VDEW

MATERIALIEN

M-18/2003

Aktionsplan WETTBEWERB

Zertifizierungsrichtlinie (Certification Practice Statement - CPS)

V D E W

VDEW

Verband der
Elektrizitätswirtschaft e.V.

Zertifizierungsrichtlinie (Certification Practice Statement – CPS)

September 2003

Beate Becker, Telefon: 069/6304-302, Mail: beate_becker@vdew.net

Ergänzend zu den Gesetzen und Rechtsvorschriften für den Einsatz der elektronischen Signatur und der Verschlüsselung haben die Verbände eine gemeinsame Erklärung zu „Sicherheitsrahmenbedingungen für den elektronischen Geschäftsverkehr im deutschen Strommarkt" abgegeben. Diese stellt die Basis für die Bildung einer Vertrauensinfrastruktur der Marktteilnehmer beim elektronischen Datenaustausch dar und zeigt Maßnahmen zur Sicherheit auf. Dadurch wird das Sicherheitsniveau auf der technischen und organisatorischen Ebene nachhaltig gehoben.

Die Zertifizierungsrichtlinie richtet sich an Marktteilnehmer, die ganz oder teilweise eine Public-Key-Infrastruktur im eigenen Hause einrichten wollen. „Teilweise“ bedeutet dabei in den meisten Fällen die Einrichtung eines Registrierungsdienstes (etwa in bestehenden Ausweisstellen), aber keines Zertifizierungsdienstes.

Das CPS behandelt den vollständigen Lebenszyklus eines Schlüsselpaares und des dazugehörigen Public-Key-Zertifikats, das im Rahmen von Business-to-Business-Transaktionen zwischen Marktteilnehmern eingesetzt wird.

Um sicherzustellen, dass alle Punkte bedacht wurden, auch wenn sie ggf. in diesem Kontext nicht oder noch nicht relevant sind, folgt dieses Dokument weitestgehend den Empfehlungen des RFC 2527 im Sinne einer Checkliste. Die Ausarbeitung hat eine Doppelfunktion:

1) Das Dokument ist ein weiteres „Policy“-Dokument und damit aus Sicht der beteiligten Markt- und Verfahrensteilnehmer eine Branchenvereinbarung für alle Bereiche, für die keine gesetzlichen Regelungen vorliegen (z. B. Signaturgesetz) bzw. in denen nicht nur firmeninterne Belange betroffen sind (z. B. bei der firmeninternen Kommunikation).
2) Dieses Dokument ist weiterhin im Sinne eines Angebotes an die betroffenen Marktteilnehmer gedacht, als Vorlage für die Firmen-PKI Verwendung zu finden und in einem inhaltlich analog aufgebauten Dokument die nötigen Regelungen zu dokumentieren. Schließlich ist dieses firmenspezifische Dokument auch wieder dort für die branchenweite PKI relevant, wo es PKI-Mechanismen an den Marktschnittstellen berührt, die die CPS aus Sicht des Einzelunternehmens mitdefiniert und damit ihren Beitrag zur branchenweiten Gesamtsicherheit des Verfahrens liefert.

Der VDEW empfiehlt seinen Mitgliedsunternehmen beim Einsatz von elektronischer Signatur und Verschlüsselung beim elektronischen Datenaustausch einen Rahmenvertrag mit den Marktpartnern zu schließen, in dem die Berücksichtigung der gemeinsamen Erklärung sowie der Folgedokumente vertraglich verankert wird.

Management Summary

Certification Practice Statement (CPS)

Das Dokument richtet sich an Marktteilnehmer, die ganz oder teilweise eine Public-Key-Infrastruktur im eigenen Hause einrichten wollen. „Teilweise“ bedeutet dabei in den meisten Fällen die Einrichtung eines Registrierungsdienstes (etwa in bestehenden Ausweisstellen), aber keines Zertifizierungsdienstes.
Das CPS behandelt den vollständigen Lebenszyklus eines Schlüsselpaares und des dazugehörigen Public-Key-Zertifikats, das im Rahmen von Business-to-Business-Transaktionen zwischen Marktteilnehmern eingesetzt wird. Es reicht von der Beantragung durch eine natürliche Person bis zum Widerruf bzw. zur Sperrung zum Ende der Gültigkeitsdauer unter den nötigen technischen, organisatorischen und verbandspolitischen Vereinbarungen. Diese verbandspolitischen Vereinbarungen können sich dabei nur auf die Kommunikation zwischen den Marktteilnehmern beziehen. Allerdings können und sollten sie auch auf weitere Kommunikationsbeziehungen mit anderen Partnern, Kunden oder Behörden übertragbar sein.

Um sicherzustellen, dass alle Punkte bedacht wurden, auch wenn sie ggf. in diesem Kontext nicht oder noch nicht relevant sind, folgt dieses Dokument weitestgehend den Empfehlungen des RFC 2527 im Sinne einer Checkliste.

Dieses Dokument hat eine Doppelfunktion:

1) Das Dokument ist ein weiteres „Policy“-Dokument und damit aus Sicht der beteiligten Markt- und Verfahrensteilnehmer eine Branchenvereinbarung für alle Bereiche, für die keine gesetzlichen Regelungen vorliegen (z.B. Signaturgesetz) bzw. in denen nicht nur firmeninterne Belange betroffen sind (z.B. bei der firmeninternen Kommunikation).

2) Dieses Dokument ist weiterhin im Sinne eines Angebotes an die betroffenen Marktteilnehmer gedacht, als Vorlage für die Firmen-PKI Verwendung zu finden und in einem inhaltlich analog aufgebauten Dokument die nötigen Regelungen zu dokumentieren. Schließlich ist dieses firmenspezifische Dokument auch wieder dort für die branchenweite PKI relevant, wo es PKI-Mechanismen an den Marktschnittstellen berührt, die die CPS aus Sicht des Einzelunternehmens mitdefiniert und damit ihren Beitrag zur branchenweiten Gesamtsicherheit des Verfahrens liefert.

Ein Public Key-Zertifikat verbindet den öffentlichen Schlüssel eines asymmetrischen Schlüsselpaares mit der eindeutigen Kennung (Distinguished Name, DN) eines Nutzers. Durch die digitale Signatur des Zertifikats verleiht die signierende Certification Authority des am Verfahren teilnehmenden Marktteilnehmers oder entsprechend qualifizierten Zertifizierungsdienstleisters dem öffentlichen Schlüssel eines Nutzers ein dezidiertes Maß an Vertrauenswürdigkeit.
Das Certification Practice Statement macht Aussagen zu dem Regelungsbedarf, der dieses Maß an vergleichbarer Vertrauenswürdigkeit determiniert bzw. gewährleistet.

Zertifizierungsrichtlinie

(Certification Practice Statement)

Sicherheit beim elektronischen Geschäfts-verkehr in der deutschen Elektrizitätswirtschaft

Empfehlungen für die Marktteilnehmer

Stand: 1. September 2003

Version 1.0

Inhaltsverzeichnis

0. Historie

Datum	Abschnitt	Änderungen	Name
01.09.2003		VDEW-Freigabe	VDEW-LA

1. Allgemeine Bemerkungen

Die VDEW-Projektgruppe „Sicherheit im elektronischen Datenaustausch“ hat zur Gewährleistung einer sicheren Kommunikation zwischen den Marktteilnehmern in der deutschen Elektrizitätswirtschaft eine gemeinsame Erklärung zwischen den beteiligten Verbänden angeregt. Diese Erklärung hat keine rechtliche Verbindlichkeit, stellt allerdings insoweit „moralische“ Anforderungen an die Solidargemeinschaft der Marktteilnehmer, als Sicherheitsbelange im Geschäftsverkehr in der Branche angemessen berücksichtigt werden sollen.

Die gemeinsame Erklärung auf der verbandspolitischen Ebene muss durch entsprechende Dokumente im organisatorischen und technischen Umfeld ergänzt und ausgestaltet werden.

Allgemein definiert haben die organisatorischen Teile dieser Folgedokumente den Anspruch, ein in etwa gleiches organisatorisches Sicherheitsniveau bei der Verschlüsselung und Signatur von unternehmensübergreifenden Transaktionen zwischen den Marktteilnehmern zu gewährleisten.

Ebenso allgemein definiert sollen die technischen Teile der Dokumente auch beim Einsatz unterschiedlicher Produkte oder Dienstleistungen Interoperabilität auf der technischen Ebene gewährleisten.

Die politischen, organisatorischen und technischen Aussagen in der gemeinsamen Erklärung und ihren Folgedokumenten haben Empfehlungscharakter und sollen in der Solidargemeinschaft der Marktteilnehmer eine Vertrauensinfrastruktur ermöglichen.

Insofern zählt bei der Umsetzung der Vorschläge im eigenen Unternehmen und der nachfolgenden Anwendung an den Marktschnittstellen der „Geist“ und nicht der „Wortlaut“. Allerdings sollen gegenüber den Verbandsempfehlungen geänderte Vorgehensweisen begründbar sein und das allgemeine Sicherheitsniveau unbeeinträchtigt lassen.

Die Mehrheit der Marktteilnehmer ist wirtschaftlich daran interessiert, dass die Vertrauensinfrastruktur nicht ausgehöhlt wird, weil nur dadurch die sichere elektronische Abwicklung der Geschäfte mittelfristig gewährleistet ist und so ausgebaut werden kann, dass auch weitere Automatisierungsschritte beherrschbar bleiben.

2. Einführung

Mittlerweile werden zum Datenaustausch zunehmend keine Festverbindungen oder X.400-Verbindungen genutzt, sondern es wird z. B. per E-Mail über preiswertere Internetverbindungen kommuniziert. Die zunehmend bessere Dienstgüte rechtfertigt diese Vorgehensweise, allerdings müssen bei der Kommunikation über ein offenes Netz entsprechende Vertraulichkeits-, Integritäts- und Authentizitätsanforderungen berücksichtigt werden.

In einer EDI-Beziehung zwischen Marktpartnern sollten diese Anforderungen abgedeckt werden können, ohne dass jeweils bilaterale Absprachen getroffen werden müssen.

Die VDEW-Projektgruppe „Sicherheit beim elektronischen Datenaustausch“ hat zum Einsatz von elektronischer Signatur zur Gewährleistung von Datenintegrität und Absenderauthentizität und zum Einsatz von starker Verschlüsselung zur Gewährleistung von Vertraulichkeit beim elektronischen Datenaustausch Dokumente erarbeitet, die dazu geeignet sind, als technische und organisatorische Referenzdokumente für den Bereich Datensicherheit zu dienen und damit einen EDI-Vertrag zu ergänzen. Auf Verbandsebene

haben sie empfehlenden Charakter. Ebenso wie die empfohlenen EDI-Marktschnittstellen, welche die Interoperabilität auf Anwendungsebene gewährleisten, sichert die Zertifizierungsrichtlinie Interoperabilität und vergleichbares Niveau auf der Sicherheitsebene. Die meisten Dokumente können allgemein und damit unabhängig vom jeweiligen Unternehmenseinsatz formuliert werden. Lediglich die Zertifizierungsrichtlinie (Certification Practice Statement, CPS) ist durch ihre spezifischen, durch den jeweiligen organisatorischen Kontext bestimmten Regelungen unternehmensabhängig. Die CPS ist deshalb zur Vergleichbarkeit von Sicherheitsbedingungen das wichtigste Dokument.

2.1. Übersicht

Dieses vorliegende Dokument soll das Certification Practice Statement (CPS) spezifizieren. Es hat Übersichtscharakter.

Diese Übersicht soll eine Einführung in die Methodik, mit der die Spezifikation organisiert und strukturiert ist, in die Transaktionstypen, die von der Certificate Policy unterstützt werden, in die in den Transaktionen eingebundenen Parteien, in die allgemeinen Voraussetzungen für das Verständnis und die Auslegung der Spezifikation geben.

Dieses Dokument folgt weitestgehend den Empfehlungen des RFC 2527.[i]

Dieses Dokument hat eine Doppelfunktion:

1) Das Dokument ist ein weiteres „Policy“-Dokument und damit aus Sicht der beteiligten Markt- und Verfahrensteilnehmer Branchenempfehlung für alle Bereiche, in denen keine gesetzlichen Regelungen vorliegen (z. B. Signaturgesetz) bzw. in denen nicht nur firmeninterne Belange betroffen sind.

2) Dieses Dokument ist weiterhin im Sinne eines Angebotes an die betroffenen Marktteilnehmer dafür gedacht, für die Firmen-PKI als Vorlage Verwendung zu finden und in einem inhaltlich analog aufgebauten Dokument die nötigen Regelungen zu dokumentieren.

Das (VDEW-)CPS behandelt den vollständigen Lebenszyklus eines Schlüsselpaares und des dazugehörigen Public-Key-Zertifikats, das im Rahmen von Business-to-Business-Transaktionen zwischen Marktteilnehmern eingesetzt wird von der Beantragung durch eine natürliche Person bis zum Widerruf bzw. zur Sperrung zum Ende der Gültigkeitsdauer unter den nötigen technischen, organisatorischen, rechtlichen und sonstigen[1] Vereinbarungen.

Ein Public-Key-Zertifikat verbindet den öffentlichen Schlüssel eines asymmetrischen Schlüsselpaares mit der eindeutigen Kennung (Distinguished Name, DN) eines Nutzers. Durch die digitale Signatur des Zertifikats verleiht die signierende CA des am Verfahren teilnehmenden Marktteilnehmers oder des durch den VDEW zugelassenen Zertifizierungsdienstleisters dem öffentlichen Schlüssel eines Nutzers ein dezidiertes Maß an Vertrauenswürdigkeit.

Akkreditierte deutsche Zertifizierungsdienstleister sind bei qualifizierten Zertifikaten (mit Anbieterakkreditierung) durch das Signaturgesetz zugelassen. Ausländische Zertifizierungsdienstleister und Anbieter von fortgeschrittenen Zertifikaten sollten in der Bewertung des Sicherheitsniveaus diesem CPS entsprechen.

---

[1] Unter dem Begriff „sonstigen“ sind auch Branchenvereinbarungen gemeint, die ein Teilnehmer am Verfahren einhalten muss (z. B. Abkommen zu Sicherheitsrahmenbedingungen für den elektronischen Rechts- und Geschäftsverkehr im deutschen Strommarkt).

Durch die Pflege der Certification Revocation List (oder durch ein Positivverfahren), d. h. der ständigen Aktualisierung und Bekanntgabe ungültiger Zertifikate, erhält die Revocation Authority diese Vertrauenswürdigkeit bis zum Ablauf der Gültigkeit bzw. bis zur Revokation/Widerruf eines Zertifikats.

Das Maß der Vertrauenswürdigkeit eines Zertifikats wird darüber hinaus oft durch die Einstufung in eine von drei verschiedenen Sicherheitsklassen bestimmt: High, Medium und Low Level, sowie ggf. noch differenziert für den internen und externen Gebrauch in einem Unternehmen. Der interne Gebrauch dient hier als Beispiel im Gesamtzusammenhang. Diese Differenzierung erlaubt ein Höchstmaß an Flexibilität in bezug auf die Registrierung und die einzusetzende Sicherheitstechnologie.

Die folgende Differenzierung bezieht sich insbesondere auf Signaturzertifikate:

High = Qualifizierte Zertifikate (mit/ohne Anbieterakkreditierung) mit sicherer Signaturerstellungseinheit (i. Allg. SmartCard, Class2 Leser oder entsprechende Krypto-Module),

> Rechtsrahmen ist das Signaturgesetz und es besteht damit kein weiterer formaler Vereinbarungsbedarf im Rahmen des VDEW

Medium = Fortgeschrittene Zertifikate ohne geprüfte Signaturerstellungseinheit (i.A. SmartCard, Class1-Leser oder sonstige sichere PSE), aber mit begrenzt gültigem Zertifikat,

> Handlungsrahmen wird über die gemeinsame Erklärung und die Folgedokumente geschaffen.

Low = Username/Password, schwächere oder auch nur andere Zertifizierungsmechanismen, unternehmensinterne Verwendung,

> „Rechtsrahmen“ sind Unternehmensrichtlinien, die keine Relevanz im Rahmen von externen PKI-Vereinbarungen haben.

Das vorliegende Dokument adressiert insbesondere den Einsatz von fortgeschrittenen Signatur-Zertifikaten der Kategorie Medium in der PKI. High, Medium und Low Level sagt also nichts über die tatsächliche Sicherheitsstufe aus, sondern charakterisiert lediglich den Handlungsrahmen.

Allerdings hat das jeweilige Unternehmen die Freiheit, bei Low Level auch „Low Security Level“ zu wählen.

Bezüglich Verschlüsselung entfällt der allgemeine Rechtsrahmen. Das Signaturgesetz bezieht sich nicht auf die Verschlüsselung. Das Telekommunikationsgesetz, das in bestimmten Fällen staatlichen Instanzen entschlüsseltes „Mithören“ gestattet, hat im Marktraum „Elektrizitätswirtschaft“ anwenderseitig keine Geltung. Lediglich das Steuerrecht (GDPdU) schreibt die Archivierung von verschlüsselten, steuerrechtlich relevanten Daten und ihrer kryptographischen Schlüssel vor. Dies ist z. B. im Falle einer steuerlichen Außenprüfung, die nach der progressiven Methode (belegorientiert, beginnend beim Beleg, Prüfung in den am Vorgang wirtschaftlich beteiligten Unternehmen) durchgeführt wird, von Bedeutung. Diesen Bereich muss also das vorliegende CPS auch adressieren. Die Ausgestaltung erfolgt aber durch das jeweilige Unternehmen. Im Gegensatz zur Signatur mit ihren Haftungsanforderungen sollten pragmatischerweise bei der Verschlüsselung mehr Spielräume gelassen werden. Dies gilt insbesondere für das Trägermedium, die zentrale Key-Generierung, die Archivierung der Schlüssel, etc. Die untenstehende Tabelle nennt allerdings bewusst SmartCard auch als Trägermedium für Verschlüsselungsschlüssel im Rahmen der vertraulichen Marktkommunikation.

Generell gilt: Die Anpassung des entsprechenden Sicherheitsniveaus an die jeweiligen Anforderungen der B2B- bzw. E-Business-Applikationen vermeidet unnötig hohe Sicherheitsanforderungen für einen Großteil der Nutzer und somit unnötige Kosten im Betrieb der PKI. Allerdings werden High-Zertifikate durch gesetzliche Rahmenbedingungen gefordert. Es sei darauf hingewiesen, dass mit der Steuerdatenübermittlungsverordnung ein rechtlicher Kontext entstanden ist, in dem zwar fortgeschrittene Signaturen ausreichen, diese aber bestimmten Kriterien genügen müssen (z. B. SmartCard als Schlüsselträger). Sinnvollerweise werden unternehmensintern diese Anforderungen berücksichtigt, weil die gesicherte Kommunikation zwischen den Marktteilnehmern nur ein Bruchteil der weiteren Einsatzfelder besonders von elektronischen Signaturen zur Vermeidung von Papierbegleit-dokumenten umfasst. Entsprechender Aufwand in (Public Key) Infrastrukturen sollten also investitionssicher bezüglich dieser weiteren Einsatzfelder sein.

Die Solidargemeinschaft der beteiligten Marktteilnehmer kann und muss in allen Fällen beim Geschäftspartner ein stabiles Sicherheitsniveau erwarten. Unabhängig von der Einstufung in eine der drei Sicherheitsklassen wird deshalb von jedem Nutzer der sorgfältige Umgang mit dem zur Verfügung gestellten Schlüsselmaterial erwartet, unabhängig davon, ob es im Rahmen der Verbands-PKI-Empfehlungen eingesetzt wird. Es liegt sowohl im Interesse der PKI-Teilnehmer als auch eines jeden Marktteilnehmers selbst, dass jeglicher Missbrauch von Schlüsselmaterial vermieden wird, da eine Unterscheidung in internen und externen Einsatz vom Benutzer schwerlich gemacht wird. Diese Sicherheitskultur ist Grundlage der Vertrauensinfrastruktur.

Auch wenn die Verbands-PKI-Empfehlungen maßgeblich zur Unterstützung von B2B-Anwendungen (EDIFACT, XML, CSV) aufgebaut werden, bedeutet dies keineswegs die Beschränkung der damit verbundenen Gesamtstruktur oder auch einzelner Teile auf diesem Anwendungsfeld. Im Folgenden wird der Einfachheit halber von B2B-Applikationen gesprochen.

Grundanliegen des VDEW ist es, nicht eine eigenständige PKI zu definieren, sondern die branchenweite Vertrauensinfrastruktur zu unterstützen. Diese sollte auf weitere Geschäftsbeziehungen übertragbar sein. Einziger Zweck dieses Dokumentes ist die Nivellierung von Sicherheitsniveaus. Durch die vertikale Interoperabilität der Zertifikate wird ein höherwertiges Zertifikat, als die Anwendung fordert, zugelassen (z. B. qualifiziert statt fortgeschritten).

Die Bindung eines Zertifikats an eine Policy wird durch den Eintrag des zugehörigen PolicyObject Identifier (OID) in das Zertifikat dokumentiert. Die formelle Registrierung der Policies erfolgt ggf. später durch die Internet Policy Registration Authority gemäß RFC 1422, Abs. 3.14. Die Policies der PKI´s stehen dabei nicht gleichberechtigt nebeneinander, sondern qualitativ bezüglich des Sicherheitsniveaus in einer hierarchischen Beziehung:

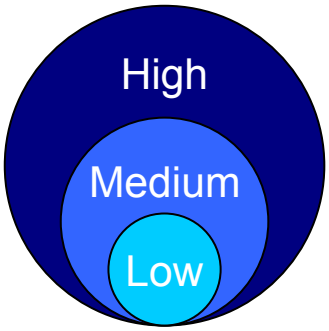

Abbildung 1: Policy-Hierarchie

Regelungsbedarf für die Verbände gibt es nur bei Medium Extern, da hier die gemeinsame Erklärung indirekt die fehlenden Rahmenbedingungen definieren muss.

Die nachfolgende Tabelle gibt einen Überblick über die Auswirkungen der verschiedenen Policies/Sicherheitsklassen auf die PKI:

Nutzer	Policy/ Klasse	Signatur	Archiv. Sig Key	Verschlüs-selung	Archiv. Verschl. Key	Schlüsselpaare	Träger-medium
Extern	High	X	-	X	X	2+	SmartCard
Extern	***Medium***	***X***	***-***	***X***	***X***	***2***	***sichere PSE[2]***
Intern	Low	-	-	X	X	1	entfällt

Tabelle 1: Die Sicherheitsklassen der Zertifikate (der Gültigkeitsbereich der vorliegenden CPS ist *kursiv* gekennzeichnet)

Grundsätzlich wird zwischen internen und externen Nutzern unterschieden, da insbesondere keine zentrale Archivierung des Schlüsselmaterials externer Nutzer durchgeführt wird. Zu beachten ist, dass für den Bereich Low Level Security lediglich Zertifikate für Verschlüsselungsschlüssel ausgestellt werden; die Nutzung dieser Schlüssel für die digitale Signatur ist durch den fehlenden Eintrag im Zertifikatsfeld „Key Usage“ ausgeschlossen. Technisch ergeben sich aus dieser Aussage zurzeit noch Probleme, da wenige Anwendungen die Auswertung des Feldes/der Felder unterstützen.

Schlüssel für digitale Signaturen werden ausschließlich über eine sichere PSE verwaltet.[3]

Es findet keine Archivierung von Signaturschlüsseln in der externen Verwendung statt.

Eine zentrale Archivierung der Verschlüsselungsschlüssel und ggf. Key Recovery unterliegt der Verantwortung der einzelnen Unternehmen. Gleiches gilt für ausschließlich interne Nutzer von Signaturschlüsseln, obwohl davon an dieser Stelle abgeraten wird.

Bei externen Nutzern der Sicherheitsklassen High (SigG-konform, wo es ohnehin ausgeschlossen ist) und Medium (fortgeschritten, Trägermedium SmartCard) wird den Unternehmen dringend empfohlen, keine Kopien der privaten Signaturschlüssel zentral zu speichern.

---

[2] PSE Personal Security Environment: Kombination von geheimen Schlüsseln und Zertifikaten (mit/ohne Trägermedium), die einem PKI-Nutzer fest zugeordnet und durch ein Kennwort geschützt sind.

[3] Bei Sicherheitsklasse „High“ wird ein kartenspezifischer Authentisierungsschlüssel verwendet, der (falls dazu überhaupt unterschiedliche Schlüssel verwendet werden) auch im Medium Level zu Secure Messaging dienen kann. Die prinzipielle Möglichkeit, Secure Messaging auch im Rahmen „Medium“ (fortgeschritten, qualifiziert ohne Anbieterakkreditierung) einsetzen zu können, wird empfohlen. D.h. jede SmartCard sollte neben den personenbezogenen Schlüsseln für Authentisierung, Signatur und Verschlüsselung auch einen kartenspezifischen, zertifizierten Schlüssel für die Authentisierung mit einem Class2/3-Leser haben (IFD/ICC-Authentication). Dies ist wirtschaftlich sinnvoll, damit z. B. eine Zertifikatserneuerung über das Web ohne Sicherheitsabstriche möglich ist. Dies ist allerdings nicht Gegenstand dieses Dokumentes, das nur den Umgang mit personenbezogenen Schlüsseln behandelt.

Auch bei fortgeschrittenen Zertifikaten sollte möglichst nach dem heutigen Stand der Technik das Signatur-Schlüsselpaar auf der Karte erzeugt werden. Anschließend kann der öffentliche Schlüssel zu einem Zeitpunkt, zu dem es nach dem Registrierungsprozess organisatorisch sinnvoll ist, per genormtem PKCS#10-Request an die CA exportiert und zertifiziert werden. Sollte trotzdem zentrale Key-Generierung zum Einsatz kommen, so müssen die Teilnehmer, das private Signatur-Schlüsselmaterial sofort nach Übertragung in das Trägermedium SmartCard auf der Platte des Key-GenerationRechners löschen.

2.2. Identifikation

Angabe aller verwendeten Namen und Identifikatoren

einschließlich der ASN.1-Objekte, insbesondere die Objekt-ID ("OID") der Certificate Policy

Das Namensmodell sollte sich auf Codenummern stützen, die in Anlehnung an die Norm ISO/IEC 6523 gebildet werden. Daraus sollten sich alle physikalischen Namen ableiten.

Die Norm ISO/IEC 6523 definiert eine Struktur für eine global einmalige und eindeutige Identifikation von Organisationen und Teilen davon zum Zweck des Datenaustausches. Dabei wird einer Organisation vom BSI (British Standards Institution) eine weltweit eindeutige ICD zugeordnet (International Code Designator).

Diese ICD ist äquivalent zu der OID Struktur (Object Identifier) des MIB/SNMP Private-Enterprise-Number-Schemas unterhalb der Notation 1.3 {1(iso). 3(identified organization)}. Informationen dazu sind unter http://www.iana.org/assignments/smi-numbers zu finden.

Auf http://www.iana.org/cgi-bin/enterprise.pl können sich Unternehmen kostenlos unterhalb der Ebene 1.3.6.1.4.1 eine eigene OID registrieren lassen.

Beispiel: 1.3.6.1.4.1.17722 = OID der STEAG AG

Kostenpflichtige ICDs/OIDs können beim BSI (British Standards Institution) registriert werden. Weitere Informationen dazu sind per E-Mail (Telecoms@bsi-global.com) zu erfragen.

Die kostenlosen OIDs unterscheiden sich von den kostenpflichtigen in Art und Umfang des Überprüfungsprozesses der Registrierungsdaten.

Auf Personenebene sollte daraus ein eineindeutiger, langfristig (z. B. 100 Jahre) nur einmal vergebener Kennzeichner entstehen. Dieser Kennzeichner wird gerne als Global Identification -Global-ID- des Zertifikatsinhabers (Person, CA, etc.) bezeichnet. Ideal wäre es, wenn über die gesamte Nummer ein Plausibilitätsalgorithmus zugrunde liegt.

Als physikalische Namen sind weiterhin zu nennen:

- Zertifikatsinhaber (als mind. 2-stufiger Distinguished Name)
- Global-ID des Zertifikatsinhabers
- CA-Name (bei selbstbetriebener CA in einer Tochterorganisation für einen Konzern, z. B. RWE Systems für RWE)
- CA-Name bei akkreditiertem Zertifizierungsdienstleister

- Object-ID pro Policy mit externer Relevanz, insbesondere unterschiedlich differenziert für Authentisierung, Verschlüsselung, Signatur

Zur Vereinfachung des weiteren Dokumentes folgt hier ein Glossar. Weitere und ausführlichere Abkürzungen und ihre Erläuterungen sind im PKI-Policy-Dokument[4] enthalten.

Verwendete Abkürzungen und ihre Kurzbedeutung

ASN > Abstract Syntax Notation

Eine Grammatik zur Definition von Datenstrukturen sowie Festlegungen zur Umsetzung von Datenstrukturen und Elementen in ein netzeinheitliches Format (Transfer Syntax).

CA > Certification Authority

Instanz einer PKI, die Zertifikate ausstellt, d. h. die Echtheit eines öffentlichen Schlüssels sowie die Authentizität des Zertifikatsinhabers beglaubigt und sich verpflichtet, Informationen über den Status der ausgestellten Zertifikate über einen definierten Zeitraum bereitzustellen.

CP > Certificate Policy

Eine formelle Menge von Vorschriften, die die Eignung von Zertifikaten für eine bestimmte Gemeinschaft von PKI-Nutzern sowie für eine bestimmte Art von Applikationen unter gemeinsamen Sicherheitsanforderungen kennzeichnet. Eine CP kann durch einen einmalig vergebenen Object Identifier (OID) identifiziert werden.

CPS > Certification Practice Statement

Die Erklärung einer Instanz (CA, Trust Center) eines vertrauenswürdigen Systems (PKI) über verbindliche Vorgaben, Regularien und Verfahren für die Ausgabe und Behandlung von Zertifikaten.

CRL > Certification Revocation List

Möglichkeit einer CA, anhand einer stetig zu aktualisierenden Liste Informationen über gesperrte Zertifikate einer Öffentlichkeit zugänglich zu machen.

Digitale Signatur

Eindeutige Kennzeichnung digitaler Daten durch die Anwendung asymmetrischer kryptographischer Verfahren.

Directory

[4] Sicherheitspolitik

Ein für die Nutzer einer PKI zugänglicher Verzeichnisdienst, in dem Zertifikate und CRLs abgelegt und gelöscht werden können bzw. als Suchergebnis einer Abfrage ausgegeben werden.

DN > Distinguished Name

Eindeutiges Identifizierungsmerkmal eines Zertifikatsinhabers innerhalb einer PKI anhand einer Zeichenkette, die aus verschiedenen hierarchisch geordneten Namensteilen zusammengestellt wird.

DSA > Digital Signature Algorythm

Mathematisches Verfahren zur digitalen Signatur, basierend auf dem Problem des diskreten Logarithmus in multiplikativen Gruppen.

ECDH > Elliptic Curves Diffie Hellman

Mathematisches Verfahren zum Schlüsselaustausch, basierend auf dem Problem des diskreten Logarithmus, übertragen auf elliptische Kurven.

ECDSA > Elliptic Curves Digital Signature Algorythm

Mathematisches Verfahren zur digitalen Signatur, basierend auf dem Problem des diskreten Logarithmus, übertragen auf elliptische Kurven.

HSM > Hardware Security Module

Modul, in dem geheime Schlüssel vor unbefugtem Zugriff geschützt, erzeugt, gespeichert und verwendet werden können.

PKI > Public Key Infrastructure

Unter dem Begriff PKI werden die Instanzen zusammengefasst, die für die Anwendung asymmetrischer kryptographischer Verfahren insbesondere für die digitale Signatur erforderlich sind.

LDAP > Lightweight Directory Access Protocol

Protokoll für den vereinfachten Zugriff auf Verzeichnisdienste nach X.500.

LRA > Local Registration Authority

Registrierstelle, die nicht als zentraler Dienst, sondern in relativer Nähe zum Nutzer als erste Schnittstelle zur PKI Anträge entgegennimmt und bearbeitet.

PIN > Personal Identification Number

Im Zusammenhang mit SmartCards ein alphanumerisches Passwort, das die vor unbefugtem Zugriff geschützte Anwendung geheimer Schlüssel ermöglicht.

PSE > Personal Security Environment

Kombination von geheimen Schlüsseln und Zertifikaten einschließlich Trägermedium, die einem PKI-Nutzer fest zugeordnet sind.

Privater Schlüssel

Eine Hälfte eines asymmetrischen Schlüsselpaares, die nur dem PKI-Nutzer selbst bekannt bzw. zugänglich sein darf. Mit diesem Schlüssel kryptierte Daten können nur mit dem zugehörigen öffentlichen Schlüssel dekryptiert werden, z. B. zur Überprüfung einer digitalen Signatur.

PKI > Public Key Infrastructure

Summe der Dienste und Instanzen, die für den Einsatz von Public-Key-Kryptographie notwendig sind.

Öffentlicher Schlüssel

Eine Hälfte eines asymmetrischen Schlüsselpaares, die öffentlich zugänglich ist. Mit diesem Schlüssel kryptierte Daten können nur mit dem zugehörigen privaten Schlüssel dekryptiert werden.

RA > Registration Authority

Zentrale Registrierungsinstanz einer PKI, die Anträge zur Erstellung von Zertifikaten annimmt (z. B. von verschiedenen LRAs), bearbeitet und an eine CA weiterleitet.

RevA > Revocation Authority

Dienst einer PKI, der für die Sperrung von Zertifikaten z. B. durch Eintrag in eine CRL, zuständig ist.

Roll-Over

Wechsel von Schlüssel und Zertifikat, deren Ende der Gültigkeit erreicht wurde.

RSA > Rivest, Shamir, Adelman

Entwickler des gleichnamigen mathematischen Verfahrens zur digitalen Signatur. Die Sicherheit des Verfahrens basiert auf dem Problem der Faktorisierung ganzer Zahlen.

SHA-1 > Secure Hash Algorythm 1

Eine kryptographische Hashfunktion, die beliebig lange Daten ohne geheimen Schlüssel zu einem nicht manipulierbaren Prüfwert („Digitaler Fingerabdruck“) fester Länge von 160 Bit komprimiert. Dieser Prüfwert wird auch Hashwert genannt.

SmartCard

Trägermedium für geheime Schlüssel und Zertifikate, die durch verschiedenste Eigenschaften und Mechanismen (z. B. PIN) vor unbefugtem Zugriff geschützt sind.

Trust Center

Unter diesem Begriff werden Dienste und Instanzen einer PKI zusammengefasst, die für die Erzeugung, Ausgabe und Information über die Gültigkeit von Zertifikaten verantwortlich sind.

Zertifikat

Datensatz, mit dem eine CA die Vertrauenswürdigkeit eines öffentlichen Schlüssels eines PKI-Nutzers durch Anwendung der digitalen Signatur dokumentiert.

2.3. Gemeinschaft und Anwendung

In diesem Abschnitt werden beschrieben:

Instanzen und Entitäten

CA, RA

Teilnehmer (Subscriber): alle Instanzen (Personen, Anwendungen, Maschinen[5]), die ein von der CA erstelltes Zertifikat besitzen können. Dies wurde ausführlich im Dokument zur „PKI-Policy“ beschrieben.[6]

Anwendungen

Hier werden zugelassene, ausschließliche und verbotene Anwendungen angegeben, in denen die in diesem Dokument angegebenen Zertifikatstypen benutzt bzw. nicht benutzt werden dürfen. Diese Listen sind besonders kritisch hinsichtlich der Haftung, die die CA eingeht, so dass diese Policy im Zertifikat an geeigneter Stelle einzutragen ist.

Grundsätzlich werden zwei Typen von Anwendungen adressiert:

1. (Formatierter) Geschäftsverkehr (EDIFACT, XML, CSV)
2. (Unformatierter) Rechtsverkehr (Freitext im pdf-Format oder gebräuchlichen MS Office-Formaten)

Grundsätzlich ist es das Ziel, in der Gemeinschaft von Marktteilnehmern geschäftliche Tätigkeit durch firmenübergreifende Kommunikation die Geschäftsprozesse zu verbessern oder sogar erst zu ermöglichen. Dadurch sind einheitlich nivellierte und angewendete Trust Services nötig geworden. Bezüglich dieser Untermenge an firmenübergreifender Kommunikation und Geschäftsprozessen müssen deshalb

- Sicherheitspolitik,

[5] Rechner, Server, Messeinrichtungen etc.

[6] Sicherheitspolitik für Aufbau und Betrieb von verbandsübergreifenden Zertifizierungsinfrastrukturen

- Vergabepraxis der Legitimation und
- Anwendungsbezug

vergleichbaren Regeln unterliegen.

Den beteiligten Unternehmen und Instanzen der PKI wird deshalb die Einhaltung der PKI-Policy, des Certification Practice Statement (CPS) sowie der damit verbundenen Certificate Policies (CP) bei allen Anwendungen, die mit Hilfe der Trust Services abgesichert werden sollen (Mail, EDI, Dokumentensignatur) dringend empfohlen.

Teilnehmer/Subscriber sind zunächst natürliche Personen in den beteiligten Unternehmen. Eine Ausdehnung auf technische Instanzen (Serverzertifikate etc.) bedarf lediglich Erweiterungen auf CPS und CP-Ebene und nicht auf Policy -Ebene.

Instanzen sind CA, RA bzw. LRA und Verzeichnisdienst. Daneben sind technische Instanzen, wie SmartCard-Initialisierung und –Personalisierung, zu betrachten.

Dies gilt insbesondere für die sichere Erzeugung und Archivierung von Schlüsselmaterial, die Generierung und Veröffentlichung von Zertifikaten auf Grundlage von zweifelsfrei registrierten und legitimierten Personen sowie die Pflege und Veröffentlichung von gesperrten Zertifikaten (Certificate Revocation Lists).

Mit Beantragung und Aushändigung des Personal Security Environments (PSE) verpflichtet sich der Zertifikatsinhaber zur Anerkennung des CPS, insbesondere zum sorgfältigen Umgang mit Schlüssel- und Zertifikatsmaterial, zum Schutz vor unbefugtem Zugriff, zur ausschließlichen Nutzung des Schlüsselmaterials für die vorgesehenen Zwecke sowie zur unverzüglichen Benachrichtigung der Registrierungsstellen bei Verlust oder Verdacht auf Kompromittierung des Schlüsselmaterial (siehe dazu[7]) Die beteiligten Unternehmen sorgen durch Kontroll- und Revisionsmechanismen, dass mindestens die gleiche Sicherheit, wie bei den heutigen Unterschriftsberechtigungen und ihrer Kontrolle besteht. Haftungsgegner ist der Zertifikatsaussteller (intern z. B. E.ON-Energie, extern z. B. TCTrustCenter) im Rahmen der vertikalen Hierarchie (fortgeschritten, qualifiziert).

Zugelassene Anwendungen sind z. B.:

E-Mail (S/MIME-Standard nach ISIS-MTT V2 auf TCP/IP)

EDIFACT (16560-15 "AUTACK-Guide“ bzw. 16560-16 und Syntax-Versionen 3,4)

sowie entsprechende XML-Anwendungen

Es wird keine nachrichten-inhaltliche Differenzierung vorgenommen (z. B. Verfügungsrahmen). Dieser wird im Rahmen der firmeninternen Unterschriftenregelung vorausgesetzt.

Alle folgenden Hinweise unter 1.3 sind hier redundant aufgeführt siehe dazu [PKI-Policy]

---

[7] Anwendung von Schlüsselmaterial im elektronischen Rechts- und Geschäftsverkehr der deutschen Elektrizitätswirtschaft bei Verschlüsselung, elektronischer Signatur und Authentisierungsvorgängen

Umgang mit Schlüsselmaterial

2.3.1. CertificationAuthorities

Beschreibung der Instanzen/Entitäten, die Zertifikate ausstellen oder die als CA zugelassen sind

Beispiele:

IT-Abteilung eines Unternehmens, akkreditierter Zertifikatsdiensteanbieter

CA als Sicherheitseinrichtung direkt unter der Unternehmensführung (CIO als Auftraggeber und SLA-Unterzeichner)

siehe dazu [PKI-Policy]

2.3.2. RegistrationAuthorities

Beschreibung der Instanzen/Entitäten, die RA-Funktionen ausführen

Beispiele:

RAs als Außenstellen der Personalabteilung, als lokale Sicherheitseinrichtungen auf regionaler Ebene

siehe dazu [PKI-Policy]

2.3.3. EndEntities

Beschreibung der Instanzen/Entitäten, die als persönliche oder institutionelle Zertifikatsbesitzer in Frage kommen.

Beispiele:

Angestellte einer Firma, Einzelfirmen eines Konzerns (bei Verschlüsselung)

siehe dazu [PKI-Policy]

2.3.4. Anwendungszulassungen und -einschränkungen

Liste der Anwendungen/Prozesse, in denen der hier beschriebene Zertifikatstyp für Sicherheitsdienste benutzt werden darf.

Geschäftsverkehr (formatiert) z. B.:

Fahrplan, Bilanzkreisdaten, Lieferantenwechsel, Rechnung, Zähldaten auf der Kommunikationsplattform e-Mail, EDI, CSV, XML

Rechtsverkehr (unformatiert)

Prozesse sind unternehmensintern festzulegen

Kommunikationsplattform z. B. E-Mail, Datei, pdf, MS Office

Liste der Anwendungsfälle, bei denen der hier beschriebene Zertifikatstyp nicht benutzt werden darf, z. B. Verträge mit besonderer Tragweite (sollten rechtlich geprüft werden).

2.4. Kontakte

2.4.1. Organisation für die Verwaltung dieser Spezifikation

Name und E-Mail-Adresse der Instanz, die für die Registration, Pflege und Auslegung dieser CPS zuständig ist.

VDEW, PG Sicherheit beim elektronischen Datenaustausch

2.4.2. Verantwortlicher für die CPS

Verbandsebene: VDEW-Projektgruppe Sicherheit beim elektronischen Datenaustausch

Unternehmensebene: Name, E-Mail-Adresse, Telefonnummer, Fax-Nummer

2.4.3. Kontaktperson

Verbandsebene: VDEW-Projektgruppe Sicherheit beim elektronischen Datenaustausch

Unternehmensebene: Name, E-Mail-Adresse, Telefonnummer, Fax-Nummer der Kontaktpersonen, die für die Kommunikation dieser Policy zuständig sind

3. Allgemeine Bestimmungen

Beschreibung aller allgemeinen und rechtlichen Aspekte einer CPS, getrennt für jede beteiligte Instanz (Entity); die endgültigen Festlegungen sollen möglichst unter rechtlicher Fachberatung erfolgen.

Um die Terminologie eindeutig und überschaubar zu halten, wird im Folgenden immer der Begriff Revokation für den endgültigen Widerruf eines Zertifikats und Suspendierung für die vorläufige, aufhebbare Sperre eines Zertifikats verwendet; meist werden beide Begriffe angegeben, da in der deutschsprachigen Literatur beide parallel verwendet werden.

Für Verzeichnisdienst, Directory etc. wird der Begriff Repository verwendet.

Es wird zwischen den natürlichen Personen Zertifikatsbesitzer (Eigentümer) und Zertifikatsnutzer (Anwender) unterschieden, um Differenzierungspotential in den Anwendungen zu haben.

3.1. Aufgaben und Pflichten

Gemeint sind vor allem die Pflichten gegenüber anderen Instanzen, die dieser CPS unterliegen.

3.1.1. CA-Pflichten

Beim Benachrichtigungsmechanismus sollte in jedem Fall eine E-Mail mit digitaler Signatur genutzt werden.

Archivierung, Logging etc. insbesondere als Vorgabe für externe Zertifizierungsdienstleister s. u.

3.1.1.1. Benachrichtigung über Zertifikatserstellung

Benachrichtigung der betroffenen Instanzen

3.1.1.2. Benachrichtigung bei Revokation/Widerruf oder Suspendierung/Sperrung eines Zertifikats

Benachrichtigung ggf. des Zertifikatsinhaber

3.1.1.3. Speicherung von Zertifikaten in Repositories oder Datenbasen

Speicherung erfolgt unmittelbar nach dessen Erstellung; Repository = Directory, Datenbasis, Datenbank

3.1.1.4. Dokumentation von Revokationen/Widerrufen in Repositories oder Datenbasen

Die Dokumentation ist schnellstens als Certificate Revocation Lists (CRLs) oder in einer anderen Form in einem Repository zu veröffentlichen.

3.1.2. RA-Pflichten

Analog zu „CA-Pflichten“

3.1.2.1. Benachrichtigung über Zertifikatserstellung

Wird vom jeweiligen Unternehmen ausgestaltet.

3.1.2.2. Benachrichtigung bei Revokation/Widerruf oder Suspendierung/Sperrung eines Zertifikats

Wird vom jeweiligen Unternehmen ausgestaltet.

3.1.3. Teilnehmer-Pflichten

Als Pflichten des Zertifikatsbesitzers gelten die nachstehenden Unterpunkte.

3.1.3.1. Genauigkeit bei der Angabe von Identifikationsdaten für Zertifikate

Wird vom jeweiligen Unternehmen ausgestaltet.

3.1.3.2. Schutz des privaten Schlüssels

Wird vom jeweiligen Unternehmen ausgestaltet.

3.1.3.3. Beachtung von Nutzungseinschränkungen von Schlüsseln

Wird vom jeweiligen Unternehmen ausgestaltet.

3.1.3.4. Benachrichtigung bei Offenlegung oder Missbrauch des privaten Schlüssels

Genaueres siehe dazu[8]

3.1.4. Nutzer-Pflichten

Pflichten desjenigen, der ein Zertifikat benutzt (siehe dazu [PKI-Policy])

3.1.4.1. Verwendungszweck der Zertifikate

Die Zertifikate werden im Geschäftsverkehr der deutschen Stromwirtschaft bei B2B-Transaktionen eingesetzt. Dazu gehören z. B. die Prozesse:

Kundenstammdatenübermittlung, Rechnungen, Zählwerte

auf Basis der unter 2.3 aufgeführten Anwendungen (insbesondere E-Mail, EDIFACT, XML).

Jeder Marktteilnehmer kann die Zertifikate für weitere Anwendungen (falls nicht explizit in 1.3.4 ausgeschlossen) einsetzen, wenn dadurch die Sicherheitsanforderungen nicht beeinträchtigt werden.

3.1.4.2. Verantwortlichkeiten bei der Validierung von Digitalen Signaturen

Der Nutzer muss bei der Validierung einer Signatur die Zertifikate der gesamten Zertifikatskette überprüfen können. Dabei sind jeweils zu prüfen: Unversehrtheit des Zertifikats, Einhaltung des Gültigkeitszeitraums, Einhaltung des Verwendungszwecks des Zertifikats, unwiderrufener und nicht gesperrter Zustand des Zertifikats.

---

[8] Anwendung von Schlüsselmaterial im elektronischen Geschäftsverkehr der deutschen Elektrizitätswirtschaft bei Verschlüsselung, elektronischer Signatur und Authentisierungsvorgängen

Umgang mit Schlüsselmaterial

Verantwortlichkeiten und Zugang zu den notwendigen Informationen bezüglich Prüfung auf Revokation/Widerruf oder Suspendierung/Sperre müssen beim Endanwender bekannt sein.

Einem Nutzer muss die neueste CRL leicht und möglichst automatisiert zugänglich sein und die Zertifikate müssen dagegen möglichst automatisiert geprüft werden können. Wenn ein Zertifikat in der CRL auftaucht, darf der Nutzer das Zertifikat nicht benutzen.

3.1.4.3. Verantwortlichkeiten bezüglich Prüfung auf Revokation/Widerruf oder Suspendierung/Sperre

Ein Nutzer muss sich die notwendigen Informationen (z. B. die neueste CRL) beschaffen können und die Zertifikate dagegen prüfen können. Wenn ein Zertifikat in der CRL auftaucht, darf der Nutzer das Zertifikat nicht benutzen.

3.1.4.4. Kenntnisnahme von geltenden Haftungsbeschränkungen und Garantien

Die Kenntnisnahme von geltenden Haftungsbeschränkungen und Garantien beim Endanwender garantiert der Marktteilnehmer (juristische Person) durch einen Zeichnungsberechtigten (natürliche Person).

3.1.5. Repository-Pflichten

Extern benötigte Zertifikate müssen in einem von extern zugänglichen LDAP-Verzeichnis (Replik oder Verzeichnisdienst-Proxy) für die berechtigten Kommunikationspartner abrufbar sein. Zum Abruf genügt die E-Mail-Adresse als vollqualifizierte Suchanfrage.

Das Repository muss die Zertifikate und CRLs unmittelbar nach Erhalt zugänglich machen.

Es darf die Zertifikate und CRLs nur von der zuständigen CA übernehmen. Die Bereitstellung erfolgt ereignisgetrieben innerhalb eines Arbeitstages.

3.2. Verantwortlichkeiten und Haftung

Angaben zur Haftung und deren Grenzen. Empfohlen wird eine vollständige Gleichstellung

- von elektronischer Form mit nicht elektronischer Form (keine 2-Klassen-Haftung)
- unabhängig von der Signaturkategorie (Qualifiziert/Fortgeschritten)
- unter Verweis auf die bisherigen Haftungs- und Verantwortungsregeln (PKI schafft keine neuen Regeln)

3.2.1. Verantwortlichkeiten und Haftung CA

Kein VDEW-Thema, allerdings sollte der Dienstleister (intern/extern) des Marktteilnehmers im Rahmen von SLA-Vereinbarungen entsprechend vertraglich verpflichtet werden.

3.2.1.1. Garantien und deren Grenzen

Wird vom jeweiligen Unternehmen ausgestaltet.

3.2.1.2. Art der abgedeckten und anerkannten Schadensfälle

Wird vom jeweiligen Unternehmen ausgestaltet.

3.2.1.3. Verlustabgrenzung (caps)

Bezogen auf das Zertifikat oder auf Transaktionen

3.2.1.4. Sonstige Ausschließungsgründe

Wird vom jeweiligen Unternehmen ausgestaltet.

3.2.2. Verantwortlichkeiten und Haftung der RA

Wie 3.2.1

3.2.2.1. Garantien und deren Grenzen

Wird vom jeweiligen Unternehmen ausgestaltet.

3.2.2.2. Art der abgedeckten und anerkannten Schadensfälle

Wird vom jeweiligen Unternehmen ausgestaltet.

3.2.2.3. Verlustabgrenzung (caps)

Wird vom jeweiligen Unternehmen ausgestaltet.

3.2.2.4. Sonstige Ausschließungsgründe

Wird vom jeweiligen Unternehmen ausgestaltet.

3.3. Finanzielle Verantwortlichkeit

Für jede CA, RA und jedes Repository

Dieser Abschnitt sollte unter Hinzuziehung einer juristischen Fachkraft formuliert werden. Nichtzutreffende Abschnitte sollten als solche kenntlich gemacht werden. Innerhalb einer Firmen-PKI, bei der einzelne Zertifikatsbesitzer an der Branchen-PKI teilnehmen, können im Rahmen und als Charakter von firmeninternen Regelungen einzelne Abschnitte weiter ausgearbeitet werden.

3.3.1. Entschädigung

von CA und/oder RA durch Nutzer

3.3.2. Treuhänderische Beziehungen

zwischen verschiedenen Instanzen oder auch deren ausdrücklicher Ausschluss

3.3.3. Verwaltungsvorgänge

Beispiel:

Abrechnungsverfahren, Rechnungsprüfung (Accounting, Audit)

3.4. Interpretation und Durchführung

Rechtliche Grundlagen der CPS für die Durchsetzung von Abmachungen, welche rechtlichen und vertrauensbildenden Charakter haben oder Verantwortungen festlegen.

3.4.1.1. Auftrennbarkeit der CPS

Es gilt weiter bestehende Gültigkeit des CPS auch bei Ungültigkeit von Teilen des CPS.

3.4.1.2. Fortbestehende Verpflichtungen

Es gilt weiter bestehende Verpflichtungen auch nach Auflösung des CPS.

Geschäftliche Transaktionen, die im Rahmen dieser Vereinbarungen geschlossen wurden, müssen abgewickelt werden, sofern keine anderen Vereinbarungen zwischen den betroffenen Marktteilnehmern greifen.

3.4.1.3. Zusammenschluss

Übergang von Rechte und Pflichten eines Zertifikats auf andere

Bei Carve-Outs, Mergern oder Akquisition sollten Rechte und Pflichten zunächst auf den neuen Eigentümer übergehen, bis die Gültigkeit aufgekündigt ist und wirksam geworden ist.

3.4.1.4. Notizen

Regeln zum Schriftverkehr zwischen den Parteien über dieses CPS

Fortschreibungen und Änderungen dieses Dokumentes werden durch den VDEW moderiert.

3.4.2. Zu beachtende Gesetze

Es gelten unverändert die gesetzlichen Anforderungen und Aufbewahrungspflichten für alle Dokumente, die den Anforderungen an die GoBS, Abgabenordnung (AO), GDPdU etc. genügen müssen.

Entsprechend sind die Anforderungen von Signaturgesetz (inkl. fortgeschrittener Signaturen), Bundesdatenschutzgesetz (BDSG) etc. zu beachten.

Es werden keine weitergehenden Festlegungen für Nutzdaten in der Policy getroffen.

Unabhängig von den gesetzlichen Anforderungen werden Definitionen in der Branche oder Vorgaben der Aufsichtsgremien für bestimmte Geschäftsvorfälle/-Prozesse zu berücksichtigen sein.

3.4.3. Aufteilung, Beendigung, Zusammenschluss, Notizen

Vorgehensweisen in Bezug auf das CPS, wenn Teile davon ungültig werden; Übergang von Rechten und Pflichten bei Auflösung der CA oder bei Zusammenschlüssen; „Notizen“ steht auch für „Absprachen“ oder „Anforderungen“

3.4.4. Schiedsverfahren

- Zur einvernehmlichen Beilegung von Meinungsverschiedenheiten, die die Auslegung dieser Zertifizierungsrichtlinie betreffen, richtet der VDEW bei Bedarf im Einzelfall eine Schiedsstelle ein. Sind alle jeweils beteiligten Marktpartner einverstanden, wird ein Schiedsverfahren durchgeführt.

- Die Schiedsstelle wird gebildet aus Verbandsvertretern und neutralen Sachkennern, die den Unternehmen der beteiligten Marktpartner nicht angehören dürfen.

- Die Teilnehmer am Schiedsverfahren sind zur Vertraulichkeit verpflichtet.

- Die Schiedsstelle wird den beteiligten Marktpartnern eine angemessene Regelung zur Beilegung der Meinungsverschiedenheit vorschlagen. Kommt hierdurch keine Einigung zustande, bleibt es jeder Partei unbenommen, die ihr zweckmäßig erscheinenden Schritte zu unternehmen.

- Die am Konflikt beteiligten Marktteilnehmer legen gegenüber der Schiedsstelle die technischen und organisatorischen Sachverhalte offen.

- Die Inanspruchnahme des Rechtsweges oder die Einleitung anderer Schritte bleiben unberührt.

3.5. Gebühren

Zahlungen von Teilnehmern und Nutzern an CA, RA, Repository

Im Rahmen der Verbandsarbeit werden dazu keine Empfehlungen ausgesprochen.

3.5.1. Ausstellung und Erneuerung von Zertifikaten

Wird vom Marktteilnehmer getragen

3.5.2. Zugriff auf Zertifikate

Wird vom Marktteilnehmer getragen

3.5.3. Widerruf/Revokation von Zertifikaten oder Zugriff auf den Zertifikatsstatus

Wird vom Marktteilnehmer getragen

3.5.4. Sonstige Dienste

Zurzeit ist kein zentraler Verzeichnisdienst vorgesehen, sondern optional ein Verzeichnisdienst-Proxy.

3.5.5. Erstattungsregeln

Im Rahmen der Verbandsarbeit werden dazu keine Empfehlungen ausgesprochen.

3.6. Veröffentlichung und Repository

Beschreibung der Anforderungen an die Veröffentlichung von und den Zugriff auf CP, CPS und CRLs

3.6.1. Veröffentlichung von CA-Informationen

Die Verpflichtung der CA, Informationen über ihre Durchführungspraktiken, ihre Zertifikate und deren derzeitigen Status zu veröffentlichen.

3.6.2. Häufigkeit der Veröffentlichung

CRL kurzfristig, mindestens innerhalb eines Arbeitstages

3.6.3. Zugriffsregeln für veröffentlichte Informationen

Soweit „Community-relevant“ lesend auf Zertifikate, Zertifikatszustand und CRLs innerhalb der geschlossenen Benutzergruppe. Der Zugriff auf Zertifikate erfolgt vollqualifiziert über die E-Mail-Adresse.

3.6.4. Benutzung von Repositories

Anforderungen, welche die Nutzung von Repositories betreffen, die durch CAs oder andere unabhängige Parteien betrieben werden.

Lesende Zugriffe werden von dem Unternehmen für Berechtigte freigeschaltet, das das Zertifikat veröffentlicht. Auch ein entsprechender Verzeichnisdienst-Proxy wird in analoger Berechtigung berücksichtigt. Das Zugriffsprotokoll sollte in der Regel LDAP sein.

Schreibender Zugriff ist extern nicht vorgesehen.

3.7. Revisionen über Regeleinhaltung

Die Revisionen sind unabhängige Kontrollen darüber, ob von CA, RA und anderen Instanzen die in der CP/CPS definierten Regeln eingehalten werden.

Revisionen über Regeleinhaltung: unabhängige interne Kontrollen/Audits durch hausinterne Revision

Veröffentlichung: veröffentlichter Revisionsbericht im Rahmen der geschlossenen Benutzergruppe

Umgang mit Mängeln siehe unten

Konfliktfälle im Außenverhältnis: siehe Schiedsverfahren

3.7.1. Abstände der Revisionen

Im Rahmen der Verbandsarbeit werden dazu keine Empfehlungen ausgesprochen. Für die interne Revisionssicherheit sind Regelungen sinnvoll (z. B. der Audit findet das erste Mal 3 Monate nach Inbetriebnahme der CA und dann in Abständen von mind. 24 Monaten statt.).

3.7.2. Identität und Qualifikationen des Auditors

Im Rahmen der Verbandsarbeit werden dazu keine Empfehlungen ausgesprochen. Für die interne Revisionssicherheit sind Regelungen sinnvoll (z. B. der Auditor ist geprüftes Mitglied des Revisorenteams des Unternehmens).

3.7.3. Beziehungen zwischen Auditor und Auditiertem

Im Rahmen der Verbandsarbeit werden dazu keine Empfehlungen ausgesprochen. Für die interne Revisionssicherheit sind Regelungen sinnvoll (z. B. im Sinne der Organisation oder im Sinne der PKI hierarchisch. Geprüft wird z. B. eine Level 2 CA durch eine Level 1 CA).

3.7.4. Geprüfte Topics

Im Rahmen der Verbandsarbeit werden dazu keine Empfehlungen ausgesprochen. Für die interne Revisionssicherheit sind Regelungen sinnvoll .

Beispiele:

Stichproben von Policies; umfassende Prüfung auf Einhaltung von Key-Management-Regeln, von Systemsicherheitskontrollen und Durchführungsregeln; umfangreichere Prüfungen von Zertifikatsprofilen

3.7.5. Maßnahme bei Mängeln

Im Rahmen der Verbandsarbeit werden dazu keine Empfehlungen ausgesprochen. Für die interne Revisionssicherheit sind Regelungen sinnvoll .

Beispiele:

Bei kleineren Auffälligkeiten Benachrichtigung der betroffenen Instanz (CA, RA, Repository, Teilnehmer) durch den Auditor; größere Mängel mit einer Behebungsfrist versehen und Nachkontrolle festlegen; dazu befristetes Aussetzen der Tätigkeiten, bis die Unregelmäßigkeiten beseitigt sind; bei Weiterbestehen der Mängel Revokation/Widerruf von Zertifikaten betroffener Instanzen; Personalumsetzungen; Verkürzung des Revisionsabstandes;

3.7.6. Veröffentlichung der Revisionsberichte

Im Rahmen der Verbandsarbeit werden dazu keine Empfehlungen ausgesprochen. Für die interne Revisionssicherheit sind Regelungen sinnvoll .

Beispiel:

Der Revisionsbericht muss intern veröffentlicht werden.

3.8. Geheimhaltung

Der Zertifikatsbesitzer muss in geeigneter Form informiert werden, welche der über ihn bestehenden Informationen vertraulich behandelt und welche in bestimmten Fällen weitergegeben werden.

In einer unternehmens-spezifischen CPS sind hier auch die Mittel zur physischen Rechnersicherheit (z. B. B1-Sicherheitssystem) und des Netzschutzes (z. B. Firewalls)

aufzuführen, die aufgewandt werden, wenn der Rechner, der die vertraulichen Informationen speichert, an das öffentliche Netz angeschlossen ist.

3.8.1. Art der geheim zu haltenden Information

betrifft vorwiegend CA oder RA

Hier sollen entweder

- detaillierte technische und nichttechnische Verfahren und Prozeduren zur Geheimhaltung der Informationen beschrieben werden, z. B. Informationen aus Dokumenten, die für die Identifikation und Authentisierung benutzt werden, wie Führerschein, Personalausweis, Registerauszüge.
- Hinweis auf entsprechende Dokumente des Dienstleisters

3.8.2. Öffentliche Informationen

Unter „öffentlich“ ist hier immer die Veröffentlichung zumindest in der geschlossenen Benutzergruppe gemeint.

3.8.3. Veröffentlichung von Informationen über Revokation oder Suspendierung vonZertifikaten

Eine entsprechende Veröffentlichung von Sperrinformationen sollte Angaben zu Personen enthalten, die berechtigt sind, über die Gründe für einen Revokation/Widerruf oder eine Sperre Auskunft zu geben.

Die Begründung einer unplanmäßigen Revokation ist eine öffentliche Information, um die Vertrauensinfrastruktur transparent zu halten und für die Teilnehmer einschätzbarer zu machen.

3.8.4. Weitergabe von Informationen an Ermittlungsinstanzen

Informationen, die für ein Ermittlungsverfahren offenbart werden können:

wie bisher, keine PKI-Sonderregelung

3.8.5. Weitergabe von Informationen im Rahmen einer zivilen Ermittlung

Informationen, die im Zuge eines zivilen Ermittlungsverfahrens weitergegeben werden können:

wie bisher, keine PKI-Sonderregelung

3.8.6. Veröffentlichung auf Wunsch des Besitzers von Informationen

Bedingungen, unter denen die CA oder RA Informationen veröffentlichen darf, wenn dies deren Besitzer wünscht.

Hier sollte nur zwischen „ganz öffentlich“ (Internet) und öffentlich in der geschlossenen Benutzergruppe unterschieden werden.

3.8.7. Sonstige Veröffentlichungsgründe

wie bisher, keine PKI-Sonderregelung

3.9. Geistiges Eigentum und dessen Rechte

wie bisher, keine PKI-Sonderregelung

4. Identifizierung und Authentisierung

Alle oder einige der nachfolgenden Abschnitte können für die verschiedenen Instanzen (CA, RA, End-Entities) unterschiedlich sein.

Da die sichere Identifikation und Authentisierung die Grundlage für die vertrauensbildende Verknüpfung von Namen und öffentlichem Schlüssel bildet, ist dieser Abschnitt extrem sicherheitsrelevant.

4.1. Erst-Registrierung

In diesem Abschnitt soll sichergestellt werden, dass sichere Verfahren zur Identifikation und Authentisierung von Zertifikatsbesitzern eingesetzt werden. Die organisatorischen Aspekte wurden in dem Dokument [PKI-Policy] bereits beschrieben.

Prinzipiell gilt: Ein Antragsteller für ein Zertifikat soll während des Anmeldeprozesses oder zumindest vor der Erstellung des Zertifikats eine Einverständniserklärung für Zertifikatsbesitzer unterzeichnen. Innerhalb eines auf der Transportebene geschützten Firmennetzes können Antragsteller und die Bearbeitungsstelle oder andere PKI-Dienstleister per E-Mail kommunizieren. Der Ausweis wird gegen Vorlage einer Legitimation persönlich abgeholt. Die PIN wird über einen anderen Weg zugestellt.

RA und CA kommunizieren grundsätzlich vertraulich und integer (z. B. über ein Virtual Private Network (VPN) mit elektronisch signierten Nachrichten).

4.1.1. Namenstypen für Subjekte

Siehe dazu das VDEW-Dokument[9]

Als technische Namen sind zulässig; X.500 Distinguished Names (DN), RFC822-Namen, X.400 O/R Names, Internet E-Mail-Adressen, URL

4.1.2. Sinnhafte Namen

„Sinnhaft“ bedeutet, dass die Namensform einen allgemein verständlichen Bedeutungsinhalt besitzt, der die Identität einer Person und/oder Organisation bestimmen kann. Dies mag für DN und RFC822-Namen mehr oder weniger zutreffen. Dabei kann der „sprechende Namensteil“ noch um einen firmenspezifischen nicht-sprechenden Anteil ergänzt werden.

4.1.3. Regeln zur Interpretation von Namenformen

Besonders zu beachten: Bei Verwendung von Organizational Name (O) als Bestandteil des Namens für einen Teilnehmer muss klargestellt werden, ob O nur eine zusätzliche Bezeichnung ist oder die Mitgliedschaft des Teilnehmers in der Organisation bedeutet. Es können sonst unberechtigte Sinnzusammenhänge entstehen (z. B. „Teilnehmer handelt im Sinne von O“).

Die Eindeutigkeit des Namensraumes innerhalb der lokalen und globalen Domäne sollte durch entsprechende Maßnahmen (OID) gewährleistet werden. Eine Namen-Domäne ist im Allgemeinen der Gültigkeitsbereich eines lokalen (im Sinne „begrenzten“) Verzeichnisdienstes (VD) – unabhängig von PKI (z. B. in einem Konzern mit Holding-Struktur). Dieser VD ist i. Allg. historisch gewachsen und hat nicht nur PKI-Anforderungen zu berücksichtigen. Ein Teil der Inhalte (z. B. Name, E-Mail) muss wegen der PKI-Thematik in einen globalen VD überführt werden und ggf. ergänzt werden (z. B. um Zertifikate). Die zunächst inkompatible Struktur des VD (Schema) und seine Inhalte (Felder) müssen in den globalen VD geeignet überführt werden. Dazu wird i. Allg. ein Austausch-Schema definiert. Grundsätzlich bestehen zwei Kommunikationsmöglichkeiten:

X.500 (DAP) und

LDAP (z. B. mit dem Austauschformat LDIF)

Dabei können Namenskonflikte entstehen.

4.1.4. Verfahren zur Auflösung von Namenskonflikten

Beschreibung des Verfahrens zur Entscheidung bei Namenskonflikten

Die Eindeutigkeit wird durch Namenszusätze bei den natürlichen Personen (z. B. peter.mueller17) und nicht durch Zusätze bei den Namen der juristischen Personen (Firmenname) erreicht.

4.1.5. Erkennung, Authentisierung und Rolle von geschützten Namen

CA-Namen und andere geschützte Namen (z. B. Global-ID der CA) sollten einvernehmlich definiert werden können.

---

[9] Technische PKI-Interoperabilität

4.1.6. Methode zum Besitznachweis des privaten Schlüssels

Es müssen Vorkehrungen getroffen sein, dass der Antragsteller beweisen muss, den privaten Schlüssel zu besitzen, der zum öffentlichen Schlüssel gehört und für den er den Antrag auf Zertifizierung stellt.

Dazu bekommt der Antragsteller in der Regel von der RA eine Information (Zufallszahl), die er signiert zurückschicken muss (Challenge-Response-Verfahren).

4.1.7. Authentisierung von Organisationen

Antragstellende Organisationen, die als Antragsteller auftreten, werden durch eine Person vertreten. Diese muss die Beweise beibringen, welche die Organisation authentisieren, und Beweise, die den Antragsteller als solchen autorisieren.

Beispiele:

Gründungsdokumente, ordnungsgemäß abgezeichnete gesellschaftliche Beschlüsse, Siegelzeichen des Unternehmens, notariell beglaubigte Dokumente.

4.1.8. Authentisierung von Personen

Für die Authentisierung von (natürlichen) Personen soll das gleiche Antragsverfahren gelten wie für antragstellende Organisationen. Es wird keine prinzipielle Einschränkung auf Mitarbeiter des Marktteilnehmers vorgenommen.

4.1.8.1. Benötigte Identifikationsbeweise

Pass/Ausweis, später offen für biometrische Mittel (Fingerabdrücke, Gesichtsabbild, Handfläche, Netzhautbild)

4.1.8.2. Validierung durch CA oder RA

Beschreibung der Verfahren zur Validierung von Identitätsbeweisen durch CA oder RA.

RA (Ausweisstelle, Personalabteilung, Postident-Verfahren etc.) prüft die Identität.

4.1.8.3. Persönliche Authentifizierung

Das Antragsverfahren muss zur eindeutigen Identifizierung der natürlichen Person führen.[10]

---

[10] Das Sicherheits-Level für den Registrierungsprozess sollte mit den Anforderungen der European Bridge-CA kompatibel sein, weil ggf. Dienste der EB-CA in Anspruch genommen werden. In der EB-CA Teilnahmeanforderung heißt es

„Persönliche Identifikation und Registrierung des Zertifikatsinhabers."

In der Selbsterklärung unter dem Punkt Identifikation:

„Die Nutzer der PKI sind zuverlässig zu identifizieren. Der Charakter anderer Zertifikate (Server-, Rollen-, Organisations-Zertifikate) muss eindeutig für die Empfänger erkennbar sein; ein als Pseudonym ausgestelltes Zertifikat muss als solches ebenfalls kenntlich sein."

Die Registrierung ist jedenfalls der organisatorisch sensibelste Prozess, der die zweifelsfreie Identifikation des Zertifikatsinhabers gewährleistet. Nur eine ununterbrochene Kausalkette zwischen Identifikation und Zertifizierung sollte akzeptiert werden. Ist diese aber gewährleistet, sollten flexible Organisationsmodelle zur Zeit- und Kostenoptimierung genutzt werden können.

4.1.8.4. Authentisierung einer natürlichen Person als Vertreter einer juristischen Person

Festlegungen darüber, ob und wie die Antragstellung von einer Person auf eine andere delegiert werden kann (analog zur Problematik in 3.1.8).

4.2. Schlüsselerneuerung im Normalfall

Identifikation und Authentisierung anlässlich einer Schlüssel- bzw. Zertifikatserneuerung

Dieser Fall tritt auf, wenn ein Zertifikat abläuft oder abgelaufen ist (betrifft sowohl CA und RA, als auch End-Entities). Unabhängig davon, ob in der Erneuerungsprozedur ein neues Schlüsselpaar erzeugt oder das bestehende weiterverwendet wird, gibt es Anforderungen an die Identifikation und Authentisierung des Schlüsselbesitzers, die hier festzulegen sind.

Erneuerung der Zertifikate vor deren Ablauf durch Identifizierung mit den bestehenden Zertifikaten ist möglich.

Die Anforderungen an die Zahl der Identitätsbeweise kann geringer sein als bei „Erst-Registrierung“, da die RA bereits Identitätsbeweise archiviert hat.

4.3. Schlüsselerneuerung nach Revokation

Zur Erinnerung: Revokation ist der nicht mehr rückgängig zu machende Widerruf eines Zertifikats; Suspendierung ist die temporäre Sperre.

Hier ist festzulegen, was bezüglich Identifikation und Authentisierung erforderlich ist, wenn nach einer Revokation/Widerruf der Teilnehmer (betrifft sowohl CA und RA, als auch End-Entities) ein neues Zertifikat erhalten soll (unabhängig davon, dass ein Schlüsselpaar nicht mehr weiterverwendet werden darf, wenn es einmal revoziert/widerrufen ist).

Erfolgte die Revokation/Widerruf wegen einer Offenlegung des privaten Schlüssels, wird wie bei „Erst-Registrierung“ verfahren.

Erfolgte die Revokation/Widerruf z. B. wegen einer Namensänderung, kann wie bei „Schlüsselerneuerung im Normalfall“ verfahren werden.

Widerrufsgründe: Beendigung eines Beschäftigungsverhältnisses, Namensänderung z. B. durch Heirat oder Umorganisation (DN-Änderung), Kündigung einer Mitgliedschaft, Offenlegung des privaten Schlüssels, Verlust des Schlüsselträgers für den privaten Schlüssel, Zweckentfremdung des privaten Schlüssels

Revokations/Widerrufsberechtigte sind Zertifikatsbesitzer, RA, Bevollmächtigte

Latenzzeit (Zeitdauer zwischen Erhalt und Sperrung): 2 Stunden

Sperrgründe sind:

- Genereller Verdacht auf Korrumpierung
- Es wird eine Smart Card gefunden.
- RA vermutet eine Offenlegung eines privaten Schlüssels und der Besitzer des dazugehörigen Zertifikats ist in Urlaub.

- Die RA erfährt von einer Vermutung, dass mit einem Schlüssel, der nur für Verschlüsselung zugelassen ist, Signaturen erzeugt worden sind.

4.4. Antrag auf Revokation

Hier sind die Anforderungen an Identifikation und Authentisierung des Antragstellers (CA, RA oder End-Entity) für einen Widerruf=Revokation zu definieren.

Die CA widerruft/revoziert ein Zertifikat, wenn der Zertifikatsbesitzer oder die zuständige RA einen signierten Revokations-/Widerrufsantrag sendet. Die RA sendet aber nur einen Revokations-Antrag, wenn der Zertifikatsbesitzer persönlich bei der RA erscheint oder sich nachweislich authentisiert und die Berechtigung für die Revokation/Widerruf nachweist (z. B. wenn er die Organisation vertritt, deren Zertifikat widerrufen werden soll).

Antragsberechtigte für Sperren: Zertifikatsbesitzer, RA, oder sonstige, in der Firmen-PKI-Policy festgelegte Instanzen (z. B. Personalabteilung, Mutterkonzern)

Antragsverfahren für Widerrufe auf Basis digital signiertem Antrag vom Marktteilnehmer: Zertifikatsbesitzer selbst, RA oder Bevollmächtigte

5. Operationelle Bedingungen

Betrifft CAs, RAs und End-Entites, wenn auch in unterschiedlichen Umfängen

5.1. Antrag auf Zertifizierung

Die RA sammelt die Antragsdaten und erstellt daraus den Zertifikatsantrag an die CA. Technisch sollte der PKCS#10-Request oder PKIX-CMP verwendet werden, signiert von der RA.

5.2. Erstellung des Zertifikats

Die CA erhält von der RA einen Antrag mit den zu beglaubigenden Daten, validiert diese und erzeugt dann das Zertifikat. Das Zertifikat wird an die RA zurückgesendet und in das Repository gestellt, so dass es innerhalb eines Arbeitstages in der geschlossenen Benutzergruppe abrufbar ist. Eine direkte Zustellung an den Zertifikatsbesitzer, z. B. bei erneuter Ausstellung, ist möglich.

5.3. Übernahme eines Zertifikats

Nach der Antragstellung erhält der Antragsteller das Zertifikat, das er anschließend bezüglich der organisatorischen Aussagen überprüfen muss.

5.4. Zertifikatsperre/-suspendierung und –widerruf/-revokation

5.4.1. Widerrufsgründe (Revokation)

Beendigung eines Beschäftigungsverhältnisses, Namensänderung z. B. durch Heirat oder Umorganisation (DN-Änderung), Kündigung oder Änderungskündigung der Mitgliedschaft am Verfahren, Offenlegung des privaten Schlüssels, Verlust des Schlüsselträgers für den privaten Schlüssel, Zweckentfremdung des privaten Schlüssels

5.4.2. Revokations-/Widerrufsberechtigte

Immer Zertifikatsbesitzer, RA und ggf. zusätzliche Instanzen, die der Marktteilnehmer benennt

5.4.3. Antragsverfahren für Revokationen/Widerrufe

Digital signierter Antrag vom Zertifikatsbesitzer oder von der RA.

Revoziert können alle Formen von End-Entity-Zertifikaten werden. Ein Antrag kann mehrere/viele Zertifikate betreffen.

5.4.4. Latenzzeit

Die Zeitdauer zwischen Erhalt eines Revokations/Widerrufsantrags bei der zuständigen CA und dem Wirksamwerden des Widerrufs/ Revokation

Veröffentlichung der CRL mit dem revozierten/ widerrufenen Zertifikat aktionsgetrieben innerhalb eines Arbeitstages

Wirksamwerden über OCSP: 10 Minuten

5.4.5. Sperrgründe/Suspendierung

Es wird eine SmartCard gefunden.

Die RA vermutet eine Offenlegung eines privaten Schlüssels und der Besitzer des dazugehörigen Zertifikats ist in Urlaub.

Die RA erfährt von einer Vermutung, dass mit einem Schlüssel, der nur für Verschlüsselung zugelassen ist, Signaturen erzeugt worden sind.

5.4.6. Antragsberechtigte für Suspendierung/Sperren

Zertifikatsbesitzer, RA

5.4.7. Antragsverfahren für Suspendierung/Sperren

Digital signierter Antrag von der RA, E-Mail vom Anwender innerhalb des Corporate Network, Webschnittstelle

Bewährt haben sich die Hinterlegung von Suspend-Kennwörtern für die telefonische Sperrung (analog Kreditkarten).

5.4.8. Suspendierungszeitbegrenzung

30 Tage, anschließend erfolgt Revozierung

5.4.9. Periode für CRL-Erstellung

Sollte eine Revokation oder Suspendierung stattgefunden haben, wird dies aktionsgetrieben innerhalb eines Arbeitstages durch das Einzelunternehmen angezeigt und je nach Gesamtarchitektur in einem weiteren Schritt durch den zentralen Verzeichnisdienst eine neue CRL veröffentlicht. Der Gesamtzeitraum bis zur allgemeinen Informationsbereitstellung für alle Verfahrensteilnehmer darf nicht länger als 24 h in Anspruch nehmen.

5.4.10. CRL-Prüfbedingungen

Anforderungen an den Zertifikatsbenutzer bei der Durchführung von Prüfungen anhand einer CRL

Es soll immer die neueste CRL verwendet werden. Diese muss als solche erkennbar sein.

5.4.11. Online-Prüfung des Zertifikatszustandes

Mit Verfahrensstart wird es optional über Zusatzdienste z. B. der European Bridge CA Möglichkeiten geben, den Revokations/Widerruf-Status eines Zertifikats Online zu prüfen (Validierungsdienst, OCSP-Responder).

5.4.12. Bedingungen für den Einsatz der Online-Prüfung des Revokations-/Widerruf-Status

Festlegung, unter welchen Bedingungen der Zertifikatsanwendung eine Online-Prüfung des Zertifikatszustandes bzgl. Revokation/Widerrufs durchgeführt werden sollte.

z. B. bei der Prüfung einer Finanztransaktion und bei jedem zu evaluierenden Zertifikat

5.4.13. Sonstige Hilfen/Beratungen für die Revokation/Widerrufsanfrage

web URL mit Hinweisen

5.4.14. Prüfbedingungen für andere Formen der Revokationsanzeige

entfällt

5.4.15. Spezielle Maßnahmen bei Schlüsseloffenlegung

Die oben definierten Anweisungen können variiert werden, wenn der Widerrufsgrund hinreichend ernst ist.

Bei einer Offenlegung des privaten Schlüssels erfolgt der Revokation/Widerruf im Schnellverfahren ohne Einwilligung des Zertifikatsbesitzers.

5.5. Security-Audit

Beschreibung des eingesetzten Event-Logging- und Audit-Systems

Firmen-intern weiter spezifizierbar

5.5.1. Aufzuzeichnende Ereignisse

Festlegung, welche Daten bei welchen Ereignissen zu sammeln sind, mit Zeitstempel zu versehen und /oder zu signieren sind. Grundsätzlich sind zu verfolgende Ereignisse solche, die den Life-Cycle von Schlüssel, Zustandsänderungen von PKI-Komponenten und die Kommunikation zwischen PKI-Komponenten (einschließlich End-Entities) betreffen.

Insbesondere:

Erzeugung eines Zertifizierungsantrags, Erzeugung eines Zertifikats, Auslieferung eines Zertifikats, Mitteilung einer Schlüsseloffenlegung, Stellung eines Revokation/Widerrufsantrags, Revokation/Widerruf eines Zertifikats, Erstellung einer CRL, Einrichtung von vertrauenswürdigen Rollen in der CA, Schlüsselwechsel der CA; Wechsel der Software-Version in der CA, administrative Aktionen einschließlich der für Auditing und Archivierung

5.5.2. Häufigkeit der Log-Bearbeitung

Die Loggingdaten sollten regelmäßig überprüft werden.

Review des Audit-Log: wöchentlich; ggf. automatisiert

Archivierung des Audit-Log: monatlich

5.5.3. Aufbewahrungsfristen

Aufbewahrung des Audit-Log außerhalb des Archivs: max. 1 Monat;

Aufbewahrung des Audit-Log im Archiv: mindestens 10 Jahre.

5.5.4. Backup-Verfahren für den Audit-Log

z. B. Archivierung durch den Auditor

5.5.5. Schutz des Audit-Log

Hier stehen die technischen und organisatorischen Anforderungen zur Gewährleistung der Sicherheit des Audit-Systems.

Technisch z. B. Betriebssystem mit C2-Sicherheit

5.5.5.1. Zugriffsberechtigte

Z. B. nur der Auditor

5.5.5.2. Änderungsberechtigte

Niemand

5.5.5.3. Löschberechtigte

Nur der Auditor nach Archivierung der Audit-Daten

5.5.6. Sammelsystem für Audit-Daten (intern vs extern)

Festlegung, ob die Datensammlung innerhalb oder außerhalb des Log-Systems stattfindet

z. B. bei der CA innerhalb der CA

5.5.7. Alarmierung

Festlegung, anhand welcher Ereignisse eine festzulegende Person oder ein Überwachungsprogramm über Log-Daten zu unterrichten oder zu alarmieren ist.

5.5.8. Beurteilung der Verwundbarkeit

Festlegung, wer und wann außergewöhnliche Ereignisse bezüglich Sicherheitsrisiken bewertet und berichtet

z. B. Vertreter von CA, RA und Repository wöchentlich

5.6. Archiv für Aufzeichnungen

Dieses Archiv bildet die Grundlage für Entscheidungen bei Streitfällen und für Untersuchungen über potentielle Sicherheitsrisiken.

Im Extremfall müssen Logdaten aber auch ihren Beitrag für den Nachweis einer betriebswirtschaftlich ordnungsgemäßen Transaktion nach GoBS absichern können. Dies geht bis zur Revisionssicherheit bei steuerlichen Außenprüfungen.

5.6.1. Zu archivierende Daten

Grundsätzlich sollen die Audit-Log-Daten archiviert werden, die eine Zustandsänderung des PKI-Systems belegen oder die eine Kommunikation zwischen wesentlichen Komponenten des PKI-Systems betreffen. Ebenfalls zu archivieren sind Daten mit historischem Charakter.

Einträge des Audit-Log wie z. B.:

Erzeugung eines Zertifikats, Mitteilung einer Schlüsseloffenlegung, Revokation/Widerruf eines Zertifikats, Erstellung einer CRL, Einrichtung von vertrauenswürdigen Rollen in der CA, Schlüsselwechsel der CA, Wechsel der Software-Version in der CA, administrative Aktionen für Auditing und Archivierung, CRLs, Key History, etc

5.6.2. Aufbewahrungsfristen

Empfohlen wird, die Aufbewahrung analog der handelsrechtlichen Vorgaben zur Revisionssicherheit und zur ordnungsgemäßen Buchführung gemäß §147 ff Abgabenordnung zu regeln.

5.6.3. Schutzmaßnahmen

5.6.3.1. Zugriffsberechtigte

Auditor, CA-Administrator

5.6.3.2. Änderungsschutz

u. a. auch die technischen und prozeduralen Maßnahmen festlegen bzw. auf bestehende verweisen

Änderungen durch Niemandem, erzwungen durch Archivierung auf write-once-read-only-Datenträger (WORM)

5.6.3.3. Löschschutz

u. a. auch die technischen und prozeduralen Maßnahmen festlegen bzw. auf bestehende verweisen

z. B. durch Verwahrung eines Duplikats im Tresor

5.6.4. Back-Up-Verfahren

Aufbewahrung von zwei Kopien an zwei verschiedenen Orten durch zwei verschiedene Personen; Vergleich beider Kopien, wenn eine zum Zweck des Restore benutzt wurde.

5.6.5. Zeitstempelung

Festlegung, ob und durch welchen Dienst eine Zeitstempelung der zu archivierenden Daten erfolgt bzw. erfolgen muss.

5.6.6. Datensammelsystem für die Archivierung

Festlegung, ob ein internes oder externes Datensammelsystem verwendet wird.

5.6.7. Verfahren zur Wiedergewinnung und Verifikation von Archivdaten

Festlegung, durch wen und mit welchen Mitteln in welcher Umgebung die Integrität von Archivdaten geprüft und sichergestellt wird.

Prinzip könnte sein: clean room – clean person – clean system

Der Auditor kontrolliert im Rahmen eines Security-Audit in einem gesicherten Raum (clean room) zwei Kopien von Archivdaten auf Übereinstimmung. Dazu verwendet er besonders geprüfte Stand-alone-Systeme mit gehärteten Betriebssystemen

5.7. Schlüsselwechsel

Beschreibt das Verfahren, mit dem ein Nutzer ein neues Zertifikat erhält, wenn in einer CA der Schlüssel gewechselt wird; vor dem Ablauf eines Zertifikats wird ein neues Schlüsselpaar und Zertifikat erzeugt, wobei das neue Schlüsselpaar für Signierungen eingesetzt wird und Verifikationen von „alten“ Signaturen mindestens bis zum Ablauf des alten Zertifikats möglich ist.

Beispiel:

Die CA erzeugt aus dem neuen öffentlichen Schlüssel zwei selbstsignierte Zertifikate (mit altem und neuem privaten Schlüssel) und aus dem alten öffentlichen Schlüssel mit dem neuen privaten Schlüssel ein drittes selbstsigniertes Zertifikat und gibt diese über die RAs als an die übrigen Nutzer weiter. Durch diese Art Cross-Zertifizierung können unvollständige Zertifizierungsketten in der Übergangsphase vervollständigt werden.

5.8. Wiederanlauf nach Schutzverletzung und Großschaden

Maßnahmen zur Unterrichtung und Schadensbehebung, falls bei der CA eine Kompromittierung der Sicherheit oder ein Schadensfall eingetreten ist.

Firmen-intern weiter spezifizierbar

Beispiel:

Die CA baut wieder die Sicherheitsumgebung auf:

- durch Generierung eines neuen Schlüsselpaars,
- Revokation/Widerruf aller von der CA erteilten Zertifikate,
- Übergabe des neuen öffentlichen Schlüssels an die RAs,
- von diesen aus Benachrichtigung aller Zertifikatsbesitzer über die Revokation/ Widerruf ihrer Zertifikate,
- Übergabe des neuen öffentlichen Schlüssels der CA an alle Teilnehmer,
- Installation neuer Schlüsselpaare für die RAs durch die RAs mit Zertifizierung durch die CA,
- die Teilnehmer oder die zuständigen RAs fordern neue Schlüssel bzw. Zertifikate bei der CA an.

5.8.1. Korrumpierte Ressourcen, Software und/oder Daten

5.8.2. Revozierter/Widerrufener Public-Key

5.8.3. Offengelegter Private-Key

5.8.4. Sicherheitsnotbetrieb nach einer Katastrophe

Beispiele:

Maßnahmen zur Diebstahlsicherung nach einem Großbrand, Transport und Übergabe der CA-Daten an eine Ausweich-CA

5.9. CA-Beendigung

Beschreibung der Maßnahmen, wenn eine CA oder RA aufgelöst wird, einschließlich der erforderlichen Benachrichtigungen und der geordneten Archivierung des Datenmaterials der CA oder RA.

6. Physische, prozedurale und personelle Sicherheitsmaßnahmen

Nicht-technische Maßnahmen für den ordnungsgemäßen Betrieb der CA bzgl. Schlüsselerzeugung, Authentisierung von Subjekten, Zertifikatserstellung und –revokation/widerruf, Audits und Archivierung mit unterschiedlichen Ausprägungen für CA, RA oder End-Entity.

6.1. Physische Sicherheit

Firmen-intern weiter spezifizierbar

Beispiele:

Monitore, Wachen, Schlösser, Karten für den Zutritt, biometrische Kontrollen, Kontroll-Listen

6.1.1. Ort und Aufbau der Rechenanlage

6.1.2. Zutrittsschutz

CAs und RAs sind in der Regel in Räumen mit Zutrittsschutz untergebracht; besondere Regeln für den Zutritt von Operator-, Wartungs- und Pflegepersonal

6.1.3. Stromversorgung und Klimaanlage

6.1.4. Wassereinbruchsschutz

6.1.5. Feuerverhütung und Feuerschutz

6.1.6. Speichermedien

6.1.7. Abfallentsorgung

Insbesondere Papier oder Datenträger, aus denen von Dritten sicherheitskritische Rückschlüsse gewonnen werden können, müssen sicher entsorgt werden.

6.1.8. Ausgelagertes Backup

Auslagerung einer Kopie der Audit- und Archivierungsdaten, der Unterlagen über Identität und Authentizität von Teilnehmern und der eingesetzten Software in räumlich getrennten und physisch sicheren Orten.

6.2. Prozedurale Schutzmaßnahmen

Bei sensitiven CA-Funktionen, Firmen-intern weiter spezifizierbar

6.2.1. Vertrauenswürdige Rollen

Rollen mit ihren Berechtigungen

Beispiele:

- System-Administrator

  Generierung, Konfigurierung, Hochfahren, Bedienung, Beendigung des Systems
- System-Sicherheitsoffizier

  Zuteilung von Accounts und Berechtigungen
- System-Auditor

  Planung und Durchführung von System-Audits, Verwaltung der Audit-Berichte, Review von Audits
- Administrator/Operator (RA, CA)

  Ausübung aller übrigen CA/RA-bezogenen operativen Funktionen
- Auditor, Archivar

  Verwaltung und Archivierung der Audit-Logs
- Sicherheitsoffizier

  Verfügungsgewalt über die in der CA eingesetzten kryptographischen Module CA einschließlich deren Aktivierung und Deaktivierung

So werden für die Zertifikats- und CRL-Erstellung der CA-Administrator und der Sicherheitsoffizier benötigt (der erstere startet das System, der zweite aktiviert die Krypto-Module).

Der Backup des privaten Schlüssels der CA wird durch den CA-Administrator und den System-Sicherheitsoffizier verwaltet.

Je eine Kopie der archivierten Daten ist unter der Zuständigkeit des Auditors und des Archivars.

6.2.2. Anzahl benötigter Personen je Aufgabe

Beispiele:

Zwei Personen nach dem 4-Augen-Prinzip

Zwei von vier möglichen Personen müssen ihre Chipkarte aktivieren, um eine CA-Funktion einzuschalten.

6.2.3. Identifikation und Authentisierung bei jeder Rolle

Beispiel:

Das CA-Computersystem erfordert individuelle Identifizierung und Authentisierung für jede Rolle. Die dazu benötigten Mechanismen erfüllen den Level C2 bzgl. Identifizierung und Authentisierung.

6.3. Personelle Schutzmaßnahmen

Firmen-intern weiter spezifizierbar

6.3.1. Anforderungen an Hintergrund, Qualifikation, Erfahrung und Sicherheit

Festlegung, welche Informationen durch wen überprüft werden

Beispiele:

Prüfung des Hintergrunds: Einbeziehung einer bereits erfolgten Sicherheitseinstufung (z. B. none, sensitive, confidential, secret, top secret etc.) und des Namen der überprüfenden Stelle ein.

Anstelle von oder zusätzlich zur Sicherheitseinstufung werden andere Informationen herangezogen (z. B. Name, Geburtsort, Geburtsdatum, aktuelle Anschrift, frühere Anschriften, frühere Beschäftigungsverhältnisse, sonstige Hintergrundinformationen, welche die Vertrauenswürdigkeit abschätzbar machen).

6.3.2. Sicherheitsüberprüfungen

Verfahren zur Klärung des Hintergrunds und der Unbedenklichkeit, wie sie für anderes Personal notwendig ist, z. B. Pförtner, Reinigungspersonal, usw., aber auch für Netzwerk-Administrator.

6.3.3. Anforderungen an die Ausbildung

Für jede Rolle zu definieren

6.3.4. Trainingwiederholungsmaßnahmen

Anforderungen und Häufigkeit für jede Rolle zu definieren

6.3.5. Häufigkeit und Abfolge von Job-Rotation

6.3.6. Maßnahmen bei unzulässigen Aktionen

Unautorisierte Aktionen, unberechtigter Gebrauch von Zuständigkeiten, unerlaubte Nutzung von Endsystemen usw.

Die Maßnahmen sollen unabhängig von der Person oder der Rolle definiert werden.

Für diesen Abschnitt sollte Hilfe der Rechts- und der Personalabteilung herangezogen werden.

6.3.7. Anforderung an die Gestaltung von Arbeitsverträgen

Für diesen Abschnitt sollte Hilfe der Rechts- und Personalabteilung herangezogen werden.

6.3.7.1. Bindende Anforderungen an das Vertragspersonal

Wird vom jeweiligen Unternehmen ausgestaltet.

6.3.7.2. Anforderungen an die Vertragsgestaltung

Mit Regelungen für den Schadensersatz bei Schäden, die durch Handlungen des Personals bei der vertragsabschließenden Partei beschäftigt sind

6.3.7.3. Auditierung und Überwachung von Vertragspersonal

Wird vom jeweiligen Unternehmen ausgestaltet.

6.3.7.4. Sonstige Kontrollen

Wird vom jeweiligen Unternehmen ausgestaltet.

6.3.8. Arbeitsunterlagen für Personal

7. Technische Sicherheitsmaßnahmen

Firmen-intern weiter spezifizierbar

Hauptziele: Schutz kryptographischer Schlüssel und deren Aktivierungsdaten (PINs, Passwörter) bei ihrer Erstellung, Speicherung, Transport und Nutzung; betrifft den Life Cycle von Schlüsseln und Zertifikaten und alle Instanzen (CAs und Repositories, RAs und End-Entities)

In die Spezifikation sind auch die Sicherheitskontrollen von Entwicklungsumgebungen oder die Entwicklungsmethodik für vertrauenswürdige Software mit einzubeziehen.

7.1. Erzeugung und Installation von Schlüsselpaaren

7.1.1. Erzeugung von Schlüsselpaaren

Beispiel:

Die CAs, RAs und End-Entities generieren ihre eigenen Schlüsselpaare und schützen ihren privaten Schlüssel so, dass keinerlei Zugriff auf ihn möglich ist (z. B. Setzen des Parametrisierungs-Bits „READ_NEVER“ bei Befehlen des SmartCard-Betriebsystems).

7.1.2. Ausgabe der privaten Schlüssel an die Beteiligten

Insbesondere Lieferung an End-Entities

7.1.3. Lieferung des öffentlichen Schlüssel an die Instanz für Zertifikatserzeugung

Minimalschutz ist digitales Signieren des öffentlichen Schlüssels

7.1.4. Übergabe der öffentlichen Schlüssel von der CA an die Nutzer

Die Schlüssel werden geschützt an die RA übergeben und dort an die Endbenutzer.

7.1.5. Schlüssellängen

Es gelten die vom BSI im Bundesanzeiger zu entsprechenden sicheren Algorithmen veröffentlichten empfohlenen Schlüssellängen.

7.1.6. Erzeugung von Public-Key-Parameterwerten

Die Parameter werden in dem Sicherheitsmodul erzeugt, das auch die Schlüsselpaare erzeugt oder in vergleichbarer Umgebung

7.1.7. Qualitätsprüfung von Parameterwerten

7.1.8. Hardware/Software für Schlüsselerzeugung

Die CA-Schlüsselpaare werden in einem Krypto-Hardware-Modul erzeugt. In den übrigen Instanzen darf auch ein Krypto-Software-Modul verwendet werden.

7.1.9. Verwendungszweck von Schlüsseln

Siehe Key Usage Fields von X.509 v3

Beispiel: für digitale Signaturen

Nähere Angaben siehe: Technische PKI-Interoperabilität

7.2. Schutz des privaten Schlüssels

Festzulegen für CAs, Repositories, RAs und End -Entities.

Für das Folgende gilt:

Die Absicht des Key-Recovery ist es, im Notfall einer berechtigten Person im Unternehmen den Zugang zum privaten Schlüssel ohne Einwilligung des Schlüsselbesitzers legal zu ermöglichen und damit Unternehmensdaten wieder entschlüsseln zu können. Für Verschlüsselungsschlüssel darf ein Key-Backup im eigenen Hause oder im Auftrag dessen vorgesehen werden; für Signierschlüssel im Rahmen der Verbands-PKI-Empfehlungen nicht.

Im Gegensatz dazu steht Key-Escrow

Key-Escrow (Hinterlegung bei Dritten, Notaren, staatliche Sicherheitsbehörden etc.) ist in Deutschland gesetzlich nicht vorgesehen (im Gegensatz zu Telekommunikationsdienstleister).

Eine Schlüsselhinterlegung von Schlüsseln, die nur Signierungszwecken dienen, ist immer unzulässig.

7.2.1. Standards für kryptographische Module

Die CA-Schlüsselpaare werden in einem FIPS 140-1 level 2 validierten Modul generiert. Dieser Standard wird in Kürze im europäischen Kontext durch das dem deutschen E4 hoch weitgehend entspricht, ersetzt.

Die übrigen Schlüssel (der RA, und Teilnehmer) werden in einem nach FIPS 140-1 level 1 (s. o. EAL4++) validierten Modul generiert.

7.2.2. Multi-personelle Kontrolle von privaten Schlüsseln

Aus dem privaten Schlüssel werden m Teile erzeugt und an m verschiedene Personen verteilt. Es sind jeweils genau n Personen mit ihren Schlüsselteilen notwendig, um den privaten Schlüssel zu rekonstruieren.

7.2.3. Verwahrung von privaten Schlüsseln (key escrow)

Falls eine Schlüsselhinterlegung stattfinden muss, sind die Aufbewahrungsagenten und -verfahren zu definieren. Eine Schlüsselhinterlegung von Schlüsseln, die nur Signierungszwecken dienen, ist immer unzulässig.

7.2.4. Backup von privaten Schlüsseln

Falls ein Backup vorgesehen ist, müssen hier beschrieben werden: der Agent für Backup, die Art und Weise und die Sicherheitsverfahren des Backup-Systems.

Falls kein Backup vorgesehen ist, muss eine Schlüsselerneuerung mit der Vergabe eines neuen Schlüsselpaars durchgeführt werden, allerdings ohne die Möglichkeit, den neuen Schlüssel mit dem alten zu signieren (in-band rekeying).

Beispiele:

Backup des privaten Schlüssels erfolgt in verschlüsselter Form. Ein Recovery sollte nur nach dem 4-Augen-Prinzip durch dazu berechtigte Personen erfolgen können.

7.2.5. Archivierung von privaten Schlüsseln

Falls eine Archivierung vorgesehen ist, müssen hier beschrieben werden: der Archivar, die Art und Weise und die Sicherheitsverfahren des Archiv-Systems.

Eine Archivierung privater Schlüssel (native) ist heute nicht begründbar.

7.2.6. Übergabe von privaten Schlüsseln an kryptographische Module

Zu definieren: Wer darf mit welchem Protokoll in welcher Form private Schlüssel in ein Krypto-Modul abspeichern, das z. B. im Rahmen eines Business Integration Servers für EDI genutzt wird.

7.2.7. Methoden zur Aktivierung von privaten Schlüsseln

Folgende Festlegungen sind zu treffen: Wer kann einen privaten Schlüssel durch welche Aktionen aktivieren; Dauer der Aktivierung (unendlich, nur für eine Aktion, für eine feste Zeitspanne etc.)

Der Schlüsselbesitzer muss ein Passwort (PIN) angeben. Der private Schlüssel wird dadurch entschlüsselt.

Die Zeitspanne sollte nicht unendlich sein.

Vorschlag: 1 mal pro Monat bei EDI-Systemen mit Kryptomodul, z. B. zur Rechnungskonvertierung und Signierung.

Vorschlag: 1 mal pro Session bei Karten-basierten Anwendungen. Kartenentnahme muss die Session beenden, d. h. den privaten Schlüssel deaktivieren.

7.2.8. Methoden zur Deaktivierung von privaten Schlüsseln

Folgende Festlegungen sind zu treffen: Wer kann einen privaten Schlüssel durch welche Aktionen deaktivieren.

Beispiel:

Aktionen = Logout, Power off, Remove Token, Automatik, Zeitablauf.

Der Schlüsselbesitzer deaktiviert beim Logout. Bei der Deaktivierung werden alle Schlüsselkopien im Speicher der Anwendungen vernichtet.

7.2.9. Methode zur Vernichtung von privaten Schlüsseln

Folgende Festlegungen sind zu treffen: Wer kann einen privaten Schlüssel durch welche Aktionen vernichten.

Private Schlüssel müssen unmittelbar nach Ablauf der Zertifikats des dazugehörigen öffentlichen Schlüssels und nach Schlüsselerneuerung vernichtet werden.

Beispiele:

Zerstörung der SmartCard,

Bei Verwendung von Krypto-Modulen Anwendung des eingebauten Zerstörungsmechanismus nach FIPS 140-1

7.3. Sonstige Aspekte des Schlüsselmanagements

Grundsätze:

Signaturen müssen auch nach Ablauf des Zertifikats evaluiert werden können. Empfohlen sind die Vorgaben für angemeldete Certification Authorities (z. Zt. 30 Jahre).

7.3.1. Archivierung von öffentlichen Schlüsseln

Folgende Festlegungen sind zu treffen: Wer kann einen öffentlichen Schlüssel durch welche Aktionen archivieren; Sicherheitsvorkehrungen.

Bei sehr langen Archivierungszeiten wird ein anderes Integritätsschutzverfahren als die digitale Signatur auf Einzeldatum verwendet. Dazu werden Hashbäume gebildet und es greifen die Prinzipien der Langzeitarchivierung elektronisch signierter Daten.

7.3.2. Nutzungszeiträume von öffentlichen und privaten Schlüsseln

Die Zeiträume hängen vom Stand der Krypto-Analysemethoden und von der Art der Anwendung ab.

Vorschlag:

Der private Schlüssel darf für 2 Jahre zum Signieren, der dazugehörige öffentliche Schlüssel für 7 Jahre für Signatur-Verifikationen verwendet werden.

7.4. Schlüssel-Aktivierungsdaten

Aktivierungsdaten sind (anders als Schlüssel) Daten, die benötigt werden, um kryptographische Module zu steuern (Beispiel: PIN oder Passphrase, die den Zugang zur SmartCard eröffnet). Für diese Daten gibt es ebenfalls einen Life-Cycle von der Generierung bis zur Archivierung oder Vernichtung und wie Schlüssel sind diese Daten vor Offenlegung zu schützen.

Die zu treffenden Festlegungen für Aktivierungsdaten betreffen alle Mitwirkenden der PKI (CA, RA, Repository, End-Entities).

7.4.1. Erzeugung und Installation der Schlüssel-Aktivierungsdaten

Das Passwort/PIN wird durch die in der Instanz eingebaute Schlüsselgenerierungsmethode erzeugt.

7.4.2. Schutz von Schlüssel-Aktivierungsdaten

Es gibt immer eine Transport-PIN, die vom Nutzer in eine Schlüsselaktivierungs-PIN geändert werden muss.

7.4.3. Sonstige Aspekte bei Schlüssel-Aktivierungsdaten

Siehe die Norm zum Password Management FIPS 181.

7.5. Maßnahmen zur Computer-Sicherheit

Hier sind festzulegen:

Einsatz eines Trusted Computing Base Concept, einer diskreten Zugriffskontrolle, von Labels, von Mandatory Access Control; Verfahren wie Object Reuse, Audit, Identifikation und Authentisierung, Trusted Path, Security Testing, Eindringversuche und –erkennung; Produktsicherheit, Entscheidung über Computer Security für Computersysteme (nach TCSEC, ITSEC usw.), Anforderungen an die Produktevaluierung, -tests, -zertifizierung, -zulassung

7.5.1. Spezifische technische Anforderungen an die Computer-Sicherheit

Die CA benutzt ein Betriebssystem, das nach C2 entworfen, implementiert und betrieben wird.

7.5.2. Auswahl der Sicherheitsmaßnahmen

7.6. Technische Kontrollen des Software-Life-Cycle

Technische Kontrollen im Sinne von Qualitätskontrollen sollten unabhängig von Auditierungen etabliert werden.

Betrifft:

Sicherheit der Entwicklungsumgebung, Sicherheitsanforderungen an die Entwickler, sicheres Konfigurationsmanagement in der Wartungsphase, Software-Engineering-Erfahrung, Software-Entwicklungsmethodik, Anforderungen an die Modularität und Schichtung, Anwendung des Fail-Safe-Prinzips, Implementierungstechniken (z. B. defensive programming), Sicherheitsbeurteilung (z. B. mit Trusted Software Development Methodology (TSDM) level IV and V, Software Engineering Institute's Capability Maturity Model (SEI-CMM)), Prüfwerkzeuge für die Einhaltung der Sicherheitsrichtlinien und Integrität im System und im Netzwerk, in Firm- und Hardware.

7.6.1. Kontrollmaßnahmen der Systementwicklung

7.6.2. Überwachung durch das Security Management

Festlegungen für ein Konfigurationsmanagement und Überwachung des Software-Life-Cycle, damit die eingesetzten Produkte die angestrebte Sicherheitsebene halten.

7.6.3. Beurteilung der Life Cycle Security

7.7. Kontrolle der Netzwerksicherheit

Betrifft: Network Security Related Controls, einschließlich Firewalls

7.8. Cryptographic Module Engineering Controls

Festlegungen zum Krypto-Modul: Identifizierung der Begrenzungen, Input/Output, Rollen, Dienste, Beschreibung der Finite State Machine, physische Sicherheit, Software-Sicherheit, Sicherheit des Betriebssystems, Einhaltung von Algorithmen, elektromagnetische Verträglichkeit, Selbsttests

8. Profile für Zertifikate und CRL

8.1. Zertifikatsprofil

siehe dazu das VDEW-Dokument [Technische PKI-Interoperabilität]

8.1.1. Unterstützte Versionen

X.509 version 3 siehe dazu das VDEW-Dokument [Technische PKI-Interoperabilität]

8.1.2. Certificate Extensions und ihre Kritikalität

siehe dazu das VDEW-Dokument [Technische PKI-Interoperabilität]

8.1.3. Objekt-Id für Verschlüsselungsalgorithmen

Es werden die vom BSI empfohlenen und veröffentlichten Algorithmen mit ihren Standard Objekt-ID´s verwendet.

8.1.4. Namensformate

DN für alle Instanzen (CA, RA, Repository, End-Entities)

8.1.5. Einschränkungen für Namensformen

siehe dazu das VDEW-Dokument [Technische PKI-Interoperabilität]

Es sollte auf Umlaute verzichtet werden.

8.1.6. Objekt-Id für Certificate-Policies

siehe dazu das VDEW-Dokument [Technische PKI-Interoperabilität]

PKIX-konform

8.1.7. Nutzung von Policy Constraints Extension

siehe dazu das VDEW-Dokument [Technische PKI-Interoperabilität]

8.1.8. Syntax und Semantik von Policy Qualifiers

8.1.9. Ausführung der Semantik der kritischen Certificate Policy Extension

8.2. CRL-Profile

Eine CRL enthält Version, Signature, Issuer Name, Date Issued, Issue Date for Next Update, Revoked Certificates.

8.2.1. Unterstützte Versionen

X.509 version 2

8.2.2. CRL, CRL Entry Extensions und ihre Kritikalität

CRL´s sollten ISIS-MTT kompatibel sein, wobei möglichst wenige Felder auf „kritisch“ gesetzt werden sollten.

9. Verwaltung der CPS-Spezifikationen

Festzulegen: Pflege dieser CPS

Arten der Änderungen:

Keine wesentliche Änderung; CPS-Pointer (URL) bleiben unverändert.

Wesentliche Änderung, Akzeptanz der CPS ist betroffen; neue URL für CPS nötig.

9.1. Änderungsverfahren

Möglicher Inhalt:

Liste von Abschnitten der CPS, die ohne Mitteilung geändert werden können;

CPS-URL bleiben unverändert;

Liste von Abschnitten, bei deren Änderung eine Mitteilung und Aufforderung zum Review (mit Beschreibung des Review-Verfahrens) verteilt werden muss:

Liste von Abschnitten, bei deren Änderung eine neue CPS-URL vergeben werden muss.

9.2. Veröffentlichungen und Mitteilungen

Beschreibung der Verteilungsverfahren für CP/CPS einschließlich Zugriffsbedingungen

Die Teile von unternehmensinternen Dokumenten, wie

- Policy
- Certification Policy
- Certification Practice Statement,

die sich in ihrem Regelungscharakter auf Schnittstellen zum Business Partner Network beziehen, sollten auf der Homepage des Unternehmens veröffentlicht bzw. der geschlossenen Benutzergruppe zugänglich gemacht werden. Änderungen sollten zeitnah gepflegt werden.

Die Dokumente sollten an den externen Schnittstellen nicht im Widerspruch zu Verbands-PKI-Empfehlungen stehen.

Eine Liste von Abschnitten, die nicht veröffentlicht werden, ist zulässig.

9.3. CP-/CPS-Verträglichkeit

Festlegung darüber, wie die Verträglichkeit zwischen CP und CPS erreicht werden kann.

Firmen-intern weiter spezifizierbar

10. Anhang: Weiterführende Informationen

- Einsatz von Verschlüsselung und Elektronischer Signatur im elektronischen Geschäftsverkehr der deutschen Elektrizitätswirtschaft

  Studie, Status veröffentlicht, 28 Seiten

- Sicherheitsrahmenbedingungen für den elektronischen Geschäftsverkehr im deutschen Strommarkt

  Gemeinsame Erklärung der Verbände

- Sicherheitspolitik (PKI-Policy), Version 1.0
  VDEW-Empfehlungen

- Umgang mit Schlüsselmaterial, Version 1.0
  VDEW-Empfehlungen

- Technische PKI-Interoperabilität, Version 1.0
  VDEW-Empfehlungen

- Umsetzungsempfehlungen, Version 1.0
  VDEW-Empfehlungen

- Zertifizierungsrichtlinie (Certification Practice Statement), Version 1.0
  VDEW-Empfehlungen