ARGE DATEN

A-CERT Certificate Policy

[valid for A-CERT ADVANCED certificates for simple and advanced signatures]

Version 1.5/Juni 07 - a-cert-certificate-policy.english.last.doc
OID-Nummer: 1.2.40.0.24.1.1.1.12

ARGE DATEN - Österr. Gesellschaft für Datenschutz A-1160 Wien, Redtenbacherg. 20 ☎ +43/676/9107032, Fax +43/1/4803209
www.argedaten.at DVR 0530794 info@argedaten.at Gerichtsstand Wien
ZVR 774004629 UID ATU 56627966 PSK 7.214.741 (BLZ 60000, IBAN: AT15 6000 0000 0721 4741, BIC: OPSKATWW)

CONTENTS:

APPENDIX:

CN = Mag. Dr. Hans G. Zeger, Abwicklung A-CERT-Service, C = AT, L = Wien, S = Wien, O = ARGE DATEN - Österreichische Gesellschaft für Datenschutz
2009.08.03 14:45:00 +02'00'

I. DOCUMENTATION OF MODIFICATIONS

A. CHANGES 12 APRIL 2007

- Added ETSI 102 042 conformity statement.
- Clarified the secure storage of private keys with respect to simple signatures (e.g. A-CERT CLIENT)
- Additions to private key storage in the signature-creation device.
- Rules for including information about the signature-creation device as a X.509v3 extension in the certificate and as additional information in the directory service.
- More precise seperation of issuer and certification service.
- Assigned an OID number to the english translation of this policy.
- Correction of spelling and enumeration errors.

B. CHANGES 12 DEZEMBER 2005

- The OID number of this document was added to the cover sheet.
- The retention period of the certification documentation is set at 35 years.
- Test certificates and a OID number identifying them are defined.
- A X.509v3 extension to identify test certificates is defined.
- The revocation facilities of the issuer are extended.
- Correction of spelling and enumeration errors.

C. CHANGES 4 OKTOBER 2004

- Additions to the identity check of the signatory.

D. CHANGES 22 SEPTEMBER 2004

- Additions to the private key generation by the signatory.

E. ORIGINAL VERSION 11 SEPTEMBER 2004

II. BASICS

A. DEFINITIONS AND ABBREVIATIONS

Issuer
Issuer of this certificate policy is ARGE DATEN - the Austrian Society for Data Protection.

A-CERT
Is the collective term for all of the issuer's certification services. Different certification services are specified through additions to the term "A-CERT". The A-CERT website's address is: www.a-cert.at.

Policy
The term used for the certificate-policy in this document is "policy". This policy is the frame for the provision of all certification services by the issuer. This frame cannot be expanded. To restrict the applicability of this policy to specific certification-cases and signing procedures is however possible after agreement. The issuer's terms and conditions or additional agreements of contracting parties cannot overrule this policy. This document describes the policy validated for A-CERT ADVANCED with the OID-Number 1.2.40.0.24.1.1.1.3. Historical versions of this document can be accessed with the OID-Number 1.2.40.0.24.1.1.1.99.at the control authority. If necessary, the policy will be translated and provided in other languages.

Test-certificates
The term is used for certificates, based on the X.509-standard, that are issued to third parties for testing.
Signatories or requesters do not need to undergo an identity-check. Test-certificates fulfil at least one of the following criteria:
- the issuer's **CN-entry** is **A-CERT FREECERT or A-CERT GOVERNMENT TEST**,
- the subject's **O-entry** has the leading remark "Test" (for organisations) or "Testzertifikat" (for individuals),
- the certificate has the additional X.509v3 extension **1.2.40.0.24.4.1.0=DER:01:01:FF** (test-property=TRUE).

The characteristics of a test-certificate can appear in arbitrary combinations. For these certificates applies the deviating certificate policy for testing (OID-Number: 1.2.40.0.24.1.1.4.1).

Requester
The signatory, who on the basis of this policy, the issuer's terms and conditions, and possible additional terms of contracting parties files a request for issuing a certificate, is called requester.

Registration authority
The term is used for the issuer's agencies and other persons and agencies authorised by the issuer to accept and authorise certification requests.

Signature regulations
The entirety of all regulations, adopted in the documents [SigG] (=Austrian Signature Act), [SigV] (=Austrian Signature Regulation), [SigRL] (=EU-signature directive).

Control authority
The control authority responsible for A-CERT certification services.

Confirmation authority
The Austrian confirmation authority, set up according to the Austrian Signature Act [SigG]. In other countries, the confirmation authority is set up according to legal terms based on the EU-Directive 1999/93/EG for secure signature-creation devices.(§18 Abs.5,Phrase 3 SigG).

Furthermore the terms according SigG, SigV, SigRL, X.509 and the RFCs 3280 and 3647 are used.

B. OVERVIEW

The present certification policy comprises all regulations for issuing certificates for simple and advanced signatures. The certificates conform to the definition §2 para. 8 [SigG]. The certificate policy conforms to the “Normalized Certificate Policy” profile in [ETSI TS 102 042].

This policy was written in accordance with the signature regulations. Together with the issuer's terms and conditions and the notification of the control authority this policy lays the foundation for the use of A-CERT certificates by the signatory.

Alterations following modifications in legal requirements, are effective when the legal requirements come into effect, other alterations are effective four weeks after publication on the A-CERT homepage.

C. AREA OF APPLICATION

This certification policy applies to all certificates, that were issued for simple or advanced signatures. Further this policy applies to all services, that are operated by the issuer by means of using A-CERT certificates.

The issued certificates can be used by the issuer to perform signature and secrecy operations and also to sign single electronic documents (files).

Certificates that are issued on the basis of this policy can also be used for generating signatures under §2 Z 3 lit.a to d [SigG].

III. COMMITMENTS AND TERMS OF LIABILITIES

A. THE ISSUER'S COMMITMENTS

The issuer is committed to insure that all requirements laid down in section III of this document are fulfilled.

The issuer is responsible for conforming to all directives, that are described in this present policy; this also applies to functions using operations that were outsourced to contracting parties, (e.g. maintaining a directory service, distribution and identity check). No additional commitments are made directly or by reference in the certificates.

Certificates for keys that were generated with procedures that are no longer considered safe according to the signature regulations or the control authority's decision or accredited standardisation committees (especially according to the special recommendation ETSI SR 002 176 or ETSI TS 102 176) are revoked by the issuer.

The issuer reserves his right to revoke certificates if the procedures that were used are no longer considered safe according to internal findings or if the certificate's contents are misleading or incomplete.

If the issuer revokes a certificate before expiry of the validity provided in the contract, the signatory is entitled to receive an equivalent certificate which is generated using safe procedures for the remaining duration of his/her contract. Additional compensations and reimbursements are not provided.

B. THE SIGNATORY'S COMMITMENTS

The signatory is bound by the issuer's contract to fulfil the following commitments.

The requester can access all terms of the contract via the issuer's homepage. When submitting the order form, the requester confirms the notice and acceptance of these terms.

The signatory's commitments comprise:

1. The provision of complete and correct information in accordance with the requirements of this policy, especially during the registration procedure.
2. The generation and storage of the private key in a hardware unit that can be accessed exclusively by the signatory (i.e. saving the private key in encrypted form with the use of a password or passphrase, specific signature-creation devices that prevent or hamper the extraction of the key).

In the case of simple signatures, for example A-CERT CLIENT, also access restrictions and organisational measures that limit access to the computer containing the certificate are regarded as adequate security measures with respect to this policy.

3. The private key must be generated by means of adequate secure procedures, that guarantee high random quality when generating the key (i.e. hardware-components that are especially designed for key generation like HSM modules or software-components that use system events to improve the randomness (e.g. files containing random numbers, mouse movements or keyboard entries). The issuer reserves his right to demand complete information from the requester about the procedure used for key generation and in case of doubts about the random quality to dismiss the request. Inadequate procedures for key generation are published on the A-CERT website, they must not be used.
4. Caution must be applied to prevent the unauthorised use of the private key and after expiry of the validity period, the key must be destroyed.
5. The issuer must be notified immediately if one of the following conditions occurs before expiry of the validity period:
   - the signatory's private key was possibly compromised,
   - control about the private key was lost,
   - the information contained in the certificate is wrong or has changed,
   - further use of the key according to this policy is no longer permitted.
6. The secure storage of the key is exclusively the signatory's responsibility.

As long as the private key is saved on external data storage media (i.e. disc, USB-Stick, hard drive...) that can be read out, the signatory is obliged to carefully store the data storage media and to store the password in an alternative location. Transportable data storage media (Disc, USB-Stick, CD) must be stored in locked containers that can only be accessed by the signatory. In the case of built in data storage media (e.g. hard drives) access must be limited to the signatory. System administrators must be obliged to secure the integrity of the private key. All copies or backups of the private key must have the signatory's authorisation.

Further the signatory assures that the data media in use is free of malicious programs that could extract, copy, or modify the private key. In particular, the signatory uses safety precautions, against worms, viruses, trapdoor programs and spyware.

C. THE RECIPIENT'S COMMITMENTS

The issuer's certificates are only valid within the frame of this policy, therefore recipients of certificates must take the following verification steps:

- The validity period and the revocation status must be investigated by using the services provided by the issuer.

- The limitations concerning the use of the certificate that are laid down in the issuer's terms and conditions must be taken into account.

In case of doubt about the validity of the certificate, the issuer must be notified. In these cases appropriate measures are taken to clarify the certificate's validity.

D. LIABILITIES

The issuer is liable for

- the abidance of this policy in respect to the revocation procedure, especially for promptly publishing the updated revocation list and to obey the revocation standards (ITU X.509v2) as laid down in this policy.
- examining the requester's data at the time when the certificate is issued, and to ensure that there are no discrepancies between the given data and the data in authorised directories. Examination measures are documented in this policy. Which authorised directory is used depends on the type of request made. Sources can differ factually and regionally. Which sources to use for which type of request is laid down in detail in the internal process documentation.

The issuer is not liable for breaches of these commitments if he can prove that they were not his fault.

IV. SPECIFICATIONS FOR PROVIDING CERTIFICATION SERVICES

A. GENERAL

This policy applies to the following specified services: provision of registration services, generation of certificates, issuing of certificates, revocation services, certificate status query services.

B. OPERATIONAL MEASURES FOR PROVIDING CERTIFICATION SERVICES

To provide correct and traceable step by step certification procedures the following measures have been taken:

1. All procedures necessary for the certification are documented in detail by the issuer.
2. This certification policy, the issuer‘s terms and conditions, as well as detailed information about all provided services are accessible at the issuer‘s website.
3. The issuer's board of directors approves all necessary documentation and certification policies and appoints the staff and external contracting parties, who are responsible for the operational implementation of this policy. The appointments are documented in writing.
4. The issuer's board of directors decides where the certification takes place.
5. Any changes of the certification policy are published on the issuer‘s website. Holders of certificates are notified about the changes using e-mail (if available).
6. The event logs pertaining to the operation of the certification services are retained for 35 years.

C. KEY ADMINISTRATION

1. GENERATION OF CA KEYS

The keys necessary for the provision of certification services according to this policy are generated in a dedicated system by 'two sets of eyes'.

All algorithms and key lengths used are included in the announcement submitted to the Telekom-Control-Kommission, the Austrian Telecommunications Control Authority.

2. CA KEY STORAGE

The key is stored in the system which is designed for conduction of the certification procedure. A backup copy is stored in an external vault. The two passphrases, which are necessary for the use of the key are stored separately by two members of staff.

3. DISTRIBUTION OF THE PUBLIC CA-KEYS

The issuer applies the following measures regarding distribution to guarantee the integrity and authenticity of the public keys:
- The root key is sent to the control authority for publication in the form of a signed PKCS#10 certificate request.
- A self-signed root certificate is issued and published.

The certificate of the CA key can be accessed by the signatory through the directory service. The issuer guarantees the authenticity of this certificate.

4. KEY DISCLOSURE

The private/secret key is not published..

5. USAGE OF CA-KEYS

The private key of the certification authority is used exclusively for issuing certificates that are explicitly intended for this purpose, and for signing the corresponding revocation lists within the locations dedicated to the certification procedure.

6. END OF THE VALIDITY PERIOD OF CA KEYS

Secret keys for signing certificates can be used as long as the key's algorithms are safe according to II.A of this policy. Keys that no longer conform to the safety requirements laid out in this policy, or that for other reasons are no longer in use are deleted and are not archived thereafter.

7. KEY GENERATION FOR SIGNATORIES

Depending on the specific certification service, signatories' keys are generated by the signatories, by the issuer or through a method chosen by the signatory. The control authority is notified about the chosen method when the specific service is submitted.

8. STORAGE OF THE PRIVATE KEY IN A HARDWARE SECURITY MODULE

If special hardware components that prevent the extraction of the private key are used as signature-creation devices , these components can either be evaluated by a ratification authority or their adequacy asserted by the manufacturer.

The use of signature generation units of this type can be incorporated in the certificate as an X.509v3 extension in two different forms:
- Issuer-supplied
- Signatory-specified

a) ISSUER-SUPPLIED HSMS

The private key is generated by the issuer in a special signature generation unit. The key is only provided in this signature-creation device – no copy of the private key in any other form exists.

The corresponding certificate then contains the following X.509v3 extension:
1.2.40.0.24.4.1.1: <hardware used>

„<hardware used>“ is the commercial denomination or the denomination used by a ratification authority to identify the used hardware components, e.g. „Aladdin eToken PRO64k“ for a USB token manufactured by the company Aladdin containing the evaluated component „CardOS V4.2 CNS with Application for Digital Signature“ produced by the company Siemens.

The currently supported hardware components, the names of the ratification authorities and the legal regulations under which evaluations take place can be found at the issuer’s website.

If the certificate is published in the issuer’s LDAP directory service, the name of the hardware used is stored in the attribute **acertIssuerInfo**.

b) SIGNATORY-SPECIFIED HSMS

The signatory specifies the hardware he/she used to generate the private key.

This information is checked by the issuer insofar that it is verified whether the product specified by the signatory is really qualified to store a private key. The basis for this verification is information supplied by the hardware manufacturer or in reports published by ratification authorities.

The corresponding certificate then contains the following X.509v3 extension:
1.2.40.0.24.4.1.2: <hardware used>

„<hardware used>“ is the commercial denomination or the denomination used by a ratification authority to identify the used hardware components.

If the certificate is published in the issuer's LDAP directory service, the name of the hardware used is stored in the attribute **acertSignerInfo**.

c) CONCLUSION

If both X509v3 extensions are not present in the certificate, the terms of storage in section „The Signatory's Commitments" apply.

D. REQUESTER'S CERTIFICATES

1. FILING A REQUEST

Certification requests can be filed online as well as offline.

The measures and procedures for confirming the requester's identity and registration depend on the specific certification service. They can differ factually or regionally.

The requester's identification procedure is completed if there is no justified doubt about his/her identity. To successfully conclude the identification procedures, a document authenticated by a notary or court or a written confirmation by an authorised member of the issuer's staff is needed.

This policy describes the basic steps of the identification procedure, Individual cases may need some variations because of factual or legal reasons.

1. Before the contract between the signatory and the issuer is closed, the signatory receives the terms and conditions and other possible terms in electronic form.
2. The request-form and all information can be accessed through the website of the issuer or the contracting party.
3. The certification request covers the following minimal information:
   The complete name and address of the signatory.
4. Additional details about the signatory's person:
   telephone number, fax number, eMail address, details about profession and qualification, additional contact data (if needed). Depending on the certification service some information may be optional or obligatory. As long as the signatory is a natural person the card-number and details about the issuing authority of his/her official identity card must be submitted. The issuer demands the original document, a certified copy or alternatively a copy of the identity card. Certified copies of a document must be handed in as an original copy.
5. Additional data about the organisation the requester represents:
   If a person requests a certificate to perform acts of legal significance for an organisation or another person, the

following additional information must be provided: The organisation's / person's name and address, and the legal form of the organisation (i.e. incorporated society, registered company). Additionally, at least one authority must be named that is responsible to confirm the legal status of the organisation (register of associations, Chamber of Commerce...). All state-run authorities that keep directories of organisations which are accessible to the general public can confirm the legal status, as long as they examine the organisation's identity before listing. Organisations that are set up according to law must quote the relevant text of the law. To verify the address data, the official telephone directory or the directory of public authorities is used. Organisations without official registration or legal regulation are treated equally to private persons. Details about such organisations are considered like optional information comparable to the profession or qualification of a private person.
Additionally the signatory must state in which areas he has the power of representation (if necessary the scope of power can be limited in terms of the amount or procedure).

6. Information about the certificate's purpose:
   The details about the purpose can be optional or obligatory depending on the service offered.
7. Acceptance of approval to of the issuer's terms and conditions, this policy, and possibly to additional agreements concerning the certification procedures.
8. The requester has to submit an activation password that is required before access to the personal certificate and the private key, after completion of the certification process, is granted.

2. EXAMINATION OF THE REQUEST

The certificate authority carries out the following examinations of the request:

- verifying the organisation data by matching the information with trustworthy databases or information given directly by the organisation's control-authority,
- verifying the requester's power of representation within the organisation,

- The identity-check is completed after the person hands in the request personally together with an official identity document or a certified copy of the document in its original version in one of the issuer's offices. In all other cases, the identity check is completed using the procedure outlined in „Handling the request“.

The issuer reserves to himself to carry through additional verifications if

- the control-authority cannot provide information to verify the organisation's data,

- there are justified doubts whether the requester is entitled to use certain elements of numbers or names i.e. domain names,
- the power of representation is not documented adequately,
- there are other contradictions in the request.

3. HANDLING THE REQUEST

To guarantee the signatory's identity, a certification-confirmation is issued and delivered after certification.

Depending on the certification request the confirmation is delivered in
- a standard letter
- a registered letter with a return receipt to be signed personally, if the identity check needs to be completed

The registered letter with a return receipt to be signed personally, must be handed personally to the requester as laid down in the Austrian Post‘s delivery-regulations. The receipt of the letter is confirmed by means of the return receipt that carries the requestor's signature.
The recipient signs the certificate-confirmation and returns it per fax to the certificate authority.

As soon as the signed certificate confirmation letter is back at the certificate authority's office, the access to the download area of the requester's certificate and the private key (if requested) is activated. To access this information the requester needs to fill in his activation password and the reference number that he received in the confirmation letter.

These measures guarantee that the requester's identity is definitely verified and the complete handling of the request can be attributed to a single person.

4. REQUEST ARCHIVAL

The certification request and all data that were submitted on paper or electronically with the request are archived on paper or electronically for at least 35 years after the certificate's validity expires.
Private keys, in the case that the issuer has generated the private key for the signatory, are deleted after the signatory has downloaded the key and confirmed its reception.

5. CERTIFICATE GENERATION

The issuer generates certificates according to the notification given to the control authority. Certificates have X.509v3 format or PGP format.

The unambiguous attribution of the certificate to the signatory is secured by:

- The filing of the PKCS#10-request (for X509v3 certificates) or the PGP-request (for PGP-certificates) as the basis for the certification,
- The generation of the certificate after the registration authority has examined all data that were submitted in the request.

The registration authority collects and signs all data and transmits it over an encrypted channel (SSL) to the certification authority. This procedure guarantees confidentiality and integrity of all data.

Certificates for testing purposes carry the X.509v3 extension "certificate for testing only", 1.2.40.0.24.4.1.0=TRUE.

6. CERTIFICATE CONTENT

Content and technical description of the certificate can be reviewed in the notification of the service.

7. EXTENSION OF A CERTIFICATE'S VALIDITY, GENERATION OF ADDITIONAL CERTIFICATES AND CERTIFICATE REGENERATION

The following measures ensure that new requests of signatories that are already registered with the certification authority because of earlier certificates that were issued to these requesters can be authorised completely and correctly.

These measures are applicable for the extension of the certificate's validity as well as the generation of additional equivalent certificates, as well as for the regeneration of a certificate after expiry or revocation.

- The registration authority examines all data in the certificate and verifies that the information is not out of date.
- Any changes in the certification policy or the terms and conditions are sent to the requester.

E. PUBLICATION OF THE TERMS OF CONTRACT

The issuer informs all signatories and users who trust in the reliability of A-CERT services about the specific conditions for the use of each certificate by publishing the following documents on the A-CERT website.

1. the current certification policy,
2. the terms and conditions,
3. additional descriptions about the specific services,
4. a link to the notification of the certification service at the control authority's website,
5. other information.

Changes are displayed at the A-CERT website and in some cases certificate holders are notified per eMail or per letter.

F. CERTIFICATE PUBLICATION

In general, all certificates that are issued by this certification authority are made available to signatories and others who need to inspect the signature:

1. All certificates are published through the issuer's directory service. Details concerning its use are published on the A-CERT website.
2. The conditions for the use of any certificate are announced in this policy.
4. The directory service is available seven days a week, 24 hours a day. Interruptions of more than 24 hours are documented as incidents.
5. The directory services are public and accessible world-wide.

A listing in the directory service can be avoided on the signatory's demand and if the specific certification service permits it (essential is the wording in the notification that was submitted to the control authority).

Certificates that are not publicly available through the directory service are disclosed to applicants who can accredit a legal interest.

G. REVOCATION

To insure a practical use of certificates, a two-step revocation concept is applied.

Provisional revocation is effective immediately, even if the identity check cannot be completed. The reason for the revocation is mentioned in the revocation list. Then, the signatory is informed about the revocation and asked to either confirm or cancel the provisional revocation.

The provisional revocation becomes an irreversible revocation if the confirmation of the revocation arrives within 3 working days; alternatively, if no cancellation of the revocation is demanded.

The revocation is irreversible after the identity-check is completed. Consequently, the certificate’s validity expires early.

The signatory is entitled to revoke his/her certificate. In the case that the signatory acts per procurationem for a person or an organisation, this person or appointed representatives of this organisation are entitled to revoke the certificate.

A revocation request can be submitted informally by submitting data that identifies the certificate (e.g. product name, serial number, fingerprint). Requests per phone, fax, letter or eMail are accepted during working hours Monday to Friday between 9 a.m. and 5 p.m. Revocations via http are accepted at any time, and if

sufficiently specified, they are dealt with immediately and automated (other cases are treated as eMails).

The provisional revocation is effective within one hour after arrival of the revocation request.

The revocation lists that are accessible via Internet are updated automatically after every revocation, otherwise after 30 days.

The directory services for revocation lists are publicly accessible world-wide.

It is not possible to prevent the publication of revoked certificates.

H. REVOCATION CONTENT

The content of the revocation list can be reviewed in the notification of the specific certification service from the control authority.

V. COMPANY ORGANISATION

A. SECURITY MANAGEMENT

The issuer is responsible for all processes that take place as part of the certification service; this also applies to services that are outsourced to contractual partners. The responsibilities of the contractual partners, as well as mechanisms to review the proper fulfilment, are clearly defined. Those procedures that pertain to security are published in this policy.

The issuer's company infrastructure undergoes perpetual examination and is adapted to changing requirements. All changes that influence the level of security have to be authorised by the issuer's board of directors.

All security measures and all functions that pertain to the provision of the certification services are documented. They are implemented and maintained according to this documentation.

The technical operation takes place at the premises of the issuer or at adequately qualified contractual partners. The current contractual partners are announced to the control authority and published on the A-CERT website. All contractual partners are contractually bound to protect the security of data in terms of this policy, the DSG 2000 and the signature regulations.

Four levels of security are introduced that correspond to appropriate operational security measures:

- Level public: Comprises all data that is intended or adequate for publication. The access to this data is not limited by the issuer. Measures to secure availability and integrity of the data are taken.

All other levels of security contain data that are not intended for publication. Access to this data is restricted to those employees that are intended to work with this data. Restrictions also apply to the measures taken to provide availability and data integrity.

- - Level administration: Comprises all data that are necessary for the administrational control of the business. This includes internal documentation, accounting, customer administration, billing.

- Level system administration: Comprises all data that are necessary for the maintenance and upkeep of the IT services.

- Level security: Comprises all data that are subject to special processes, in particular data that has a direct connection to key generation and certification.

B. ACCESS CONTROL

A system for user administration that grants different access rights to different functions is established; in particular, functions that pertain to security are carefully separated from functions that do not have relevance for security considerations. All technical processes that are directly concerned with the certification are secured from unauthorised access by requiring

- physical access to certain securely stored hardware components and/o
- one to two passwords.

The individual requirements of every process are documented.

The internal network is protected from unauthorised access by firewalls.

Confidential data is protected through encryption before being transmitted over insecure networks.

Changes in access rights are implemented into the system immediately. The review of the user administration is part of the internal audit.

Access to information and applications is restricted by the access rights. Administrative and operational processes are separated.

Authentication is necessary for the personnel before critical access to applications that are connected to the certificate management is possible.

Application access is recorded in log files. The personnel is held to account for the actions taken.

Changes (Deletions, Additions) to the directory and revocation services are secured through a signature of the certification service.

Unauthorised connection attempts to the directory and revocation services are recorded.

The system administrators and other personnel are obligated to observe the data security regulations according to DSG 2000 §14.

C. PERSONELL SECURITY MEASURES

The issuer's employees are qualified personnel and as such especially capable of implementing and guaranteeing the regulations presented in this policy.

- Functions and responsibilities pertaining to security are documented in the job description. Those functions on which the security of the certification services depends are explicitly identified.
- Precise job descriptions for the personnel of the issuer are laid down. In these job descriptions, duties, access rights and competencies are formulated.
- All leadership functions are occupied by persons that have experience with digital signatures, encryption and the management of personnel that is responsible for carrying out security-critical actions.
- Corresponding to § 10 para. 4 [SigV], the issuer does not employ any persons that have committed criminal acts that make them appear unfit to hold a position of trust.

D. PHYSICAL AND ORGANISATIONAL SECURITY MEASURES

It is ensured that the access to premises in which security-critical functions are carried out is restricted and the risks of physical damage to equipment is minimised.

In particular:

1. The access to equipment with which certification and revocation services are performed is restricted to authorised personnel. The systems that issue certificates are protected from environmental disasters through constructional measures.
2. Measures are taken to prevent the loss, damage or compromise of equipment and the disruption of services.
3. Further measures ensure that a compromise or theft of data equipment and data processing equipment is not possible.
4. The systems that perform generation of certificates and revocation services are operated in a secure environment by means of technical and organisational measures that prevent a compromise through unauthorised access.
5. The separation of systems that perform certificate generation and revocation services is carried out through explicitly defined security zones (i.e. spatial separation from other organisational units and physical admission control).
6. The security measures include the protection of the premises, the computer systems themselves and all other equipment that is necessary for their operation. The protection of the facilities used for certificate generation and provision of revocation services comprises physical access control, prevention of dangers evoked by natural forces, fire, flooding, and collapse of buildings, protection from failure of supply units as well as theft, burglary and system outage.
7. The unauthorised removal of information, media, software, and fixtures that belong to the certification services, are prevented through control measures.

E. PERPETUAL OPERATIONAL MEASURES

1. Damage through security-critical incidents and malfunctions are detected at an early stage, prevented or at least minimised by means of records and error recovery procedures.
2. Media are protected from damage, theft and unauthorised access.
3. Detailed processes are used to carry out security-critical and administrative tasks that influence the provision of the certification services.
4. Media are dealt with and stored according to their security levels. Obsolete media that contain confidential data are destroyed in a secure way.
5. The integrity of computer systems and information is protected from viruses and malicious or unauthorised software.
6. Capacity requirements are observed and future developments are forecast to allow provision of adequate bandwidth, processing power and other IT resources.
7. The security-critical functions pertaining to certification and revocation services are strictly separated from administrative functions. Security-critical functions are all IT measures that serve the sustainment of the certification service. In particular, these are
   - planning and technical approval of security systems,
   - protection from malicious software and attacks,
   - active review of log files and test reports, analysis of incidents,
   - general system maintenance tasks,
   - network administration,
   - data management, media management and security,
   - software updates.

The inspection of security-critical functions is performed by a security officer nominated by the board of directors.

F. SYSTEM DEVELOPMENT

The processes necessary to provision the certification services are perpetually enhanced and optimised. Besides maximising the security of the system, the customer's ease of use determines the further development of the system.

The operational software modules are digitally signed to allow immediate identification of undesired changes.

Transfer procedures exist that allow installation of new software modules.

G. PRESERVATION OF UNINTERRUPTED SERVICE AND TREATMENT OF INCIDENTS

Technical, structural and organisational security measures like redundant system connections, emergency power supply and fire protection exist to prevent physical disruptions. In the case of

total destruction of the primary site, these measures allow resumption of services within a workday.

The compromise of a certification key is viewed as the worst-case scenario. In this case the issuer notifies the control authority (in accordance with § 6 para. 6 [SigG]), the signatories, the persons that trust the dependability of the certification services and, if applicable, other certification service providers with whom agreements exist that the revocation and certificate information can not be regarded as reliable anymore.

Certificates and revocation lists are marked as invalid. Using a newly generated secure certification key, new certificates are issued to the signatories.

VI. MISCELLANEOUS

A. CESSATION OF OPERATION

In accordance with §12 SigG the issuer will immediately notify the control authority of the cessation of operation. He will ensure that possible disturbances of the services for signatories and for everybody who trusts in the issuer's services are minimised.

B. INFORMATION ACCORDING TO DSG 2000

In general, all data obtained for certification services are kept in confidence. They are only used for certification purposes and for communication concerning the issuer's certification services.

The signatory's data are only published to fulfil the requirements of specific certification services (directory service, revocation service) or on the signatory's explicit demand.

Legal obligations to store or transfer data will remain unaffected. Datatransfer acc. to §151 GewO to address-dealers is definitely ruled out.

APPENDIX

APPENDIX A: BIBLIOGRAPHY

[DSG 2000] Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000). BGBl. I Nr. 165/1999

[ETSI] ETSI SR 002 176 V1.1.1 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures

[ETSI TS 102 042] ETSI TS 102 042 V1.1.1 (2002-04) Policy requirements for certification authorities issuing public key certificates

[POS] RTR GmbH, Positionspapier zu § 2 Z 3 lit. a bis d SigG („fortgeschrittene elektronische Signatur“), Version 1.0, 13.4.2004

[RFC3280] RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002

[RFC3647] RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003[RFC3671] RFC 3671, Collective Attributes in the Lightweight Directory Access Protocol (LDAP), Dezember 2003

[RFC3672] RFC 3672, Subentries in the Lightweight Directory Access Protocol (LDAP), Dezember 2003

[RFC3673] RFC 3673, Lightweight Directory Access Protocol version 3 (LDAPv3), Dezember 2003

[RFC3377] RFC 3377, Lightweight Directory Access Protocol (v3): Technical Specification, September 2002

[RFC1305] RFC 1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis (NTP), März 1992

[RFC3161] RFC 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), August 2001[SigG] Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG). BGBl. I Nr. 190/1999

[SigRL] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, 13.12.1999

[SigV] Verordnung zum Signaturgesetz, BGBl II 2000/30, 02. 02. 2000

[X.509] ITU-T Recommendation X.509, März 2000

APPENDIX B: DOCUMENT INFORMATION

AUTHOR(S):

Name	Version	Bearbeitung	Datei	Kommentar
	0	0	dokumentation-argedaten.dot	Template
Hans G. Zeger	1.1	11.09.04 10:38	a-cert-certificate-policy.doc	Original Version (german only)
Hans G. Zeger	1.2	22.09.2004	a-cert-certificate-policy.doc	Additions (german only)
Hans G. Zeger	1.3	04.10.2004	a-cert-certificate-policy.doc	Additions (german only)
Hans G. Zeger	1.4	30.08.2005	a-cert-certificate-policy.doc	See I. DOCUMENTATION OF MODIFICATIONS (german)
Hans G. Zeger	1.4	13.03.2007	a-cert-certificate-policy.doc	See I. DOCUMENTATION OF MODIFICATIONS (english)
Hans G. Zeger	1.5	12.04.2007	a-cert-certificate-policy.english.doc	See I. DOCUMENTATION OF MODIFICATIONS (english + german)