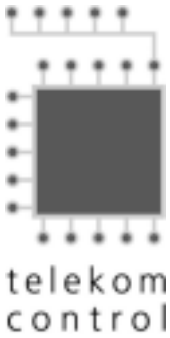


Telekom-Control GmbH

Ausschreibungsunterlagen für die Public-Key-Infrastruktur der Aufsichtsstelle

FAUS 19/2000

Version 1.0

29.11.2000

Aufsichtsstelle für elektronische Signaturen
Telekom-Control-Kommission und Telekom-Control GmbH
Mariahilfer Straße 77–79, 1060 Wien, Tel. +43/(0)1/58058-0, Fax: +43/(0)1/58058-9191
http://www.signatur.tkc.at/, signatur@tkc.at

1. Ausgangssituation

Die Telekom-Control GmbH ist eine nicht gewinnorientierte Gesellschaft, deren Geschäftsanteile zu 100 % dem Bund vorbehalten sind. Der Telekom-Control GmbH kommt nach dem Telekommunikationsgesetz 1997 in Zusammenarbeit mit der Telekom-Control Kommission die Rolle der Regulierungsbehörde für die österreichischen Telekommunikationsmärkte zu. Durch das Signaturgesetz (BGBl I 1999/190) wurde die Telekom-Control GmbH weiters damit beauftragt, die Telekom-Control-Kommission in deren Aufgabe als Aufsichtsstelle für elektronische Signaturen zu unterstützen.

Die Telekom-Control GmbH hat dabei insbesondere die Zertifizierungsdiensteanbieter nach der Anzeige der Aufgabe ihrer Tätigkeit zu registrieren und Verzeichnisse der Zertifikate für Zertifizierungsdiensteanbieter sowie ein Verzeichnis der akkreditierten Zertifizierungsdiensteanbieter zu führen (§ 15 Abs. 2 Z 2 und 3 SigG).

Die Telekom-Control GmbH wird zu diesem Zweck den einzelnen Zertifizierungsdiensten X.509v3-Zertifikate ausstellen, welche in einem Verzeichnis über LDAP und über HTTP abrufbar sind. Weiters wird ein Widerrufsdienst in Form von X.509v2-CRLs geführt, welche ebenfalls mittels LDAP und HTTP abrufbar sein werden.

Das Signaturgesetz (BGBl I 1999/190) und die Signaturverordnung (BGBl II 2000/30) enthalten detaillierte Anforderungen betreffend die von der Telekom-Control GmbH erbrachten Zertifizierungsdienste.

Die IT-Infrastruktur der Telekom-Control GmbH für die Aufgaben nach dem Signaturgesetz ist von der IT-Infrastruktur für die Aufgaben nach dem Telekommunikationsgesetz einerseits aus Sicherheitsgründen, andererseits wegen des gesetzlichen Gebotes der organisatorischen und finanziellen Trennung der Aufgabenbereiche (§ 13 Abs. 3 und § 15 Abs. 5 SigG) getrennt.

Derzeit ist die Eingliederung der Telekom-Control GmbH in eine neu zu schaffende Regulierungsbehörde (KommAustria GmbH) in Diskussion. Diese Ausschreibung gilt für die Telekom-Control GmbH und alle ihre allfälligen Nachfolgegesellschaften im Wege der Einzel- oder Gesamtrechtsnachfolge.

2. Vergabeverfahren

2.1 Gesetzliche Grundlagen und Vergabeart

Das Vergabeverfahren und die Angebote der Bieter unterliegen den Bestimmungen des Bundesvergabegesetzes, BGBl I 1997/56 idgF.

Das Verfahren erfolgt in Form eines offenen Verfahrens (§ 18 Abs. 2 BVergG)).

2.2 Erklärung der Bieter

Mit der Abgabe des Angebotes hat jeder Bieter zu erklären (siehe Anlage 2),

– dass er die Ausschreibung und die in ihr enthaltenen bzw. ihr zugrundeliegenden Auflagen, Bedingungen, Richtlinien und Rechtsvorschriften akzeptiert;

– dass er keine Vereinbarung über die Preisbildung und andere für die Telekom-Control GmbH nachteilige, gegen Rechtsvorschriften, die guten Sitten oder gegen den Grundsatz des Wettbewerbs verstoßende Abreden mit anderen Unternehmen getroffen hat und sich

bewusst ist, dass eine falsche Abgabe dieser Erklärung seinen Ausschluss vom Vergabeverfahren zur Folge hat;

– dass er zur Durchführung der angebotenen Lieferungen und Leistungen nach den gesetzlichen Bestimmungen seines Herkunftslandes und Österreichs berechtigt ist und bei der Durchführung die einschlägigen gesetzlichen Bestimmungen beachten wird;

– dass er über die entsprechende wirtschaftliche, finanzielle und technische Leistungsfähigkeit verfügt, um die geforderten Lieferungen und Leistungen vertragsgemäß zu erbringen;

– dass er bei der Durchführung des Leistungsvertrages auf die Beschäftigung von Personen im Ausbildungsverhältnis bedacht nimmt;

– dass er die Ausschreibungsunterlagen, insbesondere hinsichtlich der technischen Beschreibungen, prüfen wird und allfällige Berichtigungen der Telekom-Control GmbH mitteilen wird;

– dass die Angebote unter dem Gesichtspunkt der vollen Funktionsfähigkeit der angebotenen Lieferungen und Leistungen erstellt wurden.

Zur Feststellung der wirtschaftlichen, finanziellen und technischen Leistungsfähigkeit sind die Fragen in Anlage 2 zu beantworten.

Es wird darauf hingewiesen, dass im Angebot keinerlei Teile, Komponenten oder sonstige Leistungen (z. B. Dokumentation, Schulung, etc.) fehlen dürfen, soweit diese für die Inbetriebnahme des Systems erforderlich sind, auch wenn diese Teile, Komponenten oder sonstige Leistungen in der Ausschreibung nicht ausdrücklich erwähnt wurden. Fehlende Teile oder Leistungen gelten als angeboten und sind ohne Mehrkosten zu liefern bzw. zu erbringen.

2.3 Vertraulichkeit

Der Auftragnehmer verpflichtet sich während der und auch nach der Durchführung oder Beendigung des Leistungsvertrages zur Geheimhaltung der ihm beim Abschluss des Leistungsvertrages bekannten und aller ihm während der Zusammenarbeit mit der Telekom-Control GmbH zur Kenntnis gekommenen Geschäfts- und Betriebsgeheimnisse sowie der sonstigen betrieblichen Angelegenheiten, Daten, Materialien, Berichte etc. der Telekom-Control GmbH, insbesondere auch der von der Telekom-Control GmbH verwalteten personenbezogenen Daten, soweit diese Information nicht bereits öffentlich bekannt ist.

Diese Verpflichtung des Auftragnehmers gilt zeitlich unbeschränkt und auch gegenüber mit dem Auftragnehmer verbundenen Unternehmen, nicht jedoch gegenüber für die Auftragsdurchführung herangezogenen Subunternehmen, soweit die Subunternehmer Informationen zur Leistungserbringung benötigen. Der Auftragnehmer wird für die Projektdurchführung nur solche Subunternehmer und Mitarbeiter einsetzen, die sich gemäß § 15 Datenschutzgesetz 2000 verpflichtet haben, das Datengeheimnis hinsichtlich aller ihnen im Rahmen der zu erbringenden Lieferungen und Leistungen bekannt gewordenen Daten zu wahren. Der Auftragnehmer wird diese Verpflichtung einschließlich der Überbindungsverpflichtung auf alle Angestellten und alle Dritten überbinden, die von ihm zur Erbringung von Lieferungen oder Leistungen für die Telekom-Control GmbH herangezogen werden.

Die Telekom-Control GmbH wird den vertraulichen Charakter aller die Bieter und deren Angebote betreffenden Angaben wahren.

2.4 Zustelladressen

2.4.1 Angebote

Die Angebote sind zu adressieren an: (siehe auch 2.13.1)

Telekom-Control GmbH
Mariahilfer Straße 77-79
A-1060 Wien
z. Hd. Hrn. Dieter Kronegger
E-Mail: signatur@tkc.at

2.4.2 Berichtigungen, Fragen und Mitteilungen

Allfällige Berichtigungen, Fragen und sonstige Mitteilungen der Bewerber und Bieter sind zu adressieren an:

Telekom-Control GmbH
Mariahilfer Straße 77-79
A-1060 Wien
z. Hd. Hrn. Dieter Kronegger
Tel.: +43/(0)1/58058-407
Fax.: +43/(0)1/58058-9191
E-Mail: signatur@tkc.at

2.4.3 Bewerber, Bieter und Auftragnehmer

Interessenten können die Ausschreibungsunterlagen bei der Telekom-Control GmbH persönlich, brieflich, per Fax oder per E-Mail unter Angabe des Vermerks "Ausschreibung Publik-Key-Infrastruktur GZ FAUS 19/2000" anfordern. Voraussetzung für die Ausfolgung (Mo-Fr 10-12 Uhr, ausgenommen gesetzliche Feiertage) ist die Zahlung eines Kostenersatzes in Höhe von ATS 5.000,– (Euro 363,36) für das Zurverfügungstellen der Ausschreibungsunterlagen in bar oder mittels eines Bankschecks. Bei einer brieflichen Übersendung der Ausschreibungsunterlagen ist dieser Kostenersatz auf das Konto der Telekom-Control GmbH bei der Bank Austria AG, Bankleitzahl 20151, Konto Nr. 696 170 133 zu überweisen. Voraussetzung für die Ausfolgung bzw. briefliche Übersendung ist weiters, dass der Interessent Name, Anschrift, sowie Fax- und Telefonnummer sowie E-Mail-Adresse angibt. Die Ausschreibungsunterlagen werden den Interessenten sowohl in Papierform als auch auf Datenträger in den Formaten PDF und Microsoft Word 97 bereitgestellt.

Für die interessierte Öffentlichkeit werden die Ausschreibungsunterlagen zum Download im Format PDF zur Verfügung gestellt. Dies dient ausschließlich der Information. Die für die Telekom-Control GmbH rechtsverbindlichen Ausschreibungsunterlagen sind ausschließlich jene, die gegen Erlag des Kostenersatzes bei der Telekom-Control GmbH zu erwerben sind. Der Erwerb der Ausschreibungsunterlagen ist aber keine Bedingung für die Beteiligung im Vergabeverfahren.

Jeder Bewerber hat bei Übernahme der Ausschreibungsunterlagen eine Zustelladresse bekannt zu geben, die auch eine Telefaxnummer und eine E-Mail-Adresse umfassen soll. Bei Anforderung der Bewerbungsunterlagen per Post oder E-Mail wird, mangels Bekanntgabe einer anderen Zustelladresse, davon ausgegangen, dass diejenige Adresse, an die die Ausschreibungsunterlagen übermittelt werden, als Zustelladresse im Sinne dieses Absatzes gilt. Mit Bekanntgabe dieser Zustelladresse und der Anforderung per Post erklärt der Bewerber, dass Zustellungen und Mitteilungen an diese Adresse als Zustellungen und Mitteilungen im Sinne dieser Ausschreibung gelten.

Die Zustelladresse des Bewerbers gilt nach Einbringung eines Angebots auch als Zustelladresse des Bieters. Änderungen der Zustelladresse sind der Telekom-Control GmbH unverzüglich bekannt zu geben.

Die von dem Bieter, der aufgrund Zuschlagserteilung Auftragnehmer wird, bekannt gegebene Zustelladresse gilt als Zustelladresse für jegliche Erklärung gemäß dem Leistungsvertrag, solange der Auftragnehmer nicht eine andere Zustelladresse mittels eingeschriebenen Briefes bekannt gegeben hat. An diese Zustelladresse erfolgen schriftlich oder per Fax Mitteilungen an den Auftragnehmer.

2.5 Angebotslegung

2.5.1 Umfang

Der Bieter hat für ein Angebot zumindest Folgendes vorzulegen:

– ausgefülltes Deckblatt Anlage 1

– ausgefüllter Fragenkatalog Anlage 2 (Angaben zum Bieter) mit entsprechenden Beilagen, firmenmäßig gezeichnet

– ausgefüllter Fragenkatalog Anlage 3 (Technische Fragen) mit entsprechenden Beilagen, firmenmäßig gezeichnet

– ausgefüllter Preisraster Anlage 4, firmenmäßig gezeichnet

– firmenmäßige Zeichnung der Vertragsbestimmungen Anlage 5

– die unter 2.5.3 angeführten Nachweise

– bei Bietergemeinschaften Erklärungen gemäß 2.9

– Unterlagen zur Evaluation der technischen Komponenten gemäß 3.7

2.5.2 Sonstige Richtlinien

a) Soweit in diesen Ausschreibungsunterlagen nicht etwas anderes angegeben ist, hat das Angebot den Bestimmungen des Bundesvergabegesetzes idgF zu entsprechen.

b) Das Angebot ist in den Ausschreibungsunterlagen in kopierfähiger, farbbeständiger Block- oder Maschinenschrift ohne Korrekturen der Ausschreibung auf Papier zu erstellen und hat zumindest die Vordrucke und die geforderten Erläuterungen und Angaben zu enthalten. Das Angebot kann auch in elektronischer Form abgegeben werden, wenn es mit der sicheren elektronischen Signatur des Bieters versehen ist. Falls in den Vordrucken der zur Verfügung stehende Platz nicht ausreicht, sind Ergänzungsblätter zu verwenden und mit einem Hinweis auf den entsprechenden Punkt der Ausschreibung zu versehen. Um die Angebotserstellung zu erleichtern, werden die Ausschreibungsunterlagen auch in elektronischer Form bereitgestellt (siehe 2.4.3). Den Ausschreibungsbedingungen widersprechende sowie fehlerhafte oder unvollständige Angebote werden, wenn die Mängel nicht behoben wurden und nicht behebbar sind, ausgeschieden. Weist ein Angebot solche Mängel auf, dass der Telekom-Control GmbH eine Bearbeitung nicht zugemutet werden kann, wird es nicht weiter behandelt.

c) Die Angebote und sämtliche Beilagen, Fragebögen, Bestätigungen und Erklärungen sind in deutscher Sprache zu erstellen. Produktbeschreibungen, Handbücher,

Evaluierungsberichte und dergleichen können auch in englischer Sprache vorgelegt werden. Bei Unterlagen in anderen Sprachen ist eine beglaubigte Übersetzung beizulegen.

d) Der Bieter hat etwaige Betriebs- und Bedienungsvorschriften sowie Programmdokumentationen, Installations- und Ablaufbeschreibung etc. in deutscher oder englischer Sprache mit dem Angebot zu übergeben. Die nach Zuschlagserteilung zu erstellenden Sicherheitskonzepte, Dokumentationen, Betriebs- und Bedienungsvorschriften sind in deutscher Sprache zu erstellen.

e) Änderungen oder Ergänzungen der Ausschreibungsbedingungen – mit Ausnahme von Alternativangeboten – sind unzulässig. Angebote, die nicht den Ausschreibungsbedingungen gemäß gestaltet sind, werden vom Verfahren ausgeschieden. Ausgenommen davon sind lediglich behebbare Mängel, wenn sie behoben werden, oder unwesentliche Mängel.

f) Die Bieter sind verpflichtet, auf ihnen auffallende Fehler in der Ausschreibung hinzuweisen, anderenfalls sie sich auf derartige Fehler nicht berufen können.

g) Die Telekom-Control GmbH behält sich vor, allfällige Fehler in der Ausschreibung zu berichtigen.

h) Auf Anforderungen, die vom Bieter nicht erfüllt werden können, ist jedenfalls besonders hinzuweisen. Produkte oder Modelle, von denen zu erwarten ist oder bekannt ist, dass deren Produktion innerhalb der der Angebotslegung folgenden 12 Monate eingestellt wird, sind im Angebot als „Auslaufmodell“ zu bezeichnen.

i) Bei angebotenen Produkten sind die Firmenbezeichnung und, soweit vorhanden, die Artikelnummer anzuführen. Weiters sind Produktbeschreibungen und detaillierte Unterlagen, soweit vorhanden, beizulegen. Aus diesen Unterlagen muss die genaue technische Funktionsweise des angebotenen Systems ersichtlich sein. Die Unterlagen müssen eine hinreichende Beurteilung ermöglichen.

j) Falls in dieser Ausschreibung aus Gründen der Verständlichkeit in technischen Spezifikationen Produktbezeichnungen, geschützte Marken oder Bezeichnungen von Industriestandards verwendet werden, sind auch Lieferungen gleichwertiger Systeme und Leistungen gleichwertiger Art, die zu den genannten Produkten voll kompatibel sind, ausschreibungskonform. In jedem Fall sind die genauen Produktbezeichnungen inklusive allfälliger Versionsnummern anzugeben.

2.5.3 Nachweise

Der Bieter hat dem Angebot folgende Nachweise beizulegen. Die entsprechenden Nachweise sind auch für die Subunternehmen, die einen wesentlichen Teil der ausgeschriebenen Leistung erbringen sollten, vorzulegen:

– Einen Nachweis der Gewerbeberechtigung oder Befugnisverleihung;

– einen Auszug aus dem Firmenbuch;

– eine Erklärung des Unternehmers, in welcher er ausdrücklich seine Zuverlässigkeit, das Nichtzutreffen eines abgeschlossenen oder laufenden Insolvenzverfahrens sowie seine strafrechtliche und arbeitsrechtliche Unbescholtenheit bestätigt.

Zu den weiteren vorzulegenden Unterlagen siehe Punkt 2.5.1.

2.6 Keine Vergütung für Angebotserstellung

Für die Angebotserstellung steht den Bietern keinerlei Vergütung zu.

2.7 Ausschließungsgründe

Von der Teilnahme am Vergabeverfahren werden Bewerber ausgeschlossen, wenn

– gegen sie ein Konkursverfahren oder ein gerichtliches Ausgleichverfahren eingeleitet oder die Eröffnung eines Konkursverfahrens mangels hinreichenden Vermögens abgewiesen wurde;

– sie sich in Liquidation befinden oder ihre gewerbliche Tätigkeit eingestellt haben;

– gegen sie oder – sofern es sich um juristische Personen, handelsrechtliche Personengesellschaften, eingetragene Erwerbsgesellschaften oder Arbeitsgemeinschaften handelt – gegen physische Personen, die in der Geschäftsführung tätig sind, ein rechtskräftiges Urteil ergangen ist, das ihre berufliche Zuverlässigkeit in Frage stellt;

– sie im Rahmen ihrer beruflichen Tätigkeit eine schwere Verfehlung begangen haben, die von der Telekom-Control GmbH nachweislich festgestellt wurde;

– sie ihre Verpflichtungen zur Zahlung der Sozialversicherungsbeiträge oder der Steuern oder Abgaben nicht erfüllt haben, oder

– sie sich bei der Erteilung von Auskünften nach dieser Ausschreibung oder des Bundesvergabegesetzes in erheblichen Maßen falscher Erklärungen schuldig gemacht haben.

Wegen zu erwartender Interessenkonflikte (insb. Befangenheit iSd § 7 AVG) werden von der Teilnahme am Vergabeverfahren weiters Bewerber ausgeschlossen, welche als Zertifizierungsdiensteanbieter der Aufsicht der Aufsichtsstelle unterliegen oder die Aufnahme der Tätigkeit eines Zertifizierungsdiensteanbieters beabsichtigen. Der Bieter hat in der Bietererklärung (siehe Anlage 2) auch zu erklären, dass er in Österreich nicht als Zertifizierungsdiensteanbieter tätig ist und für die nächsten drei Jahre auch nicht beabsichtigt, eine Tätigkeit als Zertifizierungsdiensteanbieter aufzunehmen.

Die Telekom-Control GmbH hat iSd. § 16 Abs. 3 BVergG eine Auskunft aus der zentralen Verwaltungsstrafevidenz des Bundesministers für Arbeit, Gesundheit und Soziales gemäß § 28 b des Ausländerbeschäftigungsgesetzes zur Beurteilung der beruflichen Zuverlässigkeit von für die Zuschlagserteilung in Frage kommenden Bewerbern, Bietern und deren Subunternehmen einzuholen. Die Bieter werden eingeladen, einen solchen Auszug – sollten sie über einen solche verfügen, und dieser nicht älter als 6 Monate ist – ihren Unterlagen beizulegen.

2.8 Ausscheidungsgründe

Von der Wahl des Angebotes für den Zuschlag werden gemäß § 52 Abs. 1 BVergG ausgeschieden:

– Angebote von Bietern, bei welchen die Befugnis oder die finanzielle, wirtschaftliche oder technische Leistungsfähigkeit bzw. die Zuverlässigkeit nicht gegeben ist;

– Angebote von Bietern, die nach § 16 Abs. 4 BVergG vom Wettbewerb ausgeschlossen sind;

– Angebote, die eine nicht plausible Zusammensetzung des Gesamtpreises aufweisen;

– Angebote, bei denen der Bieter keine Preise angibt, sondern nur erklärt, das billigste Angebot um einen bestimmten Prozentsatz oder Wert zu unterbieten;

– Angebote von Bietern, die es unterlassen haben, innerhalb der von ihnen gestellten Frist die verlangten Aufklärungen zu geben oder deren Aufklärung eine nachvollziehbare Begründung entbehrt;

– verspätet eingebrachte Angebote;

– den Ausschreibungsbestimmungen widersprechende sowie fehlerhafte oder unvollständige Angebote, wenn die Mängel nicht behoben wurden oder nicht behebbar sind oder Teilangebote, wenn sie nicht zugelassen wurden;

– Angebote von Bietern, die mit anderen Bietern für den Auftraggeber nachteilige, gegen die guten Sitten oder gegen den Grundsatz des Wettbewerbes verstoßende Absprachen getroffen haben;

– Angebote von Arbeits- und Bietergemeinschaften, die keine Erklärung gemäß § 17 dritter Satz BVergG abgegeben haben;

– rechnerisch fehlerhafte Angebote, die nicht weiter zu berücksichtigen sind.

2.9 Bietergemeinschaften

Bietergemeinschaften (Arbeitsgemeinschaften) können Angebote einreichen (§ 17 BVergG).

Die Mitglieder der Bietergemeinschaft haben die Erklärung abzugeben, dass sie im Auftragsfall die Leistungen als Arbeitsgemeinschaft erbringen und dafür und für sämtliche Folgen einer allenfalls nicht vertragsgemäßen Leistungserbringung zu ungeteilten Hand (solidarisch) haften.

Im Angebot muss eine zentrale Stelle (allenfalls ein Mitglied) genannt werden, an die alle Erklärungen der Telekom-Control GmbH mit bindender Wirkung für die Bietergemeinschaft (Arbeitsgemeinschaft) und für jedes Mitglied gerichtet werden können.

2.10 Subunternehmer

Die Beauftragung von Subunternehmern ist zulässig. Die Vergabe von mehr als 50 % des Auftragswertes an einen einzigen Subunternehmer ist jedoch unzulässig.

Ein Wechsel der im Angebot genannten Subunternehmer ist nur mit Genehmigung der Telekom-Control GmbH zulässig. Bei Wechsel eines Subunternehmers ist die ausschreibungsgemäße Vorgangsweise, insbesondere die Vorlage von Nachweisen und Bestätigungen (siehe oben) einzuhalten.

Der Auftragnehmer haftet für Tätigkeiten seiner Subunternehmer und deren Leute, wie für seine eigenen Tätigkeiten und Unterlassungen und seiner eigenen Leute.

2.11 Alternativangebote, Varianten

2.11.1 Alternativangebote

Alternativangebote sind grundsätzlich zulässig und sind als solche zu kennzeichnen und in separater Bindung (Heftung) oder gesondertem Kuvert zu überreichen. Das Kuvert hat außen einen Hinweis auf das Hauptangebot aufzuweisen. Weiters ist das Vorliegen von Alternativangeboten auf dem Deckblatt zum ausschreibungsgemäßen Angebot zu vermerken.

Alternativangebote müssen den in der Ausschreibung beschriebenen Anforderungen mindestens gleichwertig sein. Bezieht sich das Alternativangebot auf die rechtlichen Vertragsbestimmungen, ist es nur neben einem bezüglich dieser Bestimmungen ausschreibungsgemäßen Angebot zulässig.

2.11.2 Varianten

Variantenangebote sind als solche zu kennzeichnen und in separater Bindung (Heftung) oder gesondertem Kuvert zu überreichen. Das Kuvert hat außen einen Hinweis auf das Hauptangebot aufzuweisen. Weiters ist das Vorliegen von Variantenangeboten auf dem Deckblatt zum Hauptangebot zu vermerken.

2.12 Teilangebote

Teilangebote sind nicht zugelassen.

2.13 Fristen

2.13.1 Angebotsfrist

Die Angebotsfrist endet am 05.02.2001 um 09:30 Uhr. Bis zu diesem Zeitpunkt muss das Angebot in einem verschlossenen Umschlag mit der Aufschrift „Nicht öffnen – Angebot Public-Key-Infrastruktur; GZ FAUS 19/2000“ per Einschreiben oder per Boten bei der Telekom-Control GmbH eingelangt sein.

2.13.2 Berichtigungen, Fragen

Allfällige Berichtigungen der Bewerber und Bieter zur Ausschreibung und Fragen der Bewerber und Bieter sind schriftlich oder per E-Mail so rechtzeitig an die Telekom-Control GmbH zu richten, dass sie spätestens bis zum 01.01.2001 um 24:00 Uhr bei der Telekom-Control GmbH einlangen. Es werden nur die Fragen jener Bewerber und Bieter beantwortet, die die Ausschreibungsunterlagen gemäß Punkt 2.4.3 erworben haben. Die Beantwortung erfolgt gesammelt schriftlich sowie per E-Mail und ergeht an alle Bewerber und Bieter, die die Ausschreibungsunterlagen gemäß Punkt 2.4.3 erworben haben, an die von diesen bekannt gegebenen Zustelladressen bis spätestens 15.01.2001. Zur Fristwahrung für die Beantwortung ist der Tag des Absendens maßgeblich.

2.13.3 Öffnung der Angebote

Die Öffnung der Angebote erfolgt am 05.02.2001 um 10:00 Uhr in den Räumlichkeiten der Telekom-Control GmbH durch eine Kommission der Telekom-Control GmbH. Die Bieter (jeweils ein Vertreter) sind berechtigt, an der Öffnung teilzunehmen.

2.13.4 Vertiefte Angebotsprüfung

Für den Fall einer vertieften Angebotsprüfung (§ 49 BVergG) gelten die im Preisraster Anlage 4 angeführten Positionen als wesentlich.

2.13.5 Zuschlagskriterien

Die Wahl des Angebotes für den Zuschlag erfolgt nach folgenden Kriterien, die in der angegebenen Reihenfolge von 1. – 5. gewichtet werden:

1. Erfüllung der Anforderungen des Signaturgesetzes, der Signaturverordnung und des Entwurfs des Certification Practice Statements (Anhang A)

2. Zeitrahmen für Implementierung und Abnahme

3. Preisgestaltung

4. Technologieneutralität (Unterstützung möglichst vieler international anerkannter Standards)

5. Wartung, Support und Schulung

6. Referenzen

2.13.6 Verständigung vom Zuschlag

Der Bieter, der den Zuschlag erhält, wird davon bis spätestens 05.03.2001 verständigt. Dieser Bieter (Auftragnehmer) hat den Zugang dieser schriftlichen Verständigung unverzüglich schriftlich und vorab per Fax oder E-Mail zu bestätigen. Auch ohne eine derartige Bestätigung des Auftragnehmers ist der Leistungsvertrag durch Verständigung von der Erteilung des Zuschlages zu Stande gekommen.

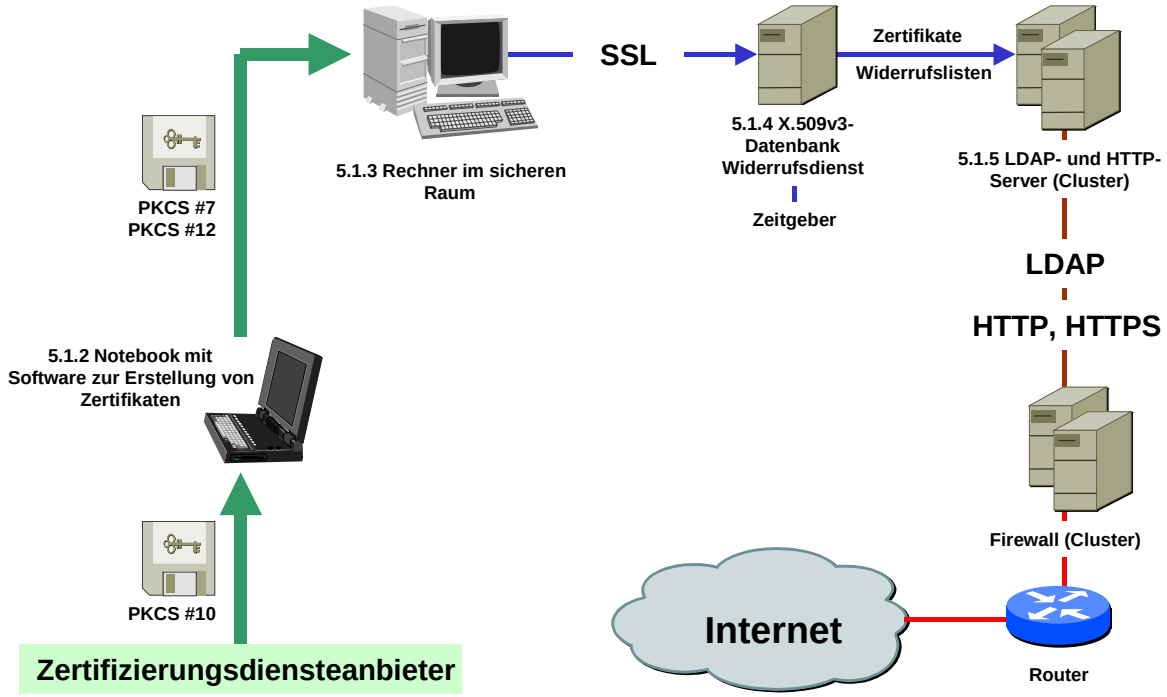
3. Beschreibung der Public-Key-Infrastruktur

3.1 Allgemeines

3.1.1 Überblick

Die Telekom-Control GmbH wird im Namen der Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen X.509v3-Zertifikate für Zertifizierungsdiensteanbieter ausstellen, diese Zertifikate in einem LDAP-Verzeichnis und über HTTP abrufbar halten und gegebenenfalls widerrufen.

Die technische Infrastruktur ist in der folgenden Grafik dargestellt:



Der Antrag des Zertifizierungsdiensteanbieters auf Ausstellung eines Zertifikates wird im Format PKCS#10 oder einem anderen geeigneten Format auf einem Datenträger wie z. B. einer Diskette übergeben.

Die Erstellung der Zertifikate wird auf einem Rechner (im Folgenden „Notebook im Tresor der Aufsichtsstelle“) vorgenommen, der keinerlei Netzverbindung hat. Die Signaturerstellungshardware muss den Anforderungen an sichere Signaturerstellungseinheiten entsprechen. Die Hardware wird in einem Tresor im sicheren Raum der Aufsichtsstelle aufbewahrt.

Die erstellten Zertifikate werden in einem geeigneten Format (z. B. PKCS#7 oder PKCS#12) auf einem Datenträger wie z. B. eine Diskette exportiert und von einem Rechner, der sich im sicheren Raum (aber nicht im Tresor) befindet (im Folgenden „Rechner im sicheren Raum“), in den Verzeichnisdienst eingespielt. Die Verbindungsleitung ist eine Standleitung oder eine Wählleitung, die Übertragung wird durch beiderseitige Authentifizierung und starke Verschlüsselung gesichert (z. B. mittels SSL oder TLS).

In einem noch auszuwählenden Rechenzentrum im Raum befindet sich ein Server, der eine Datenbank der X.509v3-Zertifikate samt Status (gültig, abgelaufen, widerrufen) verwaltet und in regelmäßigen Abständen Widerrufslisten erzeugt und signiert. Die dafür verwendete Signaturerstellungshardware muss den Anforderungen an sichere Signaturerstellungs-einheiten entsprechen. Ein Zeitgeber muss eine qualitätsgesicherte Zeit bereitstellen. Dieser Rechner verarbeitet auch Anträge auf Widerruf eines Zertifikates.

Verzeichnisdienst: Die Zertifikate und Widerrufslisten sind über einen weiteren Server im Rechenzentrum mittels LDAP (auch mit SSL- bzw. TLS-Unterstützung), HTTP und HTTPS abrufbar. Dieser Server fungiert auch als Webserver und stellt Informationen über die Aufsichtsstelle sowie die Möglichkeit, nach einzelnen Zertifikaten zu suchen, bereit. Der Server wird, um Ausfallsicherheit zu gewährleisten, als Cluster ausgeführt.

Über die Firewall, welche ebenfalls als Cluster ausgeführt wird, werden ausschließlich Zugriffe mit den Protokollen LDAP (auch mit SSL- bzw. TLS-Unterstützung), HTTP und HTTPS auf den Server des Verzeichnisdienstes zugelassen.

Zur räumlichen Unterbringung: Im wesentlichen werden die Dienste der Aufsichtsstelle an zwei verschiedenen Orten untergebracht, nämlich in einem sicheren Raum der Aufsichtsstelle (Zertifizierungsdienst) und in einem noch zu suchenden Rechenzentrum im Raum Wien (Verzeichnis- und Widerrufsdienst). Im Rechenzentrum sollen alle Komponenten in einem gemeinsamen Sicherheitsschrank untergebracht werden (siehe aber 3.4.2). Teile der Dienste werden in einem Call-Center (Entgegennahme der Widerrufsanträge und Eingabe in das Widerrufssystem), Teile in einem Banktresor oder dergleichen (Zweitsystem des Zertifizierungsdienstes) untergebracht.

3.1.2 Abgrenzung der Ausschreibung

Gegenstand der Ausschreibung ist

– die gesamte Hardware und Software, die zum Ausstellen von Zertifikaten benötigt wird

– die gesamte Hardware und Software, die zum Betrieb des Verzeichnisdienstes benötigt wird

– die gesamte Hardware und Software, die zum Betrieb des Widerrufsdienstes benötigt wird

– die Integration dieser Leistungen zu einem betriebssicheren Gesamtsystem

– die Erstellung der nötigen Dokumentation und Sicherheitskonzepte und die Einschulung

– Wartungsleistungen

Von dieser Ausschreibung ist insbesondere nicht umfasst:

– der Betrieb des Zertifizierungs-, Verzeichnis- oder Widerrufsdienstes (abgesehen von Wartungsleistungen)

– Rechenzentrumsleistungen

– Call-Center-Leistungen für den Widerruf

– die Erstellung von Webseiten für den Verzeichnisdienst (von der Ausschreibung umfasst ist aber die Erstellung von Musterscripts für die Abfrage im Verzeichnis)

– die Bereitstellung des Internetzuganges oder von Hardware dafür (z. B. Router), weiters die Firewall für den Verzeichnis- und Widerrufsdienst

– die Verbindungsleitung zwischen der Telekom-Control GmbH und dem Rechenzentrum und Modems (von der Ausschreibung umfasst ist aber die Software für das sichere Übertragungsprotokoll)

– Systeme zur Erstellung von Backups (z. B. Bandlaufwerke) für den Verzeichnis- und Widerrufsdienst

– Zutrittskontrollsysteme, Alarmanlage, Brandschutz, Behältnisse, ...

3.1.3 Allgemeine Anforderungen

Die Anforderungen an die Zertifizierungs-, Verzeichnis- und Widerrufsdienste der Aufsichtsstelle ergeben sich aus dem Signaturgesetz und aus der Signaturverordnung.

Der aktuelle Entwurf des Certification Practice Statement der Aufsichtsstelle für elektronische Signaturen ist diesen Ausschreibungsunterlagen als Anhang A beigelegt. Daraus ergeben sich die geplanten Tätigkeiten und Sicherheitsmaßnahmen der Aufsichtsstelle und damit auch konkretere Anforderungen an die eingesetzten technischen Komponenten.

Die Telekom-Control GmbH nimmt aber an, dass die Anforderungen sich in den nächsten Jahren immer wieder ändern werden. Die Anwendung elektronischer Signaturen befindet sich erst in den Anfängen ihrer technischen Entwicklung. Das mit dieser Ausschreibung zu vergebende System soll daher größtmögliche Flexibilität bieten, um nach Möglichkeit auch andere Anforderungen (z. B. durch ein anderes Certification Practice Statement oder einen anderen Aufbau der Zertifizierungshierarchie) unterstützen zu können.

Die Aufsichtsstelle ist bemüht, ihre Dienste möglichst technologieneutral anzubieten. Soweit möglich sollen allgemein anerkannte technische Normen unterstützt werden. Eine Bevorzugung bestimmter technischer Produkte soll nicht stattfinden.

3.2 Zertifizierungsdienste

3.2.1 Allgemeines

Ausgestellt werden X.509v3-Zertifikate. Die geplante Zertifizierungshierarchie kann Punkt 1.3 des beiliegenden Entwurfs des Certification Practice Statement (Anhang A) entnommen werden. Es ist aber nicht auszuschließen, dass später andere Anforderungen an die Zertifizierungshierarchie gestellt werden. Zukünftige Erweiterungen oder Umgestaltungen der Zertifizierungshierarchie sollen daher leicht möglich sein.

Vom Umfang dieser Ausschreibung umfasst sind:

– die Ausstellung von TOP-Zertifikaten nach 1.3.0.1 des Entwurfs des CPS

– die Ausstellung von ACCREDITED-CERTIFICATION-SERVICES-Zertifikaten nach 1.3.0.2 des Entwurfs des CPS

– die Ausstellung von QUALIFIED-CERTIFICATION-SERVICES-Zertifikaten nach 1.3.0.3 des Entwurfs des CPS

– die Ausstellung von CERTIFICATION-SERVICES-Zertifikaten nach 1.3.0.4 des Entwurfs des CPS

– die entsprechenden Zweitsysteme dazu (siehe Punkt 4.7 des Entwurfs des CPS).

Als Option ist die zusätzliche Möglichkeit der Ausstellung von CROSS-CERTIFICATION-Zertifikaten nach 1.3.0.5 des Entwurfs des CPS samt eines entsprechenden Zweitsystems anzubieten.

Die Ausstellung von Zertifikaten erfolgt offline. Das Notebook des Zertifizierungsdienstes sind also zu keinem Zeitpunkt an ein Netz angebunden. Es darf nicht notwendig sein, dass zu irgendeinem Zeitpunkt (nach der Erstinstallation des Notebooks) eine Netzanbindung vorgenommen wird.

3.2.2 Zertifikatsinhalt

Hinsichtlich der Inhalte der auszustellenden Zertifikate muss jedenfalls die Aufnahme der Inhalte nach Punkt 7.1 des Entwurfs des CPS möglich sein.

Darüber hinaus ist eine möglichst freie Konfigurierbarkeit hinsichtlich zusätzlicher Einträge in den Zertifikaten wünschenswert.

3.2.3 Zertifikatsanträge

Die Anträge auf Ausstellung eines Zertifikates werden – da das Notebook des Zertifizierungsdienstes immer offline ist – auf einem Datenträger wie z. B. einer Diskette in den Zertifizierungsdienst eingebracht.

Es muss jedenfalls das Datenformat PKCS#10 für den Zertifikatsantrag unterstützt werden.

Die Zertifizierungsdienste der Aufsichtsstelle sollen so technologieneutral wie möglich angeboten werden. Nach Möglichkeit sollen daher auch Zertifikate an Zertifizierungsdiensteanbieter ausgestellt werden können, die selbst nicht die Technologie X.509v3 einsetzen. Die Unterstützung weiterer Datenformate für den Zertifikatsantrag ist daher wünschenswert.

3.2.4 Zertifikate

Die ausgestellten Zertifikate werden – da das Notebook des Zertifizierungsdienstes immer offline ist – auf einen Datenträger wie z. B. eine Diskette übertragen.

Als Datenformat kann beispielsweise PKCS#7 oder PKCS#12 verwendet werden. Das Datenformat muss jedenfalls vom Verzeichnisdienst unterstützt werden, sodass eine problemlose Einbringung der Zertifikate in den Verzeichnisdienst möglich ist.

3.2.5 Räumliche Unterbringung und Platzangebot

Die Zertifizierungsdienste der Aufsichtsstelle werden in einem eigenen Raum, der entsprechend gesichert wird, untergebracht. Die Zweitsysteme der Aufsichtsstelle (siehe § 3 Abs. 1 SigV und Punkt 4.7 des Entwurfs des Certification Practice Statement) werden in einem Banktresor untergebracht.

Das Sicherheitskonzept sieht vor, dass die gesamte Hardware (also sowohl die Signaturerstellungshardware als auch die Rechner, auf denen die Software für den Zertifizierungsvorgang installiert ist) in einem Tresor untergebracht sind. Während des Ausstellungsvorganges selbst wird die Hardware gegebenenfalls dem Tresor entnommen, nicht aber aus dem sicheren Raum entfernt.

Der zur Verfügung stehende Tresor weist Innenmaße von 1585 mm (Höhe) x 729 mm (Breite) x 504 mm (Tiefe) auf.

Sowohl für das Hauptsystem als auch für das Zweitsystem besteht also die Anforderung, dass die eingesetzte Hardware auf kleinem Raum untergebracht werden kann und nicht sensibel auf Bewegungen reagiert. Beispielsweise wäre eine Lösung denkbar, bei welcher die Software auf einem Notebook (oder auf mehreren Notebooks) installiert ist. Als kryptographische Module kämen Chipkarten in Frage.

Bevorzugt würde eine Lösung, bei welcher mehrere verschiedene Signaturerstellungsdaten mit demselben Rechner und derselben Software verwaltet werden können. Es ist aber – im

Rahmen des zur Verfügung stehenden Platzes – auch eine Lösung denkbar, bei welcher für jede Kategorie von Zertifikaten eine eigene Hardware verwendet wird.

3.2.6 Signaturerstellungshardware und Zeitgeber

Die Signaturerstellungshardware muss den Anforderungen an sichere Signaturerstellungseinheiten entsprechen.

Angesichts der geringen Anzahl ausgestellter Zertifikate und der geforderten Genauigkeit von maximal einer Minute Abweichung von der tatsächlichen Zeit ist eine manuelle Adjustierung der Systemzeit am Notebook des Zertifizierungsdienstes möglich. Es kann aber als Option auch ein Zeitgeber (z. B. DCF 77, GPS) mit direkter Verbindung zum Rechner des Zertifizierungsdienstes angeboten werden.

3.2.7 Vier-Augen-Prinzip

Es muss sichergestellt sein, dass ein Zertifikat im Namen der Aufsichtsstelle nur dann ausgestellt werden kann, wenn zwei dazu berechtigte Personen gemeinsam das Zertifikat ausstellen. Das System des Zertifizierungsdienstes muss mindestens acht User verwalten können und überprüfen, ob zwei dieser mindestens acht Personen gemeinsam die Ausstellung vornehmen.

3.2.8 Dimensionierung

Da die Aufsichtsstelle nicht am Markt tätig wird, sondern lediglich an andere Zertifizierungsdienste Zertifikate ausstellt, ist davon auszugehen, dass nur eine sehr kleine Anzahl von unter 100 Zertifikaten pro Jahr ausgestellt wird.

3.3 Widerrufsdienste

3.3.1 Allgemeines

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, welches in einer separaten Ausschreibung ausgewählt wird, geführt. In regelmäßigen Abständen von einigen Stunden werden Widerrufslisten (CRLs) im Format X.509v2 (RFC 2459) erzeugt. Bei jedem einzelnen Widerruf wird zudem umgehend eine neue Widerrufsliste erzeugt. Die Abstände zwischen der Erzeugung von Widerrufslisten sollen frei konfigurierbar sein. Hinsichtlich der Inhalte der auszustellenden Widerrufslisten muss jedenfalls die Aufnahme der Inhalte nach Punkt 7.2 des Entwurfs des CPS möglich sein.

Die Widerrufslisten werden vom jeweils gültigen CERTIFICATE-REVOCATION-Schlüssel der Aufsichtsstelle signiert. Für die Signatur unter Widerrufslisten wird also ein anderer Schlüssel eingesetzt als für die Signatur unter Zertifikate.

Zu Beginn wird nur eine einzige Widerrufsliste für alle Zertifizierungsdienste der Aufsichtsstelle ausgegeben – also für alle jemals von der Aufsichtsstelle ausgegebenen Zertifikate, die widerrufen wurden.

Möglicherweise werden zu einem späteren Zeitpunkt auf Grund 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. Die Möglichkeit, zu einem späteren Zeitpunkt mehrere verschiedene Widerrufslisten auszugeben, muss durch das angebotene System gewährleistet sein.

Es bestehen zwei Möglichkeiten, einen Widerruf vorzunehmen: Widerruf durch Zertifikatsinhaber und Widerruf durch die Telekom-Control GmbH.

3.3.2 Automatisierter Widerruf durch Zertifikatsinhaber

Jeder Zertifikatsempfänger soll die Möglichkeit haben, sein eigenes Zertifikat selbsttätig zu widerrufen. Diese Möglichkeit des automatisierten Widerrufs besteht darin, dass der Zertifikatsempfänger bei der Ausstellung des Zertifikates eine Codezahl aussucht, 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. Die Entgegennahme des Widerrufs erfolgt rund um die Uhr durch ein Call-Center, welches in einer separaten Ausschreibung ermittelt wird.

Besonders kritisch ist natürlich die Möglichkeit von Attacken auf das Widerrufssystem, mit welchen versucht wird, das Zertifikat eines Zertifizierungsdiensteanbieters zu widerrufen, um ihn in Misskredit zu bringen. Eine mögliche Realisierung würde so aussehen, dass der Zertifikatsempfänger der Telekom-Control GmbH bei der Ausstellung des Zertifikates lediglich den Hashwert der Codezahl bekanntgibt und die Codezahl bis zum Widerruf geheimhält.

Das vom Bieter angebotene Widerrufssystem müsste dazu umfassen:

– Regeln für die Auswahl der Codezahlen, die gewährleisten, dass die Codezahl nicht ableitbar und so lang ist, dass sie nicht erraten oder durchprobiert werden kann, und dass sie in einem Telefonat übertragen werden kann (z. B. nur Ziffern und Kleinbuchstaben, keine Sonderzeichen, ...)

– eine einfache Software, die diese Regeln überprüft und den Hashwert errechnet (es muss sichergestellt werden, dass der Hashwert vom Zertifikatsempfänger in derselben Weise ausgerechnet wird, wie er im Widerrufsfall vom Widerrufssystem errechnet wird). Hinsichtlich dieser Software muss auch die Möglichkeit bestehen, sie an beliebig viele Zertifikatsempfänger kostenlos weiterzugeben.

– eine Eingabemöglichkeit für die Call-Center-Agents, in welchen das zu widerrufende Zertifikat, die Codezahl, der vom Anrufer angegebene Name und die von ihm angegebene Rückrufnummer und der Name des Call-Center-Agents eingegeben und an den Widerrufsdienst übermittelt werden können. Für die detaillierte Beschreibung in Kapitel 4 wird angenommen, dass dies als Webformular auf den Rechnern 5.1.5 realisiert wird und die Verbindung zwischen Call-Center und Webserver als HTTPS-Verbindung mit beiderseitiger Authentifizierung aufgebaut wird

– die Prüfung der übermittelten Daten durch den Rechner des Widerrufsdienstes und gegebenenfalls die umgehende Erstellung einer neuen Widerrufsliste

Die nähere Ausgestaltung des Widerrufssystems obliegt dem Bieter. Es steht dem Bieter auch frei, statt dem beschriebenen Widerrufssystem ein anderes Widerrufssystem

anzubieten, welches in gleichwertiger Weise einen sicheren Widerruf durch den Zertifikatsinhaber Gewähr leistet.

3.3.3 Widerruf durch die Telekom-Control GmbH

Es muss die Möglichkeit bestehen, beliebige Zertifikate auf die Widerrufsliste zu setzen. Ein Widerruf durch die Mitarbeiter der Telekom-Control GmbH darf nur möglich sein, wenn zwei dazu berechtigte Personen gemeinsam den Widerruf durchführen. Die Benutzerverwaltung des Widerrufssystems muss mindestens acht User verwalten können.

Der Widerruf soll sowohl von einem Rechner im sicheren Raum der Telekom-Control GmbH aus durchgeführt werden können (Regelfall) als auch direkt im Rechenzentrum (beispielsweise dann, wenn in den sicheren Raum eingebrochen und der Rechner beschädigt wurde).

Die Verbindung zwischen dem Rechner im sicheren Raum der Telekom-Control GmbH und dem Rechenzentrum ist mittels beiderseitiger Authentifikation sowie starker Verschlüsselung zu sichern (z. B. SSL oder TLS).

Die Auswahl der Verbindungsleitung selbst ist nicht Gegenstand dieser Ausschreibung.

3.3.4 Signaturerstellungshardware und Zeitgeber

Die für das Signieren von Widerrufslisten eingesetzte Signaturerstellungshardware muss den Anforderungen an sichere Signaturerstellungseinheiten entsprechen. Weiters ist ein Zeitgeber (z. B. DCF 77, GPS) einzusetzen. Die Abweichung der Zeit des Widerrufsdienstes von der tatsächlichen Zeit darf maximal eine Minute betragen. Es sind Maßnahmen vorzusehen, um die Richtigkeit des empfangenen Zeitsignals im Rahmen der vorgegebenen Toleranz sicherzustellen.

3.4 Verzeichnisdienste

3.4.1 Allgemeines

Über die Verzeichnisse der Aufsichtsstelle müssen sämtliche jemals ausgestellten Zertifikate der Aufsichtsstelle und die Widerrufslisten abgerufen werden können. Der Abruf muss sowohl mittels LDAP als auch mittels HTTP (jeweils mit SSL- und TLS-Unterstützung) über ein entsprechendes Webformular möglich sein.

Die Verzeichnisdienste werden in einem Rechenzentrum im Raum Wien untergebracht werden, welches in einer separaten Ausschreibung ausgewählt wird.

3.4.2 Ausfallsicherheit

Ausfälle des Verzeichnisdienstes müssen innerhalb der in Anlage 5 Punkt 6 angeführten maximalen Ausfallzeiten liegen. Die Server sind als Cluster auszuführen, wobei davon ausgegangen wird, dass beide Rechner im selben Sicherheitsschrank im Rechenzentrum untergebracht werden.

Als Option ist die Möglichkeit anzubieten, die Rechner räumlich getrennt (über eine Entfernung von einigen Hundert Metern) aufzustellen, sodass z. B. auch bei einem Brand im Rechenzentrum der Dienst weiter erbracht werden kann.

Eine Katastrophenausfallsicherheit (Aufstellung der Rechner in zwei verschiedenen Rechenzentren) ist aber nicht geplant.

3.4.3 Konfiguration der X.509v3-Datenbank

Die Konfiguration der X.509v3-Datenbank (Einbringen neuer Zertifikate,...) soll von einem Rechner aus dem sicheren Raum der Aufsichtsstelle heraus möglich sein.

Die Verbindung zwischen dem Rechner im sicheren Raum der Telekom-Control GmbH und dem Rechenzentrum ist mittels beiderseitiger Authentifikation sowie starker Verschlüsselung zu sichern (z. B. SSL oder TLS).

Die Auswahl der Verbindungsleitung selbst ist nicht Gegenstand dieser Ausschreibung.

3.4.4 LDAP- und HTTP-Server

Der HTTP-Server muss auch HTTPS (SSL- und TLS-Serverauthentifikation mit mindestens 1023 Bit RSA sowie Verschlüsselung mit mindestens 90 Bit symmetrisch) unterstützen können. Eine Clientauthentifikation erfolgt für den HTTPS-Zugriff nicht (außer bei Zugriff durch das Call-Center beim Widerruf); der Zugang zu den Verzeichnisdiensten ist anonym möglich.

Die Erstellung von Webseiten und dergleichen ist nicht Gegenstand dieser Ausschreibung. Im Rahmen der Ausschreibung sind aber exemplarische Scripts zu erstellen, mittels derer Abfragen aus dem LDAP-Verzeichnis erstellt werden können, wobei Abfragen nach dem Namen des Zertifikatsempfängers, nach dem Ausstellungsdatum des Zertifikates, nach der Seriennummer des Zertifikates, nach dem Status des Zertifikates (gültig, abgelaufen, widerrufen), nach dem Widerrufszeitpunkt oder nach einer Kombination dieser Merkmale möglich sein müssen. Mit diesen Scripts soll ausschließlich auf den (am selben Rechner laufenden) LDAP-Server zugegriffen werden, nicht aber auf die Datenbank des Widerrufsdienstes.

Die vom HTTP-Server angebotenen Inhalte werden als HTML-Seiten oder in anderen Dateiformaten (z. B. GIF, JPG, PDF oder dergleichen) bei der Telekom-Control GmbH erstellt und in dieser Form auf den HTTP-Server überspielt. Der HTTP-Server soll die Dateien in diesen Dateiformaten abrufbar halten und keine proprietären Datenformate verwenden.

Die Verbindung zwischen der Telekom-Control GmbH und dem Rechenzentrum ist mittels beiderseitiger Authentifikation sowie starker Verschlüsselung zu sichern (z. B. SSL oder TLS).

3.5 Verbindung zwischen den Komponenten

Zwischen der Telekom-Control GmbH und dem Rechenzentrum wird eine Standleitung oder eine Wählleitung eingerichtet. Die Auswahl der Leitung und der Modems ist nicht Gegenstand dieser Ausschreibung.

Die Verbindung zwischen der Telekom-Control GmbH und dem Rechenzentrum ist mittels beiderseitiger Authentifikation sowie starker Verschlüsselung zu sichern (z. B. SSL oder TLS).

Folgende Zugriffe müssen möglich sein:

– Einbringen von Zertifikaten in den Verzeichnisdienst. Dieser Zugriff wird vom Rechner im sicheren Raum aus vorgenommen. Bevor das Zertifikat in die Datenbank und auf den LDAP-Server aufgenommen wird, wird die Gültigkeit des Zertifikates überprüft.

– Widerruf eines Zertifikates im Verzeichnisdienst. Dieser Zugriff darf nur vom Rechner im sicheren Raum aus (oder direkt im Rechenzentrum) möglich sein.

– Wartung des HTTP-Servers (Einspielen neuer Webseiten, Löschen von Webseiten). Dieser Zugriff wird von einem Rechner außerhalb des sicheren Raumes vorgenommen, es gibt auch kein Vier-Augen-Prinzip. Daher wird für diesen Zugriff auch nur ein Schreibrecht auf die Verzeichnisse mit den Inhalten des Webservers eingeräumt.

– Wartung der Firewall. Dieser Zugriff wird von einem Rechner außerhalb des sicheren Raumes vorgenommen.

– Übermittlung von Codes im Zuge eines Widerrufs via Call-Center (siehe 3.3.2).

– Aktivierung und Deaktivierung der Systemuhr-Synchronisierung (siehe 5.2.11).

Die SSL- bzw. TLS-Clientauthentifikation wird mit kryptographischen Modulen vorgenommen, die die Anforderungen an sichere Signaturerstellungseinheiten oder vergleichbare Sicherheitsanforderungen erfüllen (z. B. mittels Chipkarte).

Innerhalb des Rechenzentrums ist für die Verbindungen zwischen den einzelnen Komponenten zu beachten:

– Auf den Server des Widerrufsdienstes darf zugegriffen werden, um Zertifikate in die Datenbank einzubringen oder Widerrufe auszulösen. Bevor ein neues Zertifikat in die Datenbank und auf den LDAP-Server aufgenommen wird, wird die Gültigkeit des Zertifikates überprüft.

– Die Verbindung zwischen dem Server des Widerrufsdienstes und dem Server des Verzeichnisdienstes (LDAP, HTTP) wird so ausgestaltet, dass X.509v3-Zertifikate und X.509v2-Widerrufslisten vom Server des Widerrufsdienstes zum Server des Verzeichnisdienstes übertragen werden. Zugriffe in umgekehrter Richtung vom Server des Verzeichnisdienstes auf den Server des Widerrufsdienstes (etwa von Scripts zur Abfrage, ob ein Zertifikat gültig ist) sollen nur zu folgenden Zwecken erfolgen:

  – Übermittlung von Codes im Zuge eines Widerrufs via Call-Center (siehe 3.3.2).

  – Aktivierung und Deaktivierung der Systemuhr-Synchronisierung (siehe 5.2.11).

– Der Zugriff vom Call-Center, das Widerrufsanträge entgegennimmt, auf den Server des Widerrufsdienstes erfolgt über das Internet und die Firewall und kann so realisiert werden, dass der Call-Center-Agent eine Verbindung zum HTTP-Server aufbaut und dort ein entsprechendes Webformular ausfüllt. Die Inhalte des Webformulars werden dann an den Server des Widerrufsdienstes weitergeleitet.

Ungeachtet des Umstandes, dass eine Firewall eingesetzt werden wird, muss in der Konfiguration aller Rechner sichergestellt werden, dass außer den dokumentierten Transport- und Diensteprotokollen keine weiteren Protokolle eingesetzt werden können.

3.6 Dokumentation

Jener Bieter, der den Zuschlag erhält, hat auch detaillierte Produktinformationen zu liefern und dem Certification Practice Statement der Aufsichtsstelle entsprechende Betriebshandbücher zu erstellen. Die Dokumentation muss in deutscher Sprache vorliegen und hat zu enthalten:

- Dokumentation der gesamten eingesetzten Hardware inklusive der Signaturerstellungshardware und der Zeitgeber

- Dokumentation aller eingesetzten Betriebssysteme und der gesamten installierten Software

- Für die Server im Rechenzentrum sind Betriebshandbücher mit den folgenden Inhalten zu erstellen:

  - Detaillierte Angaben darüber, welche Bestandteile der Hardware und welche Prozesse vom Rechenzentrumspersonal überwacht werden müssen.

  - Detaillierte Angaben zur Konfiguration der Benutzerverwaltung und Zugriffsberechtigung auf die einzelnen Verzeichnisse, Dateien etc. Dazu ist das Certification Practice Statement der Aufsichtsstelle heranzuziehen.

  - Detaillierte Angaben über mögliche Störfälle und Fehlermeldungen und die jeweils zu ergreifenden Maßnahmen. Dabei ist unter Berücksichtigung der Zugriffsberechtigung festzulegen, wer jeweils einzuschreiten hat (Rechenzentrumspersonal oder Systemadministratoren der Telekom-Control GmbH).

3.7 Evaluation

An den folgenden Stellen werden kryptographische Module eingesetzt, welche den rechtlichen Erfordernisse an sichere Signaturerstellungseinheiten entsprechen müssen:

- Signatur unter Zertifikate im Zertifizierungsdienst (sowohl im sicheren Raum der Aufsichtsstelle als auch bei den Zweitsystemen)

- Signatur unter Widerrufslisten im Widerrufsdienst

- sichere Zeitstempeldienste für die Dokumentation

Weiters werden für die mittels SSL bzw. TLS gesicherte Verbindungen kryptographische Module eingesetzt, die zwar nicht für Signaturzwecke verwendet werden, im Rahmen dieser Ausschreibung aber vergleichbaren Sicherheitsanforderungen entsprechen müssen.

3.7.1 Kryptographische Module zur Signaturerstellung

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.

Der Bieter hat dem Angebot beizulegen:

- entweder die Bescheinigung einer Bestätigungsstelle gemäß § 19 SigG, mit welcher die Erfüllung der Sicherheitsanforderungen bestätigt wird, samt einem detaillierten Prüfbericht, auf welchem die Bescheinigung beruht,

– oder eine gleichwertige Bescheinigung durch eine Stelle, welche gemäß Art. 3 Abs. 4 der Signaturrichtlinie der EU-Kommission als geeignete Stelle notifiziert wurde, samt einem detaillierten Prüfbericht, auf welchem die Bescheinigung beruht,

– oder ein detailliertes Evaluierungsgutachten einer allgemein anerkannten Prüfstelle, welches nach einem allgemein anerkannten Sicherheitsprofil der Common Criteria, nach ITSEC E3 hoch oder nach vergleichbaren Evaluationskriterien erstellt wurde und in welchem sämtliche Sicherheitsanforderungen, welche die Signaturverordnung an sichere Signaturerstellungseinheiten richtet, umfasst sind.

  In diesem Fall wird die Telekom-Control GmbH eine Bestätigungsstelle gemäß § 19 SigG mit der Prüfung der Evaluierungsgutachten befassen und eine Bescheinigung gemäß § 9 SigV einholen. Der damit voraussichtlich verbundene zeitliche und finanzielle Aufwand wird bei der Bewertung der Angebote berücksichtigt werden.

  Der Bieter hat dem Angebot diesfalls eine Erklärung beizulegen, dass er der Vorlage der Unterlagen an eine Bestätigungsstelle sowie der direkten Kontaktaufnahme zwischen Bestätigungsstelle und Evaluator zustimmt.

In jedem Fall ist die Vorlage detaillierter und vollständiger Prüfberichte unbedingt erforderlich. Diese werden als Betriebs- und Geschäftsgeheimnis des Bieters behandelt und – abgesehen von der Übermittlung an eine Bestätigungsstelle, wenn keine Bescheinigung einer solchen Stelle vorliegt – unter Verschluss gehalten. Es wird darauf hingewiesen, dass die Mitarbeiter der Telekom-Control GmbH dem Amtsgeheimnis (§ 310 StGB) unterliegen.

3.7.2 Signaturerstellungssoftware

Die Software, die zur Erstellung von Signaturen unter Zertifikate oder Widerrufslisten eingesetzt werden (Hashbildung – falls diese in der Software erfolgt –, Darstellung der Zertifikatsinhalte am Bildschirm vor dem Auslösen der Signatur, Auslösung der Signatur) muss nach dem Stand der Technik geprüft sein (§ 18 SigG, § 9 SigV). Entsprechende Evaluierungsgutachten oder Bescheinigung einer Bestätigungsstelle oder einer Stelle, welche gemäß Art. 3 Abs. 4 der Signaturrichtlinie der EU-Kommission als geeignete Stelle notifiziert wurde, sind vom Bieter vorzulegen.

3.7.3 Verbindung zwischen der Telekom-Control GmbH und dem Rechenzentrum

Die Software, die zur Realisierung der sicheren Datenübertragung zwischen der Telekom-Control GmbH und dem Rechenzentrum (z. B. SSL oder TLS, beiderseitige Authentifikation, starke Verschlüsselung) eingesetzt wird, soll nach dem Stand der Technik geprüft sein. Entsprechende Evaluierungsgutachten sind vom Bieter vorzulegen.

3.7.4 Andere technische Komponenten

Evaluierungen nach anerkannten Normen der IT-Sicherheit sind wünschenswert.

3.8 Liste der nicht X.509-kompatiblen Anbieter

Jene Anbieter, denen die Aufsichtsstelle kein Zertifikat ausstellen kann, werden in eine sicher elektronisch signierten Liste aufgenommen, welche mit einer eigens dafür gewidmeten Signaturerstellungseinheit sicher elektronisch signiert wird. Die Signatur wird am Rechner im sicheren Raum der Aufsichtsstelle vorgenommen, die jeweils aktuelle Liste wird am Webserver der Aufsichtsstelle veröffentlicht.

Auch für diese Software gelten die Anforderungen an die Evaluierung gemäß 3.7.2.

3.9 Signaturprüfung

Es ist Software bereitzustellen, mit welcher die Zertifikate und Widerrufslisten der Aufsichtsstelle und die Signaturen der Aufsichtsstelle mit der rechtlich geforderten Sicherheit überprüft werden können.

4. Übersicht über einige Anforderungen aus der SigV

Aus der Signaturverordnung (BGBl II 2000/30) ergeben sich für die Public-Key-Infrastruktur der Aufsichtsstelle insbesondere die folgenden Anforderungen. Zu beachten ist, dass auf die Dienste der Aufsichtsstelle auch die meisten Anforderungen, die an Zertifizierungsdiensteanbieter, die sichere elektronische Signaturverfahren bereitstellen, anzuwenden sind.

Von einer vollständigen Auflistung der rechtlichen Anforderungen wurde abgesehen. Die Anforderungen wurden in den Entwurf eines Certification Practice Statement (Anhang A) eingearbeitet.

§ 3 Abs. 1 bis 5 SigV

(1) Die Signaturerstellungsdaten der Aufsichtsstelle müssen dem Anhang 1 Punkt 1 entsprechen (Hauptsystem). Das Erzeugungssystem muss isoliert, ausschließlich für diesen Zweck bestimmt und auf angemessene Weise vor Eingriffen und Störungen geschützt sein. Die Aufsichtsstelle hat zu ihren Signaturerstellungsdaten ein Zweitsystem an Signaturerstellungsdaten (Zweitschlüssel) zu erzeugen und alle eigenen elektronischen Signaturen, mit denen die bei ihr geführten Verzeichnisse signiert werden, auch mit diesem Zweitsystem als Backup durchzuführen. Die Signaturprüfdaten (der öffentliche Signaturschlüssel) des Zweitsystems sind mit den Signaturerstellungsdaten der Aufsichtsstelle zu signieren. Das Zweitsystem ist unter Verschluss zu halten. Die Signaturprüfdaten des Zweitsystems dürfen nur bei einem Ausfall des Hauptsystems verwendet werden, sodass auch in einem solchen Fall der ungestörte Betrieb der Signatur- und Zertifizierungsdienste der Aufsichtsstelle sichergestellt ist. Werden von der Aufsichtsstelle zusätzlich auch andere als die im Anhang 1 Punkt 1 genannten Signaturerstellungsdaten eingesetzt, so sind die Zertifikate, die die entsprechenden Signaturprüfdaten enthalten, mit dem Hauptsystem zu signieren und elektronisch jederzeit allgemein abrufbar zu halten. Die Aufsichtsstelle hat sicherzustellen, dass die von ihr eingesetzten Signaturerstellungsdaten und die Signaturprüfdaten des entsprechenden Zertifikats in komplementärer Weise anwendbar sind.

Anmerkung: Zu den Zweitsystemen siehe Punkt 4.7 des beiliegenden Entwurfs eines Certification Practice Statement (Anhang A). Die Zweitsysteme werden in einen Banktresor oder vergleichbar ausgelagert.

(2) Die Signaturerstellungsdaten ... müssen in deren Signaturerstellungseinheit erzeugt werden und dürfen diese nicht verlassen. ... Im Übrigen gelten die Anforderungen für sichere elektronische Signaturen der übrigen Signatoren.

(3) Die Signaturerstellungsdaten für sichere elektronische Signaturen der Signatoren müssen die im Anhang 1 Punkt 2 festgesetzte Mindestlänge aufweisen. ... Die verwendeten Algorithmen müssen offen gelegt sein. Die Signaturerstellungsdaten für sichere elektronische Signaturen dürfen mit an Sicherheit grenzender Wahrscheinlichkeit ausschließlich beim Signator vorkommen. Sie müssen nach dem jeweiligen Stand der Technik den eindeutigen Rückschluss auf den Signator ermöglichen. Die wiederholte Erzeugung von Signaturerstellungsdaten für sichere elektronische Signaturen darf nicht dazu

führen, dass sich die Schlüsselqualität unter das für das jeweilige Signaturverfahren maßgebliche Sicherheitsniveau vermindert.

(4) Wiederholte Anwendungen der Signaturerstellungsdaten für sichere elektronische Signaturen dürfen nicht zu einer Verminderung der Schlüsselqualität führen. Anwendungen, die die Qualität der Signaturerstellungsdaten vermindern können (zB RSA-Anwendungen auf zufällig gewählte Daten), müssen wirksam ausgeschlossen sein. Die Signaturerstellungsdaten dürfen nur für diejenigen Zwecke verwendet werden, für die sie bestimmt sind.

(5) Die Erzeugung der Signaturerstellungsdaten für sichere elektronische Signaturen muss auf einer tatsächlichen Zufälligkeit beruhen, der ein technischer Zufall oder ein signatorbezogener Zufall zu Grunde liegt. Die Signaturerstellungsdaten müssen in der im Anhang 1 Punkt 3 festgelegten Anzahl von Bitstellen durch tatsächliche Zufallselemente beeinflusst sein (qualitätsvoller Zufall). Die Zufallselemente müssen auf ihre Eignung hin ausreichend geprüft sein. Pseudozufallszahlen dürfen nicht als Ausgangsbasis verwendet werden. Wird das Erzeugungssystem für Signaturerstellungsdaten unterschiedlicher Signatoren eingesetzt, so ist ein verwendeter technischer Zufall periodisch, zumindest in Abständen von einem Monat, auf die statistische Zufallsqualität zu überprüfen. Die Prüfprotokolle sind zu dokumentieren. Liegt ein negatives Prüfergebnis vor, so sind die auf den betroffenen Signaturerstellungsdaten beruhenden Zertifikate, die seit dem letzten Prüfzeitpunkt mit positivem Ergebnis ausgestellt wurden, zu widerrufen.

§ 4 SigV

Die Aufsichtsstelle wird kein Backup der Signaturerstellungsdaten und keine Verteilung auf mehrere Signaturerstellungseinheiten vornehmen.

§ 5 SigV

Die von der Aufsichtsstelle eingesetzten Systeme, insbesondere Produkte und technische Verfahren, müssen den Sicherheitsanforderungen für sichere elektronische Signaturen entsprechen. Die Aufsichtsstelle darf nur Algorithmen, die im Anhang 2 genannt sind, einsetzen.

§ 6 Abs. 2 SigV

Zur Erstellung sicherer elektronischer Signaturen sind Hashverfahren, die im Anhang 2 Punkt 2 genannt sind, einzusetzen. Die Algorithmen zur Erzeugung des Hashwerts sind bis zu dem im Anhang 2 Punkt 2 genannten Zeitpunkt als sicher anzusehen. Zur Ergänzung des Hashwerts dürfen auch Pseudozufallszahlen verwendet werden. Zur Verschlüsselung des Hashwerts sind Algorithmen, die im Anhang 2 Punkt 3 genannt sind, einzusetzen. Die Algorithmen zur Signaturerstellung sind bis zu dem im Anhang 2 Punkt 3 genannten Zeitpunkt als sicher anzusehen. Bei der Anwendung von Signaturalgorithmen, die Zufallszahlen benötigen (zB DSA), dürfen auch Pseudozufallszahlen verwendet werden.

Anhang 1 SigV

1. Signaturerstellungsdaten der Aufsichtsstelle

Die Signaturerstellungsdaten der Aufsichtsstelle müssen dem Verfahren RSA (zur Verschlüsselung des Hashwerts) entsprechen (Hauptsystem). ...

Anmerkung: Es werden keine anderen Verfahren als RSA eingesetzt.

2. Signaturerstellungsdaten für sichere elektronische Signaturen

Die Schlüssellänge der Signaturerstellungsdaten für sichere elektronische Signaturen muss zumindest betragen:

– beim Verfahren RSA 1023 Bit, ...

Führende Nullbit sind in die Schlüssellänge nicht einzurechnen. Die Schlüssellänge ist jedenfalls für den geheimen Teil der Signaturerstellungsdaten maßgeblich.

3. Zufälle für Signaturerstellungsdaten für sichere elektronische Signaturen

Die Signaturerstellungsdaten für sichere elektronische Signaturen müssen zumindest in folgender Anzahl von Bitstellen durch tatsächliche Zufallselemente beeinflusst sein:

bei den Verfahren RSA und DSA 1023 Bit, ...

In diesen Fällen liegt ein qualitätsvoller Zufall vor.

Werden zur Sicherstellung der Einzigartigkeit von Signaturerstellungsdaten bei deren Erzeugung weitere Schlüsselelemente, zB führende oder nachlaufende Bit, in festgelegter oder in zufälliger Form eingebunden, so darf die Anzahl der durch einen qualitätsvollen Zufall beeinflussten Bitstellen dadurch nicht verringert werden.

Anhang 2 SigV

1. Technische Verfahren der Aufsichtsstelle

Bei der Aufsichtsstelle ist als Hashverfahren das Verfahren SHA-1 und zur Verschlüsselung des Hashwerts das Verfahren RSA einzusetzen (Hauptsystem). Die Verwendung des Chinese Remainder Theorem (CRT) ist nicht zulässig. ...

Anmerkung: Es werden keine anderen Verfahren als RSA und SHA-1 eingesetzt.

4. Formate für sichere elektronische Signaturen

Die für sichere elektronische Signaturen eingesetzten Formate sollten einem international anerkannten Standard oder einer anerkannten Empfehlung (zB PKCS#7 Cryptographic Message Syntax Standard) entsprechen.

5. Formate für qualifizierte Zertifikate

Die European Electronic Signatures Standardization Initiative (EESSI) ist derzeit damit beschäftigt, Formate und Normen für die Darstellung qualifizierter Zertifikate sowie für deren Inhalte auszuarbeiten. Vorläufig wird empfohlen, international anerkannte Normungsvorschläge (zB X.509 v3 certificate oder X.509 v2 CRL for use in the Internet) anzuwenden. Die detaillierte Ausprägung des Formats ist im Sicherheits- und Zertifizierungskonzept darzustellen. Zur Beschreibung ist eine Formale Notation (zB CCITT bzw. ITU-T Recommendation X.208: Specification of Abstract Syntax Notation One - ASN.1 - 1988) zu verwenden. Dies gilt auch für die Codierung der Kennzeichnung „qualifiziert“ in einem qualifizierten Zertifikat. ...

Anmerkung: Die Aufsichtsstelle signiert lediglich qualifizierte Zertifikate und Widerrufslisten. Zertifikate werden im Format X.509v3, Widerrufslisten im Format X.509v2 erstellt. Siehe dazu Punkt 7 des Entwurfs eines Certification Practice Statement (Anhang A).

5. Detaillierte technische Beschreibung der Komponenten

Kapitel 3 der Ausschreibungsunterlagen enthält eine allgemeine Beschreibung der Public-Key-Infrastruktur und der Anforderungen an diese, Kapitel 4 eine Übersicht über die Anforderungen der SigV. In diesem Kapitel werden konkretere Anforderungen an die einzelnen Komponenten der Public-Key-Infrastruktur beschrieben. Der Fragebogen in Anlage 3 dieser Ausschreibungsunterlagen dient zur Charakterisierung zusätzlicher Merkmale.

Es steht dem Bieter frei, zur Erreichung der allgemeinen Anforderungen der Kapitel 3 und 4 auch eine andere als die in Kapitel 5 gewählte Kombination technischer Komponenten vorzusehen. Diese Abweichungen sind im Angebot bei den Fragekatalogen (Anlage 3) und dem Preisraster (Anlage 4) erkenntlich zu machen und zu begründen.

Die Bieter haben den angebotenen Gesamtpreis entsprechend der folgenden Komponentenbeschreibung aufzuschlüsseln (Preisraster in Anlage 4). Wenn einzelne Komponenten höhere als die hier genannten Anforderungen erfüllen, sind diese bei der Beantwortung des Fragebogens (Anlage 3) zu spezifizieren.

5.1 Hardware

5.1.1 Signaturerstellungshardware

Die Signaturerstellungshardware umfasst kryptographische Module (z. B. Chipkarten) und Hardware-Schnittstellen, d. h. Geräte für den Zugriff auf kryptographische Module mit Hilfe eines Rechners (z. B. Chipkarten-Lesegeräte).

Es werden mindestens 12 kryptographische Module für insgesamt 20 private Schlüssel benötigt, und zwar:

Verwendungszweck	kryptographische Module (Minimum)	Private Schlüssel
C=AT, O=Telekom-Control-Kommission, OU=top C=AT, O=Telekom-Control-Kommission, OU=accredited certification services C=AT, O=Telekom-Control-Kommission, OU=qualified certification services C=AT, O=Telekom-Control-Kommission, OU=certification services C=AT, O=Telekom-Control-Kommission, OU=cross certification services C=AT, O=Telekom-Control-Kommission, OU=non-X.509-services	2	12
C=AT, O=Telekom-Control-Kommission, OU=certificate revocation	*2*	*2*
C=AT, O=Telekom-Control GmbH, CN=www.signatur.tkc.at	*2*	*2*
Server-Authentifikation des Rechners für X.509-Datenbank und Widerrufsdienst	*1*	*1*

Sichere Zeitstempeldienste bei der Dokumentation (§§ 14 u. 16 Abs. 1 SigV)	1	1
Client-Authentifikation des Rechners im sicheren Raum	1	1
Client-Authentifikation des Widerrufsdienstes (Call-Center)	1	1
Summe	10	20

Die Anzahl der benötigten kryptographischen Module lässt sich möglicherweise verringern, wenn z. B. die Rechner 5.1.4 (Widerrufsdienst) und 5.1.5 (Webserver) auf dasselbe Modul zugreifen können. Soweit ein Zweitsystem realisiert wird (siehe Punkt 4.7 des Entwurfs des CPS, Anhang A), müssen aber zwei verschiedene Module eingesetzt werden.

Alle kryptographischen Module müssen den rechtlichen Anforderungen an sichere Signaturerstellungseinheiten entsprechen (siehe Kapitel 4.7 und 6) – mit Ausnahme der Anforderungen des § 7 SigV, welche nicht von den kryptographischen Modulen selbst, sondern (soweit erforderlich) von der Software abgedeckt werden müssen.

Auch die für die Authentifikation eingesetzten kryptographischen Module müssen vergleichbaren Sicherheitsanforderungen entsprechen, obwohl sie nicht für Signaturzwecke eingesetzt werden. Dabei soll vor allem die Evaluierung des für die Authentifizierung verwendeten asymmetrischen kryptographischen Verfahrens (RSA) – insbesondere die Speicherung des privaten Schlüssels – der Evaluierung einer sicheren Signaturerstellungseinheit vergleichbar sein.

Es ist nicht notwendig, dass es sich bei allen kryptographischen Modulen um dasselbe Modell handelt. Beispielsweise könnte für den Großteil der Module Chipkarten, für das kryptographischen Modul am Rechner www.signatur.tkc.at ein Krypto-Koprozessor eingesetzt werden.

Jene kryptographische Module, die in der Tabelle kursiv dargestellt sind, müssen so konfiguriert sein, dass kryptographische Operationen (einschließlich Signatur) nach einmaliger Aktivierung des privaten Schlüssels beliebig oft ausgeführt werden können – und zwar auch dann, wenn der angeschlossene Rechner in der Zwischenzeit neu gestartet wurde. Alle übrigen kryptographischen Module sind so zu konfigurieren, dass nur zwei berechtigte Personen gemeinsam kryptographische Operationen auslösen können.

Es werden fünf Hardware-Schnittstellen benötigt: eine am Notebook im Tresor, eine am Rechner im sicheren Raum der Aufsichtsstelle, eine am Notebook des Zweitsystems, eine am Rechner für die X.509v3-Datenbank und den Widerrufsdienst und eine am LDAP- und HTTP-Server. Es soll mühelos möglich sein, die Hardware-Schnittstelle von einem Rechner zu entfernen und an einen anderen Rechner anzuschließen.

Die Signaturerstellungshardware wird die meiste Zeit über stromlos in einem Tresor aufbewahrt. Wenn für die Aufrechterhaltung der Funktionalität eine Stromversorgung erforderlich wäre, wäre diese ebenfalls bereitzustellen und es wären im Fragebogen Angaben zum Platzbedarf, der Wärmeentwicklung und der Zeitdauer bis zur Notwendigkeit eines Austausches der Stromversorgung zu machen.

5.1.2 Notebook im Tresor der Aufsichtsstelle/Notebook für das Zweitsystem

Das Notebook muss alle Erfordernisse erfüllen, damit die unter 5.2.1 bis 5.2.3 genannte Software funktionsfähig ist. Bei der Dimensionierung ist auf allfällige Software-Aktualisierungen in einem Zeitraum von drei Jahren ab Lieferung Bedacht zu nehmen.

Das Notebook muss mit einem Diskettenlaufwerk und mit einem CD-Laufwerk ausgestattet sein.

Darüber hinaus muss das Notebook über jene Schnittstellen verfügen, die zum Anschluss der Signaturerstellungshardware erforderlich sind.

Das Notebook wird die meiste Zeit über stromlos in einem Tresor aufbewahrt. Wenn für die Aufrechterhaltung der Funktionalität eine Stromversorgung erforderlich wäre, wäre diese ebenfalls bereitzustellen und es wären im Fragebogen Angaben zum Platzbedarf, der Wärmeentwicklung und der Zeitdauer bis zur Notwendigkeit eines Austausches der Stromversorgung zu machen.

Für das Zweitsystem ist ein weiteres Notebook anzubieten, das denselben Anforderungen entspricht.

Wenn die Software nicht auf einem Notebook installiert werden kann, sondern auf mehreren Notebooks oder auf einem größeren Rechner installiert werden muss, ist im Fragebogen anzugeben, wie viele Rechner benötigt werden und welcher Platzbedarf besteht.

5.1.3 Rechner im sicheren Raum

Der Rechner im sicheren Raum muss alle Erfordernisse erfüllen, damit die unter 5.2.1, 5.2.2 und 5.2.4 genannte Software funktionsfähig ist. Bei der Dimensionierung ist auf allfällige Software-Aktualisierungen in einem Zeitraum von drei Jahren ab Lieferung Bedacht zu nehmen.

Der Rechner muss mit einem Ethernet-Adapter, mit einem Diskettenlaufwerk und mit einem CD-Laufwerk ausgestattet sein.

Darüber hinaus muss der Rechner über jene Schnittstellen verfügen, die zum Anschluss der Signaturerstellungshardware erforderlich sind (für die Dokumentation nach § 11 SigG und § 16 SigV).

5.1.4 Rechner für X.509v3-Datenbank und Widerrufsdienst

Der Rechner für die X.509v3-Datenbank und den Widerrufsdienst muss alle Erfordernisse erfüllen, damit die unter 5.2.1, 5.2.2, 5.2.4 bis 5.2.6, 5.2.9, 5.2.11 und 5.2.12 genannte Software funktionsfähig ist. Bei der Dimensionierung ist auf allfällige Software-Aktualisierungen in einem Zeitraum von drei Jahren ab Lieferung Bedacht zu nehmen.

Der Rechner muss mit einem Diskettenlaufwerk und mit einem CD-Laufwerk ausgestattet sein.

Der Rechner muss mit den HTTP- und LDAP-Servern vernetzt sein. Dabei muss aber gewährleistet sein, dass von diesem Rechner aus kein Zugang zum Internet möglich ist. Darüber hinaus muss der Rechner mit einem von der Schnittstelle zu den HTTP- und LDAP-Servern unabhängigen Ethernet-Adapter ausgestattet sein.

Außerdem muss der Rechner über jene Schnittstellen verfügen, die zum Anschluss der Signaturerstellungshardware 5.1.1 erforderlich sind.

Weiters muss der Rechner mit einer Systemuhr ausgestattet sein, die automatisch abzugleichen ist, damit die Abweichung von der tatsächlichen Zeit maximal 30 Sekunden beträgt. Zu diesem Zweck können etwa DCF-77- oder GPS-Funksignale verwendet werden. Es muss jedoch gewährleistet sein, dass auch im Sicherheitsschrank des Rechenzentrums ein Empfang möglich ist (z. B. mit Hilfe einer externen Antenne). Der chronische Abgleich der Systemuhr muss mittels Software 5.2.12 aktiviert und deaktiviert werden können.

5.1.5 LDAP- und HTTP-Server (Cluster)

Die beiden LDAP- und HTTP-Server müssen alle Erfordernisse erfüllen, damit die unter 5.2.1 und 5.2.7 bis 5.2.12 genannte Software funktionsfähig ist. Bei der Dimensionierung ist vor allem zu beachten, dass bei diesen Geräten mit einer überaus hohen Zugriffshäufigkeit zu rechnen ist. Weiters ist anzunehmen, dass für unzählige Übertragungen jeweils geringer Datenmengen von wenigen tausend Byte eigene SSL- oder TLS-Verbindungen aufgebaut werden müssen. Entsprechend schnell sollte die Server-Hardware bzw. das am Server eingesetzte kryptographische Modul sein. Die Server-Hardware braucht jedoch nicht schneller zu sein, als bei einer Anbindung ans Internet mittels 2-MBit/s-Leitung sinnvoll ist.

Die beiden Rechner sind als Cluster zu konfigurieren, wobei jedes System jederzeit die jeweiligen Services des anderen Systems übernehmen können muss. Die maximale Umschaltzeit für die entsprechenden Betriebssystemparameter beträgt 5 Minuten. Die vitalen Systemparameter müssen über SNMP zu überwachen sein. Die Plattensysteme sind als RAID 5 oder RAID 0 zu konzipieren.

Bei diesen Rechnern sind Ethernet-Adapter für die Anbindung ans Internet sowie an den Rechner 5.1.4 vorzusehen. Noch einmal sei aber hervorgehoben, dass vom Internet aus keinerlei Zugang zum Rechner 5.1.4 möglich sein darf.

Da der Schlüssel für den Webserver (abgesehen vom Zweitsystem) nur einmal vorliegt, muss an beide Rechner dieselbe Signaturerstellungseinheit (siehe 5.1.1) angeschlossen werden können.

5.2 Software

5.2.1 Betriebssysteme

Alle in 5.1 genannten Rechner müssen mit geeigneten Betriebssystemen ausgestattet sein, die im Hinblick auf die IT-Sicherheit gut erforscht sind. Die Rechner können auch mit unterschiedlichen Betriebssystemen ausgestattet sein.

Für die Rechner 5.1.4 und 5.1.5 müssen Betriebssysteme eingesetzt werden, welche eine besonders hohe Ausfallssicherheit, eine gut entwickelte Berechtigungsverwaltung sowie die leichte Überwachbarkeit der vitalen Systemparameter durch das Rechenzentrumspersonal gewährleisten. Die weitere Wartung des Betriebssystems über zumindest die nächsten drei Jahre muss gewährleistet sein.

Als Betriebssystem kann etwa ein System der Unix-Familie eingesetzt werden.

5.2.2 CAPI

Die Signaturerstellungshardware muss ein CAPI nach dem Standard PKCS#11 aufweisen (einschließlich Programmbibliotheken für die Betriebssysteme der Rechner 5.1.2, 5.1.3 und 5.1.4).

5.2.3 Software zur Erstellung von Zertifikaten

Die Software zur Erstellung von Zertifikaten wird auf dem Rechner 5.1.2 eingesetzt und muss mit der Signaturerstellungshardware kompatibel sein. Insbesondere sollte der Zugriff auf kryptographische Operationen dem Standard PKCS#11 entsprechen.

Die Software muss gewährleisten, dass Zertifikate nur dann signiert werden, wenn zwei berechtigte Personen gemeinsam diese Signatur ausgelöst haben.

Die Software muss Zertifikate nach X.509 v3 unterstützen. Alle in RFC 2459 beschriebenen Extensions – insbesondere jene, die in Kapitel 7.1 des Entwurfs des Certification Practice Statements (Anhang A) erwähnt werden – müssen unterstützt werden.

Die Software muss auch die Signaturen von Zertifikaten und von PKCS#10-Anträgen prüfen können.

5.2.4 Datenbank-Client

Der Datenbank-Client wird auf den Rechnern 5.1.3 sowie 5.1.4 eingesetzt und dient dem Zugriff auf die Datenbank, die sich auf dem Rechner 5.1.4 befindet. Er muss mit dem Datenbank-Server 5.2.5 kompatibel sein.

Die Kommunikation zwischen Client und Server darf nur nach gegenseitiger Authentifizierung und nur verschlüsselt geschehen, wobei das Protokoll SSL oder TLS einzusetzen ist. Dabei dient der Rechner 5.1.3 als Client und der Rechner 5.1.4 als Server. Beide Geräte akzeptieren bei der Authentifizierung nur das Zertifikat des jeweils anderen.

5.2.5 Datenbank-Server

Der Datenbank-Server wird auf dem Rechner 5.1.4 eingesetzt. Die Datenbank dient zur Speicherung der in die Verzeichnisse gemäß § 13 Abs. 3 SigG eingetragenen Informationen. Die Realisierung könnte etwa mittels LDAP geschehen, wobei die Informationen gemäß RFC 2587 dargestellt werden. Im Falle einer Realisierung mittels LDAP könnten die Daten auf die LDAP-Server 5.1.5 repliziert werden.

Die Kommunikation zwischen Client und Server darf nur nach gegenseitiger Authentifizierung und nur verschlüsselt geschehen, wobei das Protokoll SSL oder TLS eingesetzt werden soll. Dabei dient der Rechner 5.1.3 als Client und der Rechner 5.1.4 als Server. Beide Geräte akzeptieren bei der Authentifizierung nur das Zertifikat des jeweils anderen.

5.2.6 Software zur Erstellung von Widerrufslisten

Die von der Telekom-Control-Kommission ausgestellte Widerrufsliste, die sich in der Datenbank auf dem Rechner 5.1.4 befindet, muss in regelmäßigen Abständen von einigen Stunden sowie bei jedem durchgeführten Widerruf aktualisiert, neu signiert, in die Datenbank zurückgeschrieben und auf den Servern 5.1.5 publiziert werden. Dies könnte etwa mit Hilfe eines periodisch ausgeführten Shell-Scripts geschehen. Die Software zur Erstellung von Widerrufslisten muss einerseits auf das Datenbanksystem, andererseits auf die Signaturerstellungshardware abgestimmt werden. Insbesondere sollte der Zugriff auf kryptographische Operationen dem Standard PKCS#11 entsprechen.

Die Software muss Widerrufslisten nach X.509 v2 unterstützen. Alle in RFC 2459 beschriebenen Extensions – insbesondere jene, die in Kapitel 7.2 des Entwurfs des Certification Practice Statements (Anhang A) erwähnt werden – müssen unterstützt werden.

Die Software muss auch Signaturen von Widerrufslisten prüfen können.

5.2.7 HTTP-Server

Der HTTP-Server wird auf den Rechnern 5.1.5 eingesetzt. Auf den HTTP-Server sollte

a) ohne Authentifikation (alle Inhalte außer Widerrufsdienst),

b) mit Server-Authentifikation (alle Inhalte außer Widerrufsdienst) und

c) mit Client- und Server-Authentifikation (Widerrufsdienst)

zugegriffen werden können. Die Authentifikation soll sowohl mit SSL, Version 3.0, als auch mit TLS, Version 1.0, möglich sein. Auch für die Server-Software gelten die in 5.1.5 beschriebenen Anforderungen. Falls die Rechner 5.1.5 mit kryptographischen Koprozessoren bestückt sind, müssen diese durch die Server-Software unterstützt werden.

Als HTTP-Server soll ein Produkt eingesetzt werden, welches im Hinblick auf die IT-Sicherheit gut bekannt ist. Bei entsprechender Eignung kann auch ein Open-Source-Produkt eingesetzt werden.

5.2.8 LDAP-Server

Der LDAP-Server wird auf den Rechnern 5.1.5 eingesetzt. Falls der LDAP-Server auch auf dem Rechner 5.1.4 eingesetzt wird, sollte er Replikation unterstützen. Der LDAP-Server ist so zu konfigurieren, dass beliebige Namen – also ohne vorgegebene Wurzel – erfasst werden können. Die vom LDAP-Server gelieferten Informationen sind nach den in RFC 2587 formulierten Empfehlungen darzustellen. Auf den LDAP-Server sollte sowohl mit als auch ohne Server-Authentifizierung (SSL, Version 3.0, und TLS, Version 1.0) zugegriffen werden können. Auch für die Server-Software gelten die in 5.1.5 beschriebenen Anforderungen. Falls die Rechner 5.1.5 mit kryptographischen Koprozessoren bestückt sind, müssen diese durch die Server-Software unterstützt werden.

Für den Datenbank-Server gelten auch dann die unter 5.2.5 beschriebenen Anforderungen (insbesondere Client- und Server-Authentifizierung), wenn er als LDAP-Server realisiert wird.

5.2.9 NTP-Server

Auf dem Rechner 5.1.4 ist ein primärer, auf den Rechnern 5.1.5 ein sekundärer NTP-Server zu installieren. Der primäre Server ist mit dem in 5.1.4 erwähnten Zeitgeber abzugleichen. Die Server-Software muss die in der aktuellen Version des Internet Drafts „Public-Key Cryptography for the Network Time Protocol“ <draft-ietf-stime-ntpauth-??.txt> vorgeschlagenen Authentifikationsverfahren unterstützen. Der primäre Time-Server muss in regelmäßigen Abständen mit dem Zeitgeber des Rechners 5.1.4 abgeglichen werden und der sekundäre mit dem primären. Auch für die Server-Software gelten die in 5.1.5 beschriebenen Anforderungen. Insbesondere darf eine hohe Zugriffshäufigkeit niemals dazu führen, dass die von den Rechnern 5.1.5 via Internet abgerufene Zeit um mehr als eine Minute von der tatsächlichen Zeit abweicht. Falls die Rechner 5.1.5 mit kryptographischen Koprozessoren bestückt sind, müssen diese durch die Server-Software unterstützt werden.

5.2.10 SSH-Server

Die Wartung der auf den Geräten 5.1.5 gespeicherten Programme und Daten geschieht teilweise mittels Secure Shell (SSH). Deshalb ist auf diesen Geräten ein SSH-Server zu installieren, der das Protokoll SSH 2 gemäß der Spezifikation in den relevanten Internet Drafts unterstützt.

Der SSH-Server ist so zu konfigurieren, dass die Authentifikation nur mittels X.509-Zertifikaten möglich ist. Ein direkter Zugang als Root soll ausgeschlossen sein.

5.2.11 Software zur Überwachung des Zeitgebers

Um den Zeitgeber auf dem Rechner 5.1.4 vor dem Empfang von Störsignalen zu schützen, müssen die Rechner 5.1.5 laufend die vom Rechner 5.1.4 mitgeteilte Zeit mit den Zeitangaben mehrerer vertrauenswürdiger NTP-Server im Internet vergleichen und auf ihre Plausibilität hin untersuchen. Bei einer Diskrepanz von mehr als 30 Sekunden (dies könnte beispielsweise auf absichtlich abgestrahlte Störsignale zurückzuführen sein) muss unverzüglich ein Alarm ausgelöst werden. In diesem Fall ist der Zeitgeber bis zur Ausschaltung der Störsignalquelle zu deaktivieren, wobei die Systemzeit des Rechners 5.1.5 vom Störsignal unbeeinträchtigt weiterlaufen muss. Für die Deaktivierung muss auch der Rechner 5.1.4 mit Software ausgestattet sein, die es ermöglicht, den Zeitgeber von den Rechnern 5.1.5 aus zu deaktivieren. Jede Aktivierung und Deaktivierung des Zeitgebers muss auf dem Rechner 5.1.4 protokolliert werden.

5.2.12 Software zur Kommunikation des Widerrufsdienstes mit dem Rechner 5.1.4

Es sind ein exemplarisches Webformular und ein für die Rechner 5.1.5 vorgesehenes Script zu erstellen, mit denen der Widerrufsdienst (Call-Center) nach Client- und Server-Authentifikation sowie nach Bekanntgabe des mit einem Zertifikatsinhaber vereinbarten Codes einen Widerruf an die Rechner 5.1.5 übermitteln kann. Die Rechner 5.1.5 haben ausschließlich die Formularinhalte an den Rechner 5.1.4 weiterzuleiten. Der Rechner 5.1.4 muss die Richtigkeit des Codes überprüfen, gegebenenfalls den Widerruf unter Verwendung der Software 5.2.6 durchführen.

5.2.13 Software für die sichere Signatur der Liste der nicht X.509-kompatiblen Anbieter

Die Liste wird z. B. im folgenden Dokumentenformat erstellt:

– Zeichensatz ISO 8859-1

– Von diesem Zeichensatz werden ausschließlich sichtbare Zeichen, das Leerzeichen (Code 32), das CR-Zeichen (Code 13) und das LF-Zeichen (Code 10) verwendet. Andere Steuerzeichen sind nicht zulässig.

– Die Kombination CR und LF wird als Codierung für das Zeilenende verwendet. Leerzeichen am Zeilenende sind nicht zulässig. Die Zeilenlänge beträgt maximal 80 Zeichen.

Alternativ dazu kann auch ein anderes textbasierendes Dokumentenformat angegeben werden. Das Format muss den Anforderungen des § 7 Abs. 2 SigV entsprechen. Es muss sich um ein Format handeln, welches von einer breiten Benutzergruppe lesbar ist, ohne dass diese für die Darstellung eine besondere Software installieren müssen.

Für die Signaturerstellung ist eine Software bereitzustellen, welche die Einhaltung der oben beschriebenen Regeln überprüfen und ein Dokument im beschriebenen Dokumentenformat vollständig und in einer Schriftart (Font), die die einzelnen Zeichen unmissverständlich wiedergibt, am Bildschirm anzeigen kann.

Die Signaturerstellung soll nur zwei Personen gemeinsam möglich sein.

5.2.14 Software zur sicheren Signaturprüfung

Es ist eine unter Windows NT lauffähige Software anzubieten, mit welcher die Signaturen von Zertifikaten, von Widerrufslisten, der Liste der nicht X.509-kompatiblen Anbieter und sichere Signaturen des Dokumentationssystems geprüft werden können.

5.2.15 Dokumentationssystem

Es ist ein System vorzusehen, mit dem das Archiv gemäß Punkt 4.6 des Entwurfs des Certification Practice Statement (Anlage A) realisiert werden kann.

Das System muss die Speicherung beliebiger Daten (z. B. in Protokolle in dem in 5.2.13 beschriebenen Dokumentenformat, Systemprotokolle, ...) unterstützen. Die in das System aufgenommenen Daten sollen mit einem sicheren Zeitstempel gegen nachträgliche Veränderung geschützt werden. Dafür kann der NTP-Server 5.2.9 herangezogen werden. Die nachträgliche Löschung von Daten soll nicht unerkannt möglich sein (z. B. durch Zeitstempelung von Inhaltsverzeichnissen).

Die Software wird auf einem Server im Serverraum der Telekom-Control GmbH (außerhalb des sicheren Raums, aber mit eingeschränkter Zutrittsberechtigung) installiert. Als Betriebssysteme kommen Windows 2000 und Linux in Frage. Wenn das angebotene Dokumentationssystem diese Betriebssysteme nicht unterstützt, wäre zusätzlich ein Rechner und das entsprechende Betriebssystem anzubieten.

5.3 Dokumentation, Sicherheitskonzepte, Schulung

Die produktspezifische Dokumentation ist hier nicht extra angefügt, sondern ist jeweils zu den Komponenten in 5.1 und 5.2 zu liefern.

5.3.1 Betriebshandbuch Zertifizierung

Für den gesamten Ablauf der Erstellung von Zertifikaten ist ein dem Certification Practice Statement der Aufsichtsstelle entsprechendes Betriebshandbuch in deutscher Sprache zu erstellen, welches insbesondere die folgenden Themen abdeckt:

– Sicherstellung des Vier-Augen-Prinzips, Vorgangsweise bei der Vergabe von Benutzerberechtigungen und der Entziehung der Benutzerberechtigung, Lebenszyklus aller Authentifizierungsdaten (Passwörter, PIN-Codes).

– Ablauf der Erstellung eines Zertifikates

– Einbringen des Zertifikates in die X.509v3-Datenbank

– Allfällig notwendige regelmäßige Überprüfungen der eingesetzten Komponenten

5.3.2 Betriebshandbuch Widerrufsdienst (Telekom-Control)

Für die von Telekom-Control-Mitarbeitern wahrzunehmenden Aufgaben beim Widerrufsdienst ist ein dem Certification Practice Statement der Aufsichtsstelle entsprechendes Betriebshandbuch in deutscher Sprache zu erstellen, welches insbesondere die folgenden Themen abdeckt:

– Verwaltung der Hashwerte für den automatisierten Widerruf

– Sicherstellung des Vier-Augen-Prinzips beim Widerruf durch die Telekom-Control, Vorgangsweise bei der Vergabe von Benutzerberechtigungen und der Entziehung der Benutzerberechtigung, Lebenszyklus aller Authentifizierungsdaten (Passwörter, PIN-Codes).

– Ablauf der Durchführung eines Widerrufs

– Allfällig notwendige regelmäßige Überprüfungen der eingesetzten Komponenten

5.3.3 Betriebshandbuch Widerrufsdienst (Call-Center)

Für die vom Call-Center wahrzunehmenden Aufgaben beim Widerrufsdienst ist ein dem Certification Practice Statement der Aufsichtsstelle entsprechendes Betriebshandbuch in deutscher Sprache zu erstellen, welches insbesondere die folgenden Themen abdeckt:

– Aufbau einer gesicherten Verbindung zum Rechenzentrum

– Ablauf der Durchführung eines Widerrufs

5.3.4 Betriebshandbuch für das Rechenzentrumspersonal

Für die vom Rechenzentrum wahrzunehmenden Aufgaben ist ein dem Certification Practice Statement der Aufsichtsstelle entsprechendes Betriebshandbuch in deutscher Sprache zu erstellen, welches insbesondere die folgenden Themen abdeckt:

– Detaillierte Angaben darüber, welche Bestandteile der Hardware und welche Prozesse vom Rechenzentrumspersonal überwacht werden müssen.

– Detaillierte Angaben über mögliche Störfälle und Fehlermeldungen und die jeweils zu ergreifenden Maßnahmen. Dabei ist unter Berücksichtigung der Zugriffsberechtigung festzulegen, wann das Rechenzentrumspersonal selbst einzuschreiten hat und wann es Systemadministratoren der Telekom-Control GmbH verständigen muss.

5.3.5 Betriebshandbuch Rechenzentrum (Telekom-Control)

Für die von Telekom-Control-Mitarbeitern wahrzunehmenden Aufgaben bei den im Rechenzentrum untergebrachten Komponenten ist ein dem Certification Practice Statement der Aufsichtsstelle entsprechendes Betriebshandbuch in deutscher Sprache zu erstellen, welches insbesondere die folgenden Themen abdeckt:

– Konfiguration der Systeme (Hardware/Betriebssystem/Software)

– Detaillierte Angaben zur Konfiguration der Benutzerverwaltung und Zugriffsberechtigung auf die einzelnen Verzeichnisse, Dateien etc. Dazu ist das Certification Practice Statement der Aufsichtsstelle heranzuziehen.

– Detaillierte Angaben darüber, welche regelmäßigen Überprüfungen von Mitarbeitern der Telekom-Control durchzuführen sind.

– Detaillierte Angaben über mögliche Störfälle und Fehlermeldungen und die jeweils zu ergreifenden Maßnahmen, soweit diese nicht vom Rechenzentrumspersonal ergriffen werden (siehe 5.3.4).

5.3.6 Schulung

Nach Implementierung des Gesamtsystem sind die Mitarbeiter der Telekom-Control GmbH auf das System einzuschulen.

Es ist eine zumindest eintägige Schulung für CA-Operatoren und Identitätsprüfer im Sinne des Rollenmodells (Ausstellung von Zertifikaten, Widerruf) und eine zumindest dreitägige Schulung für Systemadministratoren vorzusehen.

5.4 Wartung

Der Bieter hat gemäß den Vertragsbestimmungen (Anhang 5, Punkt 6) Wartungsleistungen anzubieten. Diese Leistungen haben folgenden Kriterien zu entsprechen:

a) Hinsichtlich der Komponenten des Zertifizierungsdienstes (= den in den Räumlichkeiten der Telekom-Control GmbH untergebrachten Komponenten) gewährleistet der Auftragnehmer:

– Entgegennahme der Störungsmeldungen:
  werktags (Mo-Fr) zwischen 08:00 und 18:00 Uhr.

– Reaktionszeit bis zum Eintreffen vor Ort:
  4 Stunden,
  bei Einlangen der Störungsmeldung nach 16:00:
  Eintreffen spätestens am nächsten Werktag 10:00

– Maximale Ausfallszeit (Call-to-Repair):
  24 Stunden (Samstage, Sonntag und Feiertage werden nicht eingerechnet)

b) Hinsichtlich der Komponenten des Verzeichnis- und Widerrufsdienstes (= den im Rechenzentrum untergebrachten Komponenten) gewährleistet der Auftragnehmer:

– Entgegennahme der Störungsmeldungen:
  an allen Tagen rund um die Uhr

– Reaktionszeit bis zum Eintreffen vor Ort:
  2 Stunden (an allen Tagen rund um die Uhr)

– Maximale Ausfallszeit (Call-to-Repair):
  4 Stunden (an allen Tagen rund um die Uhr)

– Verfügbarkeit der Systeme über das Jahr gerechnet:
  >99,9%

5.5 Zeitrahmen für Implementierung und Abnahme

Der vom Bieter angegebene Zeitrahmen für die Implementierung und Abnahme bildet ein wichtiges Kriterium für die Wahl des Angebotes für den Zuschlag (siehe Punkt 2.13.5). Der Zeitplan ist in Anlage 3 zu beschreiben. Die Implementierung und Abnahme muss aber jedenfalls bis zum 30.06.2001 abgeschlossen sein.

6. Übersicht über die Beilagen

Anhang A: Entwurf des Certification Practice Statement der Aufsichtsstelle

Anlage 1: Deckblatt

Anlage 2: Angaben zum Bieter

Anlage 3: Fragenkataloge

Anlage 4: Preisraster

Anlage 5: Vertrag

Anhang A

Sicherheits- und Zertifizierungskonzept – Certification Practice Statement – Entwurf

Der Entwurf des Certification Practice Statement bildet einen integralen Bestandteil der Ausschreibungsunterlagen.

Mit der ausgeschriebenen Public-Key-Infrastruktur müssen die im Entwurf des Certification Practice Statement enthaltenen Anforderungen umgesetzt werden können.

Der Entwurf ist aber vorerst nur für Zwecke der Ausschreibung verbindlich. Eine formelle Beschlussfassung über den Entwurf ist noch nicht erfolgt. An einigen Stellen wird das Certification Practice Statement nach Abschluss der Ausschreibung überarbeitet und konkretisiert werden. 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 0.30

31.10.2000

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

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 0.30, 31.10.2000.

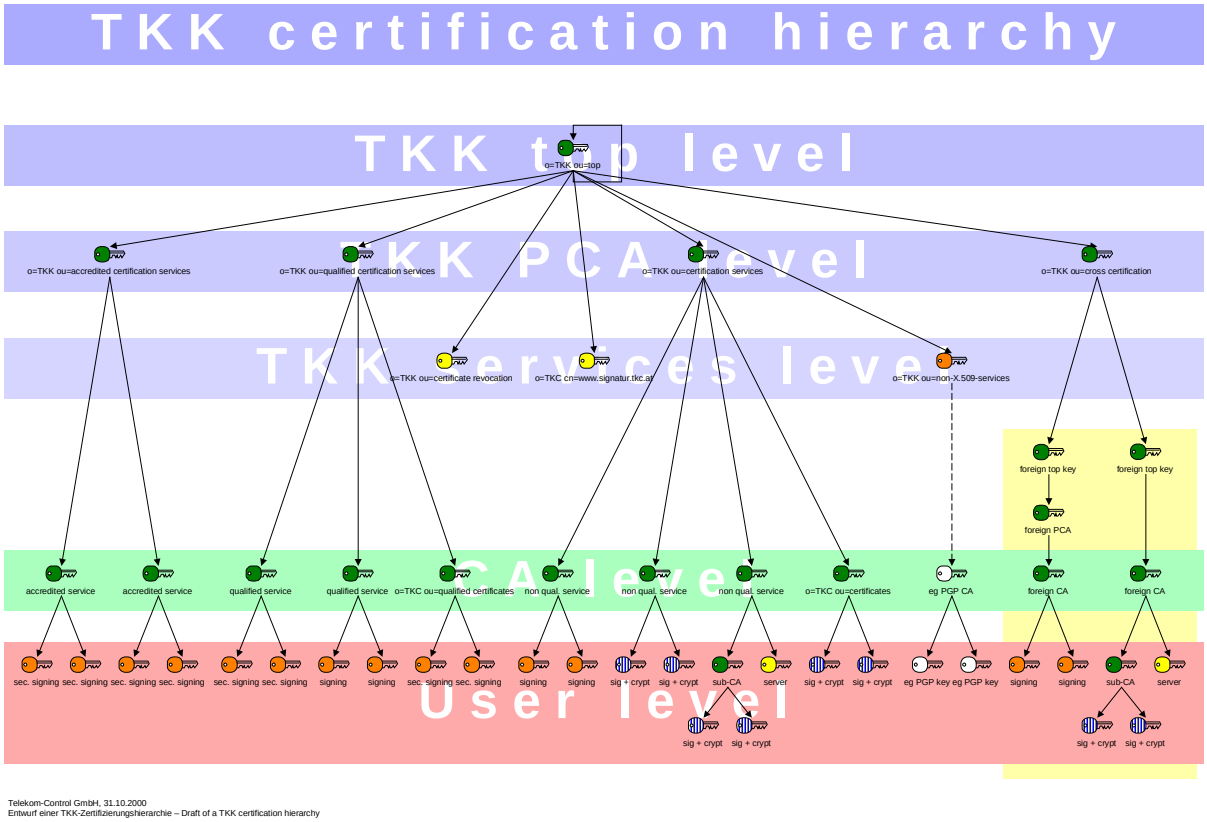
Dieses Dokument fasst die wesentlichsten Inhalte des Sicherheits- und Zertifizierungskonzepts der Aufsichtsstelle für elektronische Signaturen in Form eines Certification Practice Statement (CPS) zusammen. Die Gliederung des CPS erfolgt nach dem Muster des Standards RFC 2527 (Chokhani/Ford, Internet 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.

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.

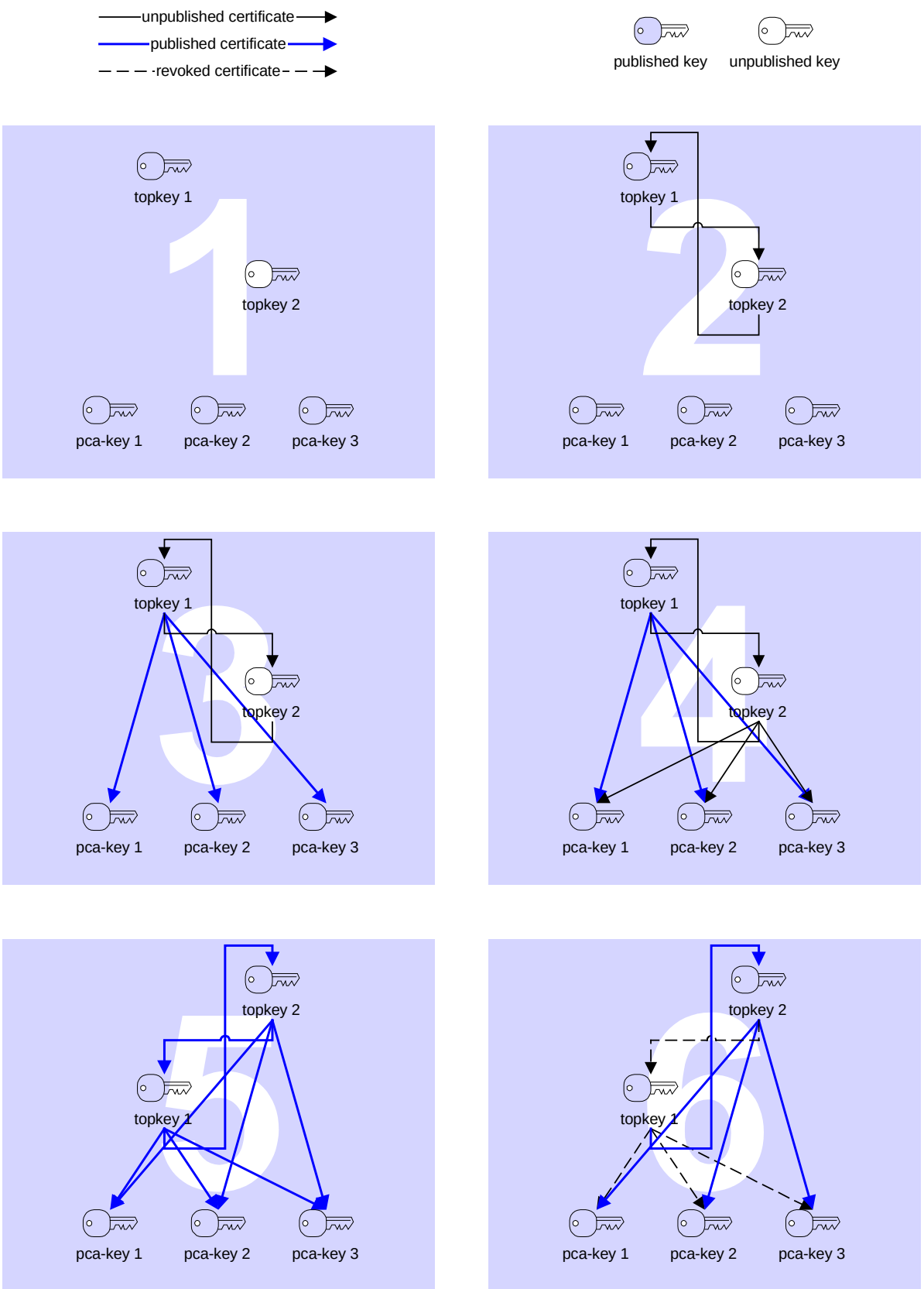
4.7 Zweitsysteme und Austausch von Schlüsseln

§ 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.

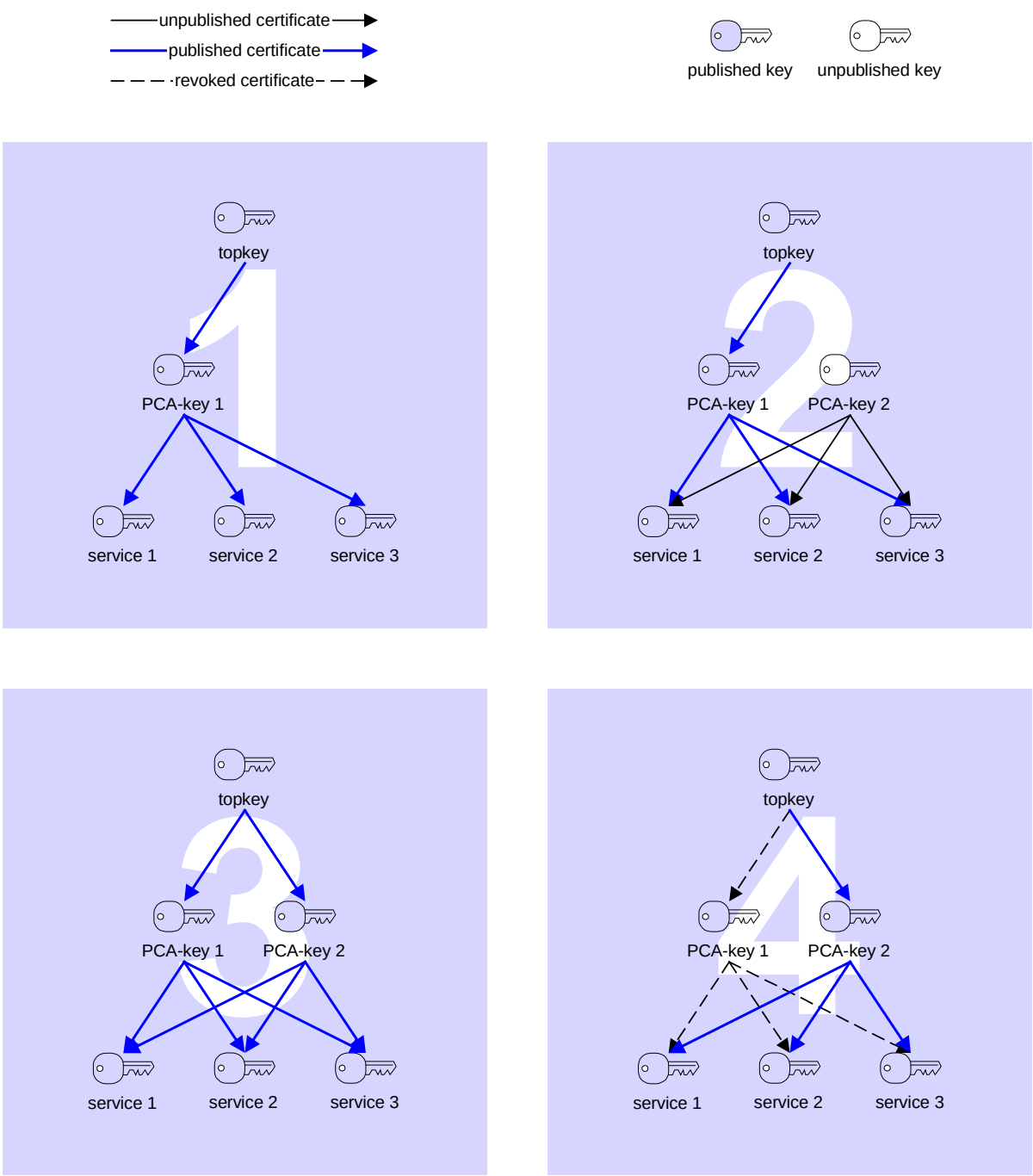
JournalistInnen und Medien werden ersucht, sich vor der Berichterstattung über einen angeblichen Wechsel des TOP-Schlüssels der Aufsichtsstelle sorgsam zu vergewissern, dass die Information tatsächlich von der Aufsichtsstelle stammt und nicht von einer Person, die sich in betrügerischer Absicht als die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

PCA-key replacement



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 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. 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.

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

<Die Aufnahme von Zertifikatserweiterungen, mit welchen die Zertifikate der Aufsichtsstelle als qualifizierte Zertifikate gekennzeichnet werden können, erfolgt dann, wenn ein entsprechender Standard vorliegt. Die derzeitigen ETSI/IETF-Drafts erlauben eine Kennzeichnung als qualifiziertes Zertifikat nur dann, wenn das Zertifikat einem Signator ausgestellt wird.>

7.1.3 ASN.1 Object Identifier für Algorithmen

Bei allen von der Aufsichtsstelle ausgestellten Zertifikaten enthalten die Felder signatureAlgorithm und signature den ASN.1 Object Identifier sha-1WithRSAEncryption gemäß RFC 2459, Abschnitt 7.2.1. Das Feld algorithm 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).

Anlage 1: Deckblatt

Auftraggeber: Telekom-Control GmbH

Angebotsgegenstand: Publik-Key-Infrastruktur

Bieter (Firma):

Firmenbuchnummer:

Anschrift:

Telefon:

Telefax:

E-Mail:

UStID:

Zustellbevollmächtigter:

Gesamtpreis exkl. USt
(Anlage 4/Punkt 6) ATS/Euro

O Bei diesem Angebot handelt es sich um das Hauptangebot.

O Der Bieter legt weiters folgende Alternativangebote/Variantenangebote separat vor:
Beschreibung der Alternativangebote/Variantenangebote:

O Bei diesem Angebot handelt es sich um ein Alternativangebot/Variantenangebot.
Beschreibung der wesentlichen Unterschiede zum Hauptangebot:

---

firmenmäßige Fertigung durch den Bieter

Anlage 2: Angaben zum Bieter

Bezeichnung des Bieters:

Für die gegenständliche Ausschreibung ist seitens des Bieters verantwortlich:
Vorname und Familienname:
Stellung im Unternehmen:
Telefon:
Fax:
E-Mail:

Vertreter für technische Rückfragen:
Vorname und Familienname:
Stellung im Unternehmen:
Telefon:
Fax:
E-Mail:

Vertreter für kaufmännische Rückfragen:
Vorname und Familienname:
Stellung im Unternehmen:
Telefon:
Fax:
E-Mail:

Liegt eine Bietergemeinschaft vor? Wenn ja: Aus welchen Unternehmen setzt sich die Bietergemeinschaft zusammen?

O Bietergemeinschaft liegt vor O Bietergemeinschaft liegt nicht vor

Namen der einzelnen Unternehmen:

Beauftragt der Bieter Subunternehmer? Wenn ja: Welche Subunternehmer erbringen welche Leistung? Wie viel Prozent des Gesamtwertes erbringt der jeweilige Subunternehmer?

O Subunternehmer werden beauftragt O Subunternehmer werden nicht beauftragt.

Namen der Subunternehmer	Leistung	%

1 Betriebswirtschaftliche Kennzahlen und Angaben zur technischen Leistungsfähigkeit

Bei Bietergemeinschaften ist dieser Abschnitt für jedes einzelne Unternehmen, bei der Beauftragung von Subunternehmern für jedes einzelne Subunternehmen auszufüllen. Tritt nur ein Unternehmen als Bieter auf, ist der Abschnitt nur einmal auszufüllen.

Unternehmen (Firma):

Firmenbuchnummer:

Anschrift:

Telefon:

Telefax:

E-Mail:

UStID:

Gesamtumsatz der letzten Jahre exklusive Umsatzsteuer

1997: _____ 1998: _____ 1999: _____ 2000 (falls verfügbar): _____

Gesamtumsatz der letzten Jahre bezüglich jener Leistungen, die Gegenstand der Ausschreibung sind (exkl. USt)

1997: _____ 1998: _____ 1999: _____ 2000 (falls verfügbar): _____

Seit wann arbeitet das Unternehmen auf dem Gebiet der ausgeschriebenen Leistung?

Gründungsjahr des Unternehmens

Anzahl der Mitarbeiter in den letzten drei Jahren international

Ende 1998: _____ Ende 1999: _____ Ende 2000: _____

Anzahl der Mitarbeiter in den letzten drei Jahren in Österreich

Ende 1998: _____ Ende 1999: _____ Ende 2000: _____

Im Folgenden sind jeweils nur Angaben zur technischen Leistungsfähigkeit des Bewerbers zu machen, soweit dies auf das jeweilige Unternehmen zutrifft. Soferne die Fragen auf andere ARGE-Mitglieder in einer Bietergemeinschaft oder auf Subunternehmer zutreffen, sind die Fragen bei dem jeweils anderen Unternehmen zu beantworten.

Angaben zu der dem Unternehmen zur Verfügung stehenden technischen Ausrüstung, den Maßnahmen des Unternehmers zur Gewährleistung der Qualität und den Untersuchungs- und Forschungsmöglichkeiten

Angaben zu den vom Unternehmen produzierten kryptographischen Modulen (z. B. Chipkarten) und Hardwareschnittstellen (z. B. Chipkartenleser)

Angaben zu der vom Unternehmen produzierten PKI-Software

Angaben zu den vom Unternehmen produzierten LDAP-Servern

Angaben zu den Erfahrungen mit der Evaluierung von kryptographischen Modulen und PKI-Software, über die das Unternehmen verfügt.

Angaben über die technische Leitung oder die technischen Stellen, unabhängig davon, ob diese dem Unternehmen angeschlossen sind oder nicht, und zwar insbesondere über diejenigen, die mit der Qualitätskontrolle beauftragt sind.

In welchem Land findet die Entwicklung der Produkte hauptsächlich statt?

Wie viele Personen des Unternehmens sind mit der Entwicklung kryptographischer Module beschäftigt?

Wie viele Personen des Unternehmens sind mit der Entwicklung von PKI-Software beschäftigt?

Wie viele Personen des Unternehmens sind mit der Entwicklung von LDAP-Servern beschäftigt?

Wie viele Personen des Unternehmens sind mit der Integration von Systemkomponenten, Consulting etc. beschäftigt?

_____ (insgesamt) _____ (Integration von PKI-Lösungen)

Das Unternehmen ist in Österreich an wie vielen Standorten vertreten, die als Servicestützpunkte arbeiten?

Das Unternehmen ist in der übrigen Welt an wie vielen Standorten vertreten, die als Servicestützpunkte arbeiten?

2 Referenzen

Der Bieter hat eine Liste von bis zu fünf Referenzen bei Kunden mit ähnlichem Aufgabenbereich anzugeben, bei denen seine Produkte eingesetzt sind bzw. für welche er eine Public-Key-Infrastruktur realisiert hat.

Dieser Abschnitt ist jeweils zu vervielfältigen. Die Reihung der Referenzen ist nach ihrer Wichtigkeit und Aussagekraft so vorzunehmen, dass die wichtigste zuerst gereiht wird.

Fortlaufende Nummer:

Projektname:

Auftraggeber:

Ansprechpartner beim Auftraggeber:

Telefon/E-Mail des Ansprechpartners:

Projektumfang in Mio. ATS:

Projektbeginn (Jahr/ Monat):

Projektende (Jahr/ Monat):

Kurzbeschreibung (eventuell Grafik beilegen)

Verwendete Komponenten (insbesondere kryptographische Module/PKI-Software)

3 Bietererklärung

Der Bieter bestätigt die Richtigkeit der oben gemachten Angaben und erklärt weiters:

– dass er die Ausschreibung und die in ihr enthaltenen bzw. ihr zugrundeliegenden Auflagen, Bedingungen, Richtlinien und Rechtsvorschriften akzeptiert;

– dass er keine Vereinbarung über die Preisbildung und andere für die Telekom-Control GmbH nachteilige, gegen Rechtsvorschriften, die guten Sitten oder gegen den Grundsatz des Wettbewerbs verstoßende Abreden mit anderen Unternehmen getroffen hat und sich bewusst ist, dass eine falsche Abgabe dieser Erklärung seinen Ausschluss vom Vergabeverfahren zur Folge hat;

– dass er zur Durchführung der angebotenen Lieferungen und Leistungen nach den gesetzlichen Bestimmungen seines Herkunftslandes und Österreichs berechtigt ist und bei der Durchführung die einschlägigen gesetzlichen Bestimmungen beachten wird;

– dass er über die entsprechende wirtschaftliche, finanzielle und technische Leistungsfähigkeit verfügt, um die geforderten Lieferungen und Leistungen vertragsgemäß zu erbringen;

– dass er bei der Durchführung des Leistungsvertrages auf die Beschäftigung von Personen im Ausbildungsverhältnis bedacht nimmt;

– dass er die Ausschreibungsunterlagen, insbesondere hinsichtlich der technischen Beschreibungen, prüfen wird und allfällige Berichtigungen der Telekom-Control GmbH mitteilen wird;

– dass die Angebote unter dem Gesichtspunkt der vollen Funktionsfähigkeit der angebotenen Lieferungen und Leistungen erstellt wurden.

Der Bieter erklärt weiters, dass er in Österreich nicht als Zertifizierungsdiensteanbieter tätig ist und für die nächsten drei Jahre auch nicht beabsichtigt, eine Tätigkeit als Zertifizierungsdiensteanbieter im Sinne des § 6 SigG aufzunehmen.

(Beizufügen sind auch die in Punkt 2.5.3 der Ausschreibungsunterlagen geforderten Nachweise. Bei Bietergemeinschaften ist von allen Mitgliedern zusätzlich eine firmenmäßig gezeichnete Erklärung gemäß Punkt 2.9 der Ausschreibungsunterlagen beizufügen.)

---

firmenmäßige Fertigung durch den Bieter

Anlage 3 Fragenkataloge

Die Ausschreibungsunterlagen werden auch in elektronischer Form im Format Microsoft Word 97 (siehe Punkt 2.4.3) zur Verfügung gestellt, um die Beantwortung zu erleichtern.

Die Fragen sind prinzipiell auf den Fragebögen zu beantworten. Handschriftliche Einträge können nicht berücksichtigt werden. Für umfangreichere Antworten ist dem Angebot eine Beilage beizufügen. Diese ist mit „Beilage zu Fragenkatalog Pkt. X.X.X“ zu kennzeichnen. Weiters sind alle Beilagen, die sich auf den Fragenkatalog beziehen mit einer fortlaufenden Nummern zu versehen. Im Fragebogen selbst ist unter dem betreffenden Punkt der Hinweis auf die Beilage und deren Nummer einzutragen.

Werbematerialien, Standard- und Verkaufsunterlagen und Ähnliches sind nur insofern zulässig, als diese genau Produktinformationen enthalten (technische Daten, Funktionsbeschreibungen u. ä.)

Fragen, die sich produktübergreifend beantworten lassen (z. B.: Hardware, DB-System) müssen nur einmal beantwortet werden. Es ist aber bei den zugehörigen Punkten des Fragenkataloges ein Hinweis auf jenen Punkt einzutragen, unter dem die Fragen beantwortet wurden.

Hinweise auf Internetseiten und ähnliche Informationsquellen außerhalb der Angebotsunterlagen werden nicht berücksichtigt. Es gelten nur die in den Angebotsunterlagen enthaltene Informationen.

Bezeichnung des Bieters (Firma):

1. Hardware

1.1 Signaturerstellungshardware

Hersteller, Marke und Version des Produkts:

Welche Technologie wird für die Signaturerstellungseinheiten verwendet?

Wie wird gewährleistet, dass private Schlüssel in der Signaturerstellungseinheit erzeugt werden und diese niemals verlassen?

Wie viele Signaturerstellungseinheiten werden eingesetzt?

Wie viele verschiedene Schlüsselpaare kann eine Signaturerstellungseinheit verwalten?

Welche der in PKCS#11 spezifizierten Operationen werden von der Signaturerstellungseinheit hardwaremäßig unterstützt?

Nach welchen Normen, Evaluations- und Sicherheitsstufen ist das Produkt evaluiert worden?

Welche kryptographischen Verfahren werden unterstützt?

Wie groß ist die maximale Länge der von der Signaturerstellungseinheit verwalteten RSA-Schlüssel?

Werden Konzepte zur Schlüsselhinterlegung (Key escrow) oder zur Schlüsselwiederherstellung (Key recovery) verwendet? Können diese unterbunden werden?

Mit welchen Verfahren werden Zufallselemente der Schlüssel erzeugt?

Mit welchen Verfahren werden private Schlüssel aktiviert?

Beschreiben Sie die Initialisierungssequenz!

Welche Hashverfahren werden unterstützt?

Welche Padding-Verfahren werden bei kryptographischen Operationen verwendet?

Wie wird das Vieraugenprinzip verwirklicht?

Wie lange bleiben die Schlüsselpaare gespeichert, wenn die Signaturerstellungseinheit an keine Energiequelle angeschlossen ist?

Für welchen Zeitraum wird die volle Funktionsfähigkeit des Produkts garantiert?

Wie lange dauert im Mittel die Erzeugung eines RSA-Schlüsselpaares bei einer Schlüssellänge von 1024 Bit?

Bieten Sie standardisierte Abnahmeprozeduren zur Qualitätssicherung des angebotenen Produktes an?

Welche Arten von Tests werden dabei durchgeführt?

1.2 Notebook im Tresor der Aufsichtsstelle/Notebook für das Zweitsystem

Hersteller, Marke und Version des Produkts:

Abmessungen des Gerätes (Breite, Höhe, Tiefe):

Gesamtgewicht:

Welcher Prozessor (Marke, Taktfrequenz) wird eingesetzt?

Wie groß ist die Kapazität des Arbeitsspeichers (RAM)?

Maximale Erweiterbarkeit des Arbeitsspeichers:

Falls ECC-RAM eingesetzt wird, beschreiben Sie die verwendete Technologie (SEC-DED, „chipkill-correct“ usw.)!

Wie groß ist die Speicherkapazität der Festplatte(n)?

Welche Art von Festplatten-Controller wird verwendet?

Durchschnittliche Zugriffszeit der Festplatte(n):

Durchschnittliche Latenzzeit der Festplatte(n):

Enthält das Gerät ein Diskettenlaufwerk?

Enthält das Gerät ein CD-Laufwerk?

Wie viele PCMCIA-Schächte (Type II, Type III) sind vorhanden?

Wie funktioniert die Prozessorkühlung?

Welche Technologien werden beim Power-Management eingesetzt?

Welche Akkumulatoren werden eingesetzt (Technologie, Kapazität)?

Wie lange kann das Notebook bei voll aufgeladenem Akku ohne Netzteil betrieben werden?

Wie groß ist das Display?

Um welche Display-Technologie handelt es sich?

Wie groß sind die maximale Auflösung und die maximale Farbtiefe?

Wie groß ist der Grafik-Speicher?

Bieten Sie standardisierte Abnahmeprozeduren zur Qualitätssicherung des angebotenen Produktes an?

Welche Arten von Tests werden dabei durchgeführt?

1.3 Rechner im sicheren Raum

Hersteller, Marke und Version des Produkts:

Abmessungen des Gerätes (Breite, Höhe, Tiefe):

Gesamtgewicht:

Welcher Prozessor (Marke, Taktfrequenz) wird eingesetzt?

Wie groß ist die Kapazität des Arbeitsspeichers (RAM)?

Maximale Erweiterbarkeit des Arbeitsspeichers:

Falls ECC-RAM eingesetzt wird, beschreiben Sie die verwendete Technologie (SEC-DED, „chipkill-correct“ usw.)!

Wie groß ist die Speicherkapazität der Festplatte(n)?

Welche Art von Festplatten-Controller wird verwendet?

Durchschnittliche Zugriffszeit der Festplatte(n):

Durchschnittliche Latenzzeit der Festplatte(n):

Enthält das Gerät ein Diskettenlaufwerk?

Enthält das Gerät ein CD-Laufwerk?

Wie funktioniert die Prozessorkühlung?

Welche Standards werden vom Ethernet-Adapter unterstützt?

Über welche anderen Schnittstellen verfügt der Rechner?

Ist eine Konsole im Lieferumfang enthalten?

Ist ein Grafikbildschirm im Lieferumfang enthalten?

Welche Auflösungen werden von der Konsole unterstützt?

Welche Tastatur ist im Lieferumfang enthalten?

Wird eine zentrale Backuplösung unterstützt?

Welches Medium wird von dieser Lösung unterstützt?

Bieten Sie standardisierte Abnahmeprozeduren zur Qualitätssicherung des angebotenen Produktes an?

Welche Arten von Tests werden dabei durchgeführt?

1.4 Rechner für X.509v3-Datenbank und Widerrufsdienst

Hersteller, Marke und Version des Produkts:

Abmessungen des Gerätes (Breite, Höhe, Tiefe):

Gesamtgewicht:

Welcher Prozessor (Marke, Taktfrequenz) wird eingesetzt?

Wie groß ist die Kapazität des Arbeitsspeichers (RAM)?

Maximale Erweiterbarkeit des Arbeitsspeichers:

Wie groß ist die Speicherkapazität der Festplatte(n)?

Welche Art von Festplatten-Controller wird verwendet?

Durchschnittliche Zugriffszeit der Festplatte(n):

Durchschnittliche Latenzzeit der Festplatte(n):

Enthält das Gerät ein Diskettenlaufwerk?

Enthält das Gerät ein CD-Laufwerk?

Falls ECC-RAM eingesetzt wird, beschreiben Sie die verwendete Technologie (SEC-DED, „chipkill-correct“ usw.)!

Wie funktioniert die Prozessorkühlung?

Über wie viele Ethernet-Adapter verfügt der Rechner?

Welche Standards werden von den Ethernet-Adaptern unterstützt?

Über welche anderen Schnittstellen verfügt der Rechner?

Auf welches Zeitsignal greift der Zeitgeber zurück?

Ist die Installation einer externen Außenantenne erforderlich?

Wie genau läuft die Zeit weiter, wenn das empfangene Zeitsignal ausfällt?

Welche Maßnahmen werden gegen Manipulationen des empfangenen Zeitsignals (Störsender) ergriffen?

Besteht für die Rechner 5.1.5 eine Möglichkeit, den Zeitgeber zu deaktivieren, wenn Hinweise auf ein deutliches Abweichen des Zeitgebersignals von der tatsächlichen Zeit vorliegen?

Ist eine Konsole im Lieferumfang enthalten?

Bieten Sie standardisierte Abnahmeprozeduren zur Qualitätssicherung des angebotenen Produktes an?

Welche Arten von Tests werden dabei durchgeführt?

1.5 LDAP- und HTTP-Server (Cluster)

Hersteller, Marke und Version des Produkts:

Abmessungen des Gerätes (Breite, Höhe, Tiefe):

Gesamtgewicht:

In welchem Temperaturbereich wird ein zuverlässiger Betrieb garantiert?

In welchem Luftfeuchtigkeitsbereich wird ein zuverlässiger Betrieb garantiert?

Wird eine RISC-CPU verwendet?

Beschreiben Sie die Rechnerarchitektur!

Beschreiben Sie, wie die im Cluster befindlichen Rechner und allfällige gemeinsame Komponenten (z. B. Massenspeicher) zusammenwirken!Anzahl der verwendeten Prozessoren:

Taktfrequenz der verwendeten Prozessoren:

Anzahl der installierten Prozessorboards:

Anzahl der maximal zu installierenden Prozessorboards:

Anzahl der maximal zu installierenden Prozessoren je Prozessorboard:

Größe des Arbeitsspeichers:

Maximale Erweiterbarkeit des Arbeitsspeichers:

Falls ECC-RAM eingesetzt wird, beschreiben Sie die verwendete Technologie (SEC-DED, „chipkill-correct“ usw.)!

Wie viele HD-Controller sind im System vorhanden?

Wie viele HD-Controller werden maximal unterstützt?

Um welche Art von HD-Controller handelt es sich?

Wird RAID unterstützt?

Welche RAID-Level werden unterstützt?

Wie viele Einschübe für Festplatten stehen zur Verfügung?

Wie viele davon für Festplatten, die im laufenden Betrieb gewechselt werden können (Hot swap)?

Wie groß ist die Speicherkapazität der Festplatte(n)?

Durchschnittliche Zugriffszeit der Festplatte(n):

Durchschnittliche Latenzzeit der Festplatte(n):

Welche kryptographischen Koprozessoren werden verwendet?

Wie viele kryptographische Koprozessoren verwendet?

Welche Kühlung wird verwendet?

Wie viele redundante Kühler werden verwendet?

Für wie viele LDAP-Zugriffe pro Minute wurde der Rechner dimensioniert?

Für wie viele HTTP-Zugriffe (Hits) pro Minute wurde der Rechner dimensioniert?

Für wie viele HTTPS-Verbindungsaufbauten (RSA-Anwendungen 1024 Bit) wurde der Rechner dimensioniert?

Bieten Sie standardisierte Abnahmeprozeduren zur Qualitätssicherung des angebotenen Produktes an?

Welche Arten von Tests werden dabei durchgeführt?

2. Software

2.1 Betriebssysteme

Hersteller, Marken und Versionen der Produkte:

Welche Besonderheiten bieten diese Betriebssysteme in Bezug auf allgemeine IT-Sicherheit?

Welche Besonderheiten bieten diese Betriebssysteme in Bezug auf Ausfallssicherheit?

Welche Besonderheiten bieten diese Betriebssysteme in Bezug auf Berechtigungsverwaltung?

Wie können die vitalen Systemparameter durch das Rechenzentrumspersonal überwacht werden?

Inwiefern unterstützt das Betriebssystem der Rechner 1.5 Cluster?

Unterstützt das Betriebssystem der Rechner 1.5 Load Balancing zwischen den im Cluster befindlichen Rechnern?

Wie lange dauert das Switch-over bei Ausfall eines der im Cluster befindlichen Rechner?

2.2 CAPI

Hersteller, Marke und Version des Produkts:

Welche Betriebssysteme werden durch das Produkt unterstützt?

Welche der in PKCS#11 spezifizierten Operationen werden von der CAPI softwaremäßig unterstützt?

Welche Funktionen der kryptographischen Module 5.2.1 werden durch das CAPI nicht oder zumindest nicht vollständig unterstützt?

Welche CAPIs werden außer PKCS#11 unterstützt?

Nach welchen Normen, Evaluations- und Sicherheitsstufen ist das Produkt evaluiert worden?

2.3 Software zur Erstellung von Zertifikaten

Hersteller, Marke und Version des Produkts:

Welche Betriebssysteme werden durch das Produkt unterstützt?

Unterstützt die Software die Verwaltung mehrerer verschiedener Zertifikatskategorien, welche jeweils mit unterschiedlichen Signaturerstellungsdaten signiert werden? Wenn ja, wie viele verschiedene Kategorien?

Verfügt die Software über ein GUI?

In welchen Datenformaten kann ein Antrag auf Ausstellung eine Zertifikats importiert werden?

Unterstützt die Software das Datenformat PKCS#10?

In welchen Datenformaten können Zertifikate exportiert werden?

Unterstützt die Software das Datenformat DER?

Unterstützt die Software das Datenformat PKCS#7?

Unterstützt die Software das Datenformat PKCS#12?

Können Zertifikate als (verständlicher) Text ausgegeben werden?

Können Zertifikate Base64-kodiert werden?

Wie viele Benutzer kann die Software verwalten?

Wie wird sichergestellt, dass nur zwei berechtigte Personen gemeinsam ein Zertifikat ausstellen können?

Wenn die Software mehrere verschiedene Zertifikatskategorien verwalten kann: Wie erfolgt die Auswahl, welche Signaturerstellungsdaten für die Signatur unter das Zertifikat heranzuziehen sind?

Wie viele verschiedene geheimzuhaltende Autorisierungscodes muss eine berechtigte Person kennen, um in allen Zertifikatskategorien Zertifikate ausstellen zu können?

Welche X.509v3-Extensions werden unterstützt?

Welche CAPIs werden beim Zugriff auf die Signaturerstellungseinheit unterstützt?

Nach welchen Normen, Evaluations- und Sicherheitsstufen ist das Produkt evaluiert worden?

2.4 Datenbank-Client

Hersteller, Marke und Version des Produkts:

Welche Betriebssysteme werden durch das Produkt unterstützt?

Welche Betriebssysteme werden durch das Produkt unterstützt?

Verfügt der Datenbank-Client über ein GUI?

Kann der Datenbank-Server mittels Shell-Scripts abgefragt werden?

Sind Änderungen der Daten via Client möglich?

Sind Änderungen der Datendefinition via Client möglich?

In welcher Sprache wurde das Server-Script erstellt?

2.5 Datenbank-Server

Hersteller, Marke und Version des Produkts:

Welche Betriebssysteme werden durch das Produkt unterstützt?

In welcher Art wird die Datenbank realisiert (z. B. Text, LDAP, SQL, ...)?

In welchem Format werden Daten vom bzw. zum Server übermittelt?

Ist die Datendefinition änderbar?

Welchen Beschränkungen unterliegt die Größe der Datenbank?

Können mehrere Zertifikate pro Zertifizierungsdienst gespeichert werden?

Welche Informationen bleiben auch nach Widerruf oder Ablauf eines Zertifikats in der Datenbank erhalten?

Sind Beziehungen zwischen Tabellen möglich?

Mit welchem Produkt wird SSL bzw. TLS verwirklicht?

2.6 Software zur Erstellung von Widerrufslisten

Hersteller, Marke und Version des Produkts:

Welche Betriebssysteme werden durch das Produkt unterstützt?

Welche X.509v2-Extensions für CRLs und für CRL-Einträge werden unterstützt?

Welche CAPIs werden beim Zugriff auf die Signaturerstellungseinheit unterstützt?

Ist eine automatische Erstellung und Signierung mittels Shell-Scripts oder Batch-Dateien möglich?

Wie kann vom Rechner 5.1.3 aus ein Widerruf durchgeführt werden?

Nach welchen Normen, Evaluations- und Sicherheitsstufen ist das Produkt evaluiert worden?

2.7 HTTP-Server

Hersteller, Marke und Version des Produkts:

Welche Betriebssysteme werden durch das Produkt unterstützt?

Welche Software wird als HTTP-Server eingesetzt?

Welche Software wird für die SSL- und TLS-Unterstützung eingesetzt?

Welche kryptographischen Verfahren und welche Parameter (Schlüssellängen) werden unterstützt?

Für wie viele HTTP-Zugriffe (Hits) pro Minute wurde der HTTP-Server dimensioniert?

Für wie viele HTTPS-Zugriffe (Hits) pro Minute wurde der HTTP-Server dimensioniert?

Wie viele SSL- bzw. TLS-Verbindungen können gleichzeitig verwaltet werden?

Welche Parameter der SSL- und TLS-Module können durch Systemadministratoren konfiguriert werden?

Welche kryptographischen Koprozessoren werden von der Server-Software unterstützt?

In welcher Form erfolgt diese Unterstützung (z. B. PKCS#11)?

2.8 LDAP-Server

Hersteller, Marke und Version des Produkts:

Welche Betriebssysteme werden durch das Produkt unterstützt?

Welche LDAP-Versionen werden durch das Produkt unterstützt?

Welche IETF-Spezifikationen (Internet Drafts und RFCs) erfüllt das Produkt?

Welche Software wird für die SSL- und TLS-Unterstützung eingesetzt?

Wie viele SSL- bzw. TLS-Verbindungen können gleichzeitig verwaltet werden?

Welche Parameter der SSL- und TLS-Module können durch Systemadministratoren konfiguriert werden?

Können mehrere Zertifikate pro Verzeichniseintrag gespeichert werden?

Welche Informationen bleiben auch nach Widerruf oder Ablauf eines Zertifikats in der Datenbank erhalten?

Können mehrere Zertifikate pro Zertifizierungsdienst gespeichert werden?

2.9 NTP-Server

Hersteller, Marke und Version des Produkts:

Welche Betriebssysteme werden durch das Produkt unterstützt?

Wie erfolgt der Zugriff auf den Zeitgeber?

Wie oft wird der primäre NTP-Server mit dem Zeitgeber synchronisiert?

Wie oft wird der sekundäre NTP-Server mit dem primären synchronisiert?

Welche Einstellungen können durch Systemadministratoren konfiguriert werden?

Welche Authentifikationsverfahren werden unterstützt?

2.10 SSH-Server

Hersteller, Marke und Version des Produkts:

Welche Betriebssysteme werden durch das Produkt unterstützt?

Welche Versionen des SSH-Protokolls werden unterstützt?

Welche Einstellungen können durch Systemadministratoren konfiguriert werden?

Welche Authentifikationsverfahren werden unterstützt?

2.11 Software zur Überwachung des Zeitgebers

Hersteller, Marke und Version des Produkts:

Welche Betriebssysteme werden durch das Produkt unterstützt?

Bei welcher Abweichung von der Referenzzeit wird ein Alarm ausgelöst?

Wie lange muss diese Abweichung anhalten, damit ein Alarm ausgelöst wird?

Sind diese Toleranzgrenzen konfigurierbar?

Wie erfolgt die Alarmierung?

2.12 Software zur Kommunikation des Widerrufsdienstes mit dem Rechner 5.1.4

Hersteller, Marke und Version des Produkts:

Welche Betriebssysteme werden durch das Produkt unterstützt?

Wenn der automatisierte Widerruf anders realisiert wird als in Kapitel 3.3.2 beschrieben: Beschreiben Sie die Funktionsweise des automatisierten Widerrufs:

Welche Methode wird zum Absenden des Webformulars verwendet (POST/GET)?

In welcher Sprache wurde das Server-Script erstellt?

Welche Maßnahmen werden ergriffen, um Sicherheitsprobleme beim Ausführen des Server-Scripts zu vermeiden?

Wie erfolgt die Übermittlung des Widerrufsantrags von den Rechnern 5.1.5 an den Rechner 5.1.4?

Wie lange dauert die Durchführung eines Widerrufs vom Absenden des Webformulars bis zur Veröffentlichung der aktualisierten Widerrufsliste?

2.13 Software für die sichere Signatur der Liste der nicht X.509-kompatiblen Anbieter

Hersteller, Marke und Version des Produkts:

Welche Betriebssysteme werden durch das Produkt unterstützt?

Wie ist das Dokumentenformat für die Liste spezifiziert?

Wie erfolgt die Auslösung der Signaturfunktion?

Verfügt die Software über eine grafische Benutzeroberfläche?

Nach welchen Normen, Evaluations- und Sicherheitsstufen ist das Produkt evaluiert worden?

2.14 Software zur sicheren Signaturprüfung

Hersteller, Marke und Version des Produkts:

Welche Betriebssysteme werden durch das Produkt unterstützt?

Verfügt die Software über eine grafische Benutzeroberfläche?

Nach welchen Normen, Evaluations- und Sicherheitsstufen ist das Produkt evaluiert worden?

2.15 Dokumentationssystem

Hersteller, Marke und Version des Produkts:

Welche Betriebssysteme werden durch das Produkt unterstützt?

Legen Sie eine ausführliche Produktbeschreibung bei.

3 Dokumentation, Sicherheitskonzepte, Schulung

Keine Fragen.

4 Wartung

Geben Sie die Adresse des Betreuungsstützpunktes an:

5 Zeitrahmen für Implementierung und Abnahme

Beschreiben Sie – ausgehend von der Annahme, dass der Zuschlag am 28.02.2001 erfolgt – den Zeitrahmen für die Implementierung und Abnahme der einzelnen Komponenten:

6 Sonstiges

Alle weiteren Angaben, die dem Bieter wesentlich erscheinen, sind bei den jeweiligen Kapiteln des Fragenkatalogs anzufügen. Sollte dies im Einzelfall nicht möglich sein, sind diese Angaben hier anzufügen.

---

firmenmäßige Fertigung durch den Bieter

Anlage 4 Preisraster

Die Gliederung des Preisrasters entspricht der Gliederung in Kapitel 5 der Ausschreibungsunterlagen und in Anlage 3 (Fragenkataloge). Die hier eingetragenen Preise werden Bestandteil des Leistungsvertrages (Anlage 5, Punkt 7).

Geben Sie für jede einzelne Komponente den Preis der Komponente in ATS oder in Euro exklusive Umsatzsteuer an. Es sind entweder einheitlich ATS oder einheitlich Euro zu verwenden. Die verwendete Währung ist jeweils anzugeben bzw. die Bezeichnung der nicht verwendeten Währung zu streichen.

Zu den Preisen sind jeweils nachvollziehbare Kalkulationsgrundlagen anzugeben, insbesondere sind die einzelnen angebotenen Komponenten zu bezeichnen, die Stückzahlen und die Einzelpreise anzugeben.

Die Ausschreibungsunterlagen werden auch in elektronischer Form im Format Microsoft Word 97 (siehe Punkt 2.4.3) zur Verfügung gestellt, um die Beantwortung zu erleichtern. Wenn diese Möglichkeit nicht genutzt wird und der Platz des Preisrasters nicht ausreicht, ist dem Angebot eine Beilage beizufügen. Diese ist mit „Beilage zu Preisraster Pkt. X.X.X“ zu kennzeichnen. Im Preisraster selbst ist unter dem betreffenden Punkt der Hinweis auf die Beilage und deren Nummer einzutragen. Die Summen der Preise sind jedenfalls im Preisraster einzutragen.

Bezeichnung des Bieters (Firma):

1. Hardware

1.1 Signaturerstellungshardware

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

1.2 Notebook im Tresor der Aufsichtsstelle/Notebook für das Zweitsystem

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

1.3 Rechner im sicheren Raum

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

1.4 Rechner für X.509v3-Datenbank und Widerrufsdienst

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

1.5 LDAP- und HTTP-Server (Cluster)

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

2. Software

2.1 Betriebssysteme

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

2.2 CAPI

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

2.3 Software zur Erstellung von Zertifikaten

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

2.4 Datenbank-Client

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

2.5 Datenbank-Server

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

2.6 Software zur Erstellung von Widerrufslisten

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

2.7 HTTP-Server

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

2.8 LDAP-Server

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

2.9 Time-Server

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

2.10 SSH-Server

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

2.11 Software zur Überwachung des Zeitgebers

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

2.12 Software zur Kommunikation des Widerrufsdienstes mit dem Rechner 5.1.4

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

2.13 Software für die sichere Signatur der Liste der nicht X.509-kompatiblen Anbieter

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

2.14 Software für die sichere Signaturprüfung

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

2.15 Dokumentationssystem

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

3 Dokumentation, Sicherheitskonzepte, Schulung

Die produktspezifischen Dokumentationen sind unter den Kapiteln 1 und 2 anzuführen.

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

4 Wartung

Es ist der Preis der Wartungsleistungen pro Monat anzugeben. Für die Berechnung der Gesamtsumme in Punkt 6 ist der Preis für 3 Jahre maßgeblich.

Preis pro Monat: **ATS/Euro**

Summe (für 36 Monate): **ATS/Euro**

5 Sonstiges

Notwendige Zusatzleistungen wie z. B. Kleinmaterial, Kabel, etc., die in Kapitel 5 der Ausschreibungsunterlagen nicht explizit erwähnt sind, sind prinzipiell beim jeweiligen Kapitel des Preisrasters einzufügen. Sollte dies im Einzelfall nicht möglich sein, sind die Preise hier einzufügen.

Bezeichnung	Stück/Menge	Einzelpreis	Gesamtpreis

Summe: **ATS/Euro**

6 Gesamtsumme

Gesamtsumme: **ATS/Euro**

---

firmenmäßige Fertigung durch den Bieter

Anlage 5 Vertragsbestimmungen

1 Gegenstand

Gegenstand dieser Ausschreibung, der Angebote der Bieter und im Falle der Zuschlagserteilung des dadurch zu Stande kommenden Leistungsvertrags ist nach Maßgabe der übrigen Bestimmungen dieser Ausschreibung:

– die Lieferung und Installation einer Public-Key-Infrastruktur

– die zum Betrieb erforderlichen Softwarelizenzen

– die Schulung von Administratoren und Lieferung der Dokumentation

– ein unbefristeter Wartungsvertrag

2 Hardwarekauf

2.1 Der Auftragnehmer verkauft und die Telekom-Control GmbH kauft die auf Grund der Ausschreibung ggf. angebotene Hardware, die fabrikneu zu sein hat. Das Eigentum geht auf die Telekom-Control GmbH mit Lieferung, das Risiko mit Abnahme über. Ein Eigentumsvorbehalt des Auftragnehmers hinsichtlich gelieferter Waren ist ausgeschlossen.

2.2 Die Hardware ist frei Aufstellungsort zu liefern. Die Hardware ist jeweils so rechtzeitig zu liefern, dass sie für die Abnahme der jeweiligen Software vor Ort zur Verfügung steht. Hardware, die dazu nicht benötigt wird, ist erst rechtzeitig vor dem Test und der Abnahme des Gesamtsystems zu liefern.

3 Softwarelizenzen

3.1 Der Auftragnehmer liefert die vertragsgegenständliche Software auf geeigneten Datenträgern samt einer entsprechenden Dokumentation und erteilt der Telekom-Control GmbH sowie allen ihr allfällig im Wege der Einzel- oder Gesamtrechtsnachfolge nachfolgenden Gesellschaften nicht ausschließliche, übertragbare und zeitlich und örtlich unbeschränkte Lizenzen zum Gebrauch (Werknutzungsbewilligung) der gesamten Software (einschließlich Betriebssystem-Software). Die Lizenzen umfassen auch das Recht, die Software mit anderen Software-Komponenten, auch anderer Hersteller, zu verbinden.

3.2 Der Auftragnehmer hält die Telekom-Control GmbH gegenüber Ansprüchen Dritter im Zusammenhang mit der in Lizenz gegebenen Software schad- und klaglos.

4 Tests und Abnahme

4.1 Allgemeines

Die Abnahme erfolgt nach Lieferung, Installation, Vorliegen der vollständigen Dokumentation, auch in maschinenlesbarer Form, Schulung und nach erfolgreicher Durchführung der Abnahmetests (Funktionstest).

Die Implementierung erfolgt nach dem vom Auftragnehmer in Anlage 3 Punkt 5 dargelegten Zeitplan, ist aber jedenfalls bis zum 30.06.2001 abzuschließen.

Für einen vom Auftragnehmer zu vertretenden Verzug über den Zeitplan hinaus wird pro begonnener Woche Verzug ein Pönale von 2 % der Gesamtauftragssumme (Anlage 4 Punkt 6) vereinbart.

4.2 Funktionstest

Im Funktionstest wird überprüft, ob die gelieferten Systeme, die im Angebot zugesagten Funktionen erfüllen. Die Tests, die fehlerfrei ablaufen müssen, umfassen:

– Durchführung der wesentlichen Funktionen der Applikationen („proof of concept“);

– Überprüfung von Handhabbarkeit und Benutzerfreundlichkeit der einzelnen Komponenten;

– Durchführung spezifischer Tests

4.3 Abnahme

Nach erfolgreicher Absolvierung des Tests und deren Bestätigung durch die Telekom-Control GmbH, hat diese schriftlich die Abnahme des getesteten Systems dem Anbieter bekanntzugeben.

5 Erfüllungsort

Erfüllungsort ist die Telekom-Control GmbH, Mariahilfer Straße 77–79, 1060 Wien. Hinsichtlich der Systemkomponenten des Widerrufs- und Verzeichnisdienstes ist der Erfüllungsort ein Rechenzentrum, welches in einer separaten Ausschreibung ermittelt wird, aber jedenfalls im Großraum Wien situiert sein soll. Dieser Erfüllungsort wird rechtzeitig bekannt gegeben.

6 Wartung

Der Wartungsvertrag wird auf unbestimmte Zeit abgeschlossen. Er kann von der Telekom-Control GmbH unter Einhaltung einer Frist von drei Monaten, vom Auftragnehmer unter Einhaltung einer Frist von 12 Monaten jeweils zum 31. Dezember eines Kalenderjahres durch eingeschriebenen Brief gekündigt werden. Für die Rechtzeitigkeit dieser Erklärung ist das Datum des Poststempels maßgeblich.

Der Bieter hat den Betreuungsstützpunkt für die Wartung im Angebot bekanntzugeben. Die Betreuung hat deutschsprachig zu erfolgen.

Die Wartungsleistungen entsprechen den Anforderungen in Punkt 5.4 der Ausschreibungsunterlagen.

7 Preise

7.1 Der Bieter hat die Preise im beigefügten Preisraster Anlage 4 einzutragen. Dabei ist darauf zu achten, dass der Preisraster vollständig ausgefüllt wird.

7.2 Die Preise des Leistungsvertrages ergeben sich aus den Preisblättern des durch den Zuschlag angenommenen Angebotes.

7.3 Sämtliche Preise für Hard- und Software verstehen sich einschließlich Lieferung an den Aufstellungsplatz, Kosten der Verpackung, Verzollung (DDP gemäß Incoterms

1990) und sonstigen Abgaben und Gebühren, Aufstellung, Installation und Inbetriebnahme, Vornahme der Tests bis zur Abnahme, sowie den Abtransport eventuell anfallender Verpackung.

7.4 Wird eine Leistung zu einem Pauschalbetrag beauftragt, so erfolgt die Abrechnung unabhängig von den tatsächlich ausgeführten Massen. Der Auftragnehmer ist verpflichtet, vor Angebotslegung die Massen zu prüfen und erkennt sie als verbindlich an. Nachträglich festgestellte Rechenfehler oder sonstige Irrtümer in der Preisermittlung haben keine Erhöhung des Pauschalbetrages zur Folge bzw. werden Nachforderungen aus diesen Gründen nicht anerkannt.

7.5 Mehr- oder Minderleistungen, bedingt durch vereinbarte Ausführungsänderungen – soweit diese nach den Vertragsbestimmungen Auswirkungen auf den Preis haben – werden getrennt ermittelt und die Kosten dem Pauschalbetrag zugeschlagen oder von diesem abgesetzt.

7.6 Rechnungen sind in zweifacher Ausfertigung zu legen. Allen Rechnungen sind Kopien der bestätigten Lieferscheine beizulegen. Die Fälligkeit der Rechnungen tritt mit erfolgreicher Abnahme der Leistung/Teilleistung ein.

7.7 Auch vorbehaltlose Zahlungen bedeuten keine Anerkennung der Ordnungsgemäßheit der Lieferung bzw. Leistung und damit keinen Verzicht auf irgendwelche der Telekom-Control GmbH zustehende Ansprüche.

7.8 Preisbestimmungen haben in Schillingbeträgen oder Eurobeträgen exklusive Umsatzsteuer zu erfolgen und gelten vorbehaltlich des folgenden Absatzesals Festpreise.

7.9 Periodische Entgelte (mit Ausnahme etwaiger laufender Lizenzgebühren) und Entgelte für Verbrauchsmaterial, Ersatzteile, Wartungsleistungen auf Abruf und Unterstützungsleistung des Auftragnehmers müssen nicht Fixpreise sein. Es genügt, Ausgangspreise zum Zeitpunkt der Angeboterstellung oder zu einem späteren Zeitpunkt zu nennen und anzugeben, wie sie sich in Zukunft ändern können. Die höchstmögliche jährliche Änderung ist anzugeben.

7.10 Dem ausgefüllten Preisraster sind nachvollziehbare Kalkulationsunterlagen beizulegen.

8 Einhaltung von Rechtsvorschriften

Der Auftragnehmer wird die österreichischen Rechtsvorschriften, insbesondere österreichische sozial- und arbeitsrechtliche Vorschriften einschließlich Vorschriften über Ausländerbeschäftigung, Arbeitnehmerschutz und Arbeitszeit einhalten.

9 Leistungsstörungen

9.1 Garantien

Der Auftragnehmer garantiert, dass die angebotenen, gelieferten oder installierten Produkte die bedungenen (im Sinne der gesamten Ausschreibungsunterlagen) und gewöhnlich vorausgesetzten Eigenschaften aufweisen, sowie den in Österreich zum Zeitpunkt der Abnahme der jeweiligen Leistung geltenden Normen (insbesondere EU-Normen) entsprechen.

Der Auftragnehmer garantiert während der Garantiefrist für sämtliche gelieferte Produkte, wie überhaupt für alle vertragsgegenständlichen Leistungen die volle Funktionsfähigkeit, für Dienstleistungen auch einwandfreie Resultate. Die Beweislast dafür, dass Funktionsausfälle oder Funktionseinschränkungen nicht ihre Ursache in den gelieferten Produkten und/oder erbrachten Dienstleistungen haben, trifft den Auftragnehmer.

Die Garantiefrist beträgt 2 Jahre ab Abnahme der Gesamtlieferung. Werden jedoch Teile der Gesamtlieferung oder damit in Verbindung stehende Produkte oder Dienstleistungen gesondert abgenommen, so beginnt damit die Garantiefrist nur für die abgenommenen Teile zu laufen, ohne dass sich dadurch etwas an der Garantie und deren Dauer für die Gesamtlieferung insgesamt ändert. Bei Ersatzlieferungen und Behebung von Fehlern (auch durch Nachlieferung von Fehlendem) beginnt die Garantiefrist für die betroffenen Komponenten, einschließlich Software, mit der Abnahme neu zu laufen.

Die Telekom-Control GmbH wird sich bemühen, Mängel oder Störungen möglichst unverzüglich dem Auftragnehmer zu melden, doch gehen die Rechte aus den Garantien auch bei verspäteter Meldung nicht unter, sofern die Meldung innerhalb der Garantiefrist erfolgt und – wenn es zu keiner Einigung kommt – binnen 6 Monaten ab Ablauf der Garantiefrist gerichtlich geltend gemacht wird. Gegen eine Klage des Auftragnehmers auf Zahlung können Einwendungen aus den Mängeln oder Störungen auch über diesen Zeitpunkt hinaus geltend gemacht werden. Die Telekom-Control GmbH trifft keine Untersuchungspflicht.

9.2 Eingriff in Rechte Dritter

Der Auftragnehmer hat die Telekom-Control GmbH zeitlich unbeschränkt gegenüber etwaigen aus der Lieferung bzw. den Leistungen entstehenden Patent-, Marken-, Musterschutz- und/oder urheberrechtlichen Streitigkeiten schad- und klaglos zu halten und den uneingeschränkten Gebrauch der gelieferten Sachen bzw. den erbrachten Leistungen zu gewährleisten.

9.3 Rücktritt

Hält der Auftragnehmer einen Termin des Zeitplanes nicht ein oder liegen sonstige wesentliche Verletzungen des Leistungsvertrages vor, hat die Telekom-Control GmbH das Recht, vom Vertrag zur Gänze oder teilweise zurückzutreten. Auch der Rücktritt vom Vertrag hinsichtlich einzelner Teilsysteme oder sonstiger einzelner Lieferungen oder Leistungen (Teilrücktritt) steht der Telekom-Control GmbH bei Vorliegen der Rücktrittsvoraussetzungen zu, wenn der Verzug diese Teillieferungen oder Teilleistungen betrifft, und zwar unbeschadet des Rechtes auf Rücktritt vom gesamten Leistungsvertrag auch bei Verzug hinsichtlich einzelner Lieferungen oder Leistungen. Der Begriff Rücktritt umfasst auch den Teilrücktritt, soweit sich nicht ausdrücklich oder aus dem Zusammenhang etwas anderes ergibt.

Ist ein Verzug des Auftragnehmers Grund für den Rücktritt, setzt die Rücktrittserklärung voraus, dass sich der Auftragnehmer zum Zeitpunkt der Abgabe dieser Erklärung bereits 4 Wochen in Verzug befindet. Die Telekom-Control GmbH kann den Rücktritt oder Teilrücktritt nur unter schriftlicher (Fax genügt) Setzung einer mindestens 6-wöchigen Nachfrist zur Erfüllung der nicht eingehaltenen Termine oder Beseitigung von sonstigen Vertragsverletzungen aussprechen. Hat die Telekom-Control GmbH vor Erklärung des Rücktritts bereits eine Nachfrist von insgesamt 10 Wochen, wenn sich der Rücktritt aber nicht auf einen Verzug, sondern auf eine sonstige wesentliche Verletzung des Leistungsvertrages gründet, von 6 Wochen zur Erfüllung des oder der nicht eingehaltenen Termine oder Beseitigung von sonstigen Vertragsverletzungen gesetzt, ohne dass die Erfüllung oder die Beseitigung von sonstigen Vertragsverletzungen erfolgt ist, ist eine neuerliche Setzung einer Nachfrist nicht erforderlich. Dieses Recht, wie auch alle sonstigen

Rechte der Telekom-Control GmbH, gehen nicht dadurch verloren, dass sie nicht unverzüglich geltend gemacht werden. Die Beweislast dafür, dass kein Verzug oder keine sonstige wesentliche Verletzung des Leistungsvertrages vorliegt, trifft den Auftragnehmer.

Im Falle des Rücktritts hat der Auftragnehmer die von der Telekom-Control GmbH als Entgelt bereits bezahlten Beträge mit einer Verzinsung von 5 % p. a. über dem Diskontsatz der Oesterreichischen Nationalbank zurückzuerstatten. Die Telekom-Control GmbH hat dem Auftragnehmer auf dessen Kosten das von ihm Gelieferte, soweit möglich, zurückzustellen. Insbesondere erfolgt die Demontage und der Rücktransport von Gegenständen, die der Auftragnehmer geliefert hat, auf Kosten und Gefahr des Auftragnehmers. Wenn die Telekom-Control GmbH dies verlangt, ist der Auftragnehmer verpflichtet, die Demontage und den Abtransport selbst durchzuführen. Die Telekom-Control GmbH hat im Rücktrittsfall an den Auftragnehmer kein Benützungsentgelt und keine sonstigen Beträge zu zahlen, insbesondere kein Entgelt für Einschulung oder dergleichen. Bereits geleistete Zahlungen für Einschulungen sind mit der obigen Verzinsung zurückzuerstatten. Dies gilt sinngemäß für den Fall eines Teilrücktritts hinsichtlich der für die vom Teilrücktritt betroffenen Lieferung und die Entgelte für Einschulung, die im Zusammenhang mit den vom Teilrücktritt betroffenen Lieferungen und Leistungen stehen.

Das Recht zu Rücktritt steht der Telekom-Control GmbH unabhängig von einem Verschulden des Auftragnehmers zu. Teilrücktritte schließen den späteren Rücktritt vom gesamten Leistungsvertrag nicht aus.

10 Gerichtsstand, anwendbares Recht

Ausschließlicher Gerichtsstand für Streitigkeiten aus und in Zusammenhang mit dem Leistungsvertrag auch über sein Bestehen und nach seiner Beendigung, ist das sachlich zuständige Gericht für Wien 1, Innere Stadt. Die Telekom-Control GmbH kann den Auftragnehmer auch vor dem für seinen Sitz zuständigen Gericht klagen.

Auf den Leistungsvertrag ist österreichisches Recht unter Ausschluss von Verweisungsnormen und des UN-Übereinkommens über den internationalen Warenkauf anwendbar.

11 Allgemeines

11.1 Salvatorische Klausel

Sollte eine Bestimmung des Leistungsvertrages unwirksam sein oder werden, so wird die Gültigkeit des Leistungsvertrages im Übrigen hiervon nicht berührt. Anstelle der unwirksamen Bestimmungen soll eine Regelung gelten, die im Rahmen des rechtlich möglichen dem Willen der Parteien am nächsten kommt und in ihren wirtschaftlichen Auswirkungen am besten der unwirksamen Bestimmung entspricht.

11.2 Schriftform, gesamte Vereinbarung

Der Leistungsvertrag enthält die gesamte Vereinbarung der Parteien, Nebenabreden sind nicht getroffen. Änderungen oder Ergänzungen, einschließlich sämtlicher Beilagen, bedürfen zu ihrer Wirksamkeit der Schriftform.

11.3 Abtretungsverbot

Keine Partei ist berechtigt, ihre Rechte oder Pflichten nach Maßgabe des Leistungsvertrages ohne vorheriges schriftliches Einverständnis der anderen Partei auf Dritte zu übertragen.

11.4 Aufrechnung

Die Telekom-Control GmbH ist berechtigt, ihre Zahlungsverpflichtungen mit allen Forderungen gegen den Auftragnehmer gegenzuverrechnen.

11.5 Haftung zur ungeteilten Hand

Wird eine Bietergemeinschaft (Arbeitsgemeinschaft) Auftragnehmer, haften die Mitglieder der Arbeitsgemeinschaft für alle Verpflichtungen aus dem Leistungsvertrag zur gesamten Hand (Solidarhaftung).

11.6 Rechtsnachfolge

Derzeit ist die Eingliederung der Telekom-Control GmbH in eine neu zu schaffende Regulierungsbehörde (KommAustria GmbH) in Diskussion. Dieser Vertrag gilt für die Telekom-Control GmbH und alle ihre allfälligen Nachfolgegesellschaften im Wege der Einzel- oder Gesamtrechtsnachfolge.

---

firmenmäßige Fertigung durch den Bieter