Zertifizierungsrichtlinie der FMG-Konzern PKI

Version 1.01 vom 07.01.2014

Verantwortlichkeiten

Funktion	Name
Autoren	Alexander Cmarits (FMG)
Review	Robert Weilhammer (FMG) Michael Schmitz (FMG)

Änderungsverzeichnis

Version	Datum	Status	Änderungen
1.0	30.11.2012	Finale Version	Erstellung
1.01	07.01.2014	Finale Version	Unstimmigkeiten beseitigt

Inhaltsverzeichnis

1 Einleitung

1.1 Überblick

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

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 CP ist folgendermaßen identifiziert:

- Titel: Zertifizierungsrichtlinie der FMG-KONZERN PKI
- Version: 1.01
- Object Identifier (OID): 1.3.6.1.4.1.5587.30.1

Der OID [OID] ist wie folgt zusammengesetzt:

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) Flughafen Muenchen (5587) pki(30) cp(1)}

1.3 Teilnehmer der Zertifizierungsinfrastruktur (PKI)

1.3.1 Zertifizierungsstellen

Die Root-CA der FMG-Konzern PKI ist eine Wurzelinstanz, d.h. der Root-CA Schlüssel ist selbstsigniert. Untergeordnete CA-Zertifikate (Sub-CAs) werden in der Regel von der Root-CA ausgestellt. Wird eine bereits bestehende CA in die FMG-Konzern PKI integriert, ist deren Wurzelzertifikat durch die Root-CA zu signieren.

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 einzelnen CAs stellen Nutzerzertifikate aus. Hierbei handelt es sich um Zertifikate, deren Erstellung den Regeln dieser Zertifizierungsrichtlinie der FMG-Konzern PKI entsprechen.

1.3.2 Registrierungsstellen

Einer Registrierungsstelle (RA) obliegt die Antragsprüfung und Identifizierung von Teilnehmern und Zertifikatinhabern. Diese Aufgaben werden von der RA der jeweiligen CA übernommen. Die zugehörige RA einer CA sind im Certificate Practice Statement (CPS) der entsprechenden CA zu definieren.

Für jede RA gelten verbindlich die Richtlinien der FMG-Konzern PKI.

1.3.3 Zertifikatsinhaber (Subscribers)

Die FMG-Konzern PKI stellt Zertifikate für die Flughafen München GmbH und den mit ihr verbundenen Organisationen aus.

Für folgende Gruppen können Zertifikate ausgestellt werden:
Organisationen (Töchterfirmen wie z.B. Medicare, Allresto, Eurotrade)

Natürliche Personen, die zum FMG-Konzern gehören

Geräte (Hardware- oder Softwarekomponenten), die zum FMG-Konzern gehören

1.3.4 Zertifikatsprüfer (Relying Parties)

Zertifikatprüfer sind natürliche Personen und Organisationen, die unter Nutzung eines innerhalb der FMG-Konzern PKI ausgestellten Zertifikats die Authentizität von Zertifikatinhabern überprüfen.

1.3.5 Weitere Teilnehmer

Weitere Teilnehmer können natürliche Personen oder Organisationen sein, die in den Zertifizierungsprozess als Dienstleister eingebunden sind. Bei Dienstleistern, die im Namen und Auftrag eines Teilnehmers tätig werden, liegt die Verantwortung für die Einhaltung von CP und CPS bei dem beauftragenden FMG-Verantwortlichen.

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, IKEv2, L2TP/IPSEC, SSTP VPNs)

Benutzer Zertifikate (z.B. S-MIME-Verschlüsselung, SmartCard-Logon, Application-Authentifizierung)

Client Zertifikate (z.B. Mobile Endgeräte, Application-Authentifizierung, Computer-Zertifikate, Netzwerkgeräte)

Code Signatur

Die Zertifikate der FMG-Konzern PKI entsprechen nicht den Anforderungen des deutschen Signaturgesetzes.

1.4.1 Geeignete Zertifikatsnutzung

Die im Rahmen der FMG-Konzern PKI ausgestellten Zertifikate können u.a. für Authentifizierung, elektronische Signatur, Verschlüsselung und Code Signatur 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 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 das Information Security Management (ISM) der FMG Flughafen München GmbH. Für Kontaktinformationen siehe Abschnitt 1.5.2.

1.5.2 Ansprechpartner

Zuständige Organisation

Flughafen München GmbH

Servicebereich IT

Postfach 231755

85326 München

1.5.3 Freigabeverantwortliche für Dokumente zum FMG-KONZERN PKI

Das ISM der FMG Flughafen München GmbH ist für die Freigabe der Dokumente zur FMG-Konzern PKI verantwortlich.

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

Das ISM der FMG Flughafen München GmbH ist für die Prüfung aller CPS innerhalb der FMG-Konzern PKI verantwortlich.

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

Die Genehmigung der CPS erfolgt durch das ISM der FMG Flughafen München GmbH.

1.6 Definitionen und Abkürzungen

Siehe Kapitel 11.

2 VERÖFFENTLICHUNGEN UND VERZEICHNISDIENST

2.1 Informationsdienste

Für jede CA innerhalb der FMG-Konzern PKI werden die in Abschnitt 2.2 genannten Informationen gemäß Abschnitt 2.3 und Abschnitt 2.4 vorgehalten.

2.2 Veröffentlichung von Zertifizierungs-Informationen

Die folgenden Informationen werden veröffentlicht:

Zertifizierungsrichtlinie der FMG-Konzern PKI (CP)

Erklärung zum Zertifizierungsbetrieb der Root-CA der FMG-Konzern PKI (CPS)

FMG-Konzern Root CA 1-Zertifikat der FMG-Konzern PKI inkl. Fingerabdruck

Sperrinformationen der FMG-Konzern PKI

Kontaktinformationen, unter denen eine Sperrung beantragt werden kann

Diese Informationen werden auf der Seite http://pki.munich-airport.de veröffentlicht.

2.3 Aktualisierung der Informationen (Zeitpunkt, Frequenz)

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

Zertifikate:	spätestens eine Woche nach der Ausstellung
CP und CPS:	spätestens eine Woche nach Freigabe einer neuen Version
CRLs:	siehe Abschnitt 4.9.7.

2.4 Zugangskontrolle zu Verzeichnisdiensten

Den Endteilnehmern und der Öffentlichkeit wird lesender Zugriff auf die o.g. Informationen gewährt. Schreibenden Zugriff haben nur berechtigte Personen.

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 FMG-Konzern PKI wird eine einheitliche Namenshierarchie verwendet. Alle innerhalb der FMG-Konzern 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

Der DN muss den Zertifikatnehmer eindeutig identifizieren. Bei der Namensvergabe gelten die folgenden Regelungen:

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 Teilnehmers 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, wenn diese in einem amtlichen Ausweispapiers mit Lichtbild enthalten sind, z.B. "CN=Manuela Musterfrau, Dr.". Bei Namensgleichheit werden ab dem zweiten Namen laufendende Nummern vergeben.

Bei der Vergabe von Zertifikaten für Datenverarbeitungssysteme muss für den Namen der voll qualifizierte Domainname verwendet werden, z.B. "CN=ca.munich-airport.de".

Sogenannte "Wildcard Zertifikate", wie zum Beispiel "CN=*.munich-airport.de" sind grundsätzlich nicht zulässig. Ausnahmen müssen explizit begründet und beim ISM beantragt werden.

3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsinhaber

Keine Angaben.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Ausschließlich die folgenden Zeichen dürfen in den Attributen des DN 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

Das ISM pflegt eine Liste berechtigter Organisationen im FMG-Konzern, die ein Zertifikat anfordern können.

3.2.3 Authentifizierung natürlicher Personen

Die Authentifizierung der Identität einer natürlichen Person wird durch die RA der jeweiligen CA vorgenommen.
Folgende Informationen müssen vorliegen und überprüft werden:
Name, Vorname(n) und Namenszusätze

E-Mail-Adresse

Name der zugehörigen Organisation

Nachweis der Zugehörigkeit zur angegebenen Organisation

Diese Informationen sind für die Zertifikaterstellung notwendig und werden aufgezeichnet. Anhand dieser Daten ist die eindeutige Identifizierung der natürlichen Person möglich.

3.2.4 Nicht überprüfte Teilnehmerangaben

Außer den Angaben in Abschnitt 3.2.1 und Abschnitt 3.2.3 werden keine weiteren Informationen überprüft.

3.2.5 Überprüfung der Berechtigung

Die Überprüfung der Berechtigung des Antragstellers muss dokumentiert werden.

3.2.6 Kriterien für Zusammenarbeit (Cross-Zertifizierung)

Die Möglichkeit der Cross-Zertifizierung besteht ausschließlich für die Root-CA der FMG-Konzern 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 das Information Security Management zu überprüfen.
Falls der Kooperationspartner eine Level-of-Trust 2-Einstufung nach der LoT-02 Skala des Informationssicherheits-Standards des BDL (Bundesverband der Deutschen Luftverkehrswirtschaft) besitzt, wird das Root-CA-Zertifikat des Kooperationspartners anerkannt.

3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung

Bei einer Schlüsselerneuerung 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.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Die Authentifizierung einer Sperrung kann auf die folgenden Arten erfolgen:

Übermittlung einer vorher vereinbarten Authentisierungsinformation (schriftlich, per Telefon, oder elektronisch)

Übergabe eines Sperrantrags mit einer handschriftlichen Unterschrift, Firmenstempel und Überprüfung der Korrektheit via Rückruf an die hinterlegte Telefonnummer.

Übergabe eines Sperrantrags mit einer geeigneten elektronischen Signatur, die den Zertifikatnehmer authentifiziert

4 ABLAUFORGANISATION (Certificate Life-cycle)

4.1 Zertifikatsantrag

4.1.1 Wer kann ein Zertifikat beantragen

In der FMG-Konzern PKI können Zertifikatnehmer gemäß Abschnitt 1.3.3 Zertifikate beantragen.
Sub-CAs können den Kreis der berechtigten Zertifikatnehmer in ihrem CPS weiter eingrenzen.

4.1.2 Verfahren und Verantwortungen

Um ein Zertifikat zu erhalten, muss ein Antrag bei der zuständigen Registrierungsstelle der Sub-CA eingereicht werden.
Bei der Registrierungsstelle müssen die folgenden Arbeitsschritte durchlaufen und dokumentiert werden:
Prüfung des Zertifikatantrags hinsichtlich Vollständigkeit und Korrektheit

Prüfung der Eindeutigkeit des gewünschten DN

Prüfung des Vorliegens beziehungsweise Durchführung einer Authentifizierung der Identität nach Abschnitt 3.2.3

Gegebenenfalls Überprüfung der Authentifizierung einer Organisation nach Abschnitt 3.2.2

Angefallene Papierunterlagen müssen archiviert und sicher aufbewahrt werden.

Die Übermittlung der für die Zertifizierung notwendigen Informationen an die zuständige CA erfolgt FMG-Konzern intern als E-Mail. Externe Anträge müssen entsprechend verschlüsselt und signiert 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 RA akzeptiert, wenn alle Arbeitsschritte gemäß Abschnitt 4.1.2 erfolgreich durchlaufen wurden. Andernfalls wird der Zertifikatantrag abgewiesen und dies dem Antragsteller unter der Angabe von Gründen mitgeteilt.

4.2.3 Bearbeitungsdauer bei Zertifikatsanträgen

Die Bearbeitungsdauer eines Zertifikatantrags beträgt grundsätzlich maximal 20 Werktage.

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. Insbesondere überprüft die CA die Berechtigung der RA, ein Zertifikat für den im DN angegebenen Namen zu genehmigen sowie die Gültigkeit der Signatur der RA.

4.3.2 Benachrichtigung des Antragstellers

Nach der Zertifikatausstellung wird dem Teilnehmer sowie ggf. dem Zertifikatinhaber das ausgestellte Zertifikat durch die CA per E-Mail übermittelt oder sie werden über dessen Ausstellung und die Möglichkeit zum Download informiert. Das zugehörige Passwort zur Entgegennahme des privaten Schlüssels des Zertifikats (sofern benötigt) muss entweder verschlüsselt oder über einen alternativen Kommunikationsweg übertragen werden.

4.4 Zertifikatsakzeptanz

Der Zertifikatnehmer sollte die Korrektheit des eigenen Zertifikats sowie des Zertifikats der ausstellenden CA nach Erhalt 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 2.1) 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 (sofern relevant) und das Zertifikat in Übereinstimmung mit diesem CP eingesetzt wird.

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 automatisiert erfolgen bzw. manuell beantragt werden, wenn die Gültigkeit eines Zertifikats abläuft.

4.6.2 Wer kann eine Zertifikatserneuerung beantragen

Eine Zertifikaterneuerung wird grundsätzlich durch den Zertifikatnehmer bzw. automatisiert beantragt. Es obliegt der zuständigen 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 oder das CPS nicht ein.

Der Zertifikatnehmer verlangt die Sperrung des Zertifikats.

Die zuständige CA bzw. eine RA hält die CP oder das CPS nicht ein.

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 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 RA 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 RA authentifizieren. Die möglichen Verfahren sind in Abschnitt 3.4 dargestellt.
Hat die RA erfolgreich den Zertifikatnehmer authentifiziert oder selber einen Sperrantrag gestellt, so genehmigt sie diesen und leitet ihn an die CA weiter.
Die CA führt die Sperrung durch, nachdem sie die Berechtigung der RA für die Sperrung des Zertifikats und die Signatur der RA geprüft hat.

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

CAs müssen mindestens alle 90 Tage eine CRL erstellen und veröffentlichen. Wird ein Zertifikat gesperrt, so muss die sperrende CA umgehend eine neue CRL erstellen und veröffentlichen.

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.

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)

Keine Angaben.

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 entweder durch eine Sperrung oder indem nach Ablauf der Gültigkeit kein neues Zertifikat beantragt wird.

4.12 Schlüsselhinterlegung und –wiederherstellung

Grundsätzlich sind die untergeordneten CAs der FMG-Konzern PKI zu einer Schlüsselhinterlegung und -wiederherstellung verpflichtet. Die Richtlinien und Praktiken sind dem jeweiligen CPS der untergeordneten CAs zu entnehmen.

5 INFRASTRUKTURELLE, ORGANISATORISCHE UND PERSONELLE SICHERHEITSMASSNAHMEN

Die Gewährleistung geeigneter infrastruktureller, organisatorischer und personeller 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 Kapitel 8) zur Verfügung stehen.

5.1 Infrastrukturelle Sicherheitsmaßnahmen

Jede CA muss in ihrem CPS die infrastrukturellen Sicherheitsmaßnahmen beschreiben, dies kann exemplarisch dem CPS der Root-CA entnommen werden.

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 Rollenkonzept

Für den Betrieb der FMG-Konzern PKI werden unterschiedliche 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: Die 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.

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

Rolle	Aufgabe der Rolle	Kürzel
PKI-Betrieb = RA	Entgegennahme von Zertifikat- und Sperranträgen. Authentifizierung der Identität und Prüfung der Autorisierung der Zertifikatnehmer. Beratung der Zertifikatnehmer. Verantwortlich für Anwendung und Lagerung von elektronischen Datenträgern, auf denen die privaten Schlüssel der CA gespeichert sind. Zusammen mit dem Information Security Management in der Lage den privaten Schlüssel der Root-CA der FMG-Konzern PKI wiederherzustellen.	PKI-B
Information Security Management	Definition und Überprüfung der Einhaltung der Sicherheitsbestimmungen, insbesondere CPS und Sicherheitskonzept. Zuordnung von Personen zu Rollen und zu Berechtigungen. Ansprechpartner für sicherheitsrelevante Fragen. Durchführung der betriebsinternen Audits und der Audits von Sub-CAs.	ISM

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 werden muss.

Tätigkeit	Rollen
Wiederherstellung privater Schlüssel der Root-CA	PKI-B & ISM
Wiederherstellung privater Schlüssel der SUB-CAs	PKI-B

Tabelle: Tätigkeiten, die das Vier-Augen-Prinzip erfordern

Alle anderen Tätigkeiten können von einer Person durchgeführt werden.

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

Die Rollen PKI-B und ISM sind miteinander unverträglich und deshalb von verschiedenen Mitarbeitern zu erfüllen.

5.3 Personelle Sicherheitsmaßnahmen

Jede CA muss in ihrem CPS die personellen Sicherheitsmaßnahmen beschreiben.
Dies kann exemplarisch dem CPS der Root-CA entnommen werden.

5.4 Überwachung / Protokollierung

Jede CA muss in ihrem CPS die Maßnahmen zur Sicherheitsüberwachung beschreiben.
Dies kann exemplarisch dem CPS der Root-CA entnommen werden.

5.5 Archivierung

Jede CA muss in ihrem CPS die Maßnahmen zur Archivierung beschreiben.
Dies kann exemplarisch dem CPS der Root-CA entnommen werden.

5.6 Schlüsselwechsel der Zertifizierungsstelle

Jede CA muss in ihrem CPS die Maßnahmen zum Schlüsselwechsel beschreiben.
Dies kann exemplarisch dem CPS der Root-CA entnommen werden.

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 allen Mitarbeiter zugänglich gemacht 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. Die Bewertung der Sicherheitslage obliegt dem ISM.

5.8 Einstellung des Betriebs

Stellt eine CA ihren Betrieb ein, müssen folgende Maßnahmen ergriffen werden:
Information aller Zertifikatnehmer, betroffenen RAs 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 Kapitel 8) zur Verfügung stehen.

6.1 Schlüsselerzeugung und Installation

6.1.1 Schlüsselerzeugung

Keine Angabe.

6.1.2 Übermittlung privater Schlüssels an Zertifikatsinhaber

Keine Angabe.

6.1.3 Übermittlung öffentlicher Schlüssels an Zertifikatsaussteller

Die FMG-Konzern PKI akzeptiert Zertifikatsanforderungen in den folgenden Formaten:

- PKCS#10 Format. (s. RFC 2986)
- PEM Format.

Der CSR des Zertifikatnehmers wird per E-Mail, HTTPS oder auf einem Datenträger an die CA übermittelt.

6.1.4 Übermittlung öffentlicher CA Schlüssels an Zertifikatsprüfer (Relying Parties)

Alle Teilnehmer der FMG-Konzern PKI können den öffentlichen Schlüssel jeder CA über einen Informationsdienst gemäß Kapitel 2.1 abrufen.

6.1.5 Schlüssellängen

Bei der FMG-Konzern 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. Darüber hinaus sind grundsätzlich alle kryptographischen Algorithmen entsprechend der aktuellen "Übersicht über geeignete Algorithmen" der Bundesnetzagentur [BNA] zulässig, wenn ihre Sicherheit mindestens äquivalent zu RSA mit 4096/2048 Bit ist. Bei einem Einsatz anderer Algorithmen sind diese im CPS zu beschreiben.

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 Angabe.

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

Der Zugriff auf den privaten Schlüssel einer SUB-CA muss gemäß Abschnitt 5.2.2 im 4-Augen-Prinzip durch verschiedene Mitarbeiter der Rolle PKI-B gemeinsam stattfinden. Der Zugriff auf den privaten Schlüssel der Root-CA muss gemäß Abschnitt 5.2.2 im 4-Augen-Prinzip durch die verschiedenen Rollen ISM und PKI-B gemeinsam stattfinden.

6.2.3 Hinterlegung privater Schlüssel (Key Escrow)

Eine Hinterlegung privater Schlüssel durch die FMG-Konzern PKI erfolgt nicht.

6.2.4 Backup privater Schlüssel

Die Sicherung des privaten Schlüssels der Root-CA der FMG-Konzern PKI erfolgt in verschlüsselter Form auf einem geeigneten Medium. Nur verschiedene Mitarbeiter der Rolle PKI-B haben gemeinsam Zugriff auf die Sicherung.

Die Sicherung privater Schlüssel untergeordneter SUB-CAs erfolgt auf einem verschlüsselten Medium auf welches nur verschiedene Mitarbeiter der Rolle PKI-B gemeinsam Zugriff haben.

6.2.5 Archivierung privater Schlüssel

Keine Angabe.

6.2.6 Transfer privater Schlüssel in oder aus einem kryptographischen Modul

Keine Angabe.

6.2.7 Speicherung privater Schlüssel in einem kryptographischen Modul

Keine Angabe.

6.2.8 Aktivierung privater Schlüssel

Keine Angabe.

6.2.9 Deaktivierung privater Schlüssel

Keine Angabe.

6.2.10 Vernichtung privater Schlüssel

Keine Angabe.

6.2.11 Güte kryptographischer Module

Keine Angabe.

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 FMG-Konzern PKI ausgestellten Zertifikate haben folgende Gültigkeitsdauer:

- Zertifikat der Root-CA: maximal zwanzig Jahre
- Zertifikate für untergeordnete CAs: maximal fünfzehn Jahre
- Zertifikate für Server (Serverzertifikate): maximal drei Jahre
- Zertifikate für natürliche Personen (Benutzerzertifikate): maximal zwei Jahre
- Zertifikate für Endgeräte und Anwendungen (Clientzertifikate): maximal drei Jahre
- Zertifikate für CodeSignatur: maximal 5 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

Für Passwörter bzw. PINs zur Aktivierung von privaten Schlüsseln müssen nicht triviale Kombinationen aus alphanumerischen Zeichen und Sonderzeichen gewählt werden. Die Länge muss bei der Root-CA mindestens 15 Zeichen betragen, sonst 8 Zeichen.

6.4.2 Schutz der Aktivierungsdaten

Aktivierungsdaten müssen geheim gehalten werden und dürfen nur den Mitarbeitern bekannt sein, die diese nach Abschnitt 5.2.1 für die Durchführung einer spezifischen Funktion benötigen. Eine schriftliche Fixierung ist allenfalls für die Hinterlegung nach Abschnitt 6.2.4 zulässig.

6.4.3 Weitere Aspekte

Keine Angabe.

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

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] und [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)

Der im Abschnitt 1.2 angegebene OID dieser CP muss in alle Zertifikate aufgenommen werden. Zusätzlich muss der OID des für die ausstellende CA gültigen CPS aufgenommen werden.

7.1.7 Nutzung von Erweiterungen zur Richtlinienbeschränkungen (PolicyConstraints)

Keine Angabe.

7.1.8 Syntax und Semantik von Policy Qualifiern

Keine Angabe.

7.1.9 Verarbeitung von kritischen Erweiterungen für Zertifizierungsrichtlinien (certificatePolicies)

Keine Angabe.

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 Angabe.

7.3 OCSP Profil

Keine Angabe.

7.3.1 Versionsnummer

Keine Angabe.

7.3.2 OCSP Erweiterungen

Keine Angabe.

8 KONFORMITÄTSPRÜFUNG (Compliance Audit, Assessments)

Jede CA innerhalb der FMG-Konzern PKI muss ihre Abläufe so gestalten, dass sie diesem CP und ihrem CPS entsprechen. Jeder CA ist vorbehalten, alle ihr nachgeordneten CAs und RAs auf die Einhaltung der entsprechenden CP und des CPS hin zu überprüfen. Die Überprüfung der Root-CA erfolgt durch die Rolle des ISM.

8.1 Häufigkeit und Umstände der Überprüfung

Die FMG Root-CA wird mindestens jährlich durch ISM auditiert.

Die Sub-CAs werden regelmäßig, mindestens alle 3 Jahre durch ISM auditiert.

8.2 Identität und Qualifikation des Überprüfers

Die zuständige CA kann selbst die Einhaltung der Richtlinien der ihr nachgeordneten CAs und RAs überprüfen. Eine Konformitätsprüfung kann auch durch Dritte vorgenommen werden.

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 CA 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.

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 Informationen

Alle Informationen über Teilnehmer der FMG-Konzern 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 FMG-Konzern PKI operierende CA trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen. Daten dürfen im Rahmen der Diensterbringung nur weitergegeben werden, wenn 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

Die FMG-Konzern PKI Root-CA und untergeordnete CAs müssen zur Leistungserbringung personenbezogene Daten elektronisch speichern und verarbeiten. Dies muss in Übereinstimmung mit den entsprechenden Gesetzen geschehen.

9.4.2 Vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen aus Abschnitt 9.3.1 analog.

9.4.3 Nicht vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen aus Abschnitt 9.3.2 analog.

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. Eine Sicherungskopie verbleibt bei ISM. 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

Die FMG Flughafen München GmbH ist Urheber dieser CP, sowie des CPS der Root-CA. Die genannten Dokumente können unverändert an Dritte weitergegeben werden. Weitergehende Rechte werden nicht eingeräumt. Insbesondere ist die Weitergabe veränderter Fassungen und die Überführung in maschinenlesbare oder andere veränderbare Formen der elektronischen Speicherung, auch auszugsweise, ohne Zustimmung der FMG Flughafen München GmbH nicht zulässig.

9.6 Verpflichtungen

9.6.1 Verpflichtung der Zertifizierungsstellen

Jede innerhalb der FMG-Konzern 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

Jede innerhalb der FMG-Konzern PKI operierende RA verpflichtet sich, alle in dieser CP und dem CPS ihrer zugehörigen CA beschriebenen Aufgaben nach bestem Wissen und Gewissen durch- zuführen.

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 Teilnehmer

Sofern weitere Teilnehmer 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 2.1) veröffentlicht werden. Eine Änderung von CP oder CPS der Root-CA wird von der FMG Flughafen München GmbH angekündigt, Änderungen an weiteren CPS werden von der jeweiligen CA angekündigt.

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 FMG-Konzern PKI 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 Teilnehmern

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 FMG Flughafen München GmbH 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 Abschnitt 7.1.6) erforderlich.

9.12.1 Vorgehen bei Änderungen

Keine Angabe.

9.12.2 Benachrichtigungsmechanismus und Fristen

Keine Angabe.

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

Keine Angabe.

9.13 Konfliktbeilegung

Keine Angabe.

9.14 Geltendes Recht

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

9.15 Konformität mit geltendem Recht

Keine Angabe.

9.16 Weitere Regelungen

9.16.1 Vollständigkeit

Alle in dieser CP oder einem CPS enthaltenen Regelungen gelten zwischen einer innerhalb der FMG-Konzern 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 FMG-Konzern 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
beauftragender FMG-Verantwortlicher	Ansprechpartner des Dienstleisters innerhalb des FMG-Konzerns
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 Zertifizierungsrichtlinie
Force Majeure	Vorbeugender Haftungsausschluss im Falle extremer unerwarteter Ereignisse
HSM	Gerät, das kryptographische Schlüssel sicher speichert und verarbeitet (engl.: Hardware Security Module)
Identifizierung	Personen, die Zertifikate in der PKI beantragen, müssen ihre Identität feststellen lassen. Dieser Vorgang wird als Identifizierung bezeichnet.
Informationsdienst	Link auf weitere Informationen zur PKI http://pki.munich-airport.de
ISM	Information Security Management des FMG-Konzerns
Key Escrow	Schlüsselhinterlegung (siehe Abschnitt 4.12)
Key Recovery	Schlüsselwiederherstellung (siehe Abschnitt 4.12)
LDAP	Protokoll zur Nutzung von Verzeichnisdiensten (engl.: Lightweight Directory Access Protocol)
LoT	Level-of-Trust-Einstufung nach der LoT-O Skala Weitere Informationen unter http://www.bdl.aero, Publikationen, Informationssicherheit
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 Überprüfung 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)
PKCS	Public Key Cryptography Standards und bezeichnet eine Reihe von kryptographischen Spezifikationen
PKCS#7	Datenaustauschformat zur Übermittlung von Signaturen und verschlüsselten Daten oder auch zur Verteilung von Zertifikaten
PKI-B	Jeweilige Einheit, welche den PKI-Betrieb sicherstellt
Root-CA	Oberste CA einer PKI (engl.: Policy Certification Authority)
X.509	Standard für eine Public-Key-Infrastruktur zum Erstellen digitaler Zertifikate