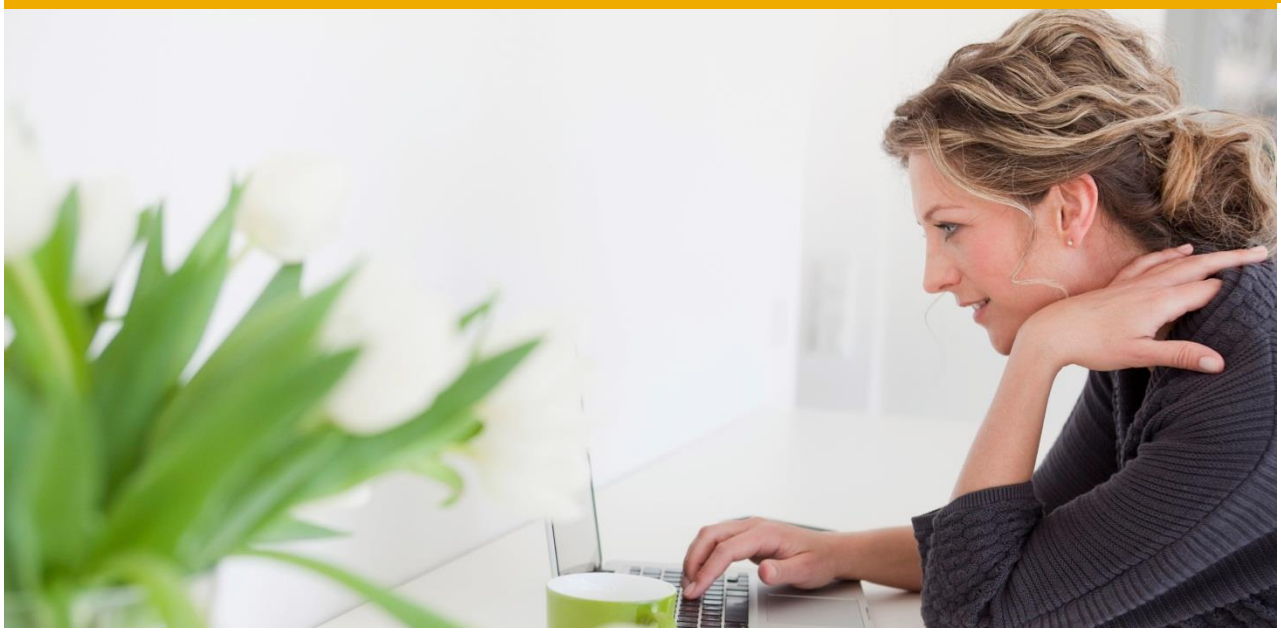


SAP Global PKI Zertifizierungsrichtlinie (Certificate Policy – CP)

INFORMATIONEN ZUM DOKUMENT

Übersicht

Titel des Dokuments	SAP Global PKI Zertifizierungsrichtlinie (Certificate Policy – CP)
Dateiname	SAP-PKI-CP-v1-german.docx
Beschreibung	Zertifizierungsrichtlinie der SAP Global PKI auf Basis des RFC 3647
Version	1.1
Object Identifier	OID 1.3.6.1.4.1.694.4.100.2
Abgelöste Dokumente	Keine
Autoren	Walther, Ralf; Hackenschmidt, Chrstopher; Christian Rothländer
Verantwortlicher Ansprechpartner bei SAP	Christian Rothländer

Versionshistorie

Version	Datum	Kommentar
0.1	23.01.2013	Komplette Neufassung in Deutsch auf Basis des Dokuments in Englisch von Herrn Höltkemeier (Microsoft)
0.91	16.09.2013	Endgültige Fassung (ohne LEGAL involvement Kap 9.x)
0.95	29.04.2014	Endgültige Fassung (mit Legal abgestimmt)
1.0	13.05.2014	Version zur Veröffentlichung (incl Code Signing Thematik)
1.1	09.12.2016	Aktualisiert: Org. Security 1.5, CA Betrieb 5.1, Gültigkeiten von Zertifikaten 6.3.2

TABLE OF CONTENTS

1 EINLEITUNG

Eine Zertifizierungsrichtlinie oder im Englischen *Certificate Policy* (CP) ist ein öffentlich zugängliches Dokument, welches die Eignung eines Zertifikats für bestimmte Anwendungsgebiete beschreibt. Dabei werden die Sicherheitsanforderungen definiert, die dem Betrieb der Infrastruktur und der Handhabung der Zertifikate zugrunde liegen. Anhand der CP ist es Nutzern möglich einzuschätzen, ob ein Zertifikat für ihren Anwendungsfall vertrauenswürdig ist oder nicht.

Der Zertifizierungsrichtlinie gegenüber steht das *Certification Practice Statement* (CPS), welches beschreibt wie die Anforderungen der CP umgesetzt sind. Die CP definiert also was zu tun ist, während das CPS dokumentiert wie dies geschieht. Da die Inhalte eines CPS durchaus vertrauenswürdig sind empfiehlt es sich dieses in einer Zusammenfassung nur auszugsweise zu veröffentlichen. Auf Anfrage kann eine prüfende Instanz Zugang zu dem kompletten Dokument erhalten.

Das folgende Dokument beschreibt die Zertifizierungsrichtlinie für PKIs der SAP SE mit einem Basisschutzbedarf. Sie ist Teil der SAP Sicherheitsrichtlinien und –standards und leitet sich direkt von der „*Allgemeinen Zertifizierungsrichtlinie für produktive Zertifizierungshierarchien*“ ab (Abb. 1).

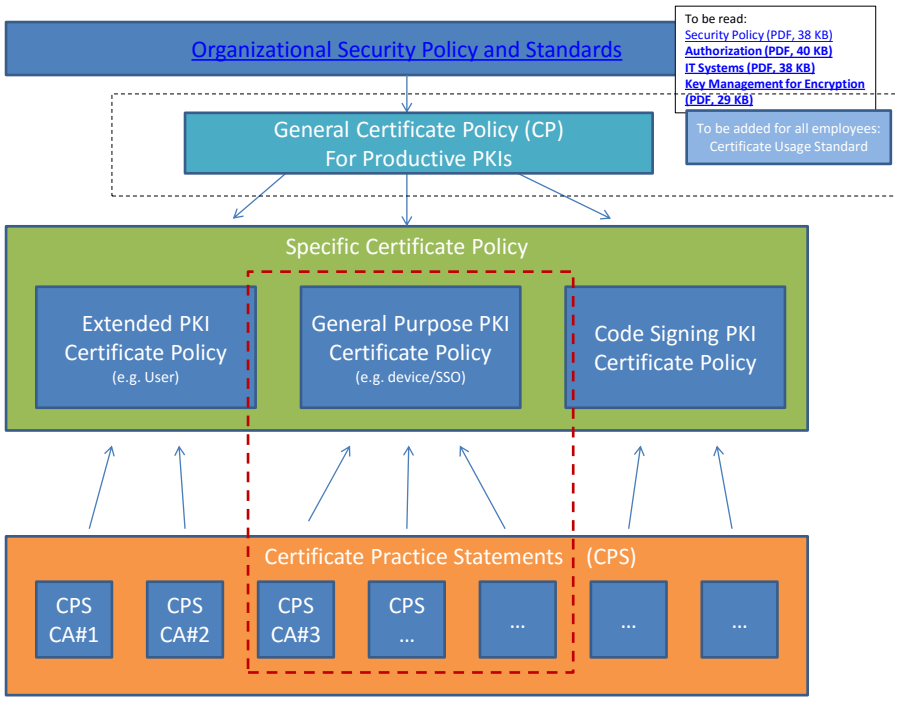


Abb. 1 - Überblick über die SAP-Zertifizierungsrichtlinien

Zu Zertifikaten für Anwendungen mit einem Basisschutzbedarf zählen Serverzertifikate für SSL/TLS oder Zertifikate zur Benutzerauthentisierung (SSO). Andere Anwendungsgebiete wie Datenverschlüsselung oder –signierung werden von dieser Zertifizierungsrichtlinie nicht behandelt.

Dieses Dokument ist gemäß der Leitlinien in RFC 3647 erstellt und richtet sich an alle Zertifikatsinhaber/-prüfer und die Betreiber der PKI sowie deren Auditoren.

1.1 Überblick

Jede von der SAP SE betriebene PKI unterliegt bestimmten Anforderungen bezüglich ihrem Aufbau und ihrer Umsetzung. Die folgenden Punkte geben einen Überblick, welche Grundvoraussetzungen zu erfüllen sind:

- **Hierarchie**: Eine PKI muss eine mindestens zweistufige aber maximal dreistufige Hierarchie von Zertifizierungsstellen sein, an deren Wurzel eine offline betriebene Root-CA steht.
- **Zweckbestimmung**: Ausgebende CAs müssen zweckgebunden sein, d.h. dediziert für Maschinen bzw. Benutzerzertifikate ausgelegt sein.
- **Zertifikatseinschränkungen**: Soweit umsetzbar ist die Zweckbestimmung in die Einschränkungen der Zertifikate aufzunehmen. Insbesondere ist über *Basic Constraints* zu gewährleisten, dass nur die Root-CA Zertifikate für Zertifizierungsstellen ausgeben kann.

- **Widerrufinformationnen**: Angaben über die Gültigkeit eines Zertifikats sind über die bekannten Mechanismen (CRL Download und OCSP) Zertifikatsprüfern zur Verfügung zu stellen.
- **Verfügbarkeit**: Alle online verfügbaren Komponenten einer PKI sind hochverfügbar auszulegen, so dass der Ausfall einer einzelnen Komponente nicht zu einem Ausfall des Dienstes führt.
- **Schlüsselschutz**: Die privaten Schlüssel aller online erreichbaren Zertifizierungsstellen sind durch Hardware-seitige (HSM, SmartCard, TPM, etc.) Mechanismen vor Angriffen zu schützen. Ausnahmen sind durch IT Security zu genehmigen.
- **Mehr-Augen Prinzip**: Alle Operationen mit oder auf dem privaten Schlüssel der Root-CA sind durch ein Mehr-Augen Prinzip zu überwachen und dokumentieren.
- **Systemhärtung**: Alle beteiligten Systeme einer PKI sind anhand ihrer Rolle gemäß den SAP-Richtlinien zu abzusichern.
- **Audits**: Die Systemumgebung ist regelmäßig, spätestens nach weitreichenden Änderungen zu auditieren. Dies kann durch einen externen Dienstleister oder intern geschehen.

1.2 Dokumentenname sowie Identifikation

Dieses Dokument heißt ***SAP Global PKI Zertifizierungsrichtlinie (Certificate Policy - CP)*** und wird über einen eigenen *Object Identifier* (OID) referenziert.

x.509 OID	Beschreibung
1.3.6.1.4.1.694.4	SAP Global PKI Base of the SAP Global PKI Namespace
1.3.6.1.4.1.694.4.100	Production environment Base of the SAP Global PKI production environment
1.3.6.1.4.1.694.4.100.1	PKI Policy SAP Global PKI Certificate Policy / Certification Practice Statement Policy Reference
1.3.6.1.4.1. 694.4.100.2	Current CP documentation SAP Global PKI Certificate Policy Version 1.0
1.3.6.1.4.1. 694.4.100.3	Current CPS documentation SAP Global PKI Certification Practice Statement Version 1.0

Die Zertifizierungsrichtlinie und das CPS sind öffentlich unter folgender Internetadresse erreichbar:

http://www.pki.co.sap.com/

1.3 Teilnehmer der Zertifizierungsinfrastruktur (PKI)

Diese Zertifizierungsrichtlinie beschreibt

1.3.1 Zertifizierungsstellen

Die Hierarchie einer SAP Basisschutzbedarf PKI

Bei der *SAP Global PKI* handelt es sich um eine zweistufige PKI Hierarchie. Unter der offline Root-CA befinden sich zwei ausstellende Sub-CAs, wobei eine ausschließlich Benutzerzertifikate und die andere nur Maschinenzertifikate ausstellt.

1.3.2 Registrierungsstellen

Registrierungsstellen sind die SAP AD und die WEB-RA.

1.3.2.1 Online Registrierung

- SAP AD
- Authentisierung / Identifikation (AD Mitgliedschaft und dazugehörige Prozesse (Hardware/Software Verteilungsprozess der SAP)
- Keine Prüfung aber Einschränkung durch AD Informationen und dadurch definierte Werte (Microsoft: autoenrollment)

1.3.2.2 Offline Anforderung

- WEB-RA
- Authentisierung / Identifikation
- Prüfung (manuell)

1.3.3 Zertifikatsinhaber (Subscribers)

Als Inhaber gelten die im Zertifikat aufgeführten Entitäten. Dies können Benutzer, Systeme (Computer, Appliances, etc.) oder auch Dienste sein.

Benutzer sind immer Personen mit einer, zum Zeitpunkt der Anfrage, gültigen SAP Benutzer ID oder ID eines Unternehmens, welches in vertraglich geregelter, partnerschaftlicher Beziehung zu SAP steht.

Als Maschinen bzw. Systeme werden nur Geräte mit einer gültigen SAP Asset Management Eintrag oder eines äquivalenten Bezeichners eines Partner-Unternehmens der SAP angesehen.

Dienste können nur auf obig als Maschinen bezeichneten Systemen ausgeführt und durch, als obig als Benutzer bezeichnete Personen betrieben werden.

Zertifikatsinhaber sind gleichzeitig auch immer die Besitzer des zum Zertifikat gehörigen privaten kryptographischen Schlüssels. Mit diesem Besitz gehen weitere Verantwortlichkeiten einher (vgl. 9.6.3)

1.3.4 Zertifikatsprüfer (Relying Parties)

Unter einem Prüfer versteht man die Partei, welche auf die Gültigkeit eines Zertifikats angewiesen ist, um die Vertrauenswürdigkeit eines Zertifikatsinhabers auf Basis der Zertifikatsrichtlinie überprüfen und einschätzen zu können.

Wer die Prüfer eines Zertifikats sind hängt von dessen Anwendung ab. Sowohl Maschinen als auch Personen kommen hier in Frage. Obwohl Zertifikate nur an einen eingeschränkten Kreis ausgestellt werden, kann potentiell jedes System oder jede Person, also auch außerhalb der SAP, eine Zertifikat auf Gültigkeit überprüfen.

Jeder Prüfer stimmt durch die Nutzung des Zertifikats implizit dieser Richtlinie zu.

1.3.5 Weitere Teilnehmer

Eine weitere Komponente der PKI stellen die Ablageorte für die Informationen hinter den Einträgen in den Zertifikaten für den *Authority Information Access* (AIA), die *Certificate Revocation Lists* (CRL) und die Zertifikatsrichtlinien dar. Diese muss zumindest ein Webserver über HTTP bereitstellen. Gleiches gilt für den *Online Certificate Status Protocol* (OCSP) Dienst.

In *Microsoft*-basierten PKIs kommt zusätzlich noch das *Active Directory* (AD) als Repository hinzu, in PKI Umgebungen anderer Hersteller ist häufig ein LDAP-Verzeichnis o.ä. Datenbank an dessen Stelle. Diese gelten genauso als Teil der PKI Umgebung, wie etwaige *Hardware Security Module* (HSM), wie hier auch gefordert und müssen gesondert berücksichtigt werden.

Darüber hinausgehende Teilnehmer wie bspw. eine Bridge-CA finden in dieser CP keine Berücksichtigung.

1.4 Anwendungsbereich

Bei den Zertifizierungsstellen einer SAP PKI mit Basisschutzbedarf handelt es sich um sog. „Basic Validation“ CAs, d.h. bei der Authentisierung der Zertifikatsinhaber wird auf vorhandene Mechanismen (Passwort, Zertifikat, Email, Zwei-Faktor, o.ä.) zurückgegriffen. Dies steht im Gegensatz zur erweiterten Überprüfung von Zertifikatsinhabern, bei der Antragsteller persönlich vorstellig werden und sich mittels Lichtbildausweis identifizieren können müssen.

Da Zertifikate für die Signatur (Stichwort: Nichtabstreitbarkeit) und zur Verschlüsselung (Stichwort: Schlüsselwiederherstellung) wesentlichen höheren Anforderungen genügen müssen, dürfen unter dieser Richtlinie nur Zertifikate für die Authentisierung von Endteilnehmern und zur Transportverschlüsselung ausgestellt werden.

Somit ist auch gegeben, dass PKIs dieses Typs keine qualifizierten Zertifikate im Sinne des Signaturgesetzes ausstellen können.

Der Einsatz aller durch diese PKIs ausgestellten Zertifikate ist ausschließlich für den SAP eigenen Gebrauch bestimmt, d.h. zur Authentisierung interner Systeme gegenüber SAP Mitarbeitern bzw. Partnern und umgekehrt, sowie zur Verschlüsselung des Netzverkehrs zwischen von der SAP oder Partnern betriebenen Systemen oder Dokumenten.

1.4.1 Geeignete Zertifikatsnutzung

Die Nutzungsbereiche der ausgestellten Zertifikate leiten sich direkt von der Validierung der Zertifikatsinhaber ab. Somit ergeben sich die folgenden geeigneten Nutzungsszenarien:

- Maschinenzertifikate
    - Authentisierung
    - Transport-Verschlüsselung
    - Code Signing
- PKI bezogenen Maschinenzertifikate
    - CA Signaturen
    - OCSP Response Signaturen
- Benutzerzertifikate
    - Authentisierung
    - Verschlüsselung

1.4.2 Eingeschränkte Zertifikatsnutzung

Alle durch SAP PKIs mit Basisschutzbedarf ausgestellten Zertifikate dienen ausschließlich der Nutzung durch SAP eigene Systeme, Mitarbeiter und Partner. Ein Einsatz in externen Szenarien, also eine Ausstellung von Zertifikaten an, - oder deren Prüfung durch Entitäten ohne ein vertraglich geregeltes Verhältnis zu SAP, ist nicht vorgesehen.

Zu beachten ist, dass die grundsätzliche Art der Identitätsvalidierung der Zertifikatsinhaber, dieselben Vertrauensannahmen erlaubt, wie die Validierungsprozesse selbst. Somit ist eine Identifizierung über ein Zertifikat dieses PKI Typs einer Anmeldung mittels Benutzername und Passwort gleichzustellen.

1.4.3 Untersagte Zertifikatsnutzung

Grundsätzlich sind alle nicht unter 1.4.1 und 1.4.2 aufgeführten Nutzungen untersagt. Insbesondere sind das:

- Nutzung von Endteilnehmerzertifikaten als CA Zertifikat
- Nutzung der Endteilnehmerzertifikate für einen anderen Zweck als im Antrag angegeben
- Einsatz der Endteilnehmerzertifikate außerhalb ihrer Gültigkeit
- Nutzung der Endteilnehmerzertifikate nach deren Rückzug durch die PKI
- Nutzung von Maschinenzertifikaten auf SAP-fremden und nicht-zertifizierten Partner-Systemen
- Einsatz für nicht-SAP-interne oder nicht-SAP-Partner-Prozesse

1.5 Verwaltung der Zertifizierungsrichtlinie

1.5.1 Änderungsmanagement

Die Richtlinie wird verwaltet und geändert durch *SAP Global Security - Secure Operations*

s.9.12

Im Dokument wird diese Abteilung mit SAP „IT Security“ bezeichnet, um häufige Aktualisierung des Dokumentes durch organisatorische Umbenennung zu vermeiden und zu vereinfachen.

1.5.2 Ansprechpartner

SAP SE
SAP Global Security - Secure Operations
Dietmar-Hopp-Allee 16
69190 Walldorf
Germany

Voice: +49 6227-7-47474
Fax: +49 6227-7-57575
Email: sap.it.security@sap.com
Web: http://www.sap.com

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

Die Prüfung einer Übereinstimmung eines *Certification Practice Statements* (CPS) mit dieser Zertifizierungsrichtlinie (CP) findet durch die unter 1.5.2 angegebene Stelle statt.

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

Die Regelungen für den Betrieb einer Zertifizierungsstelle sind durch deren Betreiber zur Verfügung zu stellen und der IT Sicherheitsabteilung (IT Security) zur Ansicht und Kontrolle vor der produktiven Inbetriebnahme vorzulegen.

Die Bestätigung der Konformität zu dieser Richtlinie wird auch durch IT Security gegeben. Änderungen am CPS sind IT Security unverzüglich anzuzeigen und erfordern eine erneute Abnahme.

1.6 Definitionen und Abkürzungen

1.6.1 Abkürzungen

CA	Certification Authority (Zertifizierungsstelle)
CP	Certificate Policy (Zertifikatsrichtlinie)
CPS	Certification Practice Statement
HSM	Hardware Security Module
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastruture
RA	Regsitration Authority
SSL/TLS	Secure Socket Layer / Transport Layer Security
SSO	Single Sign On

1.6.2 Definitionen

Zum Verständnis dieser Zertifikatsrichtlinie wird davon ausgegangen, dass grundsätzliche Begriffe wie z.B. „Zertifikat“, „PKI“, „Verzeichnisdienst“, etc., die mit dem Betrieb einer Zertifizierungsstelle zusammenhängen, bekannt sind. Dies gilt insbesondere auch für deren englische Entsprechungen. Darüber hinaus sind die folgenden Begriffe wichtig:

Endteilnehmer	Ein Endteilnehmer kann im Zusammenhang mit dieser Richtlinie entweder ein System, ein Service, ein Benutzer oder eine Gruppe aus diesen sein. Ein Endteilnehmer ist entweder ein Zertifikatsnehmer oder –prüfer.
Maschine/System	Eine Maschine bzw. System bezieht sich auf alle Objekte, welche durch eine Equipment-Nummer bzw. einen *Asset Management* Eintrag oder einen ähnlichen Bezeichner eines SAP Partners eindeutig identifiziert sind.
Benutzer	Benutzer sind alle Individuen, die in den offiziellen HR Systemen SAPs bzw. eines Partners gepflegt werden und eine eindeutige ID besitzen.
Auto-Enrollment	Der Begriff ist synonym für einen automatisierten und ereignisgesteuerten Prozess im Zusammenhang mit der Verteilung und Erneuerung von Endteilnehmer-Zertifikaten zu verstehen.
Basisschutzbedarf	
Registrierungsstelle (RA)	Eine *Registration Authority (RA)* bezeichnet eine einer CA vorgelagerte Instanz, deren Aufgaben die Authentisierung und Autorisierung von Endteilnehmern und die Überprüfung der Korrektheit der Angaben der Zertifikats- und Sperrlistenanträge ist.

2 VERÖFFENTLICHUNGEN UND VERZEICHNISDIENST

2.1 Verzeichnisdienste

Für den Betrieb einer SAP Grundschutz CA ist es erforderlich bestimmte Daten vorzuhalten und zu speichern. Dazu ist der Einsatz mindestens eines oder mehrerer Verzeichnisse vorgesehen, welche im CPS genauer spezifiziert werden. Verzeichnisse können u.a. Informationen zu Endteilnehmern, Zertifikaten und deren Gültigkeit haben.

Verzeichnisdienste müssen so betrieben werden, dass sie denselben Verfügbarkeitsanforderungen genügen, wie der PKI Dienst selbst. Es sind alle durch die PKI genutzten Verzeichnisse und deren Protokolle im CPS aufzuführen.

2.2 Veröffentlichung von Zertifizierungs-Informationen

Die Betreiber einer SAP CA sind verpflichtet bestimmte Informationen über die Zertifizierungsstelle und deren ausgestellte Zertifikate öffentlich bzw. gemäß des Einsatzzweckes SAP intern zur Verfügung zu stellen. Hierzu zählen vor allem auch die Zertifikatsrichtlinie, das zugehörige CPS Abstract und etwaige Vereinbarung mit Zertifikatsinhabern und –prüfern. Der Ort, an dem diese Informationen abrufbar sind ist mittels „CP qualifier“ in die ausgestellten Zertifikate aufzunehmen.

Darüber hinaus sind Gültigkeitsinformationen zu den ausgestellten Zertifikaten zu veröffentlichen, so dass Zertifikatsprüfer einfach in der Lage sind möglichst aktuelle Angaben über Zertifikatssperrungen zu erlangen. Es sind sowohl Veröffentlichungen von Sperrlisten als auch Einzelinformationen über das *Online Certificate Status Protocol* (OCSP) gefordert. Die zweckdienliche Bereitstellung des öffentlichen Teils der ausgestellten Zertifikate und deren Replikation in auch SAP fremde Verzeichnisse sind, bei Wahrung der hier vorgegebenen Richtlinien, möglich

2.3 Aktualisierung der Informationen (Zeitpunkt, Frequenz)

CP, CPS und damit zusammenhängenden Dokumenten sollten möglichst selten überarbeitet werden. Geringfügige Änderungen sind daher zu sammeln und dürfen höchstens einmal im Jahr in aktualisierte Versionen der Dokumente eingepflegt werden. Weitrechende Veränderungen sind hingegen sofort einzuarbeiten und zu veröffentlichen.

Gültigkeitsinformationen zu Zertifikaten sind abhängig von der zugrundliegenden Technologie maximal aktuell vorzuhalten und dürfen nicht länger als 14 Tage zwischengespeichert werden. Genaue Angaben finden sich in die Absätzen (CRL) und (Zertifikate).

2.4 Zugangskontrolle zu Verzeichnisdiensten

Lesender Zugriff auf die PKI relevanten Informationen in den Verzeichnissen ist grundsätzlich unkritisch und kann somit anonym und unautorisiert erfolgen. Für den Einsatzzweck nicht erforderlicher Zugriff sollte aber verhindert werden.

Schreibender Zugriff und insbesondere das Hinzufügen oder Löschen von Datensätzen darf nur durch autorisierte Rollen der PKI erfolgen. Hier sind logische und physikalische Schutzmaßnahmen zu ergreifen, so dass dies nach Stand der Technik gewährleistet werden kann.

3 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

3.1 Namen

SAP PKIs sind nach dem x.509 Standard aufgebaut und haben somit zugehörige Vorgaben zu erfüllen. Dies gilt für das Format der Zertifikate und auch die darin angegebenen Namen, welche in den Feldern *Subject* und *Subject Alternate Name* (SAN) vorkommen können.

Angaben zu Endteilnehmern sind dabei relativ frei in ihrer Form welche direkt von dem Einsatz der Zertifikate und der verarbeitenden Instanzen abhängt. Trotzdem sind hier Namen so zu wählen, dass es möglich ist ein Zertifikat eindeutig und zweifelsfrei einem Endteilnehmer zuzuordnen.

Einen Spezialfall stellen CA und CRL Signatur Zertifikate dar. Hier definiert RFC 5280, dass *Subject* und Aussteller im Zertifikat übereinstimmen müssen.

3.1.1 Namensformen

Alle Namen, die in durch eine SAP-CA ausgestellten Zertifikaten vorkommen, folgen dem Format der *Distinguished Names* (DN) des X.500 Standards der internationalen Fernmeldeunion (ITU-T), genauer der Empfehlungen X.501 und X.520.

Die Details über nötige und optionale Attribute des DN sind im jeweiligen CPS spezifiziert wobei es egal ist, ob der DN aus manuell gemachten Angaben oder automatisch bspw. durch einen Verzeichnisabgleich erstellt wird. Da im letzteren Fall eine Trennung zwischen Antragsteller und Namensquelle besteht können hier die Mindestanforderungen leicht unterschiedlich ausfallen.

Im Folgenden sind die Mindestanforderungen für die einzelnen Zertifikatstypen definiert.

3.1.1.1 CA Zertifikate

Bei Zertifikaten von Zertifizierungsstellen und solchen, die für die Signatur von Sperrlisten (CRL) verwendet werden macht RFC 5280 genaue Vorgaben. So müssen *Subjec* und *Issuer* übereinstimmen und ein nicht leerer DN nach X.500 Standard sein.

Die folgenden Attribute und Werte sind im *Subject* mindestens anzugeben:

- **CN** (commonName)
  Der Name der CA kann frei gewählt sein, muss aber aussagekräftig sein, so dass die Funktion der CA hervorgeht
- **O** (organization)
  Die Organisation also das Unternehmen welches die CA betreibt, also im Normalfall „SAP SE“
- **C** (country)
  Das Land nach ISO3166-1, Alpha2 (2 Ländercodes), in welchem die CA betrieben wird

Für den SAN werden keine Vorgaben gemacht, dessen Angabe ist auch unüblich und empfiehlt sich nicht.

3.1.1.2 Domain Controller Certificates

Domain Controller Zertifikate entsprechen Server Zertifikate (s. 3.1.1.3)

3.1.1.3 Server Zertifikate (incl. DC und OCSP)

Zertifikate dieses Typs dienen i.a. dem Authentisieren eines Dienstes gegenüber einem Client. Entscheidend hierfür sind der *Common Name* (CN) im *Subject* und der *DNS Name* bzw. *IP* im SAN. Für einen automatischen Ausstellungsprozess, welcher seine Angaben aus einem Verzeichnis bezieht, kann ein CN bereits ausreichend sein, es muss aber sichergestellt sein, dass sich der Dienst und somit der Betreiber über diesen Namen eindeutig identifizieren lassen.

Die folgenden Mindestanforderungen gelten für das ***Subject*** wenn es nicht leer ist:

- **CN** (commonName)
  Wertbelegung ist offen, muss aber den Host-/Dienstnamen bzw. den Host-Header der Webseite enthalten und konform zum relevanten Standard ausgeführt sein (X.400, X.500, RFC822, etc.)
- **OU** (organizationalUnit) – nur bei manuellem Antrag
  Wertbelegung frei wählbar, muss eine existierende SAP Abteilung oder eine äquivalente Organisationsstruktur eines Partners so präzise wie möglich beschreiben
- **O** (organization) – nur bei manuellem Antrag
  Die Organisation welche den Dienst betreibt, also im Normalfall „SAP SE“ bzw. ein Partner Unternehmen

- **C** (country) – nur bei manuellem Antrag
  Das Land nach ISO3166-1, Alpha2 (2 Ländercodes), in welchem der Dienst betrieben wird

Für **SANs** (falls vorhanden) sind mindestens die folgenden Angaben zu machen:

- **DNSName**
  Analog zum *Common Name **des** Subject*
- **IP** (iPAddress) – nur bei manuellem Antrag
  die IP Adresse des Systems

3.1.1.4 Code Signing Zertifikate (SAP intern)

Zertifikate dieses Typs dienen i.a. dem Authentisieren einer Software gegenüber einem Client. Entscheidend hierfür sind der *Common Name* (CN) im *Subject* und der *Zeitstempel*. Es muss sichergestellt sein, dass sich der Hersteller der Software, insbesondere die SAP interne Abteilung über diesen Namen eindeutig identifizieren lassen.

Die folgenden Mindestanforderungen gelten für das ***Subject*** wenn es nicht leer ist:

- **CN** (commonName)
  Wertbelegung ist offen, muss aber den Einsatzzweck des Zertifikates beschreiben und konform zum relevanten Standard ausgeführt sein (X.400, X.500, RFC822, etc.)
- **OU** (organizationalUnit)
  Wertbelegung frei wählbar, muss eine existierende SAP Abteilung oder eine äquivalente Organisationsstruktur eines Partners so präzise wie möglich beschreiben, Abteilungs-mailadresse ist anzugeben falls vorhanden
- **O** (organization)
  Die Organisation welche den Dienst betreibt, also im Normalfall „SAP SE“ bzw. ein Partner Unternehmen
- **C** (country)
  Das Land nach ISO3166-1, Alpha2 (2 Ländercodes), in welchem das Zertifikat ausgestellt wird

Subject Alternate Names (SANs) erfordern, falls angegeben, mindestens eine der folgenden Angaben:

- **rfc822Name**
  Ein Name in der Form einer Internet E-Mail Adresse (Kontaktperson der das Zertifikat Zugeordnet werden kann)

3.1.1.5 Benutzer Zertifikate

Aufgabe dieses Zertifikatstyps ist die Identifizierung und das Authentisieren eines Individuums bzw. einer Gruppe von Individuen. Der Bezug zum Zertifikatsnehmer muss aus dem *Common Name* des *Subjects* und/oder dem *Subject Alternate Name* hervorgehen.

Im ***Subject*** müssen mindestens die folgenden Angaben gemacht werden:

- **CN** (common Name)
  Wert ist frei wählbar, muss den Benutzer oder die Gruppe aber eindeutig identifizieren
- **O** (organization) – nur bei manuellem Antrag
  Die Organisation für die der/die Zertifikatsnehmer tätig sind.
- **C** (country) – nur bei manuellem Antrag
  Das Land nach ISO3166-1, Alpha2 (2 Ländercodes), in dem die Organisation für die der Zertifikatsnehmer tätig ist gemeldet ist.

Subject Alternate Names (SANs) erfordern, falls angegeben, mindestens eine der folgenden Angaben:

- **rfc822Name**
  Ein Name in der Form einer Internet E-Mail Adresse
- **x400Address**
  Ein Name in der Form einer x.400 Adresse
- **otherName**
  Nach Bedarf ein Name einer anderen Form, welche durch die Applikation benötigt wird.

3.1.2 Aussagekraft von Namen

Ein Zertifikat muss mittels des *Subject* und/oder des SAN eindeutig und nachvollziehbar einer Organisation und der zugehörigen Person bzw. dem zugehörigen Dienst zuzuordnen sein. Darüber hinaus sind Namen so zu wählen, dass sie allgemein verständlich und aussagekräftig sind.

3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsinhaber

Zertifikatsnehmer dürfen nicht anonym sein. Pseudonyme und Aliase sind hingegen so lange möglich, wie diese einmalig im Namensraum der SAP sind und die Zusammenführung zu einem administrativen Kontakt während des Antrags möglich ist und dokumentiert wird.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Grundsätzlich sind standardisierte Namensformen wie z.B. X.500 *Distinguished Names* vorzuziehen. In Ausnahmenfällen, wo dies nicht möglich ist, können auch proprietäre Namensformen genutzt werden, diese müssen jedoch ausreichend dokumentiert sein.

Eingesetzte Formate oder Verweise zu den Dokumentationen sind im CPS an dieser Stelle aufzuführen.

3.1.5 Eindeutigkeit von Namen

Namen im *Subject* und/oder *Subject Alternate Name* müssen im SAP Namensraum oder dem des Partners einzigartig sein. Zertifikate mit demselben Namen sind möglich so lange sie demselben Zertifikatsnehmer zugeordnet sind und sich in ihrer Seriennummer unterscheiden.

3.1.6 Anerkennung, Authentifizierung und Funktion von Warenzeichen

Die bewusste Nutzung von rechtlich geschützten Namen ist nicht gestattet. Eine explizite Prüfung der Namen eines Antrags von Seiten des CA Betreibers muss nicht stattfinden. Es liegt in der Verantwortung des Antragstellers zu überprüfen, dass keine Namensrechte Dritter verletzt werden.

Aus fälschlicherweise verwendeten Namen lassen sich keine Schadensersatzansprüche an den Betreiber der Zertifizierungsstelle ableiten.

3.2 Identitätsüberprüfung bei Neuantrag

3.2.1 Nachweis des Besitzes des privaten Schlüssels

Ein Antragsteller muss durch eine geeignete Methode nachweisen, dass er sich im Besitz des zugehörigen privaten Schlüssels befindet, woraus sich weitere Verantwortungen zu dessen Schutz ableiten (siehe 9.6.3). Zertifikatsanträge mittels PKCS#10 (RFC 2986) oder CMC (RFC 5272) erfüllen diese Anforderung.

3.2.2 Authentifizierung einer Organisation

Agiert ein Antragsteller im Namen einer Organisation, also eines Partners, dann muss diese Zugehörigkeit mittels geeigneter Mechanismen nachgewiesen werden. In automatisierten Prozessen kann dies z.B. durch eine bestimmte Gruppenzugehörigkeit erfolgen. Die Vorgehensweise ist durch IT Security freizugeben:

3.2.3 Authentifizierung natürlicher Personen

SAP CAs mit Basisschutzbedarf kennzeichnen sich u.a. dadurch aus, dass die Authentisierung nicht direkt durch die CA vorgenommen wird, sondern auf bereits vorhandenen Mechanismen beruhen kann. Dies sind bspw. ein Benutzername und Passwort wie sie auch bei der Anmeldung an einem Rechner genutzt werden oder ein Prozess ähnlich einem E-Mail Handshake, bei dem der Zugang zu einer Mailbox als ausreichende Identifizierung gelten kann.

Die Authentifizierung von Personen kann in unterschiedlichen Szenarien erforderlich werden. In allen Fällen gilt, dass sich der Antragssteller mittels eines geeigneten Mechanismus nachweisbar identifizieren muss und dieser im CPS zu beschreiben ist.

Ausnahmeregelungen sind möglich erfordern aber die Bestätigung durch IT Security.

3.2.4 Nicht überprüfte Teilnehmerangaben

Bei der Überprüfung von Teilnehmerangaben müssen zwei Fälle unterschieden werden:

1.) Die **Angaben** für das Zertifikat stammen **vom Antragsteller** selbst
In diesem Fall werden nur die unter 3.1.1 genannten Felder überprüft. Zusätzlich Angaben sowohl im *Subject*, SAN oder anderen Zertifikatserweiterungen werden ungeprüft in das Zertifikat übernommen, sofern für die SUB CA und den speziellen Zertifikatstyp keine weiteren Policies definiert sind.

2.) Die Zertifikate werden mit Angaben aus einem Verzeichnis **automatisch** erzeugt
In diesem Fall dürfen keine ungeprüften Quellen für die Angaben im Zertifikat genutzt werden. Es muss sichergestellt werden, dass bei der Aufnahme der Datensätze in das Verzeichnis diese korrekt sind.

3.2.5 Überprüfung der Berechtigung

Abhängig davon, ob ein Antrag für den Antragsteller selbst gilt oder im Auftrag einer anderen Entität ausgeführt wird gelten unterschiedliche Bestimmungen zur Berechtigung des Vorgangs:

Selbstantrag

Die Überprüfung einer Gruppenmitgliedschaft eines offiziellen SAP Verzeichnisses oder einem ähnlichen System eins Partnerunternehmens wird als ausreichend Berechtigungsprüfung angesehen.

Antrag für eine andere Person

Eine Ausstellung eines Zertifikats geht immer an den Inhaber des privaten Schlüssels, dessen Besitz wie unter 3.2.1 nachgewiesen wurde.

Antrag für einen Dienst bzw. eine Maschine

Der Antragsteller muss die Genehmigung eines administrativen Kontakts für den Dienst bzw. die Maschine (Service Owner, Projektleitung, etc.) vorweisen können. Es sind gruppenbasierte oder Workflow-basierte Ansätze möglich.

Zertifikate dürfen nur für Geräte, welche über einem SAP Asset Management Eintrag oder eine ähnliche ID eines Partnerunternehmens verfügen ausgestellt werden oder, im Falle einer Leihstellung, muss eine offizielle Genehmigung durch den Projektverantwortlichen vorliegen.

3.2.6 Kriterien für Zusammenarbeit

Eine Zusammenarbeit mit externen PKIs (z.B. eine Cross-Zertifizierung) erfordert eine gründliche Revision dieser Richtlinie und ist zum derzeitigen Zeitpunkt nicht vorgesehen.

3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung

3.3.1 Routinemäßige Zertifikatserneuerung

Eine routinemäßige Erneuerung eines Zertifikats, d.h. bei noch vorhandenem gültigem Zertifikat kann einerseits klassisch, also wie bei einem Neuantrag erfolgen oder durch eine Signatur des existierenden noch gültigen Zertifikats geschehen. In letzteren Fall können die Inhalte für das Zertifikat aus dem Vorhandenen übernommen werden. Stammen die Angaben aus der Anfrage aber nicht aus dem Zertifikat selbst, dann ist dies nicht möglich.

3.3.2 Zertifikatserneuerung nach einer Sperrung

Der Vorgang bei einer Zertifikatserneuerung bei vorausgegangener Sperrung des vorherigen Zertifikats entspricht einem Neuantrag. Dabei dürfen Schlüssel nicht wiederverwendet, sondern es müssen Neue generiert werden

3.4 Identifizierung und Authentifizierung von Sperranträgen

Um unnötige Verzögerungen bei der Deaktivierung kompromittierter Identitäten zu verhindern kann jeder SAP Mitarbeiter oder Partner temporäre Sperrungen beantragen, welche nur minimale Anforderungen an die Identifizierung des Sperrantragstellers stellen. Dies kann z.B. das Wissen einer Telefonnummer, E-Mailadresse oder einem ähnlichen persönlichen Datum sein.

Einer temporären Sperrung folgt immer ein Prozess welcher die endgültige Sperrung oder deren Rücknahme zum Ziel hat. Dieser Prozess muss zeitnah der temporären Sperrung folgen und beinhaltet eine erweiterte Überprüfung der Identität das Antragstellers und der Rechtmäßigkeit des Antrags.

Serverzertifikate können nicht vorübergehend gesperrt werden sondern müssen immer den vollständigen Sperrprozess durchlaufen.

Für eine schnelle vorübergehenden Sperrung sind folgenden oder gleichwertige Authentifizierungen möglich:

- Details aus dem Adressbuch bekannt
- Sperrantrag mit Zertifikat signiert
- Digitale Signatur einer *Registration Authority (RA)*

Die erweiterte Authentifizierung muss immer ein nachweisbar dokumentierter Prozess sein, bei dem das Einverständnis des Zertifikatinhabers oder eines dessen Vorgesetzten oder des Service Owners bzw. des Projektverantwortlichen vorliegt.

4 ABLAUFORGANISATION (CERTIFICATE LIFE-CYCLE)

4.1 Zertifikatsantrag

4.1.1 Wer kann ein Zertifikat beantragen

Zertifikate können durch Systeme oder Benutzer beantragt werden, die den Definitionen gemäß Kapitel 1.6.2 entsprechen. Zusätzlich können Registrierungsstellen (RA) diese Funktion wahrnehmen, wenn sie eine Überprüfung gemäß diesen Definitionen sicherstellen.

4.1.2 Verfahren und Verantwortungen

Grundsätzlich sind zwei Verfahren für einen Zertifikatsantrag möglich: ein automatisierter ereignisgesteuerter Prozess, der ohne Benutzerinteraktion abläuft und ein manueller Ablauf, bei dem ein Endteilnehmer (vgl. 4.1.1) Schlüssel und Antrag generiert und diesen online oder offline bei der CA bzw. einer RA einreicht.

Bei diesen Verfahren können drei Rollen unterschieden werden, die nicht unbedingt von unterschiedlichen Parteien ausgefüllt werden müssen:

- **CA Betreiber**
  Die Betreiber der CA müssen geeignete Schnittstellen zur Verfügung stellen, so dass beide Verfahren (automatisiert und manuell) unterstützt werden. Auch muss die Möglichkeit einer externen RA gegeben sein. Zusätzlich muss eine Kontaktmöglichkeit für etwaige Nachfragen vorhanden sein.
- **Antragsteller**
  Diese Rolle beschreibt denjenigen, der den Antrag nach erfolgreicher Überprüfung und Authentisierung des Zertifikatsnehmers bei der CA einreicht. Dies kann der Zertifikatsnehmer selbst oder eine Registrierungsstelle (RA) sein. Eine RA muss die nötigen Schnittstellen bereitstellen, so dass Anträge entgegen und an die CA übermittelt werden können.
  Auch hier muss eine Kontaktmöglichkeit bestehen.
- **Zertifikatsnehmer**
  Der Besitzer eines privaten Schlüssels ist der Nehmer des zugehörigen Zertifikats. Der Bedarf dieser Rolle löst den Prozess eines Zertifikatsantrags aus. Die Verantwortungen dazu beschreibt das *Subscriber Party Agreement* in Kapitel 9.6.3, diese sind vornehmlich:
  - Wahrheitsgemäße Angaben
  - Schlüsselgenerierung
  - Nachweis des Besitzes des privaten Schlüssels nach 3.2.1

4.2 Bearbeitung von Zertifikatsanträgen

Nach der Übermittlung eines Zertifikatsantrags an die CA/RA müssen eine Autorisationsprüfung und Verifizierung der Angaben vorgenommen werden. Dies kann durch ein automatisiertes Verfahren oder manuell durch eine Person erfolgen.

Alle Anfragen sind in einer geeigneten Datenbank für eine im CPS zu definierenden Zeitraum aufzubewahren.

4.2.1 Durchführung von Identifikation und Authentifizierung

Abhängig davon, ob ein Antrag durch den Zertifikatsnehmer selbst oder durch einen Dritten erfolgt unterscheiden sich die Anforderungen an die Authentisierung. In allen Fällen muss der Antragsteller durch einen geeigneten Mechanismus nachvollziehbar identifiziert sein. Dies kann z.B. durch vorhandene Methoden wie Benutzername/Passwort, eine Client-Zertifikat, E-Mail Handshake oder einen Workflow Prozess mit ähnlichen Merkmalen geschehen.

Wird der Antrag im Namen eines Endteilnehmers eingereicht, so muss dieser den Vorgang zusätzlich autorisieren und bestätigen, dass er (Person) oder der Zertifikatsnehmer (Service/Maschine) den privaten Schlüssel zum Zertifikat besitzt. Dieser Vorgang muss nachvollziehbar umgesetzt sein (z.B. Workflow im Ticketsystem).

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Grundsätzlich ist im CPS die Voraussetzung für eine Autorisierung zum Erlangen eines Zertifikats zu definieren und im Betrieb umzusetzen. Entspricht der Antrag zusätzlich den Richtlinien in diesem Dokument und wurden die offiziellen Schnittstellen für den Antrag genutzt, so kann das Zertifikat durch die CA ausgestellt werden.

In allen anderen Fällen und insbesondere auch, wenn der Antragsteller auf Nachfragen nicht reagiert, ist ein Antrag abzulehnen. Dies muss in einer informellen Nachricht an den angegeben Kontakt (falls angegeben) übermittelt werden und kann auch kommentarlos geschehen, falls das System dies nicht unterstützt.

4.2.3 Bearbeitungsdauer bei Zertifikatsanträgen

Die Dauer der Bearbeitung eines Zertifikatantrags bis zu dessen Annahme bzw. Ablehnung ist angemessen zu wählen und im CPS Dokument an dieser Stelle anzugeben.

4.3 Zertifikatsausstellung

Ein automatischer Prozess wie bspw. Microsofts Auto-Enrollment, d.h. die Ausstellung und Zustellung des Zertifikats ohne weitere Prüfung durch eine Person, unterliegt strengeren Anforderungen als die manuelle ausgeführte Ausstellung.

Damit ein Zertifikat ohne Zutun einer Person direkt ausgestellt werden kann müssen folgende Punkte gewährleistet sein:

- Die Werte der Zertifikatsattribute dürfen nicht aus dem Zertifikatsantrag ausgelesen werden sondern müssen von einer dritten unabhängigen und geprüften Instanz (Repository wie bspw. AD, LDAP, DB, etc.) bezogen werden.
- Zertifikate können im Falle einer Anfrage ohne vorgelagerte RA nur für Anfragende selbst und nicht on-behalf ausgestellt werden
- Im Falle einer RA, die immer on-behalf Anfragen stellt, muss die Validierung durch den Zertifikatsnehmer oder dessen Verantwortlichen auf der RA nachprüfbar sichergestellt sein.

Eine manuelle Ausstellung, d.h. mit Angaben für die Zertifikatsattribute innerhalb des Antrags, ist prinzipiell immer auf „Pending“ zu setzen und erfordert die Einbeziehung einer autorisierten Person. Nach erfolgreicher Prüfung kann das Zertifikat mit den zur Verfügung stehenden Mitteln ausgestellt werden (bspw. Microsoft CA Management Console)

4.3.1 Aufgaben der Zertifizierungsstelle

Eine CA muss alle mit der Ausstellung eines Zertifikats zusammenhängende Aufgaben ausführen können. Insbesondere sind das:

- Das Erstellen und Signieren des Zertifikats
- Die Bereitstellung einer Abrufmöglichkeit bzw. Zustellungsmöglichkeit für das Zertifikat
- Alle im Zusammenhang mit der Ausstellung entstandenen Daten und das Zertifikat selbst sind, für eine im CPS zu definierende Zeitspanne, zu archivieren

4.3.2 Benachrichtigung des Antragstellers

Der Zertifikatsnehmer oder der zu dem Antrag angegebene administrative Kontakt sind über die erfolgreiche Ausstellung des Zertifikats zu informieren. In einem automatisierten Szenario ist die Zustellung des Zertifikats eine ausreichende Benachrichtigung.

4.4 Zertifikatsakzeptanz

4.4.1 Annahme des Zertifikats

Der Zertifikatsnehmer oder der zugehörige administrative Kontakt sind verpflichtet nach Erhalt des Zertifikats dieses auf Korrektheit zu überprüfen und im Falle von Fehlern dies umgehend sperren zu lassen (siehe 4.9)

Sind Format und Angaben des Zertifikats in Ordnung gilt das Zertifikat als abgenommen.

Bei automatisierten Vorgängen gilt ein Zertifikat nach erfolgreicher Zustellung als akzeptiert.

4.4.2 Veröffentlichung des Zertifikats durch die Zertifizierungsstelle

Die Zertifikate der PKI selbst, also der einzelne CAs, welche für die komplette Zusammenstellung der Vertrauenskette notwendig sind, müssen mind. über die im Zertifikat angegebenen Stellen, falls vorhanden, publiziert werden.

Darüber hinaus ist es notwendig, dass das Root-Zertifikat der PKI auf allen beteiligten Systemen, welche eine Zertifikatsprüfung vornehmen, als vertrauenswürdiges Wurzelzertifizierungsstellenzertifikat verfügbar ist, so dass eine Vertrauensstellung ohne Zutun des Benutzers ermöglicht wird.

Endteilnehmerzertifikate können gemäß der technischen Anforderungen der Applikation in zentralen Verzeichnissen veröffentlicht werden.

4.4.3 Benachrichtigung weiterer Instanzen durch die Zertifizierungsstelle

Keine Bestimmung.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

4.5.1 Nutzung durch den Zertifikatsinhaber

Die Nutzung des Zertifikats und der zugehörigen kryptographischen Schlüssel unterliegt dem *Subscriber Party Agreement*¸ wie es unter 9.6.3 definiert ist. Eine anderweitige Nutzung ist untersagt.

4.5.2 Nutzung des Zertifikats durch die Relying Party

Zertifikate dieses CA-Typs dienen der Authentisierung von Diensten, Systemen und Benutzern durch Zertifikatsprüfer, welche einer Nutzung, wie sie im *Relying Party Agreement* (siehe 9.6.4) vereinbart ist implizit zustimmen.

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

Eine Zertifikatserneuerung verlängert nur die Laufzeit eines Zertifikats, ohne dass dabei Änderungen an den kryptographischen Schlüsseln noch an anderen Angaben im Zertifikat vorgenommen werden. Ein solches Vorgehen ist nur möglich, wenn das vorhandene Zertifikat noch gültig und nicht gesperrt ist. Andernfalls muss ein Neuantrag gemäß 4.1 gestellt werden.

Diese Form der Zertifikatsverlängerung ist nur für durch spezielle Hardware (HSM, Smart Card, TPM, etc.) geschützte Zertifikate zulässig. Die eingesetzte Hardware darf dabei nicht kompromittiert sein.

4.6.1 Gründe für eine Zertifikatserneuerung

Gründe für einen Zertifikatserneuerung können der bevorstehende normale Ablauf der Gültigkeit des Zertifikats oder eine vorzeitige Verlängerung aufgrund unzureichender Laufzeiten des Zertifikats sein.

4.6.2 Wer kann eine Zertifikatserneuerung beantragen

Zertifikatserneuerungen sind durch dieselben Instanzen möglich, die 4.1.1 beschreibt,

4.6.3 Ablauf der Zertifikatserneuerung

Der Vorgang entspricht einem Zertifikatsantrag wie in den Kapiteln 4.1, 4.2 und 4.3.

Die Überprüfung der Angaben für das Zertifikat kann ausfallen, wenn ein noch gültiges Zertifikat den Antrag signiert. In diesem Fall müssen die Werte aus dem vorhanden Zertifikat komplett übernommen und dürfen nicht verändert werden.

4.6.4 Benachrichtigung des Zertifikatsinhabers nach Zertifikatserneuerung

Siehe 4.4.3

4.6.5 Annahme einer Zertifikatserneuerung

Siehe 4.4.1

4.6.6 Veröffentlichung einer Zertifikatserneuerung durch die Zertifizierungsstelle

Siehe 4.4.2

4.6.7 Benachrichtigung weiterer Instanzen durch die Zertifizierungsstelle

Keine Bestimmung.

4.7 Schlüssel- und Zertifikatserneuerung (Re-key)

Bei einer Zertifikatserneuerung mittels „*Re-Key*“ ändern sich nur die Gültigkeit und die zugehörigen kryptographischen Schlüssel eines Zertifikats, unter Beibehaltung der Hash- und Signaturalgorithmen, also des *Cryptographic Service Providers* (CSP). Änderungen die darüber hinausgehen sind in Kapitel 4.8 beschrieben.

Gelten die im CSP genutzten Algorithmen für die Dauer der Nutzung des Zertifikats als ausreichend sicher, so ist ein „*Re-Key*“ zulässig, ansonsten muss ein komplett neues Zertifikat ausgestellt werden (siehe 4.1). Auch muss das zu erneuernde Zertifikat noch gültig und darf nicht gesperrt sein. Andernfalls ist auch hier ein komplett neuer Antrag notwendig.

4.7.1 Gründe für eine Schlüssel- und Zertifikatserneuerung

Neben denselben Gründen, die für eine Zertifikatserneuerung ohne „*Re-Key“* (4.6.1) sprechen kommen in diesem Fall noch zu erwartende Probleme mit der gewählten Schlüssellänge hinzu. Gilt ein Algorithmus mit der ursprünglichen Schlüssellänge als absehbar nicht mehr sicher und kann eine Erhöhung der Schlüssellänge das Problem beheben, so ist eine Erneuerung des Zertifikates mit „*Re-Key*“ sinnvoll.

4.7.2 Wer kann eine Schlüssel- und Zertifikatserneuerung beantragen

Siehe 4.1.1

4.7.3 Ablauf der Schlüssel- und Zertifikatserneuerung

Der Vorgang entspricht einem Zertifikatsantrag wie in den Kapiteln 4.1, 4.2 und 4.3.

Die Überprüfung der Angaben für das Zertifikat kann entfallen, wenn ein noch gültiges Zertifikat den Antrag signiert. In diesem Fall müssen die Werte aus dem vorhanden Zertifikat komplett übernommen und dürfen nicht verändert werden.

4.7.4 Benachrichtigung des Zertifikatsinhabers

Siehe 4.4.3

4.7.5 Annahme der Schlüssel- und Zertifikatserneuerung

Siehe 4.4.1

4.7.6 Veröffentlichung einer Zertifikatserneuerung durch die Zertifizierungsstelle

Siehe 4.4.2

4.7.7 Benachrichtigung weiterer Instanzen durch die Zertifizierungsstelle

Keine Bestimmung.

4.8 Zertifikatsmodifizierung

Sind Änderungen der Angaben eines Zertifikats z.B. durch einen Namenswechsel nach einer Heirat notwendig, so kann dies durch mit vorhandenem oder neuem Schlüsselpaar geschehen. Wird ein neuer Schlüssel benötigt, so entspricht dies einem Neuantrag (4.1).Im Weiteren werden nur Modifikationen mit selben Schlüssel betrachtet.

Für eine Zertifikatsmodifikation ist es notwendig, dass das vorhandene Zertifikat noch gültig und nicht gesperrt ist. Zusätzlich ist es erforderlich, dass der private Schlüssel durch Hardware (HSM, Smart Card, TPM, etc.) geschützt wird und nicht kompromittiert ist. Ist dies nicht der Fall, so muss ein Neuantrag gestellt werden.

Änderungen an den zugrundeliegenden kryptographischen Algorithmen erfordern einen Neuantrag () oder eine Erneuerung mittels „*Re-Key*“ (4.7). Dies kann nicht durch eine Zertifikatsmodifizierung erreicht werden.

4.8.1 Gründe für eine Zertifikatsmodifizierung

Eine Zertifikatsmodifizierung unter beibehält der kryptographischen Schlüssel wird dann nötig, wenn Änderungen im *Subject* oder SAN notwendig werden. Dies kann z.B. nach einer Heirat oder einer Umstrukturierung der Organisation der Fall sein.

4.8.2 Wer kann eine Zertifikatsmodifizierung beantragen

Siehe 4.1.1

4.8.3 Ablauf der Zertifikatsmodifizierung

Der Vorgang entspricht einem Zertifikatsantrag wie in den Kapiteln 4.1, 4.2 und 4.3. Eine Umgehung der Validierungen der Angaben für das Zertifikat kann nicht durch die Signatur mittels des vorhandenen gültigen Schlüssels erreicht werden.

4.8.4 Benachrichtigung des Zertifikatsinhabers

Siehe 4.4.3

4.8.5 Annahme der Zertifikatsmodifizierung

Siehe 4.4.1

4.8.6 Veröffentlichung einer Zertifikatsmodifizierung durch die Zertifizierungsstelle

Siehe 4.4.2

4.8.7 Benachrichtigung weiterer Instanzen durch die Zertifizierungsstelle

Keine Bestimmung.

4.9 Widerruf / Sperrung und Suspendierung von Zertifikaten

4.9.1 Gründe für Widerruf / Sperrung

Gründe die eine Sperrung eines Zertifikats erfordern sind u.a.:

- Verdacht auf Kompromittierung des privaten Schlüssels
- Verdacht auf Kompromittierung einer CA der Vertrauenskette
- Neuinstallation von Systemen
- Ersetzen eines gültigen Zertifikats durch ein Neues
- Betriebseinstellung des nutzenden Systems
- Deaktivieren eines Benutzer- oder Maschinenkontos

- Verlust eines Systems oder Schlüssels

4.9.2 Wer kann Widerruf / Sperrung beantragen

Grundsätzlich kann ein Benutzer immer die Sperrung für das eigene Zertifikat oder das Zertifikat eines ihm zugewiesenen Geräts oder Dienstes (administrativer Kontakt, Service Owner, Projektleiter, etc.) beantragen.

Darüber hinaus können direkte Vorgesetzte oder deren Vorgesetzte einen Widerruf im Namen des Endteilnehmers beantragen. In Ausnahmefällen, die besondere Relevanz für die Sicherheit beteiligter Personen und Unternehmen haben, kann der zuständige *Security Officer* eine Sperrung verlangen.

Auch ein HR Prozess Prozess (Person verlässt das Unternehmen, *Instant Dismissal*, etc.) kann zu einem berechtigten Widerruf eines Zertifikats führen.

4.9.3 Ablauf von Widerruf / Sperrung

Der Betreiber einer SAP Basisschutz CA muss eine Möglichkeit schaffen Sperranträge rund um die Uhr (24/7) anzunehmen und zu bearbeiten. Dies kann auch über einen „Self-Service“ bewerkstelligt werden, welcher die nötigen Prüfungen automatisiert vornimmt (vgl. 3.4.) und eine ausreichend sichere Schnittstelle bietet (digital Signatur des Sperrantrags, etc.).

Sperranträge müssen zumindest über die folgenden Schnittstellen unterstützt werden:

- Anruf oder Email an das SAP Helpdesk
- Eine zusätzliche schriftliche Form wie z.B. das IT Helpdesk Webportal

4.9.4 Fristen für den Zertifikatsinhaber

Bei einem Verdacht auf Kompromittierung eines Zertifikates muss der Inhaber schnellstmöglich den PKI Betreiber informieren und die Sperrung des Zertifikates beantragen.

4.9.5 Bearbeitungsfristen für die Zertifizierungsstelle

Eine Anfrage zum Zurückziehen/Widerruf eines Zertifikates hat zunächst höchste Bearbeitungspriorität gemäß SAP internen Standard-SLAs für das *Incident management*.

Bearbeitungszeiten werden im CPS definiert und können sich nach der Kritikalität des Zertifikats richten, also nach der Zertifikatsklasse.

4.9.6 Anforderung zu Sperrprüfungen durch eine Relying Party

Prüfer von Zertifikaten einer SAP Basisschutz PKI müssen in der Lage sein die gesamte Vertrauenskette inklusive Sperrinformationen zu den einzelnen Zertifikaten zu überprüfen.

SAP Basisschutz PKIs bieten sowohl CRLs als auch OCSP Dienste für diesen Zweck an, wobei die OCSP Dienste immer zu bevorzugen sind und nur, falls OCSP durch die Applikation nicht unterstützt wird, kann auf CRLs ausgewichen werden.

Ist eine Sperrlistenprüfung durch die Applikation nicht vorgesehen, so darf die prüfende Instanz nicht von einer validen SAP Authentisieren ausgehen..

4.9.7 Häufigkeit der Sperrlistenveröffentlichung

Sperrlisten einer offline Root-CA können wesentlich längere Laufzeiten als due ausgebender CAs haben:

Veröffentlichungsintervall	Maximal sechs Monate
Überschneidungszeitraum	Maximal zwei Monate
Lebens	Maximal acht Monate (Veröffentlichungsintervall + Überschneidungszeitraum)

Sperrlisten von ausgebenden online CA müssen wesentlich häufiger veröffentlicht werden:

Veröffentlichungsintervall	Maximal sieben Tage
Überschneidungszeitraum	Maximal vier Tage
Lebens	Maximal elf Tage (Veröffentlichungsintervall + Überschneidungszeitraum)

CRL Einträge, welche außerhalb der Gültigkeit des Zertifikats liegen können gelöscht werden.

4.9.8 Maximale Latenzzeit für Sperrlisten

Generell sind die definierten Veröffentlichungszeiträume möglichst einzuhalten und die CRL schnellstmöglich in die Verzeichnisse zu überführen. Zu jeder Zeit muss gewährleistet sein, dass in den Verzeichnissen immer eine gültige CRL vorhanden ist.

4.9.9 Verfügbarkeit von Online-Statusabfragen

Die online Verfügbarkeit von Sperrlisten bzw. des OCSP Services muss auf 7x24 ausgelegt sein um jederzeit Statusanfragen bedienen zu können.

4.9.10 Anforderungen an Online-Statusabfragen

Alle PKI Teilnehmer, Zertifikatsnehmer und –prüfer müssen in der Lage sein eine der zur Verfügung stehenden Sperrlisten-Methoden (Sperrlisten bzw. OCSP Abfragen) auszuwerten.

4.9.11 Andere verfügbare Formen der Widerrufsbekanntmachung

Keine Bestimmung.

4.9.12 Anforderungen bei Kompromittierung von privaten Schlüsseln

Keine Bestimmung da bereits ausreichend durch vorhanden Prozesse und Regelungen abgedeckt.

4.9.13 Gründe für eine Suspendierung

Ein Zertifikat wird suspendiert, wenn ein Zertifikatssperrantrag nicht ausreichend sicher geprüft werden kann (vgl. 3.4) aber die Situation es gebietet zeitnah ein Zertifikat ungültig zu machen. Eine Suspendierung lässt sich nachträglich wieder rückgängig machen, so dass die Konsequenzen einer fälschlichen Sperrung sich in Grenzen halten.

4.9.14 Wer kann Suspendierung beantragen

Siehe 4.1.1

4.9.15 Ablauf einer Suspendierung

Siehe 4.9.3

Es ist erforderlich, dass schnellstmöglich die erweiterte Überprüfung des Sperrantrags und ggf. eine Untersuchung der Gründe für die Sperrung stattfinden, damit die Suspendierung in eine endgültige Sperrung oder eine Reaktivierung überführt werden kann.

4.9.16 Maximale Sperrdauer bei Suspendierung

Eine Suspendierung eines Zertifikats darf ein Jahr oder die Laufzeit eines Zertifikats nicht überschreiten. Nach Ablauf der maximalen Suspendierungszeit, ohne endgültige Klärung des Sachverhalts, muss das Zertifikat endgültig gesperrt werden.

4.10 Dienst zur Statusabfrage von Zertifikaten (OCSP)

Zusätzlich zur Veröffentlichung der Sperrlisten muss ein *Online Certificate Status* Dienst angeboten werden.

4.10.1 Betriebsbedingte Eigenschaften

Der OCSP Dienst ist generell bei der Abfrage von Sperrinformationen gegenüber einfacher CRL Prüfung zu bevorzugen, da diese Informationen über OCSP sehr zeitnah veröffentlicht werden können und daher die aktuelleren Statusinformationen bieten.

4.10.2 Verfügbarkeit des Dienstes

Siehe 4.9.9.

4.10.3 Weitere Merkmale

OCSP Informationen werden mit OCSP Zertifikaten signiert, d.h. es ist empfohlen den privaten Schlüssel der OCSP Instanz mit Hardware-Methoden zu schützen (HSM/TPM/ Smartcard).

4.11 Beendigung des Vertragsverhältnisses

Wenn das Zertifikat vor Ablauf der Gültigkeit nicht mehr genutzt wird, muss der Inhaber die Sperrung beantragen

Wenn die PKI oder CA vor Ablauf der Lebensdauer aus wirtschaftlichen oder sicherheitsrelevanten Gründen deaktiviert oder abgebaut werden muss, können alle noch gültigen ausgestellten Zertifikate widerrufen werden.

Einzelne Zertifikate können vom PKI Betreiber auch aus Sicherheitsrelevanten Gründen widerrufen werden.

4.12 Schlüsselhinterlegung und –wiederherstellung (Key Escrow und Recovery)

Keine Bestimmung.

4.13 Richtlinien und Praktiken zur Schlüsselhinterlegung und –wiederherstellung

Keine Bestimmung.

4.14 Richtlinien und Praktiken zum Schutz und Wiederherstellung von Sitzungsschlüsseln

Keine Bestimmung.

5 INFRASTRUKTURELLE, ORGANISATORISCHE UND PERSONELLE SICHERHEITSMAßNAHMEN

Das folgende Kapitel beschäftigt sich mit den nicht-technischen Sicherheitsmaßnahmen der SAP PKIs für Anwendungen mit Basisschutzbedarf. Dazu gehören Gebäudesicherheit sowie Verwaltungs- und Betriebskontrollen.

5.1 Infrastrukturelle Sicherheitsmaßnahmen

Der „Trust Anker“ (Root CA & entsprechende HSM & zugehöriger privater Schlüssel) der PKI muss „on Premise“ im SAP eigenen Datacenter betrieben werden.

Siehe auch: http://www.sapdatacenter.com

Issuing CAs der PKI können im SAP datacenter oder bei authorisierten PKI Dienstleistern im Rechenzentrum betrieben werden (sofern diese entsprechende physikalische und infrastrukturelle Sicherheitsmassnahmen umgesetzt haben die dieser Zertifitzierungsrichtlinie entsprechen).

5.1.1 Einsatzort und Bauweise

Alle von SAP betriebenen *Public Key Infrastrukturen* müssen höchsten Sicherheitsanforderungen genügen. Dies gilt auch für die Gebäudesicherheit. Systeme einer PKI können nur in Rechenzentren der Kategorie „*SAP Tier IV Level*“ oder einer vergleichbaren Kategorie betrieben werden (genaue Angaben auf Anfrage). Dies entspricht dem höchsten Sicherheitsniveau, unter dem SAP Rechenzentren betreibt.

Grundsätzlich gilt, dass alle betriebsrelevanten Komponenten redundant ausgelegt sind, auch die Gebäude. Darüber hinaus müssen diese durch SAP selbst oder durch einen von SAP authorisierten PKI Dienstleister betrieben werden.

5.1.2 Räumlicher Zugang

Grundsätzlich gilt, dass der Zugang zu Rechenzentren (RZ), die PKI Komponenten aufnehmen physikalisch so gesichert sein muss, dass nur autorisiertes Personal Zugang zum Gebäude erhält.

Die eigentlichen PKI Komponenten müssen zusätzlich innerhalb des RZ vor physikalischem Zugriff gesichert sein, so dass nur Benutzer in den unter 5.2.1. aufgeführten Rollen Zugang erhalten. Geeignete Maßnahmen können speziell gesicherte Käfige oder Racks sein. Diese dürfen nicht durch dasselbe System wie das Gebäude selbst geschützt werden sondern muss durch ein alternatives Konzept umgesetzt sein (z. Bsp. biometrisches System).

Ausnahmen, um bspw. Herstellern zu Supportzwecken Zutritt zu gewähren, erfordern das ständige Beisein einer berechtigten Person.

5.1.3 Stromversorgung und Klimaanlagen

Alle Komponenten entsprechen der redundanten Ausführungen gemäß „*SAP Tier IV Level“*.

5.1.4 Gefährdung durch Wasser

Die Standorte der SAP Rechenzentren sind so gewählt, dass Risiken durch Überschwemmungen o.ä. minimiert sind.

5.1.5 Brandschutz

Alle Brandschutzmaßnahmen erfolgen gemäß den Ausführungen in „*SAP Tier IV Level“* konform zu geltenden Bestimmungen.

5.1.6 Aufbewahrung von Datenträgern

Datenträger, die Informationen im Zusammenhang mit einer SAP PKI enthalten müssen so gelagert sein, dass dieselben physikalischen und logischen Zutrittskontrollen, wie für die Systeme selbst gewährleistet sind. Zusätzlich müssen die Räume Schutz vor Unfallschäden, wie z.B. durch Feuer, Wasser oder Strahlung, bieten

5.1.7 Entsorgung

Vertrauliche Dokumente und Datenträger, die vertrauliche Informationen enthalten müssen so zerstört werden, dass sie nicht mehr auslesbar und wiederherstellbar sind.

Bei speziellen kryptographischen Geräten, wie *Hardware Security Modulen* (HSM) oder Smartcards, sind die Vorgehensweisen der Hersteller zu befolgen.

Die SAP Entsorgungsrichtlinien sind generell zu befolgen.

5.1.8 Externe Datensicherung

Prinzipiell ist von allen PKI relevanten Komponenten eine regelmäßige Sicherung zu erstellen, so dass der Betrieb nach einem Ausfall bis hin zu allen Komponenten, wieder hergestellt werden kann.

Dabei ist mindestens eine Kopie so räumlich von den Systemen zu trennen, dass gemäß der lokalen Risikolage eine Zerstörung der gesamten Infrastruktur keinen unwiederbringlichen Schaden verursachen kann.

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 Rollenkonzept

Mitarbeiter, die den Betrieb der PKI gewährleisten, insbesondere Personen, die Zugriff und Kontrolle über kryptographische Schlüssel und Operationen haben, tun dies innerhalb einer besonderen und vertrauenswürdigen Rolle. Eine vertrauenswürdige Rolle kennzeichnet sich dadurch, dass falsch ausgeführte und ihr zugeordnete Aufgaben ein Sicherheitsrisiko darstellen. Dabei ist es unwesentlich, ob dies absichtlich, oder versehentlich geschieht.

Die folgenden Rollen sind mindestens durch die PKI Verantwortlichen zu beschreiben:

- PKI Betreiber
- Information Security Officer
- Service Owner und Manager
- Auditoren (Log Review)

5.2.2 Anzahl involvierter Personen pro Aufgabe

Die Mehrheit der Aufgaben im Zusammenhang mit einer Basisschutz PKI der SAP erfordern nicht mehrere Personen für ihre Ausführung. Dies gilt jedoch nicht für Aktionen die direkt die Root-CA oder die sicheren Schlüsselcontainer (HSM) betreffen. In diesen Fällen ist mindestens ein Vieraugen-Prinzip technisch durchzusetzen. Beispiele für solche Aufgaben sind z.B. das Ausstellen einer neuen Root-CRL oder sicherheitskritische Änderungen an den HSM Systemen.

5.2.3 Identifizierung und Authentifizierung jeder Rolle

Im Zuge ihrer bisherigen Tätigkeit bei SAP erlangen Mitarbeiter den erforderlichen Status, welcher sie zu den Tätigkeiten im Zusammenhang mit einer SAP PKI ermächtigen. SAP stellt sicher, dass die relevanten Personen einen vertrauenswürdigen Status genießen.

Ist es nötig im Zuge von Audits o.ä. Personen ohne diesen Status Zugang zu gewähren, so muss dies durch die IT Security Abteilung genehmigt und überwacht werden.

Es ist mittels technischer Schranken sicherzustellen, dass nur Inhaber einer vertrauenswürdigen Rolle Zugang zu den System erhalten.

5.2.4 Rollen, die eine Aufgabentrennung erfordern

SAP PKIs die dem Basisschutzniveau entsprechen erfordern keine Trennung bestimmter Aufgaben. Sollte Schlüsselwiederherstellung auf einer der SUB CAs angeboten werden müssen, dann sind die Rollen mit dieser Berechtigung möglichst von normalen PKI Admin Rollen zu trennen oder es ist ein 4 Augen Prinzip umzusetzen.

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 Anforderungen an Mitarbeiter

Personen, die Aufgaben einer vertrauenswürdigen Rolle wahrnehmen, müssen nachweislich für diese Tätigkeit qualifiziert sein. Darüber hinaus kommen nur interne Mitarbeiter der SAP oder Partner mit bereits seit geraumer Zeit bestehenden Langzeitverträgen in Frage.

Alle Personen müssen eine Erklärung unterschreiben, welche besondere Sorgfalt in Bezug auf den Umgang mit Vertraulichen Daten und die Einhaltung der beschriebene Prozess, sowie der Kenntnisnahme der Zertifikatsrichtlinie verlangt.

5.3.2 Sicherheitsüberprüfung der Mitarbeiter

Alle Mitarbeiter der SAP und Partner werden bei Ihrer Einstellung bzw. Beauftragung einem hohen regional unterschiedlichen Standard bzgl. ihrer Sorgfaltspflicht unterworfen.

Über diese Anforderungen hinaus findet keine weitere Sicherheitsüberprüfung der Mitarbeiter statt.

5.3.3 Anforderungen an Schulungen

Personen mit PKI-bezogenen Tätigkeiten müssen regelmäßig an Fortbildungen teilnehmen und SAP muss die dazu nötigen Mittel zur Verfügung stellen, so dass die anfallenden Aufgaben dauerhaft und zufriedenstellend durch die Mitarbeiter ausgeführt werden können. Insbesondere sind die folgende Qualifikationen zu erbringen:

- IT Security und Datenschutz Basiswissen
- PKI Administration im Allgemeinen und Microsoft PKI Wissen im Speziellen

- HSM Administration (herstellerspezifisch und falls vorhanden)

5.3.4 Häufigkeit und Anforderungen an Fortbildungen

Im Idealfall sind Schulungen zur Auffrischung und Weiterentwicklung der PKI-Themen jährlich durchzuführen. Mindestens muss dies aber so häufig erfolgen, dass der Anschluss an aktuelle Entwicklungen und Anforderungen und das vorhandenen Wissen nicht verloren gehen.

5.3.5 Häufigkeit und Ablauf von Arbeitsplatzwechseln

Eine Untersuchung der bisherigen Arbeitsplätze und der Häufigkeit ihrer Wechsel ist nicht notwendig. Es ist im allgemeinen Betriebsinteresse der PKI, häufige Wechsel der für die PKI zuständigen Mitarbeiter und Partner durch bedachte Auswahl der Personen von vorneherein gering zu halten.

5.3.6 Sanktionen für unerlaubte Handlungen

Handeln einzelne Personen oder Gruppen in ihrer Rolle der SAP PKI Umgebung den Interessen der SAP SE im Allgemeinen oder der PKI Umgebungen im Speziellen zuwider, so erfolgen Maßnahmen gemäß der üblichen SAP Richtlinien. Diese können regional unterschiedlich ausgelegt sein.

Darüber hinaus müssen Personen ihrer PKI-bezogenen Rollen entbunden werden, sollten sie wissentlich und schwerwiegend gegen SAP-Richtlinien verstoßen.

5.3.7 Anforderungen an unabhängige, selbstständige Zulieferer

Für Zulieferer, die Aufgaben im PKI Umfeld wahrnehmen, gelten Im Prinzip die gleichen Anforderungen wie an Mitarbeiter, d.h. sie brauchen jedenfalls eine SAP user ID und alle damit verbundenen Pflichten. Zulieferer die kurzfristig von SAP für Arbeiten an der PKI Infrastruktur beauftragt wurden, müssen von PKI Mitarbeitern und oder IT Security Personal begleitet und überwacht werden.

5.3.8 Dokumentation für das Personal

Alle Personen, die eine SAP PKI Rolle innehaben sind verpflichtet die Zertifikatsrichtlinie ihrer PKI und alle zugehörigen Dokumente (CPS, System Dokumentation, Betriebsleitfaden, etc.) zu lesen. Zusätzlich können weitere Dokumente der Rolle entsprechend erforderlich sein.

5.4 Überwachung / Protokollierung

Im Zusammenhang mit dem Betrieb der PKI fallen Daten an, welche zu überwachen und für die spätere Analyse aufzuheben sind. Hierbei können die folgenden Ursprünge unterschieden werden:

- Ereignisse im Zusammenhang mit betrieblichen Prozessen
- Log-Daten der unterliegenden Systeme (Netzwerk, Betriebssystem, Appliance, etc.)
- Ereignisprotokolle der Applikation (CA, Webserver, HSM, etc.)

Diese Informationen sind an zentraler Stelle zu sammeln und zugänglich zu machen. Dies muss mit angemessenen Methoden und unterstützenden Technologien umgesetzt sein und kann für Prozesse durchaus in handschriftlicher Form erfolgen.

5.4.1 Überwachte Ereignisse

Grundsätzlich sind alle sicherheitsrelevanten Ereignisse, die auf Systemen der PKI erzeugt werden zu protokollieren. Insbesondere aber nicht ausschließlich sind dies die folgenden Informationen:

- An- und Abmeldevorgänge an den Systemen
- Systemlogs gemäß SAP Hardening Richtlinien
- Ereignisse bezüglich Life-Cycle Operationen auf den Zertifikaten der CA selbst und der End-Entitäten. Zum Life-Cycle eines Zertifikats gehören u.a.:
    - Ausstellung und Verlängerung
    - Rückruf und Löschung
    - Sicherung und Archivierung
- Spezielle „Key Ceremony“ der Root-CA
- Sicherung/Wiederherstellung der Systeme und privaten PKI-Schlüssel
- Ereignisse auf kryptografischen Hardware-Modulen
- Betriebsbedingte Änderungen an den Systemen gemäß SAP Change Management Prozessen

- Audit Protokolle und Ergebnisse

Manuell erstellte Protokolle sind durch beteiligte Personen gegenzuzeichnen und in das von IT Security bereitgestellte Aufbewahrungssystem zu überführen.

5.4.2 Häufigkeit der Protokollanalyse

Alle Ereignisse, die sich durch eine Kritikalität von mindestens dem Level „Warnung“ (Klassifizierung gemäß Hersteller) auszeichnen müssen auf allen Systemen der PKI einen Alarm im Monitoring-System auslösen, welcher durch die PKI Administratoren zu kontrollieren und einzuschätzen ist. Somit ist eine permanente ereignisgesteuerte Überwachung der Protokolldaten gewährleistet.

Manuell erstellte Protokolle sind bei der Einstellung in das Aufbewahrungssystem durch IT Security gegenzulesen.

5.4.3 Aufbewahrungsfrist für Protokolldaten

Protokolldateien sind mindestens 1 Jahr aufzubewahren.

5.4.4 Schutz von Protokolldaten

Es ist sicherzustellen, dass Ereignisprotokolle nicht durch unautorisierte Personen manipuliert oder gelöscht werden können. Dies kann durch Log-Systeme geschehen, welche durch vertrauenswürdige Administratoren betrieben werden, welche nicht auch gleichzeitig die PKI betreiben. Kann dies für die Standardmethoden nicht umgesetzt werden, so ist eine Kopie der Protokolldaten in ein weiteres System zu überführen (Forking), welches diesen Vorgaben entspricht.

Für manuell erstellte Protokolle ist durch IT Security an zentraler Stelle ein Aufbewahrungssystem zu schaffen, welches eine sichere Aufbewahrung und einen kontrollierten Zugang zu den Informationen gewährleistet.

Lesenden Zugriff erhalten alle Personen deren betriebsbedingten Aufgaben dies erfordern.

5.4.5 Backup der Protokolldaten

Für Online-System müssen die Ereignisprotokolle so gesichert werden, dass maximal Daten eines Tages verloren gehen können.

Offline-Systeme (Root CA) sind nach einem definierten Prozess zu sichern, mindestens aber vor oder nach jeder Änderung am Offline-System.

5.4.6 Überwachungssystem (intern oder extern)

Das System zur Speicherung und Überwachung der Ereignisse ist extern auszuführen, d.h. vom PKI System komplett unabhängig. Das Sammeln der Informationen kann über einen lokal installierten Agenten oder durch ein geeignetes entferntes Ausleseverfahren geschehen, muss in jedem Fall aber vor Manipulationen gesichert sein.

5.4.7 Benachrichtigung des Ereignisverursachers

Grundsätzlich müssen Ereignisse, die einen Alarm auslösen den Betreibern der PKI immer auf geeignete Weise angezeigt und zugänglich gemacht werden.

In besonders schwerwiegenden Fällen, wie einer Kompromittierung des Systems oder einem Ausfall des Dienstes oder einer Komponente, so dass der Dienst nicht nutzbar ist (z.B. CRL Veröffentlichung ist fehlgeschlagen) muss nach dem SAP IT Emergency Management Prozess verfahren werden.

5.4.8 Schwachstellenanalyse

Die Sicherheit des Systems muss sowohl mit automatischen als auch manuellen Maßnahmen überprüft werden. Dies sind mindestens:

- **Port bzw. Security Scans**: Die über das Netzwerk erreichbaren Dienste müssen durch ein geeignetes Mittel regelmäßig grundsätzlichen Sicherheitstest unterzogen werden. Es empfiehlt sich dies durch Software zu automatisieren.
- **Netzwerk IDS/IPS**: Systeme, welche aus unsicheren Netzwerkzonen wie dem Internet erreichbar sind müssen zusätzlich durch Systeme zur Einbruchserkennung abgesichert werden.
- **Regelmäßige Audits**: In regelmäßigen Abstand sind System und betriebliche Prozesse durch extern oder interne Audits zu überprüfen.

5.5 Archivierung

Im Gegensatz zur Protokollierung, welche auch allgemeine Ereignisse berücksichtigt, geht es bei der Archivierung um die Historie der dienstrelevanten Aktionen im System. Die Archivierung für forensische Analysen ist hier nicht betrachtet.

5.5.1 Archivierte Daten

Die zu archivierenden Daten umfassen alle Informationen rund um den Lebenszyklus der ausgestellten Zertifikate, inkl. der PKI-Zertifikate selbst, und alle handschriftlich festgehaltenen Protokolle (s. 5.4.1). Andere Daten das System betreffend müssen nicht archiviert werden.

Informationen zu den Zertifikaten beinhalten u.a.:

- Das Zertifikat selbst
- Antragsteller
- Zeitpunkt der Anfrage und Ausgabe
- Bei CA-Zertifikaten die letzte ausgestellte komplette CRL

5.5.2 Aufbewahrungsfrist für archivierte Daten

Informationen zum Lebenszyklus der Zertifikate sind für ein Jahr über die Dauer ihrer Gültigkeit hinaus aufzubewahren. Schriftliche Protokolle müssen ein Jahr über die Gültigkeit der PKI hinaus aufgehoben werden. Sind auch Daten betroffen, welche zwischen Diensten geteilte Komponenten betreffen, so ist hier die Lebensdauer der Komponenten selbst plus ein Jahr anzusetzen.

5.5.3 Schutz der Archive

Analog zu 5.4.4

5.5.4 Backup der Archive (Datensicherungskonzept)

Sind die zu archivierenden Daten in ihrer Gesamtheit durch das generelle Sicherungsverfahren für die PKI abgedeckt, so ist eine zusätzliche Sicherung nicht notwendig. Andernfalls muss ein System zu Archivierung denselben Anforderungen genügen.

Besonderes Augenmerk gilt bei der Archivierung möglichen Aufräumprozessen, durch die ungültige Zertifikate aus den produktiven Systemen entfernt werden. Hierbei ist sicherzustellen, dass die Fristen aus 5.5.2 eingehalten werden.

Im Falle einer Einstellung des PKI Betriebs ist die Vorhaltung der Archive im Auflösungsplan (5.8) zu beschreiben.

5.5.5 Anforderungen an Zeitstempel

Ereignisprotokolle, archivierte Datensätze, Zertifikate, CRLs und andere Einträge müssen zuverlässige Zeit- und Datumsinformationen beinhalten. Dazu ist es notwendig, dass alle beteiligten Systeme ihrer Zeit abgleichen bzw. von einer zentralen Instanz beziehen.

Anforderungen an einen kryptographischen Zeitdienst gemäß RFC3161 bestehen nicht.

5.5.6 Archivierungssystem (intern oder extern)

Analog 5.4.6

5.5.7 Prozeduren für Abruf und Überprüfung archivierter Daten

Analog 5.4.4

5.6 Schlüsselwechsel der Zertifizierungsstelle

Ein normales Ablaufen eines Zertifizierungsstellenzertifikats erfordert nicht unbedingt den Wechsel der kryptographischen Schlüssel. In einem solchen Fall kann analog einer Zertifikatserneuerung in Kapitel 4.6 vorgegangen werden.

Sind nur Änderungen am Zertifikat aber nicht an den Schlüsseln erforderlich, so handelt es sich um eine Zertifikatsmodifizierung welche in 4.8 beschrieben ist.

Andere Ursachen, wie z.B. eine Schlüsselkompromittierung, ein Wechsel der kryptographischen Algorithmen, Änderungen der Schlüssellänge, also alle Vorgänge, die die Kryptographie des Zertifikats und der Schlüssel betreffen machen eine Zertifikatserneuerung mittels „*Re-Key*“ notwendig.

Ein solches Vorgehen bei einer Zertifizierungsstelle erfordert eine sog. Schlüsselzeremonie oder *Key Ceremony*. Siehe hierzu Abschnitt 6.1. Grundsätzlich finden die Vorgaben rund um den Lebenszyklus von Zertifikaten aus Kapitel 6.3.2. auch für CA Zertifikate Anwendung.

Spezialfall Cross-Zertifizierung der Root-CA Zertifikate

Bei der Erneuerung eines Root-CA Zertifikates kann es notwendig sein das sich das alte und neue Zertifikat gegenseitig signieren (Cross-Zertifizierung), so dass Zertifikatsprüfer Zertifikate der neuen Root-CA auch dann als gültig akzeptieren,

wenn das neue Root-CA Zertifikat noch nicht den vertrauenswürdigen Wurzelzertifizierungsstellen hinzugefügt wurde. Dies kann bspw. durch langsame Replikationsprozesse der Falls sein.

Ist ein solches Vorgehen vorgesehen, so müssen zu den eigentlichen Root-Zertifikaten auch die jeweiligen Cross-Zertifikate an den relevanten Stellen (4.4.2) veröffentlicht werden.

5.7 Kompromittierung und Wiederherstellung (disaster recovery)

Grundsätzlich gilt es Ausfälle der PKI schnellstmöglich so zu beheben, dass der Dienst wieder in einen geregelten Betrieb überführt werden kann. Dazu müssen alle Maßnahmen ergriffen werden (Cluster, HSM, etc.), die in einem wirtschaftlichen Rahmen sinnvoll sind.

5.7.1 Vorgehen bei Sicherheitsvorfällen und Kompromittierung

Wird ein sicherheitsrelevanter Vorfall im Zusammenhang mit der PKI registriert, so muss dieser an den Kontakt aus Kapitel 1.5.2 eskaliert werden. Danach muss gemäß der definierten SAP Prozesse zum Incident und Emergency Management weiter verfahren werden.

5.7.2 Betriebsmittel, Software und/oder Daten sind korrumpiert

Wann immer ein Verdacht besteht, das System oder Teile davon könnten korrumpiert sein, ist in Absprache mit IT Security für eine offene Außenkommunikation zu sorgen.

Des Weiteren sind der Zeitpunkt und die schwere des Integritätsverlustes festzustellen und abhängig davon zu verfahren:

- Ist der Zeitpunkt bekannt und nur das System, nicht aber der Schlüssel (weil in Hardware) betroffen, so müssen alle seit dem Zeitpunkt des Vorfalls durch die betroffene CA ausgestellten Zertifikate zurückgezogen werden.
- Ist der Zeitpunkt unbekannt und nur das System ohne den Schlüssel betroffen, so müssen alle gültigen Zertifikate der CA zurückgezogen werden.
- Ist auch der Schlüssel betroffen so ist wie in 5.7.3 zu verfahren

Zusätzlich ist das System in einen sauberen Integritätszustand zurückzuversetzen wobei die Ursache des Vorfalls behoben werden muss.

Das gesamte Vorgehen erfolgt gemäß SAP Incident/Problem Management Prozess.

5.7.3 Kompromittierung des privaten Schlüssels

Wann immer ein Verdacht besteht, das System oder Teile davon könnten korrumpiert sein, ist in Absprache mit IT Security für eine offene Außenkommunikation zu sorgen.

Ist bei dem Vorfall ein in Hardware gesicherter Schlüssel betroffen, so muss genau analysiert werden, ob es hierbei um eine Konfigurationsfehler oder eine Sicherheitslücke im Produkt handelt. Gegebenenfalls ist das Produkt zu wechseln.

Ist nur der Schlüssel einer untergeordneten CA betroffen, so müssen alle durch sie ausgestellte und gültige Zertifikate zurückgezogen werden und im Anschluss durch die Root-CA auch das Zertifikat der CA selbst.

Im Falle eines Schlüssels der Root-CA sind alle gültigen End-Entitäten Zertifiakte durch die jeweiligen Sub-CAs und alle Sub-CA Zertifikate durch die Root-CA zurückzuziehen. Anschließend muss die Root-CA auf allen Systemen von Zertifikatsprüfern aus der Liste der vertrauten Wurzelzertifizierungsstellen entfernt werden.

Zusätzlich ist das System in einen sauberen Integritätszustand zurückzuversetzen wobei die Ursache des Vorfalls behoben werden muss. De facto bedeutet dies, dass eine neue PKI aufgebaut werden muss.

Das gesamte Vorgehen erfolgt gemäß SAP Incident/Problem Management Prozess.

5.7.4 Wiederaufnahme des Betriebs nach einem Notfall

Der PKI Betreiber muss einen Notfallplan erstellen, welcher die schnellstmögliche Wiederherstellung des Dienstes ermöglicht. Dieser ist durch den Betreiber regelmäßig zu testen.

Zusätzlich sind alle wirtschaftlich sinnvollen Maßnahmen (Redundanz, HSM, geographische Verteilung, etc.) zu ergreifen, Notfälle möglichst auszuschließen.

Wird eine Region durch eine Naturkatastrophe oder ähnlich schwerwiegendes Ereignis unbenutzbar, so ist mittels eines weltweit verteilten Sicherheitskonzepts der entfernte Wiederaufbau an einem anderen Standort zu ermöglichen. Dies kann analog dem ursprünglichen Systemaufbau erfolgen.

Soweit möglich müssen Katastrophengebiete, die PKI-Komponente bergen, durch Sicherheitspersonal rund um die Uhr abgesichert werden.

5.8 Einstellung des Betriebs

Sollte es nötig werden, dass SAP den Betrieb der PKI einstellt, so sind alle betroffenen Parteien (Inhaber, Prüfer, etc.) ausreichend früh darüber zu informieren, so dass adäquat darauf reagiert werden kann.

Darüber hinaus garantiert SAP die Aufbewahrungsfristen für die PKI-Archive und Protokolle gemäß den Abschnitten 5.4.3 und 5.5.2.

Zu gegebenem Zeitpunkt wird SAP einen Auflösungsplan erstellen, welcher u.a. die folgenden Aspekt berücksichtigt:

- Benachrichtigung der Betroffenen und vertrauender Dritter über die Einstellung des Betriebes
- Beschreibung der weitergeführten Supportleistungen
- Ob und wie die Ausstellung von Zertifikatsrückzugsinformationen fortgeführt werden
- Informationen zum Sperren gültiger CA-Zertifikate
- Regelungen bzgl. einer Nachfolge-CA
- Zerstören der privaten Schlüssel und der kryptographischen Module
- Archivierung der Unterlagen und Protokolle

6 TECHNISCHE SICHERHEITSMAßNAHMEN

6.1 Schlüsselerzeugung und Installation

Im Allgemeinen findet eine Schlüsselerzeugung beim Erstellen einer Zertifikatssignaturanfrage statt und immer dann, wenn ein vorhandenes Zertifikat mittels Re-Key erneuert wird. Dies gilt sowohl für die PKI-Zertifikate selbst (CA, RA, OCSP) als auch die End-Entitäten Zertifikate.

- Es ist zu beachten, dass Schlüssel möglichst nicht unnötig zwischen Systemen (Rechner, SmartCard, HSM, etc.) transportiert werden. Da SAP PKIs des Basis-Schutzbedarfs keine Schlüsselsicherung vornehmen ergibt sich somit für Dienste, welche nach einem Wiederherstellungsprozess neu aufgesetzt werden, automatisch die Anforderung ein neues Zertifikat zu beantragen, obwohl das vorher genutzte Zertifikat noch nicht ungültig geworden ist. In einem solchen Fall ist das alte Zertifikat zu sperren.

6.1.1 Schlüsselerzeugung

Die Schlüsselerzeugung hat durch die Zertifikatsnehmer selbst, bzw. deren Betreiber oder Verantwortlichen zu erfolgen. Zur Erzeugung sind mindestens software-, besser jedoch hardware-basierte kryptographische Module zu verwenden, die mindestens den Anforderungen des FIPS 140-2 Level 1 Standards entsprechen.

Beim Betrieb von PKI-Lösungen sind Hardware Security Module (HSM) des Sicherheitslevels FIPS 140-2 Level 2 zum Schutz der CA-Schlüssel zu verwenden.

Bei der Erstellung eines Root-CA Schlüssels muss dies durch eine Schlüsselzeremonie (Key Ceremony) geschehen, deren Ablauf zu protokollieren und archivieren ist. Die gesamte Prozedur muss sicherstellen, dass die Schlüssel und deren Schutzmaßnahmen zu keinem Zeitpunkt durch einzelne Personen kompromittierbar waren. Das Ergebnis ist von allen beteiligten Personen zu unterzeichnen.

6.1.2 Übermittlung privater Schlüssels an Zertifikatsinhaber

Die Erstellung der Schlüssel für die PKI selbst, also für CA, RA oder OCSP, hat auf den Systemen selbst stattzufinden, so dass sich kein Bedarf für eine Übermittlung der Schlüssel ergibt. Ist dies aus technischer Sicht notwendig (Cluster, etc.) so sind Schutzmechanismen (HSM) zu wählen, welche eine solchen Transport erlauben, ohne dass dabei die Integrität des Schlüssels gefährdet wird. Eine Übermittlung mittels Software basiertem Schutz ist nicht zulässig. PKI Zertifikate sind grundsätzlich als nicht exportierbar zu kennzeichnen.

Für private Schlüssel der End-Entitäten gelten im Prinzip dieselben Regeln. Hier besteht jedoch die Möglichkeit Schlüssel zwischen Systemen mittels durch Software geschützter Prozesse zwischen Systemen zu übertragen. Dabei ist zu gewährleisten, dass Schlüssel auf den Systemen selbst als nicht exportierbar gekennzeichnet werden und die exportierte Variante vor Missbrauch geschützt wird.

6.1.3 Übermittlung öffentlicher Schlüssels an Zertifikatsaussteller

Der entscheidende Aspekt bei der Übertragung des öffentlichen Schlüssels und der Zertifikatsanfrage ist, dass die Identität des Anfragenden fehlerfrei feststeht und bei der Übertragung keine Änderungen der Informationen möglich sind.

Der öffentliche Schlüssel muss in einem standardisierten und von der CA unterstützen Format für Zertifikatsanträge enthalten sein.

6.1.4 Übermittlung öffentlicher CA Schlüssels an Zertifikatsprüfer (Relying Parties)

Die Verteilung der öffentlichen Teile der CA-Schlüssel ist über viele Mechanismen denkbar und muss nicht eingeschränkt werden. Die Zertifikate aller CAs müssen aber mindestens über eine der im *Authority Information Access* (AIA) Feld hinterlegten Lokationen erreichbar sein. Empfohlen ist zusätzlich:

- Alle Zertifikate der Vertrauenskette in die Zertifikate selbst mit aufzunehmen
- Eine automatisiertes Verteilungssystem zumindest für interne Nutzer zu implementieren (z.B. AD Group Policies, Logon Skripte, etc.)

6.1.5 Schlüssellängen

SAP folgt den Empfehlungen des NIST und BSI für Schlüssellängen. Unterscheiden sich die Empfehlungen oder sind Angaben für Verschlüsselung und Signatur nicht gleich, so ist immer die kryptographisch stärkere Variante zu wählen.

Schlüssellängen sind so zu wählen, dass Zertifikate über die gesamte Laufzeit als sicher angenommen werden können, somit sind Zertifikate mit langen Laufzeiten (Root-CA) größer zu wählen als End-Entitäten Zertifikate.

Letztlich bestimmt die SAP Security Policy das genaue Vorgehen und die Angaben sind im CPS zu konkretisieren.

Ausnahmen müssen technisch plausibel begründet, dokumentiert und mit einer Risikoeinschätzung versehen werden.

6.1.6 Erzeugung der Public Key Parameter und Qualitätssicherung

Analog zu den Schlüssellängen gilt, dass aktuelle und durch die genannten Gremien empfohlene Werte und Algorithmen einzusetzen sind. Die Schlüsselersteller müssen dies gewährleisten und somit dafür sorgen, dass die eingesetzten kryptographischen Provider und Tools immer dem neusten Stand entsprechen.

Eine Qualitätssicherung für End-Entitäten Zertifikate seitens der PKI findet nicht statt.

6.1.7 Schlüsselverwendungszwecke (X.509v3 Key Usage)

Bei allen durch die PKI ausgestellten Zertifikaten ist entweder die „Key Usage“ Erweiterung oder die „Extended key Usage“ Erweiterung zu setzen, wobei mindestens eine davon als „kritisch“ zu markieren ist.

Die in diesen Feldern gemachten Angaben müssen die Nutzungsbestimmung des Zertifikats maximal einschränken, so dass keine andere Nutzung des Zertifikats möglich ist. Bei einer CA sind dies:

- keyCertSign
- cRLSign

Darüber hinaus müssen die Angaben konform zu den Vorgaben in Kapitel 1.4 sein.

6.2 Schutz privater Schlüssel und Einsatz kryptographischer Module

SAP schützt kryptographische Schlüssel mittels physikalischer, organisatorischer und verfahrenstechnischer Methoden. Endteilnehmer sind verpflichtet ihre privaten Schlüssel gemäß der SAP Richtlinien vor Verlust, Offenlegung und unberechtigter Nutzung bestmöglich zu schützen. Dies kann und sollte in besonders kritischen Bereichen durch den Einsatz hardwaregestützter kryptographischer Module (TPM, Smart Card, HSM, etc.) erfolgen.

Private Schlüssel von Zertifizierungsstellen sind grundsätzlich durch Hardware Security Module zu schützen.

6.2.1 Standard kryptographischer Module

SAP bezieht sich bei den Anforderungen an kryptographische Module auf die Publikation 140-2 des *Federal Information Processing Standard* (FIPS). Dies gilt sowohl für softwarebasierte (140-2 Level 1) als hardwaregestützte Module (140-2 Level 2 und höher).

Cryptographic Service Providers (CSP) für softwarebasierte Module müssen die Anforderungen von FIPS 140-2 Level 1 erfüllen. Zertifikate einer SAP Basisschutz PKI für Endteilnehmer müssen mindestens diesem Schutzniveau entsprechen.

Eingesetzte Hardwaremodule müssen mindestens FIPS 140-2 Level 2 oder höher entsprechen. Private Schlüssel von Zertifizierungsstellen sind immer durch Systeme dieser Kategorie zu schützen.

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

Eine Aufteilung des privaten Schlüssels auf mehrere Personen, so dass dieser nicht durch eine Einzelne zum Einsatz gebracht werden kann ist für Endteilnehmer und ausstellende untergeordnete CAs nicht erforderlich.

Die privaten Schlüssel von Root-CAs sind auf mindestens zwei Personen aus unterschiedlichen Abteilungen zu verteilen, so dass ein Vieraugenprinzip gewährleistet ist. Dies muss durch technische Maßnahmen (Smart Cards, geteilte Passwörter, etc.) umgesetzt sein.

Aus Gründen der Praktikabilität wird empfohlen den Schlüssel auf so viele Personen zu verteilen, dass bei Unverfügbarkeit einzelner trotzdem noch zeitnah auf Vorkommnisse reagiert werden kann. Zusätzlich ist es angeraten sicherheitskritische und technisch komplexe Aktionen von zwei fachlich ausgebildeten Personen gemeinsam durchführen und von einer weiteren Person einer fremden Abteilung begleiten zu lassen, also mindestens drei Personen für diese Aufgaben abzustellen.

6.2.3 Hinterlegung privater Schlüssel (Key Escrow)

Eine Hinterlegung etwaiger privater Schlüssel bei einer dritten SAP-fremden Instanz ist nicht zulässig.

6.2.4 Backup privater Schlüssel

Für Endteilnehmer ist eine Sicherung der privaten Schlüssel nicht erforderlich, da die volle Funktionalität durch einen Widerruf des verlorenen Zertifikats und die Ausstellung eines Neuen wieder vollständig erreicht werden kann.

Für Schlüssel von Zertifizierungsstellen muss gewährleistet sein, dass die Sicherung genauso gut geschützt wird wie der produktive Schlüssel selbst. Das heißt u.a.:

- Bei Root-CAs mindestens ein vier-, besser ein Sechsaugenprinzip um den Schlüssel wieder herzustellen. Zu keinem Zeitpunkt des Verfahrens darf der Schlüssel einzelnen Personen ausschließlich zugänglich sein.
- Zugriff nur durch autorisierte Rollen der PKI

- Backup nur in verschlüsselter Form,
- Vorhaltung an geographisch getrenntem Ort der CA

6.2.5 Archivierung privater Schlüssel

Eine Archivierung privater Schlüssel, also über den Zeitraum ihrer Nutzung hinaus, ist nicht zulässig.

6.2.6 Transfer privater Schlüssel in oder aus einem kryptographischen Modul

Eine Übertragung privater Schlüssel ist nur dann möglich, wenn das Zielsystem das gleiche Schutzniveau bietet, wie das System, in dem sich der Schlüssel befindet. Während des gesamten Prozesses darf dieser Sicherheitslevel nicht unterschritten werden, d.h. insbesondere, dass der Übertragungsweg verschlüsselt sein muss.

6.2.7 Speicherung privater Schlüssel in einem kryptographischen Modul

Schlüssel dürfen außerhalb der kryptographischen Module nie unverschlüsselt vorliegen. Somit impliziert sich eine verschlüsselte Speicherung im System.

6.2.8 Aktivierung privater Schlüssel

Die Voraussetzungen für eine Aktivierung, also den Zugriff zum Zwecke der Nutzung eines privaten Schlüssels hängt vom Typ des Zertifikats ab:

- **Root CA**
  Es muss gewährleistet sein, dass eine einzelne Person nicht unbemerkt Aktionen auf dem Schlüssel ausführen kann. Somit muss der Schlüssel kryptographisch aufgeteilt werden. Der Zugriff auf die einzelnen Fragmente ist zusätzlich mit personalisierten oder zufälligen PINs abzusichern, welche bei Aktivierung eingeben werden müssen (vgl. 6.4).
  Während der Nutzung des Schlüssels muss ein Fragment im System verbleiben und bei Entzug muss der Zugriff auf den Schlüssel gesperrt werden (Stichwort: Smartcard bleibt stecken)
  Das System muss immer offline also ohne Netzwerkverbindung bleiben.
- **Untergeordnete CA**
  Aus Verfügbarkeitsgründen ist es notwendig, dass private Schlüssel von ausgebenden CAs nach einem Systemstart oder Failover auf ein anderes System ohne Zutun eines Administrators zur Verfügung stehen. Daher muss gewährleistet sein, dass der Schlüssel nur auf den relevanten Systemen zugreifbar und nicht kopierbar ist.
  Bei netzwerkbasierten Lösungen muss eine Form der Authentisierung des Systems sicherstellen, dass nur die CA Systeme Zugriff erhalten.
- **Endteilnehmer**
  Schlüssel für Endteilnehmer müssen mindestens so geschützt sein, dass zur Aktivierung des Schlüssels ein bestimmter Kontext (Benutzer, Service Account, Maschine, etc.) besteht, der nur durch Nachweis eines Geheimnisses (Passwort, Smartcard, Zertifikat, etc.) erstellt werden kann.

6.2.9 Deaktivierung privater Schlüssel

- **Root CA**
  Der Zugriff erfolgt immer innerhalb einer aktiven Benutzersession. Fällt diese weg, so ist auch der Zugriff auf den Schlüssel zu sperren. Dies ist gemeinhin bei der Abmeldung oder dem Herunterfahren des Systems der Fall.
  Verliert das System Zugriff auf das Schlüsselfragment, welches für die Aktivierung notwendig ist, so muss auch der Zugriff auf den Schlüssel deaktiviert werden.
  Verliert das System die Verbindung zum Hardwaremodul so hat dies eine Sperrung des Schlüsselzugriffs zur Folge.
- **Untergeordnete CA**
  Bei eine Nichtverfügbarkeit des kryptographischen Moduls oder nach Abmeldung bzw. Herunterfahren des Systems ist der Zugriff auf den Schlüssel zu deaktivieren.
- **Endteilnehmer**
  Nach Beendigung einer Benutzersession muss der Zugriff deaktiviert werden.

6.2.10 Vernichtung privater Schlüssel

Ein besonderes Vorgehen zur Vernichtung von Schlüsseln von Endteilnehmern ist nicht vorgesehen. Zertifikatsinhaber müssen jedoch immer die Sicherheit des privaten Schlüssels gewährleisten, wobei eine normaler systemspezifischer Löschvorgang als ausreichend erachtet wird.

Bei Schlüsseln von Zertifizierungsstellen müssen alle Orte, an denen der Schlüssel in irgendeiner Form gespeichert wurde nachweislich sicher (nach Stand der Technik) gelöscht werden.

6.2.11 Güte kryptographischer Module

Siehe 6.2.1

6.3 Weitere Aspekte des Schlüsselmanagements

6.3.1 Archivierung öffentlicher Schlüssel

Public Keys der gesamten PKI müssen mindestens ein Jahr (vgl. 5.5.2) über die Gültigkeit der Zertifikate hinaus sicher nutzbar archiviert werden. Hierbei handelt es sich um eine betriebliche Anforderungen. Im Zuge der Möglichkeit forensischer Analysen kann eine längere Archivierung nützlich oder aus Compliance-Gründen durchaus verlangt sein. Längere Fristen sind abhängig von der Applikation und stehen nicht im Zusammenhang mit diesem Dokument.

6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren

Bei der Wahl der Gültigkeitsdauer von Zertifikaten spielen zum einen operative und zum anderen sicherheitsrelevante Aspekte eine Rolle. Ziel ist es bei möglichst geringem Aufwand die Sicherheit von Zertifikaten möglichst lange zu gewährleisten. Hierbei sind die Einsatzzwecke der Zertifikate von zusätzlicher Bedeutung, da die Aufwände für einen Zertifikatserneuerung einer Zertifizierungsstelle ungemein größer sind als bei einem Endteilnehmer.

Grundsätzlich darf eine Laufzeit eines Zertifikats nie länger als die voraussichtliche Sicherheit der eingesetzten kryptographischen Schlüssel und Schlüssellängen sein (vgl. 6.1.5). Aber selbst wenn Schlüssel für einen sehr langen Zeitraum als sicher erachtet werden empfiehlt es sich trotzdem Gültigkeiten zusätzlich zu beschränken, damit eine regelmäßige Erneuerung und Begutachtung der Systeme stattfindet. SAP legt die maximal Laufzeit für Wurzelzertifizierungsstellen (Root CA) auf 20 Jahre fest. Aus diesem Wert leiten sich die maximalen Laufzeiten für die in der Hierarchie ausgegebenen Zertifikate ab.

SAP Basisschutz PKIs müssen dem sog. Zwiebelprinzip folgen, d.h. dass eine CA niemals länger gültige Zertifikate ausstellen darf als das ausstellende Zertifikat selbst gültig ist. Also wenn eine Root-CA nur noch zwei Jahre gültig ist und ausstellende CAs normalerweise fünf Jahre Laufzeit haben, so darf die Root-CA trotzdem ein nur zwei Jahre gültiges Zertifikat ausstellen. Damit ist gewährleistet, dass alle ausgestellten Zertifikate einer PKI immer eine komplett gültige Vertrauenskette, hinsichtlich der Laufzeiten, haben. Diese Regel vererbt sich in der Hierarchie auf weitere CAs.

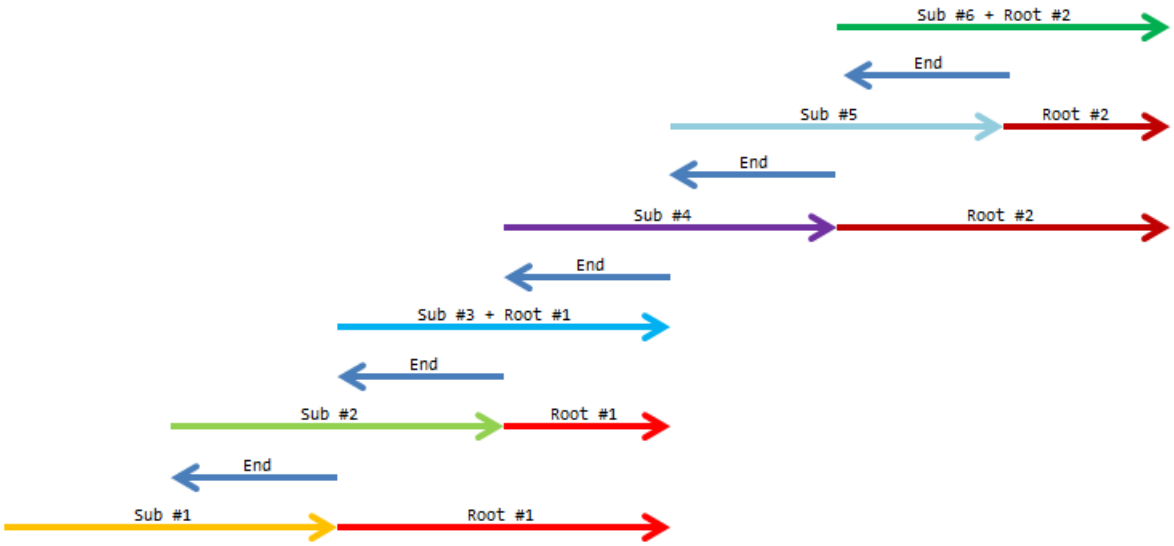
Trotzdem soll erreicht werden, dass immer maximal gültige Zertifikate ausgestellt werden können. Somit ergibt sich die folgende Formel für den spätesten Zeitpunkt einer Zertifikatserneuerung einer ausstellenden Instanz:

```
Zeitpunkt Erneuerung <= Zertifikatslaufzeit – maximale Laufzeit der angebotenen Zertifikate
```

D.h., damit nicht bei jeder Neuausstellung gleichzeitig auch das eigene und möglicherweise alle Zertifikate der Vertrauenskette erneuert werden müssen, sollten die maximalen Laufzeiten der von einer CA ausgestellten Zertifikate maximal 50% der Laufzeit der CA selbst entsprechen. Bei Endteilnehmer Zertifikaten empfiehlt es sich die Laufzeiten noch kürzer als 50% der Laufzeit der ausgebenden CA zu wählen.

```
Max Root = 20 Jahre ➔ Max Sub = 0.5 * RootCA = 10 Jahre ➔ Max Endteilnehmer = 0.5 * SubCA = 5 Jahre
```

Diese Formel ist entscheidend für den Zeitpunkt der Erneuerung der CA Zertifikate, da dieser weit vor dem Ende der eigentlichen Gültigkeit des Zertifikats sein kann. Damit eine ausgebende CA fünf Jahre gültige Zertifikate ausgeben kann muss sie bei einer Laufzeit von zehn Jahren schon nach fünf Jahren erneuert werden, Die zugehörige Root spätestens nach 15, frühestens nach etwas mehr als zehn Jahren, wenn zu diesem Zeitpunkt eine neue ausstellende CA ausgegeben werden sollte.



Falls die Schlüssel einer zu erneuernden CA noch als sicher angesehen werden können und ansonsten keine Änderungen an Attributen im Zertifikat nötig sind, kann eine Erneuerung auch durch Re-Zertifizierung des bestehenden Zertifikates nach Kap 4.6 erfolgen. Für den Fall einer Erneuerung einer bereits einmal erneuerten CA empfehlen wir die Erneuerungsmethode durch Re-Key gemäss Kap 4.7. Dieses Re-Key Vorgehen hat zur Konsequenz, dass es eine Phase der Überlappung gibt, in der zwei CRLs ausgestellt werden müssen, einmal durch das Zertifikat der ablaufenden aber noch gültigen CA und einmal durch die neue CA. OCSP Antworten für die erneuerte CA müssen dann neu aufgebaut werden. Auch müssen bei Root-CAs für diesen Zeitraum beide als vertrauenswürdig auf den Clients vorhanden sein.

Es ist dem Betrieb freigestellt die Ausstellung kürzere Zertifikatslaufzeiten zu akzeptieren und so die Aufwände für Erneuerungen auf Seiten der PKI maximal gering zu halten. Das Zwiebelprinzip muss aber immer gewährleistet sein.

Bei CA Zertifikaten sollte spätestens ein Jahr vor dem eigentlichen Ablauf des Zertifikats mit der Erneuerung begonnen werden. Zu jedem Zeitpunkt muss die komplette Vertrauenskette gültig sein.

Bei Zertifikaten von Endteilnehmern sind kurze Laufzeiten erwünscht, um so Versäumnisse im Zertifikatsmanagement zu bereinigen. Es werden die folgenden maximalen Laufzeiten vorgegeben:

Root CA	Maximal 20 Jahre
SUB CA	Maximal 10 Jahre
Server/Dienste	Maximal 5 Jahre (mit IT Security Genehmigung, ansonsten empfohlen: 2 Jahre)
Code Signing	Maximal ein Jahr
Benutzer	Maximal ein Jahr
OCSP	Maximal vier Wochen Die kurze Laufzeit erklärt sich durch die nicht vorhandene CRL Information im Zertifikat

6.4 Aktivierungsdaten

6.4.1 Erzeugung und Installation der Aktivierungsdaten

Für CA bezogene Daten müssen die Schlüsselfragmente durch Hardware erzeugt werden und durch die Fragmenthalter in mit einer nur ihr bekannten PIN geschützt werden (personalisierte Fragmente).

Im Falle hinterlegter Fragmente ist der PIN durch drei Individuen unabhängig zu erzeugen und blind zusammenzuführen. Die Hinterlegung muss sicher erfolgen und Bedarf immer eines Vieraugenprinzips.

PINs sollten den maximal möglichen Komplexitätsanforderungen genügen, müssen aber mindestens Buchstaben und Zahlen enthalten.

Vergleich hierzu „*Key Ceremony*“.

Für Endteilnehmer ist die Erstellung der Aktivierungsdaten Teil der unterliegenden Systeme und Applikationen, welche allgemein gültigen Vertraulichkeitsstufen genügen müssen.

6.4.2 Schutz der Aktivierungsdaten

Die Administratoren einer SAP PKI und deren Zertifikatsnehmer müssen versichern, dass jegliche Aktivierungsdaten (Smartcard, PIN, Passwort, etc.) für die privaten Schlüssel geheim gehalten werden und niemals Dritten zugänglich gemacht werden.

Bei Root-Zertifikaten müssen die Fragmente zur Aktivierung durch einen PIN geschützt sein, welcher sicher aufzubewahren ist (Tresor, Passwortsafe, etc.)

Ungeschützte Aktivierungsdaten müssen immer mindestens durch zwei Personen (Vieraugenprinzip) gesichert werden und sind, bei einem Transport, schnellstmöglich in einen sicheren Zustand zu überführen.

6.4.3 Weitere Aspekte

Keine Bestimmungen.

6.5 Sicherheitsmaßnahmen für Computer

Grundsätzlich müssen alle Systeme der PKI nach dem Stand der Technik und den *Best Practices* Angaben der Hersteller für ihren Einsatzzweck gehärtet werden. Zusätzliche sind die SAP internen und öffentlichen Sicherheitsstandards bei Relevanz zu befolgen.

6.5.1 Spezifische Anforderungen an technische Sicherheitsmaßnahmen

U.a. werden die folgenden Maßnahmen für die Systemsicherheit der PKI Komponenten verlangt:

- Der physikalische und digitale Zugriff zu den Systemen darf nur vertrauenswürdigen Personen ermöglicht werden, die diesen für die Ausübung ihrer PKI Rolle benötigen.
- Wo immer möglich müssen Anti-Virus und Anti-Malware Produkte installiert, betrieben und durch SAP auf Unregelmäßigkeiten überprüft werden
- Es müssen komplexe Passwörter für die genutzten Benutzerkonten eingesetzt werden, die gemäß der SAP Passwortrichtlinien zu pflegen sind. Für offline Maschinen bestehen keine Vorgaben zur Gültigkeitsdauer der Passwörter.
- Alle Systeme sind zu sperren oder herunterzufahren, wenn sie nicht genutzt werden.

6.5.2 Güte der Sicherheitsmaßnahmen

Die Sicherheitsmaßnahmen sind gemäß der SAP Richtlinien für hoch sichere Systeme umzusetzen.

6.6 Technische Maßnahmen im Lebenszyklus

6.6.1 Maßnahmen der Systementwicklung

Keine Bestimmungen.

6.6.2 Maßnahmen im Sicherheitsmanagement

Alle PKI Systeme sind regelmäßig durch die SAP IT Abteilung auf ihre Übereinstimmung mit den geforderten Richtlinien zu überprüfen. Dazu zählen mindestens die folgenden Methoden:

- Ereignisüberwachung, –sammlung und –sichtung an zentraler Stelle
- Wiederkehrende Penetrationstest für die extern sichtbaren Komponenten
- Ein zentrales Konfigurationsmanagement und regelmäßiges Auffrischen der Komponenten wo immer möglich

Monitoring and or auditing is used to ensure that systems and networks are operated in compliance with the SAP internal IT Department and SAP Global PKI specified security policies.

Verlangt sind u.a.: Eventmonitoring und Collection, Regelmäßiger Penetration Test für extern sichtbare Komponenten, Zentrale Systemkonfiguration (bspw. AD Group Policies) und Refresh selbiger.

6.6.3 Lebenszyklus der Sicherheitsmaßnahmen

Keine Bestimmungen.

6.7 Sicherheitsmaßnahmen für das Netzwerk

Die PKI Systeme müssen in dedizierten Netzwerksegmenten betrieben werden, welche durch Firewalls voneinander getrennt sind. Es sind mindestens die Netzwerksegmente „extern“, „DMZ“ und „intern“ zu unterscheiden, wobei das PKI Segment auch vom eigentlichen Office-Netzwerk abzuschotten ist.

Es dürfen nur die für die Funktion der PKI notwendigen Protokolle zwischen den Segmenten gesprochen werden. Für alle administrativen Aufgaben sind dedizierte sog. *Jump-Hosts* zu verwenden, welche einen Zwei-Faktor Authentisierung für die Benutzeranmeldung erfordern.

Auf den extern erreichbaren Komponenten müssen *Intrusion Detection* Systeme den Netzwerkverkehr zu den PKI Systemen überwachen.

6.8 Zeitstempel

Sowohl Zertifikate, CRLs als auch Ereignisprotokolle und andere relevante Informationen erhalten Zeitstempel. Diese müssen durch einen zentralen Dienst, der sein Zeit von einer verlässlichen Quelle bezieht, bestimmt sein, so dass eine Korrelation der Daten möglich ist. Hierzu empfiehlt es sich den zentralen Zeitgeberdienst durch eine externe Quelle (Funkuhr, Zeitserver, etc.) mit der korrekten Zeit zu versorgen.

Es ist ausreichend die Systeme so zu konfigurieren, dass sie ihre Systemzeit mit dem Zeitgeberdienst abgleichen und alle Systeme die gleiche Zeit haben. Kryptographisch sichere Zeitstempel durch einen entsprechenden Dienst sind nicht erforderlich.

7 PROFILE FÜR ZERTIFIKATE, SPERRLISTEN UND ONLINESTATUSABFRAGEN

7.1 Zertifikatsprofil

Die SAP Basisschutz PKI stellt Zertifikate konform zu den folgenden Standards aus:

- ITU-T recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, Juni 1997.
- RFC 5280 (obsoletes RFC 3280): Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Mai 2008

7.1.1 Versionsnummer

Zertifikate entsprechen X.509 Zertifikaten der Version 3.

7.1.2 Zertifikatserweiterungen

Zertifikatserweiterungen folgen strikt den Vorgaben des RFC 5280. Alle zur Anwendung kommenden Erweiterungen sind im CPS samt ihrer Kritikalität aufzuführen und zu erläutern.

Gemäß 6.1.7 sind *Key Usage* und/oder *Extended Key Usage* in Zertifikaten zu setzen. Letztere sollte die Zertifikatsnutzung gemäß ihrem Einsatzziel maximal weiter einschränken.

Für die *Key Usage* gelten die folgenden Vorgaben. Nicht angegebene Werte sind untersagt:

Key Usage Merkmal	CA Zertifikat	OCSP Sigantur	SSO	Server	DCs	Code
digitalSignature		✓	✓	✓	✓	✓
nonRepudation						
keyEncipherment			✓	✓	✓	
dataEncipherment						
keyAgreement						
keyCertSign	✓					
CRLSign	✓					
encipherOnly						
decipherOnly						

7.1.3 Algorithmus Bezeichner (OID)

Die eingesetzten Algorithmen müssen für den Gültigkeitszeitraum der der Zertifikate als sicher gelten. Ihre OID Nummern sind im CPS an dieser Stelle aufzuführen.

7.1.4 Namensformen

Siehe 3.1.1

7.1.5 Namensbeschränkungen

Keine Bestimmung.

7.1.6 Bezeichner für Zertifizierungsrichtlinien (OID)

Siehe 1.2

7.1.7 Nutzung von Erweiterungen zur Richtlinienbeschränkungen (PolicyConstraints)

Keine Bestimmung

7.1.8 Syntax und Semantik von Policy Qualifiern

Alle Endteilnehmer-Zertifikate müssen einen Policy Qualifier enthalten, welcher dem Typ CPS entspricht. Als URL ist die Webseite anzugeben, von welcher die Zertifizierungsrichtlinie, das CPS und alle weiteren zugehörigen Dokumente bezogen bzw. angefragt werden können.

7.1.9 Verarbeitung von kritischen Erweiterungen für Zertifizierungsrichtlinien (certificatePolicies)

Keine Bestimmung.

7.2 Sperrlistenprofil

Die SAP Basisschutz PKI stellt Sperrlisten konform zu den folgenden Standards aus:

- ITU-T recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, Juni 1997.
- RFC 5280 (obsoletes RFC 3280): Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Mai 2008

7.2.1 Versionsnummer

Sperrlisten entsprechen X.509 Sperrlisten der Version 2.

7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen

Sperrlistenerweiterungen müssen konform zu RFC 5280 und im CPS angegeben sein. Eine Begründung (*Reasoncode*) ist bei einer Sperrung immer anzugeben, wobei „*unspecified*“ nicht zulässig ist.

7.3 OCSP Profil

7.3.1 Versionsnummer

OCSP Anfragen und Rückantworten werden nach RFC 2560 in der Version 1 erstellt.

7.3.2 OCSP Erweiterungen

Keine Bestimmung

8 KONFORMITÄTSPRÜFUNG (COMPLIANCE AUDIT, ASSESSMENTS)

8.1 Häufigkeit und Umstände der Überprüfung

Überprüfungen der SAP PKIs werden regelmäßig und aufgrund bestimmter Vorkommnisse durchgeführt. Dies geschieht in Abstimmung mit den üblichen IT und Sicherheitsaudits und wird durch die IT Security Abteilung koordiniert.

Neben den normalen Audits könne die folgenden Gründe eine außerplanmäßige Überprüfung zur Folge haben:

- Verdacht auf Compliance-Verstöße von Teilen der PKI-Umgebung oder deren Betrieb
- Anforderungen durch angestrebte Zertifizierungen
- Eingehen partnerschaftlicher Beziehungen zu anderen PKI Betreibern, z.B. *Qualified Subordination* durch andere oder *Cross Certification* mit anderen CAs

8.2 Identität und Qualifikation des Überprüfers

Audits des Aufbaus und des Betriebs der SAP PKIs erfolgen sowohl durch SAP interne als auch unabhängige fremde Prüfer, die nicht dem Unternehmen zugehören. Diese sind allesamt qualifizierte Auditoren, die Erfahrungen im Bereich PKI nachweisen können.

8.3 Verhältnis von Prüfer zu Überprüftem

Im Falle von internen Überprüfungen, darf der Audit nicht von den Betreibern der PKI erfolgen, sondern muss durch unbeteiligte SAP Mitarbeiter durchgeführt werden.

Externe Audits werden grundsätzlich von qualifizierten und unabhängigen Dritten ausgeführt.

8.4 Überprüfte Bereiche

Die Prüfer müssen frei entscheiden können, welche Bereiche der PKI überprüft werden sollen. Mindestens müssen die Punkte der Zertifizierungsrichtlinie und diese selbst Bestandteil des Audits sein. Insbesondere ist dabei auf die folgende Aspekte einzugehen:

- Prozess rund um den Lebenszyklus der Zertifikate
- Physikalischer und digitaler Zugangsschutz inklusive dem Berechtigungs- und Rollenkonzept
- Notfallkonzept

8.5 Mängelbeseitigung

Werden durch die Überprüfung Defizite, die einer Risikominderung bedürfen, erkannt, so wird durch den PKI Betreiber und/oder die IT Abteilung ein Aktionsplan erstellt. Dieser priorisiert die einzelnen gefundenen Schwächen und zeigt die Lösungswege zur Rückkehr zu einem ordentlichen Betrieb auf.

Nach Umsetzung des Plans wird überprüft, ob die Schwachstellen komplett beseitigt wurden. Das Management der SAP IT, der PKI Betreiber und die zuständigen *Security Officers* werden über die Ergebnisse der Prüfung informiert.

Erkenntnisse mit durchschnittlicher Auswirkung auf die Sicherheit des Betriebs müssen innerhalp angemessener Zeit adressiert und deren Ursache beseitigt werden. In schwerwiegenden Fällen ist der Aktionsplan schnellstmöglich zu erstellen und gemäß diesem zu verfahren. Nötigenfalls sind temporäre Workarounds zu implementieren, wenn die endgültige Lösung des Problems nicht zeitnah umgesetzt werden kann.

8.6 Veröffentlichung der Ergebnisse

Die Ergebnisse aller Überprüfungen und Audits werden grundsätzlich unter Verschluss gehalten. Auf Anfrage können diese komplett oder auszugsweise internen Abteilungen oder Partnern zugänglich gemacht werden. Ein solcher Vorgang unterliegt der Aufsicht der IT Security Abteilung.

9 ANDERE GESCHÄFTLICHE UND RECHTLICHE ANGELEGENHEITEN

9.1 Gebühren

Die Nutzung der PKI und ihrer Zertifikate ist ausschliesslich für SAP Benutzer (Hier: SAP Mitarbeiter und externe Berater mit SAP Benutzer ID) und SAP eigene oder der SAP zur Verfügung gestellte Geräte vorgesehen. Es gelten daher die SAP internen Regelungen und Standards sowie etwaige mit externen abgeschlossene Vereinbarungen. Es werden in diesem Kapitel daher keine Abweichenden Regelungen definiert.

9.1.1 Gebühren für Zertifikatserstellung oder –erneuerung

Keine Bestimmung.

9.1.2 Gebühren für Zugriff auf Zertifikate

Keine Bestimmung.

9.1.3 Gebühren für Sperrung oder Statusabfragen

Keine Bestimmung.

9.1.4 Andere Gebühren

Keine Bestimmung.

9.1.5 Gebührenerstattung

Keine Bestimmung.

9.2 Finanzielle Verantwortung

SAP übernimmt keine Verantwortung für finanzielle Schäden gegenüber Dritten, die durch die Nutzung des Dienstes entstehen.

9.2.1 Deckungsvorsorge

Keine Bestimmung.

9.2.2 Weitere Vermögenswerte

Keine Bestimmung.

9.2.3 Versicherung oder Garantie für Endteilnehmer

Keine Bestimmung.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Vertraulich zu behandelnde Daten

Alle Informationen die im Zuge eines mit dem Lebenszyklus eines Zertifikats zusammenhängenden Prozesses entstehen und nicht unter 9.3.2. aufgeführt sind, sind gemäß der SAP Informationsklassifizierung mind. der Vertraulichkeitsstufe „intern“ zuzuordnen.

9.3.2 Nicht vertraulich zu behandelnde Daten

Alle Angaben die Teil eines Zertifikats, einer Sperrliste oder anderer öffentlich zugänglichen Informationen sind, werden nicht als vertraulich eingestuft.

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Die Maßnahmen die zum Schutz vertraulicher Daten zu ergreifen sind, ergeben sich aus dem Klassifizierungslevel gemäß der aktuellen SAP Informationsklassifizierungsrichtlinie.

9.4 Schutz personenbezogener Daten

9.4.1 Richtlinie zur Verarbeitung personenbezogener Daten

Es findet die generell gültige SAP Richtlinie zum Datenschutz Anwendung.

9.4.2 Vertraulich zu behandelnde Daten

Die SAP Datenschutzrichtlinie definiert die als personenbezogenen Daten zu klassifizierenden Informationen.

9.4.3 Nicht vertraulich zu behandelnde Daten

Siehe 9.3.2

9.4.4 Verantwortung zum Schutz personenbezogener Daten

Die Maßnahmen die zum Schutz personenbezogener Daten zu ergreifen sind, ergeben sich aus dem Klassifizierungslevel gemäß der aktuellen SAP Informationsklassifizierungsrichtlinie.

9.4.5 Einwilligung und Nutzung personenbezogener Daten

Keine Bestimmung.

9.4.6 Offenlegung bei gerichtlicher Anordnung oder im Rahmen gerichtlicher Beweisführung

Gemäß geltender Gesetze.

9.4.7 Andere Umstände einer Veröffentlichung

Keine Bestimmung.

9.5 Urheberrechte

Alle Rechte verbleiben bei SAP.

Eine unveränderte, unentgeltliche und nicht ausschließende Verbreitung aller veröffentlichen Informationen bedarf keiner ausdrücklichen vorherigen Genehmigung durch SAP.

9.6 Verpflichtungen

9.6.1 Verpflichtung der Zertifizierungsstellen

Der Betreiber der Zertifizierungsstellen verpflichtet sich gemäß der hier veröffentlichen Richtlinien und den Angaben im jeweiligen CPS zu handeln. Dazu gehört u.a. die Veröffentlichung und Zugänglichmachung dieser Dokumente.

9.6.2 Verpflichtung der Registrierungsstellen

RA sind verpflichtet sich an diese Zertifizierungsrichtlinie zu halten und das nötige Maß Sorgfalt bei allen durchgeführten Aktionen walten zu lassen.

Alle Angaben durch Zertifikatsnehmer und anderer Dienstnehmer sind nach bestem Wissen und Gewissen auf Korrektheit zu überprüfen.

Der Betreiber der Registrierungsstelle verpflichtet sich nicht wissentlich falsche Angaben an die CA zu übermitteln.

9.6.3 Verpflichtung des Zertifikatsinhabers (Subscriber Party Agreement)

Zertifikatsinhaber besitzen den privaten Schlüssel zu den Zertifikaten. Dieser Schlüssel ist gemäß der SAP Datenklassifizierungsrichtlinien als *Confidential* zu behandeln. Zertifikatsnehmer verpflichten sich den privaten Schlüssel sorgfältig zu schützen und einzusetzen. Dies beinhaltet u.a:

- Kein Einsatz des Schlüssels vor der Ausstellung des Zertifikats durch die CA und dessen offizieller Akzeptanz durch den Zertifikatsinhaber
- Keine Duplizierung des Schlüssels und keine Übertragung über unsichere Kanäle
- Keine weitere Nutzung nach Ablauf oder Widerruf des Zertifikats

Darüber hinaus sind alle Angaben im Zertifikatsantrag wahrheitsgemäß zu machen und das Zertifikat nach Erhalt auf Korrektheit zu überprüfen.

Zertifikate dürfen nur im gültigen Zustand und gemäß ihres vorgesehenen Zweckes (vgl. 1.4) eingesetzt werden, insbesondere darf das Zertifikat nicht als Zertifizierungsstellenzertifikat zum Einsatz kommen Der Zertifikatsnehmer ist verpflichtet Missbrauch und illegale Verwendung des Zertifikats und der kryptographischen Schlüssel zu unterlassen und einen solchen Einsatz unverzüglich den zuständigen Stellen anzuzeigen.

Desweitern ist eine Sperrung des Zertifikats bei Verlust, Verdacht auf Kompromittierung oder Änderungen der Daten, z.B. des Nachnamens zu veranlassen.

Der Zertifikatsinhaber verpflichtet sich gemäß dieser Richtlinie zu handelnd und trägt die möglichen rechtlichen Konsequenzen, die auf ein fehlerhaftes Verhalte zurückzuführen sind.

SAP behält sich vorher weitere Vereinbarung mit Endteilnehmern unabhängig von dieser Zertifizierungsrichtlinie zu vereinbaren.

9.6.4 Verpflichtung der Zertifikatsprüfer (Relying Party Agreement)

Zertifikatsprüfer sind verpflichtet eine RFC-konforme Überprüfung der Gültigkeit der Zertifikate der SAP PKI durchzuführen. Insbesondere ist die Vertrauenskette komplett bis zur Wurzelzertifizierungsstelle inklusive aller zwischenliegenden CAs zu validieren.

Auch sind die Zertifikate mittels der erlaubten Mechanismen (vgl. 4.9) auf ihren Widerruf zu untersuchen. Dabei ist das *Online Certificate Status Protocol* (OCSP) CRLs immer zu bevorzugen. Nur bei Nichtverfügbarkeit des OCSP Dienstes oder Nichtunterstützung durch die Applikation soll auf CRLs zurückgegriffen werden.

Der Prüfer ist verpflichtet Zertifikaten nur für die ausdrücklich im Zertifikat angegeben Zwecke (*Key Usage* bzw.*Extended Key Usage*) zu vertrauen (vgl. 1.4).

Bei einem negativen also ungültigen Resultat der Prüfung muss der zugehörige Vorgang abgebrochen werden.

Entsteht bei dem Prüfer der Verdacht des Missbrauchs eines Zertifikats, so ist dieser verpflichtet, dies schnellstmöglich den zuständigen Stellen anzuzeigen. In einem solchen Fall darf selbst ein technisch gültiges Zertifikat nicht mehr als vertrauenswürdig eingestuft werden.

9.6.5 Verpflichtung anderer Teilnehmer

Keine Bestimmung.

9.7 Gewährleistung (Haftungsauschluss)

Siehe 9.1

9.8 Haftungsbeschränkung

Siehe 9.1

9.9 Haftungsfreistellung

Siehe 9.1

9.10 Inkrafttreten und Aufhebung

9.10.1 Inkrafttreten

Diese Richtlinie tritt mit dem Zeitpunkt ihrer Veröffentlichung und der Inbetriebnahme der sich auf diese Zertifizierungsrichtlinie beziehenden PKI bzw. CA in Kraft.

9.10.2 Aufhebung

Eine Aufhebung der Zertifizierungsrichtlinie ist frühestens bei Einstellen des Betriebs zusätzlich der Zeit, für die PKI bezogenen Daten darüber hinaus archiviert werden. Dies ist mindestens ein Jahr der Fall.

9.10.3 Konsequenzen der Aufhebung

Alle Vereinbarung zur (SAP) Standards, rechtliche Verpflichtungen, etc. bleiben von der Aufhebung der Richtlinie unberührt.

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

Keine Bestimmung.

9.12 Änderungen der Richtlinie

9.12.1 Vorgehen bei Änderungen

Die aktuell gültige Zertifizierungsrichtlinie ist immer die, an der in den Zertifikaten angegebenen *Policy Qualifier* URL Veröffentlichte. Änderungen setzen automatisch alle vorhergehenden Richtlinien außer Kraft und die aktualisierte Version ist an selbigem Ort zugänglich zu machen und mittels aufsteigender Versionsnummer und Veröffentlichungsdatum zu versehen.

Alter Versionen sind weiterhing verfügbar zu halten.

Weitere Informationen finden sich auch in Kapitel 1.5.

9.12.2 Benachrichtigungsmechanismus und Fristen

Keine Bestimmung.

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

Weitreichende Änderungen, die eine grundlegende neue Basis für die Anwendung der Zertifizierungsrichtlinie schaffen, erfordern eine Änderung der zu der Richtlinie gehörenden OID (siehe 1.2).

9.13 Konfliktbeilegung

Keine Bestimmung.

9.14 Geltendes Recht

Der Betrieb der SAP PKIs unterliegt dem Recht der Bundesrepublik Deutschland (BRD) und der Europäischen Union (EU).

9.15 Konformität mit geltendem Recht

Im Zweifel überwiegt immer das geltende Recht die Vorgaben dieses Dokuments.

9.16 Weitere Regelungen

9.16.1 Vollständigkeit

Keine Bestimmung.

9.16.2 Abtretung der Rechte

Keine Bestimmung.

9.16.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieses CP/CPS unwirksam oder undurchführbar sein oder werden, bleibt davon die Wirksamkeit der Richtlinie im Übrigen unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der wirtschaftlichen Zielsetzung am nächsten kommen, die die Parteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich der Vertrag als lückenhaft erweist

9.16.4 Rechtliche Auseinandersetzungen / Erfüllungsort

Siehe 9.1

9.16.5 Force Majeure

Siehe 9.1

9.17 Andere Regelungen

Keine Bestimmungen

10 BEGLEITDOKUMENTE

Im Text verwiesene SAP interne Dokumente sind:

- Verschwiegenheitserklärung
- RZ Zertifizierungen
- SAP Datacenter Security
- SAP Server Hardening Richtlinien
- SAP Change Management Prozess
- IT Emergency Management Prozess
- SAP Security Policy
- SAP Richtlinien zu hochsicheren Systemen

Weitere extern verfügbare Dokumente:die zur Erstellung dienten:

Document title	**RFC 3647**
Document Name	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
Description	http://www.ietf.org/rfc/rfc3647.txt
Latest available version	
Last changed	November 2003

Document title	**RFC 5280**
Document Name	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
Description	http://tools.ietf.org/html/rfc5280
Latest available version	
Last changed	May 2008