Sicherheits- und Zertifizierungskonzept – Certification Practice Statement – Entwurf

Die formelle Beschlussfassung der Telekom-Control-Kommission über das Certification Practice Statement ist erst für den Zeitpunkt vorgesehen, an welchem die Publik-Key-Infrastruktur der Aufsichtsstelle implementiert ist.

Version 0.31

14.12.2000

Aufsichtsstelle für elektronische Signaturen
Telekom-Control-Kommission und Telekom-Control GmbH
Mariahilfer Straße 77–79, 1060 Wien, Tel. 01/58058-0, Fax: 01/58058-9191
http://www.signatur.tkc.at, signatur@tkc.at

Inhaltsverzeichnis

0. Änderungen gegenüber früheren Versionen

Änderungen gegenüber Version 0.30

2.6.4: Erläuterungen zum LDAP-Verzeichnis eingefügt

7.1.2: Erweiterung BasicConstraints aus Zertifikaten zur CRL-Verifikation entfernt

7.1.3: Beschreibung von Signaturalgorithmen in Zertifikaten genauer spezifiziert, Verwendung von SubjectAltName erläutert, Nichtverwendung des Qualified-Certificate-Policy-Identifiers begründet

1. Einführung

1.1 Überblick

Dieses Dokument enthält das Sicherheits- und Zertifizierungskonzept der Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen.

Die vorliegende Fassung dieses Dokuments ist ein Entwurf in einem frühen Stadium. Vorgesehen ist, dass die erste gültige Fassung des Dokuments die Versionsnummer 1.0 tragen wird.

1.2 Identifikation

Bezeichnung des Dokuments: Sicherheits- und Zertifizierungskonzept – Certification Practice Statement, Version 0.31, 14.12.2000.

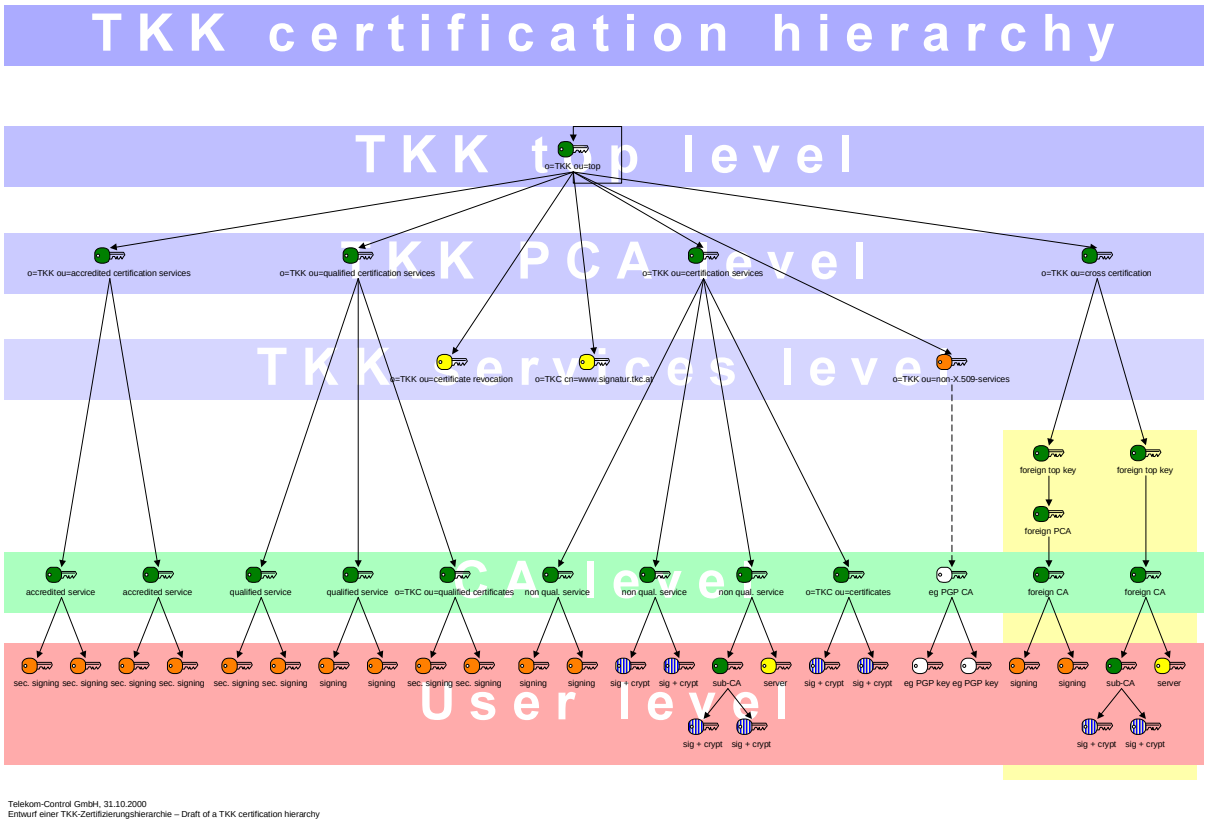
Dieses Dokument fasst die wesentlichsten Inhalte des Sicherheits- und Zertifizierungskonzepts der Aufsichtsstelle für elektronische Signaturen in Form eines Certification Practice Statement (CPS) zusammen. Die Gliederung des CPS erfolgt nach dem Muster des Standards RFC 2527 (Chokhani/Ford, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, 1999). Darüber hinaus umfasst das Sicherheits- und Zertifizierungskonzept auch weitere Bestandteile, welche nicht veröffentlicht werden (siehe 8.2).

Das CPS wird von der Telekom-Control GmbH im Auftrag der Aufsichtsstelle für elektronische Signaturen unter http://www.signatur.tkc.at/ in der Rubrik „Dokumente“ („Repository“) veröffentlicht.

Ein ASN.1 Object Identifier für dieses Dokument wird erst ab Version 1.0 vergeben werden.

1.3 Zertifizierungsinfrastruktur und Anwendungsbereiche

Eine Übersicht über die Zertifizierungsinfrastruktur der Aufsichtsstelle ist in der folgenden Grafik dargestellt. Diese Grafik zeigt das Grundkonzept der Zertifizierungshierarchie der Aufsichtsstelle.



Auf der obersten Ebene („TKK top level“) befinden sich ausschließlich der TOP-Schlüssel der Aufsichtsstelle, seine Vorgänger und Nachfolger.

Auf der zweiten Ebene („TKK PCA level“) befinden sich die Policy Certification Authorities der Aufsichtsstelle. Die an Zertifizierungsdiensteanbieter für deren Zertifizierungsdienste ausgestellten Zertifikate werden mit unterschiedlichen PCA-Schlüsseln signiert. Mit dem ACCREDITED-CERTIFICATION-SERVICES-Schlüssel werden Zertifikate für Zertifizierungsdienste signiert, auf welche sich eine Akkreditierung bezieht. Mit dem QUALIFIED-CERTIFICATION-SERVICES-Schlüssel werden Zertifikate für andere Zertifizierungsdienste, bei denen qualifizierte Zertifikate ausgegeben werden, signiert. Der CERTIFICATION-SERVICES-Schlüssel signiert Zertifikate für andere (nicht qualifizierte) Dienste. Ein weiterer Schlüssel ist für die Cross-Zertifizierung vorgesehen.

Auf der dritten Ebene („TKK services level“) sind die Schlüssel der Aufsichtsstelle dargestellt, die nicht für das Signieren von Zertifikaten vorgesehen sind. Für diese Schlüssel sind teilweise geringere Sicherheitsmaßnahmen vorgesehen (im Gegensatz zu den Schlüsseln der ersten beiden Ebenen werden sie z. B. nicht ausschließlich offline eingesetzt.) Vorgesehen ist ein Schlüssel, mit dem Widerrufslisten signiert werden, ein Schlüssel für den HTTPS-Zugang zum Verzeichnisdienst der Aufsichtsstelle und ein Schlüssel, mit dem eine Liste jener Anbieter signiert wird, denen aus technischen Gründen kein X.509v3-Zertifikat ausgestellt werden kann. Weiters sind Schlüssel zur Verwaltung der Verzeichnis-, Widerrufs- und WWW-Dienste und zur Erstellung sicherer Zeitstempel in der Dokumentation vorgesehen (die zu solchen Schlüsseln gehörigen Zertifikate werden nur veröffentlicht, wenn sie für die Öffentlichkeit von Belang sind).

Auf der Ebene „CA level“ sind die Schlüssel der verschiedenen Diensteanbieter dargestellt, auf der Ebene „User level“ die Schlüssel der Signatoren und anderen Nutzer.

1.3.0 Zertifizierungsdienste der Aufsichtsstelle

Zertifikate der folgenden Zertifikatsklassen werden von der Aufsichtsstelle ausgestellt. Jeder Zertifikatsklasse entspricht ein Schlüsselpaar, mit dessen privatem Schlüssel die Zertifikate signiert werden.

1.3.0.1 TOP-Zertifikate

TOP-Zertifikate werden mit dem TOP-Schlüssel der Aufsichtsstelle signiert. TOP-Zertifikate werden ausschließlich für öffentliche Schlüssel ausgestellt, deren korrespondierende private Schlüssel im ausschließlichen Einflussbereich der Aufsichtsstelle oder der Telekom-Control GmbH stehen.

Der TOP-Schlüssel könnte auch Root-Schlüssel oder Wurzelschlüssel genannt werden. Im Einklang mit der Terminologie von IETF PKIX und mit den Überlegungen des Justizausschusses zu § 13 Abs. 3 SigG (siehe *Brenn*, Signaturgesetz, 102f) wird aber die Bezeichnung TOP-Schlüssel verwendet (vgl. auch die Bezeichnung „Hauptsystem“ in § 3 Abs. 1 SigV). Damit wird zum Ausdruck gebracht, dass es sich bei diesem Schlüssel nicht um eine zentrale Wurzel handelt, der allgemeines Vertrauen entgegengebracht werden muss. Die Gültigkeit einer elektronischen Signatur kann unabhängig davon geprüft werden, ob man dem TOP-Schlüssel der Aufsichtsstelle vertraut.

Mit dem TOP-Schlüssel werden ausschließlich Zertifikate für die folgenden Schlüssel signiert:

- Vorgänger und Nachfolger des TOP-Schlüssels (siehe 4.7.1).
- Alle PCA-Schlüssel der Aufsichtsstelle (also die Schlüssel der zweiten Ebene, siehe oben 1.3).
- Die Schlüssel der sonstigen Dienste der Aufsichtsstelle, insbesondere die CERTIFICATE-REVOCATION-Schlüssel der Aufsichtsstelle (das sind jene Schlüssel, mit denen Widerrufslisten signiert werden (siehe 4.4)).
- Weiters wird für jeden TOP-Schlüssel ein selbstsigniertes Zertifikat ausgestellt.

Mit dem TOP-Schlüssel werden jedenfalls nur Zertifikate für Schlüssel signiert, die im jeweils aktuellen Certification Practice Statement der Aufsichtsstelle genannt sind. Zu späteren Änderungen des CPS siehe Kapitel 8.

Der momentan gültige TOP-Schlüssel und alle PCA-Schlüssel der Aufsichtsstelle befinden sich in einer sicheren Signaturerstellungseinheit im sicheren Raum der Aufsichtsstelle. Die Vorgänger dieser Schlüssel befinden sich entweder ebenfalls in diesem Raum oder sie wurden vernichtet. Die auf die Vorgänger verweisenden Zertifikate der Aufsichtsstelle werden widerrufen. Die Nachfolger der gültigen Schlüssel sind – solange sie nicht gültig sind – auswärts gelagert. Zu den Zweitsystemen der Aufsichtsstelle siehe 4.7.

In TOP-Zertifikaten für Vorgänger und Nachfolger des TOP-Schlüssels und für PCA-Schlüssel ist im Attribut KeyUsage ausschließlich das Bit keyCertSign gesetzt. Diese Zertifikate dienen also ausschließlich der Signatur weiterer Zertifikate. In TOP-Zertifikaten für die Schlüssel auf der Ebene „TKK services level“ ist dieses Bit keinesfalls gesetzt. Diese Zertifikate können also nicht für die Signatur weiterer Zertifikate eingesetzt werden. In Zertifikaten für die CERTIFICATE-REVOCATION-Schlüssel der Aufsichtsstelle ist im Attribut KeyUsage ausschließlich das Bit cRLSign gesetzt. Diese Zertifikate dienen also ausschließlich der Signatur von Widerrufslisten.

Die Aufsichtsstelle behält sich vor, in Zukunft weitere Zertifizierungsdienste aufzunehmen und für diese Dienste Zertifikate auszustellen, die mit dem TOP-Schlüssel der Aufsichtsstelle signiert sind. Ein mit dem TOP-Schlüssel der Aufsichtsstelle signiertes Zertifikat sagt nichts über die Qualität der Gesamtheit der Zertifikate aus, die sich in der Zertifizierungshierarchie der Aufsichtsstelle unterhalb des TOP-Schlüssels befinden. In dieser Hierarchie befinden sich sowohl qualifizierte als auch nicht qualifizierte Zertifizierungsdienste, sowohl Dienste, die der Aufsicht der Aufsichtsstelle unterliegen als auch ausländische Dienste, die der Aufsicht der österreichischen Aufsichtsstelle nicht unterliegen. Das mit dem TOP-Schlüssel der Aufsichtsstelle signierte Zertifikat sagt ausschließlich aus, dass der zertifizierte Schlüssel sich in der alleinigen Kontrolle der Aufsichtsstelle entsprechend deren Sicherheitskonzept befindet.

Der TOP-Schlüssel der Aufsichtsstelle eignet sich daher nicht dazu, als Wurzel des Vertrauens für die Gesamtheit der darunter liegenden Dienste und Zertifikate ausgewählt zu werden. Sein Zweck liegt vielmehr darin, alle Zertifizierungsdienste der Aufsichtsstelle zusammenzufassen und den Nutzern einen einheitlichen Einstiegspunkt in die Zertifizierungshierarchie der Aufsichtsstelle zu bieten, von welchem aus die anderen Schlüssel in der Zertifizierungshierarchie und – im Wege der Cross-Zertifizierung – insbesondere auch ausländische Aufsichtsstellen und Zertifizierungsdienste gesichert erreicht werden können. Der sich vom TOP-Schlüssel aus wegbewegende Nutzer muss aber bei jedem einzelnen Schritt durch die Zertifizierungshierarchie die entsprechende Policy prüfen, um entscheiden zu können, welches Vertrauen er in den jeweiligen Zertifizierungsdienst setzt.

Inwieweit als Ausgangspunkt des Vertrauens stattdessen der ACCREDITED-CERTIFICATION-SERVICES-Schlüssel der Aufsichtsstelle und der QUALIFIED-CERTIFICATION-SERVICES-Schlüssel geeignet sein können, wird in Kapitel 2.1.4 erörtert.

Im Wege der Cross-Zertifizierung kann der TOP-Schlüssel der Aufsichtsstelle zertifiziert werden, um den Aufwand der Cross-Zertifizierung zu minimieren. Die Aufsichtsstelle wird bemüht sein, ihren jeweils gültigen TOP-Schlüssel von möglichst vielen Stellen zertifizieren zu lassen, um eine optimale internationale Vernetzung zu erreichen.

1.3.0.2 ACCREDITED-CERTIFICATION-SERVICES-Zertifikate

Diese Zertifikate werden ausschließlich für Zertifizierungsdienste ausgestellt, auf die sich eine von der Aufsichtsstelle gemäß § 17 SigG ausgesprochene Akkreditierung bezieht. Ein Zertifizierungsdiensteanbieter, der gemäß § 17 SigG akkreditiert wurde, kann neben den Zertifizierungsdiensten, mit welchen er die Voraussetzungen für die Akkreditierung erfüllt, auch andere Zertifizierungsdienste erbringen. Ein ACCREDITED-CERTIFICATION-SERVICES-Zertifikat wird dem Anbieter nur für solche Zertifizierungsdienste ausgestellt, bei welchen die Voraussetzungen für eine Akkreditierung erfüllt sind.

Das Zertifikat wird von der Telekom-Control GmbH im Namen der Telekom-Control-Kommission ausgestellt, wenn der Akkreditierungsbescheid rechtskräftig wurde und die vorgeschriebenen Gebühren entrichtet wurden. Das Zertifikat wird widerrufen, wenn die Akkreditierung widerrufen oder die Tätigkeit des Zertifizierungsdiensteanbieters gemäß § 14 SigG untersagt wird, wenn der Zertifizierungsdiensteanbieter die Einstellung der Tätigkeit anzeigt (§ 12 SigG), wenn er den zertifizierten Schlüssel ändert oder wenn er um den Widerruf des Zertifikates ersucht.

Nach § 17 SigG ist die Akkreditierung eines Zertifizierungsdiensteanbieters durch die österreichische Aufsichtsstelle sowohl möglich, wenn der Anbieter seinen Sitz in Österreich hat, als auch dann, wenn er seinen Sitz im Ausland hat. Der Sitzstaat des Anbieters ist aus dem ACCREDITED-CERTIFICATION-SERVICES-Zertifikat ersichtlich. Ein ACCREDITED-

CERTIFICATION-SERVICES-Zertifikat wird aber nur solchen Anbietern ausgestellt, die von der österreichischen Aufsichtsstelle selbst akkreditiert wurden, also ihrer Aufsicht unterstehen. Anbietern, die im Ausland akkreditiert wurden, kann in Österreich gegebenenfalls ein QUALIFIED-CERTIFICATION-SERVICES-Zertifikat ausgestellt werden (siehe 1.3.0.3).

Die Zertifikate werden mit dem jeweils gültigen ACCREDITED-CERTIFICATION-SERVICES-Schlüssel der Aufsichtsstelle signiert. Die zugehörigen Widerrufslisten werden mit dem jeweils gültigen CERTIFICATE-REVOCATION-Schlüssel der Aufsichtsstelle signiert (siehe 4.4).

Damit für einen Zertifizierungsdienst ein ACCREDITED-CERTIFICATION-SERVICES-Zertifikat ausgestellt wird, ist erforderlich, dass der Zertifizierungsdiensteanbieter in den von ihm ausgestellten Zertifikaten das Attribut KeyUsage korrekt setzt. Da gemäß § 17 SigG nur ein Zertifizierungsdienst, dessen Zertifikate der sicheren elektronischen Signatur dienen, akkreditiert werden kann, darf in den vom Zertifizierungsdiensteanbieter ausgestellten X.509v3-Zertifikaten im Attribut KeyUsage ausschließlich das Bit nonRepudiation (1) gesetzt sein. Da manche Produkte entgegen RFC 2459, Punkt 4.2.1.3 derzeit das Bit digitalSignature (0) auswerten und diesbezüglich noch keine einheitliche Standardisierung und Praxis besteht, behält sich die Aufsichtsstelle vorläufig die Möglichkeit vor, auch für solche Diensten ein ACCREDITED-CERTIFICATION-SERVICES-Zertifikat auszustellen, bei welchen der Zertifizierungsdiensteanbieter beide Bits setzt. – Wenn zu einem späteren Zeitpunkt auch die Akkreditierung anderer Dienste gesetzlich vorgesehen wäre, müsste auch hier das Attribut KeyUsage entsprechend gesetzt werden.

Inwieweit der ACCREDITED-CERTIFICATION-SERVICES-Schlüssel der Aufsichtsstelle als Ausgangspunkt des Vertrauens für die darunter liegenden Ebenen der Zertifizierungshierarchie geeignet sein kann, wird in Kapitel 2.1.4 erörtert. Mit dem ACCREDITED-CERTIFICATION-SERVICES-Schlüssel werden ausschließlich die Schlüssel von Zertifizierungsdiensten zertifiziert, die die Voraussetzungen für eine Akkreditierung erfüllen. Die Akkreditierung gemäß § 17 SigG bedingt, dass im Zuge des Dienstes ausschließlich qualifizierte Zertifikate an Signatoren ausgestellt werden, deren Signaturerstellungsdaten (private Schlüssel) in einer sicheren Signaturerstellungseinheit gespeichert sind.

Die von der Aufsichtsstelle für Zertifizierungsdienste ausgestellten ACCREDITED-CERTIFICATION-SERVICES-Zertifikate gewährleisten nicht, dass diese Zertifizierungsdienste in allen Einzelheiten technisch gleichartig sind. Beispielsweise könnte es möglich sein, dass ein Zertifizierungsdiensteanbieter zwischen dem von der Aufsichtsstelle zertifizierten Schlüssel und den Schlüsseln der Signatoren mehrere hierarchische Ebenen vorsieht. Dies kann Auswirkungen auf die Signaturprüfung haben.

1.3.0.3 QUALIFIED-CERTIFICATION-SERVICES-Zertifikate

Diese Zertifikate werden ausschließlich für Zertifizierungsdienste ausgestellt, die der Aufsichtsstelle gemäß § 6 Abs. 2 SigG angezeigt wurden und deren Gegenstand die Ausstellung qualifizierter Zertifikate ist. Ein Zertifizierungsdiensteanbieter kann neben qualifizierten Zertifikaten auch nicht qualifizierte Zertifikate ausstellen. Ein QUALIFIED-CERTIFICATION-SERVICES-Zertifikat wird dem Anbieter nur für solche Zertifizierungsdienste ausgestellt, bei welchen ausschließlich qualifizierte Zertifikate ausgestellt werden.

Das Zertifikat wird von der Telekom-Control GmbH im Namen der Telekom-Control-Kommission ausgestellt, sobald die Telekom-Control-Kommission aufgrund der Anzeige beschlossen hat, die Anzeige zur Kenntnis zu nehmen und gegen den angezeigten Dienst

keine Aufsichtsmaßnahmen zu ergreifen und wenn die vorgeschriebenen Gebühren entrichtet wurden. Das Zertifikat wird widerrufen, wenn die Tätigkeit des Zertifizierungsdiensteanbieters gemäß § 14 SigG untersagt wird, wenn der Zertifizierungsdiensteanbieter die Einstellung der Tätigkeit anzeigt (§ 12 SigG), wenn er den zertifizierten Schlüssel ändert oder wenn er um den Widerruf des Zertifikates ersucht.

Ein QUALIFIED-CERTIFICATION-SERVICES-Zertifikat wird jedenfalls für alle qualifizierten Zertifizierungsdiensten von in Österreich niedergelassenen Zertifizierungsdiensteanbietern ausgestellt. Diese unterstehen der Aufsicht der österreichischen Aufsichtsstelle. Gemäß § 13 Abs. 3 SigG hat die Aufsichtsstelle auch Zertifizierungsdienste von im Ausland niedergelassenen Zertifizierungsdiensteanbietern zu registrieren. Wenn deren Zertifikate gemäß § 24 SigG österreichischen qualifizierten Zertifikaten gleichgestellt sind, wird dem Anbieter für den Dienst ein QUALIFIED-CERTIFICATION-SERVICES-Zertifikat ausgestellt. Ausländische Zertifizierungsdiensteanbieter unterstehen – soferne sie nicht nach österreichischem Recht akkreditiert sind – nicht der Aufsicht der österreichischen Aufsichtsstelle. Der Sitzstaat des Anbieters ist aus dem QUALIFIED-CERTIFICATION-SERVICES-Zertifikat ersichtlich.

Ein akkreditierter Zertifizierungsdiensteanbieter muss zwar immer auch die Anforderungen an einen Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt. Einem solchen Anbieter werden aber für die Zertifizierungsdienste, welche die Voraussetzungen für eine Akkreditierung erfüllen, immer nur ACCREDITED-CERTIFICATION-SERVICES-Zertifikate (siehe 1.3.0.2) und nicht zusätzlich auch QUALIFIED-CERTIFICATION-SERVICES-Zertifikate ausgestellt.

Die Zertifikate werden mit dem jeweils gültigen QUALIFIED-CERTIFICATION-SERVICES-Schlüssel der Aufsichtsstelle signiert. Die zugehörigen Widerrufslisten werden mit dem jeweils gültigen CERTIFICATE-REVOCATION-Schlüssel der Aufsichtsstelle signiert (siehe 4.4).

Damit für einen Zertifizierungsdienst ein QUALIFIED-CERTIFICATION-SERVICES-Zertifikat ausgestellt wird, ist erforderlich, dass der Zertifizierungsdiensteanbieter in den von ihm ausgestellten Zertifikaten das Attribut KeyUsage korrekt setzt. Da gemäß den Definitionen in § 2 Z 8 und 9 SigG nur solche X.509v3-Zertifikate, die „Signaturprüfdaten“ enthalten, als Zertifikate bzw. qualifizierte Zertifikate im Sinne des SigG angesehen werden, soll in den vom Zertifizierungsdiensteanbieter ausgestellten X.509v3-Zertifikaten im Attribut KeyUsage ausschließlich das Bit nonRepudiation (1) gesetzt sein. Da manche Produkte entgegen RFC 2459, Punkt 4.2.1.3 derzeit das Bit digitalSignature (0) auswerten und diesbezüglich noch keine einheitliche Standardisierung und Praxis besteht, behält sich die Aufsichtsstelle vorläufig die Möglichkeit vor, auch für solche Diensten ein QUALIFIED-CERTIFICATION-SERVICES-Zertifikat auszustellen, bei welchen der Zertifizierungsdiensteanbieter beide Bits setzt. – Falls zu einem späteren Zeitpunkt auch anderen Zwecken dienende Zertifikate als qualifizierte Zertifikate im Sinne des SigG ausgegeben werden können, muss auch hier das Attribut KeyUsage entsprechend gesetzt werden.

Inwieweit der QUALIFIED-CERTIFICATION-SERVICES-Schlüssel der Aufsichtsstelle als Ausgangspunkt des Vertrauens für die darunter liegenden Ebenen der Zertifizierungshierarchie geeignet sein kann, wird in Kapitel 2.1.4 erörtert. Mit dem QUALIFIED-CERTIFICATION-SERVICES-Schlüssel werden ausschließlich die Schlüssel von Zertifizierungsdiensten zertifiziert, mittels derer ausschließlich qualifizierte Zertifikate ausgestellt werden.

Die von der Aufsichtsstelle für Zertifizierungsdienste ausgestellten QUALIFIED-CERTIFICATION-SERVICES-Zertifikate gewährleisten nicht, dass diese Zertifizierungsdienste in allen Einzelheiten technisch gleichartig sind. Beispielsweise könnte

es möglich sein, dass ein Zertifizierungsdiensteanbieter zwischen dem von der Aufsichtsstelle zertifizierten Schlüssel und den Schlüsseln der Signatoren mehrere hierarchische Ebenen vorsieht. Dies kann Auswirkungen auf die Signaturprüfung haben.

1.3.0.4 CERTIFICATION-SERVICES-Zertifikate

Diese Zertifikate werden an Zertifizierungsdiensteanbieter für solche Zertifizierungsdienste ausgestellt, bei denen keine qualifizierten Zertifikate ausgestellt werden.

Das Zertifikat wird von der Telekom-Control GmbH im Namen der Telekom-Control-Kommission ausgestellt, sobald die Telekom-Control-Kommission aufgrund der Anzeige gemäß § 6 Abs. 2 SigG beschlossen hat, die Anzeige zur Kenntnis zu nehmen und gegen den angezeigten Dienst keine Aufsichtsmaßnahmen zu ergreifen und wenn die vorgeschriebenen Gebühren entrichtet wurden. Das Zertifikat wird widerrufen, wenn die Tätigkeit des Zertifizierungsdiensteanbieters gemäß § 14 SigG untersagt wird, wenn der Zertifizierungsdiensteanbieter die Einstellung der Tätigkeit anzeigt (§ 12 SigG), wenn er den zertifizierten Schlüssel ändert oder wenn er um den Widerruf des Zertifikates ersucht.

Ein CERTIFICATION-SERVICES-Zertifikat wird für all jene Zertifizierungsdienste von in Österreich niedergelassenen Zertifizierungsdiensteanbietern ausgestellt, bei denen keine qualifizierten Zertifikate ausgestellt werden. Die österreichischen Dienste unterstehen der Aufsicht der österreichischen Aufsichtsstelle. Gemäß § 13 Abs. 3 SigG hat die Aufsichtsstelle auch Zertifizierungsdienste von im Ausland niedergelassenen Zertifizierungsdiensteanbietern zu registrieren. Wenn deren Zertifikate gemäß § 24 SigG österreichischen Zertifikaten gleichgestellt sind, wird dem Anbieter für den Dienst ein CERTIFICATION-SERVICES-Zertifikat ausgestellt. Ausländische Zertifizierungsdiensteanbieter unterstehen – soferne sie nicht nach österreichischem Recht akkreditiert sind – nicht der Aufsicht der österreichischen Aufsichtsstelle. Der Sitzstaat des Anbieters ist aus dem CERTIFICATION-SERVICES-Zertifikat ersichtlich.

Die Zertifikate werden mit dem jeweils gültigen CERTIFICATION-SERVICES-Schlüssel der Aufsichtsstelle signiert. Die zugehörigen Widerrufslisten werden mit dem jeweils gültigen CERTIFICATE-REVOCATION-Schlüssel der Aufsichtsstelle signiert (siehe 4.4).

Damit für einen Zertifizierungsdienst ein CERTIFICATION-SERVICES-Zertifikat ausgestellt wird, ist nicht erforderlich, dass der Zertifizierungsdiensteanbieter in den von ihm ausgestellten Zertifikaten das Attribut KeyUsage auf die Verwendung der Zertifikate für die elektronische Signatur beschränkt. Die nicht qualifizierten Zertifikate können daher beispielsweise auch gemischt für Signatur und Verschlüsselung eingesetzt werden.

Ein CERTIFICATION-SERVICES-Zertifikat wird im Rahmen der technischen Möglichkeiten auch für solche Zertifizierungsdienste ausgestellt, bei denen qualifizierte Zertifikate ausgestellt werden oder auf die sich eine Akkreditierung der Aufsichtsstelle bezieht, für die aber aus Gründen der technischen Inkompatibilität kein ACCREDITED-CERTIFICATION-SERVICES-Zertifikat bzw. kein QUALIFIED-CERTIFICATION-SERVICES-Zertifikat ausgestellt werden kann. Ist auch die Ausstellung eines CERTIFICATION-SERVICES-Zertifikat technisch nicht möglich, so wird der Zertifizierungsdiensteanbieter von der Aufsichtsstelle auf der Liste der NON-X.509-SERVICES registriert.

Ein CERTIFICATION-SERVICES-Zertifikat sagt nichts über die Qualität des angebotenen Zertifizierungsdienstes aus. Für seine Verwendung im Rahmen der Signaturprüfung wird daher empfohlen, den CERTIFICATION-SERVICES-Schlüssel der Aufsichtsstelle nicht als Ausgangspunkt des Vertrauens einzusetzen (siehe auch 2.1.4).

1.3.0.5 CROSS-CERTIFICATION-Zertifikate

Diese Zertifikate werden an ausländische Stellen, welche als Wurzel von Zertifizierungshierarchien oder dergleichen fungieren, ausgestellt. Als Empfänger eines CROSS-CERTIFICATION-Zertifikates kommen insbesondere Aufsichtsstellen gemäß Art. 3 Abs. 3 der Signaturrichtlinie 1999/93/EG in Frage. Zertifiziert wird jeweils der in der Zertifizierungshierarchie der ausländischen Stelle höchstgelegene Schlüssel. Mit der Ausstellung des Zertifikates bestätigt die österreichische Aufsichtsstelle lediglich die Identität der ausländischen Stelle und schafft damit österreichischen Nutzern einen sicheren Pfad zur ausländischen Stelle. Über die Qualität der in der ausländischen Zertifizierungshierarchie enthaltenen Dienste wird keine Aussage getroffen. Wie innerhalb der ausländischen Hierarchie qualifizierte und nicht qualifizierte Dienste zu unterscheiden sind, ist aus dem Zertifizierungskonzept der ausländischen Stelle zu ersehen.

Die Ausstellung von CROSS-CERTIFICATION-Zertifikaten ist erst für einen späteren Zeitpunkt vorgesehen. Diese Änderung des Zertifizierungskonzeptes wird in einem geänderten Certification Practice Statement festgehalten werden (siehe Kapitel 8).

CROSS-CERTIFICATION-Zertifikate werden widerrufen, wenn die zertifizierte Stelle die für die Ausstellung des Zertifikates maßgebliche Eigenschaft verliert, wenn sie ihren Dienst einstellt, wenn sie den zertifizierten Schlüssel ändert, wenn sie um den Widerruf des Zertifikates ersucht oder wenn der österreichischen Aufsichtsstelle die Kompromittierung des zertifizierten Schlüssels bekannt wird.

1.3.1 Zertifizierungsstellen

Sämtliche Zertifizierungsstellen nach diesem Dokument werden von der Telekom-Control GmbH für die Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen geführt (§ 15 Abs. 2 Z 2 und 3 SigG).

Der Telekom-Control-Kommission obliegt der Beschluss über die Einrichtung und Ausgestaltung der Zertifizierungsinfrastruktur, sowie der Beschluss über Änderungen dieses CPS.

ACCREDITED-CERTIFICATION-SERVICES-Zertifikate werden von der Telekom-Control GmbH im Namen der Telekom-Control-Kommission ausgestellt, wenn die Telekom-Control-Kommission die Akkreditierung eines Zertifizierungsdiensteanbieters beschlossen hat. QUALIFIED-CERTIFICATION-SERVICES und CERTIFICATION-SERVICES-Zertifikate für qualifizierte oder nicht qualifizierte Zertifizierungsdiensteanbieter werden von der Telekom-Control GmbH im Namen der Telekom-Control-Kommission ausgestellt, wenn die Telekom-Control-Kommission die Anzeige eines Zertifizierungsdiensteanbieters gemäß § 6 Abs. 2 SigG zur Kenntnis genommen hat und beschlossen hat, keine Aufsichtsmaßnahmen gegen den Anbieter dieses Dienstes zu ergreifen. Die Ausstellung von CROSS-CERTIFICATION-Zertifikaten wird von der Telekom-Control-Kommission im Einzelfall angeordnet und von der Telekom-Control GmbH vorgenommen.

1.3.2 Registrierungsstellen

Einzige Registrierungsstelle nach diesem CPS ist die Telekom-Control GmbH.

1.3.3 Zertifikatsempfänger

Zertifikatsempfänger im Rahmen dieses CPS sind ausschließlich die Anbieter von Zertifizierungsdiensten. Zertifikate werden entweder an am Markt auftretende Zertifizierungsdiensteanbieter für deren Dienste (akkreditiert, qualifiziert, nicht qualifiziert),

oder an die Aufsichtsstelle bzw. die Telekom-Control GmbH für deren eigenen Zertifizierungsdienste ausgestellt. CROSS-CERTIFICATION-Zertifikate werden an ausländische Stellen, welche als Wurzel von Zertifizierungshierarchien oder dergleichen fungieren, ausgestellt.

Die Zertifizierungsdienste, für welche im Rahmen dieses CPS Zertifikate ausgestellt werden, können unterschieden werden in:

- Zertifizierungsdienste, mit welchen der Zertifikatsempfänger die Voraussetzungen für eine Akkreditierung nach § 17 SigG erfüllt,
- Zertifizierungsdienste, mit denen qualifizierte Zertifikate angeboten werden,
- Zertifizierungsdienste, mit denen nicht qualifizierte Zertifikate angeboten werden und
- Zertifizierungsdienste der Aufsichtsstelle oder der Telekom-Control GmbH.

1.3.4 Anwendungsbereich

Dieses CPS umfasst sämtliche Zertifizierungsdienste, die von der Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen oder von der Telekom-Control GmbH als Geschäftsstelle der Aufsichtsstelle erbracht werden.

Der Umfang dieser Dienste ergibt sich aus dem Anwendungsbereich des Signaturgesetzes.

1.4 Kontaktinformation

1.4.1 Aufsichtsstelle

Aufsichtsstelle ist die bei der Telekom-Control GmbH angesiedelte Telekom-Control-Kommission. Die Telekom-Control GmbH ist Geschäftsstelle der Telekom-Control-Kommission.

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

1.4.2 Kontaktpersonen

Es wird empfohlen, Mitteilungen an die Aufsichtsstelle nicht an bestimmte Personen zu richten, sondern an die Adresse **signatur@signatur.tkc.at** (derzeit noch: signatur@tkc.at). Diese E-Mails werden an alle mit der elektronischen Signatur befassten MitarbeiterInnen weitergeleitet und können daher auch bei Abwesenheit einzelner Personen behandelt werden.

Dieter Kronegger, dieter.kronegger@tkc.at

Ulrich Latzenhofer, ulrich.latzenhofer@tkc.at

2. Allgemeine Richtlinien

2.1 Pflichten

2.1.1 Pflichten einer Zertifizierungsstelle

Einzige Zertifizierungsstelle nach diesem CPS ist die Telekom-Control GmbH im Auftrag der Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen. Die Telekom-Control GmbH ist verpflichtet, alle sich aus diesem CPS, dem SigG und der SigV ergebenden Sicherheitsanforderungen einzuhalten. Dies bedeutet insbesondere:

2.1.1.1 Signaturerstellungsdaten (§ 3 und 4 SigV)

Sämtliche in diesem CPS genannten Signaturerstellungsdaten (privaten Schlüssel) müssen den Anforderungen des § 3 und 4 SigV entsprechen. Die Signaturerstellungsdaten müssen in der Signaturerstellungseinheit gespeichert werden und dürfen diese nicht verlassen (§ 3 Abs. 1 SigV). Die Signaturerstellungsdaten entsprechen dem Verfahren RSA und weisen eine Mindestlänge von 1023 Bit auf (§ 3 Abs. 3 SigV, Anhang 1 Punkt 1 und 2 SigV). Die wiederholte Erzeugung von Signaturerstellungsdaten in einer Signaturerstellungseinheit oder die wiederholte Anwendung der Signaturerstellungsdaten zur Signierung von Zertifikaten darf nicht zu einer Verminderung der Schlüsselqualität führen. (§ 3 Abs. 3 und 4 SigV). Die Erzeugung der Signaturerstellungsdaten muss auf einer tatsächlichen Zufälligkeit beruhen, der ein technischer Zufall oder ein signatorbezogener Zufall zu Grunde liegt. Die Signaturerstellungsdaten müssen für mindestens 1023 Bit auf einer tatsächlichen Zufälligkeit beruhen. Die Signaturerstellungseinheit muss die Zufallsqualität prüfen (§ 3 Abs. 5 SigV). Ein Duplizieren von Signaturerstellungsdaten nach deren Erzeugung ist nicht zulässig (§ 4 Abs. 1 SigV).

2.1.1.2 Technische Verfahren (§ 5 und 6 SigV)

Als Hashverfahren wird das Verfahren SHA-1 eingesetzt. Zur Verschlüsselung des Hashwerts wird das Verfahren RSA eingesetzt. Als Padding wird gemäß RFC 2459 Abschnitt 7.2.1 das in PKCS#1 beschriebene Verfahren eingesetzt. Die Verwendung des Chinese Remainder Theorem ist nicht zulässig (§ 5 SigV, Anhang 2 Abs. 1 SigV).

Die eingesetzten Systeme, insbesondere Produkte und technische Verfahren, sind entsprechend ihrem aktuellen Stand und auf nachprüfbare Weise zu dokumentieren. Die für die Erbringung der Dienste der Aufsichtsstelle eingesetzten Systemelemente werden nicht gleichzeitig auch für andere Tätigkeiten verwendet. (§ 6 SigV)

2.1.1.3 Schutz der technischen Komponenten (§ 8 SigV)

Die Signaturerstellungsdaten (privaten Schlüssel), die zum Erstellen der Zertifikate und die zum Abrufbarhalten der Verzeichnis- und Widerrufsdienste eingesetzten technischen Komponenten müssen vor Kompromittierung und unbefugtem Zugriff geschützt werden. Unbefugte Zugriffe müssen erkennbar sein.

Der Schutz der privaten Schlüssel ist in Kapitel 6.2 beschrieben, die Maßnahmen gegen unbefugten Zutritt in Kapitel 5. Die Protokolle der Zutrittskontrolle werden gemäß Kapitel 4.5 regelmäßig überprüft.

2.1.1.4 Evaluation (§ 9 SigV)

Die für die Erzeugung und Speicherung der Signaturerstellungsdaten (privaten Schlüssel) der Aufsichtsstelle verwendeten Komponenten müssen evaluiert und von einer Bestätigungsstelle bescheinigt sein (§ 18 Abs. 5 SigG, § 9 SigV).

Zur Prüfung dieser Komponenten sind einerseits geeignete und von einer Bestätigungsstelle anerkannte Sicherheitsprofile der Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation, ISO 15408) anwendbar.

Die Prüfung der Komponenten kann auch nach den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), soweit anwendbar auch nach den Security Requirements for Cryptographic Modules (FIPS 140-1, level 2) erfolgen. Bei der Anwendung von ITSEC muss die Evaluationsstufe E 3 mit der Mindeststärke der Sicherheitsmechanismen „hoch“ eingehalten werden.

2.1.1.5 Sicherheit der Datenübertragung (§ 10 Abs. 1 SigV)

Der Zertifizierungsdienst der Aufsichtsstelle einerseits und der Verzeichnisdienst und Widerrufsdienst der Aufsichtsstelle werden getrennt geführt. Die Erstellung von Zertifikaten erfolgt in einem sicheren Raum in den Räumlichkeiten der Aufsichtsstelle, Verzeichnis- und Widerrufsdienst in einem Rechenzentrum.

Die Konsole, von der aus die Mitarbeiter der Aufsichtsstelle auf den Verzeichnisdienst zugreifen und insbesondere die erstellten Zertifikate in den Verzeichnisdienst einbringen können, befindet sich im sicheren Raum der Aufsichtsstelle. Die Verbindung zum Rechenzentrum erfolgt als Wählverbindung oder als Standleitung. Über ein geeignetes Protokoll (SSL bzw. TLS) erfolgt eine beiderseitige Authentifizierung (zumindest mit RSA 1024 Bit); die Verbindung ist mit einem starken Verschlüsselungsalgorithmus (zumindest 90 Bit symmetrisch) verschlüsselt. Server ist dabei der Rechner im Rechenzentrum, Client der Rechner im sicheren Raum der Aufsichtsstelle. Beide Rechner werden so konfiguriert, dass sie jeweils nur das Zertifikat des anderen Rechners akzeptieren.

Unmittelbar nach der Erstellung eines Zertifikates wird dieses in den Verzeichnisdienst eingebracht. Ein Zugriff von außen auf die Rechner des Zertifizierungsdienstes ist nicht möglich, da diese Rechner niemals an eine Netzwerkverbindung angeschlossen sind. Die erzeugten Zertifikate werden auf einen Datenträger (z. B. eine Diskette) exportiert und händisch auf die ebenfalls im sicheren Raum befindliche Konsole übertragen.

Die Kommunikation zwischen der Eingabekonsole, von der aus ein Widerruf ausgelöst werden kann, und dem Widerrufsdienst (welcher ebenfalls im Rechenzentrum untergebracht ist), wird ebenfalls mittels eines geeigneten Protokolls (SSL bzw. TLS) und beiderseitiger Authentifizierung gesichert, wobei die Eingabekonsole als Client und der im Rechenzentrum befindliche Rechner als Server fungiert. Die zur Authentifizierung verwendeten Zertifikate werden nicht veröffentlicht und daher auch nicht in der Zertifizierungshierarchie der Aufsichtsstelle (vgl. 1.3) geführt.

2.1.1.6 Trennung der technischen Anwendungen (§ 10 Abs. 2 SigV)

Die technischen Einrichtungen des Zertifizierungsdienstes, des Verzeichnisdienstes und des Widerrufsdienstes sind von allen anderen Anwendungen der Telekom-Control GmbH getrennt.

2.1.1.7 Zutrittsschutz (§ 10 Abs. 3 SigV)

Die Rechner des Zertifizierungsdienstes befinden sich in einem Tresor in einem eigenen Raum. Der Raum ist mit einer Zutrittskontrolle ausgestattet, die nur von zwei Personen gemeinsam bedient werden kann. Auch der Tresor kann nur von zwei Personen gemeinsam geöffnet werden.

Der Raum ist durch eine Alarmanlage gegen Einbruch gesichert. Der Tresor ist so widerstandsfähig ausgestattet, dass er bei einem Einbruch in den Raum bis zum Eintreffen des Wachdienstes bzw. der Polizei Öffnungsversuchen standhält.

Der Zutrittsschutz zu den Rechnern des Verzeichnisdienstes und des Widerrufsdienstes ist durch das Sicherheitskonzept des Rechenzentrums gewährleistet. Gegen unbefugten Zugriff durch das Rechenzentrumspersonal sind die Rechner dadurch geschützt, dass sie in versperrbaren Schränken untergebracht sind. Das Rechenzentrumspersonal erhält gewisse Zugriffsberechtigungen, um auf den Rechnern Prozesse starten und stoppen zu können, hat aber keinen physikalischen Zugriff auf die Rechner.

2.1.1.8 Personal (§ 10 Abs. 4 und 5 SigV)

Die Zuverlässigkeit des Personals der Aufsichtsstelle wird durch Einholung von Strafregisterauskünften (beschränkte Auskünfte iSd § 6 Tilgungsgesetz 1972) in Abständen von höchstens zwei Jahren überprüft (§ 10 Abs. 4 SigV). Dies gilt für das gesamte Personal, das eine Aufgabe nach dem Rollenmodell der Aufsichtsstelle wahrnimmt.

Das technische Personal der Aufsichtsstelle verfügt über ausreichendes Fachwissen (§ 10 Abs. 5 SigV). Dies wird bei der Zuordnung der Rollen des Rollenmodells der Aufsichtsstelle zu den einzelnen Personen berücksichtigt.

2.1.1.9 Widerrufsdienste (§ 13 SigV)

Siehe Punkt 4.4.

2.1.1.10 Dokumentation (§ 11 SigG, § 16 SigV)

Die Sicherheitsmaßnahmen, die zur Einhaltung des SigG und der SigV getroffen werden, das Ausstellen und der Widerruf von Zertifikaten werden dokumentiert. Die Dokumentation erfolgt in elektronischer Form. Die in der Dokumentation enthaltenen Daten werden mit einer sicheren elektronischen Signatur versehen und enthalten sichere Zeitstempel. Die Dokumentation wird zumindest 33 Jahre ab der letzten Eintragung aufbewahrt und wird so gesichert, dass sie innerhalb dieses Zeitraums lesbar und verfügbar bleibt.

2.1.2 Pflichten einer Registrierungsstelle

Einzige Registrierungsstelle nach diesem CPS ist die Telekom-Control GmbH.

Die für die Registrierung zuständigen Mitarbeiter der Telekom-Control GmbH müssen sich vor jedem Zertifizierungsvorgang überzeugen: von der Identität des Zertifizierungswerbers (siehe 3.1.8 und 3.1.9), von dessen Verfügungsgewalt über die privaten Schlüssel (siehe 3.1.7) und davon, dass ein den Zertifizierungsvorgang deckender Beschluss der Telekom-Control-Kommission vorliegt.

2.1.3 Verpflichtungen der Zertifikatsempfänger

Zertifikatsempfänger nach diesem CPS sind nicht natürliche Personen, sondern Zertifizierungsdiensteanbieter. Die Verpflichtungen, die diese Zertifikatsempfänger treffen, ergeben sich aus dem SigG und der SigV bzw. im Falle ausländischer Zertifikatsempfänger aus der jeweils anwendbaren Rechtsordnung.

Empfänger von ACCREDITED-CERTIFICATION-SERVICES-Zertifikaten sind Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate anbieten und sichere elektronische Signaturverfahren bereitstellen. Auf sie sind die entsprechenden Bestimmungen des SigG, der SigV und allfällige Auflagen des Akkreditierungsbescheides anzuwenden.

Empfänger von QUALIFIED-CERTIFICATION-SERVICES-Zertifikaten sind Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate anbieten und/oder sichere elektronische Signaturverfahren bereitstellen. Auf sie sind die entsprechenden Bestimmungen des SigG und der SigV bzw. im Falle ausländischer Zertifikatsempfänger aus der jeweils anwendbaren Rechtsordnung anzuwenden.

Empfänger von CERTIFICATION-SERVICES-Zertifikaten sind Zertifizierungsdiensteanbieter, die weder qualifizierte Zertifikate anbieten noch sichere elektronische Signaturverfahren bereitstellen. Diese Anbieter treffen nach dem SigG und der SigV nur sehr wenige Verpflichtungen. Im Einzelfall könnte es vorkommen (siehe 1.3.0.4), dass einem Zertifizierungsdiensteanbieter ein CERTIFICATION-SERVICES-Zertifikat ausgestellt wird, obwohl er rechtlich als Anbieter qualifizierter Zertifikate anzusehen ist oder von der Aufsichtsstelle akkreditiert wurde – nämlich, dann, wenn aus Gründen der technischen Inkompatibilität kein ACCREDITED-CERTIFICATION-SERVICES-Zertifikat bzw. kein QUALIFIED-CERTIFICATION-SERVICES-Zertifikat ausgestellt werden kann. Einen solchen Anbieter treffen dann trotz Ausstellung des CERTIFICATION-SERVICES-Zertifikates die strengeren Verpflichtungen eines akkreditierten bzw. qualifizierten Zertifizierungsdiensteanbieters.

Empfänger von CROSS-CERTIFICATION-Zertifikaten sind z. B. ausländische Aufsichtsstellen. Inwieweit diese Anbieter Verpflichtungen aus dem SigG (beispielsweise § 21 SigG) oder der SigV unterliegen können, wird im Einzelfall zu prüfen sein.

Alleiniger Empfänger von TOP-Zertifikaten ist die Aufsichtsstelle (Telekom-Control-Kommission) selbst oder die Telekom-Control GmbH. Die jeweiligen Verpflichtungen zur Verwendung dieser Zertifikate ergeben sich aus diesem CPS, mit welchem die rechtlichen Anforderungen des SigG und der SigV umgesetzt werden.

2.1.4 Verpflichtungen Dritter

Das Signaturgesetz sieht keine Verpflichtungen für Dritte vor, die auf Zertifikate vertrauen. Wer auf ein Zertifikat oder eine elektronische Signatur aber ohne entsprechend sorgfältige Prüfung vertraut, den können dennoch Rechtsfolgen treffen. Beispielsweise könnte im Fall, dass der Empfänger einer signierten Nachricht einen Schadenersatzanspruch geltend macht, ein Mitverschulden des Empfängers festgestellt werden, aufgrund dessen der Schadenersatz gemindert wird oder sogar ganz entfällt.

Für die Prüfung von Zertifikaten und von elektronischen Signaturen wird daher empfohlen,

- die elektronische Signatur mit einem zuverlässigen Produkt zu überprüfen (vgl. die Empfehlungen für eine sichere Signaturprüfung in § 18 Abs. 4 SigG und Anhang IV der Signaturrichtlinie),

- bei jedem im Zuge der Signaturprüfung verwendeten Zertifikat zu überprüfen, ob der Gültigkeitszeitraum des Zertifikates abgelaufen ist und ob das Zertifikat widerrufen wurde,

- zu überprüfen, wer das Zertifikat ausgestellt hat und welche Empfehlungen der Aussteller dieses Zertifikates für die Signaturprüfung veröffentlicht hat.

Soweit im Zuge der Signaturprüfung Zertifikate der Aufsichtsstelle überprüft werden, wird insbesondere empfohlen, zu überprüfen, welche der in Kapitel 1.3.0 beschriebenen Klassen von Zertifikaten vorliegt. Die verschiedenen Zertifikatsklassen sind mit unterschiedlichen Qualitätsaussagen hinsichtlich der Zertifizierungsdienste, für welche ein Zertifikat ausgestellt wurde, verbunden.

Bei der Verwendung von Software zur Signaturprüfung ist vom Benutzer in der Regel einer oder mehrere Ausgangspunkte (manchmal auch als „Wurzel“ bezeichnet) einzutragen, in welchen der Benutzer sein Vertrauen setzt. Bei der Auswahl dieses Ausgangspunktes ist sorgfältig vorzugehen. Einerseits sollte man gründlich überprüfen, ob man die Informationen über das Zertifikat, welches man als Wurzel des Vertrauens einträgt, aus zuverlässiger Quelle erfahren hat.

Andererseits ist zu überprüfen, ob das Verifikationsmodell, mit welchem die eingesetzte Software arbeitet, den überprüften Zertifizierungshierarchien entspricht.

Im Hinblick auf die Zertifizierungshierarchie der Aufsichtsstelle kann unter Umständen der jeweils gültige ACCREDITED-CERTIFICATION-SERVICES-Schlüssel und/oder der jeweils gültige QUALIFIED-CERTIFICATION-SERVICES-Schlüssel geeignet sein, als Ausgangspunkt („Wurzel“) für das in die darunterliegende Zertifizierungshierarchie gesetzte Vertrauen ausgewählt zu werden (vgl. die Beschreibung der Zertifizierungsdienste der Aufsichtsstelle in 1.3.0). Mit diesen Schlüsseln werden ausschließlich die Schlüssel von Zertifizierungsdiensten zertifiziert, mittels derer ausschließlich qualifizierte Zertifikate ausgestellt werden. Der TOP-Schlüssel der Aufsichtsstelle hingegen eignet sich nicht als Wurzel des Vertrauens für die Gesamtheit der in der Hierarchie darunter liegenden Dienste und Zertifikate (siehe 1.3.0.1).

Weiters wird empfohlen, Software einzusetzen, die die KeyUsage-Attribute der Zertifikate korrekt auswerten kann.

2.1.5 Verpflichtungen betreffend Veröffentlichungen

Die Telekom-Control GmbH ist verpflichtet, die in Punkt 2.6 genannten Informationen zu veröffentlichen. Dieser Verpflichtung wird auf der Website http://www.signatur.tkc.at/ entsprochen. Die Informationen über die TOP-Schlüssel der Aufsichtsstelle werden zudem im Amtsblatt zur Wiener Zeitung veröffentlicht (§ 13 Abs. 3 SigG).

2.2 Haftung

Die Haftung der Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen und der Telekom-Control GmbH ergibt sich aus dem Amtshaftungsgesetz und aus der sinngemäßen Anwendung des § 23 SigG.

2.3 Finanzielle Verantwortlichkeit

Die Haftung der Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen und der Telekom-Control GmbH ergibt sich aus dem Amtshaftungsgesetz und aus der sinngemäßen Anwendung des § 23 SigG.

2.4 Auslegung und Durchsetzung

2.4.1 Rechtsvorschriften

Die Tätigkeit der Aufsichtsstelle erfolgt in Vollziehung des Signaturgesetzes, BGBl I 1999/190, und der Signaturverordnung, BGBl II 2000/30. Mit dem Signaturgesetz wird die Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. L 13 vom 19.01.2000, S. 12) innerstaatlich umgesetzt.

Unklarheiten in diesem CPS sind im Sinne dieser Rechtsvorschriften auszulegen.

Zur Durchsetzung dieses CPS stehen der Aufsichtsstelle die im Signaturgesetz vorgesehenen aufsichtsbehördlichen Maßnahmen (vgl. insbesondere § 16 SigG) zur Verfügung.

Da im Rahmen dieses CPS keine Zertifizierungsdienste für Endkunden erbracht werden, ist kein Streitschlichtungsverfahren gemäß § 15 Abs. 3 SigG möglich.

2.5 Gebühren und Entgelte

Die Gebühren für Aufsichtstätigkeiten sind in § 1 SigV geregelt.

2.5.1 Zertifikatsausstellung und -erneuerung

Für die Führung der Verzeichnisse bei der Aufsichtsstelle ist gemäß § 1 Abs. 1 Z 10 SigV eine Gebühr von 500 Euro pro Zertifizierungsdiensteanbieter und Jahr zu entrichten.

2.5.2 Gebühren für den Abruf von Zertifikaten

Der Zugang zum Verzeichnisdienst ist gebühren- und entgeltfrei.

2.5.3 Gebühren für den Zugang zu Widerrufsdiensten und Statusinformation

Der Zugang zum Widerrufsdienst ist gebühren- und entgeltfrei.

2.5.4 Gebühren für andere Dienste wie z. B. Information über Policies

Der Zugang zu den von der Aufsichtsstelle zu veröffentlichenden Informationen ist gebühren- und entgeltfrei.

2.6 Veröffentlichung und Archiv

2.6.1 Veröffentlichte Inhalte

Zu veröffentlichen sind:

- das Certification Practice Statement und die Certificate Policies der Aufsichtsstelle,
- alle von der Aufsichtsstelle ausgestellten Zertifikate samt Statusinformationen (gültig, widerrufen, abgelaufen),
- die jeweils aktuelle Widerrufsliste und

- Informationen über den Zugang zu den Verzeichnissen der Aufsichtsstelle und zum Widerrufsdienst

2.6.2 Häufigkeit der Veröffentlichung

Das Certification Practice Statement und die Policies der Aufsichtsstelle werden bei jeder Änderung veröffentlicht. Auch alle früheren Versionen werden abrufbar gehalten.

Die Zertifikate der Aufsichtsstelle werden umgehend nach ihrer Erstellung in den Verzeichnisdienst eingebracht. (Dies gilt nicht für manche Zertifikate der Zweitsysteme, die vorerst unveröffentlicht bleiben und erst bei der Aktivierung des Zweitsystems veröffentlicht werden, siehe 4.7.) Auch abgelaufene Zertifikate werden abrufbar gehalten.

Die Häufigkeit der Veröffentlichung von Widerrufslisten ist in Punkt 4.4.9 geregelt. Ein widerrufenes Zertifikat wird zumindest auf Dauer von 33 Jahren auf der jeweils aktuellen Widerrufsliste geführt (allerdings müssen künftige Widerrufslisten nicht unbedingt das im vorliegenden CPS beschriebene Format aufweisen; zu Änderungen des Sicherheits- und Zertifizierungskonzeptes siehe 8.1).

2.6.3 Zugangskontrolle

Die zu veröffentlichenden Informationen sind für jedermann gebühren- und entgeltfrei und anonym zugänglich.

2.6.4 Archiv

Die zu veröffentlichten Informationen können auf der Website der Aufsichtsstelle, http://www.signatur.tkc.at/, abgerufen werden. Die Dokumente können über HTTP abgefragt werden. Für den Abruf von Zertifikaten samt Statusinformationen wird ein Webformular zur Verfügung stehen, welches über HTTP abgefragt werden kann. Zertifikate und Widerrufslisten können auch über LDAP abgefragt werden. Sowohl HTTP als auch LDAP werden auch über SSL bzw. TLS mit Serverauthentifikation angeboten. Für diesen Zweck wird an den Server (C=AT, O=Telekom-Control GmbH, CN=www.signatur.tkc.at) ein TOP-Zertifikat ausgestellt (siehe 1.3.0.1). Die technischen Details der Abfrage werden auf der Website erläutert.

Die Veröffentlichung von Informationen über die TOP-Schlüssel der Aufsichtsstelle erfolgt zusätzlich im Amtsblatt zur Wiener Zeitung.

Das Verzeichnis, das die von der Aufsichtsstelle ausgestellten Zertifikate und Widerrufslisten enthält, wird im Format LDAP v2 gemäß der Spezifikation in RFC 2587 geführt. Als LDAP-Server wird ebenfalls der Rechner www.signatur.tkc.at eingesetzt. Die Suchbasis lautet C=AT, O=Telekom-Control-Kommission. Auf den LDAP-Dienst kann ohne Server-Authentifikation (Port 389) oder mit Server-Authentifikation (Port 636) zugegriffen werden.

Die Aufsichtsstelle bietet einen Newsletter an, über den auf wichtigere Informationen hingewiesen wird. Auf den Mailverteiler des Newsletters kann sich jedermann eintragen lassen. Die Aufsichtsstelle übernimmt keine Haftung dafür, dass im konkreten Einzelfall ein Newsletter ausgesandt wird bzw. dass der Newsletter allen Interessenten zugestellt wird.

2.7 Interne Prüfungen (Audits)

Im Hinblick darauf, dass die Aufsichtsstelle nicht am Markt tätig ist, werden für die erbrachten Zertifizierungsdienste ausschließlich interne Prüfungen vorgesehen. Die Aufsichtsstelle selbst unterliegt nach dem Signaturgesetz keiner weiteren Aufsicht. Daher soll auch nicht der

Eindruck erweckt werden, die Aufsichtsstelle würde von einer weiteren Stelle beaufsichtigt werden. Die Audits sind daher rein interne Überprüfungen, deren Ergebnisse nicht veröffentlicht werden.

2.7.1 Häufigkeit der Audits

Zumindest einmal jährlich wird die Einhaltung des Sicherheits- und Zertifizierungskonzeptes durch einen Auditor überprüft. Die erste Überprüfung wird spätestens drei Monate nach der Aufnahme der Zertifizierungsdienste der Aufsichtsstelle vorgenommen.

2.7.2 Identität/Qualifikation des Auditors

Der Auditor wird vom Geschäftsführer der Telekom-Control GmbH ausgewählt und muss über ausreichende Erfahrungen im Hinblick auf die organisatorische Abwicklung technischer Aufgaben verfügen, um die Einhaltung des Sicherheits- und Zertifizierungskonzeptes überprüfen zu können.

2.7.3 Verhältnis zwischen dem Auditor und der überprüften Einheit

Der Auditor ist Angestellter der Telekom-Control GmbH, aber – abgesehen von seiner Tätigkeit als Auditor – nicht mit den Zertifizierungsdiensten befasst.

2.7.4 Vom Audit umfasste Themen

Im Rahmen des Audit wird die organisatorische Abwicklung des Zertifizierungsdienstes und die Einhaltung des Sicherheits- und Zertifizierungskonzeptes überprüft. Der Auditor hat dazu Zugang zur gesamten verfügbaren Dokumentation, insbesondere zu allen Protokollen und Logdateien.

Im Rahmen des Audit ist auch zu überprüfen, ob die eingesetzten technischen Komponenten dem Stand der Technik entsprechen und – soweit dies erforderlich ist – von einer Bestätigungsstelle bescheinigt wurden.

In technischen Fragen hat sich der Auditor mit einer Bestätigungsstelle abzustimmen (§ 15 Abs. 3 SigG).

2.7.5 Aktionen, die bei festgestellten Mängeln vorgenommen werden

Wenn im Rahmen des Audit Mängel festgestellt werden, dann werden diese vom Auditor dem Sicherheitsteam, der Geschäftsführung der Telekom-Control GmbH und der Telekom-Control-Kommission mitgeteilt.

Das Sicherheitsteam erarbeitet – gegebenenfalls in Zusammenarbeit mit dem Auditor – Lösungsvorschläge zur Behebung der Mängel. Soweit zur Mängelbehebung Änderungen des Certification Practice Statement erforderlich sind, entscheidet darüber die Telekom-Control-Kommission. Über andere organisatorische oder technische Maßnahmen entscheidet die Geschäftsführung der Telekom-Control GmbH.

2.7.6 Veröffentlichung der Ergebnisse

Die Ergebnisse eines Audit werden im Regelfall nicht veröffentlicht.

2.8 Geheimhaltung

2.8.1 Vertraulich zu behandelnde Daten

Als vertrauliche Daten gelten:

- Betriebs- und Geschäftsgeheimnisse der Zertifizierungsdiensteanbieter, für deren Zertifizierungsdiensten ein Zertifikat ausgestellt wird, und

- jene Bestandteile des Sicherheitskonzeptes der Aufsichtsstelle, die nicht in dieses CPS aufgenommen wurden, insbesondere Informationen über die Zutrittskontrolle und Alarmanlage des sicheren Raumes der Aufsichtsstelle, Informationen über die Sicherungsmaßnahmen auf den eingesetzten Rechnern, sämtliche Passwörter etc.

2.8.2 Nicht vertraulich zu behandelnde Daten

Nicht als vertraulich zu behandelnde Daten gelten

- die gemäß 2.6 zu veröffentlichenden Informationen,

- Zertifikate, Widerrufslisten und Informationen über die Gründe für den Widerruf,

- die Certification Practice Statements und Policies der Zertifizierungsdiensteanbieter (das sind die nach § 6 Abs. 2 SigG anzuzeigenden Sicherheits- und Zertifizierungskonzepte mit Ausnahme der für interne Zwecke bestimmten Bestandteile der Sicherheitskonzepte) sowie Informationen über die von den Zertifizierungsdiensteanbietern angebotenen Signaturverfahren und -produkte.

2.8.3 Offenlegung von Widerrufen eines Zertifikates

Wird ein Zertifikat widerrufen, so wird der Grund für den Widerruf zumindest auf Anfrage veröffentlicht. Die Verwendung von Reason Codes in der Widerrufsliste (RFC 2459, Punkt 5.3.1) wird angestrebt.

Im Regelfall werden Zertifikate widerrufen werden, weil die zertifizierten Schlüssel ausgetauscht werden oder weil der zertifizierte Dienst eingestellt wird. In ersterem Fall erfolgt keine besondere Information. Über die Einstellung von Diensten eines Zertifizierungsdiensteanbieters wird auf der Website der Aufsichtsstelle informiert.

Wird ein Zertifikat widerrufen, weil der zertifizierte Schlüssel kompromittiert wurde, so erfolgt jedenfalls eine Information der Öffentlichkeit.

2.8.4 Informationsweitergabe an andere Behörden

Die Weitergabe von Informationen – gegebenenfalls auch solcher, die gemäß Punkt 2.8.1 als vertraulich zu behandeln sind – erfolgt entsprechend den Bestimmungen zur Amtshilfe (Art. 22 B-VG), zur Amtsverschwiegenheit (Art. 20 Abs. 3 B-VG) und zum Datenschutz (§ 1 DSG 2000).

2.8.5 Informationsweitergabe an Gerichte

Die Weitergabe von Informationen – gegebenenfalls auch solcher, die gemäß Punkt 2.8.1 als vertraulich zu behandeln sind – erfolgt entsprechend den Bestimmungen zur Amtshilfe (Art. 22 B-VG), zur Amtsverschwiegenheit (Art. 20 Abs. 3 B-VG) und zum Datenschutz (§ 1 DSG 2000).

3. Identifizierung und Authentifizierung

3.1 Erstregistrierung

3.1.1 Namen

Die Namen in allen nach diesem CPS ausgestellten Zertifikaten richten sich nach den Standards X.501 und X.520. Folgende Namensbestandteile werden verwendet:

Common Name (CN), Organizational Unit (OU), Organization (O) und Country (C).

Die Telekom-Control-Kommission wird mit C=AT, O=Telekom-Control-Kommission, die Telekom-Control GmbH mit C=AT, O=Telekom-Control GmbH bezeichnet.

Die verschiedenen Zertifikatskategorien werden unter OU ersichtlich gemacht.

3.1.2 Bedeutungstragende Namen

Für die Ausstellung eines Zertifikates an einen Zertifizierungsdienst ist erforderlich, dass der Name des Zertifizierungsdiensteanbieters korrekt geschrieben ist.

Bei natürlichen Personen muss der Vorname und Nachname im X.500-Namen aufscheinen. Die Beifügung einer frei gewählten Bezeichnung oder Marke, unter welcher der Anbieter im Geschäftsverkehr auftritt, ist zulässig und kann in das Attribut O oder in das Attribut OU aufgenommen werden.

Bei juristischen Personen muss die Firma – wenn diese im Firmenbuch aufscheint, in der dort verwendeten Schreibweise, soweit diese mit X.500 kompatibel ist – im X.500-Namen aufscheinen. Die Beifügung einer Marke oder Bezeichnung, unter der der Zertifizierungsdienst im Geschäftsverkehr angeboten wird, ist zulässig.

Bietet ein Zertifizierungsdiensteanbieter mehrere Zertifizierungsdienste an, so sind diese durch Namenszusätze zu unterscheiden. Diese Namenszusätze dürfen nicht irreführend sein. Insbesondere darf die Bezeichnung „qualifiziert“ nur für Dienste verwendet werden, bei welchen ausschließlich qualifizierte Zertifikate ausgestellt werden, und die Bezeichnung „akkreditiert“ nur für Zertifizierungsdienste, auf welche sich eine Akkreditierung gemäß § 17 SigG bezieht.

3.1.3 Regeln zur Interpretation verschiedener Namensformen

Verschiedene Namensformen gelten als äquivalent, wenn sie nach der Regel distinguishedNameMatch (X.501, 12.5.2) einander entsprechen.

3.1.4 Eindeutigkeit von Namen

Innerhalb der Zertifizierungshierarchie der Aufsichtsstelle müssen Namen eindeutig sein.

3.1.5 Prozeduren zur Auflösung von Namensstreitigkeiten

Die Aufsichtsstelle bietet keine Prozeduren zur Auflösung von Namensstreitigkeiten an. Diese sind durch namensrechtliche oder wettbewerbsrechtliche Maßnahmen im Zivilrechtsweg zu lösen.

Im Falle einer Namensänderung ist ein neues Zertifikat auszustellen.

3.1.6 Marken und Warenzeichen

Zur Beifügung von Marken oder Warenzeichen als Namenszusatz siehe 3.1.2.

Die Aufsichtsstelle bietet keine Prozeduren zur Auflösung von Markenstreitigkeiten an. Diese sind durch markenrechtliche oder wettbewerbsrechtliche Maßnahmen im Zivilrechtsweg zu lösen.

Im Falle der Änderung oder Streichung eines Namenszusatzes, der eine Marke oder ein Warenzeichen enthält, ist ein neues Zertifikat auszustellen.

3.1.7 Nachweis des Besitzes der privaten Schlüssel

Der Zertifikatswerber muss den Besitz des privaten Schlüssels nachweisen, indem ein PKCS#10-Zertifikatsantrag gestellt wird, welcher mit diesem privaten Schlüssel signiert wurde. Bei der Registrierung wird überprüft, ob die Signatur mit dem im Zertifikatsantrag enthaltenen öffentlichen Schlüssel verifiziert werden kann. Damit wird sichergestellt, dass es sich um korrespondierende Schlüssel handelt.

Die Unterstützung zusätzlicher Datenformate für einen Zertifikatsantrag wird angestrebt.

Weiters muss der Zertifikatswerber erklären, dass es sich beim vorgelegten öffentlichen Schlüssel (Signaturprüfdaten) um jenen handelt, dessen korrespondierender privater Schlüssel (Signaturerstellungsdaten) bei dem zu zertifizierenden Dienst eingesetzt wird.

3.1.8 Identitätsüberprüfung bei juristischen Personen

Für die Identitätsüberprüfung ist das persönliche Erscheinen eines entsprechend Bevollmächtigten erforderlich. Die Identität wird anhand eines amtlichen Lichtbildausweises geprüft. Die Vollmacht wird auf Plausibilität geprüft, beispielsweise durch einen Firmenbuchauszug oder durch telefonische Rückfrage. Eine Kopie des Lichtbildausweises sowie die Vollmacht und ein Vermerk über die vorgenommenen Überprüfungen werden zur Dokumentation genommen. <Die Prozedur der Identitätsüberprüfung bei juristischen Personen wird noch überarbeitet.>

3.1.9 Identitätsüberprüfung bei natürlichen Personen

Für die Identitätsüberprüfung ist das persönliche Erscheinen des Zertifizierungswerbers erforderlich. Die Identität wird anhand eines amtlichen Lichtbildausweises geprüft. Eine Kopie des Lichtbildausweises wird zur Dokumentation genommen.

3.2 Routinemäßige Zertifikatserneuerung

Die Zertifikate nach diesem CPS werden für eine Dauer von drei Jahren ausgestellt.

Im Monat vor Ablauf des Zertifikates wird ein neues Zertifikat ausgestellt. Wenn keine Änderung des Namens des Ausstellers oder des Zertifikatsempfängers und keine Änderung des öffentlichen Schlüssels vorliegt, ist keine neuerliche Identitätsprüfung und kein Antrag auf Verlängerung erforderlich.

Ist die Ausstellung eines neuen Zertifikats erforderlich, weil eine Namensänderung eingetreten ist oder weil ein Schlüssel ausgetauscht wurde, dann ist nach 3.1 vorzugehen.

3.3 Zertifikatserneuerung nach einem Widerruf

Grundsätzlich ist für die Ausstellung eines neuen Zertifikats nach 3.1 vorzugehen, insbesondere dann, wenn der Schlüssel des Zertifizierten ausgetauscht wurde.

Ein Schlüsselaustausch der Aufsichtsstelle wird im Regelfall so vorgenommen, dass zunächst die Ausstellung eines neuen Zertifikates und erst danach der Widerruf eines früheren Zertifikats erfolgt (siehe insbesondere die Ausführung zu den Zweitsystemen, 4.7). Ist dies im Einzelfall nicht möglich, so ist nach 3.1 vorzugehen.

3.4 Antrag auf Widerruf

Ein Antrag auf Widerruf von Zertifikaten kann von jedem Zertifikatsempfänger gestellt werden. Die verschiedenen Möglichkeiten zur Durchführung eines Widerrufs sind in Kapitel 4.4.3 erläutert.

Zertifikate, die die Aufsichtsstelle an sich selbst oder an die Telekom-Control GmbH ausgestellt hat, werden nur aufgrund eines entsprechenden Beschlusses der Aufsichtsstelle widerrufen.

Bei Zertifikaten, die die Aufsichtsstelle einem Zertifizierungsdiensteanbieter für einen seiner Zertifizierungsdienste ausgestellt hat, kann der Zertifikatsempfänger den Widerruf selbst veranlassen (siehe 4.4.3). Bei diesem automatisierten Widerruf ist keine Angabe von Gründen erforderlich. Da das Verzeichnis der Aufsichtsstelle gemäß § 13 Abs. 3 SigG vollständig sein muss, wird bei Auslösung des automatisierten Widerrufes aber eine Anzeige der Einstellung eines Zertifizierungsdienstes (§ 12 SigG) oder die Anzeige eines Umstandes, der eine ordnungsgemäße und dem Sicherheits- und Zertifizierungskonzept entsprechende Tätigkeit nicht mehr ermöglicht (§ 6 Abs. 5 SigG) vorzunehmen sein.

4. Anforderungen an den Betrieb

4.1 Antrag auf Ausstellung eines Zertifikats

Vor der Ausstellung eines Zertifikats werden folgende Daten des Zertifikatsempfängers erfasst:

- Name (siehe 3.1.1)
- Adresse
- Telefon- und Faxnummer (soweit vorhanden)
- E-Mail-Adresse(n)
- Website (soweit vorhanden)
- bei natürlichen Personen: Geburtsdatum und -ort
- bei juristischen Personen: Name, Geburtsdatum und -ort des Bevollmächtigten

- Weiters muss der Zertifikatsempfänger einen Antrag auf Ausstellung eines Zertifikates im Format PKCS#10 vorlegen.

Die Zuordnung, welche Kategorie von Zertifikaten auf den Zertifikatsempfänger anwendbar ist, wird von der Aufsichtsstelle vorgenommen.

Vor der Ausstellung des Zertifikates wird von zwei Mitarbeitern der Aufsichtsstelle gemeinsam geprüft:

- Geprüft wird, ob ein die Ausstellung des Zertifikates deckender Beschluss der Telekom-Control-Kommission vorliegt.

- Die oben genannten Daten werden auf ihre Korrektheit geprüft.

- Bei juristischen Personen wird der Bevollmächtigte zur Korrektheit der Daten und darüber befragt, ob es sich bei dem vorliegenden PKCS#10-Antrag um jene Schlüssel handelt, mit denen der zu zertifizierende Dienst erbracht wird. Weiters wird die Vollmacht auf Plausibilität geprüft und die Identität des Bevollmächtigten anhand eines amtlichen Lichtbildausweises überprüft. Die Vollmacht sowie eine Kopie des Lichtbildausweises wird zum Protokoll genommen.

- Bei natürlichen Personen wird die Person zur Korrektheit der Daten und darüber befragt, ob es sich bei dem vorliegenden PKCS#10-Antrag um jene Schlüssel handelt, mit denen der zu zertifizierende Dienst erbracht wird. Weiters wird die Identität anhand eines amtlichen Lichtbildausweises überprüft. Eine Kopie des Lichtbildausweises wird zum Protokoll genommen.

- Der Zertifikatsantrag muss dem Standard PKCS#10 entsprechen. <Die Unterstützung zusätzlicher Formate für den Zertifikatsantrag wird angestrebt.> Die Signatur des Antrags muss mit den im Antrag enthaltenen öffentlichen Schlüssel nachprüfbar sein, also mit dem korrespondierenden privaten Schlüssel erzeugt worden sein.

Über die vorgenommenen Überprüfungen wird ein Protokoll erstellt, welches vom Zertifizierungswerber und von beiden Mitarbeitern der Aufsichtsstelle unterschrieben wird.

Stellt sich bei der Überprüfung heraus, dass eine Voraussetzung nicht erfüllt ist, so wird dies dem Zertifizierungswerber, wenn davon auszugehen ist, dass das Problem leicht behebbar ist, mündlich mitgeteilt. Ansonsten lehnt die Telekom-Control GmbH die Ausstellung des Zertifikates im Auftrag der Telekom-Control-Kommission unter Angabe des Grundes schriftlich ab. Diese Ablehnung erfolgt nicht in Bescheidform.

Ist ein Zertifizierungswerber der Ansicht, ihm werde zu Unrecht kein Zertifikat ausgestellt, so steht es ihm frei, einen entsprechenden – insb. auf § 13 Abs. 3 bzw. § 17 SigG gestützten – Antrag zu stellen, über welchen bescheidmäßig abgesprochen wird.

4.2 Ausgabe von Zertifikaten

Ergibt die Überprüfung des Antrages, dass das Zertifikat auszustellen ist, so wird von den beiden Mitarbeitern der Telekom-Control GmbH gemeinsam das Zertifikat erstellt.

Die Erstellung des Zertifikates erfolgt in einem eigens dafür vorgesehenen Raum, welcher nur von zwei Personen gemeinsam betreten werden kann. Die beiden Mitarbeiter begeben sich in diesen Raum und schließen dessen Türe.

Die für den Zertifizierungsvorgang notwendige Hardware und Software befindet sich in einem Tresor, welcher nur von zwei Personen gemeinsam geöffnet werden kann. Die beiden Mitarbeiter öffnen den Tresor und entnehmen die Hardware.

Das Zertifikat wird mit den im Zertifizierungskonzept vorgesehenen Angaben vorbereitet.

Beide Mitarbeiter prüfen unabhängig voneinander die einzelnen Bestandteile des Zertifikates entsprechend Kapitel 7.1. Danach wird das Zertifikat von beiden gemeinsam erstellt. Die Software für die Zertifikatserstellung ist so konfiguriert, dass nur zwei berechtigte Personen das Zertifikat gemeinsam erstellen können.

Das erstellte Zertifikat wird auf eine leere Diskette exportiert, anschließend wird die Hardware wieder in den Tresor verbracht und der Tresor wird versperrt.

Von einem ebenfalls im sicheren Raum befindlichen Rechner wird eine gesicherte Verbindung in das Rechenzentrum aufgebaut und das Zertifikat wird in den Verzeichnisdienst der Aufsichtsstelle eingespielt. Anschließend wird überprüft, ob das Zertifikat allgemein abrufbar ist.

Die Diskette wird dem Zertifikatsempfänger ausgehändigt bzw. der Zertifikatsempfänger wird davon verständigt, dass das ausgestellte Zertifikat abrufbar ist.

4.3 Überprüfen von Zertifikaten

Beim Überprüfen von Zertifikaten der Aufsichtsstelle ist nach anerkannten Normen (insbesondere RFC 2459) vorzugehen. Punkt 2.1.4 dieses CPS enthält Empfehlungen für die Prüfung von Signaturen und Zertifikaten.

4.4 Sperre und Widerruf von Zertifikaten

Die Aufsichtsstelle nimmt prinzipiell keine zeitlich befristete Sperre von Zertifikaten vor, sondern ausschließlich Widerrufe. Falls sich herausstellt, dass die Gründe für einen Widerruf weggefallen sind, wird ein neues Zertifikat ausgestellt.

Der Widerrufsdienst der Aufsichtsstelle wird räumlich getrennt vom Zertifizierungsdienst in einem Rechenzentrum geführt. In regelmäßigen Abständen von einigen Stunden (siehe 4.4.9) werden Widerrufslisten (CRLs) im Format X.509v2 (RFC 2459) erzeugt. Bei jedem einzelnen Widerruf wird zudem umgehend eine neue Widerrufsliste erzeugt.

Die Widerrufslisten werden vom jeweils gültigen CERTIFICATE-REVOCATION-Schlüssel der Aufsichtsstelle signiert. Für diesen Schlüssel wird ein TOP-Zertifikat ausgestellt. Wird der CERTIFICATE-REVOCATION-Schlüssel ausgetauscht (z. B. im Fall der Kompromittierung), dann wird das TOP-Zertifikat für den alten Schlüssel widerrufen, indem es auf die mit dem neuen Schlüssel signierte Widerrufsliste aufgenommen wird.

Zu Beginn wird nur eine einzige Widerrufsliste für alle Zertifizierungsdienste der Aufsichtsstelle ausgegeben – also für alle jemals von der Aufsichtsstelle ausgegebenen und in diesem CPS beschriebenen Zertifikate, die widerrufen wurden. Möglicherweise werden zu einem späteren Zeitpunkt aufgrund des wachsenden Umfangs der Widerrufslisten mehrere verschiedene Widerrufslisten ausgegeben. In diesem Fall wird nach Maßgabe der technischen Möglichkeiten versucht werden, trotzdem eine Widerrufsliste zur Verfügung zu stellen, die die Gesamtheit der widerrufenen Zertifikate enthält. Zu Änderungen des Certification Practice Statement siehe Kapitel 8.

4.4.1 Gründe für einen Widerruf

Ein Widerruf ist in folgenden Fällen vorzunehmen:

4.4.1.1 Gründe, die auf der Seite des Zertifikatsempfängers liegen

- Der private Schlüssel, dessen korrespondierender öffentlicher Schlüssel im Zertifikat aufscheint, wurde kompromittiert, d. h. er wurde offenbart oder es ist Unbefugten gelungen, darauf zuzugreifen.

- Der Zertifizierungsdienst, für welchen das Zertifikat ausgestellt wurde, wurde eingestellt oder die weitere Ausübung des Dienstes wurde von der Aufsichtsstelle (§ 14 Abs. 2 und 5 TKG) oder von der Telekom-Control GmbH (§ 15 Abs. 2 Z 7 SigG) untersagt.

- Eine für die Ausstellung des Zertifikates wesentliche Eigenschaft des zertifizierten Dienstes oder des Zertifizierungsdiensteanbieters ist weggefallen. Insbesondere: Eine Akkreditierung wurde aufgehoben (ACCREDITED-CERTIFICATION-SERVICES-Zertifikate) oder die für die Ausstellung eines CROSS-CERTIFICATION-Zertifikates maßgebliche Eigenschaft ist weggefallen.

- Die Aufsichtsstelle oder die Telekom-Control GmbH haben aus einem anderen Grund den Widerruf eines Zertifikates angeordnet.

- Ein Widerruf des Zertifikates kann auch, muss aber nicht erfolgen, wenn der Zertifikatsempfänger seinen privaten Schlüssel verliert, ohne dass die Gefahr besteht, dass der private Schlüssel missbraucht werden kann (beispielsweise durch einen technischen Defekt der eingesetzten Signaturerstellungseinheit).

4.4.1.2 Gründe, die auf der Seite des Zertifikatsausstellers liegen

- Der private Schlüssel, mit welchen das Zertifikat signiert wurde, wurden kompromittiert, d. h. er wurden offenbart oder es ist Unbefugten gelungen, darauf zuzugreifen.

- Der entsprechende Zertifizierungsdienst der Aufsichtsstelle wird eingestellt oder durch einen anderen Zertifizierungsdienst ersetzt (vgl. dazu die Darstellung des Schlüsselaustausches im Rahmen der von der Aufsichtsstelle eingesetzten Zweitsysteme, 4.7).

4.4.1.3 Technische Gründe

Im Fall, dass die von der Aufsichtsstelle eingesetzten Algorithmen oder Schlüssellängen nicht mehr sicher genug erscheinen, entscheidet die Aufsichtsstelle, ob angesichts der konkreten Bedrohung die ausgestellten Zertifikate zu widerrufen sind oder ob innerhalb einer angemessenen Frist andere Algorithmen oder größere Schlüssellängen eingesetzt werden.

4.4.2 Wer kann einen Widerruf beantragen

Der Widerruf kann vom Zertifikatsempfänger beantragt werden. Die Zertifikatsempfänger haben dazu die Möglichkeit eines automatisierten Widerrufs. Diese ermöglicht es ihnen, selbsttätig und jederzeit einen Widerruf vorzunehmen, der umgehend im Widerrufsdienst der Aufsichtsstelle verzeichnet und veröffentlicht wird. Darüber hinaus besteht die Möglichkeit, eines schriftlichen Antrages auf Widerruf. (Siehe oben 3.4)

Darüber hinaus ist der Widerruf vorzunehmen, wenn eine entsprechende Entscheidung der Telekom-Control-Kommission oder der Telekom-Control GmbH vorliegt.

Dritte Personen können einen Widerruf lediglich anregen.

4.4.3 Verfahren zur Durchführung eines Widerrufs

Die zur Durchführung eines Widerrufs berechtigten Mitarbeiter der Aufsichtsstelle haben einen Widerruf dann vorzunehmen, wenn

- eine rechtskräftige Entscheidung der Telekom-Control-Kommission oder der Telekom-Control GmbH dazu vorliegt oder

- eine entsprechende Entscheidung bloß deshalb noch nicht rechtskräftig ist, weil ihre Zustellung nicht vorgenommen werden kann, oder

- auf Antrag des Zertifikatsempfängers.

Bei der Ausstellung eines ACCREDITED-CERTIFICATION-SERVICES-Zertifikats, eines QUALIFIED-CERTIFICATION-SERVICES-Zertifikats, eines CERTIFICATION-SERVICES-Zertifikats oder eines CROSS-CERTIFICATION-SERVICES-Zertifikats wird dem Zertifikatsempfänger die Möglichkeit eines automatisierten Widerrufs gegeben. Diese ermöglicht es ihm, selbsttätig und jederzeit einen Widerruf vorzunehmen, der umgehend im Widerrufsdienst der Aufsichtsstelle verzeichnet und veröffentlicht wird.

Die Möglichkeit des automatisierten Widerrufs besteht darin, dass dem Zertifikatsempfänger bei der Ausstellung des Zertifikates eine Codezahl übergeben wird, mit welcher der Widerruf genau dieses Zertifikates möglich ist. Weiters wird dem Zertifikatsempfänger eine Telefonnummer genannt, unter welcher der Widerruf rund um die Uhr beantragt werden kann. Bei der Bekanntgabe der Codezahl in einem Telefonat zu dieser Telefonnummer erfolgt keine Identitätsprüfung, sondern lediglich ein Rückruf zur Dokumentation des Widerrufsvorgangs. Der Widerruf kann also von jeder Person ausgelöst werden, die über die Kenntnis der Codezahl verfügt.

Ist einem Zertifikatsempfänger der automatisierte Widerruf nicht mehr möglich, so kann er den Widerruf auch entsprechend den Bestimmungen des Allgemeinen Verwaltungsverfahrensgesetzes (vgl. insbesondere § 13 AVG) beantragen. Als Amtsstunden iSd § 13 Abs. 4 AVG gelten die Zeiten von 09:00 bis 15:30 (Montag bis Donnerstag, wenn Werktag) bzw. 09:00 bis 13:00 (Freitag, wenn Werktag). Der Antrag muss vom Antragsteller selbst oder von Personen, die für den Antragsteller vertretungsbefugt sind, entweder eigenhändig unterschrieben oder mit einer gültigen sicheren elektronischen Signatur versehen werden. Ein Widerruf wird aufgrund eines solchen Antrages erst dann vorgenommen, wenn sich aus dem Antrag unmissverständlich ergibt, dass der Antragsteller den Widerruf eines ihn selbst betreffenden Zertifikates wünscht, wenn das zu widerrufende Zertifikat genau bezeichnet ist, wenn der Antrag nicht an Bedingungen geknüpft ist und wenn dargelegt ist, warum der Antragsteller die Möglichkeit, den Widerruf selbst vorzunehmen, nicht nutzen kann. Diesfalls wird der Widerruf innerhalb von maximal drei Stunden vorgenommen. Bei Mängeln des Antrages geht die Aufsichtsstelle nach § 13 Abs. 3 AVG vor und trägt dem Antragsteller die Behebung des Mangels auf.

Ein Widerruf kann auch von der Aufsichtsstelle gemäß § 14 Abs. 1 SigG oder von der Telekom-Control GmbH gemäß § 15 Abs. 2 Z 7 SigG angeordnet werden.

Der Zertifikatsempfänger ist in jedem Fall vom erfolgten Widerruf zu verständigen.

4.4.4 Dauer der Durchführung eines Widerrufs

Ein vom Zertifikatsempfänger veranlasster Widerruf in automatisierter Form wird umgehend innerhalb weniger Minuten durchgeführt, indem eine neue Widerrufsliste erstellt und veröffentlicht wird.

Ein schriftlich beantragter Widerruf wird – unter der Voraussetzung, dass der Antrag mängelfrei eingebracht wird – innerhalb der Geschäftszeiten in maximal drei Stunden bearbeitet (siehe oben 4.4.3).

4.4.5 Gründe für eine Sperre

Nicht anwendbar. Die Zertifikate der Aufsichtsstelle werden niemals auf eine befristete Zeit gesperrt, sondern ausschließlich widerrufen.

4.4.6 Wer kann eine Sperre beantragen?

Nicht anwendbar.

4.4.7 Verfahren zur Durchführung einer Sperre

Nicht anwendbar.

4.4.8 Begrenzung der Dauer einer Sperre

Nicht anwendbar

4.4.9 Häufigkeit der Veröffentlichung von Widerrufslisten (CRLs)

Widerrufslisten werden in Abständen von einigen Stunden veröffentlicht. Der genaue Abstand wird nach den Möglichkeiten der von der Aufsichtsstelle eingesetzten Software und nach den Bedürfnissen der Abfragenden festgelegt und auf der Website der Aufsichtsstelle veröffentlicht (http://www.signatur.tkc.at/de/directory/ und https://www.signatur.tkc.at/de/directory/). Es werden kurze Abstände zwischen den einzelnen Veröffentlichungen angestrebt. Dabei soll aber darauf Bedacht genommen werden, dass für jene Nutzer, die das Verzeichnis häufig abfragen, der notwendige Datenverkehr im vernünftigen Ausmaß begrenzt bleibt.

Im Falle eines Widerrufs wird jedenfalls umgehend innerhalb einiger Minuten eine neue Widerrufsliste veröffentlicht.

4.4.10 Anforderungen an die Überprüfung von Widerrufslisten

Für sämtliche Zertifizierungsdienste der Aufsichtsstelle wird nur eine Widerrufsliste geführt, in die alle jemals widerrufenen Zertifikate aufgenommen werden. Da der Standard X.509 erst ab Version 2 eine Unterscheidung mehrerer Zertifikatsherausgeber innerhalb einer Widerrufsliste ermöglicht, muss auch die bei der Überprüfung verwendete Software X.509v2-Widerrufslisten interpretieren können.

Um Abfragezeiten zu verkürzen, wird eine weitere Widerrufsliste geführt, in die nur jene Zertifikate aufgenommen werden, die noch gültig wären. Soll eine Signatur daraufhin überprüft werden, ob sie momentan gültig ist, so genügt es, diese kürzere Liste zu überprüfen. Soll die Gültigkeit einer Signatur zu einem früheren Zeitpunkt überprüft werden, so muss die vollständige Liste herangezogen werden.

Die Aufsichtsstelle behält sich vor, zu einem späteren Zeitpunkt mehrere verschiedene Widerrufslisten zu erstellen oder für den Widerrufsdienst eine andere Technologie als Widerrufslisten zu verwenden. In diesem Fall wird mindestens ein Jahr vor der Systemumstellung das Certification Practice Statement entsprechend geändert. Programme, die eine automatisierte Signaturprüfung vornehmen und dabei auf die Widerrufsdienste der Aufsichtsstelle zugreifen, sollten daher zumindest jährlich auf ihre korrekte Funktion überprüft werden.

4.4.11 Online-Möglichkeit, Widerrufe zu überprüfen

Der Status eines Zertifikates kann auch über die Website der Aufsichtsstelle überprüft werden (http://www.signatur.tkc.at/de/directory/ und https://www.signatur.tkc.at/de/directory/). Auf der Website der Aufsichtsstelle sind die näheren Modalitäten beschrieben.

Eine Überprüfung mittels OCSP wird vorerst nicht angeboten.

4.5 Protokolle

4.5.1 Protokollierte Ereignisse

Zu protokollieren sind:

- Zutritte zum sicheren Raum der Aufsichtsstelle, zum Tresor im sicheren Raum und zu den Rechnern des Verzeichnisdienstes und des Widerrufsdienstes
- ausgelöste Alarme bei der Alarmanlage des sicheren Raumes
- jeder über die Firewall erfolgte Zugriff oder Zugriffsversuch (IP-Adressen, Ports, etc.)
- <Systemprotokolle: Nach dem Ankauf der Systeme für die Publik-Key-Infrastruktur wird die Protokollierung weiterer Ereignisse (wie der Start und die Beendigung von Systemprozessen, Störfälle und besondere Betriebssituationen sowie systembedingte Fehlermeldungen) spezifiziert werden.>

4.5.2 Häufigkeit der Protokollüberprüfung

Die Protokolle der Zutrittskontrolle zum sicheren Raum der Aufsichtsstelle werden mindestens einmal wöchentlich, die Protokolle der Zutrittskontrolle zum Sicherheitsschrank im Rechenzentrum mindestens einmal monatlich überprüft.

Alarme werden jeweils umgehend bearbeitet.

Firewallprotokolle und andere Systemprotokolle werden an Werktagen täglich überprüft.

4.5.3 Aufbewahrungsdauer der Protokolldateien

Die Protokolle werden grundsätzlich drei Jahre lang aufbewahrt.

4.5.4 Schutz der Protokolldateien

Die Protokolle der Firewall und die Systemprotokolle (Start und Beendigung von Systemprozessen, systembedingte Fehlermeldungen etc.) werden als Logdateien auf den Rechnern des Verzeichnis- und Widerrufsdienstes gespeichert und mit dem jeweiligen Betriebssystem gegen unbefugten Zugriff geschützt. Diese Rechner sind entweder nicht an das Internet angebunden oder durch Firewalls zusätzlich gegen unbefugten Zugriff geschützt.

Die Zutrittsprotokolle und Alarmanlagenprotokolle werden vom Zutrittskontrollsystem bzw. von der Alarmzentrale verwaltet und durch diese gegen unbefugten Zugriff bzw. Veränderung geschützt.

Eine Person, die die Rolle „Zutrittsverwaltung“ oder „Zutrittskontrolle“ wahrnimmt, hat lediglich Zugang zu den Zutrittsprotokollen.

„Systemadministratoren“ haben Zugang zu allen Systemprotokollen von Rechnern, die zur Public-Key-Infrastruktur der Aufsichtsstelle gehören.

„Identitätsprüfer“ und „CA-Operatoren“ haben Zugang zu allen Protokollen des Zertifizierungsdienstes, des Verzeichnisdienstes und des Widerrufsdienstes.

Eine Person, die die Rolle „Widerruf (Call-Center)“ wahrnimmt, hat keinen Zugang zu Protokollen (abgesehen von den allenfalls von ihr selbst erstellten Protokollen des Widerrufsdienstes).

„Rechenzentrumsmitarbeiter“ und „Rechenzentrumsprüfer“ haben Zugang zu jenen Systemprotokollen, die zur Aufrechterhaltung des Verzeichnisdienstes und zur Bereithaltung der aktuellen Widerrufsliste erforderlich sind.

Eine Person, die die Rolle „Backup Verzeichnisse“ wahrnimmt, kann von allen Protokolldateien Sicherungskopien anfertigen, nimmt aber selbst nur in die Protokolle des Archivierungsprogramms Einsicht.

Jene Person, die die Rolle „Auditor“ wahrnimmt, hat uneingeschränkten Zugang zu allen Protokollen.

Den Personen wird jeweils nur ein Leserecht, kein Schreibrecht oder eine Möglichkeit der Löschung eingeräumt. Soweit dies nicht möglich ist (Systemadministratoren), sind die Protokolle durch das Vier-Augen-Prinzip geschützt.

Für die Firewallprotokolle und die Systemprotokolle wird angestrebt, die Protokolle in regelmäßigen Abständen (z. B. täglich) in das Archivierungssystem gemäß Punkt 4.6 zu übernehmen. Das Archivierungssystem schützt die enthaltenen Daten durch sichere Zeitstempel vor nachträglichen Veränderungen.

4.5.5 Backups der Protokolldateien

Von den Firewallprotokollen und Systemprotokollen wird zumindest täglich (werktags) ein Backup erstellt.

4.5.6 Protokollsystem (intern/extern)

Das Zutrittskontrollsystem und die Alarmanlage und damit die von diesen Systemen geschützten Daten befinden sich innerhalb des sicheren Raumes.

Logdateien werden auf den jeweiligen Rechnern gespeichert und befinden sich innerhalb der gegen unbefugten Zutritt gesicherten Bereiche.

4.5.7 Bekanntgabe an den Auslöser eines Ereignisses

Im Regelfall ist den Mitarbeitern, deren Tätigkeit die Protokollierung eines Ereignisses auslöst, der Umstand der Protokollierung bekannt.

Von Unbefugten ausgelöste Alarme (Alarmanlage, Firewall, etc.) werden den betreffenden Personen im Regelfall nicht bekannt gegeben.

4.5.8 Bewertung der Sicherheitsrisiken

Folgenden Sicherheitsrisiken wird durch das vorliegende Konzept entgegengewirkt:

- Ausfall des Protokollsystems durch unzulässige Handlungen von Eindringlingen oder einzelnen Mitarbeitern der Aufsichtsstelle sowie durch technisches Versagen

- Einsichtnahme in Protokolle durch Unbefugte infolge einer Indiskretion oder eines technischen Versagens

4.6 Archivierung

4.6.1 Arten erfasster Ereignisse

Folgende Ereignisse werden archiviert:

- Der Lebenszyklus jedes Schlüsselpaares: Zeitpunkt der Erzeugung des Schlüsselpaars, Namen der Mitarbeiter, die das Schlüsselpaar erzeugt haben, Rolle des Schlüsselpaares in der Zertifizierungshierarchie (Bezeichnung des Schlüsselpaares), öffentlicher Schlüssel; Zeitpunkte, an denen die Rolle eines Schlüsselpaares geändert wurde (z. B. wenn das Zweitsystem zum Hauptsystem wird); jeder Einsatz des privaten Schlüssels und die Namen der Mitarbeiter, die den Einsatz veranlasst haben; Zeitpunkt und Umstände der Zerstörung oder Inaktivierung des privaten Schlüssels und die Namen der beteiligten Mitarbeiter.

- Der Lebenszyklus jedes Zertifikates: Zertifizierungsanträge, die in 4.1 genannten Daten, Zeitpunkt der Ausstellung und der Veröffentlichung und Namen der Mitarbeiter, die das Zertifikat erzeugt haben; Anträge auf Widerruf bzw. die Umstände eines automatisierten Widerrufes, Zeitpunkt des Widerrufs, die dafür maßgeblichen Gründe und die Namen der Mitarbeiter, die das Zertifikat widerrufen haben, Ende der Gültigkeitsdauer des Zertifikates.

- Die Ausgabezeitpunkte von Widerrufslisten.

- Protokolle über die Abläufe beim Wechsel auf das Zweitsystem (siehe 4.7)

- Störfälle und besondere Betriebssituationen

- Nach Möglichkeit auch die Firewallprotokolle und Systemprotokolle (siehe 4.5.6)

4.6.2 Aufbewahrungsdauer archivierter Daten

Archivierte Daten werde gemäß § 16 Abs. 2 SigV zumindest 33 Jahre nach der letzten Eintragung in das Archivierungssystem aufbewahrt und lesbar gehalten

Firewallprotokolle und Systemprotokolle werden grundsätzlich drei Jahre aufbewahrt.

4.6.3 Schutz des Archivs

Das Archivsystem befindet sich außerhalb des sicheren Raumes der Aufsichtsstelle in einem Raum der Telekom-Control GmbH. Der Zutritt ist nur einem Teil der Mitarbeiter möglich, es gibt aber kein Vier-Augen-Prinzip.

Die archivierten Dateien sind auf Betriebssystemebene oder im Archivierungssystem durch die Vergabe von Zugriffsrechten entsprechend den in 4.5.4 beschriebenen Rollen geschützt.

Gegen nachträgliche Veränderungen werden die Daten durch sichere Zeitstempel geschützt. Die Zeitstempel sind so anzubringen, dass auch die Löschung von Daten auffallen würde (z. B. durch Zeitstempelung eines Inhaltsverzeichnisses).

4.6.4 Vorgangsweisen beim Erstellen von Sicherungskopien des Archivs

Vom Archiv wird täglich (an Werktagen) ein Backup erstellt. Die Backups werden entsprechend dem Backupkonzept der Telekom-Control GmbH, welches einen nicht veröffentlichten Teil des Sicherheits- und Zertifizierungskonzeptes bildet (siehe 8.2), regelmäßig ausgelagert.

4.6.5 Erfordernisse für Zeitstempel auf Archivinhalten

Die Zeitstempel entsprechen den Anforderungen an sichere Zeitstempel gemäß §§ 9 und 14 SigV.

4.6.6 Internes oder externes Archivierungssystem

Die zur Archivierung bestimmten Daten werden durch die für den Zertifizierungsdienst, für den Verzeichnisdienst bzw. für den Widerrufsdienst verwendete Software intern gesammelt.

4.6.7 Vorgangsweisen beim Erfassen und Überprüfen von Archivinformation

Die Erfassung von Archivinformation geschieht automatisch durch das jeweilige Programm.

Beim Überprüfen von Archivinformation soll der Zeitstempel beachtet werden.

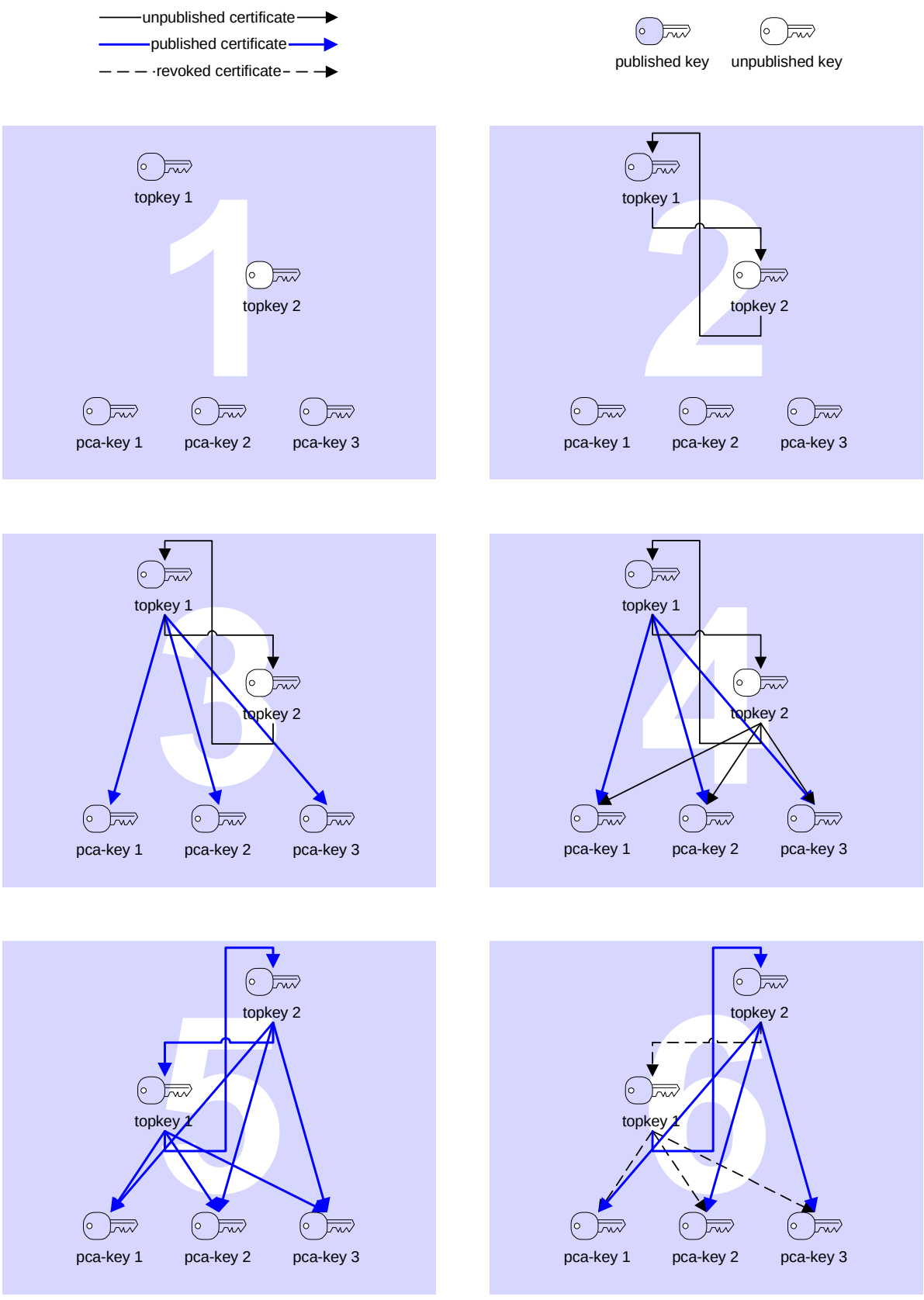
4.7 Zweitsysteme und Austausch von Schlüsseln

§ 3 Abs. 1 SigV verpflichtet die Aufsichtsstelle dazu, ein Zweitsystem zu führen, auf das im Falle des Ausfalls oder der Kompromittierung des Hauptsystems zurückgegriffen werden kann. Dieser Verpflichtung wird folgendermaßen entsprochen:

4.7.1 Zweitsystem für den TOP-Schlüssel

Das Zweitsystem für den TOP-Schlüssel ist in der folgenden Grafik dargestellt:

Topkey replacement



Schritt 1: Für den aktuellen TOP-Schlüssel (in der Grafik Topkey1) wird ein Zweitschlüssel (in der Grafik Topkey2) als Backup erzeugt. Beide Schlüsselpaare werden in einer separaten Hardwareeinheit (die die Erfordernisse einer sicheren Signaturerstellungseinheit erfüllt) erzeugt und gespeichert. Die privaten Schlüssel verlassen die jeweilige Signaturerstellungseinheit niemals.

Schritt 2: Mit jedem der beiden TOP-Schlüssel wird für den jeweils anderen Schlüssel ein Zertifikat ausgestellt. Das von Topkey1 für Topkey2 ausgestellte Zertifikat dient später dazu, den nahtlosen Übergang vom Vorgänger (Topkey1) auf den Nachfolger (Topkey2) sicherzustellen. Das umgekehrte Zertifikat dient später dazu, auch vom Nachfolger (Topkey2) ausgehend eine ununterbrochene Zertifikatskette zu Zertifikaten des Vorgängers (Topkey1) herstellen zu können (obwohl diese Kette nicht unbedingt erforderlich ist). Beide Zertifikate werden vorerst geheim gehalten und getrennt von den beiden Schlüsseln aufbewahrt.

Schritt 3: Topkey1 ist der aktuelle TOP-Schlüssel. Mit ihm werden die TOP-Zertifikate für die PCA-Schlüssel der Aufsichtsstelle und die CERTIFICATE-REVOCATION-Schlüssel der Aufsichtsstelle signiert. Diese Zertifikate werden veröffentlicht.

Schritt 4: Topkey2 ist der Nachfolger des aktuellen TOP-Schlüssels. Mit ihm werden Zertifikate für die PCA-Schlüssel der Aufsichtsstelle und die CERTIFICATE-REVOCATION-Schlüssel der Aufsichtsstelle signiert. Diese Zertifikate werden vorerst nicht veröffentlicht. Der in der Grafik in Schritt 4 dargestellte Zustand ist der Normalzustand.

Schritt 5: Wenn Topkey1 kompromittiert wird oder wenn er ersetzt wird (z. B. weil die Schlüssellänge nicht mehr ausreicht oder weil die Signaturerstellungseinheit, in der er gespeichert ist, ausgefallen ist), dann wird sein Nachfolger Topkey2 zum aktuellen Schlüssel erklärt. Dieser Wechsel wird im Amtsblatt zur Wiener Zeitung (§ 13 Abs. 3 SigG) und auf der Website der Aufsichtsstelle (§ 18 Abs. 6 SigV) verlautbart (siehe unten 4.7.1.1). Gleichzeitig werden die von Topkey1 und Topkey2 wechselseitig ausgestellten Zertifikate veröffentlicht. Das von Topkey1 signierte Zertifikat des Topkey2 ermöglicht es den Nutzern, die Korrektheit des Schlüsselaustausches nachzuvollziehen.

Schritt 6: Wenn der Schlüsselaustausch vorgenommen wurde, weil der TOP-Schlüssel Topkey1 kompromittiert wurde, werden die von Topkey1 an die PCA-Schlüssel und die CERTIFICATE-REVOCATION-Schlüssel ausgestellten Zertifikate umgehend widerrufen. Weiters wird das von Topkey2 an Topkey1 ausgestellte Zertifikat widerrufen, da Topkey1 nicht mehr vertraut werden darf. Das von Topkey1 an Topkey2 ausgestellte Zertifikat wird nicht widerrufen, um die in Schritt 5 dargestellte Nachvollziehbarkeit des Schlüsselwechsels nicht zu gefährden. – Wenn keine Kompromittierung von Topkey1 vorlag, dann wird Schritt 6 erst eine gewisse Zeit nach der allgemeinen Verlautbarung gemäß Schritt 5 vorgenommen, um den Nutzern einen langsameren Übergang zu ermöglichen. Der Zeitpunkt des Widerrufs gemäß Schritt 6 wird in den Verlautbarungen nach Schritt 5 angekündigt.

Schritt 7 (in der Grafik nicht dargestellt): Nach dem Wechsel von Topkey1 zu Topkey2 wird in einem Drittsystem Topkey3 erzeugt und sinngemäß bei Schritt 2 fortgesetzt.

Der Übersicht halber ist in der Grafik oben nicht dargestellt, dass es für jeden TOP-Schlüssel auch ein selbstsigniertes Zertifikat gibt.

Die oben beschriebene Prozedur dient unter anderem der Vorbeugung für den Fall der Kompromittierung des Hauptsystems. Im Falle der Kompromittierung des Zweitsystems werden die von Topkey1 für Topkey2 und alle von Topkey2 ausgestellten Zertifikate widerrufen. Anschließend wird ein neues Zweitsystem eingerichtet (Wiederholung ab Schritt 2). Um der Gefahr einer Kompromittierung des Zweitsystems vorzubeugen, werden die

Signaturerstellungseinheit des Topkey2 und die von Topkey1 und Topkey2 wechselseitig ausgestellten Zertifikate getrennt aufbewahrt (siehe Schritt 2).

4.7.1.1 Veröffentlichung eines Wechsel des TOP-Schlüssels

Der Wechsel des TOP-Schlüssels der Aufsichtsstelle ist ein sicherheitskritisches Ereignis und betrifft alle, die auf die Zertifizierungsdienste der Aufsichtsstelle vertrauen und den TOP-Schlüssel der Aufsichtsstelle in ihrer Software in irgendeiner Form als Wurzel des Vertrauens oder dergleichen eingetragen haben. Diese Personen haben vor allem darauf zu achten, dass der Wechsel tatsächlich von der Aufsichtsstelle verlautbart wird und nicht von einer Person, die sich in betrügerischer Absicht als die Aufsichtsstelle ausgibt.

Die Veröffentlichung des Wechsels erfolgt

- durch die Veröffentlichung des vom alten TOP-Schlüssel signierten Zertifikates für den neuen TOP-Schlüssel im Verzeichnis der Aufsichtsstelle,
- im Amtsblatt zur Wiener Zeitung (§ 13 Abs. 3 SigG),
- auf der Website der Aufsichtsstelle (§ 18 Abs. 6 SigV) unter der Adresse http://www.signatur.tkc.at/de/directory/ und https://www.signatur.tkc.at/de/directory/,
- durch eine Presseaussendung an die einschlägige Fachpresse und
- durch Versenden eines Newsletters der Aufsichtsstelle.

In allen Veröffentlichungen werden jedenfalls Informationen genannt, mit denen das selbstsignierte Zertifikat des neuen TOP-Schlüssels eindeutig identifiziert werden kann, insbesondere der Fingerprint des Zertifikates.

Alle Zertifikatsempfänger werden über den Wechsel verständigt.

Weiters werden umgehend jene Stellen informiert, die dem alten TOP-Schlüssel ein Cross-Zertifikat ausgestellt haben. Diese Information erfolgt aber nur dann, wenn das Cross-Zertifikat unter Mitwirkung der Aufsichtsstelle zustandegekommen ist. Personen oder Einrichtungen, die der Aufsichtsstelle ohne deren Mitwirkung ein Cross-Zertifikat ausgestellt haben, haben keinen Anspruch darauf, verständigt zu werden. Die Aufsichtsstelle übernimmt auch keine Haftung dafür, dass der Newsletter alle Personen erreicht, die sich auf den entsprechenden Mailverteiler eintragen haben lassen.

Personen, die überprüfen wollen, ob der neue TOP-Schlüssel sich tatsächlich im Besitz der Aufsichtsstelle befinden, können

- das vom alten TOP-Schlüssel signierte Zertifikat für den neuen TOP-Schlüssel überprüfen. Diese Methode der Überprüfung ist die sicherste, zusätzlich sollten aber allfällige Hinweise in der Verlautbarung der Aufsichtsstelle geprüft werden.
- die Veröffentlichung im Amtsblatt zur Wiener Zeitung heranziehen. Zusätzlich sollten andere Methoden der Überprüfung gewählt werden, da auch ein Unbefugter die Veröffentlichung hätte veranlassen können.
- die Veröffentlichung auf der Website der Aufsichtsstelle heranziehen. Dabei sollte darauf geachtet werden, dass eine gesicherte Verbindung mit HTTPS aufgebaut wird. Das dabei vom Server verwendete Zertifikat sollte geprüft werden. Zusätzlich sollten andere Methoden der Überprüfung gewählt werden.

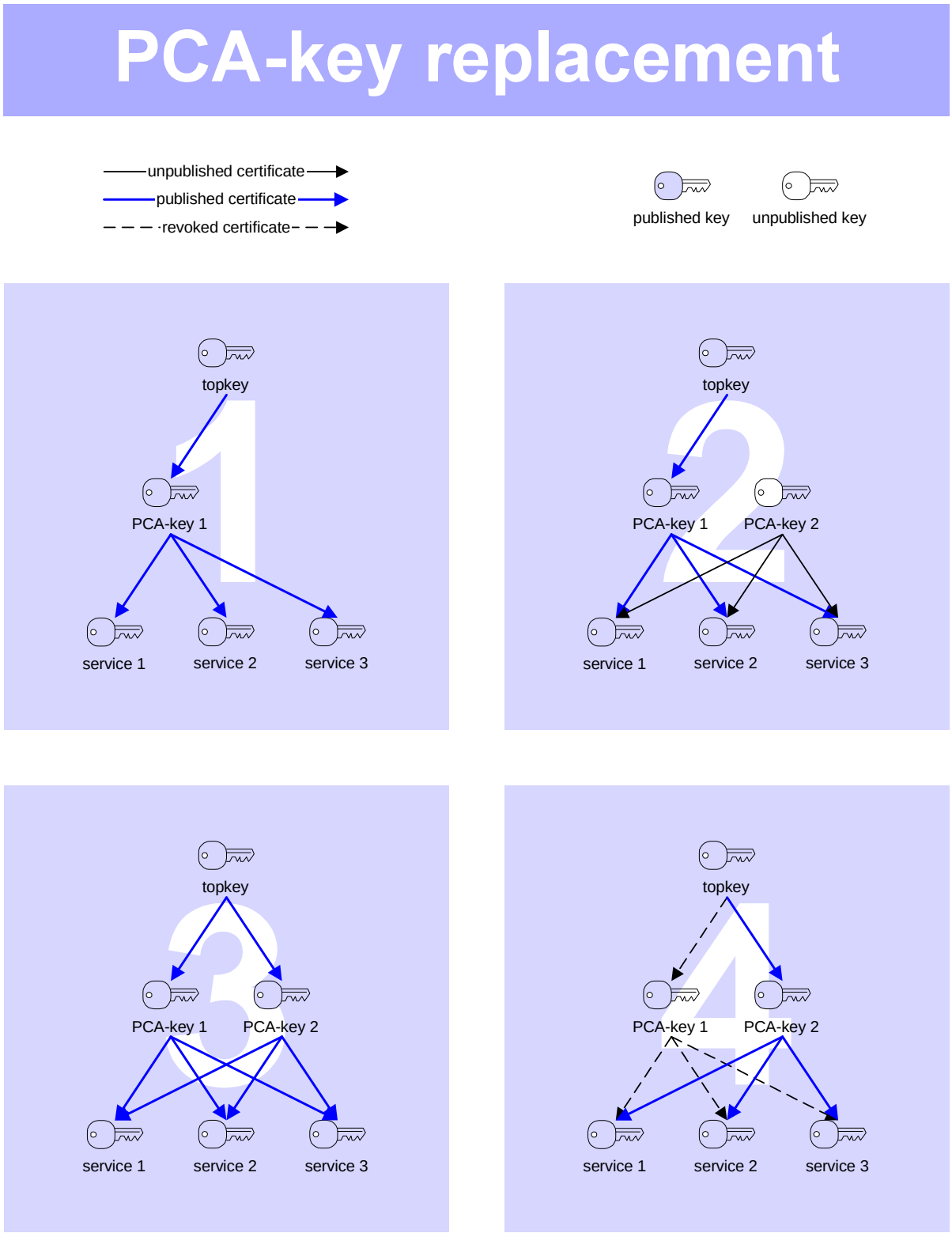
- den Fingerprint bei der Hotline der Aufsichtsstelle, 0800/300300 erfragen <Das ist noch nicht implementiert. Es ist noch zu entscheiden, ob es implementiert wird.> Vor dem Anruf bei der Hotline sollte den Hinweisen auf der Website der Aufsichtsstelle entsprechend das neue TOP-Zertifikat installiert und der Fingerprint errechnet werden. Die MitarbeiterInnen der Hotline erteilen keine technischen Hinweise und geben keine Unterstützung beim Wechsel des Zertifikates, sondern geben ausschließlich den Fingerprint des neuen Zertifikates bekannt.

JournalistInnen und Medien werden ersucht, sich vor der Berichterstattung über einen angeblichen Wechsel des TOP-Schlüssels der Aufsichtsstelle sorgsam zu vergewissern, dass die Information tatsächlich von der Aufsichtsstelle stammt und nicht von einer Person, die sich in betrügerischer Absicht als die Aufsichtsstelle ausgeben will.

Vgl. auch die Kontaktinformationen unter Punkt 1.4.

4.7.2 Zweitsysteme für die PCA-Schlüssel

Das Zweitsystem für einen PCA-Schlüssel ist in der folgenden Grafik in vier Schritten dargestellt:



Schritt 1 zeigt die Zertifizierungshierarchie im Grundzustand. Es ist kein Zweitsystem eingesetzt. Die beiden oberen Schlüssel (topkey und PCA-key 1) sind die Schlüssel der Aufsichtsstelle, die drei unteren Schlüssel sind Schlüssel dreier Zertifizierungsdiensteanbieter.

In Schritt 2 wird in einer separaten Hardwareeinheit (die die Erfordernisse einer sicheren Signaturerstellungseinheit erfüllt) ein weiterer PCA-Schlüssel erzeugt und gespeichert. Die jeweiligen privaten Schlüssel verlassen die jeweilige Signaturerstellungseinheit niemals. Mit

dem zweiten PCA-Schlüssel werden ebenfalls Zertifikate für die Zertifizierungsdienste ausgestellt, aber vorerst nicht veröffentlicht.

Schritt 3: Wenn der PCA-Schlüssel ausgetauscht werden soll (z. B. im Falle der Kompromittierung von PCA-key 1, aber auch dann, wenn seine Schlüssellänge nicht mehr ausreicht oder wenn die Signaturerstellungseinheit, in der PCA-key 1 gespeichert ist, ausfällt), dann wird der PCA-key 2 zum aktuellen PCA-Schlüssel erklärt, indem ihm ein TOP-Zertifikat ausgestellt wird. Gleichzeitig wird der PCA-key 2 und alle seine Zertifikate veröffentlicht. Die Aufsichtsstelle wird über den Wechsel des PCA-Schlüssels auch auf ihrer Website informieren.

Schritt 4: Nach dem Wechsel werden alle Zertifikate von und für PCA-key 1 widerrufen. Im Fall der Kompromittierung des PCA-key 1 wird dieser Widerruf umgehend vorgenommen, ansonsten kann, um einen langsameren Übergang zu ermöglichen, einige Zeit zugewartet werden. Über den Zeitraum bis zum Widerruf wird die Aufsichtsstelle in der Information gemäß Schritt 3 informieren.

Ein Programm, das die Signaturprüfung automatisiert vornimmt, muss den in Schritt 4 vorgenommenen Widerruf aus der Widerrufsliste erkennen. Es kann in diesem Fall automatisch nach dem Nachfolger des widerrufenen Schlüssels suchen. Zu diesem Zweck wird der Verzeichnisdienst nach einem Zertifikat befragt, das auf denselben Namen ausgestellt ist wie das widerrufene Zertifikat (zur Übereinstimmung von Namen siehe 3.1.3).

Solange von einem PCA-Schlüssel höchstens fünf Zertifikate ausgestellt wurden, wird die Aufsichtsstelle lediglich die nötige Technologie für ein Zweitsystem vorrätig halten, dieses aber nicht einsetzen. Der Normalzustand ist daher der in Schritt 1 dargestellte Zustand. Die Schlüsselgenerierung des PCA-key 2 und die Ausstellung von Ersatzzertifikaten (Schritt 2) erfolgt diesfalls erst dann, wenn der Schlüssel ausgetauscht werden soll.

Wurden von einem PCA-Schlüssel mehr als fünf Zertifikate ausgestellt, dann wird das Zweitsystem aktiviert. Der Normalzustand ist dann der in Schritt 2 dargestellte Zustand. Das Hauptsystem und das Zweitsystem werden aber nicht immer parallel geführt, da das Zweitsystem separat aufbewahrt wird. Es wird also z. B. nicht bei jeder Ausstellung eines CERTIFICATION-SERVICES-Zertifikates durch das Hauptsystem auch ein Zertifikat des zugehörigen Zweitsystems ausgestellt. Die Aktualisierung der Zweitsysteme erfolgt immer erst dann gebündelt, wenn von den Hauptsystemen insgesamt etwa fünf bis zehn Zertifikate ausgestellt wurden.

Die Gefahr einer vorzeitigen Kompromittierung des Zweitsystems besteht nicht, da das Zweitsystem erst in Schritt 3 in die Zertifizierungshierarchie der Aufsichtsstelle eingebettet wird. Vor diesem Zeitpunkt ist es für einen Angreifer wertlos.

4.7.3 Zweitsystem für den CERTIFICATE-REVOCATION-Schlüssel

Der CERTIFICATE-REVOCATION-Schlüssel ist in einer sicheren Signaturerstellungseinheit aufbewahrt. Für den Fall, dass der CERTIFICATE-REVOCATION-Schlüssel kompromittiert wird oder sonst ausgetauscht werden soll, wird eine weitere sichere Signaturerstellungseinheit vorrätig gehalten.

Der neue CERTIFICATE-REVOCATION-Schlüssel wird erst dann erzeugt, wenn der Austausch vorgenommen werden soll. Dann wird auch ein TOP-Zertifikat für den neuen CERTIFICATE-REVOCATION-Schlüssel erzeugt und das TOP-Zertifikat für den alten CERTIFICATE-REVOCATION-Schlüssel widerrufen.

Der Wechsel zwischen den Schlüsseln ist für ein Programm, das eine automatisierte Signaturprüfung vornimmt, dadurch erkennbar, dass die Widerrufsliste durch einen anderen Schlüssel signiert wurde. Es kann in diesem Fall automatisch nach dem Nachfolger des widerrufenen Schlüssels suchen. Die Suche erfolgt mit der keyIdentifier-Methode (vgl. 7.1.2 und 7.2.2).

4.8 Kompromittierung von Schlüsseln und Wiederherstellung nach Katastrophenfällen

4.8.1 Beschädigung von Hardware, Software und/oder Daten

Um Ausfälle des Zertifizierungsdienstes zu vermeiden, sind Zweitsysteme vorgesehen (siehe 4.7).

Um Ausfälle des Verzeichnisdienstes zu vermeiden, sind die Rechner des Verzeichnisdienstes als Cluster ausgeführt.

4.8.2 Widerruf eines Schlüssels

Falls ein Widerruf eines Schlüssels der Aufsichtsstelle notwendig ist, weil der Schlüssel außer Betrieb genommen werden muss, wird wie in 4.7 beschrieben auf das Zweitsystem zurückgegriffen.

4.8.3 Kompromittierung eines Schlüssels

Falls ein Widerruf eines Schlüssels der Aufsichtsstelle notwendig ist, weil der Schlüssel kompromittiert wurde, wird wie in 4.7 beschrieben auf das Zweitsystem zurückgegriffen.

4.8.4 Ausweichmöglichkeit für den Fall von Naturkatastrophen

Im Sicherheitskonzept der Aufsichtsstelle ist weder für den Zertifizierungsdienst noch für den Verzeichnisdienst ein Ausweichrechenzentrum vorgesehen.

4.9 Einstellung des Betriebes

Die Einstellung des Betriebes der Dienste der Aufsichtsstelle ist im Signaturgesetz nicht vorgesehen. Eine Einstellung des Betriebes wird nur im Falle einer Gesetzesänderung erfolgen, die Modalitäten der Einstellung – insbesondere die Einstellung oder Übergabe des Zertifizierungsdienstes, die Einstellung oder Übergabe des Verzeichnis- und Widerrufsdienstes, und die Übergabe der Dokumentation, ergeben sich aus der dadurch entstehenden Rechtslage.

Im Rahmen dieses CPS ist jedenfalls vorgesehen, dass alle ausgestellten Zertifikate zu widerrufen sind, wenn der weitere Betrieb des Widerrufsdienstes nicht aufrecht erhalten werden kann. Es wird dann zumindest eine Widerrufsliste veröffentlicht, die alle Zertifikate aufweist, deren Gültigkeitszeitraum noch nicht abgelaufen ist.

Falls die Zuständigkeit von der Telekom-Control-Kommission bzw. der Telekom-Control GmbH auf andere Behörden übergehen sollte, wird das Certification Practice Statement entsprechend der neuen Rechtslage angepasst (siehe Kapitel 8). Dasselbe gilt für eine allfällige Namensänderung der Telekom-Control-Kommission oder der Telekom-Control GmbH.

5. Physikalische, organisatorische und personelle Sicherheitsmaßnahmen

5.1 Physikalische Sicherheitsmaßnahmen

5.1.1 Räumlichkeiten

Der Zertifizierungsdienst ist in einem eigenen Raum der Telekom-Control GmbH eingerichtet, welcher durch eine Zutrittskontrolle und eine Alarmanlage vor unbefugtem Zutritt gesichert ist.

Die für die Erstellung von Zertifikaten notwendige Hardware befindet sich in diesem Raum in einem Tresor und wird nur für die Dauer des Zertifizierungsvorganges aus dem Tresor entnommen. Aus dem Raum wird die Hardware erst dann verbracht, wenn sie nicht mehr verwendet wird. Eine Netzwerkverbindung zum oder vom Zertifizierungsdienst besteht nicht.

Der Verzeichnisdienst und Widerrufsdienst ist in einem Rechenzentrum untergebracht, welches adäquaten Schutz gegen unbefugten Zutritt bietet. Innerhalb des Rechenzentrums sind die Rechner in einem versperrbaren Schrank untergebracht.

5.1.2 Physikalischer Zugriff

Der physikalische Zugriff auf die Rechner des Zertifizierungsdienstes, des Widerrufsdienstes und des Verzeichnisdienstes ist jeweils nur zwei berechtigten Personen gemeinsam möglich.

Hinsichtlich des Zertifizierungsdienstes ist dies dadurch gewährleistet, dass nur zwei Personen gemeinsam den sicheren Raum betreten können und dass nur zwei Personen gemeinsam den Tresor öffnen können.

Auf die im Rechenzentrum untergebrachten Rechner des Verzeichnis- und Widerrufsdienstes haben die Mitarbeiter des Rechenzentrums nur insoferne physikalisch Zugriff, als die Rechner aus- und eingeschaltet werden können.

5.1.3 Stromversorgung und Klimatisierung

Die Alarmanlagen des sicheren Raums der Telekom-Control GmbH sind mit einer USV gesichert. Der Raum ist belüftet. Die Stromversorgung des Rechners, von dem aus das Management des LDAP-Verzeichnisses und die Widerrufe vorgenommen werden, muss gesichert sein. Dieser Rechner wird aber nur im Anlassfall in Betrieb genommen werden.

Die ausfallsichere Stromversorgung und Klimatisierung des Verzeichnisdienstes und des Widerrufsdienstes wird vom Rechenzentrum gewährleistet.

5.1.4 Wassereinbrüche

Der sichere Raum der Telekom-Control GmbH ist mit einem Sensor, der Wassereinbrüche feststellt, ausgestattet.

Der Schutz der Rechner des Verzeichnisdienstes und des Widerrufsdienstes wird vom Rechenzentrum gewährleistet.

5.1.5 Feuerprävention

Der sichere Raum der Telekom-Control GmbH ist an die Brandmeldeanlage des Gebäudes angeschlossen. In den gesamten umliegenden Räumlichkeiten besteht Rauchverbot.

Der Schutz der Rechner des Verzeichnisdienstes und des Widerrufsdienstes wird vom Rechenzentrum gewährleistet.

5.1.6 Aufbewahrung von Daten

Backups werden in einem feuerfesten Tresor aufbewahrt. Die Dokumentation nach § 11 SigG wird zusätzlich am Ort des Zweitsystems aufbewahrt (vgl. 4.6.4).

5.1.7 Abfallentsorgung

Da bei den Zertifizierungsdiensten der Aufsichtsstelle nur geringe Datenmengen anfallen werden, werden Unterlagen im Zweifel nicht entsorgt, sondern möglichst lange aufbewahrt.

Defekte Signaturerstellungseinheiten werden – wenn darin einmal ein privater Schlüssel der Aufsichtsstelle gespeichert war – entsprechend den Anweisungen des Herstellers unbrauchbar gemacht und nach Möglichkeit weiterhin im gesicherten Bereich aufbewahrt. Eine Entsorgung findet nur statt, wenn im Hinblick auf die Konstruktion der Geräte, die Angaben des Herstellers und die dazu vorliegenden Evaluationsberichte sicher gestellt ist, dass der in diesen Signaturerstellungseinheiten einmal gespeicherte Schlüssel aus den Abfällen nicht mehr rekonstruiert werden kann.

Abfälle in Papierform werden geschreddert.

Zur Entsorgung von Datenträgern siehe 6.5.1.

5.1.8 Ausgelagertes Backup

Die Backups werden entsprechend dem Backupkonzept der Telekom-Control GmbH, welches einen nicht veröffentlichten Teil des Sicherheits- und Zertifizierungskonzeptes bildet (siehe 8.2), regelmäßig ausgelagert.

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 Rollen

Die genaue Rollenverteilung und die mit den einzelnen Rollen verbundenen Aufgaben sind in einem internen Dokument beschrieben, welches nicht veröffentlicht wird. Das Rollenmodell umfasst folgende Rollen:

- „Zutrittsverwaltung“ (ZUV)
- „Zutrittskontrolle“ (ZUK)
- „Systemadministrator 1“ (SA1)
- „Systemadministrator 2“ (SA2)
- „Identitätsprüfer“ (IDP)
- „CA-Operator“ (CAO)

- „Widerruf (Call-Center)“ (WIC)
- „Rechenzentrumsmitarbeiter“ (RZM)
- „Rechenzentrumsprüfer“ (RZP)
- „Backup Verzeichnisse“ (BCK)
- „Auditor“ (AUD)

Im Rollenmodell beschrieben sind die Verantwortungsbereiche der Personen, die die einzelnen Rollen wahrnehmen, weiters die Unvereinbarkeiten zwischen verschiedenen Rollen.

5.2.2 Anzahl der Personen, die für eine Aufgabe benötigt werden

Das Rollenmodell der Aufsichtsstelle sieht für alle heiklen Aufgaben das Vier-Augen-Prinzip vor. Insbesondere darf die Verwaltung von Zutrittsrechten, die Systemadministration, das Ausstellen von Zertifikaten und der Widerruf nur von zwei Personen gemeinsam vorgenommen werden.

5.2.3 Zutrittsrechte

5.2.3.1 Eine Person, die die Rolle „Zutrittsverwaltung“ wahrnimmt, hat selbst lediglich ein Zutrittsrecht zum sicheren Raum, in dem sich die technischen Einrichtungen für die Zutrittsverwaltung befinden. Andere Zutrittsrechte kommen der Person nur dann zu, wenn sich dies aus anderen – mit der Rolle „Zutrittsverwaltung“ vereinbaren – Rollen ergibt.

5.2.3.2 Eine Person, die die Rolle „Zutrittskontrolle“ wahrnimmt, hat selbst lediglich ein Zutrittsrecht zum sicheren Raum, in dem sich die technischen Einrichtungen für die Zutrittsverwaltung befinden. Andere Zutrittsrechte kommen der Person nur dann zu, wenn sich dies aus anderen – mit der Rolle „Zutrittskontrolle“ vereinbaren – Rollen ergibt.

5.2.3.3 Ein „Systemadministrator“ hat Zutrittsrechte zu sämtlichen Rechnern der Zertifizierungsdienstes, des Widerrufsdienstes und des Verzeichnisdienstes.

5.2.3.4 Eine Person, die die Rolle „Identitätsprüfer“ wahrnimmt, hat ein Zutrittsrecht zum sicheren Raum, und zu dem darin befindlichen Safe, in dem sich die Rechner des Zertifizierungsdienstes befinden, sowie Zugriffsrechte auf den Widerrufsdienst. Andere Zutrittsrechte kommen der Person nur dann zu, wenn sich die aus anderen – mit der Rolle „Identitätsprüfer“ vereinbaren – Rollen ergibt.

5.2.3.5 Eine Person, die die Rolle „CA-Operator“ wahrnimmt, hat ein Zutrittsrecht zum sicheren Raum, und zu dem darin befindlichen Safe, in dem sich die Rechner des Zertifizierungsdienstes befinden, sowie Zugriffsrechte auf den Widerrufsdienst. Andere Zutrittsrechte kommen der Person nur dann zu, wenn sich die aus anderen – mit der Rolle „CA-Operator“ vereinbaren – Rollen ergibt.

5.2.3.6 Eine Person, die die Rolle „Widerruf (Call-Center)“ wahrnimmt, hat keine Zutrittsrechte, sondern lediglich ein entsprechendes Zugriffsrecht auf das Widerrufssystem.

5.2.3.7 Die „Rechenzentrumsmitarbeiter“ haben keinen physikalischen Zugriff auf die von ihnen überwachten Rechner – mit Ausnahme der Möglichkeit, die Rechner abzuschalten und wieder einzuschalten.

5.2.3.8 Eine Person, die die Rolle „Rechenzentrumsprüfer“ wahrnimmt, hat selbst keine Zutrittsrechte. Andere Zutrittsrechte kommen der Person nur dann zu, wenn sich die aus anderen – mit der Rolle „Rechenzentrumsprüfer“ vereinbaren – Rollen ergibt.

5.2.3.9 Eine Person, die die Rolle „Backup Verzeichnisse“ wahrnimmt, hat ein Zutrittsrecht zum sicheren Raum. Andere Zutrittsrechte kommen der Person nur dann zu, wenn sich dies aus anderen – mit der Rolle „Backup Verzeichnisse“ vereinbaren – Rollen ergibt.

5.2.3.10 Eine Person, die die Rolle „Auditor“ wahrnimmt, hat ein Zutrittsrecht zu allen Safes und Schränken, in denen Dokumentationsdaten aufbewahrt werden.

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 Anforderungen an die Qualifikation und Erfahrung

Alle Personen, die eine Rolle nach dem Rollenmodell (5.2.1) wahrnehmen, müssen für die Wahrnehmung der mit dieser Aufgabe verbundenen Verantwortung ausreichend ausgebildet und geschult sein.

Allgemeine Geheimhaltungsstufen (z. B. vertraulich, geheim, streng geheim) sind im Rahmen der Aufsichtsstelle nicht vorgesehen, weil die Zutrittsrechte individuell je nach Rolle festgelegt sind.

Es ist Aufgabe des Sicherheitsteams, die Abbildung der Rollen auf Personen vorzubereiten und dabei insbesondere die fachliche Eignung und die Unvereinbarkeiten sowie die mit der Rolle verbundene Arbeitsbelastung zu prüfen. Die konkrete Zuweisung von Rollen an die Personen erfolgt durch den Geschäftsführer der Telekom-Control GmbH (oder einen Stellvertreter im Rahmen der Vertretungsregelung).

Im Einzelnen müssen folgende Anforderungen erfüllt sein:

5.3.1.1 Eine Person, der die Rolle „Zutrittsverwaltung“ zugewiesen wird, muss auf die jeweils eingesetzten Zutrittskontrollsysteme und das gesamte Sicherheitskonzept eingeschult worden sein.

5.3.1.2 Eine Person, der die Rolle „Zutrittskontrolle“ zugewiesen wird, muss auf die jeweils eingesetzten Zutrittskontrollsysteme und das gesamte Sicherheitskonzept eingeschult worden sein.

5.3.1.3 Ein „Systemadministrator“ muss Kenntnisse der jeweils eingesetzten Betriebssysteme und Programme haben, die so umfassend sind, dass alle im regulären Betrieb notwendigen Arbeiten selbst vorgenommen werden können und dass komplexere Arbeiten, die von beauftragten Unternehmen durchgeführt werden, wirksam überwacht werden können. Die Person muss das gesamte Sicherheitskonzept kennen. Das Fachwissen ist insbesondere an § 10 Abs. 5 SigV zu messen.

5.3.1.4 Eine Person, der die Rolle „Identitätsprüfer“ zugewiesen wird, muss über die nötigen rechtlichen Kenntnisse im Hinblick auf die Identitätsprüfung verfügen, muss das Zertifizierungskonzept und das Sicherheitskonzept kennen und auf dem System des Zertifizierungsdienstes eingeschult sein.

5.3.1.5 Eine Person, der die Rolle „CA-Operator“ zugewiesen wird, muss über die nötigen rechtlichen Kenntnisse im Hinblick auf die Identitätsprüfung verfügen, muss das Zertifizierungskonzept und das Sicherheitskonzept kennen und auf dem System des Zertifizierungsdienstes eingeschult sein.

5.3.1.6 Eine Person, der die Rolle „Widerruf (Call-Center)“ zugewiesen wird, muss auf das Widerrufssystem und die den Widerrufsvorgang betreffenden Teile des Zertifizierungskonzeptes eingeschult worden sein.

5.3.1.7 Die Auswahl der „Rechenzentrumsmitarbeiter“ erfolgt durch das beauftragte Rechenzentrum, welches die Verantwortung dafür trägt, dass nur Personal eingesetzt wird, das über die nötigen Kenntnisse (insbesondere der eingesetzten Hardware und der eingesetzten Betriebssysteme) verfügt. Das Fachwissen ist insbesondere auch an § 10 Abs. 5 SigV zu messen.

5.3.1.8 Eine Person, der die Rolle „Rechenzentrumsprüfer“ zugewiesen wird, muss über Grundkenntnisse der im Rechenzentrum eingesetzten Hardwarekomponenten, Betriebssysteme und Anwendungsprogramme verfügen und muss das Sicherheitskonzept detailliert kennen.

5.3.1.9 Eine Person, der die Rolle „Backup Verzeichnisse“ zugewiesen wird, muss auf die für das Backup verwendete Software und auf das Sicherheitskonzept eingeschult worden sein.

5.3.1.10 Die Person, die die Rolle „Auditor“ wahrnimmt, muss das Zertifizierungskonzept und das Sicherheitskonzept detailliert kennen. Grundkenntnisse der eingesetzten Hardwarekomponenten, Betriebssysteme und Anwendungsprogramme sind wünschenswert.

5.3.2 Überprüfung der Qualifikation und Erteilung der Zutrittsrechte

Die Eignung der beteiligten Personen wird im Rahmen der Rollenzuweisung überprüft und im täglichen Einsatz erprobt. Die Qualifikation gemäß 5.3.1 muss – soweit möglich oder im Hinblick auf § 10 Abs. 5 SigV erforderlich – durch Zeugnisse bzw. Diplome nachgewiesen werden.

Nach Ermessen der Telekom-Control GmbH kann eine der jeweiligen Rolle entsprechende Schulung auch durch Fortbildungsveranstaltungen erfolgen.

5.3.3 Schulungserfordernisse

Sofern nach dem Rollenmodell (siehe 5.3.1) eine besondere Einschulung auf gewisse Konzepte, Hardware- bzw. Software-Produkte erforderlich ist, wird diese im Rahmen von Fortbildungsveranstaltungen vermittelt.

5.3.4 Auffrischungskurse

Dieses CPS schreibt keine Auffrischungskurse vor.

5.3.5 Häufigkeit und Abfolge des Rollentauschs

Bei Änderungen der Rollenverteilung soll jeweils der Zeitpunkt festgelegt werden, an dem die Änderung in Kraft tritt. Das Sicherheitsteam hat insbesondere auch zu prüfen, ob beim Rollenwechsel in der Übergangsphase Unvereinbarkeiten entstehen können. Diese sind durch einen geordneten Ablauf der Übergangsphase zu verhindern. Nach Möglichkeit soll die Konzeption der Übergangsphase vor der Diskussion im Sicherheitsteam von einer der Personen, die für die „Zutrittsverwaltung“ zuständig sind, vorbereitet werden.

5.3.6 Sanktionen für unzulässige Handlungen

Sollte ein Mitarbeiter der Telekom-Control GmbH die Vorschriften des Sicherheits- und Zertifizierungskonzepts verletzen, so werden vom Sicherheitsteam Maßnahmen zur

Verhinderung zukünftiger Verletzungen erörtert. In schweren Fällen entscheidet der Geschäftsführer der Telekom-Control GmbH über arbeitsrechtliche Maßnahmen oder erstattet allenfalls auch eine Strafanzeige.

Sollte ein Rechenzentrumsmitarbeiter die Vorschriften des Sicherheits- und Zertifizierungskonzepts verletzen, so werden Maßnahmen nach dem zwischen der Telekom-Control GmbH und dem Rechenzentrum geschlossenen Vertrag ergriffen.

Ob Mitarbeiter der Telekom-Control GmbH die Vorschriften des Sicherheits- und Zertifizierungskonzepts verletzt haben, wird im Rahmen der Audits geprüft (siehe 2.7). Ob Mitarbeiter des Rechenzentrums die Vorschriften des Sicherheits- und Zertifizierungskonzepts verletzt haben, wird von dem im Rollenmodell vorgesehenen Rechenzentrumsprüfer festgestellt. Dieser entscheidet selbst darüber, wie häufig Kontrollen notwendig sind und wie detailliert sie vorgenommen werden. Jegliche Auffälligkeiten sind den Systemadministratoren und gegebenenfalls dem Sicherheitsteam zu melden.

5.3.7 Erfordernisse der Dienstverträge

Sämtliche MitarbeiterInnen der Telekom-Control GmbH sind gemäß § 15 DSG 2000 zur Wahrung des Datengeheimnisses verpflichtet.

Jene MitarbeiterInnen, die eine Rolle nach dem Rollenmodell wahrnehmen, müssen entsprechend Punkt 2.1.1.8 zumindest alle zwei Jahre eine Strafregisterauskunft vorlegen.

5.3.8 Für das Personal bereitgestellte Dokumentation

Folgende Dokumente werden Mitarbeitern der Aufsichtsstelle zur Verfügung gestellt, sofern dies zur Erfüllung der Vorschriften des Sicherheits- und Zertifizierungskonzept erforderlich ist:

- Gesetze und Verordnungen
- Technische Normen
- Sicherheits- und Zertifizierungskonzept der Aufsichtsstelle (einschließlich Certification Practice Statement und Certificate Policies)
- Unveröffentlichte Dokumente und Akten der Aufsichtsstelle
- Betriebshandbücher des PKI-Systems

6. Technische Sicherheitsmaßnahmen

6.1 Schlüsselerzeugung und -installation

6.1.1 Schlüsselerzeugung

Sämtliche Schlüsselpaare der Aufsichtsstelle entsprechen dem Verfahren RSA (§ 3 Abs. 1 SigV, Anhang 1 und Anhang 2 Punkt 1 SigV) und weisen eine Schlüssellänge von zumindest 1023 Bit auf. Die Verwendung des Chinese Remainder Theorem ist unzulässig. Die privaten Schlüssel müssen auf einer Länge von mindestens 1023 Bitstellen durch tatsächliche Zufallselemente beeinflusst sein.

Die Schlüsselerzeugung muss in der Signaturerstellungseinheit selbst vorgenommen werden, die privaten Schlüssel dürfen die Signaturerstellungseinheit nicht verlassen (§ 3 Abs. 2 SigV).

6.1.2 Übermittlung des privaten Schlüssels an Zertifikatsempfänger

Die Aufsichtsstelle erzeugt keine Schlüsselpaare für Dritte und übermittelt daher auch keine privaten Schlüssel.

Hinweis: Soweit auf einen Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, die österreichische Signaturverordnung anwendbar ist, müssen seine Signaturerstellungsdaten (der private Schlüssel) in der Signaturerstellungseinheit erzeugt werden und dürfen diese nicht verlassen (§ 3 Abs. 2 SigV). Dies gilt für alle Empfänger von ACCREDITED-CERTIFICATION-SERVICES-Zertifikaten und für alle inländischen Empfänger von QUALIFIED-CERTIFICATION-SERVICES-Zertifikaten.

6.1.3 Übermittlung des öffentlichen Schlüssels an den Zertifikatsaussteller

Die Übermittlung muss in Form eines PKCS#10-Zertifikatsantrages vorgenommen werden (siehe 4.1).

6.1.4 Übermittlung von öffentlichen Schlüsseln an die Benutzer

Die Zertifikate der Aufsichtsstelle werden auf der Website http://www.signatur.tkc.at/ veröffentlicht. Das selbstsignierte Zertifikat des jeweils gültigen TOP-Schlüssels der Aufsichtsstelle wird zudem im Amtsblatt zur Wiener Zeitung veröffentlicht.

Details der Kommunikation des jeweils gültigen TOP-Schlüssels sind in Kapitel 4.7.1.1 erläutert.

6.1.5 Schlüssellängen

Sämtliche Schlüsselpaare der Aufsichtsstelle weisen eine Schlüssellänge von zumindest 1023 Bit auf (Anhang 1 Punkt 2 SigV).

Soweit auf einen Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, die österreichische Signaturverordnung anwendbar ist, müssen die Schlüssellängen bei den Verfahren RSA und DSA mindestens 1023 Bit, bei DSA-Varianten, die auf elliptischen Kurven basieren, mindestens 160 Bit betragen (Anhang 1 Punkt 2 SigV). Dies gilt für alle Empfänger von ACCREDITED-CERTIFICATION-SERVICES-Zertifikaten und für alle inländischen Empfänger von QUALIFIED-CERTIFICATION-SERVICES-Zertifikaten.

6.1.6 Parameter des öffentlichen Schlüssels

Die Signaturverordnung sieht keine Anforderungen an die Parametrisierung öffentlicher Schlüssel vor.

6.1.7 Überprüfung der Qualität der Parameter

Die Schlüssellänge oder allfällige andere Parameter werden jeweils an die Signaturverordnung angepasst.

6.1.8 Schlüsselerzeugung in Hardware oder Software

Die Schlüsselerzeugung für alle Schlüsselpaare der Aufsichtsstelle erfolgt in sicheren Signaturerstellungseinheiten (siehe 2.1.1.1, 2.1.1.4 und 6.2).

6.1.9 Einträge im X.509v3 KeyUsage-Attribut

Im Rahmen dieses CPS werden Zertifikate an Zertifizierungsdienste oder Zertifikate für die Erstellung von Widerrufslisten ausgestellt.

TOP-Zertifikate werden an Zertifizierungsdienste der Aufsichtsstelle und an die CERTIFICATE-REVOCATION-Schlüssel der Aufsichtsstelle ausgestellt. Bei den Zertifikaten, die an Vorgänger und Nachfolger des TOP-Schlüssels, an die PCA-Schlüssel der Aufsichtsstelle und an den TOP-Schlüssel selbst ausgestellt werden, ist im KeyUsage-Attribut ausschließlich das Bit keyCertSign gesetzt. Bei den Schlüsseln, die an die CERTIFICATE-REVOCATION-Schlüssel der Aufsichtsstelle ausgestellt werden, ist im KeyUsage-Attribut ausschließlich das Bit cRLSign gesetzt. Das an C=AT, O=Telekom-Control-Kommission, CN=www.signatur.tkc.at ausgestellte Zertifikat dient dem Zugriff auf den Webserver. Bei diesem Zertifikat sind im KeyUsage-Attribut die Bits digitalSignature und keyEncipherment gesetzt. Das an C=AT, O=Telekom-Control-Kommission, OU=non-X.509-services ausgestellte Zertifikat dient der sicheren elektronischen Signatur einer Liste von Zertifizierungsdiensten. Bei diesem Zertifikat ist im KeyUsage-Attribut das Bit nonRepudiation gesetzt.

ACCREDITED-CERTIFICATION-SERVICES-Zertifikate, QUALIFIED-CERTIFICATION-SERVICES-Zertifikate, CERTIFICATION-SERVICES-Zertifikate und CROSS-CERTIFICATION-Zertifikate werden ausschließlich an Zertifizierungsdienste ausgestellt. Im KeyUsage-Attribut ist ausschließlich das Bit keyCertSign gesetzt.

6.2 Schutz der privaten Schlüssel

6.2.1 Standards für kryptographische Module

Die verwendeten Signaturerstellungseinheiten müssen den Kriterien der Signaturverordnung entsprechen (siehe 2.1.1.1 und 2.1.1.4).

6.2.2 Kontrolle über den privaten Schlüssel durch mehrere Personen

Die Anwendung sämtlicher privater Schlüssel der Aufsichtsstelle ist nur durch jeweils zwei Personen gemeinsam möglich.

6.2.3 Hinterlegung des privaten Schlüssels

Die privaten Schlüssel der Aufsichtsstelle werden in der Signaturerstellungseinheit erzeugt und verlassen diese nie. Sie werden daher auch nirgendwo hinterlegt.

6.2.4 Backup der privaten Schlüssel

Die privaten Schlüssel der Aufsichtsstelle werden in der Signaturerstellungseinheit erzeugt und verlassen diese nie. Es gibt daher kein Backup.

6.2.5 Archivierung der privaten Schlüssel

Die privaten Schlüssel der Aufsichtsstelle werden in der Signaturerstellungseinheit erzeugt und verlassen diese nie. Sie werden daher auch nicht archiviert.

6.2.6 Einbringung privater Schlüssel in kryptographische Module

Die privaten Schlüssel der Aufsichtsstelle werden in der Signaturerstellungseinheit erzeugt, also nicht in sie eingebracht.

6.2.7 Methoden, private Schlüssel zu aktivieren

Die Verwendung privater Schlüssel ist nur nach Eingabe von Aktivierungsdaten möglich, die nur den jeweiligen Berechtigten bekannt sind.

6.2.8 Methoden, private Schlüssel zu deaktivieren

Private Schlüssel werden nach einmaliger Verwendung deaktiviert. Die Aktivierungsdaten müssen also vor jeder einzelnen Anwendung eines privaten Schlüssels neuerlich eingegeben werden.

6.2.9 Methoden, private Schlüssel zu vernichten

Nach Ablauf der Gültigkeit werden private Schlüssel nicht mehr verwendet und in der Signaturerstellungseinheit gelöscht, und bei Kompromittierung privater Schlüssel werden die zugehörigen Zertifikate widerrufen. Eine Vernichtung der Signaturerstellungseinheit ist nur für den Fall vorgesehen, dass eine Aufbewahrung im sicheren Raum der Aufsichtsstelle nicht möglich ist (vgl. 6.5.1).

6.3 Andere Aspekte des Schlüsselmanagements

6.3.1 Archivierung öffentlicher Schlüssel

Zu allen öffentlichen Schlüsseln der Aufsichtsstelle wird zumindest ein Zertifikat ausgestellt. Die Zertifikate werden wie in Punkt 4.5 beschrieben archiviert.

6.3.2 Dauer der Verwendbarkeit von Schlüsseln

Die Dauer der Verwendbarkeit privater Schlüssel ergibt sich aus der Abschätzung, wie lange die verwendeten kryptographischen Algorithmen bei den gewählten Parametern als sicher anzusehen sein werden. RSA mit einer Schlüssellänge von mindestens 1023 Bit wird durch Anhang 1 Punkt 4 SigV bis zum 31.12.2005 als sicher angesehen.

Die von der Aufsichtsstelle eingesetzten Schlüssel sind daher nach gegenwärtiger Einschätzung bis zum 31.12.2005 verwendbar. Es ist möglich, dass die Einschätzung der Sicherheitsperiode in der Zukunft verändert wird, sodass die verwendeten Schlüssel auch nach dem 31.12.2005 eingesetzt werden oder aber dass sie schon zuvor durch längere Schlüssel oder andere Algorithmen ersetzt werden.

Die Gültigkeitsdauer der von der Aufsichtsstelle ausgestellten Zertifikate beträgt maximal drei Jahre und darf den Zeitraum der Eignung der eingesetzten technischen Komponenten und Verfahren sowie der zugehörigen Parameter nach den Anhängen der SigV nicht überschreiten (§ 12 Abs. 3 SigV). Zu Beginn wird die Aufsichtsstelle Zertifikate für die Dauer von einem Jahr ausstellen. Eine zukünftige Verlängerung des Gültigkeitszeitraumes der Zertifikate bleibt vorbehalten.

6.4 Aktivierungsdaten

6.4.1 Erzeugung und Installation von Aktivierungsdaten

Die Erzeugung und Installation von Aktivierungsdaten erfolgt in Abhängigkeit vom verwendeten System.

6.4.2 Schutz der Aktivierungsdaten

Jeder Mitarbeiter der Aufsichtsstelle ist verpflichtet, die ihm zugeteilten Aktivierungsdaten vertraulich zu behandeln und diese nicht aufzuschreiben.

Falls ein Mitarbeiter aus dem Dienst der Aufsichtsstelle ausscheidet, werden die ihm bekannten Aktivierungsdaten zur Vermeidung eines möglichen Missbrauchs ersetzt.

6.4.3 Andere Aspekte betreffend Aktivierungsdaten

Eine Signaturerstellungseinheit wird nach mehrmaligen Versuchen, den privaten Schlüssel mit ungültigen Aktivierungsdaten zu verwenden, automatisch gesperrt.

<Die nähere Festlegung erfolgt nach Auswahl der eingesetzten Systeme.>

6.5 Computersicherheitsmaßnahmen

6.5.1 Spezifische Sicherheitsanforderungen an Computer

Für folgende Geräte gelten spezifische Sicherheitsanforderungen: der bzw. die Rechner mit Software zur Zertifizierung, die Signaturerstellungshardware, ein Rechner, mit dem aus dem sicheren Raum auf das Rechenzentrum zugegriffen werden kann, der Datenbank-Rechner (Widerrufsdienst), zwei Internet-Server (Verzeichnisdienst), zwei Firewalls, ein Router.

Jeder verwendete Rechner enthält ausschließlich die für seinen jeweiligen Verwendungszweck erforderliche Software. Jene Rechner, bei denen auch eine Netzverbindung besteht, werden vor Computerviren geschützt. Durch solche Maßnahmen werden einerseits höchstmögliche Verfügbarkeit und Performance gewährleistet, andererseits werden Sicherheitsrisiken durch Computerviren und trojanische Pferde eliminiert.

Falls Sicherheitsrisiken in der verwendeten Software bekannt werden, ergreifen die Systemadministratoren die vom Hersteller bzw. vom Computer Emergency Response Team empfohlenen Gegenmaßnahmen (insbesondere Aktualisierung der Software).

Datenträger, die private Schlüssel, Aktivierungsdaten oder Protokollierungsdaten enthalten, müssen entweder im sicheren Raum der Aufsichtsstelle aufbewahrt werden oder, sofern sie nicht mehr benötigt werden und eine Aufbewahrung im sicheren Raum der Aufsichtsstelle unmöglich ist, nach DIN 33858 gelöscht und nach DIN 32757 vernichtet werden. Eine Ausnahme bilden Datenträger, die private Schlüssel bzw. Aktivierungsdaten zum Signieren der Widerrufslisten oder Protokollierungsdaten von Internet-Servern bzw. Firewalls, aber keine anderen sensiblen Daten enthalten: Diese dürfen auch im Sicherheitsschrank des beauftragten Rechenzentrums aufbewahrt werden.

Die Aufsichtsstelle ist mit dem Rechenzentrum über eine gesonderte Leitung verbunden. Der Datenverkehr auf dieser Leitung wird durch SSL bzw. TLS geschützt: Er kann nur nach gegenseitiger Authentifizierung der Endgeräte und nur verschlüsselt erfolgen.

Mittels eines USV-Systems können Schwankungen in der Stromversorgung ausgeglichen und Stromausfälle bis zu einer Dauer von 24 Stunden überbrückt werden.

Sollte ein längerer Ausfall (z. B. durch Elementarereignisse oder Sabotage) einen Widerruf von der Aufsichtsstelle aus verhindern, so können Mitarbeiter der Aufsichtsstelle den Widerruf auch außerhalb der Geschäftszeiten unmittelbar im beauftragten Rechenzentrum vornehmen.

6.5.2 Evaluierung der Computersicherheit

Siehe 2.1.1.4.

6.6 Sicherheitsmaßnahmen betreffend Lebenszyklus

6.6.1 Maßnahmen betreffend Systementwicklung

In der Public-Key-Infrastruktur der Aufsichtsstelle werden Software-Komponenten verwendet, die außerhalb der Aufsichtsstelle entwickelt wurden. Für Sicherheitsmaßnahmen bei der Software-Entwicklung ist der Hersteller verantwortlich (z. B. Sicherheit der Entwicklungsumgebung, Sicherheit der Konfiguration während der Wartung, Vorgangsweisen beim Software-Engineering, Methodik der Software-Entwicklung, Modularität, Programmstruktur, Verwendung störungssicherer Entwurfs- und Implementierungstechniken). Der Hersteller hat insbesondere jene Maßnahmen zu ergreifen, die entsprechend § 9 SigV notwendig sind.

6.6.2 Maßnahmen betreffend Sicherheitsmanagement

Mit Hilfe geeigneter Tools wird überprüft, ob die Sicherheit der betriebenen Systeme und Netze jenen Vorgaben entspricht, auf denen die Konfiguration beruht.

6.7 Maßnahmen zur Sicherstellung der Netzsicherheit

Um die Verfügbarkeit des Verzeichnisdienstes und der Widerrufsliste sicherzustellen, werden die Netzkomponenten laufend auf ihre korrekte Funktion überwacht. Von den Internet-Servern werden nur die unbedingt erforderlichen Dienste (LDAP und HTTP, beide auch mit SSL- bzw. TLS-Unterstützung) angeboten. Mit Hilfe der via VPN zentral konfigurierbaren Firewalls wird der Datenverkehr zusätzlichen Regeln unterworfen. Die Firewalls enthalten einen Intrusion-Detection-Mechanismus, der bei ungewöhnlichen Anhäufungen von Zugriffsverletzungen automatisch Alarm auslöst. Darüber hinaus wird die Netz-Performance ständig beobachtet.

6.8 Anforderungen an kryptographische Module

Siehe 2.1.1.4

7. Profil der Zertifikate und Widerrufslisten

7.1 Zertifikatsprofil

7.1.1 Versionsnummer

Alle Zertifikate werden im Format X.509 v3 ausgestellt.

7.1.2 Zertifikatserweiterungen

Die Zertifikate der ersten und zweiten Ebene („TKK top level“ und „TKK PCA level“) enthalten die Erweiterungen BasicConstraints, AuthorityKeyIdentifier, SubjectKeyIdentifier, KeyUsage, CertificatePolicies und CRLDistributionPoints. Die Erweiterungen BasicConstraints und KeyUsage sind als kritisch markiert, die Erweiterungen AuthorityKeyIdentifier, SubjectKeyIdentifier, CertificatePolicies und CRLDistributionPoints hingegen nicht. In BasicConstraints enthält das Feld cA den Wert TRUE. In KeyUsage ist ausschließlich das Bit keyCertSign gesetzt. AuthorityKeyIdentifier und SubjectKeyIdentifier enthalten gemäß den Empfehlungen in RFC 2459, Abschnitte 4.2.1.1 und 4.2.1.2, als keyIdentifier den SHA-1-Wert des Feldes subjectPublicKey im übergeordneten bzw. im gegenständlichen Zertifikat. Die Erweiterung CertificatePolicies enthält den ASN.1 Object Identifier der entsprechenden Certificate Policy sowie einen URI, der auf das vorliegende CPS verweist. Die Erweiterung CRLDistributionPoints enthält lediglich einen URI, der auf die Widerrufsliste verweist. Manche Zertifikate, die an Zertifizierungsdienste ausgestellt werden, enthalten auch die unkritische Erweiterung PolicyConstraints (siehe 7.1.7).

Bei den Zertifikaten der dritten Ebene („TKK services level“) werden die Erweiterungen unterschiedlich gesetzt:

Zertifikate zum Unterzeichnen von Widerrufslisten enthalten die Erweiterungen AuthorityKeyIdentifier, SubjectKeyIdentifier, KeyUsage, CertificatePolicies und CRLDistributionPoints. Die Erweiterung KeyUsage ist als kritisch markiert, die Erweiterungen AuthorityKeyIdentifier, SubjectKeyIdentifier, CertificatePolicies und CRLDistributionPoints sind hingegen nicht kritisch. BasicConstraints existieren in diesen Zertifikaten nicht. AuthorityKeyIdentifier und SubjectKeyIdentifier werden nach demselben Muster wie in den Zertifikaten der ersten und zweiten Ebene verwendet. In KeyUsage ist ausschließlich das Bit cRLSign gesetzt. Die Erweiterung CertificatePolicies enthält den ASN.1 Object Identifier der entsprechenden Certificate Policy sowie einen URI, der auf das vorliegende CPS verweist. Die Erweiterung CRLDistributionPoints enthält lediglich einen URI, der auf die Widerrufsliste verweist.

Zertifikate für HTTP- und LDAP-Server enthalten die Erweiterungen AuthorityKeyIdentifier, KeyUsage, CertificatePolicies und CRLDistributionPoints. Die Erweiterung AuthorityKeyIdentifier wird nach demselben Muster wie in den Zertifikaten der ersten und zweiten Ebene verwendet. Die Erweiterung KeyUsage ist als kritisch markiert, lediglich die Bits digitalSignature und keyEncipherment sind gesetzt. Die Erweiterung CertificatePolicies ist nicht als kritisch markiert und enthält den ASN.1 Object Identifier der entsprechenden Certificate Policy sowie einen URI, der auf das vorliegende CPS verweist. Die Erweiterung CRLDistributionPoints ist nicht als kritisch markiert und enthält lediglich einen URI, der auf die Widerrufsliste verweist.

Zertifikate zum Signieren von NON-X.509-SERVICES-Listen enthalten die Erweiterungen AuthorityKeyIdentifier, KeyUsage, CertificatePolicies und CRLDistributionPoints. Die Erweiterung AuthorityKeyIdentifier wird nach demselben Muster wie in den Zertifikaten der ersten und zweiten Ebene verwendet. Die Erweiterung KeyUsage ist als kritisch markiert, lediglich das Bit nonRepudiation ist gesetzt. Die Erweiterung CertificatePolicies ist nicht als kritisch markiert und enthält den ASN.1 Object Identifier der entsprechenden Certificate Policy sowie einen URI, der auf das vorliegende CPS verweist. Die Erweiterung CRLDistributionPoints ist nicht als kritisch markiert und enthält lediglich einen URI, der auf die Widerrufsliste verweist.

Die Zertifikate für Zertifizierungsdienste entsprechen im wesentlichen den Zertifikaten der ersten und zweiten Ebene, wobei aber die Einschränkung auf bestimmte Hash- und Verschlüsselungsverfahren wegfällt. Dennoch ergeben sich aus den rechtlichen Vorschriften

(insbesondere Anhänge zur SigV) gewisse Vorgaben für Hash- und Verschlüsselungsverfahren. Weiters wird als SubjectAltName jener Distinguished Name angegeben, unter dem das Zertifikat im LDAP-Verzeichnis der Aufsichtsstelle eingeordnet ist (C=AT, O=Telekom-Control-Kommission, OU=...).

Die für den internen Gebrauch bei der Aufsichtsstelle (z. B. für SSL- oder TLS-Verbindungen) ausgestellten Zertifikate werden im vorliegenden CPS nicht erläutert.

<>

Da die hier beschriebenen Zertifikate im Regelfall nicht an natürliche Personen ausgestellt werden und daher das „Qualified Certificates Profile“ (PKIX, ETSI) nicht anwendbar ist, werden die Zertifikate nicht mit dem dort vorgesehenen Policy-Identifier gekennzeichnet. Stattdessen werden die Certificate Policies durch eigene Object Identifier bezeichnet, die im CPS ab Version 1.0 definiert werden.

7.1.3 ASN.1 Object Identifier für Algorithmen

Bei den von der Aufsichtsstelle ausgestellten Zertifikaten enthalten die Felder signatureAlgorithm in Certificate und algorithm in TBSCertificate den ASN.1 Object Identifier sha-1WithRSAEncryption gemäß RFC 2459, Abschnitt 7.2.1.

Das Feld algorithm in SubjectPublicKeyInfo enthält für Schlüssel der Aufsichtsstelle den ASN.1 Object Identifier rsaEncryption gemäß RFC 2459, Abschnitt 7.3.1.

7.1.4 Namensformen

In den von der Aufsichtsstelle ausgestellten Zertifikaten werden Namen entsprechend den Empfehlungen in RFC 2459, Abschnitt 4.1.2.4, angegeben.

7.1.5 Namensvorschriften

In den von der Aufsichtsstelle ausgestellten Zertifikaten enthalten Namen üblicherweise die Attributstypen C, O, OU und CN, eventuell weitere Attributstypen gemäß X.520. Es werden nur die Zeichensätze PrintableString, BMPString und UTF8String verwendet, wobei PrintableString gegenüber BMPString und letzteres gegenüber UTF8String bevorzugt wird. Da Namen keine E-Mail-Adressen enthalten, ist die Verwendung von IA5String nicht erforderlich.

7.1.6 ASN.1 Object Identifier der Certificate Policies

Die ASN.1 Object Identifier der verschiedenen Certificate Policies werden erst in der Version 1.0 dieses CPS festgelegt.

7.1.7 Verwendung der Erweiterung Policy Constraints

Die Erweiterung PolicyConstraints ist lediglich in Zertifikaten vorhanden, die zur Zertifizierung akkreditierter bzw. qualifizierter Dienste vorgesehen sind. Die Erweiterung ist nicht als kritisch markiert und enthält im Feld requireExplicitPolicy den Wert 0.

7.1.8 Syntax und Semantik der Policy-Qualifikatoren

In den von der Aufsichtsstelle ausgestellten Zertifikaten wird lediglich der Qualifikator id-qt-cps verwendet, dessen Syntax und Semantik in RFC 2459, Abschnitt 4.2.1.5, definiert sind.

7.1.9 Verarbeitungssemantik für die kritische Erweiterung Certificate Policy

Da zahlreiche Software-Pakete die Erweiterung Certificate Policy (noch) nicht interpretieren können, wird in den von der Aufsichtsstelle ausgestellten Zertifikaten vorerst darauf verzichtet, diese Erweiterung als kritisch zu markieren.

7.2 CRL-Profil

7.2.1 Versionsnummer

Alle Widerrufslisten werden im Format X.509 v2 ausgestellt. Aufgrund der speziellen Zertifizierungshierarchie der Aufsichtsstelle können die Widerrufslisten nur von Anwendungen interpretiert werden, die gewisse X.509v2-Erweiterungen erkennen.

7.2.2 Erweiterungen der CRL und der CRL-Einträge

Die von der Aufsichtsstelle ausgestellten CRLs enthalten die kritische Erweiterung IssuingDistributionPoint, wobei das Feld indirectCRL den Wert TRUE enthält. Weiters enthalten sie die unkritischen Erweiterungen CRLNumber und AuthorityKeyIdentifier, wobei die Identifikation auf der keyIdentifier-Methode beruht (der keyIdentifier im AuthorityKeyIdentifier der CRL muss mit dem keyIdentifier im SubjectKeyIdentifier des zugehörigen CERTIFICATE-REVOCATION-Zertifikats übereinstimmen).

Die CRL-Einträge können die kritische Erweiterung CertificateIssuer und die unkritische Erweiterung ReasonCode enthalten. Falls die Erweiterung CertificateIssuer in einem CRL-Eintrag nicht vorhanden ist, wird im Sinne von RFC 2459 angenommen, daß das widerrufene Zertifikat vom selben Zertifizierungsdienst ausgestellt worden ist wie das im vorhergehenden CRL-Eintrag widerrufene Zertifikat. Im ersten CRL-Eintrag muß die Erweiterung CertificateIssuer vorhanden sein. Als CertificateIssuer wird ein Name angegeben, der nach den in 3.1.3 genannten Vorschriften mit dem Namen jenes Zertifizierungsdienstes übereinstimmt, der das widerrufene Zertifikat ausgestellt hat.

8. Administration des Sicherheits- und Zertifizierungskonzepts

Es kann notwendig sein, dass das Sicherheits- und Zertifizierungskonzept der Aufsichtsstelle – insbesondere dieses Certification Practice Statement – zu ändern ist. Der Grund für eine solche Änderung kann insbesondere in Änderungen der gesetzlichen Aufgaben der Aufsichtsstelle oder in technischen Erfordernissen wie z. B. dem Bedarf nach Unterstützung einer weiteren Signaturtechnologie liegen.

8.1 Durchführung von Änderungen des Sicherheits- und Zertifizierungskonzepts

In der Telekom-Control GmbH wurde ein Sicherheitsteam eingerichtet, dessen Aufgabe unter anderem auch darin besteht, das Sicherheits- und Zertifizierungskonzept zu erarbeiten, es laufend daraufhin zu überprüfen, ob Änderungen notwendig sind, und diese Änderungen in das Konzept einzuarbeiten. Das Sicherheitsteam nimmt in diesem Zusammenhang die Aufgabe der Telekom-Control GmbH wahr, die Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen bei der Erfüllung ihrer Aufgaben zu unterstützen (§ 15 Abs. 3 SigG). Die Beschlussfassung über das Sicherheits- und Zertifizierungskonzept und dessen Änderungen obliegt der Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen.

An einigen Stellen dieses Certification Practice Statement wird auf mögliche zukünftige Änderungen oder Erweiterungen des Sicherheits- und Zertifizierungskonzepts verwiesen, die absehbar sind. Damit sollen die Benutzer der Zertifizierungsdienste der Aufsichtsstelle schon jetzt auf mögliche zukünftige Änderungen hingewiesen werden. Das Sicherheits- und Zertifizierungskonzepts kann aber auch in anderen Punkten jederzeit geändert werden.

Jedenfalls wird vor einer sicherheitsrelevanten Änderung der von der Aufsichtsstelle betriebenen Zertifizierungsdienste das Sicherheits- und Zertifizierungskonzepts geändert und die Änderung veröffentlicht. Soweit erforderlich wird dabei auch der zeitliche und organisatorische Ablauf der Umstellung beschrieben.

8.1.1 Versionsnummer, URL und OID

Mit jeder Änderung dieses Certification Practice Statement ist eine Änderung der Versionsnummer und des Datums des Dokumentes verbunden (vgl. das Titelblatt und Punkt 1.2).

Geringfügige Änderungen wie etwa die Korrektur von Tippfehlern und offensichtlichen Fehlern, die Beifügung zusätzlicher Erläuterungen (ohne eine damit verbundene inhaltliche Änderung) und dergleichen, können vom Sicherheitsteam ohne Befassung der Telekom-Control-Kommission vorgenommen werden. Bei einer solchen Änderung werden die Ziffern der Versionsnummer nicht geändert, sondern nur um einen – fortlaufend mit a beginnend vergebenen – Kleinbuchstaben ergänzt. Der Dateiname (und damit die URL) sowie der Object Identifier des Dokuments bleiben unverändert.

Jede inhaltliche Änderung, insbesondere jede sicherheitsrelevante Änderung, ist mit einer Änderung der Versionsnummer, des Dateinamens und des Object Identifiers verbunden. Die Beschlussfassung über solche Änderungen obliegt der Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen. Bei Änderungen ist jeweils auch festzulegen, wann diese in Kraft treten. Dabei wird nach Maßgabe der gesetzlichen Bestimmungen auf die Sicherheitsbedürfnisse der Nutzer Rücksicht zu nehmen. Erweiterungen des Sicherheits- und Zertifizierungskonzeptes, die ohne Einfluss auf bestehende Komponenten oder Dienste sind (wie z. B. die Einrichtung einer zusätzlichen Kategorie von Zertifikaten oder eine andere Aufnahme eines zusätzlichen Zertifizierungsdienstes) können im Regelfall umgehend in Kraft gesetzt werden. Bei der Einstellung von Zertifizierungsdiensten werden angemessene Übergangsfristen vorgesehen und die Nutzer möglichst umfassend über die bevorstehenden Änderungen oder die von Ihnen zu ergreifenden Maßnahmen informiert.

8.2 Veröffentlichung des Sicherheits- und Zertifizierungskonzepts

Dieses Certification Practice Statement, die Certification Policies und alle anderen zur Veröffentlichung bestimmten Teile des Sicherheits- und Zertifizierungskonzepts werden von der Telekom-Control GmbH im Auftrag der Aufsichtsstelle für elektronische Signaturen auf deren Website http://www.signatur.tkc.at/ in der Rubrik „Dokumente“ („Repository“) veröffentlicht.

Der Zugang zur Website der Aufsichtsstelle ist nicht beschränkt.

Die Aufsichtsstelle für elektronische Signaturen informiert über relevante Fragen im Zusammenhang mit elektronischen Signaturen, insbesondere auch über wichtige Änderungen ihres Sicherheits- und Zertifizierungskonzepts auch in einem Newsletter, welcher in Form einer Mailinglist verteilt wird. Auf den Verteiler des Newsletters kann sich jeder eintragen lassen, der Zugang ist nicht beschränkt. Über den Newsletter wird nur über besonders wichtige Ereignisse informiert, dazu gehört nicht unbedingt jede Änderung des Certification Practice Statement. Die Aufsichtsstelle übernimmt keine Haftung dafür, dass

über eine einem Nutzer wichtig erscheinende Änderung mit einem Newsletter informiert wird, weiters garantiert die Aufsichtsstelle auch nicht, dass ein Newsletter allen Personen, die sich auf den Verteiler setzen haben lassen, zugestellt wird.

Neben dem Certification Practice Statement umfasst das Sicherheits- und Zertifizierungskonzept der Aufsichtsstelle insbesondere auch die folgenden Dokumente, welche nicht veröffentlicht werden:

- Ein Sicherheitskonzept für den Schutz der Einrichtungen der Aufsichtsstelle vor unbefugtem Zutritt.

- Ein Rollenmodell. In diesem werden die im Rahmen der Erbringung der Zertifizierungsdienste vorzunehmenden Aufgaben einzelnen Rollen zugeordnet, es werden Unvereinbarkeiten zwischen den Rollen analysiert und für die meisten Aufgaben ein Vier-Augen-Prinzip sichergestellt, weiters wird die Zuständigkeit für die Besetzung der einzelnen Rollen mit Personen definiert.

- Dokumentation der eingesetzten Hardware und Software. Dabei werden insbesondere auch alle Zugriffsberechtigungen festgelegt, weiters wird auf technischer Ebene festgelegt, welche Ereignisse protokolliert werden und welche Prozesse des Verzeichnis- und Widerrufsdienstes laufend zu überwachen sind.

- Das Backupkonzept der Telekom-Control GmbH.

9 Glossar

Akkreditierung	→ § 17 SigG
Anbieter	In diesem Dokument als Kurzform für → Zertifizierungsdiensteanbieter verwendet.
Aufsichtsstelle	Eine gemäß Art. 3 Abs. 3 der → Signaturrichtlinie eingerichtete Behörde, die die Aufsicht über Zertifizierungsdiensteanbieter wahrnimmt. In Österreich ist gemäß § 13 → SigG die Telekom-Control-Kommission Aufsichtsstelle für elektronische Signaturen.
Bestätigungsstelle	Eine gemäß Art. 3 Abs. 4 der → Signaturrichtlinie eingerichtete Stelle, die die Übereinstimmung → sicherer Signaturerstellungseinheiten mit Anhang III der Richtlinie feststellt. In Österreich werden Bestätigungsstellen gemäß § 19 → SigG durch Verordnung als solche anerkannt.
CA	→ Certification Authority, Zertifizierungsstelle
Certification Authority (CA)	Dieser Begriff wird meist verwendet, um jene technische Einrichtung zu beschreiben, mittels der Zertifikate ausgestellt und verwaltet werden. Ein → Zertifizierungsdiensteanbieter betreibt eine oder mehrere Certification Authorities (Zertifizierungsstellen).

Certificate Policy (CP)	Ein Teil des → Sicherheits- und Zertifizierungskonzeptes, in welchem die Regeln für die Ausstellung einer bestimmten Klasse von → Zertifikaten veröffentlicht werden (siehe → RFC 2527, Punkt 3.1)
Certification Practice Statement (CPS)	Ein Teil des → Sicherheits- und Zertifizierungskonzeptes, in welchem ein → Zertifizierungsdiensteanbieter darlegt, wie er bei der Ausstellung von → Zertifikaten vorgeht (siehe → RFC 2527, Punkt 3.5)
CP	→ Certificate Policy
CPS	→ Certification Practice Statement
CRL	Certificate Revocation List, → Widerrufsliste
Cross-Zertifizierung	Die Ausstellung von Zertifikaten durch Zertifizierungsdiensteanbieter für andere Zertifizierungsdiensteanbieter
Dienst	In diesem Dokument als Kurzform für → Zertifizierungsdienst verwendet
IETF	Internet Engineering Task Force, http://ietf.org/
KeyUsage	Ein Attribut von → X.509v3-Zertifikaten, mit welchem ausgedrückt wird, für welchen Verwendungszweck das Zertifikat gewidmet ist, → vgl. RFC 2459, Punkt 4.2.1.3
Object Identifier (OID)	Objektkennung. Ein eindeutiger Name für ein Informationsobjekt, der aus einer Folge von ganzen, nicht negativen Zahlen besteht. Beispielsweise ist dieses Dokument durch einen Object Identifier eindeutig gekennzeichnet (siehe Punkt 1.2)
OID	→ Object Identifier
öffentlicher Schlüssel	Jener Teil des Schlüsselpaares eines asymmetrischen kryptographischen Verfahrens, welcher (z. B. in einem → Zertifikat) veröffentlicht und zur Signaturprüfung verwendet wird. Vgl. auch → Signaturprüfdaten
PCA	→ Policy Certification Authority
PCA-Schlüssel	→ Kapitel 1.3.0.2
PKI	Public-Key-Infrastruktur

PKIX	Eine Arbeitsgruppe innerhalb der → IETF, die an Standards im Bereich „Public-Key Infrastructure (X.509)“ arbeitet → http://ietf.org/ids.by.wg/pkix.html
Policy Certification Authority (PCA)	Eine → Certification Authority, die nicht dazu dient, Zertifikate an Endkunden auszustellen, sondern Zertifikate an andere → Certification Authorities ausstellt. Durch den Einsatz verschiedener PCAs können z. B. verschiedene Zertifikatsklassen unterschieden werden. Die Aufsichtsstelle wird mehrere PCAs betreiben, die in Kapitel 1.3 beschrieben sind.
privater Schlüssel	Jener Teil des Schlüsselpaares eines asymmetrischen kryptographischen Verfahrens, welcher geheimgehalten und z. B. zur Erstellung von Signaturen verwendet wird. Vgl. auch → Signaturerstellungsdaten
Public-Key-Infrastruktur (PKI)	Das technische Umfeld, in welchem mittels asymmetrischer Kryptographie gesicherte Kommunikation möglich ist. Der Begriff umfasst → Zertifizierungsstellen und → Registrierungsstellen bzw. → Zertifizierungsdiensteanbieter, die Inhaber von → Zertifikaten sowie die eingesetzte Hardware und Software. Innerhalb der PKI ist z. B. der Austausch digital signierter Nachrichten möglich.
qualifiziertes Zertifikat	ein → Zertifikat, das die Angaben des § 5 → SigG enthält und von einem den Anforderungen des § 7 → SigG entsprechenden Zertifizierungsdiensteanbieter ausgestellt wird
Registrierungsstelle	Jene Einrichtung, welche die Identität des → Zertifikatswerbers überprüft. Ein → Zertifizierungsdiensteanbieter betreibt in der Regel eine oder mehrere Registrierungsstellen oder beauftragt andere Unternehmen, die unter seiner Verantwortung als Registrierungsstellen tätig sind.
RFC	Request for Comments, Standardisierungsdokumente des → IETF, http://ietf.org/rfc.html
RFC 2459	Housley et. al., Internet X.509 Public Key Infrastructure Certificate and CRL Profile, 1999
RFC 2527	Chokhani/Ford, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, 1999
Root	→ Wurzel

RSA	Ein asymmetrisches kryptographisches Verfahren, mit welchem – in Kombination mit einem Hashverfahren – elektronische Signaturen erstellt werden können. Die Aufsichtsstelle verwendet für die von ihr ausgestellten Zertifikate ausschließlich RSA.
Schlüssel	In diesem Dokument wird der Begriff „Schlüssel“ in der Regel als Kurzform für „Schlüsselpaar“, „öffentlicher Schlüssel“ oder „privater Schlüssel“ verwendet. Der Begriff bezeichnet immer Schlüssel eines asymmetrischen kryptographischen Verfahrens (in der Regel → RSA).
Schlüsselpaar	In einer → Public-Key-Infrastruktur hat jeder Teilnehmer ein Schlüsselpaar, bestehend aus einem → öffentlichen Schlüssel und einem → privaten Schlüssel. Der private Schlüssel wird geheimgehalten und z. B. für die Erstellung von Signaturen verwendet. Der öffentliche Schlüssel dient der Signaturprüfung.
Schlüssel, öffentlicher	Jener Teil des Schlüsselpaares eines asymmetrischen kryptographischen Verfahrens, welcher (z. B. in einem → Zertifikat) veröffentlicht und zur Signaturprüfung verwendet wird. Vgl. auch → Signaturprüfdaten
Schlüssel, privater	Jener Teil des Schlüsselpaares eines asymmetrischen kryptographischen Verfahrens, welcher geheimgehalten und z. B. zur Erstellung von Signaturen verwendet wird. Vgl. auch → Signaturerstellungsdaten
Sicherheits- und Zertifizierungskonzept	Eine Sammlung von Dokumenten, nach denen ein Zertifizierungsdiensteanbieter bei der Ausstellung von Zertifikaten vorgeht. Das Sicherheits- und Zertifizierungskonzept umfasst Teile, die vom Anbieter veröffentlicht werden und Teile, die er nur intern verwendet oder der Aufsichtsstelle zugänglich macht. Vgl. § 15 → SigV
SigG	Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG), BGBl I 1999/190
Signaturerstellungsdaten	Einmalige Daten wie Codes oder private Signaturschlüssel, die vom Signator zur Erstellung einer elektronischen Signatur verwendet werden (§ 2 Z 4→ SigV). In diesem Dokument wird stattdessen meist der Begriff → privater Schlüssel verwendet.
Signaturprüfdaten	Daten wie Codes oder private Signaturschlüssel, die vom zur Überprüfung einer elektronischen Signatur verwendet werden (§ 2 Z 6 → SigV). In diesem

	Dokument wird stattdessen meist der Begriff → öffentlicher Schlüssel verwendet.
Signaturrichtlinie	Richtlinie 1999/93/EG des Europäischen Parlamentes und des Rates vom 13.12.1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. L 13 vom 19.01.2000, S. 12
SigV	Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung – SigV), BGBl II 2000/30
TOP-Schlüssel	→ Kapitel 1.3.0.1
TOP-Zertifikat	→ Kapitel 1.3.0.1
URL	Uniform Ressource Locator. Die Adresse einer Ressource im Internet, z. B. http://...
Widerrufsliste	(Certificate Revocation List, CRL) Eine Liste, auf der die Seriennummern gesperrter oder widerrufener Zertifikate veröffentlicht werden, siehe auch → X.509 und → RFC 2459
Wurzel	Das oberste Element einer Zertifizierungshierarchie, welches üblicherweise durch einen Wurzelschlüssel repräsentiert wird, für den ein selbstsigniertes Wurzelzertifikat ausgestellt wurde. In diesem Dokument wird stattdessen die Bezeichnung TOP-Schlüssel verwendet (→ 1.3.0.1)
X.509	Ein Standard für die Codierung von Zertifikaten und Widerrufslisten. Derzeit ist die Version 3 (X.509v3) für Zertifikate und die Version 2 (X.509v2) für Widerrufslisten gebräuchlich. → RFC 2459
Zertifikat	eine elektronische Bescheinigung, mit der → Signaturprüfdaten einer bestimmten Person zugeordnet werden und deren Identität bestätigt wird (→ § 2 Z 8 SigG)
Zertifikat, qualifiziertes	ein → Zertifikat, das die Angaben des § 5 → SigG enthält und von einem den Anforderungen des § 7 → SigG entsprechenden Zertifizierungsdiensteanbieter ausgestellt wird
Zertifikatsempfänger	Eine Person, der ein Zertifikat ausgestellt wurde. In diesem Dokument tritt als Zertifikatsempfänger in der Regel ein → Zertifizierungsdiensteanbieter auf, welchem die Aufsichtsstelle für seine → Zertifizierungsdienste Zertifikate ausgestellt hat. Vgl. auch die Definition des Begriffs „Signator“ in § 2 Z 2 → SigG.

Zertifikatswerber	Eine Person, die den Antrag auf Ausstellung eines → Zertifikates stellt. In diesem Dokument tritt als Zertifikatswerber in der Regel ein → Zertifizierungsdiensteanbieter auf, welchem die Aufsichtsstelle für seine → Zertifizierungsdienste Zertifikate ausstellt.
Zertifizierungsdienst	In diesem Dokument wird unter einem Zertifizierungsdienst vor allem die Ausstellung, Erneuerung, Verwaltung und der Widerruf von Zertifikaten verstanden (vgl. auch die Definition in § 2 Z 11 → SigG). Ein → Zertifizierungsdiensteanbieter kann mehrere Zertifizierungsdienste unterschiedlicher Qualität betreiben
Zertifizierungsdienst, akkreditierter	Ein Zertifizierungsdienst, mit welchem ein → Zertifizierungsdiensteanbieter die Voraussetzungen für eine Akkreditierung nach § 17 → SigG erfüllt hat
Zertifizierungsdienst, qualifizierter	Ein Zertifizierungsdienst, bei welchem ausschließlich qualifizierte → Zertifikate ausgestellt werden
Zertifizierungsdiensteanbieter	Eine natürliche oder juristische Person oder eine sonstige rechtsfähige Einrichtung, die Zertifikate ausstellt oder andere Signatur- und Zertifizierungsdienste erbringt (§ 2 Z 10 → SigG). Auch die Aufsichtsstelle tritt als Zertifizierungsdiensteanbieter auf. Dieses Dokument beschreibt die Tätigkeit der Aufsichtsstelle als Zertifizierungsdiensteanbieter.
Zertifizierungshierarchie	Zertifikate können auch an Zertifizierungsstellen ausgestellt werden, die ihrerseits weitere Zertifikate ausstellen. Auf diese Weise kann eine Hierarchie gebildet werden, wie sie beispielsweise in → Kapitel 1.3 beschrieben ist.
Zertifizierungsstelle	auch: Certification Authority (CA). Dieser Begriff wird meist verwendet, um jene technische Einrichtung zu beschreiben, mittels der Zertifikate ausgestellt und verwaltet werden. Ein → Zertifizierungsdiensteanbieter betreibt eine oder mehrere Certification Authorities (Zertifizierungsstellen).