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
office@a-trust.at
www.a-trust.at

a.trust

Certificate Policy for Simple Certificates a.sign corporate light

Version: 1.0.3

Date: 21.05.2008

Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH.
A-1030 Wien, Landstraßer Hauptstraße 5

Contents

1 Introduction

1.1 Overview

A Certificate Policy contains a set of rules, which defines a certificate's area of application for a certain user group and/or application class with common security requirements.

1.2 Document identification

Policy name: a.trust Certificate Policy for simple certificates
a.sign corporate light

Version: 1.0.3/2

Object Identifier: **1.2.040.0.17** (a.trust) **.1** (Policy) **.7.1** (a.sign corporate light) **.1.0.3** (Version) present version

This policy adheres to the requirements in [RFC3647].

1.3 Scope

The a.sign corporate light policy applies for simple a.sign corporate light certificates according to the definition § 2 section 8 [SigG], which are issued to organizations that operate servers with signature -, encryption - or authentication operations. The certificate holders' private keys are stored in their computers.

1.4 Compliance with the policy

a.trust uses the object identifier from chapter 1.2 for certificate production only when the published regulations of the present policy for a.sign corporate light certificates are considered.

2Obligations and regulations

2.1a.trust's obligations

a.trust is obliged to guarantee that all requirements, which are stated in section 3 are fulfilled.

a.trust is responsible for adherence to all guidelines, which are described in the present policy; this applies also to the functions which are outsourced to a contractual party (e.g. directory service).

There are no additional obligations, directly or by references, in the certificates; hence, no additional obligations are included in this document.

a.trust provides the certification services in agreement with the certificate practices of a.sign corporate (see [CPS]).

2.2The certificate holders' obligations

a.trust binds the certificate holder contractually to the contents of the following stated obligations. The certificate requestor has access to the contract conditions on the homepage, and confirms its information and acceptance when mailing the purchase order form.

The certificate holder's obligations include:

1. to provide complete and correct information in compliance with the requirements of this policy, in particular during the registration process,
2. to be cautious in order to prevent unauthorized use of the private key and to desctruct the same when its validity period expires,
3. to immediately notify a.trust if one of the following cases occurs before an a.sign corporate light certificate expires:
    - the certificate holder's private key may have been compromised,
    - the control of the private key is lost,
    - the contents of the certificate is incorrect or has changed.

2.3 Obligations of the auditors of the certificates

An auditor, who uses an a.trust certificate for verification of a signature or for decryption, can trust this only if he

- verifies the validity period and the revocation status of the certificate by using a.trust's validation services,
- considers possible restrictions stated in the published trading conditions or in the use of the certificate (see also below and section 1.3),
- and adheres to all other prescribed precautionary measures (see [CPS]).

2.4 Liability

a.trust is liable as issuer of a.sign corporate light certificates

- for the contents of the corresponding certificate practices (see [CPS]), in particular to ensure prompt publication of revocation lists and adherence to the standards specified in the certificate practices (International Telecommunication Union X.509)
- as the data of the certificate holder in the certificate was correct at the time of issuance and was validated during registration.

a.trust can not be held liable if it can prove that it does not caused any injury due to the obligations stated above.

3Requirements on the provisioning of the certification services

This policy is intended for provisioning of simple certification services. This covers the provisioning of registration services, creation of certificates, certificate issuance, revocation services, and certificate validation services.

3.1Certification Practice Statement

a.trust has taken the following measures in order to ensure the required security and reliability for provisioning of the certification services:

1. a.trust has a description of all processes and procedures, which are required to fulfill the requirements in this policy.
2. The certification practices of a.sign corporate describes the obligations of a.trust and all external contractual parties, which provide services for a.trust with respect to each case in the applicable policies and practices.
3. a.trust provides access to the certification practice statement and any other documentation, which describes the compliance with this policy, for all certificate holders and other persons who rely upon the reliability of a.trust's services (see chapter 3.3.4).
4. The management of a.trust constitutes the exclusive decision-making body, which is responsible for the approval of the a.sign corporate certification practices.
5. The management of a.trust has also the responsibility for the standard implementation of the certification practices of a.sign corporate.
6. a.trust has defined a revision process for auditing the certification procedures, which also covers maintenance of the certification practices of a.sign corporate.
7. a.trust informs regularly about changes to the Certification Practice statement, and a revised version of the certification practices of a.sign corporate are immediately published according to point 3 of this paragraph.

3.2 Administration of the keys for provisioning of the certification services

3.2.1 Creation of the CA keys

The generation of keys that are used by a.trust for provisioning of certification services used in compliance with regulations §§ 6 and 8 [SigV] and thus in compliance with [SigRL] annex II (f) and (g):

1. The key generation is performed by authorized personnel (see chapter 3.4.3), by the four-eye principle in a secured environment (see 3.4.4).

2. For the key generation an algorithm is used, which is regarded as appropriate also for qualified certificates.

3. The key length and the algorithm would also be suitable for qualified certificates and correspond to appendix I [SigV].

3.2.2 Storage of the CA keys

a.trust ensures in compliance with the regulations of § 10 [SigV] that the private keys are kept secret and their integrity remains, and considers also for the provisioning of simple certification services according to the regulations § 10 [SigV].

3.2.3 Distribution of the public CA keys

a.trust ensures, by taking the following measures, that the integrity and authenticity of the public keys remain protected at the time of distribution:

- by delivering the root key in a signed PKCS #10 certificate request to the supervision body for publication and by

- issuance and publication of a self-signed root certificate.

The certificate of the CA key used for signing a.sign corporate light certificates is published in a directory service and thus accessible to the certificate holders. a.trust ensures the authenticity of this certificate.

3.2.4 Key disclosure

Disclosure of the secret CA keys is not intended.

3.2.5 Intended purpose of CA keys

The certification authority's private key is intended to be used only for production of a.sign corporate light certificates and for signing the associated revocation lists in physically secured premises.

3.2.6 End of the CA keys' validity periods

Secret keys intended for signing a.sign corporate light certificates are used as long as the used algorithms correspond to the security recommendations. The certificates over a.trust certification authority's keys are renewed at least every ten years. If the algorithms do not correspond to the security recommendations any longer, no renewal is performed and the keys are destroyed when the end of the validity is reached.

Archiving of the secret keys is not intended.

3.2.7 Creation of keys for the certificate holders

The generation of the certificate requestors' keys are made by themselves in a secure way.

a.trust has no knowledge of the private keys.

3.3 Certificate life-cycles

3.3.1 Registration of the certificate holders

The measures for identification and registration of the certificate holders ensures that the request for issuance of a light a.sign corporate certificate is accurate, complete and authorized.

1. Before the contract between the certificate holder and a.trust is established, the trading conditions and optionally other regulations for the use of the certificate are made electronically available to the certificate holder (see 3.3.4).

2. The request form and the information are electronically available at a.trust's web page.

3. The certificate request contains among other things the following data:

   - the complete names, telephone numbers and email addresses of the applicants (e.g. server administatrators),
   - the complete names of and contact information to the authorized signatory,
   - revocation password,
   - company registration number or ERB-number (when available),
   - name and registered office of the organization,
   - optional name of the organizational unit,
   - optional name of the domain (or an IP address, see [CPS] for details),
   - optional email address of the certificate (the email address must belong to a domain which is possessed by the organization),
   - the public key component which is to be certified.

4. The contract which may be established with the applicant contains in particular:

   - acceptance of the certificate holder's obligations,
   - agreement that all recordings and data, which are received by a.trust during the registration procedure, are stored and that these recordings may be forwarded to a third party if necessary for completion of the certification services,
   - confirmation that the certificate contents are correct.

5. a.trust performs the following checks of the request:

   - identification of the organization (as per trade register or based on trusted third party databases),

- validation of the power of attorney and the identification documents,
- if necessary, validation of the ownership of the domain (IP address).

6. The certificate request submitted by the applicant and all attachments, available data and documents in paper form (identification document copies, if necessary confirmations of the enterprise, the power of attorney or legal rights to domain/IP address), are archived long term from at least seven years until expiration of the (electronical) validity.

7. Attention to the regulations of the data protection act ([DSG]) is ensured by the part of the prescribed process of a.trust's registration authorities.

3.3.2 Extension of the certificates' validity periods and new issuance

By the following measures it is ensured that requests are submitted by certificate applicants who have already been registered completely, correct and duly authorized at a preceding certificate issuance. The measures apply both to extension of the validity period and to new issuance after expiration or revocation of a certificate.

1. The registration authority must validate the certificate contents regarding its current validity.

2. Any changes in the contractual conditions are communicated to the applicant and his acceptance is thereby acknowledged. These measures are carried out adherent to section 3.3.1.

3. Any changes to the documentation contents of the initial application according to 3.3.1 are checked and confirmed by the applicant.

4. Extension of the certificates' validity period before expiration is performed according to § 12 Abs 4 [SigV]. The new validity period resulting from the extension adds up to at most five years. An extension is made only if the cryptographic security of the used algorithms is sufficiently ensured over the entire new validity period, and the applicant has not reported any compromised private keys.

3.3.3 Issuance of the certificates

By the following measures, it is ensured that issuance, extension and new issuance of certificates is performed in a secure way and do also comply with the requirements of [SigG].

1. A.sign corporate light certificates are provided as X.509 v3 certificates. The certificate contents are in particular the following:

    - Version number of the certificates: certificates of version 3 (encoded as value 2) are issued
    - Serial numbers of the certificates
    - Indicator of the certification authority
    - Beginning and ending of the validity period of the certificates
    - Distinguished name of the certificate holders:
        - Common Name
          Either the name of the certified key, which is derived from the organization and/or its abbreviation, or a key identifier and a definition which is unique for the organization or the name of the domain/IP-address,
        - Name of the organization,
        - Name of the organizational unit (department etc.): optional
        - Email address: optional
        - CIN: Cardholder Identification Number
          Identification number of the signatory
        - Country of the registered office of the organization (e.g. AT, DE)
    - Public key (with information of the used algorithm)
    - Information of the algorithm of the certificate's signature
    - Signature over the certificate
    - Certificate extensions, such as:
        - Information of the used policy and/or CPS

- Certificate usage
- Information of where the CRL can be retrieved
- optional public authority characteristics and if necessary an optional administrative indicator
- optional notification of a service authority indicator of an organization, which is acting on behalf of a public organization of the administration.

2. The certificates are created by the certification authority of a.trust, after the applicant has been identified and the correctness of all data has been confirmed. The procedure is identical for issuance and for new issuance after revocation or change of data.

3. The unambigous association of the certificate with the certificate holder is ensured through:

   - Production of PKCS #10 requests by the applicant as basis for certification.
   - Production of the certificate after all applicant data and its correctness has been validated by a.trust.
   - Confirmation of the correctness of the data submitted to the registration authority by the applicant.

4. The data received by the registration authority are signed and transferred encrypted (SSL) to the certification authority. Privacy and integrity of all data are thereby ensured.

5. All RA staff are equipped with signature cards. The authenticity of the submitted registration data is verified by the signature of the RA staff.

3.3.4 Announcement of the contractual conditions

a.trust makes the conditions, which concerns the use of a.sign corporate light certificates, accessible to the certificate holders and the users, who trust the reliability of a.trust's services, by publication of the following documents at a.trust's homepage:

1. the current certificate policy,
2. the Certification Practice Statement (certification practices of a.sign corporate),
3. the general business regulations of a.trust,

4. other messages.

Changes are announced to the certificate holders at a.trust homepage and if necessary additionally by email or briefly informed. Everyone can visit a.trust's homepage.

In these documents are amongst other the following unambiguously defined:

- a.sign corporate light certificates are issued to organizations, which operate servers,
- the obligations of the certificate holder in accordance with chapter 2.2.
- the process of certificate validation, including the necessity for validation of certificate status, so an auditor can trust the certificate with good reasons (see chapter 2.3),
- if necessary, the range of the restrictive transaction limit of a.sign corporate light certificates must be recognizable,
- the time interval for storage of registration information (see chapter 3.3.1),
- the time interval for storage of logs with important events at the certification authority (see chapter 3.4.11),
- the fact that the enterprise was indicated as a certification service tenderer to the supervision body in accordance with §6 [SigG],
- proceedings for treatment of complaints and disputes,
- the applicability of [SigG] and [SigV].

3.3.5 Publication of the certificates

Certificates issued by a.trust are made available to the certificate holders and the auditors as follows.

1. All a.sign corporate light certificates are published by a.trust in the directory service.
2. The conditions for certificate usage are distributed to everyone concerned by a.trust (see chapter 3.3.4).
3. Identification of the regulations to be used is easily derived from the unambiguous association with the product name "a.sign corporate light".

4. The directory service is available 24 hours per day seven days per week. Interruptions of more than 30 minutes are documented as incidents in accordance with § 13 section 5 [SigV].

5. The directory service is publicly and internationally accessible.

3.3.6 Revocation

Revocation is an irreversible early termination of a certificate's validity.

1. The process for executing the revocation is documented in the certification practices of a.sign corporate, in particular:

   - what justified the revocation request,
   - if a revocation request can be submitted,
   - the mechanisms for providing status information and
   - the maximum time interval, which can elapse between the revocation request and the publication of the revocation.

2. Revocation can be requested by the certificate holder by telephone within office hours to the revocation service of a.sign corporate light certificates. All requests are processed upon arrival. As proof of the authorization of the applicant the revocation password, which was selected during the certificate order, must be provided. The name of the organization, the name of the caller, and the certificate contents, e.g. common name, must be mentioned to the a.trust revocation service staff. The data from the call are noted and dispatched. If the revocation password has been forgotten, then revocation can also be requested in writing with a corporate signature.

3. A revoked certificate can not be reinstated.

4. Revoked certificates are published in a revocation list (CRL) in compliance with the following regulations:

   - The current update frequency of the revocation list is available over the Internet at a.trust's web page.
   - Each revocation list contains the time of the planned issuance of the next list.

- If necessary, a new revocation list can be published earlier (i.e. before the next planned issuance).
- Each revocation list is signed with the CA key.

5. Revocation lists are issued as X.509 v 2 CRLs. The essential data in the CRLs are the following:
   - Version number of the CRL: version 2 (encoded as value 1)
   - Description of the issuer
   - Time of the CRL issuance, as well as the next planned issuance
   - Information of the certificates that are included in the CRL:
     - Serial number,
     - Time of entry into the CRL,
     - Revocation reason
   - CRL extensions
   - Indicator of the algorithm used for the signature over the CRL
   - Signature over the CRL
6. The revocation service of a.sign corporate light certificates can be contacted during office hours. At the latest three hours after the revocation reason was reported, the revocation list is actualized. The current office hours for each case can be found at a.trust's home page.
7. Revocation lists are available daily 24 hours. In case of system failure the precautions described in the certification practices for a.sign corporate are taken into effect, in order to limit the effects to a minimum.
8. Status information of certificates can also be requested over OCSP. The integrity and authenticity of the OCSP response are ensured by a signature.
9. The directory service of revocation lists are publicly and internationally available.

3.4a.trust administration

3.4.1Security management

The following regulations apply:

1. a.trust is responsible for all processes in the context of the certification services; this applies also to the services outsourced to subcontractors. The responsibilities of the subcontractors are clearly regulated and controls for auditing the normal activities are established. The security procedures are published in the certification practices of a.sign corporate.

2. The management of a.trust is directly responsible for the definition of the security guidelines and communication to the staff concerned with security related procedures.

3. a.trust's security infrastructure is constantly audited and adapted due to changed requirements. Any changes, which have influence on attained security level, must be approved by the management of a.trust.

4. All security measures and security related functions for the provisioning of the certification services are documented by a.trust, and implemented and maintained according to the documentation.

5. The data center operations is outrsourced by a.trust to SBS Siemens Business services Ges.m.b.H.. SBS is contractually bound to the maintenance of information security.

3.4.2Information classification and administration

a.trust ensures that all data and information are secured in an appropriate way.

3.4.3Personnel security controls

a.trust's staff and the occupation modalities are suitable to strengthen the confidence of the development of the certification services. In particular to the following values are emphasized:

1. a.trust employs exclusively personnel who possess the necessary special competence, qualification and experience for respective position.

2. Security related functions and responsibilities are documented in respective job description. Those functions, on which the security of the certification services depends, are clearly identified.

3. For all a.trust staff (independent of whether employed under temporary or permanent conditions) well-defined job descriptions are prepared, in which the obligations, access rights and minimum comptence are stated.

4. The practice of both the administrative and the management functions conforms to the security guidelines.

5. All management functions are occupied with persons who have experience of digital signature and encryption technology, and who have access to personnel who are responsible for sensitive activities.

6. All employees, who have trustworthy positions, are contained from interest conflicts, which could oppose an impartial fulfilment of the tasks.

7. All trustworthy positions are described in detail in the certification practices of a.sign corporate.

8. Assignment of the positions are made by formal appointment by the management.

9. In accordance with § 10 Abs 4 [SigV] a.trust employs no persons who have committed criminal actions, which make them appear unsuitable for a trustworthy position. An employment is made only after a relevant examination.

3.4.4 Physical and organizational controls

It is ensured that access to the premises in which security critical functions are operated is secured and the risk of physical damage of the data center is minimized. In particular applies:

1. Access to the premises, in which certification and revocation services are operated, is limited to authorized personnel. The systems, which issue certificates, are protected against threats from environmental disasters.

2. Measures have been taken in order to prevent loss, damage or compromising of the data center and interruption of the operations.

3. Further measures ensure that compromising or theft of data at data processing centers is not possible.

4. The systems for certificate production and revocation services are operated in a secured environment, in which compromising by unautorized access is not possible.

5. The systems for certificate production and revocation services are separated by clearly defined security zones, i.e., by physical separation from other organizational units as well as with physical access protection.

6. The security precautions include building protection, the computer systems themselves and all other mechanisms that are essential for operations. Protection of the mechanisms for certificate production and provisioning of the revocation services covers physical access control, prevention of threats from forces of nature, fires, armed assaults and building collapses, protection from loss of power supplies as well as from theft, breakdowns and system failures.

7. Unauthorized removal of information, data media, software and equipment which belong to the certification services is prevented by control measures.

3.4.5Operational management

a.trust ensures that the certification system is securely and correctly operated, and that the risks of failure are reduced to a minimum. In particular appy:

1. The integrity of the computer systems are protected against viruses and malicious code or unauthorized software.

2. Damages by security critical incidents and malfunctionings are prevented by appropriate recordings and error reducing procedures.

3. Data media are protected against damage, theft and unauthorized access.

4. For the execution of security critical and administrative tasks, which have impact on the provisioning of the certification services, procedures have been defined and implemented.

5. All data media is treated and stored in accordance with its security class. Data media that is not needed anymore, and includes sensitive data, is destroyed in a secure way.

6. Capacity requirements are observed and future developments are forecasted, such that appropriate processor performance and sufficient storage are always available.

7. Reactions to incidents are made as fast as possible, in order to minimize security criticial events. All incidents are logged as soon as possible.

The security critical functions within the scope of certification and revocation services are strictly separated from the ordinary functions.

Security critical funtions include:

1. Opertional functions and responsibilities
2. Planning and approval of security systems
3. Protection from malicious software
4. General maintenance activities
5. Network administration
6. Active auditing of log files and test reports, analysis of incidents
7. Data media maintenance and security
8. Replacement of data and software

These tasks are controlled by a.trust's security representatives, but they can however be performed by operational personnel (under supervision) in accordance with security concept and job descriptions.

3.4.6 Access management

a.trust ensures through the following measures, that access to the certification system is exclusively and appropriately limited to authorized persons only.

1. Security measures by e.g. firewalls protect the internal network from access by third-parties.
2. Secret data are protected when being transmitted over unsecured networks.
3. A user administration, which grants different access rights to different functions, is implemented; in particular security related functions are carefully separated from not security critical ones. Changes to the access rights are immediately configured in the system. Control of the user administration is part of the internal audits.

4. Access to information and applications is restricted due to the assigned access rights. The adhering definitions are outlines in the certification practices of a.sign corporate. Administrative functions and operational ones are strictly separated. The use of system utility programs is in particular reduced.

5. All staff must be authenticated before being granted access to critical applications, which are connected to the certification management.

6. The access are logged in log files. The responsible staff is selected for the performed activities.

7. Re-use of data memories does not lead to disclosure of confidential data to unauthorized persons.

8. Components in the local network are located in a secure environment, and the configuration are periodically audited.

9. Detection of unauthorized and/or abnormal access attempts to the actual certification authority and the revocation services are secured by suitable measures, in order for immediate counter measures to be taken if required.

10. Changes (removals, addings) to the directory and revocation services must be ensured by a signature of the certification authority.

11. Unauthorized access attempts to the directory or revocation services are logged.

3.4.7 Development and maintenance of trustworthy systems

a.trust uses trustworthy systems and products, which are protected from changes.

1. An analysis of the security measures during the design and requirement specification phases of a development project must be carried out by a.trust or by a third-party on a.trust's assignment.

2. Change management procedures exist for the deployment of planned program versions, other changes and patches.

3.4.8 Maintenance of continuous operations and incident management

a.trust is devoted to recover operations as soon as possible after disasters, including compromising of a certification key. In particular the following is intended:

1. a.trust's emergency plan covers the disaster case of the private certification key being (actual or suspected) compromised.

2. If this case should occur, a.trust must inform the supervision body (see § to 6 Abs 5 [SigG]), the certificate holders who trust the reliability of the certification services, and if necessary different certification service providers with whom agreements exist, that the revocation and certificate information can not to be regarded reliable any more.

3. Certificates and revocaiton lists can not be considered as valid anymore.

3.4.9 Cessation of operations

In accordance with § 12 [SigG], a.trust must to immediately inform the supervision body about cessation of operations, and ensure that possible impact on both certificate holders and all parties trusting the reliability of services is limited to a minimum.

1. Before the services are terminated are

    - all certificate holders, certification services requestors and other parties who have a business relation with a.trust, directly or through parties that rely upon the reliablitiy of a.trust services, informed about the cessation,

    - the contracts with subcontractors (directory service etc.) for the provisioning of certification services terminated,

    - precautions met for acquisition of the directory and revocation services as well as recordings in accordance with chapter 3.4.11 by other certification service providers,

    - a.trust's private withdrawn and destroyed.

2. The cost coverage of precautions amongst other are covered by partner warranties.

3. The certification practices of a.sign corporate describes the precautions, which are taken during cessation of operations, in particular those

   - for notification of the concerned persons and organizations,
   - for transferral of obligations to third parties and
   - that the revocation status of non-expired certificates is managed.

3.4.10 Compliance with legal regulations

a.trust acts in principle in compliance with legal regulations and in accordance with injunctions [SigG], especially are the following points ensured:

1. Important recordings are protected from loss, destruction and forgery.
2. The requirements of the data protection act are fulfilled.
3. Necessary technical and organizational measures are taken to protect personal data from unauthorized and illegal processing as well as from unintended destruction or damage.
4. The certificate holder is ensured that a.trust provides the information openly in accordance with the agreement, with judicial resolution or on legal regulations basis.

3.4.11 Storage of a.sign corporate light certificates information

All information that is related to a.sign corporate light certificates is stored. In particular apply:

1. The current as well as the archived data is protected for privacy and integrity.
2. All data of a.sign corporate light certificates are archived completely, confidentially and in compliance with the published certification practices.
3. Recordings, which concerns a.sign corporate light certificates, are made available as evidence of ordinary certification in the context of judicial disputes. Additionally, the certificate holder provides access to other personal data, which concerns him, during registration.

4. The recordings cover also the exact time of important events, in conjunction with the system environment, when key and the certificate management were performed.

5. All data, which is related to a.sign corporate light certificates must be stored electronically at least seven years, unless another time period is explicitly stated.

6. All recordings take place in such a way that they cannot be deleted or destroyed easily or unintended within the storage period.

7. The specific events and data, which must be logged, are documented in the certification practices.

8. In particular all registration information, including the one used for certificate renewal, is stored electronically.

9. The privacy of the certificate holders' data is ensured.

10. All events, which concern the life cycles of a.trust keys, are logged.

11. All events, which concern the life cycles of a.trust certificates, are logged.

12. All revocation requests and related information are logged.

3.5 Organizational

a.trust is reliable as organization and adheres strictly to the aforementioned guidelines in the following chapters (see 3.5.1 and 3.5.2).

3.5.1 General

1. All guidelines and procedures are non-discriminating.

2. The services of a.trust in context of a.sign corporate light are at the disposal to organizations which operate servers.

3. a.trust is a legal entity (limited company).

4. a.trust possesses systems for quality assurance and guarantees of information security, which are appropriate for the offered certification services.

5. a.trust adheres to the regulations in § 2 [SigV] regarding the financial situation.

6. According to the regulations [SigG] (see also chapter 3.4.3), the personnel employed with a.trust has the necessary training, technical knowledge, experience and is appropriately staffed in order to be able to manage the planned scope of the certification services.

7. There are guidelines and procedures available for treatment of complaints and disputes, which are submitted to a.trust from customers or other parties who are concerned by a.trust's services.

8. The legal relations with subcontractors, which provides services to a.trust, are documented in detail and are contractually regulated.

9. There are no records of law violations held against a.trust.

3.5.2 Certificate issuance and revocation services

The organizational units intended for the provisioning of certification and revocation services are independent of other companies regarding their decisions over the provisioning, maintenance and completion of the services of a.trust. The management and the personnel, which possess sensitive and leading functions, are free from commercial, financial and other pressures, which could have negative effects on the reliability of their activities.

The units intended for the certification and revocation services have a documented structure, which ensures the impartiality of the task execution.

4Appendix

A Terms and abbreviations

a.sign corporate light certificate	A not Qualified Certificate, which is issued to a server.
Certificate Policy, Policy	A set of rules, which defines the use of a certificate for a certain user group and/or application class.
Certificate revocation list, CRL	A digitally signed data structure, which states the recalled certificates issued by a certain certification service provider.
Certification service provider, Certification Authority, CA	A person or place, which issues certificates or offers other electronic signature services to the public.
Compromising	Unauthorized disclosure or lost control of sensitive information and data which must be kept secret.
CPS, Certification Practice Statement	Statements of the procedures for the issuance of certificates by a certification service provider.
Certification practices	See CPS.
Digital signature	Electronic signature, which is created by means of asymmetric cryptography.
Email	Electronic mail; messages, which are received or dispatched in digital form over computer-based communication channels.
Electronic signature	A signature in digital form, which is contained in data, is attached to data, or is logically linked to it, and is used by a signer in order to confirm that he approves the contents of these data. Hence, it is associated with the data that a subsequent change of data is obvious.
Integrity (of data)	A condition, in which data was neither destroyed nor changed by unauthorized persons.
Key-pair	A private key and the associated public key. Dependent on the used algorithm it is possible to use the public key to verify a digital signature that was created with the private key, and/or use the private key data to decrypt data that was encrypted with the associated public key.
OCSP	Online Certificate Status Protocol
Private key, secret key	Secret part of a key-pair, which is used for creation of digital signatures as well as for decryption of messages/documents, and must be kept secret.

Public key	Public part of a key-pair. It is a component of a certificate, and is used for validation of digital signatures and/or for encryption of messages/data.
Public-key system	A cryptographic system, which uses a key-pair in conjunction with a mathematical algorithm. The public part of this key-pair can be made accessible to everyone who wants to encrypt information or validate a digital signature, while the secret part is retained securely by its owner and can be used to decrypt data or create a digital signature.
Qualified Certificate	Certificate, which complies to the regulations of § 5 [SigG].
Registration place, Registration Authority, RA	A trustworthy mechanism, which validates the identity of the certificate applicants on behalf of the certification service provider with consideration of the certification practices and issues no certificates itself.
Revocation	The irreversible procedure of the early termination of a certificate's validity starting from a certain time.
Signature creation device	Component the signer uses to create an electronic signature.
SSL	Secure Socket Layer, a protocol for secured transmission of data over the Internet with use of a public-key system.
Verification (of a digital signature)	Clarification that a digital signature was created with the private key, which was associated with the public key in a valid certificate, and that the message has not been altered after the signature was created.
X.509	The ITU standard for certificates. X.509 v3 describes certificates that can be provided with certain certificate extensions.

B Reference documents

[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. (Directive 1999/93 EC of the European Parliament and the Council on a community framework for electronic signatures, 12/13/1999)
[DSG]	Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000). BGBl. I Nr. 165/1999 (NR: GP XX RV 1613 AB 2028 S. 179. BR: 5992 AB 6034 S. 657.)
[CPS]	a.trust Certification Practice Statement for simple a.sign corporate certificates
[BWG99]	Bundesgesetz über das Bankwesen (Bankwesengesetz - BWG). BGBl. I Nr. 123/1999 (NR: GP XX RV 1793 AB 1894 S. 175. BR: 5966 AB 5978 S. 656.)
[ETSI]	Policy requirements for certification authorities issuing qualified certificates – ETSI TS 101 456
[RFC3647]	RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003