Erklärung zum Zertifizierungsbetrieb der Root-CA im FMG-KONZERN

Version 1.0 vom 30.11.2012

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

Inhaltsverzeichnis

1 Einleitung

Im Rahmen der FMG-Konzern PKI betreibt die FMG Flughafen München GmbH die oberste Zertifizierungsstelle (CA), die sogenannte Root-CA.

1.1 Überblick

Dieses Dokument ist das CPS der Root-CA der FMG-Konzern PKI. Es beschreibt Spezifikationen, Prozesse und technische Sicherheitsmaßnahmen der Root-CA für die Ausstellung von Zertifikaten.
Diesem Dokument zugehörig ist die Zertifizierungsrichtlinie (CP) der FMG-Konzern PKI in der jeweils aktuellen Version: "Zertifizierungsrichtlinie der FMG-Konzern PKI".

1.2 Dokumentenname sowie Identifikation

Diese CPS ist folgendermaßen identifiziert:

- Titel: Erklärung zum Zertifizierungsbetrieb der FMG-Konzern PKI
- Version: 1.0
- Object Identifier (OID): 1.3.6.1.4.1.5587.30.1.1.0

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) major-version(1) minor- version(0)}

1.3 Teilnehmer der Zertifizierungsinfrastruktur (PKI)

1.3.1 Zertifizierungsstellen

Siehe CP.

1.3.2 Registrierungsstellen

Die Antragsprüfung für Sub-CAs wird durch das Information Security Management und Mitarbeiter der Abteilung ITN des FMG Flughafen München GmbH vorgenommen.

1.3.3 Zertifikatsinhaber (Subscribers)

Die Root-CA der FMG-Konzern PKI stellt nur Zertifikate für untergliederte Zertifizierungsstellen (Sub-CAs) aus.

1.3.4 Zertifikatsprüfer (Relying Parties)

Siehe CP.

1.3.5 Weitere Teilnehmer

Siehe CP.

1.4 Anwendungsbereich

Siehe CP.

1.5 Verwaltung der Zertifizierungsrichtlinie

Siehe CP

1.6 Definitionen und Abkürzungen

Siehe CP.

2 VERÖFFENTLICHUNGEN UND VERZEICHNISDIENST

2.1 Verzeichnisdienste

Siehe CP.

2.2 Veröffentlichung von Zertifizierungs-Informationen

Siehe CP.

2.3 Aktualisierung der Informationen (Zeitpunkt, Frequenz)

Siehe CP.

2.4 Zugangskontrolle zu Verzeichnisdiensten

Siehe CP.

3 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

3.1 Namen

3.1.1 Namensraum

Siehe CP.

4 ABLAUFORGANISATION (Certificate Life-cycle)

Siehe CP.

5 INFRASTRUKTURELLE, ORGANISATORISCHE UND PERSONELLE SICHERHEITSMASSNAHMEN

5.1 Infrastrukturelle Sicherheitsmaßnahmen

5.1.1 Einsatzort und Bauweise

Die Komponenten der PKI sind in den Rechenzentren der FMG Flughafen München GmbH untergebracht.

5.1.2 Räumlicher Zugang

Nur autorisierte Personen haben Zutritt zu den Rechenzentren der FMG Flughafen München GmbH. Die Räume des Rechenzentrums sind Video überwacht.

5.1.3 Stromversorgung und Klimaanlagen

Die Rechenzentren der FMG Flughafen München GmbH sind mit einer redundanten Notstromversorgung ausgestattet und klimatisiert.

5.1.4 Gefährdung durch Wasser

In den Rechenzentren der FMG Flughafen München GmbH wurden Vorkehrungen gegen Überschwemmung und Wassereinbruch getroffen.

5.1.5 Brandschutz

Die Rechenzentren der FMG Flughafen München GmbH sind mit Rauchmeldern und Löscheinrichtungen gemäß gesetzlicher Anforderungen ausgestattet.

5.1.6 Aufbewahrung von Datenträgern

Alle Daten werden innerhalb der Rechenzentren der FMG Flughafen München GmbH gelagert. Die FMG Flughafen München GmbH betreibt zwei räumlich voneinander getrennte Rechenzentren. Ein ausgereiftes Backup-Konzept ermöglicht eine Spiegelung kritischer Systeme und Daten in Echtzeit.

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 Rollenkonzept

Siehe CP.

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. Alle anderen Tätigkeiten können von einer Person durchgeführt werden.

Tätigkeit	Rollen
Starten von Prozessen zur Ausstellung von Zertifikaten für Sub-CAs und	PKI-B & ISM
Austausch von Hard- und Softwarekomponenten für die Zertifizierung	PKI-B & ISM
Weitere Tätigkeiten siehe CP	PKI-B & ISM

Tätigkeiten, die das Vier-Augen-Prinzip erfordern

5.2.3 Identifizierung und Authentifizierung jeder Rolle

Siehe CP.

5.2.4 Rollen, die eine Aufgabentrennung erfordern

Siehe CP.

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 Anforderungen an Mitarbeiter

Die Mitarbeiter der Root-CA der FMG-Konzern PKI und die Freigabe-Ansprechpartner müssen mit folgenden Themen vertraut sein:

- Konzepte und internationale Standards von Public-Key-Infrastrukturen
- Benutzung von Certification Authority Software
- Rollenkonzept, Prozesse, Datenschutz und Datensicherheit der FMG-Konzern PKI

5.3.2 Sicherheitsüberprüfung der Mitarbeiter

Alle Mitarbeiter der Root-CA werden regelmäßig auf Zuverlässigkeit gem. §7 LuftSig geprüft.

5.3.3 Anforderungen an Schulungen

In der Root-CA werden ausschließlich qualifizierte Mitarbeiter eingesetzt, für die regelmäßig geeignete Schulungen durchgeführt werden. Mitarbeiter erhalten erst nach Nachweis der notwendigen Fachkunde die Berechtigung, spezifische Rollen auszuführen.

5.3.4 Häufigkeit und Anforderungen an Fortbildungen

Die Frequenz der Schulungen orientiert sich an den Anforderungen der Root-CA. Schulungen werden insbesondere bei der Einführung neuer Richtlinien, IT-Systeme und Sicherheitstechnik durchgeführt.

5.3.5 Häufigkeit und Ablauf von Arbeitsplatzwechseln

Keine Angabe.

5.3.6 Sanktionen für unerlaubte Handlungen

Unautorisierte Handlungen, die die Sicherheit der IT-Systeme der Root-CA gefährden oder gegen Datenschutzbestimmungen verstoßen, werden disziplinarisch geahndet. Bei strafrechtlicher Relevanz werden die zuständigen Behörden informiert.

5.3.7 Anforderungen an unabhängige, selbstständige Zulieferer

Keine Angabe.

5.3.8 Dokumentation für Mitarbeiter

Den Mitarbeitern der Root-CA steht neben CP und diesem CPS eine ausführliche Dokumentation zur Verfügung.

5.4 Überwachung / Protokollierung

5.4.1 Überwachte Ereignisse

Zur Abwehr von Angriffen und zur Kontrolle der ordnungsgemäßen Funktion der Root-CA werden u.a. nachfolgende Ereignisse in Form von Log-Dateien oder Papierprotokollen erfasst:

- Bootvorgänge
- fehlgeschlagene Login-Versuche
- Eingang und Genehmigung von Zertifikatanträgen und Sperranträgen
- Ausstellung und Sperrung von Zertifikaten

5.4.2 Häufigkeit der Protokollanalyse

Eine Überprüfung der Protokolldaten findet regelmäßig, mindestens alle 90 Tage statt. Bei Verdacht auf außergewöhnliche Ereignisse werden Sonderprüfungen vorgenommen.

5.4.3 Aufbewahrungsfrist für Protokolldaten

Die Aufbewahrungsdauer von Protokollen und Zertifikaten entspricht mindestens der Gültigkeitsdauer des Zertifikats der CA, mit dem das Zertifikat des Zertifikatnehmers erstellt wurde, zuzüglich eines Jahres.

5.4.4 Schutz von Protokolldaten

Elektronische Logdateien werden mit Mitteln des Betriebssystems gegen Zugriff, Löschung und Manipulation geschützt und sind nur den System- und Netzwerkadministratoren zugänglich.

5.4.5 Backup der Protokolldaten

Die Protokolldaten werden zusammen mit anderen relevanten Daten der Root-CA einem regelmäßigen Backup unterzogen.

5.4.6 Überwachungssystem (intern oder extern)

Keine Angabe.

5.4.7 Benachrichtigung bei schwerwiegenden Ereignissen

Bei schwerwiegenden Ereignissen wird unverzüglich das ISM informiert. In Zusammenarbeit mit den Systemadministratoren werden notwendige Aktionen festgelegt, um auf die Ereignisse adäquat reagieren zu können, ggf. wird die Geschäftsleitung informiert.

5.4.8 Schwachstellenanalyse

Eine Schwachstellenuntersuchung findet durch das ISM statt.

5.5 Archivierung

5.5.1 Archivierte Daten

Im Rahmen des Zertifizierungsprozesses werden folgende Daten archiviert:

- Ausgestellte Zertifikate
- Zertifikatswiderrufe und zugehörige Informationen die zwischen Sub-CAs und Root-CA ausgetauscht werden.
- Veröffentlichte CRLs
- Zertifikatsrequests
- System-Konfiguration der Root-CA
- Private Schlüssel der ausgestellten Zertifikate
- Authentifizierungsinformatino für Zertifikat-Sperrung

Vertrauliche Daten, insbesondere die privaten Schlüssel ausgestellter Zertifikate, werden auf sicheren Medien (beispielsweise verschlüsselte Laufwerke) abgelegt.

5.5.2 Aufbewahrungsfrist für archivierte Daten

Digitale Zertifikate und veröffentlichte CRLs der FMG-Konzern PKI sollen mindestens für zwei Jahre nach Gültigkeitsende aufbewahrt werden. Die privaten Signaturschlüssel der PKI werden nicht archiviert.

5.5.3 Schutz der Archive

Es wird durch geeignete Maßnahmen sichergestellt, dass die Daten nicht verändert, gelöscht, unbefugt gelesen oder kopiert werden können.

5.5.4 Backup der Archive (Datensicherungskonzept)

Die Sicherung der Konfiguration sowie des verschlüsselten privaten Schlüssels der Root-CA erfolgt manuell auf externe Datenträger. Parallel dazu wird das Image der Root-CA monatlich auf ein virtuelles Tape gesichert.

5.5.5 Anforderungen an Zeitstempel

Alle archivierten Daten sind mit einem Zeitstempel zu versehen.

5.5.6 Archivierungssystem (intern oder extern)

Es wird ein internes Archivierungssystem verwendet.

5.5.7 Prozeduren für Abruf und Überprüfung archivierter Daten

Das ISM kann den Abruf und die Prüfung der archivierten Daten autorisieren.

5.6 Schlüsselwechsel der Zertifizierungsstelle

Die Gültigkeitsdauer von Schlüsseln ist in Abschnitt 6.3 festgelegt. Falls ein Schlüssel der CA kompromittiert wurde, gelten die in Abschnitt 5.7 aufgeführten Regelungen. Nach Erzeugung eines neuen CA-Schlüssels muss dieser gemäß Kapitel 2 veröffentlicht werden.

5.7 Kompromittierung und Wiederherstellung (disaster recovery)

Siehe CP.

5.8 Einstellung des Betriebs

Siehe CP.

6 TECHNISCHE SICHERHEITSMASSNAHMEN

6.1 Schlüsselerzeugung und Installation

Siehe CP.

6.2 Schutz privater Schlüssel und Einsatz kryptographischer Module

Siehe CP.

6.3 Weitere Aspekte des Schlüsselmanagements

Siehe CP.

6.4 Aktivierungsdaten

Siehe CP.

6.5 Sicherheitsmaßnahmen für Computer

Die Root-CA wird auf einer virtuellen, verschlüsselten Maschine betrieben, welche keine Netzverbindung unterhält. Der Zugang zu dieser Maschine kann nur durch ein 4-Augen Prinzip erfolgen.

6.6 Technische Maßnahmen im Lebenszyklus

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

6.6.1 Maßnahmen der Systementwicklung

Änderungen am Systemdesign der Root-CA der FMG-Konzern PKI werden zunächst in einer Testumgebung durchgeführt und anschließend bewertet. Die Produktiv- und Testumgebung sind völlig voneinander getrennt. Die letztendliche Durchführung von Änderungen auf einem Produktivsystem erfolgt erst nach Abnahme und Freigabe der Testumgebung.

6.6.2 Maßnahmen im Sicherheitsmanagement

Die Log-Daten, die Konfigurationsdaten und relevante Systemressourcen werden regelmäßig überprüft.

Das ISM umfasst folgende Aspekte:

- jährliches Audit (Konformitätsprüfung)
- regelmäßige Evaluierung und Weiterentwicklung des Sicherheitskonzepts
- Überprüfung der Sicherheit im laufenden Betrieb (siehe Abschnitt 5.4)

- regelmäßige Integritätsprüfungen der eingesetzten Anwendungen und Betriebssysteme
- Einspielung von Upgrades und Patches sofern erforderlich

6.6.3 Lebenszyklus der Sicherheitsmaßnahmen

Keine Angaben.

6.7 Sicherheitsmaßnahmen für das Netzwerk

Die Root-CA wird auf einer virtuellen Maschine betrieben, welche keine permanente Netzverbindung unterhält. Der Zugriff auf das System erfolgt ausschließlich über gesicherte Verbindungen.

6.8 Zeitstempel

Siehe CP.

7 PROFILE FÜR ZERTIFIKATE, SPERRLISTEN UND ONLINESTATUSABFRAGEN

Siehe CP.

8 KONFORMITÄTSPRÜFUNG (Compliance Audit, Assessments)

Siehe CP.

9 INFORMATIONEN ZUM DOKUMENT

Siehe CP.

10 GLOSSAR

Siehe CP.