Zertifizierungsrichtlinie der HvS PKI

Version 1.1 vom 15.05.2020

Freigabe

	Datum
Erstellt: Marc Ströbel Technical Security Consultant HvS-Consulting AG	15.05.2020
Genehmigt: Michael Hochenrieder Vorstand HvS-Consulting AG	15.05.2020

Versionshistorie

Version	Datum	Autor	Änderungen
0.1	07.01.2013	Ströbel (HvS)	IS-FOX-Template
0.2	10.01.2013	Akbaba (HvS)	Anpassung sämtlicher Textstellen gem. Kommentare
1.0	22.01.2013	Hochenrieder (HvS)	Finales Review & Freigabe
1.1	15.05.2020	Hochenrieder (HvS)	Review & Update

Mitgeltende Unterlagen

Dokument	Veröffentlichung
Erklärung zum Zertifizierungsbetrieb der HvS PKI	http://www.hvs-consulting.de/pki

Inhaltsverzeichnis

1 Einleitung

Im nachfolgenden Dokument wird mit dem Begriff „HvS PKI" die Public Key Infrastructure (PKI) der HvS-Consulting abgekürzt.

1.1 Überblick

Die HvS PKI stellt eine Public-Key-Infrastruktur für die gesamte HvS bereit. Dieses Dokument definiert die Richtlinien für den Betrieb der HvS PKI. Es veranschaulicht die Einhaltung internationaler Standards für die Erstellung und Verwendung von Zertifikaten innerhalb der HvS.

Ein Zertifikat ist eine elektronische Bescheinigung, mit der ein öffentlicher, kryptografischer Schlüssel einer Person oder Organisation zugeordnet wird und mit der die Identität der Person oder Organisation bestätigt wird. Ein Zertifikat stellt also eine Verbindung zwischen einer Person oder Organisation und einem kryptografischen Schlüssel her. Jedes Zertifikat ist nur so vertrauenswürdig wie die Verfahren, nach denen es ausgestellt wird.

Die HvS PKI erstellt keine qualifizierten Zertifikate im Sinne des deutschen Signaturgesetzes. Damit sind diese Zertifikate nicht zur Durchführung von Rechtsgeschäften geeignet.
Diese Richtlinie ist angelehnt an das Internet "X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", veröffentlicht als RFC 3647 durch die IETF (Internet Engineering Task Force).

1.2 Dokumentenname sowie Identifikation

Diese Zertifizierungsrichtlinie ist folgendermaßen identifiziert:

- Titel: Zertifizierungsrichtlinie der HvS PKI (CP)
- Version: 1.1
- Object Identifier (OID): 1.3.6.1.4.1.39398.30.1.1.0

Der OID [OID] ist wie folgt zusammengesetzt:
{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) HvS(39398) pki(30) cp(1) major-version(1) minor- version(0)}

1.3 Teilnehmer der Zertifizierungsinfrastruktur (PKI)

1.3.1 Zertifizierungsstellen

Die Root-CA der HvS PKI ist eine Wurzelinstanz, d.h. der Root-CA Schlüssel ist selbstsigniert.

Untergeordnete CA-Zertifikate (Sub-CAs) werden von der Root-CA zertifiziert.

Die Sub-CAs stellen die Zertifikate der jeweiligen Endteilnehmer aus. Die ausgestellten Zertifikate werden u. a. auch in dem CA-System aufbewahrt. Die Root- und Sub-CAs unterzeichnen Rückruflisten (CRLs) mit ihrem privaten Schlüssel. Die Sub-CAs stellen Nutzerzertifikate aus. Hierbei handelt es sich um Zertifikate, deren Produktion den Regeln dieser Zertifizierungsrichtlinie der HvS PKI entsprechen.

Zertifikate der HvS PKI dürfen nur von Personen ausgestellt werden, den die dafür notwendigen Rollen von der HVS PKI-Administration zugewiesen wurden.

1.3.2 Registrierungsstellen
Keine Angaben.

1.3.3 Zertifikatsinhaber (Subscribers)
- Die HvS PKI stellt Zertifikate für natürliche Personen,
- Geräte (Hardware- oder Softwarekomponenten)

der HvS aus.

Grundlegende Voraussetzung für die Ausstellung eines Zertifikats ist, dass sich das Objekt, dem das Zertifikat zugeordnet ist, eindeutig identifizieren lässt. Der Zertifikatsinhaber ist diejenige Person oder Organisation, für die dieses Zertifikat gemäß den Zertifikatsattributen ausgestellt wurde und die den autorisierten Zugriff auf den zu einem Zertifikat gehörenden privaten Schlüssel besitzt.

1.3.4 Zertifikatsprüfer (Relying Parties)
Keine Angaben.

1.3.5 Weitere Zertifikatsinhaber
Keine Angaben.

1.4 Anwendungsbereich

Es werden zwei grundsätzliche Gruppen von Zertifikatstypen unterschieden:
- CA-Zertifikate
- Nutzer-Zertifikate

Nutzer-Zertifikate werden für folgende Anwendungsbereiche ausgestellt:
- Server Zertifikate (z.B. SSL/TLS)
- Benutzer Zertifikate (z.B. S-MIME-Verschlüsselung, SmartCard-Logon)
- Client Zertifikate (z.B. Computer-Zertifikate, Zertifikate für mobile Geräte, Netzwerkgeräte)
- Signatur Zertifikate (z.B. Signatur für Office-Dokumente)

Die Zertifikate des HvS PKI entsprechen nicht den Anforderungen des deutschen Signaturgesetzes.

1.4.1 Geeignete Zertifikatsnutzung
Die im Rahmen der HvS PKI ausgestellten Zertifikate können u.a. für Authentifizierung, elektronische Signatur, Verschlüsselung verwendet werden. Zertifikatnehmer sind selbst für die Nutzung in den Anwendungsprogrammen zuständig, sowie für die Prüfung, ob die damit möglichen Anwendungen den Sicherheitsanforderungen geeignet Rechnung tragen.

1.4.2 Untersagte Zertifikatsnutzung
Die Zertifikate dürfen nicht zur Verschlüsselung von gespeicherten Daten eingesetzt werden. Die Zertifikate dürfen nur für Zwecke genutzt werden, die im Attribut Key-Usage des Zertifikats hinterlegt sind.

1.5 Verwaltung der Zertifizierungsrichtlinie

1.5.1 Änderungsmanagement
Die Verwaltung dieses Dokuments erfolgt durch die PKI-Administration. Für Kontaktinformationen siehe Abschnitt 1.5.2.

1.5.2 Ansprechpartner

Zuständige Organisation

HvS-Consulting AG

Breiteicher Str. 15b

83064 Raubling

1.5.3 Freigabeverantwortliche für Dokumente zum HvS PKI

Die PKI-Administration der HvS ist für die Freigabe der Dokumente zur HvS PKI verantwortlich.

1.5.4 Eignungsprüfer für Regelungen für den Zertifizierungsbetrieb (CPS) gemäß Zertifizierungsrichtlinie

Siehe Kapitel 1.5.3

1.5.5 Verfahren zur Anerkennung von Regelungen für den Zertifizierungsbetrieb (CPS)

Siehe Kapitel 1.5.3

1.6 Definitionen und Abkürzungen

Siehe Kapitel 11.

2 VERÖFFENTLICHUNGEN UND VERZEICHNISDIENST

2.1 Verzeichnisdienste

Jede CA innerhalb der HvS PKI muss die in Abschnitt 2.2 genannten Informationen gemäß Abschnitt 2.3 und Abschnitt 2.4 vorhalten.

2.2 Veröffentlichung von Zertifizierungs-Informationen

Jede CA innerhalb der HvS PKI veröffentlicht folgende Informationen:

- Zertifizierungsrichtlinie der HvS PKI (CP)
- Erklärung zum Zertifizierungsbetrieb der Root- & Issue-CAs der HvS PKI (CPS)
- Root CA Zertifikat der HvS PKI inkl. Fingerabdruck
- Sperrinformationen der HvS PKI
- Kontaktinformationen, unter denen eine Sperrung beantragt werden kann

Diese Informationen werden für die Root-CA auf der Seite http://www.hvs-consulting.de/pki veröffentlicht.

2.3 Aktualisierung der Informationen (Zeitpunkt, Frequenz)

Für die Aktualisierung der in Abschnitt 2.2 genannten Informationen gelten folgende Fristen:

- Benutzer-Zertifikate: spätestens eine Woche nach der Ausstellung
- CP und CPS: spätestens eine Woche nach Erstellung einer neuen Version
- Liste der RAs: spätestens drei Werktage nach einer Veränderung
- CRLs: siehe Abschnitt 4.9.7

2.4 Zugangskontrolle zu Verzeichnisdiensten

Den Endteilnehmern und ggf. der Öffentlichkeit wird lesender Zugriff auf die o.g. Informationen gewährt. Schreibenden Zugriff haben nur autorisierte Personen der PKI-Administration (Fachbereich Infrastruktur). Die Systeme sind gegen unautorisierte Schreibzugriffe besonders geschützt.

3 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

In diesem Abschnitt werden die Prozeduren zur Feststellung der Identität eines Endteilnehmers, der ein Zertifikat beantragt, beschrieben.

3.1 Namen

3.1.1 Namensraum

In der HvS PKI wird eine einheitliche Namenshierarchie verwendet. Alle innerhalb der HvS PKI ausgestellten Zertifikate beinhalten eindeutige Namen (DN) gemäß der Normenserie X.500. Ein DN enthält eine Folge von kennzeichnenden Attributen, durch die jeder Zertifikatinhaber eindeutig referenziert wird:
C=<Staat>
[ST=<Bundesland>]
[L=<Ort>]
O=<Organisation>
[OU=<Organisationseinheit>]
CN=<Eindeutiger Name>
[emailAddress=<E-Mail Adresse>]

Attribute in eckigen Klammern sind optional anzugeben. Die Attribute „OU" und „emailAddress" dürfen auch mehrfach angegeben werden.

3.1.2 Aussagekraft von Namen

Das Pflichtattribut „C" muss das 2-Zeichen-Staaten-Kürzel (festgelegt im ISO Standard 3166-1 [ISO-3166-1]) des Staates enthalten, in dem die im Pflichtattribut „O" genannte Organisation ihren Standort hat.
Das optionale Attribut „ST" muss den offiziellen Namen des Bundeslandes enthalten, in dem die im Pflichtattribut „O" genannte Organisation ihren Standort hat.
Das optionale Attribut „L" muss den offiziellen Namen des Ortes enthalten, in dem die im Pflichtattribut „O" genannte Organisation ihren Standort hat.
Das Pflichtattribut „O" muss den Namen der Organisation des Zertifikatsinhabers enthalten. Die Authentizität des Namens wird nach Abschnitt 3.2.2 überprüft.
Falls das optionale Attribut „OU" ein oder mehrfach angegeben wird, muss es jeweils den Namen einer organisatorischen Untereinheit der im Pflichtattribut „O" genannten Organisation enthalten. Falls mehrere Attribute „OU" angegeben werden, müssen diese im DN jeweils direkt hintereinander aufgeführt werden und die Reihenfolge der benannten organisatorischen Untereinheiten sollte von größeren zu kleineren Untereinheiten absteigen.

Der DN enthält mindestens ein Attribut „CN". Jedes Attribut „CN" muss eine angemessene Darstellung des Namens des Zertifikatinhabers enthalten. Dabei muss folgendes gelten:

- Zertifikate für natürliche Personen dürfen nur auf einen zulässigen Namen des Zertifikatnehmers ausgestellt werden. Namenszusätze dürfen nur verwendet werden z.B. "CN=Manuela Musterfrau, Dr.".

Bei Namensgleichheit werden ab dem zweiten Namen unterschiedliche Vornamen verwendet.

- Zertifikate für Personengruppen bzw. Fachbereiche dürfen verwendet werden, z.B. "CN= Poststelle" oder „CN=Forensic“.
- Bei der Vergabe von Zertifikaten für Datenverarbeitungssysteme muss für den Namen der voll qualifizierte Domainname verwendet werden, z.B. "CN=svtest.hvs-consulting.de".
- Insbesondere sind sogenannte "Wildcard Zertifikate", z.B. "CN=*.hvs-consulting.de" nicht zulässig.
- Bei der Vergabe von Namen für Pseudonyme muss eine Verwechslung mit existierenden Namen, z.B. mit natürlichen Personen oder Organisationen, ausgeschlossen werden. Ebenso dürfen keine DNS-Namen, IP-Adressen oder andere innerhalb der HVS PKI benutzte Syntaxelemente verwendet werden. Ein Pseudonym darf keinen beleidigenden oder anzüglichen Inhalt enthalten. Der CN eines Pseudonyms muss mit dem Kennzeichen "PN:" beginnen, z.B. "CN=PN:Deckname".

3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsinhaber

Anonyme Zertifikate dürfen nicht ausgestellt werden.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Ausschließlich die folgenden Zeichen dürfen in Namen verwendet werden:
a-z A-Z 0-9 ' ( ) + , - . / : = ? Leerzeichen
Für die Ersetzung deutscher Sonderzeichen gelten folgende Substitutionsregeln:
Ä -> Ae, Ö ->Oe, Ü -> Ue, ä -> ae, ö -> oe, ü -> ue, ß -> ss
Sonderzeichen mit Akzenten verlieren diese. Ansonsten wird eine für das betreffende Zeichen gemeinhin verwendete Schreibweise aus den Zeichen a-z und A-Z so zusammengesetzt, dass der entsprechende Laut entsteht.

3.1.5 Eindeutigkeit von Namen

Vor der Zertifizierung muss die Korrektheit und Eindeutigkeit des angegebenen Namens von der zuständigen CA überprüft werden. Der DN eines Zertifikatnehmers muss eindeutig sein und darf nicht an unterschiedliche Zertifikatnehmer vergeben werden.
Bei Namensgleichheit gilt grundsätzlich das Prinzip: "Wer zuerst kommt, wird zuerst bedient". In Streitfällen entscheidet die zuständige CA.
Darüber hinaus muss jedem Zertifikat durch die ausstellende CA eine eindeutige Seriennummer zugeordnet werden, die eine eindeutige und unveränderliche Zuordnung zum Zertifikatnehmer ermöglicht.

3.1.6 Anerkennung, Authentifizierung und Funktion von Warenzeichen

Sofern sich der DN eines Zertifikats auf eine natürliche Person bezieht, ist eine Anerkennung von Warenzeichen nicht relevant. In allen anderen Fällen liegt es in der alleinigen Verantwortung des Zertifikatnehmers, dass die Namenswahl keine Warenzeichen, Marken- rechte usw. verletzt. Die CAs sind nicht verpflichtet, solche Rechte zu überprüfen. Falls eine CA über eine Verletzung solcher Rechte informiert wird, muss sie das Zertifikat sperren.

3.2 Identitätsüberprüfung bei Neuantrag

3.2.1 Nachweis des Besitzes des privaten Schlüssels

Keine Angaben.

3.2.2 Authentifizierung einer Organisation

Keine Angaben.

3.2.3 Authentifizierung natürlicher Personen

Die Authentifizierung der Identität einer natürlichen Person wird durch die jeweilige CA vorgenommen.

Bei allen Verfahren müssen folgende Informationen vorliegen und überprüft werden:

- Name, Vorname(n) und Namenszusätze
- E-Mail-Adresse
- Gültige HvS-Benutzerkennung

Der Zertifikatnehmer erscheint persönlich bei einer zuständigen CA. Ein Mitarbeiter der CA führt die Identitätsprüfung anhand der gültigen HvS-Benutzerkennung durch.

3.2.4 Nicht überprüfte Teilnehmerangaben

Außer den Angaben in Abschnitt 3.2.3 werden keine weiteren Informationen überprüft.

3.2.5 Überprüfung der Berechtigung

Keine Angaben.

3.2.6 Kriterien für Zusammenarbeit (Cross-Zertifizierung)

Die Möglichkeit der Cross-Zertifizierung besteht ausschließlich für die Root-CA der HvS PKI. Die Root-CA des jeweiligen Kooperationspartners ist anhand ihrer CP und CPS Dokumente sowie im Bedarfsfall einer Selbstauskunft bzw. eines vor Ort Audits durch die PKI-Administration (Fachbereich Infrastruktur) zu überprüfen.

3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung

Bei einer Schlüsselerneuerung für Zertifikate natürlicher Personen muss immer eine neue Erstregistrierung durchgeführt werden.

3.3.1 Routinemäßige Zertifikatserneuerung

Soweit technisch möglich erfolgt die routinemäßige Zertifikaterneuerung automatisiert, so lange ein gültiges Zertifikat mit selben Attributen vorhanden ist. Falls dies nicht möglich ist, muss gem. der definierten Methoden aus Abschnitt 3.2.3 zusätzlich die Authentifizierung der Identität geprüft werden.

3.3.2 Zertifikatserneuerung nach einer Sperrung

Nach dem Sperren eines Zertifikats kann eine Authentifizierung nicht mehr mit dem gesperrten Zertifikat durchgeführt werden. Ein Neuantrag muss an die zuständige RA gestellt werden.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Die Authentifizierung einer Sperrung kann auf die folgenden Arten erfolgen:

- Anforderung der IT-Hotline der HvS
- Sperrantrag (persönliches Vorsprechen, schriftlich, per Telefon oder elektronisch) bei (schriftlich, per Telefon, oder elektronisch), z.B. bei Verlust eines Endgeräts

4 ABLAUFORGANISATION (Certificate Life-cycle)

4.1 Zertifikatsantrag

4.1.1 Wer kann ein Zertifikat beantragen

In der HvS PKI können Zertifikatnehmer gemäß Abschnitt 1.3.3 Zertifikate beantragen.

4.1.2 Verfahren und Verantwortungen

Um ein Nutzer-Zertifikat zu erhalten, muss ein Antrag bei der zuständigen der Sub-CA eingereicht werden. Bei der CA müssen die folgenden Arbeitsschritte durchlaufen und dokumentiert werden:

- Prüfung des Zertifikatantrags (veröffentlich im Intranet der HvS) hinsichtlich Vollständigkeit und Korrektheit
- Prüfung der Eindeutigkeit des gewünschten DN sowie der Existenz einer gültigen HvS Benutzerkennung
- Prüfung des Vorliegens beziehungsweise
- Durchführung einer Authentifizierung der Identität nach Abschnitt 3.2.3
- Die Anträge in Papierform müssen archiviert und sicher aufbewahrt werden.

4.2 Bearbeitung von Zertifikatsanträgen

4.2.1 Durchführung von Identifikation und Authentifizierung

Die Identifizierung und Authentifizierung von Zertifikatnehmern wird gemäß Abschnitt 3.2 durchgeführt.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Ein Zertifikatantrag wird von der zuständigen CA akzeptiert, wenn alle Arbeitsschritte gemäß Abschnitt 4.1.2 erfolgreich durchlaufen wurden. Andernfalls wird der Zertifikatantrag abgewiesen und dies dem Antragsteller unter Angabe von Gründen mitgeteilt.

4.2.3 Bearbeitungsdauer bei Zertifikatsanträgen

Die Bearbeitungsdauer eines Zertifikatantrags beträgt grundsätzlich maximal eine Woche.

4.3 Zertifikatserstellung

4.3.1 Aufgaben der Zertifizierungsstelle

Die formalen Voraussetzungen für die Ausstellung eines Zertifikats werden durch die CA in angemessener Weise überprüft.

4.3.2 Benachrichtigung des Antragstellers

Nach der Zertifikatausstellung wird für Personenzertifikate (=Nutzerzertifikate) dem Zertifikatsinhaber das ausgestellte Zertifikat durch die CA auf einer SmartCard übergeben. Die zugehörige SmartCard PIN muss der Zertifikatsinhaber bei der Beantragung im Rahmen des Authentisierungsprozesses neu vergeben.
Server- / bzw. Client-Zertifikate werden online generiert bzw. entsprechend sicher auf die Zielssysteme transferiert.

4.4 Zertifikatsakzeptanz

Der Zertifikatnehmer ist verpflichtet, die Korrektheit des eigenen Zertifikats sowie des Zertifikats der ausstellenden CA nach Erhalt zu verifizieren.

4.4.1 Annahme des Zertifikats

Ein Zertifikat wird durch den Zertifikatnehmer akzeptiert, wenn das Zertifikat verwendet wird oder wenn innerhalb von 14 Tagen nach Erhalt kein Widerspruch erfolgt.
Durch Annahme des Zertifikats versichert der Zertifikatnehmer, dass sämtliche Angaben und Erklärungen in Bezug auf die im Zertifikat enthaltenden Informationen der Wahrheit entsprechen.

4.4.2 Veröffentlichung des Zertifikats durch die Zertifizierungsstelle

Wenn der Veröffentlichung eines Zertifikats nicht widersprochen wurde, wird dieses von einer CA über einen Informationsdienst (siehe Kapitel 2) veröffentlicht.

4.4.3 Benachrichtigung weiterer Instanzen durch die Zertifizierungsstelle

Eine Benachrichtigung weiterer Instanzen ist nicht erforderlich.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

4.5.1 Nutzung durch den Zertifikatsinhaber

Der Zertifikatnehmer muss Sorge tragen, dass sein privater Schlüssel angemessen geschützt ist und das Zertifikat in Übereinstimmung mit diesem CP eingesetzt wird.
Das Zertifikat ist unverzüglich zu sperren, wenn die Angaben des Zertifikats nicht mehr korrekt sind oder wenn der private Schlüssel abhandengekommen, gestohlen oder möglicherweise kompromittiert wurde.

4.5.2 Nutzung des Zertifikats durch die Relying Party

Zertifikatprüfer sollten vor der Nutzung eines Zertifikats dessen Gültigkeit überprüfen und das Zertifikat ausschließlich in Übereinstimmung mit dieser CP einsetzen.

4.6 Zertifikatserneuerung unter Beibehaltung des alten Schlüssels (Re-Zertifizierung)

Bei einer Zertifikaterneuerung ohne Schlüsselwechsel wird einem Zertifikatnehmer durch die zuständige CA ein neues Zertifikat unter Beibehaltung des alten Schlüsselpaars ausgestellt, sofern das Schlüsselpaar den kryptographischen Mindestanforderungen der aktuellen CP genügt, die im Zertifikat enthaltenen Informationen unverändert bleiben und kein Verdacht auf Kompromittierung des privaten Schlüssels vorliegt.

4.6.1 Gründe für eine Zertifikatserneuerung

Eine Zertifikaterneuerung kann beantragt werden, wenn die Gültigkeit eines Zertifikats abläuft.

4.6.2 Wer kann eine Zertifikatserneuerung beantragen

Eine Zertifikaterneuerung wird grundsätzlich durch den Zertifikatnehmer beantragt. Es obliegt der zuständigen Sub-CA, ob sie eine Zertifikaterneuerung aktiv unterstützt.

4.6.3 Ablauf der Zertifikatserneuerung

Der Ablauf der Zertifikaterneuerung entspricht den Regelungen unter Abschnitt 4.3, für die Identifizierung und Authentifizierung gelten die Regelungen gemäß Abschnitt 3.3.1.

4.6.4 Benachrichtigung des Zertifikatsinhabers nach Zertifikatserneuerung

Es gelten die Regelungen gemäß Abschnitt 4.3.2.

4.6.5 Annahme einer Zertifikatserneuerung
Es gelten die Regelungen gemäß Abschnitt 4.4.1.

4.6.6 Veröffentlichung einer Zertifikatserneuerung durch die Zertifizierungsstelle
Es gelten die Regelungen gemäß Abschnitt 4.4.2.

4.6.7 Benachrichtigung weiterer Instanzen durch die Zertifizierungsstelle
Es gelten die Regelungen gemäß Abschnitt 4.4.3.

4.7 Schlüssel- und Zertifikatserneuerung (Re-key)

Bei einer Zertifikaterneuerung mit Schlüsselwechsel wird einem Zertifikatnehmer, der bereits ein Zertifikat besitzt, durch die zuständige CA ein neues Zertifikat für ein neues Schlüsselpaar ausgestellt, sofern die im Zertifikat enthaltenen Informationen unverändert bleiben. Es wird analog zu Abschnitt 4.6 vorgegangen.

4.8 Zertifikatsmodifizierung

Änderungen von Zertifikatsinhalten sind nicht möglich. Wird ein Zertifikat mit geändertem Inhalt benötigt, so muss immer eine neue Erstregistrierung durchgeführt werden.

4.9 Widerruf / Sperrung und Suspendierung von Zertifikaten

4.9.1 Gründe für Widerruf / Sperrung
Ein Zertifikat muss gesperrt werden, wenn mindestens einer der folgenden Gründe vorliegt:
- Das Zertifikat enthält Angaben, die nicht gültig sind.
- Der private Schlüssel des Zertifikatnehmers wurde verloren, gestohlen, offen gelegt oder anderweitig kompromittiert bzw. missbraucht.
- Der Zertifikatnehmer ist nicht mehr berechtigt, das Zertifikat zu nutzen (siehe Abschnitt 1.3.3).
- Der Zertifikatnehmer hält die CP nicht ein.
- Der Zertifikatnehmer verlangt die Sperrung des Zertifikats.
- Das Zertifikat der Root-CA oder der entsprechenden Sub-CA wurde kompromittiert
- Die CA stellt den Zertifizierungsbetrieb ein.

4.9.2 Wer kann Widerruf / Sperrung beantragen
Sperrungen können vom Zertifikatnehmer oder von der zuständigen CA beantragt werden. Dritte können eine Sperrung beantragen, wenn sie Beweise vorlegen, dass einer der unter Abschnitt 4.9.1 genannten Gründe für eine Sperrung vorliegt. Die zuständige CA ist für die Dokumentation der Gründe für die Sperrung zuständig.

4.9.3 Ablauf von Widerruf / Sperrung
Verlangen Zertifikatnehmer eine Sperrung, so müssen sie sich gegenüber der zuständigen CA authentifizieren. Die möglichen Verfahren sind in Abschnitt 3.4 dargestellt.

4.9.4 Fristen für den Zertifikatsinhaber
Wenn Gründe (siehe Abschnitt 4.9.1) für eine Sperrung vorliegen, muss unverzüglich ein Sperrantrag gestellt werden.

4.9.5 Bearbeitungsfristen für die Zertifizierungsstelle
Eine CA muss eine Zertifikatsperrung unverzüglich vornehmen, wenn die Voraussetzungen dafür gegeben sind (siehe Abschnitt 4.9.3).

4.9.6 Anforderung zu Sperrprüfungen durch eine Relying Party
Siehe Abschnitt 4.5.2.

4.9.7 Häufigkeit der Sperrlistenveröffentlichung
CRLs müssen mindestens einmal pro Halbjahr erstellt und veröffentlicht werden. Wird ein Zertifikat gesperrt, muss umgehend (innerhalb von 24 Stunden) eine neue CRL erstellt und veröffentlicht werden.

4.9.8 Maximale Latenzzeit für Sperrlisten
Nach Erzeugung neuer CRLs müssen diese umgehend veröffentlicht werden.

4.9.9 Verfügbarkeit von Online-Statusabfragen (OCSP)
Keine Angaben.

4.9.10 Anforderungen an Online-Statusabfragen (OCSP)
Keine Angaben.

4.9.11 Andere verfügbare Formen der Widerrufsbekanntmachung
Keine Angaben.

4.9.12 Anforderungen bei Kompromittierung von privaten Schlüsseln
Bei einer Kompromittierung des privaten Schlüssels ist das entsprechende Zertifikat unverzüglich zu sperren. Bei einer Kompromittierung des privaten Schlüssels einer CA werden alle von ihr ausgestellten Zertifikate gesperrt.

4.9.13 Gründe für eine Suspendierung
Eine Suspendierung (zeitliche Aussetzung) von Zertifikaten ist nicht erlaubt. Einmal gesperrte Zertifikate können nicht erneuert oder verlängert werden.

4.9.14 Wer kann Suspendierung beantragen
Keine Angaben.

4.9.15 Ablauf einer Suspendierung
Keine Angaben.

4.9.16 Maximale Sperrdauer bei Suspendierung
Keine Angaben.

4.10 Dienst zur Statusabfrage von Zertifikaten (OCSP)

Die Pflicht jeder CA zur Bereitstellung einer CRL ist in 2 geregelt.
Werden weitere Dienste zur Statusabfrage von Zertifikaten (z.B. OCSP) von einer CA angeboten, sind die Verfahrensmerkmale, die Verfügbarkeit des Dienstes und die optionalen Merkmale im zugehörigen CPS aufzuführen.

4.10.1 Betriebsbedingte Eigenschaften
Keine Angaben.

4.10.2 Verfügbarkeit des Dienstes
Keine Angaben.

4.10.3 Weitere Merkmale
Keine Angaben.

4.11 Beendigung des Vertragsverhältnisses

Eine Beendigung der Zertifikatnutzung erfolgt durch Zertifikatnehmer entweder durch eine Sperrung oder indem nach Ablauf der Gültigkeit kein neues Zertifikat beantragt wird.

4.12 Schlüsselhinterlegung und –wiederherstellung

Die Root-CA bietet keine Schlüsselhinterlegung und -wiederherstellung für Zertifikatnehmer an.
Diese Aufgabe übernimmt die HvS Issue-CA.

4.12.1 Richtlinien und Praktiken zur Schlüsselhinterlegung und –wiederherstellung
Bei Erstellung eines neuen Nutzer-Zertifikats wird automatisch der private Schlüssel in der PKI hinterlegt.

4.12.2 Richtlinien und Praktiken zum Schutz und Wiederherstellung von Sitzungsschlüsseln
Muss aus berechtigten Gründen (z.B. Verlust einer SmartCard) der private Schlüssel eines Zertifikatnehmers wiederhergestellt werden, so ist dies nur nach folgendem Prozess möglich:

- Zugriff auf SmartCard des Key-Recovery-Agents im Vier-Augen-Prinzip
  - Öffnung des Tresors (durch spezielle Mitarbeiter der Verwaltung)
  - Zugriff auf SmartCard (durch spezielle Mitarbeiter der PKI-Administration, Fachbereich Infrastruktur)
- Wiederherstellung des Schlüssels durch speziell ausgebildete PKI-Administratoren der PKI-Administration (Fachbereich Infrastruktur)
- Dokumentation, Information an den Datenschutzbeauftragten und Rückgabe der SmartCard des Key-Recovery-Agents

5 INFRASTRUKTURELLE, ORGANISATORISCHE UND PERSONELLE SICHERHEITSMASSNAHMEN

Die Gewährleistung geeigneter infrastruktureller, organisatorischer und personeller Sicherheitsmaßnahmen ist eine Voraussetzung für den sicheren Betrieb einer PKI.

5.1 Infrastrukturelle Sicherheitsmaßnahmen

Jede CA muss in ihrem CPS die infrastrukturellen Sicherheitsmaßnahmen beschreiben.

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 Rollenkonzept

Für den Betrieb der HvS PKI werden unterschiedliche interne und externe Rollen definiert. Diese Rollen beschreiben die Tätigkeiten, die durch den einer Rolle zugeordneten Personenkreis durchgeführt werden dürfen. Im Folgenden werden die Rollen der Kundenschnittstelle beschrieben:

Die Rollen sind an verschiedene Rahmenbedingungen gebunden:

- Unvereinbarkeit: Unvereinbare Rollen dürfen nicht von ein und derselben Person wahrgenommen werden.
- Aufgabentrennung: Bestimmte Tätigkeiten innerhalb einer Rolle müssen von unterschiedlichen Personen ausgeführt werden. Durch diese Trennung wird bei bestimmten Aufgaben ein vier Augenprinzip gewährleistet.

In der folgenden Tabelle sind die sicherheitsrelevanten Rollen definiert, die im Rahmen des Zertifizierungsprozesses erforderlich sind. Um einen ordnungsgemäßen und revisionssicheren Betrieb einer CA zu gewährleisten, muss eine entsprechende Aufgabenverteilung und Funktionstrennung vorgenommen werden. Es ist möglich, eine Rolle auf mehrere Mitarbeiter zu verteilen. Ebenso kann ein Mitarbeiter in mehr als einer Rolle auftreten, dabei sind die Rollenunverträglichkeiten aus Abschnitt 5.2.4 zu beachten.

Erweiterungen am Rollenmodell sind möglich, müssen aber im CPS beschrieben werden.

Rolle	Aufgabe der Rolle	Kürzel
CA-Mitarbeiter aus PKI-Administration	Entgegennahme und Prüfung von Zertifikat- und Sperranträgen. Authentifizierung der Identität und Prüfung der Autorisierung der Zertifikatnehmer. Verifikation der Dokumente. Beratung der Zertifikatnehmer. Freigabe, Übermittlung von Zertifikat- und Sperranträgen an die zuständige CA.	CA-M
CA-Administrator	Installation, Konfiguration, Administration und Wartung der PKI-Systeme. Kontrolle über die eingesetzte Hard- und Software Betreuung der Datensicherung und –Wiederherstellung der erforderlichen Server und der CA-Anwendungssoftware.	CA-A
Auditierung Datenschutz	Durchführung der betriebsinternen Audits, Überwachung und Einhaltung der Datenschutzbestimmungen.	A

Tabelle: Rollen

5.2.2 Anzahl involvierter Personen pro Aufgabe

In der nächsten Tabelle sind die Tätigkeiten beschrieben, bei denen das Vier-Augen-Prinzip realisiert durch jeweils einen Vertreter der angegebenen Rollen - eingehalten werden muss. Alle anderen Tätigkeiten können von einer Person durchgeführt werden.

Tätigkeit	Rollen
Key-Recovery von privaten Schlüsseln	CA-M & A
Erzeugung von Schlüsselpaaren für CA-Zertifikate	CA-A & A
Austausch von Hard- und Softwarekomponenten für die Zertifizierung	CA-A & A

Tätigkeiten, die das Vier-Augen-Prinzip erfordern

5.2.3 Identifizierung und Authentifizierung jeder Rolle

Die Identifizierung und Authentifizierung der Rollen muss auf Grundlage des in Abschnitt 5.2.1 und Abschnitt 5.2.2 beschriebenen Rollenmodells erfolgen. Der technische Zugang zu den IT-Systemen wird durch Nutzerkennung und Passwort oder ein stärkeres Verfahren realisiert, eine Regelung zum Passwortgebrauch ist vorzuhalten. Der physische Zugang zu den IT-Systemen muss durch Zutrittskontrollmaßnahmen reglementiert werden.

5.2.4 Rollen, die eine Aufgabentrennung erfordern

Keine Angaben.

5.3 Personelle Sicherheitsmaßnahmen

Jede CA muss in ihrem CPS die personellen Sicherheitsmaßnahmen beschreiben.

5.4 Überwachung / Protokollierung

Jede CA muss in ihrem CPS die Maßnahmen zur Sicherheitsüberwachung beschreiben.

5.5 Archivierung

Jede CA muss in ihrem CPS die Maßnahmen zur Archivierung beschreiben.

5.6 Schlüsselwechsel der Zertifizierungsstelle

Jede CA muss in ihrem CPS die Maßnahmen zur Archivierung beschreiben.

5.7 Kompromittierung und Wiederherstellung (disaster recovery)

5.7.1 Vorgehen bei Sicherheitsvorfällen und Kompromittierung

Die Prozeduren zur Behandlung von Sicherheitsvorfällen und bei der Kompromittierung von privaten Schlüsseln einer CA müssen schriftlich dokumentiert und an alle Mitarbeiter ausgehändigt werden. Die Grundzüge der Prozeduren sind in den folgenden Unterkapiteln aufgeführt.

5.7.2 Betriebsmittel, Software und/oder Daten sind korrumpiert

Werden innerhalb einer CA fehlerhafte oder manipulierte Rechner, Software und/oder Daten festgestellt, die Auswirkungen auf die Prozesse der CA haben, darf der Betrieb des entsprechenden IT-Systems nicht fortgesetzt werden, bis die Schwachstelle beseitigt ist. Bei Verdacht einer vorsätzlichen Handlung müssen gegebenenfalls rechtliche Schritte eingeleitet werden.

5.7.3 Kompromittierung des privaten Schlüssels

Wurde ein privater Schlüssel eines Zertifikatnehmers kompromittiert, so muss das dazugehörige Zertifikat gesperrt werden (siehe Abschnitt 4.9.1).
Wurde der private Schlüssel einer CA kompromittiert, so müssen das Zertifikat der CA und alle damit ausgestellten Zertifikate gesperrt werden. Außerdem müssen alle betroffenen Zertifikatnehmer informiert werden.

5.7.4 Wiederaufnahme des Betriebs nach einem Notfall

Eine Wiederaufnahme des Zertifizierungsbetriebs nach einer Katastrophe muss Bestandteil der Notfallplanung sein und innerhalb kurzer Zeit erfolgen können, sofern die Sicherheit der Zertifizierungsdienstleistung gegeben ist.

5.8 Einstellung des Betriebs

Stellt eine CA ihren Betrieb ein, müssen folgende Maßnahmen ergriffen werden:

- Information aller Zertifikatnehmer und der Kontaktperson aus Abschnitt 1.5.2 mindestens drei Monate vor Einstellung des Betriebs
- Sperrung aller von der CA ausgestellten Zertifikate
- Sichere Zerstörung der privaten Schlüssel der CA

Der Betreiber der CA muss den Fortbestand der Archive und die Abrufmöglichkeit einer vollständigen Sperrliste für den zugesicherten Aufbewahrungszeitraum (siehe Abschnitt 5.5) sicherstellen.

6 TECHNISCHE SICHERHEITSMASSNAHMEN

Die Gewährleistung geeigneter technischer Sicherheitsmaßnahmen ist eine Voraussetzung für den sicheren Betrieb einer PKI. Diese Sicherheitsmaßnahmen müssen von jeder CA in ihrem CPS in ihren wesentlichen Grundzügen beschrieben werden. Detaillierte Informationen sollten in einem Sicherheitskonzept festgeschrieben werden. Dieses muss nicht veröffentlicht werden, aber im Rahmen der Konformitätsprüfung (siehe 8) zur Verfügung stehen.

6.1 Schlüsselerzeugung und Installation

6.1.1 Schlüsselerzeugung

Die Schüsselpaare aller CAs werden auf DVD-RAMs gespeichert und im Tresor abgelegt.

6.1.2 Übermittlung privater Schlüssels an Zertifikatsinhaber

Keine Angaben.

6.1.3 Übermittlung öffentlicher Schlüssels an Zertifikatsaussteller

Keine Angaben.

6.1.4 Übermittlung öffentlicher CA Schlüssels an Zertifikatsprüfer (Relying Parties)

Alle Zertifikatsinhaber der HvS PKI können den öffentlichen Schlüssel jeder CA über einen Informationsdienst gemäß Kapitel 2 abrufen.

6.1.5 Schlüssellängen

Bei der HvS PKI muss bei Einsatz des RSA-Algorithmus die Schlüssellänge bei CAs mindestens 4096 Bit betragen, bei allen anderen Schlüsseln mindestens 2048 Bit.

6.1.6 Erzeugung der Public Key Parameter und Qualitätssicherung

Alle Zertifikate werden unter Verwendung des SHA-256 Algorithmus signiert.

6.1.7 Schlüsselverwendungszwecke (X.509v3 Key Usage)

Die privaten Schlüssel der CAs dürfen ausschließlich für die Ausstellung von Zertifikaten und für die Signatur von Sperrinformationen verwendet werden.

6.2 Schutz privater Schlüssel und Einsatz kryptographischer Module

6.2.1 Standard kryptographischer Module

Keine Angaben.

6.2.2 Aufteilung privater Schlüssel auf mehrere Personen (n-aus-m)

Keine Angaben.

6.2.3 Keine Angaben Hinterlegung privater Schlüssel (Key Escrow)

Keine Angaben.

6.2.4 Keine Angaben Backup privater Schlüssel

Die Sicherung der privaten Schlüssel HvS PKI erfolgt in verschlüsselter Form. Die Entschlüsselung erfolgt über einen Key-Recovery-Agent. Die Verschlüsselung erfolgt mit AES-256.

6.2.5 Archivierung privater Schlüssel

Keine Angaben.

6.2.6 Transfer privater Schlüssel in oder aus einem kryptographischen Modul

Keine Angaben.

6.2.7 Speicherung privater Schlüssel in einem kryptographischen Modul

Keine Angaben.

6.2.8 Aktivierung privater Schlüssel

Keine Angaben.

6.2.9 Deaktivierung privater Schlüssel

Keine Angaben.

6.2.10 Vernichtung privater Schlüssel

Keine Angaben.

6.2.11 Güte kryptographischer Module

Siehe Abschnitt 6.2.1.

6.3 Weitere Aspekte des Schlüsselmanagements

6.3.1 Archivierung öffentlicher Schlüssel

Siehe 5.5.

6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren

Die in der HvS PKI ausgestellten Zertifikate haben folgende Gültigkeitsdauer:

- Zertifikate für CAs (auch für die Root-CA): maximal zwanzig Jahre
- Zertifikate für untergeordnete CAs: maximal zehn Jahre
- Zertifikate für Datenverarbeitungssysteme (Serverzertifikate): maximal zwei Jahre
- Zertifikate für natürliche Personen (Bennutzerzertifikate): maximal zwei Jahre
- Zertifikate für Endgeräte und Anwendungen (Clientzertifikate): maximal zwei Jahre

Zertifikate können nicht länger gültig sein als das ausstellende CA-Zertifikat.
Für die Nutzungsdauer von Schlüsselpaaren gelten die Regelungen aus Abschnitt 6.1.6.

6.4 Aktivierungsdaten

6.4.1 Erzeugung und Installation der Aktivierungsdaten

Keine Angaben.

6.4.2 Schutz der Aktivierungsdaten

Keine Angaben.

6.4.3 Weitere Aspekte

Keine Angaben.

6.5 Sicherheitsmaßnahmen für Computer

6.5.1 Spezifische Anforderungen an technische Sicherheitsmaßnahmen

Alle CAs dürfen ausschließlich auf Basis von gehärteten Betriebssystemen betrieben werden. Darüber hinaus müssen Zugriffskontrolle und Nutzerauthentifizierung als Sicherheitsmaßnahmen umgesetzt werden.

6.5.2 Güte der Sicherheitsmaßnahmen

Ein formales Rating der Computersicherheit findet nicht statt. Die in Abschnitt 6.5.1 genannten Sicherheitsmaßnahmen müssen dem aktuellen Stand der Technik entsprechen.

6.6 Technische Maßnahmen im Lebenszyklus

Jede CA muss in ihrem CPS den Lebenszyklus der Sicherheitsmaßnahmen beschreiben.

6.7 Sicherheitsmaßnahmen für das Netzwerk

Jede CA muss in ihrem CPS die Sicherheitsmaßnahmen für das Netzwerk beschreiben.

6.8 Zeitstempel

Keine Angaben.

7 PROFILE FÜR ZERTIFIKATE, SPERRLISTEN UND ONLINESTATUSABFRAGEN

7.1 Zertifikatsprofil

7.1.1 Versionsnummer

Zertifikate werden entsprechend der internationalen Norm X.509 in der Version 3 ausgestellt.

7.1.2 Zertifikatserweiterungen

Grundsätzlich sind alle Zertifikaterweiterungen nach [X.509], [NETS], [PKIX], [PKCS] sowie herstellerspezifische Erweiterungen zulässig.
In Zertifikate für CAs müssen die Erweiterung keyUsage mit den Werten "keyCertSign" und "cRLSign" sowie die Erweiterung basicConstraints mit dem Wert "CA=True" aufgenommen werden.
Zertifikate für alle anderen Verwendungszwecke werden optional mit der Erweiterung basicConstraints mit dem Wert "CA=False" als nicht-CA-Zertifikat markiert und tragen keine CA-spezifische keyUsage-Erweiterung, d.h. die Erweiterung keyUsage darf nicht die Werte "keyCertSign" oder "cRLSign" beinhalten.
Die keyUsage-Erweiterung darf nur mit dem Wert "nonRepudiation" belegt werden, wenn keine Wiederherstellung des privaten Schlüssels möglich ist und der private Schlüssel durch technische und organisatorische Maßnahmen nur dem Zertifikatnehmer zugänglich ist.

7.1.3 Algorithmus Bezeichner (OID)

Objekt Identifikatoren für Algorithmen werden nach PKIX verwendet.

7.1.4 Namensformen

Siehe Abschnitt 3.1.

7.1.5 Namensbeschränkungen

Siehe Abschnitt 3.1.

7.1.6 Bezeichner für Zertifizierungsrichtlinien (OID)

Siehe Abschnitt 1.2.

7.1.7 Nutzung von Erweiterungen zur Richtlinienbeschränkungen (PolicyConstraints)

Keine Angaben.

7.1.8 Syntax und Semantik von Policy Qualifiern

Keine Angaben.

7.1.9 Verarbeitung von kritischen Erweiterungen für Zertifizierungsrichtlinien (certificatePolicies)

Keine Angaben.

7.2 Sperrlistenprofil

7.2.1 Versionsnummer

Sperrlisten müssen gemäß der internationalen Norm X.509 in der Version 1 oder 2 erstellt werden.

7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen

Keine Angaben.

7.3 OCSP Profil

Keine Angaben.

7.3.1 Versionsnummer

Keine Angaben.

7.3.2 OCSP Erweiterungen

Keine Angaben.

8 KONFORMITÄTSPRÜFUNG (Compliance Audit, Assessments)

Jede CA innerhalb der HvS PKI muss ihre Abläufe so gestalten, dass sie diesem CP und ihrem CPS entsprechen. Jeder CA ist vorbehalten, alle ihre nachgeordneten CAs auf die Einhaltung der entsprechenden CP und des CPS hin zu überprüfen.

8.1 Häufigkeit und Umstände der Überprüfung

Die HvS PKI wird regelmäßig, mindestens alle 2 Jahre durch einen Security Auditor in Verbindung mit dem HvS Datenschutzbeauftragten auditiert.

8.2 Identität und Qualifikation des Überprüfers

Keine Angaben.

8.3 Verhältnis von Prüfer zu Überprüftem

Das Verhältnis von Prüfer zu Überprüftem ergibt sich aus Abschnitt 8.2.

8.4 Überprüfte Bereiche

Es werden alle Instanzen, Rollen, Prozesse, Personen, Protokolle und Log-Dateien der PKI stichprobenartig überprüft.
Die von einer Überprüfung betroffenen Bereiche werden jeweils durch die zuständige CA festgelegt. Für Umstände, die zwingend eine Überprüfung notwendig machen, können bestimmte Bereiche von vorne herein festgelegt werden.

8.5 Mängelbeseitigung

Werden Mängel festgestellt, werden sofort geeignete Maßnahmen zu deren Beseitigung eingeleitet. Falls die Sicherheit der PKI gefährdet ist, wird der Betrieb bis zur Beseitigung der Mängel eingestellt.

8.6 Veröffentlichung der Ergebnisse

Die Ergebnisse des Audits bzw. der Mängelbeseitigung werden nicht veröffentlicht.

9 ANDERE GESCHÄFTLICHE UND RECHTLICHE ANGELEGENHEITEN

9.1 Gebühren

Wenn eine CA Gebühren für ihre Leistungen erhebt, so ist dies in ihrem CPS auszuführen.

9.2 Finanzielle Verantwortung

Versicherungsschutz und Garantie für Sach- und Rechtsmängel sind nicht vorgesehen.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Vertraulich zu behandelnde Daten

Alle Informationen über Zertifikatsinhaber der HvS PKI, die nicht unter Abschnitt 9.3.2 fallen, werden als vertrauliche Informationen eingestuft.

9.3.2 Nicht vertraulich zu behandelnde Daten

Alle Informationen, die in den herausgegebenen Zertifikaten und Sperrlisten explizit (z.B. E-Mail-Adresse) oder implizit (z.B. Daten über die Zertifizierung) enthalten sind oder davon abgeleitet werden können, werden als nicht vertraulich eingestuft.

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Jede innerhalb der HvS PKI operierende CA trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen. Daten dürfen im Rahmen der Diensterbringung nur weitergegeben werden, wenn zuvor eine Vertraulichkeitserklärung unterzeichnet wurde und die mit den Aufgaben betrauten Mitarbeiter auf Einhaltung der gesetzlichen Bestimmungen über den Datenschutz verpflichtet wurden.

9.4 Schutz personenbezogener Daten

9.4.1 Richtlinie zur Verarbeitung personenbezogener Daten

Im Rahmen des Betriebs der PKI werden persönliche Daten erhoben. Diese werden nach dem BDSG und der Datenschutz-Policy der HvS in ihrer jeweils aktuellen gültigen Version behandelt.

9.4.2 Vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen aus Abschnitt 9.3.1 analog.

Alle persönlichen Daten, die nicht im Zertifikat enthalten sind (Ausnahme: Zertifikatssperrung, Zeitpunkt der Sperrung), gelten als vertrauliche Informationen. Eine Ausnahme stellen die Informationen dar, deren Veröffentlichung der Eigentümer der Information zugestimmt hat und die zum Auffinden oder zur eindeutigen Kennzeichnung eines Zertifikates dienen. Diese sind Name, Vorname, Nutzerkennungen, Geräteidentifikationen.

9.4.3 Nicht vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen aus Abschnitt 9.3.2 analog.

Alle Daten, die im Zertifikat enthalten sind, gelten als nicht vertraulich. Informationen, die für die Überprüfung eines Zertifikats benötigt werden, sind generell nicht vertraulich und werden veröffentlicht. Ferner gelten jene Informationen als nicht vertraulich, die zwar nicht im Zertifikat enthalten sind, deren

Veröffentlichung der Eigentümer der Information aber explizit zugestimmt hat und die zum Auffinden oder zur eindeutigen Kennzeichnung eines Zertifikates vorgesehen sind. Das HvS PKI behält sich vor, nicht vertrauliche Informationen zu veröffentlichen.

9.4.4 Verantwortung zum Schutz personenbezogener Daten

Für personenbezogene Daten gelten die Regelungen aus Abschnitt 9.3.3 analog.

9.4.5 Einwilligung und Nutzung personenbezogener Daten

Der Zertifikatnehmer stimmt der Nutzung von personenbezogenen Daten durch eine CA zu, soweit dies zur Leistungserbringung erforderlich ist. Darüber hinaus können alle Informationen veröffentlicht werden, die als nicht vertraulich behandelt werden (siehe Abschnitt 9.4.3) und deren Veröffentlichung nicht widersprochen wurde.

9.4.6 Offenlegung bei gerichtlicher Anordnung oder im Rahmen gerichtlicher Beweisführung

Bei gerichtlicher oder behördlicher Anforderung werden nach Prüfung der Rechtsgrundlagen und vorgelegten Beschlüsse alle angeforderten Informationen ausschließlich der anfordernden Behörde übergeben. Die betroffenen Endteilnehmer werden, falls zulässig, informiert.

9.4.7 Andere Umstände einer Veröffentlichung

Vertrauliche und personenbezogene Informationen werden außer den im Abschnitt 9.4 genannten Gründen unter keinen anderen Umständen veröffentlicht

9.5 Urheberrechte

Keine Angaben.

9.6 Verpflichtungen

9.6.1 Verpflichtung der Zertifizierungsstellen

Jede innerhalb der HvS PKI operierende CA verpflichtet sich, alle im Rahmen dieser CP und ihrem CPS beschriebenen Aufgaben nach bestem Wissen und Gewissen durchzuführen.

9.6.2 Verpflichtung der Registrierungsstellen

Keine Angaben.

9.6.3 Verpflichtung des Zertifikatsinhabers

Es gelten die Bestimmungen aus Abschnitt 4.5.1.

9.6.4 Verpflichtung der Relying Party

Es gelten die Bestimmungen aus Abschnitt 4.5.2.

9.6.5 Verpflichtung anderer Zertifikatsinhaber

Sofern weitere Zertifikatsinhaber als Dienstleister in den Zertifizierungsprozess eingebunden werden, ist die beauftragende CA in der Verantwortung, den Dienstleister zur Einhaltung der CP und ihres CPS zu verpflichten.

9.7 Gewährleistung

Gewährleistung wird in den Verträgen zwischen den beteiligten Parteien geregelt.

9.8 Haftungsbeschränkung

Haftungsbeschränkung wird in den Verträgen zwischen den beteiligten Parteien geregelt.

9.9 Haftungsfreistellung

Haftungsbeschränkung wird in den Verträgen zwischen den beteiligten Parteien geregelt.

9.10 Inkrafttreten und Aufhebung

9.10.1 Inkrafttreten

Das CP und alle CPS treten an dem Tag in Kraft, an dem sie über den entsprechenden Informationsdienst (siehe Kapitel 2) veröffentlicht werden.

9.10.2 Aufhebung

Dieses Dokument ist solange gültig, bis es durch eine neue Version ersetzt wird (siehe Abschnitt 9.10.1) oder der Betrieb der durch die HvS betriebenen CAs eingestellt wird.

9.10.3 Konsequenzen der Aufhebung

Von einer Aufhebung der CP oder eines CPS unberührt bleibt die Verantwortung zum Schutz vertraulicher Informationen und personenbezogener Daten.

9.11 Individuelle Benachrichtigungen und Kommunikation mit Zertifikatsinhabern

Andere als die in diesem CP festgelegten Benachrichtigungen bleiben den CAs freigestellt.

9.12 Änderungen der Richtlinie

Eine Änderung der CP kann nur durch die HvS erfolgen. Werden Änderungen vorgenommen, die sicherheitsrelevante Aspekte betreffen oder die Abläufe seitens der Zertifikatnehmer erforderlich machen, ist eine Änderung der OID des entsprechenden Dokuments (siehe Abschnitt 1.2) sowie ggf. eine Änderung der OID der CP in Zertifikaten (siehe Ab- schnitt 7.1.6) erforderlich.

9.12.1 Vorgehen bei Änderungen

Keine Angaben.

9.12.2 Benachrichtigungsmechanismus und Fristen

Keine Angaben.

9.12.3 Umstände, die eine Änderung des Richtlinienbezeichners (OID) erfordern

Keine Angaben.

9.13 Konfliktbeilegung

Keine Angaben.

9.14 Geltendes Recht

Der Betrieb der HvS PKI, diese Zertifikatsrichtlinie und Erklärung zum Zertifizierungsbetrieb unterliegen dem Recht der Bundesrepublik Deutschland. Die HvS PKI stellt keine qualifizierten Zertifikate im Sinne des deutschen Signaturgesetzes aus.

9.15 Konformität mit geltendem Recht

Keine Angaben.

9.16 Weitere Regelungen

9.16.1 Vollständigkeit

Alle in dieser CP oder einem CPS enthaltenen Regelungen gelten zwischen einer innerhalb der HvS PKI operierenden CA und deren Zertifikatnehmern. Die Ausgabe einer neuen Version ersetzt alle vorherigen Versionen. Mündliche Vereinbarungen bzw. Nebenabreden sind nicht zulässig.

9.16.2 Abtretung der Rechte

Keine Angaben.

9.16.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieser CP oder eines CPS unwirksam sein oder Lücken enthalten, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt.

9.16.4 Rechtliche Auseinandersetzungen / Erfüllungsort

Rechtliche Auseinandersetzungen, die aus dem Betrieb einer innerhalb der HvS PKI operierenden CA herrühren, obliegen den Gesetzen der Bundesrepublik Deutschland. Erfüllungsort und ausschließlicher Gerichtsstand sind Sitz des jeweiligen Betreibers.

9.16.5 Force Majeure

Keine Angaben.

9.17 Andere Regelungen

Keine Angaben.

10 INFORMATIONEN ZUM DOKUMENT

Keine Angaben.

11 GLOSSAR

Begriff	Erläuterung
HvS	HvS-Consulting AG
HvS PKI	Public Key Infrastructure (PKI) der HvS-Consulting AG
CA	Zertifizierungsstelle (engl.: Certification Authority)
CN	Bestandteil des DN: Name (engl.: Common Name)
CRL	Sperrliste (engl.: Certificate Revocation List)
CP	Zertifizierungsrichtlinie (engl.: Certificate Policy)
CPS	Erklärung zum Zertifizierungsbetrieb (engl.: Certification Practice Statement)
CSR	Zertifikatantrag (engl.: Certificate Signing Request)
DC	Bestandteil des DN: Domain Component
DN	Eindeutiger Name des Zertifikatinhabers oder –ausstellers in Zertifikaten. Ein DN wird aus mehreren Bestandteilen wie z.B. C, O, OU, CN gebildet. (engl.: Distinguished Name
Erklärung zum Zertifizierungs-betrieb (CPS)	praktische (technisch und organisatorisch) Umsetzung der Zertifizierung richtlinie
EXT	Kennzeichen im CN: externe Zertifikatnehmer (engl.: External)
GRP	Kennzeichen im CN: Personen- bzw. Funktionsgruppen (engl.: Group)
HSM	Gerät, das kryptographische Schlüssel sicher speichert und verarbeitet (engl.: Hardware Security Module)
Identifizierung	Personen, die Zertifikate in der HVS PKI beantragen, müssen ihre Identität feststellen lassen. Dieser Vorgang wird als Identifizierung bezeichnet.
Key Escrow	Schlüsselhinterlegung (siehe Abschnitt 4.12)
Key Recovery	Schlüsselwiederherstellung (siehe Abschnitt 4.12)
LDAP	Protokoll zur Nutzung von Verzeichnisdiensten (engl.: Lightweight Direc- tory Access Protocol)
O	Bestandteil des DN: Organisation
OCSP	Protokoll zur online Prüfung des Status eines Zertifikats (engl.: Online Certification Status Protocol)
Öffentlicher Schlüssel	Schlüssel eines kryptographischen Schlüsselpaares, welcher öffentlich bekannt gemacht wird. Ein öffentlicher Schlüssel kann z.B. zur Überprü- fung von elektronischen Signaturen verwendet werden (engl.: Public Key)
OID	Objekt Identifikator – eindeutige Referenz auf ein Objekt in einem Namensraum
OU	Bestandteil des DN: Organisationseinheit (engl.: Organizational Unit)

Root-CA	Oberste CA einer PKI (engl.: Policy Certification Authority)
PKCS	Serie von kryptografischen Spezifikationen (engl.: Public Key Cryptography Standard) [PKCS]
PKCS#7	Datenaustauschformat zur Übermittlung von Signaturen und verschlüsselten Daten oder auch zur Verteilung von Zertifikaten [PKCS]