a-sign Policy

Certificates *Premium*

Version: 1.2.7

Gültig ab: 30.10.2001

Policy Working Group

INHALT

1 Einführung

Dieses Kapitel gibt dem Leser einen Überblick über das vorliegende Dokument und beschreibt die Einheiten, die an den Signatur- und Zertifizierungsdiensten beteiligt sind, sowie die Einsatzmöglichkeiten für die ausgestellten Zertifikate.

1.1 Überblick

Das Ziel des vorliegenden Dokuments besteht darin, die Richtlinien bezüglich Zertifikaten der Klasse *Premium* derart festzulegen, daß die Voraussetzungen für eine sichere und zuverlässige Abwicklung der angebotenen Signatur- und Zertifizierungsdienste gewährleistet sind.

Jedes Zertifikat der Klasse *Premium* enthält einen Verweis auf die a-sign Policy Certificates *Premium*, sodaß dem Benutzer des Zertifikates die Möglichkeit eingeräumt wird, sich darüber zu informieren, ob das Zertifikat den Erfordernissen des geplanten Verwendungszwecks genügt.

1.2 Identifikation der Policy

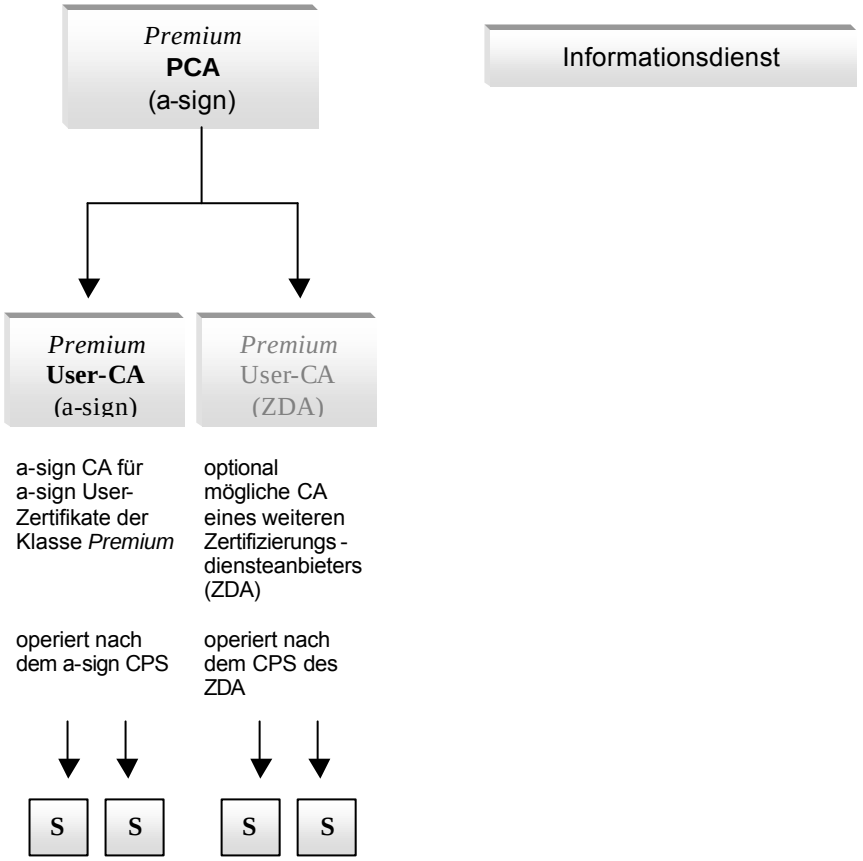
Name der Policy: a-sign Policy Certificates *Premium*, Version 1.2.6.
Object Identifier: **1.3.6.1.4.1.3733** (DATAKOM AUSTRIA) **.1** (a-sign) **.1** (Policy) .**4** (Policy Certificates *Premium*) **.1.2.7.** (Version)

In allen ausgegebenen Zertifikaten dieser Klasse ist dieser Object Identifier als Verweis auf die Policy eingetragen.

© 2000 DATAKOM AUSTRIA GMBH

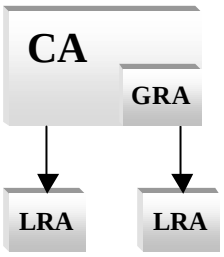
1.3 a-sign Zertifizierungsinfrastruktur und Anwendungsbereiche

1.3.1 a-sign Zertifizierungsinfrastruktur



CA ... Certification Authority
PCA ... Primary Certification Authority
CPS … Certification Practice Statement
ZDA ... Zertifizierungsdiensteanbieter
S ... Signator

ABBILDUNG 1: ZERTIFIZIERUNGSINFRASTRUKTUR FÜR ZERTIFIKATE DER KLASSE PREMIUM



CA ... Certification Authority
GRA … Global Registration Authority
LRA ... Local Registration Authority

ABBILDUNG 2: KOMPONENTEN EINER A-SIGN CA FÜR A-SIGN ZERTIFIKATE DER KLASSE PREMIUM

1.3.1.1 a-sign *Premium* Primary Certification Authority (PCA)

Die a-sign *Premium* Primary Certification Authority (PCA) stellt Zertifikate für *Premium* Certification Authorities (CAs) aus, die den Anforderungen der a-sign Policy Certificates *Premium* entsprechen oder auch darüber hinausgehen, und ist für das Management von Zertifikaten für *Premium* CAs sowie für die Umsetzung der a-sign Policy Certificates *Premium* verantwortlich.[1] Hinweis: Die PCA ist nicht implementiert.

1.3.1.2 *Premium* Certification Authorities (CAs)

Jede *Premium* Certification Authority (CA) ist direkt der a-sign *Premium* Primary Certification Authority (PCA) unterstellt.

Eine *Premium* CA stellt entsprechend den a-sign Zertifizierungsrichtlinien (d.h. der a-sign Policy Certificates *Premium* bzw. des eigenen Certification Practice Statements (CPS)) Zertifikate der Klasse *Premium* für Signatoren aus und ist für das Management dieser Zertifikate verantwortlich.

Neben der a-sign *Premium* CA sind auch *Premium* CAs weiterer Zertifizierungsdiensteanbieter optional möglich.

1.3.1.3 Global Registration Authorities (GRAs)

Jede *Premium* CA ist dazu berechtigt, eine Global Registration Authority (GRA, deutsch: Globale Registrierungsstelle) mit der zentralen Überprüfung von Zertifikatsanträgen und/oder der zentralen Registrierung von Zertifikatswerbern zu beauftragen.

1.3.1.4 Local Registration Authorities (LRAs)

Jede *Premium* CA ist dazu berechtigt, Local Registration Authorities (LRAs, deutsch: Lokale Registrierungsstellen) mit der lokalen Überprüfung von Zertifikatsanträgen und/oder der lokalen Registrierung von Zertifikatswerbern zu beauftragen. Während jeder *Premium* CA höchstens eine GRA zugeordnet ist, können ihr mehrere LRAs unterstellt sein.

1.3.1.5 Signatoren

Als Signatoren (Inhaber von Zertifikaten der Klasse *Premium*) sind ausschließlich Zertifizierungsdiensteanbieter und natürliche Personen zulässig.

1.3.1.6 a-sign Informationsdienst

Der a-sign Informationsdienst stellt Zertifikatsverzeichnisse, Widerrufslisten (CRLs), Sperrlisten, die a-sign Richtlinien (a-sign Policies, Certification Practice Statements (CPSs) aller CAs) sowie andere relevante Informationen bezüglich der Signatur- und Zertifizierungsdienste online und öffentlich zugänglich zur Verfügung.

Der a-sign Informationsdienst ist unter folgender Webadresse zugänglich:
`http://a-sign.datakom.at/`

1.3.2 Anwendung von Zertifikaten der Klasse *Premium*

Zertifikate, die im Rahmen der a-sign Zertifizierungsinfrastruktur ausgegeben werden, können in unterschiedliche Klassen (*Light*, *Medium*, *Strong* und *Premium*) und Typen (User-Zertifikate, Server-Zertifikate und Developer-Zertifikate) eingeteilt werden. Die Klasse gibt dabei die verwendete Variante bei der Registrierung an, der Typ identifiziert den zulässigen Anwendungsbereich.

[1] Im Rahmen der a-sign Zertifizierungsinfrastruktur werden Zertifikate der Klassen *Light*, *Medium*, *Strong* und *Premium* ausgegeben. Zu jeder dieser Klassen existieren eine eigene PCA und eigene CAs. Im vorliegenden Dokument ist, falls nicht anders angegeben, mit dem Begriff „a-sign PCA“ immer die a-sign *Premium* PCA, mit dem Begriff „CA“ immer eine *Premium* CA gemeint.

© 2000 DATAKOM AUSTRIA GMBH

Zertifikate der Klasse *Premium* werden ausschließlich als User-Zertifikate ausgegeben. Das Anwendungsgebiet dieser Zertifikate umfaßt das elektronische Signieren von elektronischen Dokumenten.

User-Zertifikate der Klasse *Premium* stellen qualifizierte Zertifikate im Sinne des Österreichischen Signaturgesetzes und der auf seiner Grundlage ergangenen Verordnungen dar, sodaß die auf diesen Zertifikaten beruhenden digitalen Signaturen unter gewissen zusätzlichen Voraussetzungen (siehe Kapitel 6.3) den rechtlichen Erfordernissen einer eigenhändigen Unterschrift genügen.

Weitere Informationen über die a-sign Signatur- und Zertifizierungsdienste sind unter folgender Webadresse zugänglich: `http://a-sign.datakom.at/`

1.4 Kontaktierungsmöglichkeiten

1.4.1 Kontaktinformation zur a-sign *Premium* Certification Authority

Name:	DATAKOM AUSTRIA GMBH
Adresse:	A-1040 Wien Wiedner Hauptstraße 73
Telefon:	+43 (1) 50145-0
E-Mail:	kunden.service@datakom.at
Web:	http://www.datakom.at/

1.4.2 a-sign Web-Schnittstellen

Unter der Webadresse http://a-sign.datakom.at/ werden Informationen zu folgenden Themen angeboten:

ABBILDUNG 3: A-SIGN WEB-SCHNITTSTELLEN

2 Allgemeine Richtlinien

In diesem Kapitel wird dem Leser ein Überblick über die allgemeinen Grundlagen der a-sign Signatur- und Zertifizierungsdienste (Pflichten der beteiligten Einheiten, Haftung, rechtliche Aspekte, Entgelte, Veröffentlichungen, Kontrollen, Datenschutz usw.) gegeben.

2.1 Pflichten

2.1.1 Verpflichtungen der a-sign *Premium* PCA

2.1.1.1 Allgemeine Verpflichtungen

Die a-sign *Premium* PCA hat für die Einhaltung und Umsetzung der a-sign Policy Certificates *Premium* sowie der CPSs der untergeordneten CAs durch die entsprechenden Einheiten der a-sign Zertifizierungsinfrastruktur zu sorgen.

2.1.1.2 Ausstellung und Widerruf von Zertifikaten

Die a-sign *Premium* PCA hat jene CAs, die die anzuwendenden Richtlinien einhalten, zu zertifizieren bzw. ein für eine CA ausgestelltes Zertifikat zu widerrufen, falls die Notwendigkeit dazu gegeben ist (siehe Kapitel 4.5.2).

2.1.1.3 Privater PCA-Schlüssel

Die a-sign *Premium* PCA hat durch geeignete organisatorische, infrastrukturelle, personelle und sicherheitstechnische Maßnahmen für den Schutz ihres privaten Schlüssels (Signaturschlüssels) zu sorgen.

Die a-sign *Premium* PCA hat ihren privaten Schlüssel (Signaturschlüssel) ausschließlich zum Signieren von CA-Zertifikaten und authentischen Verzeichnissen zu verwenden.

2.1.1.4 Veröffentlichungen

Die a-sign *Premium* PCA hat für die Veröffentlichung

- der a-sign Policy Certificates *Premium*,
- der CPSs aller untergeordneten CAs,
- ihres Wurzelzertifikates sowie
- aller ausgestellter bzw. widerrufener Zertifikate für die untergeordneten CAs

zu sorgen.

2.1.2 Verpflichtungen von *Premium* CAs

2.1.2.1 Definition eines Sicherheitskonzeptes

Entsprechend den Abschnitten 5 und 6 der a-sign Policy Certificates *Premium* ist von CAs ein Sicherheitskonzept zu entwickeln und zu dokumentieren.

2.1.2.2 Allgemeine Verpflichtungen

Jede von einer a-sign *Premium* PCA zertifizierte *Premium* CA ist dazu verpflichtet, die a-sign Policy Certificates *Premium* bzw. das von ihr selbst definierte CPS umzusetzen und einzuhalten. Dies erfordert insbesondere, daß die CA

- die Einhaltung der in diesen Richtlinien spezifizierten Identifikations- und Authentifikationsmechanismen sicherzustellen hat,

© 2000 DATAKOM AUSTRIA GMBH

- Zertifikate für Signatoren gemäß dieser Richtlinien auszustellen hat,
- dafür zu sorgen hat, daß der private Schlüssel bzgl. eines Zertifikates, das für eine natürliche Person ausgestellt wird, an eine entsprechende Hardware-Signaturerstellungseinheit (z.B. Chipkarte, siehe Kapitel 6.3.2) gebunden ist,
- Zertifikate für Signatoren gegebenenfalls zu widerrufen oder zu sperren hat und
- Aktivitäten einer ihr zugeordneten GRA bzw. LRA zu überwachen hat.

2.1.2.3 Privater CA-Schlüssel

Jede *Premium* CA hat durch geeignete organisatorische, infrastrukturelle, personelle und sicherheitstechnische Maßnahmen für den Schutz ihres privaten Schlüssels (Signaturschlüssels) zu sorgen (siehe Kapitel 6.2.1).
Jede *Premium* CA hat ihren privaten Schlüssel ausschließlich zum Signieren von Zertifikaten für Signatoren und authentischen Verzeichnissen zu verwenden.

2.1.2.4 Veröffentlichungen, Informationen für Signatoren

Ausgestellte Zertifikate für Signatoren sind entsprechend den a-sign Richtlinien (d.h. der a-sign Policy Certificates *Premium* bzw. des eigenen Certification Practice Statements (CPS)) zu veröffentlichen (siehe Kapitel 2.5.3). Zertifikatswerber sind von einer erfolgten Ausstellung des Zertifikates in Kenntnis zu setzen.

Widerrufene Zertifikate für Signatoren sind entsprechend den a-sign Richtlinien in Form von Certificate Revocation Lists (CRLs, deutsch: Widerrufslisten) zu veröffentlichen (siehe Kapitel 2.5.4). Signatoren sind von einem erfolgten Widerruf ihres Zertifikates in Kenntnis zu setzen.

Unterstützt eine CA den Mechanismus des Sperrens von Zertifikaten, so sind auch die gesperrten Zertifikate in Form von Sperrlisten zu veröffentlichen (siehe Kapitel 2.5.5) und Signatoren von einer erfolgten Sperre ihres Zertifikates in Kenntnis zu setzen.

Jede CA, die ein Zertifikat für einen Signator ausstellt, ist verpflichtet, den Zertifikatswerber über den Umgang mit Zertifikaten, den Umgang mit seinem privaten Schlüssel, den Schutz seines privaten Schlüssels, die Prüfung von digitalen Signaturen sowie weitere Themen zu unterrichten (siehe auch Kapitel 2.5.6).

2.1.3 Verpflichtungen von GRAs

Die GRAs haben alle an sie gestellten, in den relevanten Richtlinien (d.h. in der a-sign Policy Certificates *Premium* bzw. im Certification Practice Statements (CPS) der übergeordneten CA) festgelegten Sicherheitsanforderungen zu erfüllen und die im Zuge der angebotenen Signatur- und Zertifizierungsdienste festgelegten Aufgaben entsprechend dieser Richtlinien durchzuführen.

2.1.4 Verpflichtungen von LRAs

Die LRAs haben alle an sie gestellten, in den relevanten Richtlinien (d.h. in der a-sign Policy Certificates *Premium* bzw. im Certification Practice Statements (CPS) der übergeordneten CA) festgelegten Sicherheitsanforderungen zu erfüllen und die im Zuge der angebotenen Signatur- und Zertifizierungsdienste festgelegten Aufgaben entsprechend dieser Richtlinien durchzuführen.

Falls die Generierung des privaten Schlüssels des Zertifikatswerbers nicht in der ausstellenden CA durchgeführt wird, so hat jede LRA insbesondere sicherzustellen, daß dieser private Schlüssel an eine entsprechende Hardware-Signaturerstellungseinheit des Zertifikatswerbers (z.B. Chipkarte, siehe Kapitel 6.3.2) gebunden ist.

© 2000 DATAKOM AUSTRIA GMBH

2.1.5 Verpflichtungen von Signatoren

2.1.5.1 Allgemeine Verpflichtungen

Signatoren sind verpflichtet,

- für die Richtigkeit der angegebenen Daten im Rahmen der Registrierung Sorge zu tragen und
- die Verfahren zur Identifizierung und Authentifizierung gemäß der Richtlinien der a-sign *Premium* PCA bzw. der ausstellenden CA einzuhalten.

2.1.5.2 Schutz des privaten Schlüssels

Signatoren sind verpflichtet, den privaten Schlüssel zu schützen, d.h.

- ihn in geeigneter Weise zu verwahren (siehe Kapitel 6.2),
- die Weitergabe zu unterlassen und
- den Zugriff auf den privaten Schüssel soweit zumutbar zu verhindern.

2.1.5.3 Widerruf von Zertifikaten für Signatoren

Signatoren sind verpflichtet, die für sie ausgestellte Zertifikate zu widerrufen, falls

- der zugehörige private Schlüssel verloren geht,
- der Verdacht besteht, daß der zugehörige private Schlüssel kompromittiert wurde oder
- sich die im Zertifikat angeführten Daten geändert haben.

2.1.5.4 Sperre von Zertifikaten für Signatoren

Falls die in Kapitel 2.1.5.3 angeführten Gründe für einen erforderlichen Widerruf des Zertifikates noch nicht zweifelsfrei nachgewiesen sind und die ausstellende CA den Mechanismus des Sperrens von Zertifikaten unterstützt, so kann der Signator auch die Sperre seines Zertifikates beantragen. Hinweis: Der Mechanismus "Zertifikat sperren" wird zur Zeit nicht angeboten.

2.1.5.5 Anwendung privater Schlüssel bzw. ausgestellter Zertifikate

Natürlichen Personen ist es im Gegensatz zu Zertifizierungsdiensteanbietern untersagt, selbst Zertifikate auszustellen.

Zertifikate der Klasse *Premium* dürfen nur für den in der a-sign Policy Certificates *Premium* bzw. im CPS der ausstellenden CA festgelegten Zweck eingesetzt werden. Bei Zertifikaten der Klasse *Premium* ist jene Version der a-sign Policy Certificates *Premium* bzw. des CPS anzuwenden, die zum Zeitpunkt der Ausstellung des Zertifikates gültig war.

2.1.5.6 Digitales Signieren

Beim digitalen Signieren unter Verwendung eines zu einem Zertifikat der Klasse *Premium* gehörenden privaten Schlüssels ist die Einhaltung der in Kapitel 6.3 angeführten Punkte erforderlich, damit die erstellte digitale Signatur als sichere elektronische Signatur im Sinne des Österreichischen Signaturgesetzes und der auf seiner Grundlage ergangenen Verordnungen eingestuft werden kann.

2.1.6 Verpflichtungen Dritter

Bevor ein Zertifikat der Klasse *Premium* durch Dritte akzeptiert wird, sind diese dazu verpflichtet,

- die digitale Signatur des Zertifikates zu überprüfen,
- zu überprüfen, ob das Zertifikat abgelaufen ist,
- zu überprüfen, ob das Zertifikat widerrufen oder gesperrt wurde,

© 2000 DATAKOM AUSTRIA GMBH

- die Klasse und den Typ des Zertifikates zu identifizieren und
- zu überprüfen, ob das Zertifikat für den entsprechenden Zweck eingesetzt werden darf.

Bei der Überprüfung einer digitalen Signatur, die auf einem Zertifikat der Klasse *Premium* beruht, sind nur solche Signaturprüfeinheiten einzusetzen, die im Sicherheitskonzept der ausstellenden CA als geeignet bezeichnet sind. Insbesondere haben diese Signaturprüfeinheiten den im Österreichischen Signaturgesetz angeführten Kriterien zu genügen.

2.1.7 Verpflichtungen des a-sign Informationsdienstes

Der a-sign Informationsdienst ist verpflichtet, im Auftrag der a-sign PCA bzw. CAs die im Punkt 2.5 spezifizierten Informationen (Richtlinien, Zertifikatsverzeichnisse, Widerrufslisten, Sperrlisten und Informationen zur Unterrichtung von Signatoren) unter den dort angeführten Bedingungen und unter den im Kapitel 2.7 (Datenschutz) festgelegten Einschränkungen zu veröffentlichen.

2.2 Haftung

Jeder Zertifizierungsdiensteanbieter, der Zertifikate der Klasse *Premium* ausstellt, haftet gegenüber Personen, die diesen Zertifikaten vertrauen, dafür, daß

- alle im Zertifikat enthaltenen Angaben zum Zeitpunkt der Ausstellung des Zertifikates richtig waren,
- der private Schlüssel zum Zeitpunkt der Ausstellung des Zertifikates im Besitz des im Zertifikat angeführten Signators war und dem im Zertifikat angeführten öffentlichen Schlüssel komplementär entspricht,
- bei der Erzeugung und Speicherung des Zertifikates zulässige Komponenten und Verfahren eingesetzt wurden und
- ein erforderliches Widerrufen bzw. Sperren des Zertifikates vom Zertifizierungsdiensteanbieter unverzüglich durchgeführt wird.

Ein Zertifizierungsdiensteanbieter, der Zertifikate der Klasse *Premium* ausstellt, haftet nicht, falls er nachweisen kann, daß ihn an der Verletzung der oben angeführten Verpflichtungen keine Schuld trifft.

Ein Zertifizierungsdiensteanbieter, der Zertifikate der Klasse *Premium* ausstellt, hat die im Österreichischen Signaturgesetz und in den auf seiner Grundlage ergangenen Verordnungen angeführten Schritte zur Abdeckung des Haftungsrisikos durchzuführen.

2.3 Rechtliche Hinweise

2.3.1 Ausstellung eines Zertifikates der Klasse *Premium*

Eine CA kann einem Zertifikatswerber ohne Angabe von Gründen die Ausstellung eines Zertifikates der Klasse *Premium* verweigern, d.h. es besteht kein rechtlicher Anspruch auf die Ausstellung eines Zertifikates.

2.3.2 Verwendung eines Zertifikates der Klasse *Premium*

Die Verwendung einer digitalen Signatur, die auf einem Zertifikat der Klasse *Premium* beruht, ist im Rechts- und Geschäftsverkehr unter den Einschränkungen, die im Österreichischen Signaturgesetz und in den auf seiner Grundlage ergangenen Verordnungen enthalten sind, zulässig.

© 2000 DATAKOM AUSTRIA GMBH

2.3.3 Rechtswirkungen

Eine digitale Signatur, die auf einem Zertifikat der Klasse *Premium* beruht und bei deren Erstellung die in Kapitel 6.3 angegebenen Anforderungen für sichere elektronische Signaturen eingehalten wurden, besitzt die im Österreichischen Signaturgesetz angeführten Rechtswirkungen. Insbesondere ist eine derartige Signatur unter den dort angeführten Bedingungen einer eigenhändigen Unterschrift gleichgestellt.

2.4 Entgelte

Für

- die Ausgabe bzw. das Beziehen von Widerrufslisten (CRLs) bzw. Sperrlisten und
- die Veröffentlichung von a-sign Policies bzw. CPSs, ausgenommen Selbstkosten bei einer Ausgabe auf entsprechenden Medien,

sind von Zertifizierungsdiensteanbietern keine Entgelte einzuheben Die Entgelte für alle anderen Dienstleistungen sind vom entsprechenden Service-Anbieter festzulegen.

2.5 Veröffentlichungen

2.5.1 Allgemeines

Die in den nachfolgenden Kapiteln angeführten Veröffentlichungen (a-sign Richtlinien, Zertifikatsverzeichnisse, Widerrufslisten, Sperrlisten und Material zur Unterrichtung von Zertifikatswerbern) werden durch die a-sign PCA bzw. CAs veranlaßt und vom a-sign Informationsdienst durchgeführt. Diese Veröffentlichungen haben in geeigneter, für die Allgemeinheit jederzeit über öffentliche Telekommunikationsverbindungen zugänglicher Weise zu erfolgen.

Der a-sign Informationsdienst ist angehalten, dafür zu sorgen, daß er ohne Einschränkungen öffentlich und jederzeit zugänglich ist.

Der a-sign Informationsdienst ist unter folgender Webadresse erreichbar:

`http://a-sign.datakom.at/`

2.5.2 a-sign Richtlinien

Die a-sign PCA hat mit Hilfe des a-sign Informationsdienstes die a-sign Policy Certificates *Premium* sowie die CPSs aller untergeordneten CAs in der aktuellen und allen vorangegangenen Versionen zu veröffentlichen.

2.5.3 Zertifikatsverzeichnisse

Die a-sign PCA sowie alle CAs haben mit Hilfe des a-sign Informationsdienstes die von ihnen ausgestellten Zertifikate unter folgenden Bedingungen zu veröffentlichen:

- Die Veröffentlichungen müssen mit einer angemessenen zeitlichen Verfügbarkeit (d.h. zumindest während der Geschäftszeiten der ausstellenden PCA bzw. CA) betrieben werden.
- Die Veröffentlichungen müssen authentisch und unter Berücksichtigung der in Kapitel 2.7 (Datenschutz) getroffenen Einschränkungen erfolgen.
- Für jedes im Zertifikatsverzeichnis enthaltene Zertifikat ist der aktuelle Status anzugeben.
- Aus dem Zertifikatsverzeichnis muß der Zeitpunkt der Ausstellung aller angeführten Zertifikate bestimmt werden können.
- Zeitangaben in Zertifikatsverzeichnissen haben qualitätsgesichert zu erfolgen.

© 2000 DATAKOM AUSTRIA GMBH

- Zertifikate sind mindestens so lange in einem Zertifikatsverzeichnis zu führen, wie der im Zertifikat aufgeführte Algorithmus mit den dazugehörigen Parametern als geeignet beurteilt wird.
- Vom Verzeichnisdienst sind nur solche Formate zu verwenden, die vom Österreichischen Signaturgesetz und von den auf seiner Grundlage ergangenen Verordnungen als geeignet eingestuft werden.

2.5.4 Widerrufslisten (CRLs)

Die a-sign PCA sowie alle CAs haben mit Hilfe des a-sign Informationsdienstes widerrufene Zertifikate unter folgenden Bedingungen zu veröffentlichen:

- Widerrufene Zertifikate sind authentisch und in einer elektronisch jederzeit allgemein zugänglichen Form zu veröffentlichen.
- Die Veröffentlichung hat so zu erfolgen, daß der Zeitpunkt des Widerrufes eines Zertifikates bestimmt werden kann. Dieser Zeitpunkt des Widerrufes ist qualitätsgesichert anzuführen.
- Die Veröffentlichung der widerrufenen Zertifikate ist innerhalb der gesetzlich vorgegebenen Zeitspannen zu aktualisieren und hat den Zugriff in angemessener Zeit zuzulassen.
- Widerrufene Zertifikate sind so lange öffentlich zugänglich zu halten, bis die ursprüngliche Gültigkeitsdauer des Zertifikates überschritten ist.
- Vom Widerrufsdienst sind nur solche Formate zu verwenden, die vom Österreichischen Signaturgesetz und von den auf seiner Grundlage ergangenen Verordnungen als geeignet eingestuft werden.

2.5.5 Sperrlisten

Unterstützt eine CA neben dem Widerrufen von Zertifikaten zusätzlich den Mechanismus des Sperrens von Zertifikaten, so sind neben den widerrufenen auch die gesperrten Zertifikate zu veröffentlichen. Für diese Veröffentlichungen gelten zu Kapitel 2.5.4 analoge Bestimmungen.

2.5.6 Unterrichtung von Zertifikatswerbern

Zertifikatswerber sind über Themen im Zusammenhang mit Zertifikaten, digitalen Signaturen und ihrem privaten Schlüssel zu unterrichten. Die ausstellende CA hat daher Zertifikatswerbern schriftlich oder unter Verwendung eines dauerhaften Datenträgers entsprechendes Informationsmaterial zu den Themen

- Sicherheits- und Zertifizierungskonzept des Zertifizierungsdiensteanbieters, der die ausstellende CA betreibt,
- zulässige Verwendung des Zertifikates (Anwendungsbereich, Einschränkungen des Anwendungsbereiches, Obergrenze des zulässigen Transaktionswertes o.ä.),
- freiwillige Akkreditierung des Zertifizierungsdiensteanbieters, der die ausstellende CA betreibt, falls eine solche Akkreditierung erteilt wurde,
- besondere Streitbeilegungsverfahren,
- zulässige Komponenten und Verfahren zur Erzeugung und Überprüfung von digitalen Signaturen sowie deren Gültigkeitsdauer,
- Rechtswirkungen der vom Signator erzeugten digitalen Signaturen,
- Pflichten des Signators,
- Haftung des Zertifizierungsdiensteanbieters, der die ausstellende CA betreibt, und
- Handhabung der Hardware-Signaturerstellungseinheit (z.B. Chipkarte), auf der der private Schlüssel des Anwenders gespeichert ist,

zur Verfügung zu stellen.

© 2000 DATAKOM AUSTRIA GMBH

Auf Verlangen ist auch Dritten, die ein rechtliches Interesse glaubhaft machen, entsprechendes Informationsmaterial zu den Themen

- Sicherheits- und Zertifizierungskonzept des Zertifizierungsdiensteanbieters, der die ausstellende CA betreibt,
- zulässige Verwendung des Zertifikates (Anwendungsbereich, Einschränkungen des Anwendungsbereiches, Obergrenze des zulässigen Transaktionswertes o.ä.),
- freiwillige Akkreditierung des Zertifizierungsdiensteanbieters, der die ausstellenden CA betreibt, falls eine solche Akkreditierung erteilt wurde, und
- besondere Streitbeilegungsverfahren

zur Verfügung zu stellen.

2.6 Interne Prüfungen (Audits)

Um die Einhaltung jener Richtlinien, die in der a-sign Policy Certificates *Premium* sowie in den entsprechenden CPSs aller CAs enthalten sind, garantieren zu können, sind interne Prüfungen (Audits) durchzuführen.[2]

2.6.1 Überprüfte Einheiten der Zertifizierungsinfrastruktur

Im Rahmen dieser Überprüfungen sind alle Einheiten der a-sign Zertifizierungsinfrastruktur (PCA, CAs, GRAs, LRAs, Informationsdienst) zu kontrollieren.

2.6.2 Zeitpunkte und Frequenz der Audits

Die Überprüfungen sind vor Betriebsaufnahme der entsprechenden Einheit der a-sign Zertifizierungsinfrastruktur sowie nachfolgend mit der gesetzlich vorgesehenen Frequenz sowie bei sicherheitsrelevanten Veränderungen des Sicherheits- und Zertifizierungskonzeptes eines Zertifizierungsdiensteanbieters durchzuführen.

2.6.3 Identität und Qualifikation des Auditors

Die Überprüfungen sind von einer Kontrollinstanz durchzuführen, die von allen Zertifizierungsdiensteanbietern, die im Rahmen der a-sign Zertifizierungsinfrastruktur *Premium* CAs betreiben bzw. Zertifikate der Klasse *Premium* ausstellen, unabhängig ist.

2.6.4 Gegenstand der Audits

Der beauftragte Auditor hat zu überprüfen,

- ob die in der a-sign Policy Certificates *Premium* sowie in den CPSs der auditierten CAs enthaltenen Richtlinien mit den im Österreichischen Signaturgesetz und in den auf seiner Grundlage ergangenen Verordnungen enthaltenen Richtlinien für Anbieter qualifizierter Zertifikate konform sind, und
- ob sie von den Einheiten der Zertifizierungsinfrastruktur eingehalten werden.

2.6.5 Konsequenzen durchgeführter Audits

Aufgrund der Art und des Umfangs der identifizierten Schwachstellen kann der Auditor

- einem auditierten Zertifizierungsdiensteanbieter den Betrieb ganz untersagen,
- einem auditierten Zertifizierungsdiensteanbieter den Betrieb teilweise untersagen,

[2] Da die a-sign Policy Certificates *Premium* mit dem Ziel formuliert wurde, die gesetzeskonforme Ausgabe von qualifizierten Zertifikaten zu realisieren, ist mit einem erfolgreichen Audit gleichzeitig auch die Einhaltung jener Pflichten von Zertifizierungsdiensteanbietern für qualifizierte Zertifikate garantiert, die im Österreichischen Signaturgesetz und der auf seiner Grundlage ergangenen Verordnungen enthalten sind.

© 2000 DATAKOM AUSTRIA GMBH

- einem auditierten Zertifizierungsdiensteanbieter eine angemessene Frist zur Behebung aufgezeigter Mängel einräumen oder
- einem auditierten Zertifizierungsdiensteanbieter den Weiterbetrieb bis zum nächsten Audit gewähren.

2.6.6 Durchführung der Audits

Jede auditierte Einheit der a-sign Zertifizierungsinfrastruktur hat den im Auftrag des Auditors handelnden Personen das Betreten der Geschäfts- und Betriebsräume während der Geschäftszeiten zu gestatten, die in Betracht kommenden Unterlagen vorzulegen, Auskünfte zu erteilen und jede sonst erforderliche Unterstützung zu gewähren.

2.7 Datenschutz

Ein Zertifizierungsdiensteanbieter, der Zertifikate der Klasse *Premium* ausstellt, hat nur jene personenbezogenen Daten eines Signators zu verwenden, die er zur Durchführung seiner erbrachten Dienste benötigt. Diese Daten dürfen nur unmittelbar beim Betroffenen selbst oder mit seiner ausdrücklichen Zustimmung bei einem Dritten erhoben werden.

Bei Verwendung eines Pseudonyms hat ein Zertifizierungsdiensteanbieter, der Zertifikate der Klasse *Premium* ausstellt, die Daten über die Identität des Signators zu übermitteln, sofern an der Feststellung der Identität ein berechtigtes Interesse im Sinne des Österreichischen Datenschutzgesetzes besteht.

© 2000 DATAKOM AUSTRIA GMBH

3 Identifizierung, Authentifizierung

In diesem Kapitel wird dem Leser ein Überblick darüber gegeben, anhand welcher Merkmale Einheiten der Zertifizierungsinfrastruktur identifiziert werden und welche Authentifizierungsverfahren zulässig sind.

3.1 Erstregistrierung

3.1.1 Identifikationsmerkmale und Namenskonventionen

3.1.1.1 Zertifizierungsdiensteanbieter

Ein Zertifizierungsdiensteanbieter, der Zertifikate der Klasse *Premium* ausstellt, ist in Zertifikaten der Klasse *Premium* zumindest mit seinem unverwechselbaren Namen sowie mit dem Staat seiner Niederlassung anzuführen.

3.1.1.2 Natürliche Person

Ein Zertifikat der Klasse *Premium*, das für eine natürliche Person ausgestellt wurde, hat zumindest den Vor- und Nachnamen der Person oder ein Pseudonym, das als solches gekennzeichnet ist, zu enthalten. Im Falle der Verwendung eines Pseudonyms hat dieses weder anstößig noch offensichtlich zur Verwechslung mit Namen oder Kennzeichen geeignet zu sein.

3.1.2 Eindeutigkeit der Identifikationsmerkmale

Die in den Zertifikaten der Klasse *Premium* angeführten Identifikationsmerkmale müssen keinen eindeutigen Identifier des Signators (Sozialversicherungsnummer o.ä.) enthalten, d.h. der Signator muß nicht aufgrund dieser angeführten Merkmale eindeutig identifiziert werden können. Jede CA ist jedoch dazu berechtigt, für eine interne eindeutige Identifikation des Zertifikatswerbers zusätzliche Identifikationsmerkmale des Zertifikatswerbers zu erfassen.

3.1.3 Identitätsüberprüfung bei User-Zertifikaten

Die Identitätsüberprüfung vor der Ausgabe eines User-Zertifikates der Klasse *Premium* hat mittels des persönlichen Erscheinens des Zertifikatswerbers bei der CA bzw. bei einer von der CA autorisierten Registrierungsstelle (LRA) sowie anhand eines amtlichen Lichtbildausweises zu erfolgen.

3.1.4 Nachweis des Besitzes des privaten Schlüssels

Um ein Zertifikat der Klasse *Premium* erhalten zu können, hat der Zertifikatswerber den Besitz des privaten Schlüssels durch ein authentisches Verfahren nachzuweisen. Zusätzlich hat der Zertifikatswerber nachzuweisen, daß sich der private Schlüssel auf seiner Hardware-Signaturerstellungseinheit (z.B. Chipkarte) befindet.

3.2 Verlängerung der Gültigkeit von Zertifikaten für Signatoren

Das Verfahren zur Identifizierung bzw. Authentifizierung des Signators bei der Verlängerung der Gültigkeit eines Zertifikates ist zu jenem bei der Erstregistrierung identisch. Dieses Identifikations- bzw. Authentifikationsverfahren ist jedoch nicht notwendig, falls ein Antrag auf

© 2000 DATAKOM AUSTRIA GMBH

Verlängerung des Zertifikates vorliegt, der mit der sicheren elektronischen Signatur des Zertifikatswerbers versehen ist.

3.3 Widerruf von Zertifikaten für Signatoren

Vor der Durchführung des Widerruf eines Zertifikates der Klasse *Premium* ist die ausstellende CA dazu verpflichtet, mittels eines Authentisierungsverfahrens die Identität der Person, die den Widerruf beantragt hat, festzustellen.

3.4 Sperre von Zertifikaten für Signatoren

Unterstützt die ausstellende CA den Mechanismus des Sperrens von Zertifikaten, so ist die CA auch vor der Durchführung der Sperre eines Zertifikates der Klasse *Premium* dazu verpflichtet, mittels eines Authentisierungsverfahrens die Identität der Person, die die Sperre beantragt hat, festzustellen.

© 2000 DATAKOM AUSTRIA GMBH

4 Verfahrensanforderungen

Dieses Kapitel gibt dem Leser einen Überblick über jene Bestimmungen und Anforderungen, die sich für die Einheiten der a-sign Zertifizierungsinfrastruktur bei den einzelnen Verfahren im Rahmen der Zertifizierungsdienstleistungen ergeben.

4.1 Zertifizierung von *Premium* CAs

Die Zertifizierung einer *Premium* CA durch die übergeordnete a-sign PCA erfordert, daß

- die zu zertifizierende CA ein CPS definiert und der a-sign PCA vorlegt,
- das vorgelegte CPS von der a-sign PCA genehmigt wird,
- sich die zu zertifizierende CA einem Audit (siehe Kapitel 2.6) unterzieht und aufgrund des Ergebnisses dieses Audits die Aufnahme des Betriebes zulässig ist sowie
- ein schriftlicher Vertrag zwischen der zu zertifizierenden CA und der a-sign PCA geschlossen wird.

In dem oben angeführten Vertrag zwischen der CA und der a-sign PCA garantiert die CA die Einhaltung der in der a-sign Policy Certificates *Premium* sowie im eigenen CPS definierten Richtlinien.

4.2 Zertifizierung von natürlichen Personen

4.2.1 Beantragung eines Zertifikates

Das bei der Beantragung eines Zertifikates für natürliche Personen eingesetzte Verfahren hat die im Österreichischen Signaturgesetz und in den auf seiner Grundlage erlassenen Verordnungen enthaltenen Bestimmungen zu erfüllen. Insbesondere

- hat der Zertifikatswerber zur Abwicklung der Registrierung persönlich die CA oder eine von der CA autorisierte Registrierungsstelle (LRA) aufzusuchen,
- hat der Zertifizierungsdiensteanbieter die Feststellung der Identität des Zertifikatswerbers in der CA bzw. in der von der CA autorisierten Registrierungsstelle (LRA) anhand eines amtlichen Lichtbildausweises vorzunehmen,
- ist ein schriftlicher Antrag auf Ausstellung eines Zertifikates der Klasse *Premium* zu erstellen, der vom Zertifikatswerber eigenhändig zu unterzeichnen ist, und
- hat das eingesetzte Verfahren zu garantieren, daß der private Schlüssel des Zertifikatswerbers an eine geeignete Hardware-Signaturerstellungseinheit (siehe Kapitel 6.3.2) gebunden wird.

4.2.2 Ausstellung eines Zertifikates

- Das Ausstellen eines Zertifikates für eine natürliche Person hat unter Einhaltung der in den Kapiteln 5 und 6 definierten Sicherheitsanforderungen zu erfolgen.
- Der Zertifikatswerber ist bezüglich der durchgeführten Ausstellung seines Zertifikates, der Zertifikatinhalte und der Modalitäten der Zertifikatabholung zu informieren.
- Das ausgestellte Zertifikat darf erst nach einer erfolgreichen Authentifizierung des Zertifikatswerbers an diesen freigegeben werden.

© 2000 DATAKOM AUSTRIA GMBH

4.2.3 Entgegennehmen eines Zertifikates

Das Entgegennehmen eines Zertifikates impliziert das Akzeptieren der im entgegengenommenen Zertifikat enthaltenen Inhalte.

4.3 Verlängerung der Gültigkeit von Zertifikaten

4.3.1 Allgemeines

Es ist bis zum Ablauf der Gültigkeit eines Zertifikates zulässig, den Inhalt des Zertifikates (mit Ausnahme der Gültigkeitsdauer) neu zu zertifizieren und damit ein neues Zertifikat auszustellen, das sich auf dasselbe Schlüsselpaar bezieht. Für das Schlüsselpaar besteht daher (mit Ausnahme der auch im Kapitel 4.3.2 erwähnten Einschränkung bzgl. der Gültigkeit der bei der Erstellung, Speicherung und Anwendung des Schlüsselpaares eingesetzten technischen Komponenten und Verfahren) im Gegensatz zu Zertifikaten keine Beschränkung der Gültigkeitsdauer.

4.3.2 Durchführung der erneuten Zertifizierung

- Eine erneute Zertifizierung bezüglich eines Zertifikates der Klasse *Premium* im Sinne des Kapitels 4.3.1 ist nur zulässig, falls
  - sich die im Zertifikat enthaltenen Daten mit Ausnahme der Gültigkeitsdauer nicht geändert haben und
  - durch die Verlängerung die Gültigkeitsdauer der bei der Erstellung, Speicherung und Anwendung des Schlüsselpaares eingesetzten technischen Komponenten und Verfahren nicht überschritten wird.
- Die Gültigkeit der im Zertifikat enthaltenen Angaben ist von der CA bzw. der von der CA autorisierten Registrierungsstelle (GRA, LRA) analog zu dem Verfahren im Rahmen der Erstregistrierung erneut zu prüfen.

- Eine erneute Zertifizierung eines Schlüsselpaares eines widerrufenen Zertifikaten ist ausgeschlossen.

4.4 Überprüfung der Gültigkeit von Zertifikaten

Der a-sign Informationsdienst hat eine Online-Überprüfung des Status von Zertifikaten der Klasse *Premium* zur Verfügung zu stellen (siehe Kapitel 2.5.3).

4.5 Widerruf von Zertifikaten

4.5.1 Allgemeines

- Jeder Zertifizierungsdiensteanbieter, der Zertifikate der Klasse *Premium* ausstellt, hat den Signatoren geeignete Kommunikationsmöglichkeiten bekanntzugeben, mit denen diese jederzeit einen unverzüglichen Widerruf ihres Zertifikates veranlassen können.
- Der Widerrufsdienst hat mit einer angemessenen zeitlichen Verfügbarkeit betrieben zu werden, die zumindest während der Geschäftszeiten des Zertifizierungsdiensteanbieters gegeben sein muß.

© 2000 DATAKOM AUSTRIA GMBH

- Ein Widerruf muß den Zeitpunkt, ab dem er wirksam wird, enthalten. Der Widerruf ist ab dem Zeitpunkt des Eintragens des Widerrufs im entsprechenden Verzeichnis wirksam. Ein rückwirkender Widerruf von Zertifikaten ist nicht möglich.
- Ein Signator ist von einem erfolgten Widerruf bzgl. seines Zertifikates zu verständigen.
- Der Widerruf eines Zertifikates kann nicht rückgängig gemacht werden.

4.5.2 Gründe für den Widerruf eines Zertifikates

Ein Zertifizierungsdiensteanbieter, der Zertifikate der Klasse *Premium* ausstellt, hat ein Zertifikat unverzüglich zu widerrufen, falls

- der Signator dies verlangt,
- ein Auditor dies aufgrund des Resultats eines Audits (siehe Kapitel 2.6) anordnet,
- die im Zertifikat angeführten Angaben nicht mehr zutreffen,
- der Zertifizierungsdiensteanbieter Kenntnis vom Ableben des Signators erlangt,
- das Zertifikat aufgrund unrichtiger Angaben erwirkt wurde,
- die ausstellende CA ihre Tätigkeit einstellt und der Widerrufsdienst nicht von einem anderen Zertifizierungsdiensteanbieter übernommen wird,
- der zugehörige private Schlüssel verloren gegangen ist,
- der Diebstahl des privaten Schlüssels vermutet werden muß oder erfolgt ist,
- ein unbefugter Zugriff auf den privaten Schlüssel vermutet werden muß oder erfolgt ist,
- sich der Signator nicht an die mit dem Zertifikat verknüpften Bedingungen hält,
- der private Schlüssel des Signators öffentlich bekannt wird oder
- der private Schlüssel des Signators außer beim Signator ein weiteres Mal als privater Schlüssel vorkommt.

4.5.3 Zum Widerruf Berechtigte

Der Widerruf eines Zertifikates kann jederzeit und ohne Angabe von Gründen durch den Zertifizierungsdiensteanbieter, der die ausstellende CA betreibt, sowie durch den Besitzer des Zertifikates selbst erfolgen.

4.5.4 Verfahren zur Beantragung eines Widerrufs

Ein Zertifizierungsdiensteanbieter, der Zertifikate der Klasse *Premium* ausstellt, hat im CPS der zugehörigen CA die zulässigen Verfahren zur Beantragung eines Widerrufs zu spezifizieren. Bei der Spezifikation dieser Verfahren ist zu berücksichtigen, daß

- die CA dazu verpflichtet ist, vor der Durchführung des Widerrufs eines Zertifikates der Klasse *Premium* mittels eines Authentisierungsverfahrens die Identität der Person, die den Widerruf beantragt hat, festzustellen (siehe Kapitel 3.3) und
- sich unter den von einer CA in ihrem CPS als zulässig spezifizierten Authentifizierungsverfahren zumindest eine Variante zu befinden hat, die die Beantragung des Widerrufs eines Zertifikates der Klasse *Premium* in Papierform zuläßt.

4.5.5 Veröffentlichung widerrufener Zertifikate

Widerrufe von Zertifikaten der Klasse *Strong* sind in Form von Widerrufslisten (CRLs) unter Einhaltung der in Kapitel 2.5.4 angeführten Bestimmungen zu veröffentlichen.

© 2000 DATAKOM AUSTRIA GMBH

4.6 Sperre von Zertifikaten

Zertifizierungsdiensteanbieter, die *Zertifikate* der Klasse *Premium* ausgeben, sind dazu berechtigt, zusätzlich zum Mechanismus des Widerrufens eines Zertifikates auch den Mechanismus des Sperrens eines Zertifikates (siehe Kapitel 9.1) anzubieten und zu unterstützen. Für das Sperren eines Zertifikates sowie die Veröffentlichung gesperrter Zertifikate gelten die zum Widerrufen von Zertifikaten analogen Bestimmungen.

4.7 Schlüsselaustausch

Ein Schlüsselaustausch (siehe Kapitel 9.1) ist ausschließlich durch Beantragung eines neuen Zertifikates (siehe Kapitel 4.2.1) möglich.

4.8 Dokumentation

4.8.1 Allgemeines

Ein Zertifizierungsdiensteanbieter, der Zertifikate der Klasse *Premium* ausstellt, hat alle maßgeblichen Umstände über ein Zertifikat der Klasse *Premium* aufzuzeichnen, sodaß (vor allem in gerichtlichen Verfahren) die Zertifizierung nachgewiesen werden kann. Insbesondere sind das Ausstellen, Ausgeben, Verlängern, Widerrufen und Sperren von Zertifikaten sowie Störfälle und besondere Betriebssituationen zu dokumentieren.

4.8.2 Durchführung der Archivierung

Die Dokumentation hat derart zu erfolgen, daß die Daten und ihre Unverfälschtheit sowie der Zeitpunkt ihrer Aufnahme in das Protokollierungssystem jederzeit nachprüfbar sind. Die Dokumentation hat in elektronischer Form vorzuliegen, ist mit der sicheren elektronischen Signatur des Zertifizierungsdiensteanbieters zu versehen und hat qualitätsgesicherte Zeitangaben zu enthalten.

Die Daten sind über den gesetzlich vorgeschriebenen Zeitraum aufzubewahren und innerhalb dieses Zeitraums verfügbar zu halten und vor Verlust und Beschädigung zu schützen.

4.9 Ausnahmesituationen bezüglich eines privaten CA-Schlüssels

4.9.1 Verlust eines privaten CA-Schlüssels

Ist der private Schlüssel einer *Premium* CA verloren gegangen, ohne daß eine Kompromittierung erfolgte oder vermutet werden muß, so sind folgende Maßnahmen durchzuführen:

- Setzt die betroffene *Premium* CA den Betrieb mit einem neuen privaten Schlüssel fort, so ist analog zu Kapitel 4.9.2 (Austausch eines privaten CA-Schlüssels) vorzugehen.
- Stellt die betroffene *Premium* CA hingegen ihren Betrieb ein, so ist analog zu Kapitel 4.10 (Einstellen des Betriebes einer CA) vorzugehen.

4.9.2 Austausch eines privaten CA-Schlüssels

Die Vorgangsweise beim Auslaufen der Gültigkeit des privaten Schlüssels einer *Premium* CA und einem somit notwendig gewordenen Schlüsselaustausch ist von der betroffenen CA in ihrem CPS festzulegen.

© 2000 DATAKOM AUSTRIA GMBH

4.9.3 Kompromittierung eines privaten CA-Schlüssels

Die Vorgangsweise nach einer vermuteten oder erfolgten Kompromittierung des privaten Schlüssels einer *Premium* CA ist von der betroffenen CA in ihrem CPS festzulegen. Diese Vorgangsweise hat zumindest

- das Informieren jedes Inhabers eines gültigen, von der CA mit dem kompromittierten Schlüssel signierten Zertifikates, das Informieren jeder cross-zertifizierenden CA, jeder cross-zertifizierten CA sowie der a-sign PCA,
- den Widerruf des für die CA ausgestellten Zertifikates durch die a-sign PCA,
- das Generieren eines neuen Schlüsselpaares und die Ausstellung eines neuen CA-Zertifikates,
- den Widerruf aller Zertifikate für Signatoren, die mit dem kompromittierten Schlüssel signiert wurden, sowie das Informieren der betroffenen Signatoren und
- die Sicherstellung der Fortsetzung der authentischen Veröffentlichung von Zertifikatsverzeichnissen, Widerrufslisten und Sperrlisten

zu umfassen.

4.10 Einstellen des Betriebes einer CA

Die Vorgangsweise im Falle der Einstellung der Tätigkeit einer *Premium* CA ist von der betroffenen CA in ihrem CPS festzulegen. Diese Vorgangsweise hat zumindest

- das Informieren jedes Inhabers eines gültigen, von der CA ausgestellten Zertifikates, das Informieren jeder cross-zertifizierenden CA, jeder cross-zertifizierten CA sowie der a-sign PCA,
- die öffentliche Ankündigung der geplante Einstellung in geeigneter Form,
- den Widerruf des für die CA ausgestellten Zertifikates durch die a-sign PCA sowie
- die Sicherstellung der Fortsetzung der authentischen Veröffentlichung von Zertifikatsverzeichnissen, Widerrufslisten und Sperrlisten durch andere Einheiten der a-sign Zertifizierungsinfrastruktur bzw. andere Zertifizierungsdiensteanbieter oder (falls diese Fortsetzung nicht möglich ist) den Widerruf aller zum Zeitpunkt der Terminierung noch gültigen Zertifikate für Signatoren und das Informieren der betroffenen Signatoren

zu umfassen.

© 2000 DATAKOM AUSTRIA GMBH

5 Infrastrukturelles, organisatorisches und personelles Sicherheitskonzept

Dieses Kapitel beschreibt alle Sicherheitsanforderungen an die CAs, GRAs, LRAs und Signatoren (ausgenommen technische Sicherheitsanforderungen). Damit soll eine zuverlässige und vertrauenswürdige Abwicklung der Schlüsselgenerierung, Authentifizierung, Ausstellung von Zertifikaten, des Widerrufes oder Sperrens von Zertifikaten sowie der Audit- und Archivierungsvorgänge gewährleistet und vor allem ein Mißbrauch von privaten Schlüsseln verhindert werden.

Jede *Premium* CA ist verpflichtet, in ihrem CPS ein Sicherheitskonzept zu definieren, das die in den Kapiteln 5 und 6 behandelten Aspekte abdeckt und als Grundlage für Kontrollen (Audits) herangezogen wird.

5.1 Infrastrukturelle Sicherheitsmaßnahmen

5.1.1 *Premium* CAs

Die IT-Ausstattung für den Betrieb einer *Premium* CA muß in eigenen dafür tauglichen Räumlichkeiten untergebracht sein. Es muß gewährleistet sein, daß sich unbefugte Personen nicht Zutritt zu diesen Räumlichkeiten verschaffen können.

Die IT-Ausstattung muß durch geeignete Maßnahmen störungsfrei betrieben werden können. Dies beinhaltet insbesondere eine zuverlässige Stromversorgung sowie einen ausreichenden Feuerschutz.

Speichermedien müssen so aufbewahrt werden, daß diese vor unbefugtem Zugriff, Manipulation sowie physischer Beschädigung geschützt sind. Zusätzlich sollten CA-externe Speichermedien eingerichtet werden.

Zur Aufbewahrung von schützenswertem Schlüsselmaterial sind entsprechende Schlüsselbehältnisse einzurichten.

Für Hardware-Authentifizierungseinheiten (z.B. Chipkarten) zur Authentifizierung des Personals sowie für schriftliche oder elektronische Aufzeichnungen, die im Zuge der durchzuführenden Protokollierungs- und Archivierungsaufgaben anfallen, sind geeignete Aufbewahrungsmöglichkeiten vorzusehen.

5.1.2 GRAs

Jede einer *Premium* CA unterstellte GRA hat für Hardware-Authentifizierungseinheiten (z.B. Chipkarten) zur Authentifizierung des Personals sowie für schriftliche oder elektronische Aufzeichnungen, die im Zuge der durchzuführenden Protokollierungs- und Archivierungsaufgaben anfallen, geeignete Aufbewahrungsmöglichkeiten vorzusehen.

5.1.3 LRAs

Jede einer *Premium* CA unterstellte LRA hat zu Kapitel 5.1.2 analoge infrastrukturelle Sicherheitsmaßnahmen zu treffen.

© 2000 DATAKOM AUSTRIA GMBH

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 *Premium* CAs

Durch die genaue Definition und Überwachung der Berechtigungen der einzelnen Mitarbeiter in einer *Premium* CA ist zu verhindern, daß eine Person unberechtigt Schlüssel generiert, zertifiziert, verwendet oder vernichtet bzw. daß Zertifikatsverzeichnisse, Widerrufslisten oder Sperrlisten von Unbefugten verändert werden können.

Jede CA hat die authentische Protokollierung und Archivierung von Registrierungsdaten, Zertifizierungsdaten und Ereignissen durchzuführen, um die Nachprüfbarkeit von Daten und Abläufen jederzeit zu gewährleisten (siehe Kapitel 4.8).

Es ist organisatorisch zu gewährleisten, daß der private Schlüssel der CA nicht von einer einzigen Person allein generiert werden kann.

Alle Rechnersysteme, die zur Durchführung der diversen Zertifizierungsdienstleistungen eingesetzt werden, sind ausschließlich für diese Zwecke zu verwenden.

Stellt der Zertifizierungsdiensteanbieter neben Zertifikaten der Klasse *Premium* auch Zertifikate anderer Klassen aus, so ist der bei der Signatur von Zertifikaten der Klasse *Premium* ein anderer privater Schlüssel einzusetzen als bei der Signatur eines Zertifikates einer anderen Klasse.

5.2.2 GRAs

Jede einer *Premium* CA unterstellte GRA hat den Zugriff auf die verwendeten Rechnersysteme durch Unbefugte mittels entsprechender organisatorischer Maßnahmen zu unterbinden. Dies schließt insbesondere ein, daß sich die in der GRA arbeitenden Bediensteten (GRA-Operatoren) geeignet authentifizieren müssen.

Alle Rechnersysteme, die zum Bearbeiten von Registrierungsdaten eingesetzt werden, sind ausschließlich für diese Zwecke zu verwenden.

5.2.3 LRAs

Jede einer *Premium* CA unterstellte LRA hat den Zugriff auf die verwendeten Rechnersysteme durch Unbefugte mittels entsprechender organisatorischer Maßnahmen zu unterbinden. Dies schließt insbesondere ein, daß sich die in der LRA arbeitenden Bediensteten (LRA-Operatoren) geeignet authentifizieren müssen.

5.2.4 Signatoren

Die Signatoren haben durch Einhaltung der in Kapitel 2.1.5 angeführten organisatorischen Maßnahmen den sicheren Einsatz von Zertifikaten der Klasse *Premium* und der entsprechenden privaten Schlüssel sicherzustellen.

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 *Premium* CAs

Für den Betrieb einer *Premium* CA ist zuverlässiges Personal mit den für die bereitgestellten Dienste erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen, insbesondere mit Managementfähigkeiten sowie mit Kenntnissen der Technologie digitaler Signaturen und angemessener Sicherheitsverfahren, zu beschäftigen.

Einer *Premium* CA ist die Beschäftigung von Mitarbeitern, deren Vertrauenswürdigkeit aufgrund strafbarer Handlungen in der Vergangenheit nicht gegeben ist, untersagt.

© 2000 DATAKOM AUSTRIA GMBH

5.3.2 GRAs

Für den Betrieb einer GRA, die einer *Premium* CA unterstellt ist, ist zuverlässiges Personal mit den für die bereitgestellten Dienste erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen zu beschäftigen.

Einer GRA, die einer *Premium* CA unterstellt ist, ist die Beschäftigung von Mitarbeitern, deren Vertrauenswürdigkeit aufgrund strafbarer Handlungen in der Vergangenheit nicht gegeben ist, untersagt.

5.3.3 LRAs

Eine LRA, die einer *Premium* CA unterstellt ist, hat Personal zu beschäftigen, das den zu Kapitel 5.3.2 analogen Kriterien entspricht.

© 2000 DATAKOM AUSTRIA GMBH

6 Technisches Sicherheitskonzept

In diesem Kapitel werden alle technischen Sicherheitsanforderungen an CAs, GRAs, LRAs, Signatoren, Dritte und den Informationsdienst definiert.

6.1 Generierung des privaten Schlüssels

6.1.1 Generierung des privaten Schlüssels einer CA

Bei der Generierung des privaten Schlüssels einer *Premium* CA ist durch die Verwendung geeigneter technischer Komponenten und Verfahren zu gewährleisten, daß

- die unbefugte Verwendung des privaten Schlüssels der CA verläßlich verhindert wird,
- der private Schlüssel der CA nicht von einer Person allein generiert werden kann sowie
- der private Schlüssel der CA in einer eigenen Signaturerstellungseinheit erzeugt wird und diese nicht verläßt.

Darüber hinaus sind auch bei der Generierung des privaten Schlüssels einer CA die im Kapitel 6.1.2.1 angeführten Anforderungen zu erfüllen.

6.1.2 Generierung des privaten Schlüssels einer natürlichen Person

6.1.2.1 Allgemeines

Die privaten Schlüssel für natürliche Personen sowie die bei der Generierung eingesetzten Verfahren haben die im Österreichischen Signaturgesetz und in den auf seiner Grundlage ergangenen Verordnungen angegebenen Kriterien (Mindestlänge der Schlüssel, verwendete Zufallsmechanismen, Wahrscheinlichkeit für identische Schlüsselwerte usw.) zu erfüllen.

6.1.2.2 Generierung durch den Zertifizierungsdiensteanbieter

Wird der private Schlüssel einer natürlichen Person nicht von der natürlichen Person selbst, sondern vom einem Zertifizierungsdiensteanbieter generiert, so hat der Zertifizierungsdiensteanbieter Vorkehrungen dafür zu treffen, daß der private Schlüssel

- während und nach seiner Generierung weder vom Zertifizierungsdiensteanbieter noch von Dritten gespeichert, kopiert oder verwendet werden kann,
- ausschließlich an die entsprechende natürliche Person ausgehändigt wird und
- bei der Aushändigung an die entsprechende natürliche Person weder vom Zertifizierungsdiensteanbieter noch von Dritten gespeichert oder kopiert werden kann.

6.1.2.3 Generierung durch die natürliche Person

Wird der private Schlüssel nicht vom Zertifizierungsdiensteanbieter, sondern in der Hardware-Signaturerstellungseinheit der natürlichen Person erzeugt, so hat der Zertifizierungsdiensteanbieter für die Erzeugung sowie für die Speicherung des privaten Schlüssels nur technisch geeignete Hardware-Signaturerstellungseinheiten (siehe Kapitel 6.3.2) bereitzustellen oder zu empfehlen.

© 2000 DATAKOM AUSTRIA GMBH

6.2 Schutz des privaten Schlüssels

6.2.1 Schutz des privaten Schlüssels einer CA

- Für die Speicherung des privaten Schlüssels einer *Premium* CA sind solche technischen Komponenten und Verfahren einzusetzen, die dessen Bekanntwerden und unbefugte Verwendung verläßlich verhindern.
- Das Duplizieren des privaten Schlüssels nach dessen Erzeugung ist untersagt.
- Jede *Premium* CA hat zusätzlich dafür zu sorgen, daß jede Aktivierung ihres privaten Schlüssels nachvollziehbar ist und authentisch protokolliert wird.

6.2.2 Schutz des privaten Schlüssels einer natürlichen Person

- Der private Schlüssel ist auf einer Hardware-Signaturerstellungseinheit (z.B. Chipkarte) zu speichern. Diese Signaturerstellungseinheit hat auch die Erstellung einer sicheren elektronischen Signatur zu ermöglichen und das Bekanntwerden und die unbefugte Verwendung des privaten Schlüssels verläßlich zu verhindern (siehe Kapitel 6.3).
- Das Duplizieren des privaten Schlüssels nach dessen Erzeugung ist untersagt.

6.3 Erstellung einer sicheren elektronischen Signatur

6.3.1 Allgemeines

Um zu erreichen, daß eine digitale Signatur, die auf einem Zertifikat der Klasse *Premium* beruht, als sichere elektronische Signatur im Sinne des Österreichischen Signaturgesetzes und der auf seiner Grundlage ergangenen Verordnungen eingestuft wird, hat ein Signator bei der Erstellung der digitalen Signatur die nachfolgenden Anforderungen zu erfüllen:

- Die Eignung der verwendeten technischen Komponenten und Verfahren hat von einer unabhängigen Institution bestätigt zu werden. Insbesondere haben die verwendeten technischen Komponenten und Verfahren
  - die vollständige Anzeige der zu signierenden Daten zu ermöglichen,
  - sicherzustellen, daß die signierten Daten nicht verändert werden und
  - die unbefugte Verwendung des privaten Schlüssels zuverlässig zu verhindern.
- Die eingesetzten Algorithmen und Signaturformate müssen vom Österreichischen Signaturgesetz und von den auf seiner Grundlage ergangenen Verordnungen als geeignet eingestuft werden und im Sicherheitskonzept des entsprechenden Zertifizierungsdiensteanbieters genannt sein.

6.3.2 Anforderungen an die Hardware-Signaturerstellungseinheit

Ist der Signator eine natürliche Person, so hat die Hardware-Signaturerstellungseinheit, auf der der privater Schlüssel gespeichert ist und die zur Erstellung der digitalen Signatur verwendet wird, die im Österreichischen Signaturgesetz und in den auf seiner Grundlage ergangenen Verordnungen angegebenen Kriterien zu erfüllen. Insbesondere ist der Zugriff auf die Hardware-Signaturerstellungseinheit durch eine erforderliche Autorisierung des Signators (PIN-Eingabe, Fingerabdruck o.ä.) zu schützen.

© 2000 DATAKOM AUSTRIA GMBH

6.4 Überprüfung einer digitalen Signatur

Für die Überprüfung von Daten, die unter der Verwendung eines Zertifikates der Klasse *Premium* sicher signiert wurden, sind von Zertifizierungsdiensteanbietern und natürlichen Personen solche technischen Komponenten und Verfahren zu verwenden, die sicherstellen, daß

- die signierten Daten nicht verändert worden sind,
- die Signatur zuverlässig überprüft und das Ergebnis dieser Überprüfung korrekt angezeigt wird,
- der Überprüfer feststellen kann, auf welche Daten sich die digitale Signatur bezieht,
- der Überprüfer feststellen kann, wem die digitale Signatur zugeordnet ist, wobei die Verwendung eines Pseudonyms angezeigt werden muß, und
- sicherheitsrelevante Veränderungen der signierten Daten erkannt werden können.

6.5 Erstellung und Speicherung eines Zertifikates der Klasse *Premium*

Bei der Erstellung und Speicherung eines Zertifikates der Klasse *Premium* sind solche technischen Komponenten und Verfahren einzusetzen, die die Fälschung und Verfälschung der Zertifikate zuverlässig verhindern.

6.6 Technische Komponenten und Verfahren eines Zertifizierungsdiensteanbieters

6.6.1 Dokumentation

Sämtliche von einem Zertifizierungsdiensteanbieter eingesetzten technischen Komponenten und Verfahren sind entsprechend ihrem aktuellen Stand und auf nachprüfbare Weise zu dokumentieren.

6.6.2 Schutz der technischen Komponenten

Jeder Zertifizierungsdiensteanbieter hat Vorkehrungen zu treffen, die die zum Erstellen der Zertifikate und zum Abrufbarhalten der Verzeichnis- und Widerrufsdienste eingesetzten technischen Komponenten vor Kompromittierung und unbefugtem Zugriff schützen.

6.6.3 Prüfung der technischen Komponenten und Verfahren für qualifizierte Zertifikate und sichere elektronische Signaturen

Zur Prüfung der technischen Komponenten und Verfahren sind ausschließlich solche Sicherheitsprofile und Kriterien heranzuziehen, die vom Österreichischen Signaturgesetz und von den auf seiner Grundlage ergangenen Verordnungen als geeignet eingestuft werden.

6.6.4 Weitere Anforderungen an technische Komponenten und Verfahren

Jeder Zertifizierungsdiensteanbieter hat durch entsprechende Sicherheitsmaßnahmen sicherzustellen, daß die Übertragung von Daten zwischen Einheiten, die organisatorisch und technisch getrennt geführt werden, nicht zu einer Kompromittierung der Signatur- oder Zertifizierungsdienste führt.

6.7 Gültigkeitsdauer von Zertifikaten

Die Gültigkeitsdauer eines Zertifikates der Klasse *Premium* darf

- die im Österreichischen Signaturgesetz und in den auf seiner Grundlage ergangenen Verordnungen festgelegte Höchstgrenze für qualifizierte Zertifikate (3 Jahre) sowie
- den Zeitraum der Eignung der bei der Erstellung, Speicherung und Anwendung eingesetzten technischen Komponenten und Verfahren

nicht überschreiten.

7 Zertifikats- und CRL-Profil

In diesem Kapitel wird das Profil der ausgegebenen Zertifikate und Widerrufslisten (CRLs) definiert.

7.1 Profil der ausgegebenen Zertifikate

7.1.1 Zulässige Formate

Zertifikate der Klasse *Premium* sind ausschließlich in den vom Österreichischen Signaturgesetz und von den auf seiner Grundlage ergangenen Verordnungen als geeignet angeführten Formaten auszugeben.

7.1.2 Mindestinhalte

Zertifikate der Klasse *Premium* haben alle zur Einstufung als qualifiziertes Zertifikat im Sinne des Österreichischen Signaturgesetzes und der auf seiner Grundlage ergangenen Verordnungen erforderlichen Angaben, insbesondere

- die Information darüber, daß es sich um ein qualifiziertes Zertifikat handelt,
- die in Kapitel 3.1.1 angegebenen Identifikationsmerkmale des Zertifikatinhabers (CA oder natürliche Person) unter Berücksichtigung der dort angeführten Namenskonventionen,
- den öffentlichen Schlüssel,
- den Beginn und das Ende der Gültigkeit des Zertifikates sowie
- gegebenenfalls die Information darüber, daß der Zertifizierungsdiensteanbieter als Aussteller qualifizierter Zertifikate akkreditiert wurde,

zu enthalten. Zusätzlich sind im Zertifikat

- Informationen über die anzuwendende Policy bzw. das anzuwendende CPS und
- Informationen über den Typ des Inhabers des Zertifikates (CA oder natürliche Person),

anzuführen.

Die detaillierte Spezifikation der in einem Zertifikat der Klasse *Premium* enthaltenen Inhalte ist von der ausstellenden *Premium* CA in ihrem CPS anzuführen.

7.1.3 Weitere Anforderungen

Ein Zertifikat der Klasse *Premium* ist mit der sicheren elektronischen Signatur der ausstellenden Zertifizierungsinstanz zu versehen.

Jeder Zertifizierungsdiensteanbieter, der Zertifikate der Klasse *Premium* ausstellt, hat in den ausgestellten Zertifikaten qualitätsgesicherte Zeitangaben zu verwenden.

7.2 Profil der ausgegebenen Widerrufslisten (CRLs)

Widerrufslisten (CRLs) sind ausschließlich in den vom Österreichischen Signaturgesetz und von den auf seiner Grundlage ergangenen Verordnungen als geeignet angeführten Formaten auszugeben. Die detaillierte Spezifikation der in den Widerrufslisten (CRLs) enthaltenen Inhalte ist von der entsprechenden *Premium* CA in ihrem CPS anzuführen.

© 2000 DATAKOM AUSTRIA GMBH

8 Administration der Policy

In diesem Kapitel werden Richtlinien zur Durchführung von Änderungen an der a-sign Policy Certificates *Premium* definiert.

8.1 Durchführung der Änderungen

8.1.1 Allgemeines

Die a-sign Policy Certificates *Premium* wird von einer a-sign Expertengruppe entwickelt, die sich aus den Bereichen Technik, Wirtschaft und Rechtswissenschaften zusammensetzt.

8.1.2 Erforderliche Schritte

- Änderungsvorschläge zur aktuellen Version der a-sign Policy Certificates *Premium* müssen zunächst der Expertengruppe in schriftlicher Form übermittelt werden.
- Die eingebrachten Änderungsvorschläge werden in der Policy-Expertengruppe behandelt und verabschiedet.
- Vor der Herausgabe der geänderten a-sign Policy Certificates *Premium* muß das Anerkennungsverfahren für a-sign Policies durchlaufen werden. Dabei werden die von der Expertengruppe verabschiedeten Änderungsvorschläge dem a-sign Plenary übermittelt. Dieses Plenary hat einen Monat Zeit, um die Vorschläge zu begutachten. Sollten innerhalb dieser Frist Einwände ausbleiben, wird die geänderte Policy in einem Plenary-Meeting verabschiedet.

8.2 Veröffentlichung geänderter Policies

Jede neue Version der a-sign Policy Certificates *Premium* ist vom Informationsdienst zu veröffentlichen.

© 2000 DATAKOM AUSTRIA GMBH

9 Anhang

9.1 Definitionen

Antragsteller: siehe → Zertifikatswerber

Aussteller: siehe → Zertifizierungsdiensteanbieter

authentifizieren: beglaubigen, die Echtheit bezeugen

authentisch: echt

Authentizität: Echtheit einer Schrift, Urkunde

Certificate Revocation List (CRL): siehe → Widerrufsliste

Certification Authority (CA): Einheit der Zertifizierungshierarchie, die andere Certification Authorities sowie natürliche Personen zertifizieren kann

Certification Practice Statement (CPS): verbindliches Dokument, in dem das Vorgehen einer bestimmten Certification Authority bei Zertifizierungen sowie technische und organisatorische Anforderungen an die zugeordneten Einheiten der Zertifizierungshierarchie definiert sind

Common Name (CN): Name von Personen, Organisationen

Cross-Zertifikat: Zertifikat, mit dem eine Certification Authority einer anderen Hierarchie zertifiziert wird; erfordert Kompatibilität der Policies

Digitale Signatur: Ein eindeutiger Extrakt eines elektronischen Dokumentes wird mit dem privaten Schlüssel des Signierenden verschlüsselt**.** Mit dem dazugehörigen öffentlichen Schlüssel kann verifiziert werden, daß das elektronische Dokument vom Besitzer des privaten Schlüssels digital signiert wurde und daß das Dokument nicht nachträglich verändert wurde.

Distinguished Name (DN): eindeutiger, unverwechselbarer Name

Dritter: Person, die eine digitale Signatur empfängt oder dem Zertifikat eines anderen Signators vertraut

Elektronische Signatur: elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Feststellung der Identität des Signators dienen (siehe auch → sichere elektronische Signatur)

Global Registration Authority (GRA): siehe → Globale Registrierungsstelle

Globale Registrierungsstelle: ist einer Certification Authority zugeordnet und mit zentralen Registrierungs- und Archivierungsaufgaben betraut

Hardware-Signaturerstellungseinheit: Hardware-Einheit, die als Signaturerstellungseinheit eingesetzt wird (siehe auch: → Signaturerstellungseinheit)

Kompromittierung des privaten Schlüssels: Der private Schlüssel ist zeitweise oder permanent für Unbefugte zugänglich.

Local Registration Authority (LRA): siehe → Lokale Registrierungsstelle

Lokale Registrierungsstelle: führt im Auftrag einer Certification Authority die Überprüfung der Identität eines Zertifikatswerbers entsprechend der Policy einer Zertifikatsklasse durch

© 2000 DATAKOM AUSTRIA GMBH

Öffentlicher Schlüssel: Teil des Schlüsselpaares, der zum Verschlüsseln von Nachrichten und Dokumenten sowie zum Prüfen von digitalen Signaturen dient und weitergegeben werden kann bzw. veröffentlicht wird; ist Bestandteil eines Zertifikates (siehe auch: → Privater Schlüssel)

Policy: Zertifizierungsrichtlinien, die von den a-sign Primary Certification Authorities für jede Zertifikatsklasse ausgegeben werden

Primary Certification Authority (PCA): Certification Authority, die nur andere Certification Authorities zertifiziert; diese zertifizierten Certification Authorities müssen der entsprechenden Policy der PCA unterliegen

Private Key: siehe → Privater Schlüssel

Privater Schlüssel: Teil des Schlüsselpaares, der zum digitalen Signieren sowie zum Entschlüsseln von Nachrichten und Dokumenten erforderlich ist und geheimgehalten werden muß (siehe auch: → Öffentlicher Schlüssel)

Public Key: siehe → Öffentlicher Schlüssel

Public Key Infrastructure (PKI): siehe → Zertifizierungshierarchie

Qualifiziertes Zertifikat: Zertifikat, das bestimmte, im Österreichischen Signaturgesetz festgelegte Angaben enthält und von einem Zertifizierungsdiensteanbieter ausgestellt wird, der bestimmten, im Österreichischen Signaturgesetz und in den auf seiner Grundlage ergangenen Verordnungen angegebenen Anforderungen genügt

Schlüsselaustausch: Bindung der Identität des Signators an ein neues Schlüsselpaar

Secure Multipurpose Internet Mail Extention (S/MIME): Erweiterung des MIME-Formates, die Verschlüsselung und digitale Signatur von E-Mails unterstützt

Secure Socket Layer (SSL): Protokoll, das einen abhörsicheren und authentischen Datenaustausch ermöglicht

Sichere elektronische Signatur: elektronische Signatur, an die besondere, im Österreichischen Signaturgesetz und in den auf seiner Grundlage ergangenen Verordnungen festgelegte Sicherheitsanforderungen gestellt werden

Signator: natürliche Person, der ein Schlüsselpaar (d.h. ein öffentlicher und ein privater Schlüssel) zugeordnet ist und die im eigenen Namen eine elektronische Signatur erstellt, oder ein Zertifizierungsdiensteanbieter, der Zertifikate für die Erbringung von Zertifizierungsdiensten verwendet

Signaturerstellungseinheit: konfigurierte Software oder Hardware zur Verarbeitung des privaten Schlüssels

Signaturprüfeinheit: konfigurierte Software oder Hardware zum Überprüfen einer elektronischen Signatur

Signatur- und Zertifizierungsdienste: Bereitstellung von Signaturprodukten und Signaturverfahren; Ausstellung, Erneuerung und Verwaltung von Zertifikaten; Verzeichnisdienste; Widerrufsdienste; Registrierungsdienste; Zeitstempeldienste; Rechner- und Beratungsdienste im Zusammenhang mit elektronischen Signaturen

Sperre eines Zertifikates: reversible, temporäre Ungültigkeitserklärung eines Zertifikates, um die Umstände eines möglicherweise erforderlichen Widerrufes eines Zertifikates klären zu können (siehe auch → Widerruf eines Zertifikates)

Sperrliste: Liste von Zertifikaten, die vor dem Ablauf ihrer Gültigkeitsdauer gesperrt wurden

© 2000 DATAKOM AUSTRIA GMBH

Uniform Resource Locator (URL): Namenskonvention, die den Zugriffspfad auf Computer, Verzeichnisse und Daten im Internet eindeutig definiert; die URL beinhaltet auch das verwendete Internet-Protokoll (z.B. HTTP)

Widerrufsliste: Liste von Zertifikaten, die vor dem Ablauf ihrer Gültigkeitsdauer widerrufen wurden

Widerruf eines Zertifikates: irreversible, dauerhafte Ungültigkeitserklärung eines Zertifikates (siehe auch → Sperre eines Zertifikates)

Zeitstempel: eine mit einer digitalen Signatur versehene digitale Bescheinigung einer Zertifizierungsstelle darüber, daß ihr bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorgelegen haben

Zertifikat: elektronische Bescheinigung, mit der einer Person ein öffentlicher Schlüssel zugeordnet und die Identität der Person bestätigt wird (siehe auch → qualifiziertes Zertifikat)

Zertifikatinhaber: siehe → Signator

Zertifikatsklasse: Einteilung von Zertifikaten nach dem verwendeten Registrierungsverfahren (*Light*, *Medium*, *Strong* oder *Premium)*

Zertifikatstyp: Einteilung von Zertifikaten nach ihrem Verwendungszweck (User-, Server- oder Developer-Zertifikat)

Zertifikatsverzeichnis: Liste aller veröffentlichten Zertifikate

Zertifikatswerber: Person oder Institution, die ein Zertifikat beantragt

Zertifizierungsdienste: siehe → Signatur- und Zertifizierungsdienste

Zertifizierungsdiensteanbieter: natürliche oder juristische Person oder sonstige rechtsfähige Einrichtung, die Zertifikate ausstellt oder andere elektronische Signatur- und Zertifizierungsdienste erbringt (siehe auch → Signatur- und Zertifizierungsdienste)

Zertifizierungshierarchie: umfaßt jene Einheiten, die im Rahmen von Zertifizierungen hierarchisch voneinander abhängen (Zertifizierungsinstanzen, Signatoren)

Zertifizierungsinfrastruktur: Gesamtheit der bei den Signatur- und Zertifizierungsdiensten beteiligten Einheiten (Certification Authority, Registrierungsstellen, Informationsdienst, ...)

Zertifizierungsinstanz: siehe → Zertifizierungsdiensteanbieter

© 2000 DATAKOM AUSTRIA GMBH

9.2 Abkürzungen

CA	Certification Authority (Zertifizierungsinstanz)
CN	Common Name
CPS	Certification Practice Statement
CRL	Certificate Revocation List (Widerrufsliste für Zertifikate)
DN	Distinguished Name
FTP	File Transfer Protocol
GRA	Global Registration Authority (Globale Registrierungsstelle)
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol with SSL
LRA	Local Registration Authority (Lokale Registrierungsstelle)
MIME	Multipurpose Internet Mail Extensions
PCA	Primary Certification Authority
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
RSA	Rivest Shamir and Adelman Public Key Cryptographic System
SSL	Secure Socket Layer
S/MIME	Secure/Multipurpose Internet Mail Extensions
URL	Uniform Resource Locator

© 2000 DATAKOM AUSTRIA GMBH