Erklärung zum Zertifizierungsbetrieb der HvS PKI

Version 1.2 vom 06.04.2023

Freigabe

Ansprechpartner	Datum
Verantwortlich: 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 und Anpassung
1.2	06.04.2023	Hochenrieder (HvS)	Review & Update, speziell Einsatz von Yubikeys

Mitgeltende Unterlagen

Dokument	Veröffentlichung
Zertifizierungsrichtlinie der HvS PKI	http://www.hvs-consulting.de/pki

Inhaltsverzeichnis

1 Einleitung

1.1 Überblick

Dieses Dokument stellt die „Erklärung zum Zertifizierungsbetrieb der HvS PKI“ (CPS) dar. Es beschreibt Spezifikationen, Prozesse und technische Sicherheitsmaßnahmen der beiden CAs (Root-CA, Issue-CA) für die Ausstellung von Zertifikaten.
Diesem Dokument zugehörig ist die Zertifizierungsrichtlinie (CP) der HvS in der jeweils aktuellen Version: "Zertifizierungsrichtlinie der HvS PKI".

1.2 Dokumentenname sowie Identifikation

Diese CPS ist folgendermaßen identifiziert:
- Titel: Erklärung zum Zertifizierungsbetrieb der HvS PKI
- Version: 1.1
- Object Identifier (OID): 1.3.6.1.4.1.39398.30.2.1.0

Der OID [OID] ist wie folgt zusammengesetzt:
{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) HvS(39398) pki(30) cps(2) major-version(1) minor- version(0)}

1.3 Teilnehmer der Zertifizierungsinfrastruktur (PKI)

1.3.1 Zertifizierungsstellen

Siehe CP.

1.3.2 Registrierungsstellen

Siehe CP.

1.3.3 Zertifikatsinhaber (Subscribers)

Siehe CP.

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

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 speziell gesicherten Rechenzentren der HvS untergebracht.

5.1.2 Räumlicher Zugang

Nur autorisierte Personen haben Zutritt zu den Rechenzentren der HvS.

5.1.3 Stromversorgung und Klimaanlagen

Die Rechenzentren von HvS sind mit einer Notstromversorgung ausgestattet und klimatisiert.

5.1.4 Gefährdung durch Wasser

In den Rechenzentren von HvS wurden Vorkehrungen gegen Überschwemmung und Wassereinbruch getroffen.

5.1.5 Brandschutz

Die Rechenzentren von HvS sind mit Rauchmeldern und Löscheinrichtungen gemäß der gesetzlichen Anforderungen ausgestattet.

5.1.6 Aufbewahrung von Datenträgern

Alle Daten werden innerhalb der Rechenzentren der HvS gelagert. HvS betreibt zwei räumlich voneinander getrennte Rechenzentren.

5.1.7 Externe Datensicherung

Keine Angaben.

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 Rollenkonzept

Siehe CP.

5.2.2 Anzahl involvierter Personen pro Aufgabe

Siehe CP.

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 HvS PKI müssen mit folgenden Themen vertraut sein:

- Zertifikate und das Zusammenspiel mit dem Schlüsselmaterial
- Rollenkonzept der HvS PKI
- Prozesse der HvS PKI
- Datenschutz und Informationssicherheit bei HvS bzw. der HvS PKI

5.3.2 Sicherheitsüberprüfung der Mitarbeiter

Keine Angaben.

5.3.3 Anforderungen an Schulungen

Bei HvS 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 PKI. Schulungen müssen insbesondere bei der Einführung neuer Richtlinien, IT-Systeme und Sicherheitstechnik durchgeführt werden.

5.3.5 Häufigkeit und Ablauf von Arbeitsplatzwechseln

Keine Angaben.

5.3.6 Sanktionen für unerlaubte Handlungen

Unautorisierte Handlungen, die die Sicherheit der IT-Systeme der PKI 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 Angaben.

5.3.8 Dokumentation für Mitarbeiter

Den Mitarbeitern der PKI steht neben CP und diesem CPS die Dokumentation der PKI zur Verfügung.

5.4 Überwachung / Protokollierung

5.4.1 Überwachte Ereignisse

Zur Abwehr von Angriffen und zur Kontrolle der ordnungsgemäßen Funktion der PKI 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
- Einrichtung und Änderung von Rollenzuordnungen und Berechtigungen

Die Logs werden an das zentrale SIEM System weitergeleitet.

5.4.2 Häufigkeit der Protokollanalyse

Eine Überprüfung der Protokolldaten findet regelmäßig mindestens einmal pro Quartal statt. Bei Verdacht auf außergewöhnliche Ereignisse werden Sonderprüfungen vorgenommen.

5.4.3 Aufbewahrungsfrist für Protokolldaten

Die Aufbewahrungsdauer von Dokumenten 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 PKI einem regelmäßigen Backup unterzogen.

5.4.6 Überwachungssystem (intern oder extern)
Keine Angaben.

5.4.7 Benachrichtigung bei schwerwiegenden Ereignissen
Bei schwerwiegenden Ereignissen wird unverzüglich der IT-Sicherheitsbeauftragte der HvS 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
Mindestens einmal alle drei Jahre findet eine Schwachstellenuntersuchung im Rahmen eines Audits durch externe Dienstleister statt.

5.5 Archivierung

5.5.1 Archivierte Daten
Keine Angaben.

5.5.2 Aufbewahrungsfrist für archivierte Daten
Keine Angaben.

5.5.3 Schutz der Archive
Keine Angaben.

5.5.4 Backup der Archive (Datensicherungskonzept)
Keine Angaben.

5.5.5 Anforderungen an Zeitstempel
Keine Angaben.

5.5.6 Archivierungssystem (intern oder extern)
Keine Angaben.

5.5.7 Prozeduren für Abruf und Überprüfung archivierter Daten
Keine Angaben.

5.6 Schlüsselwechsel der Zertifizierungsstelle

Falls ein Schlüssel der CA kompromittiert wurde, gelten die in Abschnitt 5.7aufgeführten 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 offline – als Standalone-System – betrieben. Diese wird nur halbjährlich zur Aktualisierung der CRLS / Patching etc. online geschaltet. Die Issue-CAs laufen als Onlinesysteme in dedizierten Netzen und werden regelmäßig gepatcht bzw. gehärtet.

6.6 Technische Maßnahmen im Lebenszyklus

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

6.6.1 Maßnahmen der Systementwicklung

Keine Angaben.

6.6.2 Maßnahmen im Sicherheitsmanagement

Keine Angaben.

6.6.3 Lebenszyklus der Sicherheitsmaßnahmen

Keine Angaben.

6.7 Sicherheitsmaßnahmen für das Netzwerk

Das Netzwerk ist in verschiedene Sicherheitszonen unterteilt, die jeweils durch ein Firewallsystem voneinander abgeschottet sind. Darüber hinaus werden zur Abwehr von Angriffen aus dem Internet, wie auch aus dem Intranet, Intrusion Prevention bzw. Detection sowie SIEM Systeme eingesetzt.
Kritische Sicherheitsvorfälle werden unverzüglich durch die PKI-Administration verfolgt und bearbeitet. Auf allen Firewalls ist ein Regelwerk aktiviert, das nur den in einer definierten Kommunikationsmatrix erlaubten Netzwerkverkehr zulässt.

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.