification Authority

The keys of the certification authority for signing a.sign corporate medium and strong certificates are generated in a hardware security module of the certification authority. Export and backup of the certification authorityâs secret keys can only be performed at a another hardware security module which is available for reliability purposes.

The keys of the certification authority for signing a.sign corporate light certificates are generated on software basis. Backups of these secret keys may be generated in case of data is being lost in the data center.

The generation of all keys in the certification authority is always supervised by two authorized a.trust employees and has to be ordered by the a.trust business management.

6.1.1.2 Keys of the Certificate Holders

The signatoriesâ keys are generated by those in the following ways:

- a.sign corporate light:
  The keys are generated in software by the certificate holders, following a procedure that ensures sufficient quality of the key material.
- a.sign corporate medium:
  The keys of the certificate requestors are generated in a hardware, which is dedicated for this purpose, e.g. in a smart card or hardware security module.
- a.sign corporate strong:
  The keys of the certificate requestors are generated in a hardware security module which is certified according to ITSEC E3 or to at least an equivalent criteria.

a.trust has no knowledge of the private keys. The certificates are provided by the certification body based on the PKCS#10 requests created by the applicant.

6.1.2 Delivery of Private Keys to the Certificate Holders

Distribution of private keys is not performed, since only the signatory has control of the private key and a.trust has no access to the private keys.

6.1.3 Delivery of Public Keys to the Certificate Holders

6.1.3.1 Public Keys of the Certification Authority

The Root certificate and all certification authorities certificates are published in a directory on the Internet, in order to make them generally available thus giving all certificate users the opportunity to check certificates against this directory.

6.1.3.2 Public Key of the a.sign corporate Certificate

The key pair is generated by the signatory who thus possesses the public key.

6.1.4 Key Length

The keys of the Root CA and of all certification authorities currently have a length of 2048 bit (RSA key).

The hash algorithm used by a.trust for generating the signature of the certificates is SHA-1 or a stronger hash algorithm.

The signatories have to generate keys with at least 1024 bits keylenght (RSA keys).

For a.sign corporate certificates SHA-1 or stronger hash algorithm may be used.

The specified minimum key lengths may change due to algorithm weaknesses or in case they have to be adapted to new legal regulations.

6.1.5 Key Generation Parameters

The keys of the certificateion authority are generated by using a phisical random generator in a secure way.

6.1.6 Quality Control of the Parameters

The IT-security officer monitors the compliance with the legal requirements concerning the parameters for the generation of keys and ensures the correct application of the physical random number generator.

6.1.7 Hardware/Software Key Generation

The keys of the Root CA and of the certification authorities for a.sign corporate medium and a.sign corporate strong certificates are generated and used in a special hardware. The keys of the certification authorities for a.sign corporate light certificates are generated by software. The keys of the a.sign corporate certificates are generated by the signatories using software or in a suitable hardware module (see procedure in chapter 6.1.1).

Neigther the certification authority nor the registration authority know the private key of the signatory.

6.1.8 Key Usage

The purpose of the certified key is defined in the X.509 v3 certificates in the extension âkeyUsageâ

6.1.8.1 Usage of the Keys of the Root-CA

The Root CA possesses a self-signed certificate where the 'keyUsage' bits

- keyCertSign and
- cRLSign

are set.

6.1.8.2 Verwendung der SchlÃ¼ssel der Zertifizierungsstellen

The keys of the A-Trust certification authority are exclusively used for signing certificates and revocation lists. Thus the following bits are set:

- keyCertSign (signing of certificates) and
- cRLSign (signing of revocation lists)

6.1.8.3 Usage of the Key of the Certificate Holder

In case the keys of a.sign corporate light, a.sign corporate medium, or a.sign corporate strong certificates are used for key-encryption for encryption purposes, the following bits are set in the certificate:

- digitalSignature
- dataEncipherment.

The key of an a.sign corporate light, a.sign corporate medium or a.sign corporate strong certificate can also be used for creation of digital signatures and encryption at the same time; therefore all three bits are set:

- digitalSignature
- keyEncipherment
- dataEncipherment.

6.2 Protection of the Private Keys

6.2.1 Protection of the Key of the Certification Authority

The private key of the Root CA is used for signing the certificates of the certification authorities. It is only used in a secure environment.

The keys of a certification authority are used for signing certificates, revocation lists and cross certificates. They are only used in a secure environment.

For the storage and application of the private key of the Root CA and of the certification authorities for a.sign corporate medium and a.sign corporate strong certificates only hardware security modules providing an appropriate physical access protection for these keys are used.

For the storage and application of the private key of the A-Trust certification authority for a.sign corporate light certificates the appropriate access protection is guaranteed by means of a PIN.

6.2.2 Protection of the Keys of the Certificate Holders

The certificate holders keys are protected against unauthorized use either in a certified security module hardware, or in another hardware unit, or in the non-removable disk of the certificate holders server.

6.2.3 Deposit of Private Keys

Private keys are not deposited. This applies both to the keys of the certification authority and to the keys of signatories.

6.2.4 Backup of Private Keys

Backup of the Root CAs and the certification authorities secret keys can only be performed at a another hardware security module which is available for reliability purposes.

6.2.5 Archiving of Private Keys

Private keys of the certification authority are not archived.

6.2.6 Import of Private Keys into the Cryptographic Module

The design of the cryptographic hardware provides only for the generation of the private keys in this medium. Import of already generated keys is possible only by means of

import from another hardware security module, which is used to ensure reliability. The private keys are used directly in the hardware security module.

The utilization or activation of the private keys of the certification authority is protected by a user authentication.

6.2.7 Method for Deactivating Private Keys

Private keys which are no longer used are deactivated in the hardware security module by an appropriate method.

6.2.8 Method for Destroying Private Keys

Private keys of a certification authority that are no longer used are deleted.

The signatories are responsible for deleting secret keys of a.sign corporate certificates.

6.3 Further Aspects of Key Management

6.3.1 Archiving of Public Keys

Refer to section 4.6.

6.3.2 Utilization Period of Public and Private Keys

The validity model applied is a chain model. A higher-ranking authority verifies the validity of the certificate. The superior certificate has to be valid only at the time of issuance of the certificate to be verified. If a superior certificate is revoked, its subordinate certificates remain valid. As long as the certification key is considered secure a re-certification may be carried out.

The maximum validity periods of the certificates are as follows (in years):

Type of certificate	validity period
Root-CA	10
Certifications Authority	10
a.sign corporate light	5
a.sign corporate medium	5
a.sign corporate strong	5

Table 6: Validity period of certificates

6.4 Activation Data

6.4.1 Generation and Installation of Activation Data (PINs) for Keys of the Certification Authority

The keys of the Root-CA and of the certification authorities for a.sign corporate certificates may be generated by two officers by means of chip card and PIN only and exclusively by applying the four-eyes principle. The activation data is generated in a hardware security module of the CA system. Generated activation data is not put down in writing. There is a sufficient number of chip cards generated in order to avoid that the keys of the certification authority become unusable due to destruction or the loss of chip cards.

6.4.2 Protection of Activation Data

6.4.2.1 Activation Data for Keys of the Certification Authority

Employees disposing of the activation data for keys of the certification authority commit themselves to keeping them secret (PIN) and to store them securely (chip card).

6.4.2.2 Activation Data for Keys of the Certificate Holders

The signatories must not reveal the activation data of their private key (PIN) and must not store it in a place accessible to unauthorized persons.

6.5 Computer Security Regulations

6.5.1 Specific Security Requirements for Computers

No Provisions.

6.5.2 Assessment of the Computer Security

No provisions.

6.6 Life Cycle of Security Precautions

6.6.1 System Development

The requirements for system development are oriented towards the security requirements as stipulated by a.trust.

6.6.2 Security Management

The requirements for security management are oriented towards the security requirements as stipulated by a.trust.

6.6.3 Assessment

The requirements for assessment are oriented towards the security requirements as stipulated by a.trust.

6.7 Precautionary Measures with Regard to Network Security

Security-critical data is transmitted by an adequately secured communication channel. All security-relevant components, which can be accessed from the Internet, are additionally protected by firewalls.

6.8 Precautionary Measures for the Maintenance (Analysis) of the Cryptographic Module

Maintenance work is exclusively carried out by applying the four-eyes principle and in compliance with section 5.2.4.

7 Certificate and Revocation List Profiles

Certificates issued in accordance with this Certification Practice Statement are X.509 v3 certificates.

7.1 Certificate Profiles

7.1.1 CA Certificates

Attribute	Content	Explanation
Version	v3(2)	The version number is coded with the value '2' in order to indicate a X.509 certificate version 3
Serial number	Serial number of the certificate	Unambiguous within the a.trust certification infrastructure
Algorithm	≥ SHA-1	Algorithm used for the signature of the certificate
Certificate Issuer	CN = CommonName OU = OrganizationalUnit O = Organization C = AT	CommonName, OrganizationalUnit: (for CA-version 01 and 03): A-Trust-nQual-nn (for CA-version 02): A-Trust-Qual-02 Organization: (for CA-version 02 and higher):A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkeher GmbH (for CA version 01): A-Trust
Valid from Valid until	Start and end of the certificateâs validity	Validity period not exceeding ten years
Certificate holder	CN = CommonName OU = OrganizationalUnit O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	CommonName, OrganizationalUnit: a-sign-corporate-light-nn or a-sign-corporate-nn; valid up to CA-version 02: a-sign-corporate-medium-nn and a-sign-corporate-strong-nn -nn denotes the generation of the CA
Public Key	≥ RSA 2048 Bit	Public key of the certificate holder (the CA)

Table 7: Profile for CA certificate

7.1.2 Certificates for signatories

Attribute	Content	Explanation
Version	v3(2)	The version number is coded with the value '2' in order to indicate a X.509 certificate version 3
Serial number	Serial number of the certificate	Unambiguous within the a.trust certification infrastructure
Algorithm	≥ SHA-1	Algorithm used for the signature of the certificate
Certificate Issuer	CN = CommonName OU = OrganizationalUnit O = A-Trust Ges. F. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	CommonName, OrganizationalUnit: a-sign-corporate-light-nn or a-sign-corporate-nn; valid up to CA-version 02: a-sign-corporate-medium-nn and a-sign-corporate-strong-nn -nn denotes the generation of the CA
Valid from Valid until	Start and end of the certificateâs validity	Validity period not exceeding ten years
Certificate holder	C = CountryName CN = CommonName O = Organization OU = OrganizationalUnit E = E-Mailadresse Seriennummer = Serial-Number	CountryName: AT, DE etc. CommonName: Name of the organization and/or abbreviation, key usage (e.g. Sig, Enc etc) and organizational internal unambiguous additional information, e.g. 'XYZ-Bank Sig 0001'. Organization: Name of the organization (according to abbreviation or excerpt from the trade register) OrganizationalUnit: department etc, optional EmailAddress: optional SerialNumber: unambiguous identification number of the sigantory (CIN)
Public Key	≥ RSA 1024 Bit	Public key of the signatory

Table 8: Profile for a.sign corporate light, a.sign corporate medium, a.sign corporate strong

7.1.3 Certificate extensions

In the certificates issued by CAs the following extensions are used in accordance with X.509 v3 and PKIX:

Extensions	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 9: Extensions (CA-Certificate)

The utilization of extensions in the certificates issued by the CA is shown in the following tables:

Extensions	Included in the certificate	classification	
		critical	non critical
Standard Extensions			
authorityKeyIdentifier	Yes		X
subjectKeyIdentifier	Yes		X
keyUsage	Yes	X	
certificatePolicies	Yes		X
basicConstraints	Yes		X
cRLDistributionPoints	Yes		X
subjectAltName	optional		X
Private Extensions			
authorityInfoAccess	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 10: Extensions (a.sign corporate Zertifikat)

The extension key usage is described in greater detail in sections 6.1.8.

Optionally can a.sign corporate light, medium and strong certificates contain a certificate extension, which states that the signatory is an employee of a public authority (public

authority indicator - OID 1.2.40.0.10.1.1.1). Furhter, in this extension an administrative indicator can also be optionally included, which indicates the association to an organizational unit in the public administration.

Further a.sign corporate light, medium and strong certificates can optionally include a certificate extension, which associates the certificate with an organization that is active on behalf of a public administration (service authority indicator - OID 1.2.40.0.10.1.1.2).

The upper limit of liability that is described in section 2.2.1 is optionally included with the OID 1.3.36.8.3.4 into a.sign corporate light, medium and strong certificates.

7.2 Profile of the Revocation List

7.2.1 Version Numbers

The revocation lists issued by the certification authority are revocation lists according to X.509 v3 version 2.

7.2.2 CRL und CRL Entry Extensions

The non critical extensions authorityKeyIdentifier and CRLNumber are used for complete revocation lists.

In addition delta revocation lists have the critical deltaCRLIndicator extension.

As CRL entry extension only reasonCode, which is classified non critical, is applied.

8 Administration of this Specification

8.1 Procedures for Modifying this Document

Modifications of this Certification Practice Statement are exclusively carried out by a.trust and have to be approved by the business management.

Changes concerning security-relevant aspects or requiring the modification of processes on the part of the certificate holders require the adaptation of the OID of the Certificate Policies and the URI of the Certification Practice Statement. Thus, they require the general notification of the signatories. In particular these changes concern:

- obligations, liabilities, financial responsibility,
- registration,
- personalization,
- Internet addresses and contact information,
- key and certificate management,
- directory and revocation services

If these changes of the Certification Practice Statement do not concern any of the above mentioned aspects they may be carried out without prior notification. In particular this applies to changes concerning typography and layout as well as addresses or business hours of points of contact.

8.2 Procedures for Publication and Notification

After changes have been carried out the current Certification Practice Statement and Certificate Policy as well as the old versions may still be called up.

8.3 Approval and Suitability of a Certification Practice Statement

This Certification Practice Statement applies to the a.trust products a.sign corporate light, a.sign corporate medium, and a.sign corporate strong. a.trust guarantees that this Certification Practice Statement is suitable for the Certificate Policies concerned.

A Annex

A.1 Glossary

a.sign corporate	Product name of a.trust's server certificates
Activation Data	Data required for activating keys (also refer to PIN).
Audit	Security check, revision
CA	Certification authority
CA Keys	Keys of the CA, used for issuing certificates and for signing revocation lists (certification).
Certificate Policy	An unmistakably identified number of regulations, which describe the purpose of a certificate with regard to a specific group and/or category of applications with the same security requirements.
Certificate User	User, using the a.trust certificates and public keys to verify signatures.
Certification Authority	The certification authority generates the keys of the users and assigns a key to a user. It also provides additional services such as the publication of certificates or revocation.
Certification Practice Statement	Guidelines on the practices of the certification authority concerning the issuance of certificates.
Chain Model	Validity model allowing the valid application of the key provided that the certificate is valid at the time of application and that the higher-ranking certificate was valid when the applied certificate was generated.
Chip Card	Chip card / smart card on which the keys of the individual user are generated and stored in a secure manner.
Directory (Service)	Service from which the users may call up certificates of the CA or other users as well as CRLs. Access is realized via LDAP.
Keys of Services	Keys of a service (e.g. signature key for signing status information).
Policy	Refer to Certificate Policy
Registration Authority	At the registration authority users are registered and identified before obtaining the certificates. The registration authority may also assume other tasks such as the acceptance and forwarding of change requests.
Revocation List	List including all blocked and revoked certificates and which is signed with a key of the CA.
Root-CA	The Root-CA is the highest-ranking certification authority within the a.trust certification hierarchy. It issues the certificates for subordinate certification authorities.

Services (CA Services)	Services such as directory service, status information and time stamping service.
Signatory	User whose keys and personal data are contained in the a.trust certificate.
Signature Generation Data	Signature generation data is unique data such as codes or private signature keys used by the certificate holder for creating electronic signatures.
Signature Verification Data	Data such as codes or public signature keys used for checking electronic signatures.
Status Information	Services from which the user may obtain information on the current status (valid or revoked) of a certificate. Access is realized via OCSP or CRLs, which may be called up from directory services.
Time Stamp	Digital signature of digital data and point in time. With the help of a time stamp it can be proven that a digital document existed at a specific time. In order to avoid manipulations the time stamp should only be issued by a trustworthy authority (e.g. a certification authority).

A.2 Abbriviations

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 Signature and encryption procedure; named after Rivest, Shamir und Adleman

SigG Austrian Law on Electronic Signatures

SigV Directive to Austrian Law on Electronic Signatures

SO Security Officer

URI Uniform Resource Identifier

A.3 Referenzdokumente

[SigG] Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG). BGBl. I Nr. 190/1999 (NR: GP XX RV 1999 AB 2065 S. 180. BR: AB 6065 S. 657.)

[SigV] Verordnung zum Signaturgesetz, BGBl II 2000/30, 02. 02. 2000 und BGBl. II Nr. 527/2004 vom 30.12.2004

[SigRL] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, 13. 12. 1999

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