telekom control

Certification Practice Statement – Draft

The formal, official decision of the Telekom-Control Commission regarding its Certification Practice Statement (CPS) is not planned until the supervisory authority's public-key infrastructure has been implemented.

For the time being, only Sections 1, 4.7, 6.1 and 7 will be translated into English. The other sections will only be available in German.

Version 0.31 (Excerpts)

January 29, 2001

Austrian Supervisory Authority for Electronic Signatures
Telekom-Control Commission and Telekom-Control GmbH
Mariahilfer Strasse 77–79, A-1060 Vienna, Tel. (+43-1) 58058-0, Fax: 58058-9191
http://www.signatur.tkc.at, signatur@tkc.at

1. Introduction

1.1 Overview

This document contains the Certification Practice Statement (CPS) of the Telekom-Control Commission in its capacity as supervisory authority for electronic signatures in Austria.

This version of the document is an early-stage draft. The first valid version of the document will be Version 1.0.

1.2 Identification

Name of document: Certification Practice Statement, Version 0.31 (Excerpts), January 29, 2001.

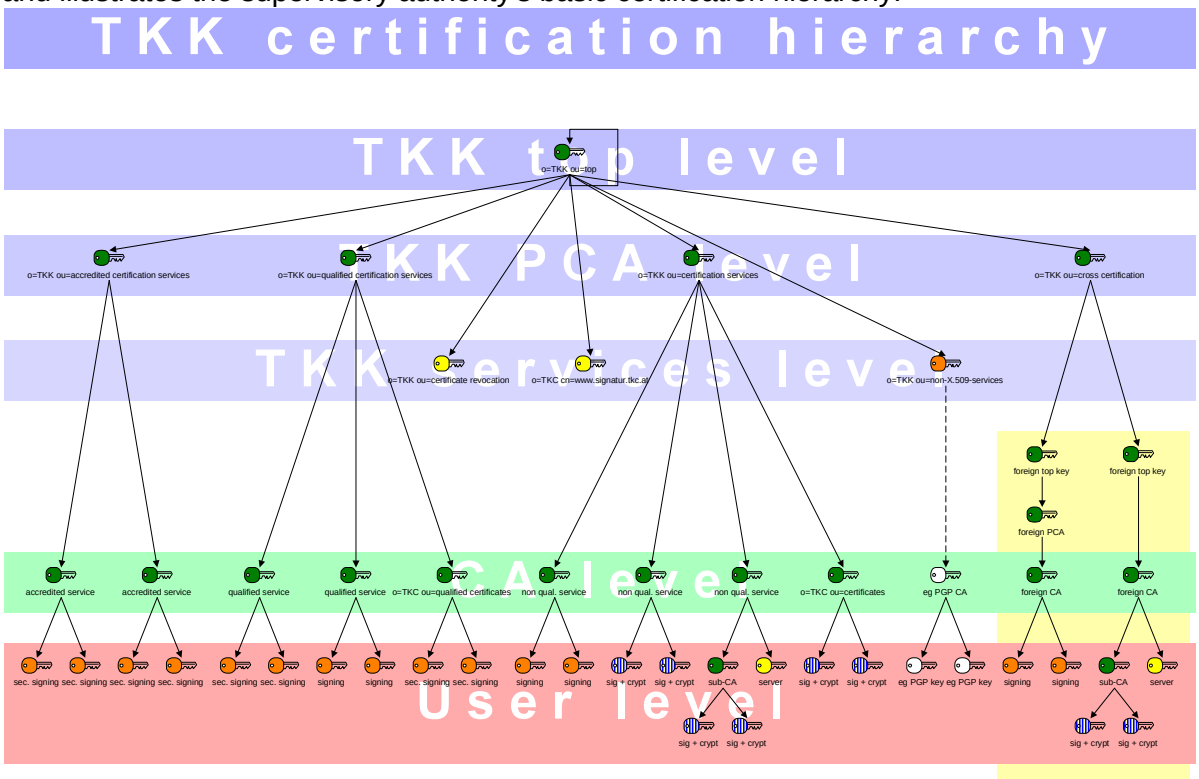
This document summarizes the essential content of the CPS issued by the Austrian supervisory authority for electronic signatures. The outline of this CPS follows the template given in the RFC 2527 standard (Chokhani/Ford, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, 1999). In addition, the CPS includes further components which will not be published (see 8.2).

The CPS will be published by Telekom-Control GmbH (as instructed by the supervisory authority for electronic signatures) under "Repository" at http://www.signatur.tkc.at/.

An ASN.1 Object Identifier will not be assigned to this document until Version 1.0.

1.3 Community and Applicability

The diagram below gives an overview of the supervisory authority's certification infrastructure and illustrates the supervisory authority's basic certification hierarchy.



Telekom-Control GmbH, 31.10.2000
Entwurf einer TKK-Zertifizierungshierarchie – Draft of a TKK certification hierarchy

The top key of the supervisory authority, as well as its predecessors and successors, is the only key located at the uppermost level (TKK top level).

The supervisory authority's policy certification authorities are located on the second level (TKK PCA level). The certificates issued to certification service providers for their certification services are signed with various PCA keys. The Accredited Certification Services key is used to sign certificates for certification services that have fulfilled all prerequisites for accreditation. The Qualified Certification Services key is used to sign certificates for certification services which issue qualified certificates. The Certification Services key is used to sign certificates for other (non-qualified) services. Another key is provided for cross-certification:

The third level (TKK services level) shows the supervisory authority's keys that are not intended for signing certificates. In some cases, lower security measures are provided for in these keys; in contrast to the keys of the first two levels, for example, they are not used exclusively offline). The supervisory authority's plans include a key for signing Certificate Revocation Lists (CRLs), a key for HTTPS access to the supervisory authority's directory service and a key for signing a list of providers to which an X.509 v3 certificate can not be issued for technical reasons. In addition, keys for the administration of directory, revocation and WWW services, and for the creation of secure time stamps in documentation are planned (the certificates belonging to such keys will only be published if they are of interest to the general public).

The keys of the various service providers are shown at the CA level, while those used by signatories and other users are depicted at the user level.

1.3.0 Certification Services of the Supervisory Authority

Certificates of the following classes will be issued by the supervisory authority. Each certificate class corresponds to a pair of keys, and the private key in the pair is used to sign certificates.

1.3.0.1 Top Certificates

Top Certificates will be signed using the supervisory authority's top key. Top Certificates are only issued for public keys whose corresponding private keys are under the exclusive control of Telekom-Control GmbH.

Top keys are also referred to as root keys. In accordance with IETF PKIX terminology and with the Austrian Justice Committee's considerations as to § 13 Par. 3 of the Austrian Signatures Act (SigG; see Brenn, *Signaturgesetz*, 102f), the term "top key" will be used (cf. also the term "main system" in § 3 Par. 1 of the Signatures Ordinance). This is intended to express the fact that the key is not to be seen as a central root which is to be generally trusted. The validity of an electronic signature can be checked independently of whether the supervisory authority's top key is trusted.

The top key is used exclusively to sign certificates for the following keys:

- Predecessors and successors to the top key (see 4.7.1).
- All of the supervisory authority's PCA keys (keys depicted on the second level, see 1.3 above).
- Keys for the other services of the supervisory authority, especially its certificate revocation keys (i.e., the keys used to sign CRLs; see 4.4).

- In addition, a self-signed certificate will be issued for each top key.

The top key will only be used to sign certificates for keys that are named in the current version of the supervisory authority's CPS. For information on later changes to the CPS, please refer to Section 8.

The currently valid top key and all PCA keys of the supervisory authority are located in a secure signature creation device on its premises. This key's predecessors are located in the same place, otherwise they have been destroyed. The certificates of the supervisory authority that refer to predecessors will be revoked. The successors to the valid keys are - as long as they are not yet valid - stored elsewhere. For more information on the supervisory authority's backup systems, please refer to 4.7.

In Top Certificates for predecessors and successors to the top key and for PCA keys, the only value to be set in the KeyUsage field is keyCertSign. These certificates therefore serve only to sign additional certificates. In Top Certificates for keys on the TKK services level, this bit is not set under any circumstances. These certificates can therefore not be used to sign other certificates. In certificates for the supervisory authority's certificate revocation keys, the only value set in the KeyUsage field is the cRLSign bit. These certificates thus serve the exclusive purpose of signing CRLs.

The supervisory authority reserves the right to add certification services in the future and to issue certificates for these services using its top key. A certificate signed with the supervisory authority's top key does not bear any significance as to the quality of all certificates below the top key in the supervisory authority's certification hierarchy. This hierarchy contains both qualified and non-qualified certification services, services subject to Austrian supervision and foreign services that are not subject to Austrian supervision. Certificates signed with the supervisory authority's top key merely signify that the certified key is under the exclusive control of the supervisory authority in accordance with its CPS.

The supervisory authority's top key is therefore not suited for selection as the root of trust for all certification services and certificates beneath it in the hierarchy. Its purpose is far more that of summarizing all of the supervisory authority's certification services and providing users with a uniform point of entry in the supervisory authority's certification hierarchy, from which the other keys in the certification hierarchy as well as - in the course of cross-certification - those of foreign supervisory authorities and certification services in particular can be reached securely. However, users who take the top key as a point of departure have to monitor the use of appropriate policy in each step of the certification hierarchy in order to decide whether or not to trust a certification service.

Section 2.1.4 discusses the extent to which the supervisory authority's Accredited Certification Services and Qualified Certification Services keys can be used as a basis for trusting certificates.

In the course of cross-certification, the supervisory authority's top key can be certified in order to minimize the effort and expense of the process. The supervisory authority will attempt to have each valid top key certified by as many other authorities as possible in order to optimize international networking.

1.3.0.2 Accredited Certification Services Certificates

These certificates are issued only to certification services that have been granted accreditation by the supervisory authority under § 17 SigG. Certification services providers that are accredited under § 17 SigG can also render other certification services in addition to the services for which they have fulfilled the accreditation prerequisites. However, Accredited

Certification Services Certificates will only be issued to providers for those certification services with which they have fulfilled the accreditation prerequisites.

Such a certificate will be issued by Telekom-Control GmbH in the name of the Telekom-Control Commission as soon as the official accreditation decision takes legal effect and all required fees have been paid. The certificate will be revoked if the accreditation is revoked, if the certification service provider's activities are prohibited under § 14 SigG, if the certification service provider reports a suspension of services (§ 12 SigG), if the provider changes the certified key, or if the provider applies for revocation of the certificate.

Under § 17 SigG, the Austrian supervisory authority is allowed to accredit certification service providers based both in Austria and abroad. The country in which the provider is headquartered can be seen in the Accredited Certification Services key. However, an Accredited Certification Services key will only be issued to providers that have been accredited by the Austrian supervisory authority itself, i.e., those which are subject to Austrian supervision. Providers accredited abroad can be issued a Qualified Certification Services certificate in Austria (see 1.3.0.3) if necessary.

The certificates will be signed with the supervisory authority's current Accredited Certification Services key. The accompanying CRLs will be signed with the supervisory authority's current certificate revocation key (see 4.4).

In order for an Accredited Certification Services certificate to be issued for a certification service, certification service providers will be required to set the KeyUsage attribute correctly in the certificates they issue. Because under § 17 SigG only those certification service providers whose certificates are used for secure signatures can be accredited, the X.509 v3 certificates issued by the service provider may only use the nonRepudiation (1) bit in the KeyUsage field. Because some products currently use the digitalSignature (0) bit (not compliant with RFC 2459, Section 4.2.1.3) and there is no uniform standardization or practice in this respect, the supervisory authority reserves the option of issuing Accredited Certification Services Certificates to those services in which the provider uses both bits. If legal regulations provided for the accreditation of other services at a later point in time, the KeyUsage field would also have to be set appropriately in this context.

Section 2.4.1 deals with the extent to which the supervisory authority's Accredited Certification Services key is suitable for use as a basis for trusting the levels beneath it in the certification hierarchy. The Accredited Certification Services key is only used to certify those certification services which fulfill the prerequisites for accreditation. Accreditation under § 17 SigG requires that the service only issue qualified certificates to signatories whose signature creation data (private keys) are stored in a secure signature creation device.

The Accredited Certification Services Certificates issued by the supervisory authority do not serve as a guarantee that these certification services will be uniform in all technical specifications. For example, it is possible that a certification service provider could establish multiple hierarchical levels between the key certified by the supervisory authority and the signatories' keys. This can have effects on the signature check.

1.3.0.3 Qualified Certification Services Certificates

These certificates are issued exclusively to certification services which have been reported to the supervisory authority in accordance with § 6 Par. 2 SigG and the purpose of which is to issue qualified certificates. A certification service provider may issue non-qualified certificates in addition to qualified certificates. However, a Qualified Certification Services certificate is only issued to providers for those services in which qualified certificates are issued exclusively.

The certificate is issued by Telekom-Control GmbH in the name of the Telekom-Control Commission as soon as the Telekom-Control Commission decides to acknowledge the reported service and not to take supervisory measures against the service, and once the required fees have been paid. The certificate will be revoked if the certification service provider's activities are prohibited under § 14 SigG, if the certification service provider reports the suspension of services (§ 12 SigG), if the provider changes the certified key or if the provider applies for revocation of the certificate.

In any case, a Qualified Certification Services certificate will be issued to certification service providers based in Austria for all qualified certification services. These providers are subject to supervision by the Austrian supervisory authority. Under § 13 Par. 3 SigG, the supervisory authority is also to register the certification services of service providers based abroad. If the certificates of these providers are considered equivalent to Austrian qualified certificates in accordance with § 24 SigG, the service provider will be issued a Qualified Certification Services certificate. Foreign certification service providers are not subject to supervision by the Austrian supervisory authority unless they are accredited under Austrian law. The country in which the provider is based can be found in the Qualified Certification Services certificate. An accredited certification service provider must also fulfill the requirements of a certification service provider that issues qualified certificates. However, such providers are only issued Accredited Certification Services Certificates for the services that fulfill the prerequisites for accreditation (see 1.3.0.2); they will not be issued additional Qualified Certification Services Certificates.

The certificates are signed with the supervisory authority's current Qualified Certification Services key. The accompanying CRLs are signed using the supervisory authority's current certificate revocation key (see 4.4).

In order for a Qualified Certification Services certificate to be issued to a certification service, the certification service provider is required to set the KeyUsage attribute correctly in the certificates it issues. Because only those X.509 v3 certificates which contain "signature check data" are regarded as certificates or qualified certificates according to the definitions in § 2 No. 8 and 9 SigG, the nonRepudiation (1) bit should be the only one set in the X.509 v3 certificates issued by the certification service provider. Because some products currently use the digitalSignature (0) bit (not compliant with RFC 2459, Section 4.2.1.3) and there is no uniform standardization or practice in this respect, the supervisory authority reserves the option to issue Qualified Certification Services Certificates to those services in which the provider uses both bits. If certificates serving other purposes than those of qualified certificates can be issued in accordance with SigG, the KeyUsage attribute will have to be set appropriately in those cases as well.

Section 2.1.4 deals with the extent to which the supervisory authority's Qualified Certification Services key is suitable for use as a basis for trusting the levels beneath it in the certification hierarchy. The Qualified Certification Services key is used to certify only those certification services in which qualified certificates are issued exclusively.

The Qualified Certification Services Certificates issued by the supervisory authority do not serve as a guarantee that these certification services will be uniform in all technical specifications. For example, it is possible that a certification service provider could establish multiple hierarchical levels between the key certified by the supervisory authority and the signatories' keys. This can have effects on the signature check.

1.3.0.4 Certification Services Certificates

These certificates are issued to certification service providers for certification services which do not issue qualified certificates.

The certificate is issued by Telekom-Control GmbH in the name of the Telekom-Control Commission, as soon as the Telekom-Control Commission decides to acknowledge the reported service and not to take supervisory measures against the service (under § 6 Par. 2 SigG), and once all required fees have been paid. The certificate will be revoked if the certification service provider's activities are prohibited under § 14 SigG, if the certification service provider reports a suspension of services (§ 12 SigG), if the provider changes the certified key, or if the provider applies for revocation of the certificate.

A Certification Services certificate is issued to certification service providers based in Austria for services which do not issue qualified certificates. Austrian services are subject to supervision by the Austrian supervisory authority. Under § 13 Par. 3 SigG, the supervisory authority is also to register the certification services of service providers based abroad. If the certificates of these providers are considered equivalent to Austrian certificates in accordance with § 24 SigG, the service providers will be issued Certification Services Certificates. Foreign certification service providers are not subject to supervision by the Austrian supervisory authority unless they are accredited under Austrian law. The country in which the provider is based can be found in the Certification Services certificate.

The certificates are signed with the supervisory authority's current Certification Services key. The corresponding CRLs are signed using the supervisory authority's current certificate revocation key (see 4.4).

In order for Certification Services Certificates to be issued, certification service providers are not required to limit the use of certificates to electronic signatures using the KeyUsage field in the certificates it issues. Non-qualified certificates can therefore be used for both signatures and encryption, for example.

Within the limits of technical feasibility, Certification Services Certificates will also be issued to certification services which also issue qualified certificates or are accredited by the supervisory authority, but for which no Accredited Certification Services certificate or Qualified Certification Services Certificate can be issued for reasons of technical incompatibility. If it is also impossible to issue a Certification Services Certificate for technical reasons, the supervisory authority will register the certification service provider in the list of Non-X.509 Services.

A Certification Services Certificate bears no significance as to the quality of the certification service provided. For the purpose of checking signatures, it is thus recommended not to take the supervisory authority's Certification Services key as the basis for trusting certificates (see also 2.1.4).

1.3.0.5 Cross-Certification Certificates

These certificates are issued to foreign agencies that act as the root of certification hierarchies and the like. Recipients of Cross-Certification Certificates especially include supervisory authorities under Art. 3 Par. 3 of the EU Signatures Directive (1999/93/EC). The highest-ranking key in each foreign authority's certification hierarchy will be certified. By issuing this certificate, the Austrian supervisory authority only confirms the identity of the foreign authority, thus providing Austrian users a secure path to the foreign authority. The certificate is not intended to make any statement about the quality of the services in the foreign certification hierarchy. The foreign authority's CPS is to be used in distinguishing between qualified and non-qualified services in the foreign certification hierarchy.

The issue of Cross-Certification Certificates is planned for a later point in time. This change will be included in a revised version of the Certification Practice Statement (see Section 8).

Cross-Certification Certificates will be revoked if the certified authority no longer possesses the capacities that qualify it for such a certificate, if it suspends its services, changes certified keys or applies for revocation of the certificate, or if any compromise of the certified key becomes known to the Austrian supervisory authority.

1.3.1 Certification Authorities

All certification authorities under the definitions in this document will be headed by Telekom-Control GmbH for the Telekom-Control Commission, as the Austrian supervisory authority for electronic signatures (§ 15 Par. 2 No. 2 and 3 SigG).

The Telekom-Control Commission is responsible for the resolution on the establishment and design of certification infrastructure in Austria and for resolutions to change this CPS.

Accredited Certification Services Certificates will be issued by Telekom-Control GmbH in the name of the Telekom-Control Commission in cases where the Commission decides to grant accreditation to a certification service provider. Qualified Certification Services and Certification Services Certificates will be issued to qualified or non-qualified certification service providers by Telekom-Control GmbH in the name of the Telekom-Control Commission in cases where the Commission acknowledges the certification service provider's report of services under § 6 Par. 2 SigG and decides not to take supervisory measures against the service provider. Cross-Certification Certificates will be ordered by the Telekom-Control Commission and issued by Telekom-Control GmbH on a case-by-case basis.

1.3.2 Registration Authorities

The only registration authority in Austria according to this CPS is Telekom-Control GmbH.

1.3.3 Certificate Recipients

The only certificate recipients in Austria according to this CPS are providers of certification services. Certificates will be issued either to certification service providers on the market (accredited, qualified, non-qualified service) or to the supervisory authority / Telekom-Control GmbH for its own certification services. Cross-Certification Certificates will be issued to foreign agencies that act as the root of certification hierarchies and the like.

The certification services for which certificates will be issued in accordance with this CPS can be categorized as follows:

- Certification services in which the certificate recipient fulfills the prerequisites for accreditation under § 17 SigG
- Certification services in which qualified certificates are offered
- Certification services in which non-qualified certificates are issued
- Certification services of the supervisory authority or Telekom-Control GmbH.

1.3.4 Applicability

This CPS applies to all certification services rendered by the Telekom-Control Commission as supervisory authority or by Telekom-Control GmbH as the agency to the supervisory authority.

The scope of these services is determined by the applicability of the Austrian Signatures Act (SigG).

1.4 Contact Details

1.4.1 Specification, Administration, Organization

The supervisory authority is the Telekom-Control Commission set up in connection with Telekom-Control GmbH. Telekom-Control GmbH acts as the agency to the Telekom-Control Commission.

Telekom-Control GmbH
Mariahilfer Strasse 77–79
A-1060 Vienna
Tel.: +43/(0)1/58058-0
Fax.: +43/(0)1/58058-9191
E-Mail: signatur@signatur.tkc.at (or: signatur@tkc.at)
Web: http://www.signatur.tkc.at/

1.4.2 Contact Persons

We recommend that messages to supervisory authority be sent to **signatur@signatur.tkc.at** (or: signatur@tkc.at) instead of specific recipients. These messages are distributed to all Telekom-Control employees concerned with electronic signatures and can thus be handled even in cases where certain employees are not present.

Dieter Kronegger, dieter.kronegger@tkc.at

Ulrich Latzenhofer, ulrich.latzenhofer@tkc.at

...

4. Operational Requirements

...

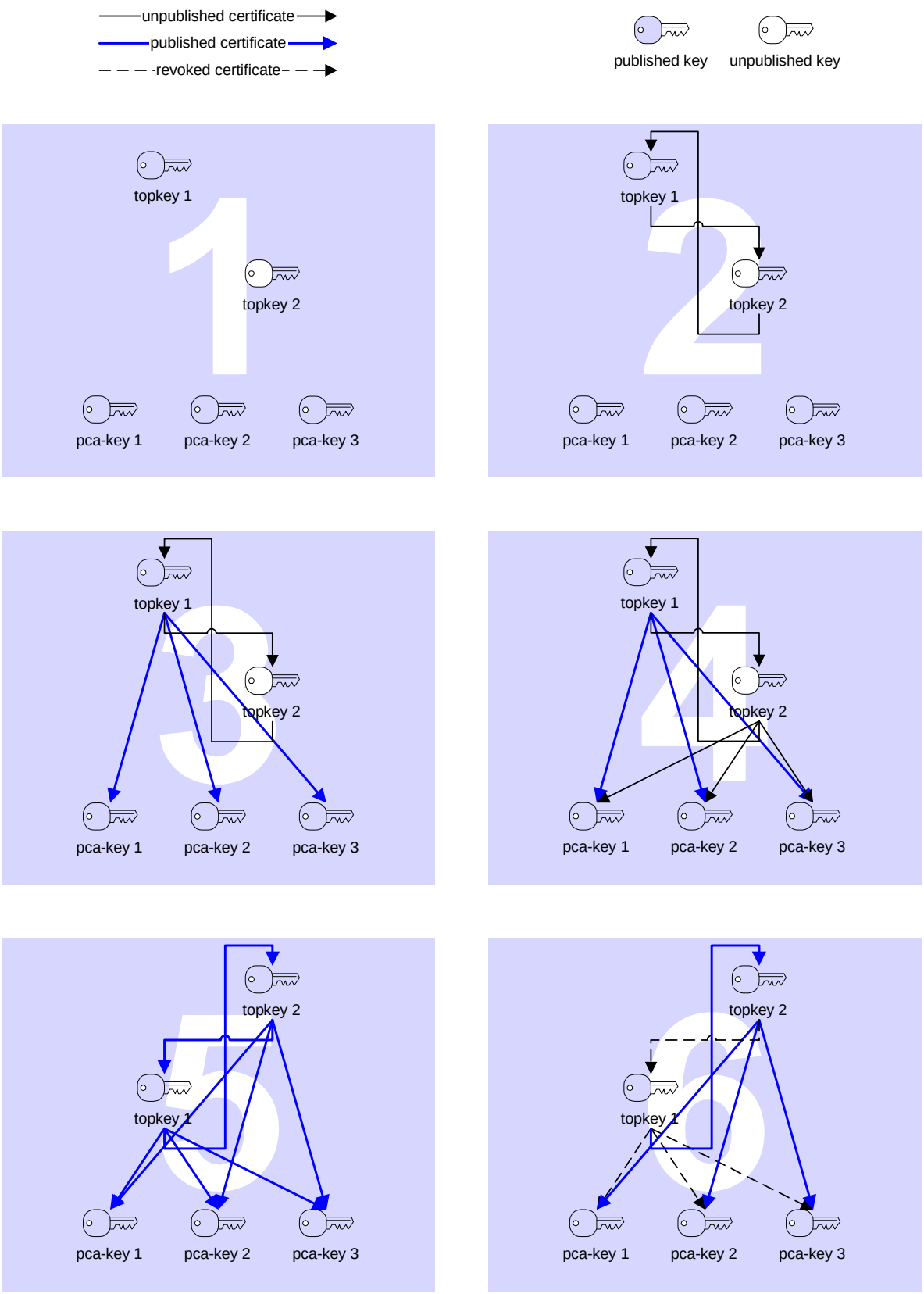
4.7 Backup Systems and Key Changeover

§ 3 Par. 1 of the Austrian Signatures Ordinance requires the supervisory authority to maintain a backup system to be used in cases where the main system is unavailable or compromised. This requirement is met as follows:

4.7.1 Backup System for the Top Key

The backup system for the top key is shown in the diagram below:

Topkey replacement



Step 1: A backup key is generated (Top Key 2) for the top key currently in use (Top Key 1). Both key pairs are generated and stored in separate hardware units which fulfill all requirements of secure signature creation devices. The private keys never leave their respective hardware units.

Step 2: With each top key, a certificate is issued for the other key. The certificate issued by Top Key 1 for Top Key 2 will later ensure a seamless transition from the predecessor (Top Key 1) to the successor (Top Key 2). The other certificate will be used later in order to create an uninterrupted chain of certificates from the successor (Top Key 2) to the predecessor (Top Key 1), although this chain is not absolutely necessary. At first, both certificates will be kept confidential and stored separately from the keys.

Step 3: Top Key 1 is the current top key. It is used to sign the Top Certificates for the supervisory authority's PCA keys and certificate revocation keys. These certificates are published.

Step 4: Top Key 2 is the successor to the current top key. It is used to sign certificates for the supervisory authority's PCA keys and certificate revocation keys. These certificates are not published at first. The state shown in Step 4 in the diagram is the normal status of the system.

Step 5: If Top Key 1 is compromised or replaced (e.g., because its key length is no longer sufficient or because the signature creation device in which it is stored is unavailable), then its successor, Top Key 2, is declared the current key. This changeover is announced in the Official Gazette of the *Wiener Zeitung* (as required under § 13 Par. 3 SigG) and on the supervisory authority's web site (§ 18 Par. 6 Signatures Ordinance). See 4.7.1.1 below. At the same time, the certificates issued by Top Key 1 for Top Key 2 and vice versa are published. The certificate signed by Top Key 1 for Top Key 2 enables users to verify the key changeover.

Step 6: If key changeover has taken place because Top Key 1 was compromised, the certificates issued by Top Key 1 for PCA keys and certificate revocation keys are revoked immediately. In addition, the certificate issued by Top Key 2 for Top Key 1 is revoked, because Top Key 1 can no longer be trusted. The certificate issued by Top Key 1 for Top Key 2 is not revoked in order to avoid endangering verification of the changeover, as described in Step 5. If Top Key 1 was not compromised, then Step 6 is not carried out until a certain period of time has passed since the general announcement in Step 5, in order to allow users more time for the changeover. The time of revocation (Step 6) is included in the announcement mentioned in Step 5.

Step 7 (not shown in diagram): After the changeover from Top Key 1 to Top Key 2, Top Key 3 is generated in a third system, and the procedure repeats itself from Step 2 onward.

For reasons of clarity, the diagram does not include the self-signed certificates that exist for each top key.

The procedure described above is, among other things, a preventive measure in the case of compromises in the main system. In cases where the backup system is compromised, the certificate issued by Top Key 1 for Top Key 2, as well as all certificates issued by Top Key 2, are revoked. Then a new backup system is set up and the procedure is repeated from Step 2 onward. In order to prevent the backup system from being compromised, the signature creation device for Top Key 2 and the certificates issued by Top Key 1 for Top Key 2 and vice versa are stored separately (see Step 2).

4.7.1.1 Publication of Top Key Changeovers

A changeover in the supervisory authority's top key is a critical security event affecting all parties who trust the supervisory authority's certification services and have entered the top key as the root of trust (or a similar function) in some form in their software. In all cases, these persons are to verify that the changeover has truly been announced by the supervisory authority itself and not by a third party for fraudulent purposes.

The publication of changeovers will be carried out as follows:

- The certificate signed with the old top key for the new top key will be made accessible in the supervisory authority's directory
- The changeover will be announced in the *Wiener Zeitung* (§ 13 Par. 3 SigG)
- The changeover will be announced on the supervisory authority's web site (§ 18 Par. 6 SigV) at the addresses http://www.signatur.tkc.at/de/directory/ and https://www.signatur.tkc.at/de/directory/
- A press release will be sent to the relevant specialized periodicals
- A newsletter will be sent by the supervisory authority

All announcements will contain information that enables the new top key's self-signed certificate to be identified unequivocally, especially the certificate's fingerprint.

All certificate recipients will be notified of the changeover.

In addition, all authorities that have issued a cross-certificate for the old top key will be notified immediately. However, this notification will only take place in cases where the cross-certificate was created in cooperation with the supervisory authority. Persons or organizations that have issued a certificate to the supervisory authority without its cooperation are not entitled to notification. The supervisory authority likewise assumes no liability for the newsletter reaching all subscribers.

Those who would like to verify that the new top key is truly in the possession of the supervisory authority can do the following:

- Verify the certificate signed by with the old top key for the new top key. This method of verification is the most secure; however, additional notes in the supervisory authority's announcement should be checked as well.
- Use the announcement in the *Wiener Zeitung* for verification. In addition, other methods of verification should be used, as such an announcement could be made by an unauthorized party.
- Use the information on the supervisory authority's web site for verification. In this context, it is important to ensure that a secure connection is established with HTTPS. The certificate used by the server in this procedure should be checked. Additional methods of verification should be used as well.
- Request the fingerprint from the supervisory authority's hotline (0800/300300, not yet implemented). However, the decision whether to implement this service is yet to be taken. Before calling the hotline, users should install the new Top Certificate according to the instructions on the supervisory authority's web site in order to calculate the

fingerprint. The hotline staff will not provide technical support or assistance in changing the certificate; their only duty is to inform callers of the new certificate's fingerprint.

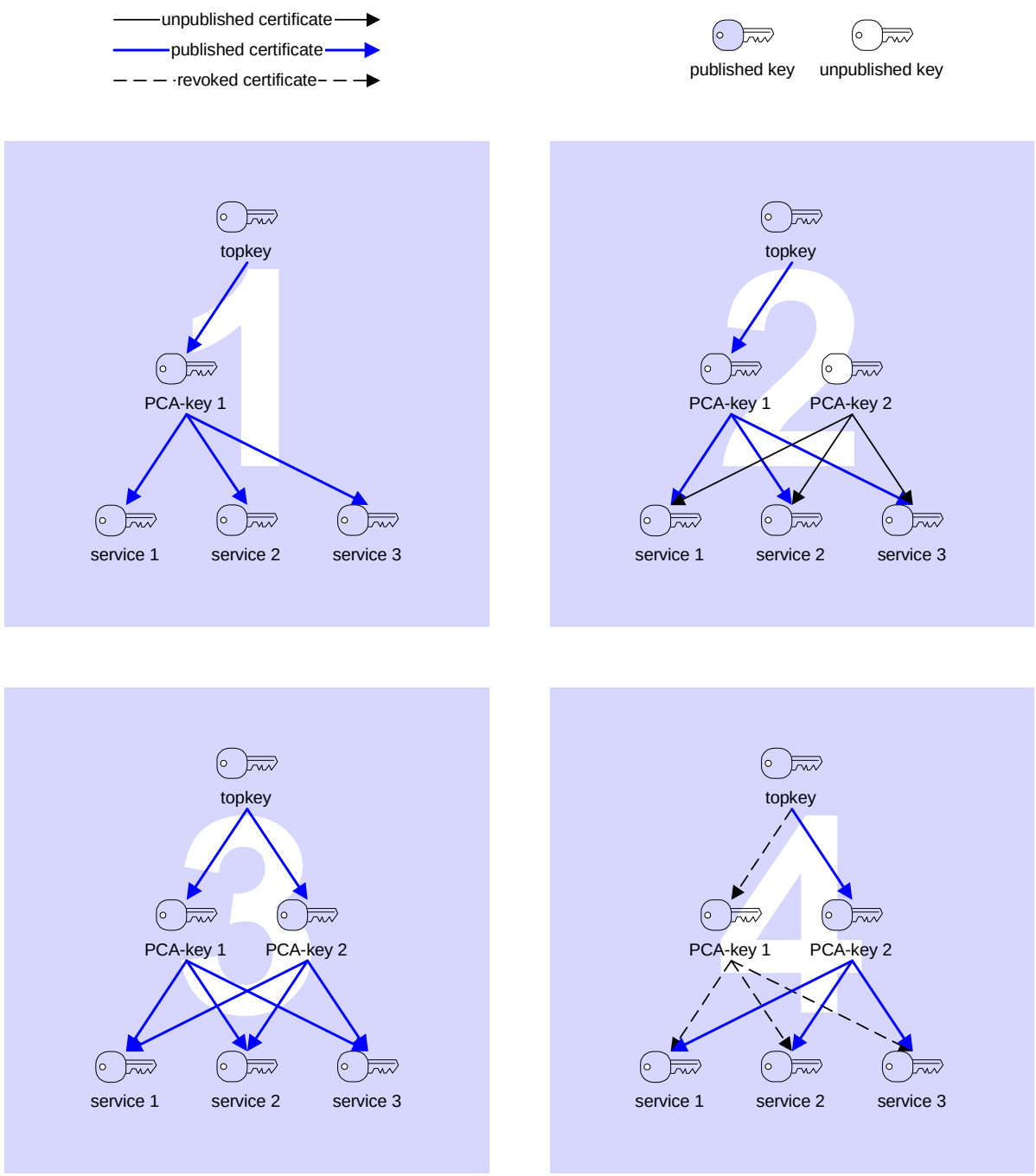
Before reporting a top key changeover, journalists and the media are urged to exercise extreme caution in verifying that all information received is truly from the supervisory authority and not from a third party imitating the supervisory authority for fraudulent purposes.

Cf. also Contact Details, Section 1.4.

4.7.2 Backup Systems for PCA Keys

The backup system for PCA keys is shown in the four steps depicted in the diagram below:

PCA-key replacement



Step 1 shows the certification hierarchy in its basic (normal) state. No backup system is deployed. The two upper keys (top key and PCA key 1) are the supervisory authority's keys, while the keys beneath them are those of three certification service providers.

In Step 2, another PCA key is generated and stored in a separate hardware unit which fulfills the requirements of a secure signature creation device. The private keys never leave their respective hardware units. The second key is also used to issue certificates for the certification services; however, these keys are not published at first.

Step 3: When the PCA key is to be changed (e.g., if PCA key 1 is compromised, or when its key length is no longer sufficient or the signature creation device in which PCA key 1 is stored becomes unavailable), then PCA key 2 is declared the current PCA key (i.e., a Top Certificate is issued for PCA key 2). At the same time, PCA key 2 and all of its certificates are published. The supervisory authority will also announce PCA key changeovers on its web site.

Step 4: After the changeover, all certificates issued by and for PCA key 1 are revoked. If PCA key 1 was compromised, the certificates are revoked immediately; in other cases, a longer time is allowed for the changeover. The supervisory authority will specify the time period allowed until revocation in the announcement (see Step 3).

A program that performs automated signature checks then has to detect the revocation (carried out in Step 4) in the CRL. In such cases, the program can search for the successor to the revoked key automatically. For this purpose, the directory service is queried for a certificate issued in the same name as the revoked certificate (for more information on interpreting various name forms, see Section 3.1.3).

As long as no more than five certificates are issued by a PCA key, the supervisory authority will only ensure that the technology necessary for a backup system is available; the backup system, however, will not actually be implemented. Thus the system's basic state is that shown in Step 1. PCA key 2 will not be generated, nor will replacement certificates (Step 2) be issued, until the key actually needs to be changed.

As soon as more than five certificates have been issued by a PCA key, the backup system will be activated. In such cases, the basic state is that shown in Step 2. However, the main system and the backup system will not always be maintained in parallel, as the backup system has to be stored separately. This means that a certificate will not be issued in the respective backup system every time a certificate (e.g., a Certification Services certificate) is issued in the main system. Backup system will be updated in batches whenever the main system has issued a total of five to ten certificates.

There is no danger of the backup system being compromised prematurely, as it is not embedded in the supervisory authority's certification hierarchy until Step 3. Before that point, the system of no use to an intruders, hackers, etc.

4.7.3 Backup System for the Certificate Revocation Key

The certificate revocation key is stored in a secure signature creation device. In case the certificate revocation key is compromised or has to be changed, an additional secure signature creation device will be kept on hand.

The new certificate revocation key will not be generated until the changeover has to be performed. In such cases, a Top Certificate will be issued for the new certificate revocation key and the Top Certificate for the old certificate revocation key will be revoked.

Key changeovers can be detected by automatic signature checking programs in that the CRL is signed with a different key. In such cases, the program can search for the successor to the revoked key automatically. The search is performed using the keyIdentifier method (cf. 7.1.2 and 7.2.2).

...

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

All of the supervisory authority's key pairs use the RSA procedure (see § 3 Par. 1, Appendix 1 and Appendix 2 Item 1 of the Austrian Signatures Ordinance) and have a key length of at least 1023 bits. The use of the Chinese Remainder Theorem is not permitted. Private keys have to be influenced by actual random elements at a length of at least 1023 bits.

Key generation has to be carried out in the signature creation device itself, and the private keys must not leave the device (§ 3 Par. 2 SigV).

6.1.2 Private Key Delivery to Certificate Recipient

The supervisory authority does not generate key pairs for third parties, thus it does not deliver private keys.

Note: In cases where the Austrian Signatures Ordinance (SigV) applies to a certification service provider that issues qualified certificates, the provider's signature creation data (the private key) has to be generated in the signature creation device and must not leave the device (§ 3 Par. 2 SigV). This also applies to all recipients of Accredited Certification Services Certificates and to all domestic recipients of Qualified Certification Services Certificates.

6.1.3 Public Key Delivery to Certificate Issuer

Delivery must be effected using a PKCS#10 certificate request (see 4.1).

6.1.4 CA Public Key Delivery to Users

The supervisory authority's certificates are published on its web site at http://www.signatur.tkc.at/. The self-signed certificate of the supervisory authority's current top key will also be published in the Official Gazette of the *Wiener Zeitung*.

Details on communication regarding the current top key can be found in Section 4.7.1.1.

6.1.5 Key Sizes

All of the supervisory authority's key pairs have a length of at least 1023 bits (SigV Appendix 1, Item 2)

If the Austrian Signatures Ordinance applies to a certification service provider that issues qualified certificates, keys using the RSA and DSA procedures must be at least 1023 bits in length, and DSA variants based on elliptical curves must be at least 160 bits in length (SigV Appendix 1, Item 2). This also applies to all recipients of Accredited Certification Services Certificates and to all domestic recipients of Qualified Certification Services Certificates.

6.1.6 Public Key Parameters Generation

The Austrian Signatures Ordinance does not set forth any requirements regarding public key parameters.

6.1.7 Parameter Quality Checking

Key lengths and any other parameters will be adapted to the current applicable version of the Austrian Signatures Ordinance.

6.1.8 Hardware/Software Key Generation

All of the supervisory authority's key pairs are generated in secure signature creation devices (see 2.1.1.1, 2.1.1.4 and 6.2).

6.1.9 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Certificates are issued to certification services or for the creation of CRLs in accordance with this CPS.

Top Certificates are issued for the supervisory authority's certification services and certificate revocation keys. For certificates issued for predecessors and successors to the current top key, for the supervisory authority's PCA keys and for the top key itself, the KeyUsage field is to be set to keyCertSign. In certificates issued for the supervisory authority's certificate revocation keys, the KeyUsage field is to be set to cRLSign. The certificate issued to C=AT, O=Telekom-Control Commission, CN=www.signatur.tkc.at supports access to the web server. In this certificate, the digitalSignature and keyEncipherment bits are to be used in the KeyUsage field. The certificate issued to C=AT, O=Telekom-Control Commission, OU=non-X.509 services supports the secure electronic signing of lists of certification services. In this certificate, the KeyUsage field is to be set to nonRepudiation.

Accredited Certification Services Certificates, Qualified Certification Services Certificates, Certification Services Certificates and Cross-Certification Certificates are only issued to certification services. Their KeyUsage field is to be set to keyCertSign only.

...

7. Certificate and CRL Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

All certificates are issued in X.509 v3 format.

7.1.2 Certificate Extensions

First and second-level certificates (TKK top level and TKK PCA level) contain the following extensions: BasicConstraints, AuthorityKeyIdentifier, SubjectKeyIdentifier, KeyUsage, CertificatePolicies und CRLDistributionPoints. BasicConstraints and KeyUsage are labeled critical, whereas the AuthorityKeyIdentifier, SubjectKeyIdentifier, CertificatePolicies und CRLDistributionPoints are not. In BasicConstraints, the cA field contains the value TRUE. Their KeyUsage is set to keyCertSign only. In accordance with the recommendations in RFC 2459, Sections 4.2.1.1 and 4.2.1.2, the AuthorityKeyIdentifier and SubjectKeyIdentifier contain the SHA-1 value of the subjectPublicKey field as the keyIdentifier in the superordinate certificate or the given certificate. The CertificatePolicies extension contains the ASN.1 Object Identifier of the corresponding certificate policy as well as a URI referring to this CPS. The CRLDistributionPoints extension only contains a URI pointing to the CRL.

Some certificates issued to certification services also contain the (non-critical) PolicyConstraints extension (see 7.1.7).

In third-level certificates (TKK services level), the extensions are set differently:

Certificates issued for signing CRLs contain the AuthorityKeyIdentifier, SubjectKeyIdentifier, KeyUsage, CertificatePolicies and CRLDistributionPoints extensions. KeyUsage is labeled critical, whereas the AuthorityKeyIdentifier, SubjectKeyIdentifier, CertificatePolicies und CRLDistributionPoints extensions are not. BasicConstraints do not exist in these certificates. AuthorityKeyIdentifier and SubjectKeyIdentifier are used according to the pattern described for the first and second levels. Their KeyUsage is set to cRLSign only. The CertificatePolicies extension contains the ASN.1 Object Identifier of the corresponding certificate policy as well as a URI referring to this CPS. The CRLDistributionPoints extension only contains a URI pointing to the CRL.

Certificates for HTTP and LDAP servers contain the AuthorityKeyIdentifier, KeyUsage, CertificatePolicies and CRLDistributionPoints extensions. The AuthorityKeyIdentifier extension is used according to the pattern described for the first and second levels. The KeyUsage extension is labeled critical, and only the digitalSignature and keyEncipherment bits are set. The CertificatePolicies extension is not labeled critical and contains the ASN.1 Object Identifier of the corresponding certificate policy as well as a URI referring to this CPS. The CRLDistributionPoints extension is not labeled critical and only contains a URI pointing to the CRL.

Certificates for signing non-X.509 services lists contain the AuthorityKeyIdentifier, KeyUsage, CertificatePolicies and CRLDistributionPoints extensions. The AuthorityKeyIdentifier extension is used according to the pattern described for the first and second levels. The KeyUsage extension is labeled critical, and only the nonRepudiation bit is set. The CertificatePolicies extension is not labeled critical and contains the ASN.1 Object Identifier for the corresponding certificate policy as well as a URI referring to this CPS. The CRLDistributionPoints extension is not labeled critical and only contains a URI pointing to the CRL.

Certificates issued for certification services generally match the first and second-level certificates; restrictions to certain hash and encryption procedures, however, are omitted. However, legal regulations (especially the Appendices to the Austrian Signatures Ordinance, or SigV) do establish certain rules for hash and encryption procedures. In addition, SubjectAltName is set to the Distinguished Name under which the certificate is categorized in the supervisory authority's LDAP directory (C=AT, O=Telekom-Control Commission, OU= etc.).

The certificates issued for internal use at the supervisory authority (e.g., for SSL or TLS connections) are not described in this CPS.

Because the certificates described here are not generally issued to physical persons and therefore the Qualified Certificates Profile (PKIX, ETSI) does not apply in this context, the certificates are not labeled with the policy identifier described in the Profile. Instead, certificate policies are labeled with their own object identifiers, which will be defined in this CPS starting with Version 1.0.

7.1.3 Algorithm Object Identifiers

In certificates issued by the supervisory authority, the fields signatureAlgorithm in Certificate and algorithm in TBSCertificate contain the ASN.1 Object Identifier sha-1WithRSAEncryption in compliance with RFC 2459, Section 7.2.1.

In the supervisory authority's keys, the algorithm field in SubjectPublicKeyInfo contains the ASN.1 Object Identifier rsaEncryption in compliance with RFC 2459, Section 7.3.1.

7.1.4 Name Forms

In certificates issued by the supervisory authority, names are indicated in compliance with RFC 2459, Section 4.1.2.4.

7.1.5 Name Constraints

In certificates issued by the supervisory authority, names usually contain the C, O, OU and CN attribute types, and possibly additional attribute types under X.520. Only the PrintableString, BMPString and UTF8String character strings are used, while PrintableString is preferred to BMPString and BMPString is preferred to UTF8String. Because names do not contain e-mail addresses, the use the of IA5String is not necessary.

7.1.6 Certificate Policy Object Identifiers

The ASN.1 Object Identifiers for various certificate policies will not be defined until Version 1.0 of this CPS.

7.1.7 Usage of Policy Constraints Extension

The PolicyConstraints extension is only found in certificates used to certify accredited or qualified services. The extension is not labeled critical and contains the value 0 in the requireExplicitPolicy field.

7.1.8 Policy Qualifiers' Syntax and Semantics

Only the id-qt-cps qualifier is used in certificates issued by the supervisory authority; this qualifier's syntax and semantics are defined in RFC 2459, Section 4.2.1.5.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Because many software packages can not (yet) interpret the Certificate Policy extension, for the time being this extension is not labeled critical in certificates issued by the supervisory authority.

7.2 CRL Profile

7.2.1 Version Number(s)

All CRLs are issued in X.509 v2 format. Because of the supervisory authority's special certification hierarchy, CRLs can only be interpreted by applications which recognize certain X.509 v2 extensions.

7.2.2 CRL and CRL Entry Extensions

The CRLs issued by the supervisory authority contain the critical IssuingDistributionPoint extension, and the indirectCRL field contains the value TRUE. In addition, they contain the non-critical extensions CRLNumber and AuthorityKeyIdentifier, where identification is based on the keyIdentifier method (the keyIdentifier in the Certificate Revocation List's AuthorityKeyIdentifier has to match the keyIdentifier in the SubjectKeyIdentifier of the corresponding Certificate Revocation certificate).

The CRL entries can contain the critical CertificateIssuer extension and the non-critical ReasonCode extension. In case the CertificateIssuer extension is not found in a CRL entry, it is assumed (see RFC 2459) that the certificate revoked was issued by the same certification service as the certificate revoked in the previous CRL entry. The CertificateIssuer extension has to be found in the first CRL entry. CertificateIssuer is indicated as a name matching that of the certification service that issued the revoked certificate, in compliance with the rules set forth in Section 3.1.3.

...