Volksverschlüsselung®

Fraunhofer SIT

Fraunhofer-Institut für Sichere Informationstechnologie SIT

# VOLKSVERSCHLÜSSELUNGS-PKI FÜR X.509-ZERTIFIKATE

## Zertifizierungsrichtlinie (CP) und Erklärung zum Zertifizierungsbetrieb (CPS)

OID: 1.3.36.15.9.1.1.1
Version: 2.1
Datum: 24.05.2018

Volksverschlüsselung®

Fraunhofer SIT

Fraunhofer-Institut für Sichere Informationstechnologie SIT

# Impressum

## Herausgeber

Fraunhofer Institut für Sichere Informationstechnologie SIT
Rheinstraße 75
D-64295 Darmstadt

## Kontakt

E-Mail: info@volksverschluesselung.de
WWW: https://volksverschluesselung.de

## Dokumentenhistorie

| Version | Datum | Beschreibung |
|---|---|---|
| 1.0 | 29.06.2016 | Version 1.0 veröffentlicht |
| 2.0 | 24.11.2017 | • Abschnitt 1.3 überarbeitet<br>• Abschnitt 1.4.1 überarbeitet<br>• Abschnitt 2.1 - Zertifikatssuche im Verzeichnis aktualisiert<br>• Abschnitt 2.3 aktualisiert<br>• Abschnitt 2.4 überarbeitet<br>• Abschnitt 3.1.1 SubjectDN aktualisiert; zur Verhinderung von Namensgleichheit wird das Attribut SerialNumber statt der E-Mail-Adresse verwendet.<br>• Abschnitt 3.1.5 bzgl. SerialNumber aktualisiert<br>• Abschnitt 3.2.2 komplett überarbeitet und aktualisiert<br>• Abschnitt 3.3.1 präzisiert<br>• Abschnitt 3.3.2 präzisiert<br>• Abschnitt 3.4 bzgl. Sperrkennwort aktualisiert<br>• Abschnitt 4.1.2 überarbeitet<br>• Abschnitt 4.2.1 überarbeitet<br>• Abschnitt 4.2.2 überarbeitet<br>• Abschnitt 4.4.1 letzten Absatz ergänzt<br>• Abschnitt 4.5.1 Absatz 3 letzten Satz ergänzt<br>• Abschnitt 4.9.3 überarbeitet<br>• Abschnitt 4.9.7 Veröffentlichungs-Frequenz aus 2.3 nach hier verschoben.<br>• Abschnitt 7.1.3 OCSP No Check ergänzt<br>• Abschnitt 7.1.4 SubjectDN gemäß Abschnitt 3.1.1 aktualisiert<br>• Abschnitt 7.2 überarbeitet<br>• Abschnitt 7.3.2 aktualisiert<br>• Abschnitt 8.3 überarbeitet<br>• Abschnitt 9.4.6 E-Mail-Adresse ergänzt<br>• Abschnitt 9.6.1 erster Satz geändert<br>• Abschnitt 9.6.2 erster Satz geändert<br>• Abschnitt 9.12 überarbeitet<br>• Kapitel 5 und 6 erweitert. |
| 2.1 | 24.05.2018 | Anpassung von Abschnitt 9.4.1, 9.4.2 und 9.4.5 an die Datenschutzgesetzgebung zum 25. Mai 2018 |

# Inhalt

# Abbildungsverzeichnis



# Tabellenverzeichnis

# 1 Einleitung

Das Fraunhofer–Institut für Sichere Informationstechnologie SIT (kurz Fraunhofer SIT), ein Institut der Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (kurz Fraunhofer), startet mit der Volksverschlüsselung eine Initiative, um die Nutzung von Ende-zu-Ende-Verschlüsselung in der Bevölkerung zu verbreiten und damit den Schutz der elektronischen Kommunikation von Privatpersonen sowie Unternehmen zu erhöhen.

Im Rahmen dieser Initiative stellt das Fraunhofer SIT die Public Key Infrastruktur Volksverschlüsselungs-PKI zur Erzeugung, Ausgabe und Verwaltung von X.509-Zertifikaten zur Verfügung, um die Vertraulichkeit, Integrität und Verbindlichkeit von Daten bzw. Nachrichten zu gewährleisten.

Zertifikate der Volksverschlüsselung sind hochwertige Zertifikate, bei denen neben der E-Mail-Überprüfung auch eine Identitätsprüfung durchgeführt wird. Mit der Ausstellung eines Zertifikats bestätigt die Volksverschlüsselungs-PKI, dass die Identität der im Zertifikat genannten Person im Rahmen der Registrierung authentifiziert wurde. Der Empfänger eines solchen Zertifikats kann somit darauf vertrauen, dass der öffentliche Schlüssel auch tatsächlich zum Zertifikatsinhaber gehört.

Die Volksverschlüsselungs-PKI stellt **keine** qualifizierten Zertifikate für elektronische Signaturen im Sinne der eIDAS-Verordnung [eIDAS-VO] bzw. dem deutschen Signaturgesetz [SigG] aus.

## 1.1 Überblick

Bei dem vorliegenden Dokument handelt es sich um die Zertifizierungsrichtlinie (engl. Certificate Policy, kurz CP) und die Erklärung zum Zertifizierungsbetrieb (engl. Certification Practice Statement, kurz CPS) der Volksverschlüsselungs-PKI für X.509-Zertifikate. Im Folgenden wird es kurz als VV-X.509 CP/CPS bezeichnet.

Das VV-X.509-CP/CPS ermöglicht den Nutzern eine Einschätzung der Vertrauenswürdigkeit der ausgestellten Zertifikate und erlaubt Zertifikatsnutzern Entscheidungen zu treffen, inwieweit das durch die Volksverschlüsselungs-PKI gewährte Vertrauens- und Sicherheitsniveau für Anwendungen geeignet ist.

Das VV-X.509-CP/CPS legt die Rahmenbedingungen für die Ausstellung von Zertifikaten entsprechend der internationalen Norm X.509 [X.509] fest. Es beschreibt das Vorgehen des Zertifizierungsdienstes bei der Beantragung, Ausstellung und Verwaltung der Endteilnehmer-Zertifikate sowie die betrieblichen Abläufe und Sicherheitsmaßnahmen der Zertifizierungsstellen der Volksverschlüsselung.

Der Betrieb der Volksverschlüsselungs-PKI erfolgt im Auftrag des Fraunhofer SIT durch die Deutsche Telekom AG.

Die Struktur dieses Dokuments orientiert sich an dem Internet Standard »Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework« [RFC 3647] und enthält die entsprechenden Gliederungspunkte, um eine Vergleichbarkeit mit anderen Policies zu ermöglichen.

**Die Regelungen in diesem Dokument beziehen sich ausschließlich auf die Volksverschlüsselungs-PKI und finden keine Anwendung auf andere Zertifizierungsdienste von Fraunhofer, die das Competence Center Public Key Infrastructures (kurz CC-PKI) für die Angestellten, externen Mitarbeiter und Geschäftskunden der Fraunhofer-Gesellschaft zur Verfügung stellt. Hierfür gelten gesonderte Regelungen.**

## 1.2 Dokumentenidentifikation

| | |
|---|---|
| Name: | Volksverschlüsselungs-PKI für X.509-Zertifikate – Zertifizierungsrichtlinie (CP) und Erklärung zum Zertifizierungsbetrieb (CPS) |
| Version | 2.0 |
| Objektbezeichnung (Object Identifier, OID): | 1.3.36.15.9.1.1.1 |

Der OID ist wie folgt zusammengesetzt:
{iso(1) identified-organization(3) teletrust(36) identified organization(15) Fraunhofer Institute for Secure Information Technology SIT (9) Volksverschlüsselung(1) cp/cps(1) private-ca (1)}.

## 1.3 Teilnehmer der Volksverschlüsselungs-PKI

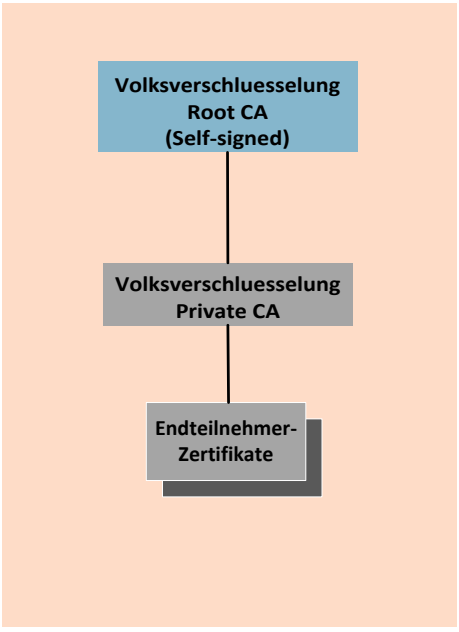
### 1.3.1 Zertifizierungsstellen (Certification Authority, CA)

Den Zertifizierungsstellen (CAs) obliegt die Ausstellung von Zertifikaten innerhalb der Volksverschlüsselungs-PKI. Die Volksverschlüsselungs-PKI folgt einer zweistufigen Zertifizierungshierarchie:

- die Root-CA, welche den Vertrauensanker der Volksverschlüsselungs-PKI darstellt.
- die Sub-CAs, die Schlüssel der Endteilnehmer zertifizieren und deren Zertifikate verwalten.

Die Abbildung 1 zeigt die Zertifizierungshierarchie der Volksverschlüsselungs-PKI.

*Abbildung 1: Zertifizierungshierarchie der Volksverschlüsselungs-PKI*




Die Rolle der Instanzen wird im Folgenden genauer erläutert.

Die „**Volksverschluesselung Root CA“** ist die Wurzelinstanz der Volksverschlüsselungs-PKI. Der öffentliche Schlüssel (Public Key) der „Volksverschluesselung Root CA“ ist in einem selbst-signierten Zertifikat (Wurzel-Zertifikat) enthalten und wird veröffentlicht (vgl. Abschnitt 2.2). Somit können alle Teilnehmer der Volksverschlüsselungs-PKI die Authentizität und Gültigkeit aller unterhalb der „Volksverschluesselung Root CA“ ausgestellten Zertifikate überprüfen.

Die „Volksverschluesselung Root CA“ stellt ausschließlich Zertifikate und Sperrlisten für die unmittelbar nachgeordneten Zertifizierungsstellen (Sub-CAs) der Volksverschlüsselungs-PKI aus.

Unterhalb der Wurzelinstanz werden nachfolgend beschriebene Sub-CAs betrieben.

Die „**Volksverschluesselung Private CA“** stellt nur Zertifikate für natürliche Personen zur privaten Nutzung aus. Die private Nutzung der Zertifikate und der zugehörigen Schlüssel ist gegeben, wenn diese an ausschließlich privat genutzte E-Mail-Adressen gebunden sind. Eine private Nutzung der Zertifikate bzw. der Schlüssel ist insbesondere dann nicht gegeben, wenn ihre Nutzung einer gewerblichen oder freiberuflichen Tätigkeit zugeordnet werden kann.

Die jeweiligen Schlüsselpaare werden vom Endteilnehmer selbst generiert. Für jeden Endteilnehmer wird das folgende Zertifikatstripel für verschiedene Schlüsselpaare erzeugt:

- Verschlüsselungszertifikat
- Signaturzertifikat
- Authentifizierungszertifikat

### 1.3.2 Registrierungsstelle (Registration Authority, RA)

Eine Registrierungsstelle (RA) ist die Stelle, welche die Identität der Zertifikatsantragsteller überprüft und Zertifikats- und Sperraufträge für Endteilnehmer-Zertifikate entgegennimmt und an die entsprechende Zertifizierungsstelle weiterleitet.

Jede Sub-CA verfügt über eine oder mehrere Registrierungsstellen. Die Sub-CAs können sich hinsichtlich der Verfahren zur Überprüfung der Identität unterscheiden. Die im Kontext der Volksverschlüsselung unterstützten Verfahren zur Identitätsprüfung des Zertifikatsinhabers sind in Abschnitt 3.2.2 beschrieben.

Fraunhofer SIT kann die Aufgaben der Registrierungsstelle an Dritte (kurz RA-Partner) delegieren. RA-Partner werden mittels Vertrag verpflichtet, insbesondere die in diesem Dokument definierten Prozesse für die Registrierung, Zertifikatsausgabe, Revokation und Archivierung einzuhalten.

### 1.3.3 Endteilnehmer (Antragsteller / Zertifikatsinhaber)

Im Kontext der „**Volksverschluesselung Private CA“** sind Endteilnehmer ausschließlich natürliche Personen, die für sich selbst ein Zertifikat zur privaten Nutzung beantragen. D.h. der Antragsteller ist mit dem Zertifikatsinhaber identisch, der im Zertifikat als *Subject* eingetragen ist. Der Zertifikatsinhaber muss seine Identität gegenüber der Registrierungsstelle (RA) nachweisen und im Besitz des privaten Schlüssels sein, der zum öffentlichen Schlüssel im Zertifikat gehört.

### 1.3.4 Zertifikatsnutzer (Vertrauende Dritte)

Zertifikatsnutzer sind Personen oder Organisationen, die Zertifikate der Volksverschlüsselungs-PKI nutzen, um mit dem Zertifikatsinhaber vertraulich kommunizieren bzw. die Gültigkeit einer digitalen Signatur verifizieren zu können. Die zum Zwecke der Authentizitäts- und Gültigkeitsprüfungen notwendigen Dienste und Informationen sind dem Zertifikatsnutzer zugänglich.

Ein Zertifikatsnutzer kann – muss aber nicht – Teilnehmer der Volksverschlüsselungs-PKI sein

### 1.3.5 Weitere Teilnehmer

Weitere Teilnehmer sind Dienstleister, die im Auftrag des Fraunhofer SIT in den Registrierungsprozess zur Authentifizierung der Identität des Zertifikatsinhabers eingebunden sind (vgl. Abschnitt 3.2.2).

## 1.4 Zertifikatsverwendung

### 1.4.1 Zulässige Verwendung von Zertifikaten

Die Verwendung der von der Volksverschlüsselungs-PKI erzeugten Zertifikate darf nur gemäß den nachfolgenden Bedingungen erfolgen (vgl. auch Abschnitt 4.5).

Die Zertifikate dürfen nur für die Anwendungen benutzt werden, die in Übereinstimmung mit der im Zertifikat angegebenen Nutzung (vgl. Abschnitt 7.1ff KeyUsage) stehen.1

Die von der „**Volksverschluesselung Private CA“** ausgestellten Endteilnehmer-Zertifikate und die zugehörigen Schlüssel können zur Verschlüsselung und zum Signieren von E-Mails und anderen Daten (Schlüssel, Nachrichten, etc.) sowie zur Authentifizierung (TLS-Client-Authentifizierung) genutzt werden (vgl. Abschnitt 7.1.4 KeyUsage). Zertifikate der „**Volksverschluesselung Private CA“** und die zugehörigen Schlüssel dürfen ausschließlich nur zu privaten Zwecken verwendet werden. Eine private Nutzung ist gegeben, wenn die Zertifikate und die zugehörigen Schlüssel an ausschließlich privat genutzte E-Mail-Adressen gebunden sind. Eine private Nutzung der Zertifikate bzw. der Schlüssel ist insbesondere dann nicht gegeben, wenn ihre Nutzung einer gewerblichen oder freiberuflichen Tätigkeit zugeordnet werden kann.

Die Schlüssel der Root-CA- werden ausschließlich zum Signieren von Sub-CA-Zertifikaten und Sperrlisten verwendet.

Die privaten Schlüssel der Sub-CAs werden zum Signieren der zugehörigen Endteilnehmer-Zertifikate, Sperrlisten und OCSP-Signer Zertifikate benutzt.

Dem Zertifikatsnutzer obliegt es zu prüfen, ob die Endteilnehmer-Zertifikate aufgrund dieser VV-X.509-CP/CPS den Sicherheitsanforderungen seiner Anwendung genügen und ob die Verwendung des betreffenden Zertifikats für einen bestimmten Zweck geeignet und nicht anderweitig verboten ist, beispielsweise aufgrund geltender gesetzlicher Bestimmungen.

### 1.4.2 Unzulässige Verwendung von Zertifikaten

Die Verwendung der Endteilnehmer-Zertifikate für Steuer- und Kontrolleinrichtungen in gefährlichen Umgebungen sowie für Dienste und Systeme, die einen störungsfreien Betrieb erfordern und ein Ausfall zu großen materiellen oder immateriellen Schäden führen sowie Schäden an Leib und Leben verursachen kann, ist nicht gestattet. Hierzu zählen u.a. Atomkraftwerke, Chemieproduktionsanlagen oder Luftfahrtsysteme sowie insbesondere Dienste und Systeme, die in Zusammenhang mit kritischen Infrastrukturen stehen.

Endteilnehmer-Zertifikate der Sub-CAs dürfen nicht als Root-CA- oder CA-Zertifikate verwendet werden. Die Verwendung eines Zertifikats muss den im Zertifikat festgelegten Schlüsselverwendungszwecken (vgl. Abschnitt 7.1ff KeyUsage) entsprechen.

Eine Nutzung der Zertifikate der „**Volksverschluesselung Private CA“** und der zugehörigen Schlüssel für geschäftliche Nutzungszwecke ist nicht gestattet (vgl. Abschnitt 1.4.1).

## 1.5 Verwaltung dieser Richtlinie

### 1.5.1 Zuständige Organisation

Das vorliegende Dokument wird vom Fraunhofer-Institut für Sichere Informationstechnologie SIT verwaltet und herausgegeben.

### 1.5.2 Kontaktinformationen

Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75
D-64295 Darmstadt.
E-Mail: info@volksverschluesselung.de
WWW: https://volksverschluesselung.de

### 1.5.3 Abnahmeverfahren

Dieses Dokument (VV-X.509-CP/CPS) behält Gültigkeit, solange es nicht von der in Abschnitt 1.5.1 genannten Organisation widerrufen wird. Es wird bei Bedarf fortgeschrieben und erhält dann jeweils eine neue aufsteigende Versionsnummer (vgl. Abschnitt 9.12.1 und 9.12.2). Die in Abschnitt 1.5.1 genannte Organisation entscheidet darüber, ob auf Basis der Änderungen oder Erweiterungen die Vergabe einer neuen Objekt-Kennung für die VV-X.509-CP/CPS notwendig wird (vgl. Abschnitt 9.12.3).

## 1.6 Definitionen und Abkürzungen

Definitionen und Abkürzungen siehe Anhang A.

# 2 Veröffentlichungen und Verzeichnisse

## 2.1 Verzeichnisse

- Das Verschlüsselungszertifikat für Endteilnehmer wird in einem öffentlichen Verzeichnis der Volksverschlüsselungs-PKI veröffentlicht und kann über LDAP abgefragt werden, sofern der Zertifikatsinhaber im Rahmen der Zertifikatsbeantragung der Veröffentlichung zugestimmt hat. Eine Zertifikatssuche ist nur anhand der E-Mail-Adresse möglich. Aus Gründen des Datenschutzes ist im Verzeichnis keine Suche über Platzhalter erlaubt und Anfragen werden nur auf Basis einer vollständigen E-Mail-Adresse beantwortet.

  Der Verzeichnisdienst der Volksverschlüsselungs-PKI ist über das Internet unter der URL ldap://ldap.volksverschluesselung.de über Port 636 (mit SSL) erreichbar.

- Die CA-Zertifikate der Volksverschlüsselungs-PKI werden über die Web-Seite https://volksverschluesselung.de/zertifikate.php veröffentlicht und stehen dort zum Herunterladen zur Verfügung. Zusätzlich werden auf dieser Webseite die Fingerprints der CA-Zertifikate zur Prüfung der Korrektheit und der Authentizität der Zertifikate veröffentlicht.

  Das Root-CA-Zertifikat ist **nicht** in den Zertifikatsspeichern von Betriebssystemen und Anwendungen als „vertrauenswürdige Stammzertifizierungsstelle“ vorinstalliert, sondern muss explizit nachinstalliert werden.

  Der vollständige zertifikatsspezifische Link ist im Zertifikatsfeld *AuthorityInfoAccess* in den Zertifikaten (vgl. Abschnitt 7.1ff) angegeben.

- Sperrlisten (CRL) der Volksverschlüsselungs-PKI werden über die folgende Adresse bereitgestellt:

  http://volksverschluesselung.de/crl

  Die vollständige zertifikatsspezifische Adresse ist dem Zertifikatsfeld *CRLDistributionPoints* in den Zertifikaten (vgl. Abschnitt 7.1) zu entnehmen.

- Ferner stellt die Volksverschlüsselungs-PKI einen Validierungsdienst zur Verfügung, der über das Internetprotokoll „Online Certificate Status Protocol“ (OCSP) agiert. Über diesen OCSP-Responder kann der Status von Zertifikaten online abgerufen werden. Der OCSP-Responder ist über folgende Adresse erreichbar: http://ocsp.volksverschluesselung.de.

  Die Adresse ist im Zertifikatsfeld *AuthorityInfoAccess* der Endteilnehmer-Zertifikaten (vgl. Abschnitt 7.1ff) vermerkt.

- Das vorliegende Dokument (VV-X.509-CP/CPS) kann im PDF-Format von der Web-Seite https://volksverschluesselung.de/dokumente.php heruntergeladen werden.

## 2.2 Veröffentlichung von Informationen

Die in Abschnitt 2.1 genannten öffentlichen Informationen wie dort beschrieben veröffentlicht.

## 2.3 Aktualisierung der Informationen

Für die in Abschnitt 2.1 genannten Informationen gelten folgende Veröffentlichungsintervalle:

| | |
|---|---|
| Root-CA-Zertifikat: | Das Root-CA-Zertifikat wird zum Zeitpunkt der Erzeugung veröffentlicht. |

| | |
|---|---|
| Sub-CA-Zertifikat "Volksverschluesselung Private CA": | Dieses Sub-CA-Zertifikat wird zum Zeitpunkt der Erzeugung veröffentlicht. |
| Endteilnehmer-Zertifikate der "Volksverschluesselung Private CA": | Das Verschlüsselungszertifikat wird nach der Erzeugung in den Verzeichnisdienst eingestellt, sofern der Zertifikatsinhaber der Veröffentlichung zugestimmt hat. Veröffentlichte Endteilnehmer-Zertifikate werden nach Ablauf ihrer Gültigkeit oder nach Sperrung aus dem Verzeichnisdienst gelöscht. |
| Sperrlisten (CRLs): | Sperrlisten (CRLS) werden wie in Abschnitt 4.9.7 beschrieben aktualisiert. |
| OCSP | Die OCSP-Datenquelle wird unmittelbar nach Ausstellung der entsprechenden CRL aktualisiert (siehe Abschnitt 4.9.7). |
| VV-X.509-CP/CPS | Die Veröffentlichung der Richtlinien erfolgt nach der Erstellung bzw. nach Änderungen. |

## 2.4 Zugang zu den Verzeichnissen

Für die in Abschnitt 2.1 aufgeführten Informationen sowie das Suchen nach Verschlüsselungszertifikaten über den Verzeichnisdienst und die Nutzung des OCSP-Responder gibt es keine Zugriffsbeschränkung für lesenden Zugriff. Die Informationen sind öffentlich zugänglich.
Schreibender Zugriff wird nur berechtigtem Personal der Volksverschlüsselungs-PKI gewährt. Hierfür sind entsprechende Sicherheitsmaßnahmen implementiert.

# 3 Identifizierung und Authentifizierung

## 3.1 Namensgebung

### 3.1.1 Namensform

Alle innerhalb der Volksverschlüsselungs-PKI ausgestellten Zertifikate enthalten im Feld *Issuer* Angaben zum Aussteller (vgl. Abschnitt 7.1ff) und im Feld *Subject* Angaben zum Zertifikatsinhaber. Diese eindeutigen Namen werden entsprechend der Normenserie x.500 und dem [RFC5280] als DistinguishedNames (DN) vergeben. Ein DN enthält eine Folge von obligatorischen und optionalen eindeutigen Namensattributen, durch die ein Teilnehmer identifiziert werden kann.

Außerdem enthalten die Endteilnehmer-Zertifikate in der X.509-Extension SubjectAltName die E-Mail-Adresse des Zertifikatsinhabers im Format nach RFC 822.

Der *SubjectDN* in Endteilnehmer-Zertifikaten der „**Volksverschluesselung Private CA“** enthält folgende Namensattribute zur Identifizierung des Zertifikatsinhabers:

- commonName (CN)
- title
- surName (SN)
- givenName (G)
- serialNumber

Das Attribut *commonName (CN)* ist obligat und enthält den bürgerlichen Namen des Zertifikatsinhabers bestehend aus Vorname(n), Name sowie ggf. akademischer Titel.

Die Länge des Attributs sollte i. d. R. auf 64 Zeichen begrenzt sein. Falls die Daten > 64 Zeichen sind, gelten folgende Kürzungsregeln:

- sind Titel, Vorname(n) und Name > 64 Zeichen, werden bis auf den ersten Vornamen alle weiteren gestrichen.

- sind Titel, Vorname und Name immer noch > 64 Zeichen, wird der Titel gestrichen.

- sind Vorname und Name immer noch > 64 Zeichen, wird nicht weiter gekürzt.

Das Attribut *title* enthält (zusätzlich zum CN) den akademischen Titel. Dieses Attribut entfällt, wenn kein Titel vorhanden ist.

Das Attribut *SurName* enthält (zusätzlich zum CN) den vollständigen Namen des Zertifikatsinhabers.

Das Attribut *givenName* enthält (zusätzlich zum CN) alle Vornamen des Zertifikatsinhabers.

Das Attribut *serialNumber* ist obligat und wird verwendet, um Namensgleichheit zu verhindern.

Beispiel:
CN = Erika Anna-Maria Mustermann
SN = Mustermann
G = Erika Anna-Maria
SERIALNUMBER = BDE3AE2ACA7529A56A6B01AA8BC2D8201E21D2CA4A35A11C07C498CF8C2D9777

### 3.1.2 Aussagekraft von Namen

Der *SubjectDN* in Endteilnehmer-Zertifikaten muss den Zertifikatsinhaber eindeutig identifizieren und in einer für Menschen verständlichen Form vorliegen. Bei der Namensvergabe gelten folgende Regelungen:

- Zertifikate für natürliche Personen sind auf den Namen der Person auszustellen.
- Die Schreibweise des Namens muss mit der Schreibweise aus dem Identifikationsverfahren übereinstimmen.
- Der Name darf nicht aufgrund von Sonderzeichen wie z.B. Umlauten geändert sein.

Für die in der Extension *SubjectAltName* angegebene E-Mail-Adresse gibt es keine Notwendigkeit für aussagefähige Namen. Der Name in der E-Mail-Adresse kann von dem Namen des Zertifikatsinhabers abweichen.
Im Rahmen der Zertifikatsbeantragung stellt die Volksverschlüsselungs-PKI sicher, dass die E-Mail-Adresse zu einem gültigen E-Mail-Postfach des Zertifikatsinhabers gehört.

### 3.1.3 Anonymität und Pseudonyme für Zertifikatsinhaber

Pseudonyme und anonyme Endteilnehmer-Zertifikate werden derzeit von der Volksverschlüsselungs-PKI nicht unterstützt (vgl. Abschnitt 3.1.2).

### 3.1.4 Regeln für die Interpretation verschiedener Namensformen

In den DistinguishedNames (DN) sind alle Attribute UTF-8 kodiert. Somit können Sonderzeichen und Umlaute verwendet werden.

### 3.1.5 Eindeutigkeit von Namen

Der in Endteilnehmer-Zertifikaten der „**Volksverschluesselung Private CA“** verwendete Name des Zertifikatsinhabers im Feld *SubjectDN* ist durch die Vergabe einer Seriennummer (*serialNumber*) stets eindeutig.

### 3.1.6 Erkennung und Authentisierung von geschützten Namen

Zertifikate der „**Volksverschluesselung Private CA“** werden nur für natürliche Personen ausgestellt. Im *SubjectDN* sind Vornamen(n) und Nachname im Attribut *commonName* identisch mit dem bürgerlichen Namen des Zertifikatsinhabers, der im Rahmen der Identitätsprüfung festgestellt wurde. Somit ist der Namensschutz gegeben.

## 3.2 Identitätsprüfung bei Erstbeantragung

### 3.2.1 Methode zum Besitznachweis des privaten Schlüssels

Die Schlüsselpaare für Verschlüsselung, Signatur und Authentifizierung werden in der Umgebung des Endteilnehmers generiert. Die privaten Schlüssel verlassen zu keinem Zeitpunkt diese Umgebung.

Mit folgendem kryptographischen Verfahren weist der Endteilnehmer nach, dass er im Besitz des privaten Schlüssels ist, der dem zu zertifizierenden öffentlichen Schlüssel zugeordnet ist: Für jeden öffentlichen Schlüssel wird ein Certificate Signing Request (CSR) gemäß PKCS#10-Methode erzeugt. Durch das Signieren des CSRs mit dem dazugehörigen privaten Schlüssel wird der Besitznachweis erbracht. Die Gültigkeit der Signatur wird überprüft.

### 3.2.2 Authentifizierung einer natürlichen Person

Die vom Zertifizierungsdienst „**Volksverschluesselung Private CA"** ausgestellten Zertifikate sind an natürliche Personen gebunden, deren Identität festgestellt werden konnte. Die Authentifizierung der Identität einer natürlichen Person wird von der Volksverschlüsselungs-PKI oder einem geeigneten Dienstleister durchgeführt, mit dem das Fraunhofer SIT einen Vertrag geschlossen hat.

Zum Nachweis der Identität werden dem Antragsteller verschiedene Verfahren angeboten.

1. Online-Ausweisfunktion des Personalausweises: Der Antragsteller authentisiert sich gegenüber der Volksverschlüsselung mit der Online-Ausweisfunktion. Hierfür wird ein Auftragsdatenverarbeiter mit der Verarbeitung der personenbezogenen Nutzerdaten beauftragt. Zu den Standardleistungen des Auftragsdatenverarbeiters gehören insbesondere die Bereitstellung der eID-Schnittstelle zur Anbindung an die Volksverschlüsselungs-PKI in Form eines Webservices gemäß der BSI-Richtline [BSI TR-03130] „eID-Server" und die damit verbundene Entgegennahme und Bearbeitung von Authentisierungsanfragen.

2. Telekom-Account: Der Antragsteller besitzt einen Festnetz-Anschluss mit Internetzugang (DSL Anschluss) bei der Deutschen Telekom AG. Der Antragsteller authentisiert sich gegenüber der Volksverschlüsselung mit seinem Telekom-Account.

3. Registrierungscode: Der Antragsteller authentisiert sich gegenüber der Volksverschlüsselung mit seinem Registrierungscode, den er im Rahmen einer Registrierung nach erfolgreicher Identitätsprüfung erhalten hat. Es stehen folgende Registrierungsverfahren zur Verfügung:

    - Der Antragsteller erscheint persönlich bei der Registrierungsstelle (Vor-Ort-Registrierung) und legt für die Identitätsprüfung ein gültiges Ausweisdokument (Personalausweis, Aufenthaltstitel, Reisepass) vor. Ein Mitarbeiter der Registrierungsstelle führt auf Basis des Ausweisdokumentes die Identitätsprüfung durch.

    - Der Antragsteller nutzt ein Registrierungsportal. In diesem Fall wird die Identität des Antragstellers entweder über die Online-Ausweisfunktion des neuen Personalausweises oder über ein von der Volksverschlüsselung anerkanntes Zertifikat festgestellt.

Im Rahmen der Identitätsfeststellung werden folgende Daten erhoben, die in das Zertifikat übernommen werden:

- Vorname(n), Name und ggf. akademischer Titel,

- E-Mail-Adresse.

Hinsichtlich der E-Mail-Adresse wird sichergestellt, dass diese valide ist und der Endteilnehmer Zugang zur Mailbox hat und diese verwenden kann. Falls die Korrektheit der angegebenen E-Mail-Adresse nicht bereits durch das Authentifizierungsverfahren bestätigt wird (z.B. Telekom-Account), erfolgt die Überprüfung durch

einen zufälligen Validierungscode, der dem Antragsteller an die von ihm angegebene E-Mail-Adresse zugesendet wird. Den Verifikationscode muss der Antragsteller im Rahmen der Zertifikatsbeantragung eingeben.

### 3.2.3 Authentifizierung von Organisationen

Von der „**Volksverschluesselung Private CA“** werden ausschließlich Zertifikate für natürliche Personen ausgestellt.

### 3.2.4 Nicht verifizierte Zertifikatsinformationen

Für die Erstellung von Endteilnehmer-Zertifikaten werden außer den Angaben in Abschnitt 3.2.1 und 3.2.2 keine weiteren persönlichen Daten des Zertifikatsinhabers erhoben und ungeprüft in das Zertifikat übernommen.

### 3.2.5 Prüfung der Berechtigung zur Antragsstellung

Im Kontext der „**Volksverschluesselung Private CA“** können natürliche Personen nur für sich selbst ein Zertifikat zur privaten Nutzung beantragen.

### 3.2.6 Kriterien für Interoperation (Cross-Zertifizierung)

Eine Cross-Zertifizierung mit anderen Zertifizierungsstellen wurde bislang noch nicht durchgeführt.

## 3.3 Identifizierung und Authentifizierung bei Zertifikatserneuerung

### 3.3.1 Routinemäßige Zertifikatserneuerung

Die Zertifikatsnehmer werden rechtzeitig vor Ablauf der Gültigkeit des Zertifikates via Mail daran erinnert, dass ihr Zertifikat ausläuft und sie ein neues Zertifikat für ein neues Schlüsselpaar beantragen sollten. Es gilt das in Abschnitt 3.2 beschriebene Verfahren.

### 3.3.2 Zertifikatserneuerung nach Sperrung

Gesperrte Zertifikate können nicht erneuert werden. Es ist ein neues Zertifikat zu beantragen. Es gilt das in Abschnitt 3.2 beschriebene Verfahren.

## 3.4 Identifizierung und Authentifizierung bei Zertifikatssperrung

Endteilnehmer können jederzeit mit Hilfe der Volksverschlüsselungs-Software die Sperrung ihrer eigenen Zertifikate veranlassen (vgl. Abschnitt 4.9). Um ein unerlaubtes Sperren zu verhindern, muss sich der Sperrende gegenüber der Registrierungsstelle authentisieren.

Zur Authentifizierung einer Sperrung muss der Zertifikatsinhaber das Sperrkennwort übermitteln, das ihm im Rahmen der Zertifikatsausstellung sicher über die Volksverschlüsselungs-Software zugestellt wurde.

Der Zertifikatsinhaber wird über die Sperrung seines Zertifikatstripels via Benachrichtigungsmail an seine E-Mail-Adresse unterrichtet.

# 4 Betriebliche Anforderungen im Lebenszyklus von Zertifikaten

## 4.1 Zertifikatsbeantragung

### 4.1.1 Wer kann ein Zertifikat beantragen

Zertifikate können von den in Abschnitt 1.3.3 benannten Endteilnehmern beantragt werden. Die Antragstellung erfolgt online über die auf dem Rechner des Endteilnehmers installierte Volksverschlüsselungs-Software.

### 4.1.2 Registrierungsprozess

Antragsteller beantragen ihre Zertifikate mit Hilfe der Volksverschlüsselungs-Software. Erst wenn der Registrierungsprozess bei der der Zertifizierungsstelle zugeordneten Registrierungsstelle erfolgreich abgeschlossen und von dieser ein geprüfter Zertifizierungsantrag an die CA übermittelt wurde, wird ein Zertifikatstripel für den Antragsteller ausgestellt.

Im Rahmen der Zertifikatsbeantragung werden die folgenden Schritte durchlaufen:

- Die Identität des Endteilnehmers wird entsprechend dem ausgewählten Authentifizierungsverfahren (vgl. Abschnitt 3.2.2) überprüft.

- Es wird überprüft, ob für die angegeben E-Mail-Adresse bereits Zertifikate ausgestellt wurden, die noch gültig sind. In diesem Fall, wird der Prozess mit entsprechender Fehlermeldung beendet.

- Die angegebene E-Mail-Adresse, die in das Zertifikat übernommen werden soll, wird validiert. Die E-Mail-Adresse wird entweder durch das Authentifizierungsverfahren bestätigt oder an die angegebene E-Mail-Adresse wird eine Bestätigungsmail mit einem Validierungscode gesendet, der eine begrenzte Gültigkeit (maximal 10 Minuten) besitzt. Wird innerhalb dieser Zeitspanne der Validierungscode nicht an die Registrierungsstelle gesendet oder nach 5-maliger Falscheingabe des Validierungscode, wird der Zertifikatsbeantragungsprozess beendet und der Vorgang muss erneut durchgeführt werden.

- Nach erfolgreicher Authentifizierung und E-Mail-Validierung werden von der Volksverschlüsselungs-Software auf dem Rechner des Endteilnehmers die jeweiligen Schlüsselpaare für Verschlüsselung, Signatur und Authentifizierung generiert. Für jeden öffentlichen Schlüssel wird ein PKCS#10-Zertifikats-Request generiert und mit dem dazugehörigen privaten Schlüssel signiert. Außerdem wird vom Endteilnehmer die Einwilligung zur Veröffentlichung seines Verschlüsselungszertifikats im Verzeichnisdienst (vgl. Abschnitt 2.1) eingeholt.

- Die Zertifikats-Requests werden zusammen mit der Einwilligung zur Zertifikatsveröffentlichung gemäß [REST-API] an die zentrale Registrierungsinstanz der Zertifizierungsstelle übermittelt.

- Nach erfolgreicher Überprüfung der Authentizität der Zertifikats-Requests (vgl. Abschnitt 3.2.1) werden diese zusammen mit den persönlichen Daten des Zertifikatsinhabers (vgl. Abschnitt 3.2.2) an die CA übermittelt.

## 4.2 Bearbeitung von Zertifikatsaufträgen

### 4.2.1 Durchführung der Identifikation und Authentifizierung

Die Identifikation und Authentifizierung des Zertifikatsantragstellers wird gemäß Abschnitt 3.2 von der zuständigen Registrierungsstelle (RA) durchgeführt.

### 4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Zertifikatsanträge (Zertifikats-Requests) werden an die der Zertifizierungsstelle zugeordnete Registrierungsstelle gerichtet-

Ein Anspruch auf Zertifikatsannahme besteht nicht. Ein Zertifikatsantrag wird von der zuständigen Registrierungsstelle angenommen, wenn alle Arbeitsschritte gemäß Abschnitt 4.1.2 erfolgreich durchlaufen wurden.

Andernfalls wird der Zertifikatsantrag abgewiesen. Eine Ablehnung eines Zertifikatsantrags kann auch erfolgen, wenn die angegebene E-Mail-Adresse anstößig erscheint.

### 4.2.3 Bearbeitungsdauer von Zertifikatsanträgen

Mit Bearbeitungsdauer ist hier der Zeitraum nach Eingang des Zertifikats-Request bei der Registrierungsstelle bis zur Bereitstellung der Zertifikate auf dem Download-Server der Volksverschlüsselungs-PKI (vgl. Abschnitt 4.4) zu verstehen.

Die Bearbeitung des Zertifikatsantrags beginnt in einem angemessenen Zeitrahmen nach Erhalt der Beauftragung.

## 4.3 Ausstellung von Zertifikaten

### 4.3.1 Vorgehen der Zertifizierungsstelle

Nach erfolgreicher Durchführung des Registrierungsprozesses (vgl. Abschnitt 4.1.2) werden die Zertifikats-Requests an die entsprechende Zertifizierungsstelle übermittelt. Auf Basis der Zertifikats-Requests werden die jeweiligen Zertifikate erstellt. Die ausgestellten Zertifikate werden persistent gespeichert und an die entsprechende Registrierungsstelle der Zertifizierungsstelle zur Ausgabe an die Endteilnehmer übermittelt.

### 4.3.2 Benachrichtigung des Zertifikatsinhabers

Die Zertifikate werden auf dem Download-Server der Volksverschlüsselungs-PKI zur Abholung bereitgestellt. Der Zertifikatsinhaber erhält an seine angegebene E-Mail-Adresse eine Benachrichtigung, dass die Zertifikate zum Download bereitstehen und innerhalb einer Woche abgeholt werden müssen.

## 4.4 Auslieferung der Zertifikate

### 4.4.1 Annahme der Zertifikate

Nachdem die Zertifikate erzeugt wurden, stehen diese auf einem Server der Volksverschlüsselungs-PKI bereit und können vom Zertifikatsinhaber mit Hilfe der Volksverschlüsselungs-Software abgeholt werden. Die Volksverschlüsselungs-Software installiert die Schlüssel und Zertifikate auf dem Rechner des Endteilnehmers und unterstützt ihn bei der Konfiguration der E-Mail-Programme, Browser und anderer kryptographischer Anwendungen, die auf seinem Rechner installiert sind.

Werden die Zertifikate innerhalb einer Frist von 8 Tagen nicht abgeholt, werden sie gesperrt und aus dem Verzeichnisdienst gelöscht, falls der Endnutzer bei der Zertifikatsbeantragung der Veröffentlichung zugestimmt hatte.

Nach Erhalt der Zertifikate muss der Zertifikatsinhaber die Korrektheit der Einträge in seinen Zertifikaten (z.B. SubjectDN) überprüfen. Bei fehlerhaften Zertifikaten muss der Zertifikatsinhaber für diese unverzüglich die Sperrung veranlassen (vgl. Abschnitt 4.9).

### 4.4.2 Veröffentlichung der Zertifikate

Die ausgestellten Endteilnehmer-Zertifikate werden gemäß Abschnitt 2.1 im Verzeichnisdienst veröffentlicht, wenn der Zertifikatsinhaber hierzu seine Einwilligung erteilt hat (vgl. Abschnitt 4.1.2).

### 4.4.3 Benachrichtigung weiterer Instanzen

Es werden keine weiteren Instanzen benachrichtigt.

## 4.5 Nutzung des Schlüsselpaares und des Zertifikats

### 4.5.1 Nutzung durch den Zertifikatsinhaber

Der private Schlüssel bzw. das dazugehörige Zertifikat der **Volksverschluesselung Private CA** darf nur in Anwendungen benutzt werden, die in Übereinstimmung mit den im Zertifikat angegebenen Schlüsselverwendungszwecken stehen. Der Zertifikatsinhaber hat sicher zu stellen, dass Zertifikate und dazugehörige Schlüssel nur zu privaten Zwecken verwendet werden ((vgl. Abschnitt 1.4.1).

Bei Verlust oder Missbrauch des Zertifikats ist unverzüglich eine Sperrung durch den Zertifikatsinhaber zu veranlassen. Dies gilt auch bei Verdacht eines Missbrauchs oder einem Verdacht auf Kompromittierung der zugehörigen Schlüssel.

Da der Zertifikatsinhaber die alleinige Kontrolle über den privaten Schlüssel hat, hat er Sorge zu tragen, dass dieser angemessen gegen Diebstahl, Missbrauch und Verlust geschützt ist. Der Zertifikatsinhaber verpflichtet sich, seinen privaten Schlüssel keinem Dritten zu übergeben oder offen zu legen.

Wenn der private Schlüssel abhandenkommt, gestohlen wird oder eine Kompromittierung nicht ausgeschlossen werden kann, sollte der Zertifikatsinhaber unverzüglich die Sperrung des Zertifikats (vgl. Abschnitt 4.9) veranlassen.

### 4.5.2 Nutzung durch Zertifikatsnutzer

Jeder Zertifikatsnutzer (vgl. Abschnitt 1.3.4), der ein Zertifikat der Volksverschlüsselungs-PKI zur Verschlüsselung, zur Validierung einer Signatur oder zu Zwecken der Authentifizierung verwendet, sollte

- sicherstellen, dass die Nutzung des Zertifikats auf Basis dieser VV-X.509-CP/CPS den Anforderungen des jeweiligen Anwendungsbereichs entspricht und der Verwendungszweck den im Zertifikat enthaltenen Schlüsselverwendungszwecken (*KeyUsage*) nicht widerspricht (vgl. Abschnitt 1.4),
- vor der Nutzung des Zertifikats die darin enthaltenen Informationen auf Richtigkeit überprüfen,
- vor der Nutzung des Zertifikats dessen Gültigkeit prüfen, in dem er unter anderem den Gültigkeitszeitraum des Zertifikats und die gesamte Zertifikatskette bis zum Wurzelzertifikat validiert und die Sperrinformationen (CRL, OCSP) überprüft.

Es liegt ausschließlich in der Verantwortung des Zertifikatsnutzers darüber zu entscheiden, ob ein Zertifikat für einen bestimmten Zweck geeignet ist.

## 4.6 Zertifikatserneuerung ohne Schlüsselwechsel (Re-Zertifizierung)

Bei einer Zertifikatserneuerung ohne Schlüsselwechsel handelt es sich um das Ausstellen eines neuen Zertifikats mit neuer Gültigkeitsdauer für einen bereits zertifizierten öffentlichen Schlüssel.

Eine Zertifikatserneuerung ohne Schlüsselwechsel wird für Zertifikate der „**Volkverschlüsselung Private CA" nicht** unterstützt.

## 4.7 Zertifikatserneuerung mit Schlüsselwechsel (Re-Key)

Die Schlüsselerneuerung von Zertifikaten bedeutet, dass ein Zertifikatsinhaber, der bereits Zertifikate besitzt oder nutzt, für neu generierte Schlüsselpaare neue Zertifikate beantragt, wobei die im Zertifikat enthaltenen Informationen des Zertifikatsinhabers unverändert bleiben.

Eine erneute Zertifizierung vor Ablauf der Gültigkeit der Zertifikate erfordert, dass der Zertifikatsinhaber zuvor seine Zertifikate sperrt (vgl. Abschnitt 4.9). Eine automatische Sperrung durch die **Volkverschlüsselung Private CA** erfolgt nicht.

Die durchzuführenden Prozessschritte entsprechen denen der Erstbeantragung und es gelten die Regelungen unter Abschnitt 3.2 und 4.1ff.

## 4.8 Änderung von Zertifikatsinhalten

Wenn sich Zertifikatsinhalte, wie der Name oder die E-Mail-Adresse, vor Ablauf der Gültigkeit der Zertifikate ändern, sollte der Zertifikatsinhaber neue Zertifikate für neue Schlüsselpaare beantragen. Es werden keine Änderungen an bereits ausgestellten Zertifikaten vorgenommen. Die durchzuführenden Prozessschritte entsprechen denen der Erstbeantragung und es gelten die Regelungen unter Abschnitt 3.2 und 4.1ff. Bleibt die E-Mail-Adresse unverändert, muss der Zertifikatsnehmer vor der Beantragung seine Zertifikate sperren.

## 4.9 Sperrung und Suspendierung von Zertifikaten

### 4.9.1 Gründe für die Sperrung

Der Zertifikatsinhaber sollte vor Ablauf der Zertifikatsgültigkeit eine Zertifikatssperrung und deren Veröffentlichung in der Sperrliste (CRL) veranlassen, wenn einer der folgenden Gründe vorliegt:

1. der private Schlüssel wurde kompromittiert, ist abhandengekommen (z.B. Verlust oder Diebstahl des Schlüsselträgers) oder nicht mehr nutzbar,

2. ein Missbrauch oder der Verdacht auf Missbrauch des privaten Schlüssels liegt vor,

3. die Angaben im Zertifikat sind fehlerhaft oder nicht mehr korrekt (z.B. Namensänderung bei Heirat),

4. das Zertifikat wird nicht mehr benötigt.

Die Zertifizierungsstelle behält sich das Recht vor, ein Zertifikat (CA-Zertifikat oder Endteilnehmer-Zertifikat) automatisch in folgenden Fällen zu sperren:

1. Die E-Mail-Adresse in einem Zertifikat erscheint anstößig.

2. Das Zertifikat der Zertifizierungsstelle wurde kompromittiert.

3. Die verwendeten kryptographischen Algorithmen oder zugehörige Parameter, mit denen die Zertifikate ausgestellt wurden, können aufgrund technologischer Fortschritte oder neuen Entwicklungen in der Kryptologie nicht mehr die notwendige Sicherheit gewährleisten.

4. Die Volksverschlüsselungs-PKI stellt den Zertifizierungsdienst ein.

### 4.9.2 Wer kann eine Sperrung veranlassen?

Zertifikatsinhaber können die Sperrung ihrer eigenen Zertifikate jederzeit ohne Angabe eines Sperrgrundes veranlassen.

In bestimmten Fällen (vgl. Abschnitt 4.9.1) ist die Volksverschlüsselungs-PKI berechtigt, ohne Zustimmung der Zertifikatsinhaber Endteilnehmer-Zertifikate zu sperren.

### 4.9.3 Verfahren zur Sperrung

Ein Zertifikatsinhaber kann die Sperrung seiner Zertifikate mit Hilfe der Volksverschlüsselungs-Software veranlassen.

Hierfür muss er die E-Mail-Adresse eingeben, die bei Zertifikatsausstellung im Attribut *SubjectAltName* eingetragen wurde, um das zu sperrende Zertifikat selektieren zu können. Es werden immer alle drei Zertifikate des Zertifikatsinhabers mit gleicher E-Mail-Adresse gesperrt.

Die Authentifizierung einer Sperrung erfolgt über ein in Abschnitt 3.4 beschriebenes Verfahren.

Nach erfolgreicher Authentifizierung werden für die ausgewählten Zertifikate die Sperranträge von der RA generiert und an die ausstellende Zertifizierungsinstanz übermittelt.

Gesperrte Zertifikate erscheinen in der Sperrliste (CRL), die einmal täglich sowie nach jedem Sperrvorgang erneuert wird (vgl. Abschnitt 2.3). Veröffentlichte Zertifikate werden nach der Sperrung aus dem Verzeichnisdienst (vgl. Abschnitt 2.1) entfernt.

Der Zertifikatsinhaber wird über die Sperrung seiner Zertifikate per E-Mail informiert.

Die Sperrung eines Zertifikats ist endgültig. Ein Zertifikat kann nach einer Sperrung nicht wieder aktiviert werden.

### 4.9.4 Fristen für den Zertifikatsinhaber

Der Zertifikatsinhaber muss in eigener Verantwortung dafür sorgen, dass er bei bekannt werden einer oder mehrerer der in Abschnitt 4.9.1 genannten Gründe die Sperrung veranlasst.

### 4.9.5 Bearbeitungszeit für Sperranträge

Eine Sperrung von Endteilnehmer-Zertifikaten erfolgt in der Regel unverzüglich nach Eingang eines Sperrantrags.

### 4.9.6 Prüfung des Zertifikatsstatus durch Zertifikatsnutzer

Zertifikatsnutzer sollten sich auf den Inhalt eines Zertifikats der Volksverschlüsselungs-PKI nur dann verlassen, wenn Sie zuvor den Zertifikatsstatus geprüft haben. Zertifikatsnutzer können dem Zertifikat vertrauen, wenn dieses nicht abgelaufen oder gesperrt ist.

Der Sperrstatus kann über die aktuellen Sperrlisten (CRLs) geprüft werden, die über die in Abschnitt 2.1 angegebenen Adressen abgerufen werden können.

Zusätzlich steht ein OCSP-Responder zur Verfügung (vgl. Abschnitt 4.10).

### 4.9.7 Veröffentlichungsfrequenz von Sperrlisten

Die Sperrliste für Endteilnehmer-Zertifikate der „**Volksverschluesselung Private CA"** wird mindestens alle 24 Stunden erzeugt und veröffentlicht. Wird ein Endteilnehmer-Zertifikat gesperrt wird umgehend eine neue CRL erstellt und veröffentlicht.

Die CRL (Sperrliste) der **Root-CA** für Sub-CA-Zertifikate wird mindestens alle 124 Tage erzeugt und veröffentlicht. Bei Sperrung einer Sub-CA wird umgehend eine neue CRL erstellt und veröffentlicht.

### 4.9.8 Maximale Latenzzeit für Sperrlisten

Sperrlisten (CRLs) werden innerhalb von 24 Stunden nach ihrer Erstellung veröffentlicht.

### 4.9.9 Verfügbarkeit von Online-Sperrinformationen

Für den Abruf von Sperrinformationen steht zusätzlich ein OCSP-Responder zur Verfügung (vgl. Abschnitte 2.1 und 4.10).

### 4.9.10 Anforderungen an Online-Sperrinformationen

Vgl. Abschnitt 4.10.

### 4.9.11 Andere Formen der Veröffentlichung von Sperrinformationen

Keine.

### 4.9.12 Spezielle Anforderungen bei Kompromittierung privater Schlüssel

Bei einer Kompromittierung des privaten Schlüssels der Root-CA oder CA werden neben dem CA-Zertifikat auch alle von ihr ausgestellten Zertifikate gesperrt.

### 4.9.13 Gründe für die Suspendierung

Eine Suspendierung (vorläufige Sperrung) von Zertifikaten wird **nicht** unterstützt. Einmal gesperrte Zertifikate können nicht reaktiviert werden.

## 4.10 Statusabfragedienst für Zertifikate (OCSP)

Die Volksverschlüsselungs-PKI betreibt einen öffentlich zugänglichen OCSP-Responder für die Abfrage des Sperrstatus von Endteilnehmer-Zertifikaten. Die OCSP-Responder (erfüllt die Anforderungen des RFC 6960[1] [RFC6960]. Für weitere Informationen siehe Abschnitte 7.2 und 7.3.

### 4.10.1 Funktionsweise des Statusabfragedienstes

Der OCSP-Responder ist über die in Abschnitt 2.1 angegebene Adresse erreichbar.
Für weitere Informationen siehe Abschnitte 7.2 und 7.3.

### 4.10.2 Verfügbarkeit des Statusabfragedienstes

Generell ist der OCSP-Responder zu jeder Zeit nutzbar. Er ist aber nicht hochverfügbar ausgelegt.

## 4.11 Ende der Zertifikatsnutzung

Die Gültigkeit eines Zertifikats endet mit dem im Zertifikat vermerkten Datum oder durch vorzeitige Sperrung.

## 4.12 Schlüsselhinterlegung und- wiederherstellung

Wird **nicht** unterstützt.

[1] Seit 2013 löst der RFC 6960 den RFC 2560 durch ab.

# 5 Physikalische, organisatorische und personelle Sicherheitsmaßnahmen

Die Volksverschlüsslungs-PKI wird als Kooperation zwischen dem Fraunhofer-SIT und der Deutschen Telekom AG von der Deutschen Telekom AG in einem nach ISO 27001 zertifiziertem Rechenzentrum in Deutschland betrieben.

## 5.1 Infrastrukturelle Sicherheitsmaßnahmen

### 5.1.1 Standort

Das nach ISO 27001 zertifizierte Rechenzentrum, in dem die technischen Systeme der Volksverschlüsselungs-PKI betrieben werden, bietet hinsichtlich der infrastrukturellen Sicherheitsmaßnahmen einen ausreichenden Schutz.

### 5.1.2 Zutritts- und Zugangskontrolle

Geeignete Maßnahmen zur Zutritts- und Zugangskontrolle gewährleisten einen hohen Schutz gegen unbefugtes Eindringen in die einzelnen Betriebsräume und unbefugten Zugriff auf die betriebenen Systeme und Daten. Der Zutritt zu den Betriebsräumen ist nur autorisierten Mitarbeitern möglich. Die Systeme der Zertifizierungsstellen sind von den Systemen der Registrierungsstelle getrennt und befinden sich in verschiedenen technischen Sicherheitszonen.

Die technischen Maßnahmen werden durch organisatorische Maßnahmen ergänzt, die Zutrittsregelungen für Mitarbeiter und Dritte (Besucher, Fremdpersonal) enthalten.

### 5.1.3 Stromversorgung und Klimatisierung

Das Rechenzentrum ist durch geeignete Maßnahmen gegen Stromausfälle abgesichert. Eine Klimatisierung der Räume und IT-Systeme ist vorhanden.

### 5.1.4 Schutz vor Wasserschäden

Das Rechenzentrum ist durch bauliche Maßnahmen vor Wassereinbrüchen gesichert.

### 5.1.5 Brandschutz

Die Richtlinien für den Brandschutz werden eingehalten. Das Rechenzentrum ist mit Brandmelde- und Feuerlöschanlagen ausgestattet.

### 5.1.6 Aufbewahrung von Datenträgern

Datenträger werden in verschlossenen Räumen oder Schränken aufbewahrt. Datenträger mit besonders kritischen Informationen (beispielsweise HSM-Backups) werden ausschließlich in Tresorschränken aufbewahrt.

### 5.1.7 Entsorgung

Vertrauliche Dokumente werden vor ihrer Entsorgung physisch zerstört.

Datenträger, auf denen vertrauliche Informationen gespeichert sind, werden vor ihrer Entsorgung derart behandelt, dass ein Auslesen oder Wiederherstellen der Daten nicht möglich ist. Kryptographische Hardware-Sicherheitsmodule werden vor ihrer Entsorgung gemäß den Herstellerrichtlinien physisch zerstört. Dies gilt für alle Krypto-Hardwaremodule unabhängig von ihrer technischen Ausprägung.

### 5.1.8 Datensicherung

Es werden von allen PKI-Systemen regelmäßig Sicherungskopien erstellte. Sicherungsdatenträger werden räumlich getrennt aufbewahrt.

## 5.2 Organisatorische Maßnahmen

### 5.2.1 Vertrauenswürdige Rollen

Sämtliche Tätigkeiten, die Auswirkungen auf die Sicherheit des Betriebes der Volksverschlüsselungs-PKI haben können, werden zu Rollen zusammengefasst. Diese Tätigkeiten dürfen ausschließlich von Personen durchgeführt werden, denen die entsprechenden Rollen zugewiesen sind. Personen in vertrauenswürdigen Rollen erfüllen die unter Abschnitt 5.3 beschriebenen Anforderungen.

Das Rollenmodell umfasst die in der folgenden Tabelle definierten Rollen. Es ist möglich, eine Rolle auf mehrere Mitarbeiter zu verteilen. Ebenso kann ein Mitarbeiter in mehr als einer Rolle auftreten, dabei sind jedoch die Anforderungen aus Abschnitt 5.2.4 zu beachten.

| Rolle | Aufgabe | Kürzel |
|---|---|---|
| Management | Gesamtverantwortung für die Volksverschlüsselungs-PKI. | Mgt |
| System-Administratoren | Autorisiert und verantwortlich für die Installation, Konfiguration, Administration und Wartung der IT- und Kommunikationssysteme. | SA |
| System-Operatoren | Autorisiert und verantwortlich für den operativen Betrieb der PKI-Systeme. Durchführung der Datensicherung und –wiederherstellung der erforderlichen PKI-Server und der Anwendungssoftware. Verwaltung der HSMs. | SO |
| RA-Mitarbeiter | Autorisiert und verantwortlich für die Identifizierung und Authentifizierung der Endteilnehmer im Rahmen der Registrierung sowie für die Zertifikatssperrung und den Widerruf im Verzeichnis, sofern diese Prozesse nicht automatisch vom Endteilnehmer durchgeführt werden können. | RO |
| Sicherheitsbeauftragter | Verantwortlich für die Einhaltung der Sicherheitsbestimmungen, insbesondere der im CPS festgelegten Grundsätze. | ISO |
| Auditor | Durchführung betriebsinterner Audits; Überwachung und Einhaltung der Datenschutzbestimmungen. | A |
| Entwickler | Verantwortlich für die Entwicklung von PKI-Systemen. | DEV |

### 5.2.2 Anzahl der für eine Tätigkeit erforderlichen Personen

Die Aufrechterhaltung des Betriebes der Volksverschlüsselungs-PKI wird von fachkundigen und vertrauenswürdigen Mitarbeitern wahrgenommen.

Besonders sicherheitskritische Vorgänge, wie z.B. die Wiederherstellung von CA-Schlüsseln und der Widerruf von CA-Zertifikaten, werden im Vier-Augen-Prinzip durchgeführt, das durch technische oder organisatorische Maßnahmen umgesetzt wird.

### 5.2.3 Identifizierung und Authentifizierung von Rollen

Die Identifizierung und Authentisierung der berechtigten Benutzer wird beim technischen Zugang zu den IT-Systemen mit Benutzerkennung und Passwort oder einem stärkeren Verfahren realisiert. Die Passwörter genügen den Sicherheitsanforderungen nach ISO 27001.

Arbeiten an Hardware-Sicherheitsmodulen (HSM) sind besonderen Authentifizierungsverfahren unterworfen.

### 5.2.4 Trennung von Aufgaben

Folgende Aufgaben werden von verschiedenen Personen wahrgenommen:

- Management
- PKI-Betrieb
- Entwickler
- Sicherheitsbeauftragter
- Auditor

## 5.3 Personelle Sicherheitsmaßnahmen

### 5.3.1 Anforderungen an Qualifikation und Erfahrungen

Für die Volksverschlüsselungs-PKI werden ausschließlich Mitarbeiter eingesetzt, die alle notwendigen Anforderungen an Vertrauenswürdigkeit, Integrität, Zuverlässigkeit und Qualifizierung erfüllen. Sie verfügen über die erforderlichen IT-Kenntnisse und besitzen Fachkenntnisse in den Bereichen Public Key Infrastrukturen, IT-Sicherheit, Datenschutz, Kryptographie, Server-Administration und Netzwerkinfrastruktur.

### 5.3.2 Sicherheitsüberprüfung

Es gelten die allgemeinen Personaleinstellungsrichtlinien der Fraunhofer Gesellschaft und der Deutschen Telekom AG.

### 5.3.3 Schulung

Für den Betrieb der Volksverschlüsselungs-PKI werden ausschließlich qualifizierte Mitarbeiter eingesetzt. Sie erfüllen alle Anforderungen, die zur kompetenten Erfüllung Ihrer beruflichen Pflichten erforderlich sind.

Neue Mitarbeiter im Bereich der Volksverschlüsselungs-PKI werden vor Aufnahme ihrer Tätigkeit durch Schulungen / Einweisungen durch Kollegen eingearbeitet und hinsichtlich der Sicherheitsrelevanz ihrer Arbeit sensibilisiert.

### 5.3.4 Häufigkeit von Schulungen

Mitarbeiter, die für den Betrieb der Volksverschlüsselungs-PKI eingesetzt werden, werden von Fraunhofer SIT bei Bedarf geschult.

### 5.3.5 Arbeitsplatzrotation / Rollenumverteilung

Nicht vorgesehen.

### 5.3.6 Maßnahmen bei unautorisierten Handlungen

Bei unautorisierten Handlungen, die die Sicherheit der Volksverschlüsselungs PKI gefährden oder gegen Datenschutzbestimmungen verstoßen, werden angemessene Maßnahmen ergriffen.

## 5.4 Sicherheitsüberwachung

### 5.4.1 Aufgezeichnete Ereignisse

Zur Abwehr von Angriffen und zur Kontrolle der ordnungsgemäßen Funktion der Zertifizierungsstellen der Volksverschlüsselung werden auf den technischen Systemen u.a. folgende Ereignisse erfasst:

- Alle Ereignisse im Lebenszyklus von CA-Schlüsseln und CA-Zertifikaten (Erstellung, Sicherung, Speicherung, Wiederherstellung, Sperrung und Vernichtung)
- Erzeugung, Auslieferung und Sperrung von Endteilnehmer-Zertifikaten
- Erzeugung und Veröffentlichung von Sperrlisten(CRL) und OCSP-Einträgen
- Fehlgeschlagene Login-Versuche

### 5.4.2 Häufigkeit der Protokollanalyse

Die Protokolldaten werden bei Verdacht auf sicherheitskritische Ereignisse umgehend sowie im Rahmen von internen Audits überprüft.

### 5.4.3 Aufbewahrungsfrist von Protokolldaten

Die Daten, die den Lebenszyklus der Zertifikate dokumentieren (insbesondere Protokolldaten der CA-Systeme) werden bis zum Ablauf der Gültigkeitsdauer des Zertifikats der ausstellenden CA aufbewahrt, zuzüglich einem Jahr.

### 5.4.4 Schutz von Protokolldaten

Elektronische Protokolldaten werden mit Mitteln des Betriebssystems gegen unbefugten Zugriff, Manipulation und Löschung geschützt.

### 5.4.5 Backup der Protokolldaten

Protokolldaten werden zusammen mit anderen relevanten Daten der Volksverschlüsselungs-PKI einem regelmäßigen Backup unterzogen.

### 5.4.6 Protokollierungssystem (intern oder extern)

Protokolldaten werden auf Anwendungs-, Betriebssystem- und Netzwerkebene automatisch erzeugt und aufgezeichnet.

### 5.4.7 Benachrichtigung bei sicherheitskritischen Ereignissen

Bei Eintreten von sicherheitskritischen Ereignissen wird umgehend das Management der Volksverschlüsselungs-PKI informiert. Es werden notwendige Maßnahmen festgelegt, um auf die Ereignisse adäquat reagieren zu können, ggf. wird die Geschäftsleitung informiert.

### 5.4.8 Schwachstellenbewertung

Eine Schwachstellenbewertung findet durch die Mitarbeiter der Volksverschlüsselungs-PKI selbst bzw. durch den Hersteller der verwendeten Software statt. Bei signifikanten Anwendungs-Upgrades wird ein Penetrationstest durchgeführt.

## 5.5 Archivierung

### 5.5.1 Archivierte Daten

Folgende Informationen werden archiviert:

- alle Ereignisse, die den Lebenszyklus der CA-Schlüssel betreffen,
- alle ausgegebenen Zertifikate, einschließlich gesperrter und abgelaufener Zertifikate;
- Sperrlisten (CRL),
- Widerruf der Einwilligung zur Veröffentlichung der E-Mail-Adresse und des öffentlichen Zertifikats,
- Registrierungsformulare von Endteilnehmern.

### 5.5.2 Aufbewahrungszeitraum

Es gelten die Regelungen in Abschnitt 5.4.3.

### 5.5.3 Schutz der archivierten Daten

Die Daten sind durch geeignete Maßnahmen vor unbefugter Einsichtnahme, Manipulation und Vernichtung geschützt.

### 5.5.4 Sicherung der archivierten Daten

Die in Abschnitt 5.4.1 und 5.5.1 aufgeführten Daten werden regelmäßig im Rahmen eines Backups gesichert.

### 5.5.5 Anforderungen an Zeitstempel von archivierten Daten

Archivierte Daten werden nicht mit Zeitstempel versehen.

### 5.5.6 Internes / externes Archivierungssystem

Es wird ein internes Archivierungssystem verwendet.

### 5.5.7 Verfahren zur Beschaffung und Überprüfung von Archivdaten

Nur autorisiertes und vertrauenswürdiges Personal darf auf die Archivdaten zugreifen.

## 5.6 Schlüsselwechsel

Zertifikat und dazugehöriges Schlüsselpaar für eine Zertifizierungsstelle wird rechtzeitig vor Ablauf der Gültigkeit gewechselt, so dass die Gültigkeitsdauer der von der CA ausgestellten Zertifikate nicht die Gültigkeitsdauer des CA-Zertifikates übersteigt. Die Gültigkeitsdauer von Schlüsseln ist in Abschnitt 6.3.2 festgelegt. Bei einem regulären CA-Schlüsselwechsel erfolgt keine Sperrung des CA-Zertifikates. Nach dem Schlüsselwechsel werden keine weiteren Zertifizierungen mehr mit dem alten Schlüsselpaar durchgeführt.

Ein außerordentlicher CA-Schlüsselwechsel findet in den folgenden Fällen statt:

- es besteht der Verdacht, dass der private Schlüssel kompromittiert wurde (es gelten die Regelungen in Abschnitt 5.7.3),
- die dem Schlüsselpaar zugeordneten Algorithmen oder die verwendete Schlüssellänge bieten nach aktuellem Wissensstand für den vorgesehen Nutzungszeitraum keine ausreichende Sicherheit mehr.

Bei einem außerordentlichen Schlüsselwechsel wird das entsprechende CA-Zertifikat gesperrt. Die Sperrung hat zur Folge, dass auch alle Zertifikate gesperrt werden, die von dieser CA ausgestellt wurden.

Neue CA-Zertifikate und ihre Fingerprints werden gemäß Abschnitt 2.1 veröffentlicht.

Abgelaufene oder gesperrte CA-Zertifikate stehen weiterhin zur Validierung auf der Webseite (vgl. Abschnitt 2.1) zur Verfügung.

## 5.7 Kompromittierung und Wiederherstellung

### 5.7.1 Prozeduren bei Sicherheitsvorfällen und Kompromittierungen

Wird ein sicherheitsrelevanter Vorfall im Zusammenhang mit der Volksverschlüsselungs-PKI registriert, so werden diese unmittelbar an das Management der Volksverschlüsselungs-PKI eskaliert. Danach muss gemäß den von Fraunhofer SIT definierten Prozeduren zur Behandlung von Sicherheitsvorfällen und bei Kompromittierung von privaten CA-Schlüsseln weiter verfahren werden. Die Grundzüge der Prozeduren sind in den folgenden Abschnitten aufgeführt.

### 5.7.2 Wiederherstellung von IT-Ressourcen

Werden innerhalb der Volksverschlüsselungs-PKI fehlerhafte oder manipulierte Rechner, Software und/oder Daten festgestellt, die gravierende Auswirkungen auf den Betrieb der Zertifizierungsstellen haben, wird der Betrieb des entsprechenden Systems unverzüglich eingestellt. Das System wird ggf. auf einer Ersatz-Hardware unter Wiederherstellung der Software und der Daten aus der Datensicherung neu aufgesetzt und nach Überprüfung in den Betrieb übernommen.

Anschließend wird die fehlerhafte IT-Ressource analysiert und es erfolgt eine Bewertung der Sicherheit. Gegebenenfalls werden zusätzliche Abwehrmaßnahmen zur Vermeidung von ähnlichen Vorfällen ergriffen.

Falls sich in einem Zertifikat fehlerhafte Angaben befinden wird der Zertifikatsinhaber unverzüglich informiert und das Zertifikat gesperrt. Bei Verdacht einer vorsätzlichen Handlung Sicherheitsvorfalls werden die notwendigen Schritte eingeleitet.

### 5.7.3 Kompromittierung privater Schlüssel von Zertifizierungsstellen

Wird der private Schlüssel einer Zertifizierungsstelle kompromittiert oder besteht ein begründeter Verdacht auf eine Kompromittierung wird der Vorfall unmittelbar untersucht, beurteilt und die notwendigen Schritte eingeleitet.

Falls erforderlich werden das CA-Zertifikat (das Root-CA-Zertifikat ist natürlich ausgenommen) sowie alle von dieser Zertifizierungsstelle ausgestellten und bisher noch nicht abgelaufenen Zertifikate gesperrt, die entsprechenden Sperrlisten generiert und gemäß Abschnitt 2.1 veröffentlicht. Gegebenenfalls werden der Verzeichnisdienst und der OCSP-Responder abgeschaltet, um inkorrekte oder ungültige Aussagen durch die Dienste zu verhindern.

Die Sperrung eines CA-Zertifikats wird auf der Web-Seite https://volksverschluesselung.de veröffentlicht.

Für die betroffene CA wird unter Berücksichtigung der Gründe für die Kompromittierung, ein Zertifikat mit neuem Schlüsselpaar generiert (vgl. Abschnitt 5.6).

### 5.7.4 Wiederaufnahme des Betriebs nach einer Katastrophe (Business Continuity)

Eine Wiederaufnahme des Zertifizierungsbetriebs nach einer Katastrophe natürlichen oder menschlichen Ursprungs ist Bestandteil des nicht öffentlichen Notfallplans des Rechenzentrums. In einem Notfall entscheiden die für die Volksverschlüsselungs-PKI verantwortlichen Stellen je nach Art des Vorfalls, ob ein Recovery des in Abschnitt 6.2.4 beschriebenen Backups der CA durchgeführt oder bei Kompromittierung gemäß Abschnitt 5.7.3 verfahren wird.

## 5.8 Einstellung der Zertifizierungsdienste

Falls der Betrieb einer Zertifizierungsstelle der Volksverschlüsselungs-PKI eingestellt werden muss, werden im Rahmen eines Beendigungsplanes u.a. folgende Maßnahmen ergriffen:

- Sperrung aller noch gültigen und von der betroffenen CA ausgestellten Zertifikate.
- Zerstörung der privaten Schlüssel der betroffenen CA.
- Veröffentlichung der Einstellung des Betriebes auf der Web-Seite https://volksverschluesselung.de.
- Information aller Teilnehmer der Volksverschlüsselungs-PKI (Zertifikatsinhaber, Registrierungsstelle, vertrauende Dritte).
- Aufbewahrung der Archive und Unterlagen der CA bis zum zugesicherten Aufbewahrungszeitraum (vg. Abschnitt 5.4.3 und 5.5.2).
- Bereitstellung der Sperrlisten und Zertifikatssperrinformationen bis zum Ende der Zertifikatsgültigkeit der Zertifizierungsstelle.

# 6 Technische Sicherheitsmaßnahmen

## 6.1 Erzeugung und Installation von Schlüsselpaaren

### 6.1.1 Erzeugung von Schlüsselpaaren

Die Schlüsselpaare der Zertifizierungsstellen werden in einem kryptographischen Hardware-Sicherheitsmodul erzeugt und gespeichert (vgl. Abschnitt 6.2).

Im Kontext der „**Volksverschluesselung Private CA“** werden die Schlüsselpaare für Endteilnehmer-Zertifikate von der Volksverschlüsselungs-Software auf dem Endgerät des Nutzers erzeugt. Die privaten Schlüssel bleiben in der alleinigen Verfügungsgewalt des Nutzers. Ausschließlich die öffentlichen Schlüssel werden zur Zertifizierung an die Zertifizierungsstelle übermittelt. Es wird sichergestellt, dass der im Zertifikat hinterlegte öffentliche Schlüssel zu dem auf dem Endgerät des Nutzers gespeicherten privaten Schlüssel gehört (vgl. Abschnitt 3.2.1).

### 6.1.2 Übermittlung privater Schlüssel an den Zertifikatsinhaber

Entfällt im Kontext der „**Volksverschluesselung Private CA“**, da die privaten Schlüssel auf dem Rechner des Zertifikatsinhabers generiert werden.

### 6.1.3 Übermittlung öffentlicher Schlüssel an den Zertifikatsaussteller

Die Übermittlung des öffentlichen Schlüssels erfolgt mittels der Volksverschlüsselungs-Software über einen PKCS#10-Zertifikats-Request in einer durch Transport Layer Security (TLS) gesicherten Sitzung (vgl. Abschnitt 3.2.1).

### 6.1.4 Übermittlung öffentlicher CA Schlüssel an Zertifikatsnutzer (vertrauende Dritte)

Die öffentlichen Schlüssel der „**Volksverschluesselung Root CA“** und der „**Volksverschluesslung Private CA“** sowie die dazugehörigen Fingerprint sind gemäß Abschnitt 2.1 veröffentlicht und abrufbar.

### 6.1.5 Schlüssellängen

Die eingesetzten Schlüssellängen und Algorithmen entsprechen dem aktuellen Stand der Technik und Kryptographie und berücksichtigen die Technischen Richtlinien TR-02102-1 des BSI [BSI TR-02102-1]. Es wird sichergestellt, dass die Schlüssel innerhalb des Verwendungszeitraums über eine ausreichende Länge verfügen.

Für die „**Volksverschluesselung Root CA“** und die „**Volksverschluesselung Private CA“** werden RSA-Schlüssel mit einer Mindestlänge von 4096 Bit verwendet.

Für Endteilnehmer-Zertifikate akzeptiert die „**Volksverschluesselung Private CA“** Schlüssel von 2048 Bit Schlüssellänge.

### 6.1.6 Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle

Im Rahmen der Zertifikatsbeauftragung wird der von einem Endteilnehmer mit einem PKCS#10-Zertifikatsrequest (CSR) eingereichte öffentliche Schlüssel auf folgende Qualitätsparameter geprüft:

- für die Erzeugung wurde das RSA-Kryptoverfahren verwendet (Public-Key Typ ist "RSA encryption" - OID=1.2.840.113549.1.1.1)
- die Länge für den RSA-Schlüssel beträgt 2048 Bit

- der CSR wurde mit dem Hasch-Algorithmus SHA 256 unter Verwendung des RSA-Algorithmus signiert (Algorithmus ist "sha256WithRSAEncryption" - OID = 1.2.840.113549.1.1.11).

### 6.1.7 Schlüsselverwendung

Die Verwendungszwecke der Schlüssel wird im entsprechenden Zertifikat im Feld *KeyUsage* festgelegt (siehe Abschnitt 7.1ff).

## 6.2 Schutz privater Schlüssel und kryptographischer Module

### 6.2.1 Standards und Schutzmechanismen der kryptographischen Module

Für CA-Schlüssel werden Hardware-Sicherheitsmodule (High Security Modul (HSM) eingesetzt, die mindesten nach FIPS-140-2 Level 3 oder nach Common Criteria mit Prüfstufe EAL4 / EAL5+ zertifiziert sind.

### 6.2.2 Mehrpersonen-Zugriffskontrolle bei privaten Schlüsseln

Die privaten CA-Schlüssel werden im HSM erzeugt, gespeichert und verlassen das HSM nur in verschlüsselter Form. Bei administrativen Zugriffen auf das HSM, wie das Erzeugen und Wiedereinspielen von CA-Sicherungskopien, wird durch den implementierten HSM-Mechanismus das Vier-Augen-Prinzip technisch durchgesetzt. Im operativen Betrieb kann eine Zertifizierungsstelle nach erfolgreicher Authentifizierung mittels Passwort Signiervorgänge durchführen.

### 6.2.3 Hinterlegung privater Schlüssel

Die privaten CA-Schlüssel werden nicht bei Dritten hinterlegt. Zur Wiederherstellung von privatem Schlüsselmaterial steht ein Schlüssel Backup zur Verfügung.

### 6.2.4 Backup privater Schlüssel

CA-Schlüssel werden mit den Backup-Mechanismen des HSM gesichert, hierbei liegen die CA-Schlüssel in verschlüsselter Form vor. Die Sicherung und Wiederherstellung der CA-Schlüssel erfolgt unter Einhaltung des Vier-Augen-Prinzips.

Die Schlüssel für Endteilnehmer werden auf dem Endgerät des Nutzers generiert. Der Nutzer kann mit Hilfe der Volksverschlüsselungs-Software ein Backup seiner Schlüssel erzeugen.

### 6.2.5 Archivierung privater Schlüssel

Wenn CA-Schlüssel das Ende ihrer Gültigkeitsdauer erreicht haben, werden sie vernichtet. Eine Archivierung findet nicht statt.

Private Schlüssel der Endteilnehmer befinden sich ausschließlich auf dem Endgerät des Nutzers.

### 6.2.6 Übertragung privater Schlüssel in oder aus kryptographischen Moduln

Eine Übertragung privater CA-Schlüssel in oder aus dem HSM erfolgt nur zu Backup- und Wiederherstellungszwecken und ist durch die HSM-Mechanismen gesichert. Das Vier-Augen-Prinzip wird technisch erzwungen.

### 6.2.7 Speicherung privater Schlüssel

Die privaten Schlüssel der Zertifizierungsstellen werden ausschließlich in kryptographischen Hardware-Sicherheitsmodulen gespeichert (vgl. Abschnitt 6.2.1).

Private Schlüssel der Endteilnehmer werden ausschließlich auf dem Endgerät des Nutzers erzeugt und gespeichert.

### 6.2.8 Aktivierung privater Schlüssel

Die privaten Schlüssel der Zertifizierungsstellen werden aktiviert, indem sich das CA-System bei Aufbau einer Benutzersession gegenüber dem HSM gemäß dem festgelegten Authentifizierungsverfahren (Passwort, Smartcard) authentisiert.

### 6.2.9 Deaktivierung privater Schlüssel

Der Zugriff auf private CA-Schlüssel erfolgt immer innerhalb einer aktiven Benutzersession. Wird die Verbindung zum HSM beendet, wird der Zugriff auf den Schlüssel deaktiviert.

### 6.2.10 Vernichtung privater Schlüssel

Private CA-Schlüssel werden nach Ablauf der Gültigkeit bzw. nach Sperrung vernichtet. Dabei wird sichergestellt, dass nach Vernichtung keine Fragmente des Schlüssels übrigbleiben, die zu einer Rekonstruktion des privaten Schlüssels führen könnten. Das physikalische Medium wird im Falle der Entsorgung physisch zerstört. Die Vernichtung von CA-Schlüsseln wird im Vier-Augen-Prinzip durchgeführt.

### 6.2.11 Bewertung kryptographischer Module

Vgl. Abschnitt 6.2.1.

## 6.3 Weitere Aspekte des Schlüsselmanagements

### 6.3.1 Archivierung öffentlicher Schlüssel

Öffentliche Schlüssel sind in den Zertifikaten (Root-CA-, CA-, Endteilnehmer-Zertifikate) enthalten und werden auf Medien für die Datensicherung archiviert.

### 6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren

Die Gültigkeit eines Zertifikats endet mit Ablauf des Gültigkeitszeitraums oder durch Sperrung. Die privaten Endteilnehmer-Schlüssel können jedoch weiterhin zur Entschlüsselung genutzt werden, sofern diese dem Zertifikatsinhaber noch zur Verfügung stehen.

Die von der Volksverschlüsselungs-PKI ausgestellten Zertifikate sind für Gültigkeitsprüfungen nach dem Schalenmodell gemäß [RFC5280] ausgelegt, d.h. das Zertifikat der Zertifizierungsstelle ist länger gültig als die von ihr ausgestellten Zertifikate.

In Tabelle 1 sind die maximalen Gültigkeitszeiträume der von der Volksverschlüsselungs-PKI ausgestellten Zertifikate dargestellt.

*Tabelle 1: Gültigkeitszeiträume der Volksverschlüsselungs-PKI Zertifikate*

| Zertifikatstyp: | Gültigkeitszeiträume (maximal): |
|---|---|
| FhG VV-Root-CA Zertifikat | 7 Jahre |
| FhG VV-CA Zertifikat | 5 Jahre |
| Endteilnehmer-Zertifikate | 2 Jahre |

| | |
|---|---|
| OCSP-Signaturzertifikat | 32 Tage |

## 6.4 Aktivierungsdaten

Daten, die zum Aktivieren von privaten CA-Schlüsseln im HSM benötigt werden, werden im Rahmen der CA-Schlüsselerstellung gemäß den Vorgaben des HSM-Herstellers erzeugt. Die Mitarbeiter der DTAG verpflichten sich, Aktivierungsdaten (Passwort, Smartcard etc.) für die privaten CA-Schlüssel geheim zu halten und vor dem Zugriff unbefugter Dritter zu schützen.

## 6.5 Computer-Sicherheitskontrollen

### 6.5.1 Spezifische Anforderungen an technische Sicherheitsmassnahmen

Alle Anwendungen innerhalb der CA werden ausschließlich auf Basis von gehärteten Betriebssystemen betrieben.

Darüber hinaus ist sichergestellt, dass alle Systeme der Volksverschlüsselungs-PKI vor unbefugtem Zugriff gesichert sind. Die CA-Komponenten werden in einer separaten technischen Sicherheitszone betrieben und sind nur von autorisiertem Personal zugängig. Schutzmechanismen (z.B. Firewalls, Zutrittsschutz, Vier-Augen-Prinzip) sind umgesetzt, um die Volksverschlüsselungs-PKI vor internen und externen Angriffen zu schützen.

### 6.5.2 Güte/Qualität der Sicherheitsmassnahmen

Die in Abschnitt 6.5.1 genannten Sicherheitsmassnahmen werden periodisch überprüft und entsprechen dem aktuellen Stand der Technik.

## 6.6 Technische Kontrollen des Lebenszyklus

### 6.6.1 Systementwicklungskontrollen

Die Entwicklung von Software erfolgt durch qualifizierte Mitarbeiter des Fraunhofer-SIT in einer gesicherten Entwicklungsumgebung. Die Übernahme der neu entwickelten/geänderten Software in das Produktivsystem erfolgt erst nach erfolgreich abgeschlossenem Test und nach erteilter Freigabe durch den Projektverantwortlichen und das Betriebspersonal.

### 6.6.2 Sicherheitsmanagement

Die Konfiguration der CA-Systeme sowie alle Änderungen und Updates bzw. Upgrades sind dokumentiert und werden von der für die Volksverschlüsselungs-PKI verantwortlichen Stelle kontrolliert. Es gibt Mechanismen zum Erkennen von unbefugten Änderungen der CA-Soft- und Hardware bzw. deren Konfiguration. Alle sicherheitsrelevanten Vorgänge werden protokolliert und die Sicherheit im laufenden Betrieb wird kontinuierlich überwacht.

Es erfolgt eine ständige Überwachung der Verfügbarkeit der von der Volksverschlüsselungs-PKI angebotenen Dienste.

### 6.6.3 Maßnahmen zur Kontrolle des Software-Lebenszyklus

Es ist sichergestellt, dass die eingesetzte Software in einer Weise entwickelt, getestet, installiert, konfiguriert, betrieben und gewartet wird, so dass ihre Authentizität, Integrität und bestimmungsmäßige Funktionsfähigkeit gewährleistet ist.

## 6.7 Maßnahmen zur Netzwerksicherheit

Es sind folgende Maßnahmen zur Netzwerksicherheit implementiert:

- Die zum Einsatz kommenden Hard- und Softwarekomponenten der Volksverschlüsselungs-PKI werden in verschiedenen technischen Sicherheitszonen betrieben.
- Die CA-Systeme befinden sich in einem internen CA-Netz und sind durch ausreichende Sicherheits-Gateways vom Internet getrennt.
- Sicherheitskritische Komponenten (RA, OCSP-Responder, Verzeichnisdienst), die vom Internet aus erreichbar sein müssen, sind in einer DMZ untergebracht, die vom Internet und dem internen CA-Netz durch Firewalls getrennt sind. Es werden nur Kommunikationswege (Ports) freigeschaltet, die zwingend erforderlich sind.

## 6.8 Zeitstempel

Ein kryptographischer Zeitstempeldienst wird nicht verwendet.

Zeitangaben in Zertifikaten Sperrlisten, OCSP-Antworten sowie in Protokolldaten und anderen wichtigen Informationen basieren auf der Systemzeit des Systems, das diese Daten generiert. Die Systemzeiten der Systeme des Zertifizierungsdienstes werden permanent mit der Zeit der physikalisch technischen Bundesanstalt in Braunschweig synchronisiert.

# 7 Profile für Zertifikate, Sperrlisten und OCSP

## 7.1 Zertifikatsprofile

Die von der Volksverschlüsselungs-PKI ausgestellten Zertifikate entsprechen den Anforderungen der Standards ITU [X.509] Version 3 und IETF [RFC5280], sowie der Profilierung Common PKI 2.0 [CommonPKI].

### 7.1.1 Zertifikatsprofil des Wurzelzertifikats „Volksverschluesselung Root CA“

| Zertifikatsfeld | Wert | Bemerkung |
|---|---|---|
| Version | V3 (0x2) | X.509-Zertifikate Version v3.<br><br>Der codierte Wert im Zertifikatsfeld ist 2. |
| SerialNumber | 71:fb:32:04:bf:fa:8c:17 | Eindeutige Zertifikatsnummer (INTEGER) innerhalb des Zertifizierungsbereichs (gleicher Issuer). |
| Signature | sha256WithRSAEncryption<br>(OID=1.2.840.113549.1.1.11) | Hash- und Signaturalgorithmus der Zertifizierungsstelle |
| Issuer - DName der Zertifizierungsstelle (Aussteller) | | |
| CountryName (C) | DE | |
| OrganisationName (O) | Fraunhofer SIT | |
| CommonName (CN) | Volksverschluesselung Root CA | |
| Validity - Gültigkeitszeitraum (Datum und Uhrzeit ) des Zertifikats (von – bis); UTC-kodiert gemäß RFC 5280 | | |
| notBefore | May 9 14:03:55 2016 GMT | |
| notAfter | May 10 14:03:55 2023 GMT | Gültigkeit 7 Jahre |
| Subject - DName des Zertifikatsinhabers; Identisch mit DName im Feld Issuer | | |
| CountryName (C) | DE | |
| OrganisationName (O) | Fraunhofer SIT | |
| CommonName (CN) | Volksverschluesselung Root CA | |
| SubjectPublicKeyInfo – Öffentlicher Schlüssel des Zertifikatsinhabers gemäß RFC 5280 | | |
| Algorithm | RsaEncryption<br>(OID = 1.2.840.113549.1.1.1) | |

| | | |
|---|---|---|
| Public Key | RSA 4096 Bit | Schlüssel und Schlüssellänge |
| Extensions - Zertifikatserweiterungen | | |
| AuthorityKeyIdentifier<br>(non-critical) | Identisch mit SubjectKeyIdentifier | Informationen zur Identifizierung des öffentlichen Schlüssels des Ausstellers |
| SubjectKeyIdentifier<br>(non-critical) | Hashwert über den SubjectPublicKey im Feld SubjectPublicKeyInfo | Informationen zur Identifizierung des öffentlichen Schlüssels des Zertifikats. |
| KeyUsage<br>(critical) | keyCertSign<br>crlSign | Verwendungszweck des Schlüssels |
| BasicConstraints<br>(critical) | CA=TRUE | Informationen zum Zertifikatstyp |
| | | |
| signatureAlgorithm | sha256WithRSAEncryption<br>(OID=1.2.840.113549.1.1.11) | Hash- und Signaturalgorithmus der Zertifizierungsstelle „Volksverschluesselung Root CA“ |
| SignatureValue | Signatur | Signatur der Zertifizierungsstelle |

### 7.1.2 Zertifikatsprofile der Volksverschluesselung Private CA

| **Zertifikatsfeld** | **Wert** | **Bemerkung** |
|---|---|---|
| Version | V3 (0x2) | X.509-Zertifikate Version v3.<br><br>Der codierte Wert im Zertifikatsfeld ist 2 |
| SerialNumber | 0e:cf:8a:22:c5:9e:c7:87 | Eindeutige Zertifikatsnummer (INTEGER) innerhalb des Zertifizierungsbereichs (gleicher Issuer). |
| Signature | sha256WithRSAEncryption<br>(OID=1.2.840.113549.1.1.11) | Hash- und Signaturalgorithmus der Zertifizierungsstelle |
| Issuer - DName der Zertifizierungsstelle (Aussteller) | | |
| CountryName | DE | |
| OrganisationName | Fraunhofer SIT | |
| CommonName | Volksverschluesselung Root CA | |

| | | |
|---|---|---|
| Validity - Gültigkeitszeitraum (Datum und Uhrzeit ) des Zertifikats (von – bis); UTC-kodiert gemäß RFC 5280 | | |
| notBefore | May 9 14:09:13 2016 GMT | |
| notAfter | May 10 14:03:13 2021 GMT | Gültigkeit 5 Jahre |
| Subject - DName des Zertifikatsinhabers; Identisch mit DName im Feld Issuer | | |
| CountryName | DE | |
| OrganisationName | Fraunhofer SIT | |
| CommonName | Volksverschluesselung Private CA | |
| SubjectPublicKeyInfo – Öffentlicher Schlüssel des Zertifikatsinhabers gemäß RFC 5280 | | |
| Algorithm | RsaEncryption<br>(OID = 1.2.840.113549.1.1.1) | |
| Public Key | RSA 4096 Bit | Schlüssel und Schlüssellänge |
| Extensions - Zertifikatserweiterungen | | |
| AuthorityKeyIdentifier<br>(non-critical) | KeyIdentifier des Schlüssel der Volksver-schlusselung Root CA | Informationen zur Identifizie-rung des öffentlichen Schlüssels des Ausstellers. |
| SubjectKeyIdentifier<br>(non-critical) | Hashwert über den SubjectPublicKey im Feld SubjectPublicKeyInfo | Informationen zur Identifizie-rung des öffentlichen Schlüssels des Zertifikats |
| KeyUsage<br>(critical) | keyCertSign<br>crlSign | Verwendungszweck des Schlüs-sels |
| BasicConstraints (critical) | CA=TRUE<br>Pathlen=0 | Informationen zum Zertifikats-typ |
| Certificates Policies<br>(non-critical) | X.509v3 Any Policy<br>(OID: 2.5.29.32.0) | Referenz auf die Policies (CP/CPS) |
| CRLDistributionPoints<br>(Non-critical) | http://volksverschluesse-lung.de/crl/rootca.crl | CRL-Issuer and URL zur Sperr-liste |
| AuthorithyInfoAccess | http://volksverschluesse-lung.de/ca/rootca.crt | Angaben über die Quelle von Statusinformationen für die Va-lidierung des Zertifikats |
| | | |

| | | |
|---|---|---|
| signatureAlgorithm | sha256WithRSAEncryption<br>(OID=1.2.840.113549.1.1.11) | Hash- und Signaturalgorithmus der Zertifizierungsstelle „Volks-verschluesselung Root CA“ |
| SignatureValue | Signatur | Signatur der Zertifizierungsstelle |

### 7.1.3 Zertifikatsprofil des OCSP-Signaturzertifikats der Volksverschluesselung Private CA

| **Zertifikatsfeld** | **Wert** | **Bemerkung** |
|---|---|---|
| Version | V3 (0x2) | X.509-Zertifikate Version v3.<br><br>Der codierte Wert im Zertifikats-feld ist 2 |
| SerialNumber | Seriennummer | Eindeutige Zertifikatsnummer (INTEGER) innerhalb des Zertifi-zierungsbereichs (gleicher Issuer). |
| Signature | sha256WithRSAEncryption<br>(OID=1.2.840.113549.1.1.11) | Hash- und Signaturalgorithmus der Zertifizierungsstelle. |
| Issuer - DName der Zertifizierungsstelle (Aussteller) | | |
| CountryName | DE | |
| OrganisationName | Fraunhofer SIT | |
| CommonName | Volksverschluesselung Private CA | |
| Validity | Datum und Uhrzeit | Gültigkeitszeitraum des Zertifi-kats (von – bis); UTC-kodiert ge-mäß RFC 5280 |
| Subject - DName des Zertifikatsinhabers | | |
| CountryName | DE | |
| OrganisationName | Fraunhofer SIT | |
| CommonName | OCSP Responder Volksverschluesselung Private CA | |
| SubjectPublicKeyInfo – Öffentlicher Schlüssel des Zertifikatsinhabers gemäß RFC 5280 | | |
| Algorithm | RsaEncryption<br>(OID = 1.2.840.113549.1.1.1) | |
| Public Key | RSA 2048 Bit | Schlüssel und Schlüssellänge |

| Extensions - Zertifikatserweiterungen | | |
|---|---|---|
| AuthorityKeyIdentifier<br>(non-critical) | KeyIdentifier des öffentlichen Schlüssels der **Volksverschluesselung Private CA** | Informationen zur Identifizierung des öffentlichen Schlüssels des Ausstellers. |
| SubjectPublicKeyInfo | Hashwert über den SubjectPublicKey im Feld SubjectPublicKeyInfo | Informationen zur Identifizierung des öffentlichen Schlüssels des Zertifikats. |
| KeyUsage<br>(critical) | digitalSignature | Verwendungszweck des Schlüssels. |
| BasicConstraints (critical) | CA=FALSE | Informationen zum Zertifikatstyp. |
| Certificates Policies<br>(non-critical) | VV-X509-CP/CPS<br>(OID: 1.3.36.15.9.1.1.1) | Referenz auf die Policies (CP/CPS) |
| ExtendedKeyUsage | OCSPSigning | Erweiterte Nutzung des Schlüssels. |
| OCSP No Check<br>(Non-critical) | NULL | Vertrauen in das Zertifikat (vgl. Abschnitt 4.2.2.2.1 in [RFC6960]). |
| | | |
| signatureAlgorithm | sha256WithRSAEncryption<br>(OID=1.2.840.113549.1.1.11) | Hash- und Signaturalgorithmus der **Volksverschluesselung Private CA** |
| SignatureValue | Signatur | Signatur der Zertifizierungsstelle |

### 7.1.4 Zertifikatsprofil der Endteilnehmer-Zertifikate der Volksverschluesselung Private CA

**Profil des Verschlüsselungszertifikats**

| Zertifikatsfeld | Wert | Bemerkung |
|---|---|---|
| Version | V3 (0x2) | X.509-Zertifikate Version v3.<br><br>Der codierte Wert im Zertifikatsfeld ist 2. |
| SerialNumber | Seriennummer | Eindeutige Zertifikatsnummer (INTEGER) innerhalb des Zertifizierungsbereichs (gleicher Issuer). |

| | | |
|---|---|---|
| Signature | sha256WithRSAEncryption<br>(OID=1.2.840.113549.1.1.11) | Hash- und Signaturalgorithmus der Zertifizierungsstelle |
| Issuer - DName der Zertifizierungsstelle (Aussteller) | | |
| CountryName | DE | |
| OrganisationName | Fraunhofer SIT | |
| CommonName | Volksverschluesselung Private CA | |
| Validity | Datum und Uhrzeit | Gültigkeitszeitraum des Zertifikats (von – bis); UTC-kodiert gemäß RFC 5280 |
| Subject - DName des Zertifikatsinhabers | | |
| CommonName | Name des Zertifikatsinhabers | |
| serialNumber | Seriennummer | Eindeutiger Wert, um eine Unterscheidung bei Namensgleichheit zu gewährleisten. |
| Title (optional) | Titel | |
| surName | Name | |
| givenName | Vorname(n) | |
| SubjectPublicKeyInfo – Öffentlicher Schlüssel des Zertifikatsinhabers gemäß RFC 5280 | | |
| Algorithm | RsaEncryption<br>(OID = 1.2.840.113549.1.1.1) | |
| Public Key | RSA 2048 Bit | Schlüssel und Schlüssellänge |
| Extensions - Zertifikatserweiterungen | | |
| AuthorityKeyIdentifier<br>(non-critical) | KeyIdentifier des öffentlichen Schlüssels der Volksverschluesselung Private CA | Informationen zur Identifizierung des öffentlichen Schlüssels des Ausstellers. |
| SubjectPublicKeyInfo | Hashwert über den SubjectPublicKey im Feld SubjectPublicKeyInfo | Informationen zur Identifizierung des öffentlichen Schlüssels des Zertifikats |
| KeyUsage<br>(critical) | keyEncipher<br>dataEncipher | Verwendungszweck des Schlüssels |
| BasicConstraints<br>(critical) | CA=FALSE | Informationen zum Zertifikatstyp |

| | | |
|---|---|---|
| Certificates Policies<br>(non-critical) | VV-X509-CP/CPS<br>(OID: 1.3.36.15.9.1.1.1) | Referenz auf die Policies (CP/CPS) |
| ExtendedKeyUsage | eMailProtection<br>Microsoft EFS | Erweiterte Nutzung des Schlüssels |
| SubjectAltNames<br>(non-critical) | Private E-Mail-Adresse des Zertifikatsinhabers | Weitergehende Informationen zu Subject |
| CRLDistributionPoints<br>(Non-critical) | http://volksverschluesselung.de/crl/privateca.crl | CRL-Issuer and URL zur Sperrliste |
| AuthorithyInfoAccess | http://volksverschluesselung.de/ca/privateca.crt<br>http://ocsp.volksverschluesslung.de | Angaben über die Quelle von Statusinformationen für die Validierung des Zertifikats |
| | | |
| signatureAlgorithm | sha256WithRSAEncryption<br>(OID=1.2.840.113549.1.1.11) | Hash- und Signaturalgorithmus der **Volksverschluesselung Private CA** |
| SignatureValue | Signatur | Signatur der Zertifizierungsstelle |

**Profil des Signaturzertifikats**

| **Zertifikatsfeld** | **Wert** | **Bemerkung** |
|---|---|---|
| Version | V3 (0x2) | X.509-Zertifikate Version v3.<br><br>Der codierte Wert im Zertifikatsfeld ist 2 |
| SerialNumber | Seriennummer | Eindeutige Zertifikatsnummer (INTEGER) innerhalb des Zertifizierungsbereichs (gleicher Issuer). |
| Signature | sha256WithRSAEncryption<br>(OID=1.2.840.113549.1.1.11) | Hash- und Signaturalgorithmus der Zertifizierungsstelle |
| Issuer - DName der Zertifizierungsstelle (Aussteller) | | |
| CountryName | DE | |
| OrganisationName | Fraunhofer SIT | |
| CommonName | Volksverschluesselung Private CA | |

| | | |
|---|---|---|
| Validity | Datum und Uhrzeit | Gültigkeitszeitraum des Zertifikats (von – bis); UTC-kodiert gemäß RFC 5280 |
| Subject - DName des Zertifikatsinhabers | | |
| CommonName | Name des Zertifikatsinhabers | |
| serialNumber | Seriennummer | Eindeutiger Wert, um eine Unterscheidung bei Namensgleichheit zu gewährleisten. |
| Title (optional) | Titel | |
| surName | Name | |
| givenName | Vorname(n) | |
| SubjectPublicKeyInfo – Öffentlicher Schlüssel des Zertifikatsinhabers gemäß RFC 5280 | | |
| Algorithm | RsaEncryption<br>(OID = 1.2.840.113549.1.1.1) | |
| Public Key | RSA 2048 Bit | Schlüssel und Schlüssellänge |
| Extensions - Zertifikatserweiterungen | | |
| AuthorityKeyIdentifier<br>(non-critical) | KeyIdentifier des öffentlichen Schlüssels der Volksverschluesselung Private CA | Informationen zur Identifizierung des öffentlichen Schlüssels des Ausstellers. |
| SubjectPublicKeyInfo | Hashwert über den SubjectPublicKey im Feld SubjectPublicKeyInfo | Informationen zur Identifizierung des öffentlichen Schlüssels des Zertifikats |
| KeyUsage<br>(critical) | digitalSignature<br>nonReputiation | Verwendungszweck des Schlüssels |
| BasicConstraints (critical) | CA=FALSE | Informationen zum Zertifikatstyp |
| Certificates Policies<br>(non-critical) | VV-X509-CP/CPS<br>(OID: 1.3.36.15.9.1.1.1) | Referenz auf die Policies (CP/CPS) |
| ExtendedKeyUsage | eMailProtection | Erweiterte Nutzung des Schlüssels |
| SubjectAltNames<br>(non-critical) | Private E-Mail-Adresse des Zertifikatsinhabers | Weitergehende Informationen zu Subject |
| CRLDistributionPoints<br>(Non-critical) | http://volksverschluesselung.de/crl/privateca.crl | CRL-Issuer and URL zur Sperrliste |

| | | |
|---|---|---|
| AuthorithyInfoAccess | http://volksverschluesselung.de/ca/priva-teca.crt<br>http://ocsp.volksverschluesslung.de | Angaben über die Quelle von Statusinformationen für die Validierung des Zertifikats |
| | | |
| signatureAlgorithm | sha256WithRSAEncryption<br>(OID=1.2.840.113549.1.1.11) | Hash- und Signaturalgorithmus der **Volksverschluesselung Private CA** |
| SignatureValue | Signatur | Signatur der Zertifizierungsstelle |

**Profil des Authentifizierungszertifikats**

| **Zertifikatsfeld** | **Wert** | **Bemerkung** |
|---|---|---|
| Version | V3 (0x2) | X.509-Zertifikate Version v3.<br><br>Der codierte Wert im Zertifikatsfeld ist 2 |
| SerialNumber | Seriennummer | Eindeutige Zertifikatsnummer (INTEGER) innerhalb des Zertifizierungsbereichs (gleicher Issuer). |
| Signature | sha256WithRSAEncryption<br>(OID=1.2.840.113549.1.1.11) | Hash- und Signaturalgorithmus der Zertifizierungsstelle |
| Issuer - DName der Zertifizierungsstelle (Aussteller) | | |
| CountryName | DE | |
| OrganisationName | Fraunhofer SIT | |
| CommonName | Volksverschluesselung Private CA | |
| Validity | Datum und Uhrzeit | Gültigkeitszeitraum des Zertifikats (von – bis); UTC-kodiert gemäß RFC 5280 |
| Subject - DName des Zertifikatsinhabers | | |
| CommonName | Name des Zertifikatsinhabers | |
| serialNumber | Seriennummer | Eindeutiger Wert, um eine Unterscheidung bei Namensgleichheit zu gewährleisten. |
| Title (optional) | Titel | |
| surName | Name | |
| givenName | Vorname(n) | |

| SubjectPublicKeyInfo – Öffentlicher Schlüssel des Zertifikatsinhabers gemäß RFC 5280 | | |
|---|---|---|
| Algorithm | RsaEncryption<br>(OID = 1.2.840.113549.1.1.1) | |
| Public Key | RSA 2048 Bit | Schlüssel und Schlüssellänge |
| Extensions - Zertifikatserweiterungen | | |
| AuthorityKeyIdentifier<br>(non-critical) | KeyIdentifier des öffentlichen Schlüssels der Volksverschluesselung Private CA | Informationen zur Identifizierung des öffentlichen Schlüssels des Ausstellers. |
| SubjectPublicKeyInfo | Hashwert über den SubjectPublicKey im Feld SubjectPublicKeyInfo | Informationen zur Identifizierung des öffentlichen Schlüssels des Zertifikats |
| KeyUsage<br>(critical) | digitalSignature | Verwendungszweck des Schlüssels |
| BasicConstraints (critical) | CA=FALSE | Informationen zum Zertifikatstyp |
| Certificates Policies<br>(non-critical) | VV-X509-CP/CPS<br>(OID: 1.3.36.15.9.1.1.1) | Referenz auf die Policies (CP/CPS) |
| ExtendedKeyUsage | clientAuth | Erweiterte Nutzung des Schlüssels |
| SubjectAltNames<br>(non-critical) | Private E-Mail-Adresse des Zertifikatsinhabers | Weitergehende Informationen zu Subject |
| CRLDistributionPoints<br>(Non-critical) | http://volksverschluesselung.de/crl/privateca.crl | CRL-Issuer and URL zur Sperrliste |
| AuthorithyInfoAccess | http://volksverschluesselung.de/ca/privateca.crt<br>http://ocsp.volsverschluesslung.de | Angaben über die Quelle von Statusinformationen für die Validierung des Zertifikats |
| | | |
| signatureAlgorithm | sha256WithRSAEncryption<br>(OID=1.2.840.113549.1.1.11) | Hash- und Signaturalgorithmus der **Volksverschluesselung Private CA** |
| SignatureValue | Signatur | Signatur der Zertifizierungsstelle |

## 7.2 Profil der Sperrlisten

Die von den Zertifizierungsstellen der Volksverschlüsselungs-PKI ausgestellten Sperrlisten entsprechen den Anforderungen der Standards ITU [X.509] Version 2 und IETF [RFC5280], sowie der Profilierung Common PKI 2.0 [CommonPKI].

Die folgende Tabelle 2 zeigt das Profil der ausgestellten Sperrlisten.

*Tabelle 2: Profil der Sperrlisten*

| **Zertifikatsfeld** | **Wert** | **Bemerkung** |
|---|---|---|
| TBSCertList | | |
| Version | V2(0x1) | Abschnitt 7.2.1 |
| Signature | sha256WithRSAEncryption<br>(OID=1.2.840.113549.1.1.11) | Hash- und Signaturalgorithmus der ausstellenden Zertifizierungsstelle. |
| Issuer | DName der Zertifizierungsstelle (Aussteller) | Abschnitt 7.1.1 / Abschnitt 7.1.2 |
| ThisUpdate | Gültig ab (creation time) | UTCTime kodiert gemäß RFC 5280 |
| NextUpdate | Nächste Aktualisierung | UTCTime kodiert gemäß RFC 5280 / siehe Abschnitt 4.9.7 |
| RevokedCertificates | | |
| userCertificate | Identifikation des gesperrten Zertifikats | Seriennummer |
| revocationDate | Datum und Uhrzeit der Sperrung | UTCTime kodiert gemäß RFC 5280 |
| crlEntryExtensions | Erweiterungen der Sperrliste | Abschnitt 7.2.2 |
| | | |
| crlExtensions | Erweiterungen der Sperrlisten | Abschnitt 7.2.2 |
| signatureAlgorithm | sha256WithRSAEncryption<br>(OID=1.2.840.113549.1.1.11) | Verwendeter Hash- und Signaturalgorithmus der ausstellenden Zertifizierungsstelle. |
| SignatureValue | Signatur der Zertifizierungsstelle | |

### 7.2.1 Versionsnummer(n)

Die von der Volksverschlüsselungs-PKI ausgestellten X.509-Zertifikatssperrlisten entsprechen der Version 2 gemäß [RFC5280]. Delta-CRLs sind nicht vorgesehen.

### 7.2.2 Erweiterungen der Sperrliste

Die Sperrlisten der Volksverschlüsselungs-PKI unterstützen die folgenden Erweiterungen:

*Tabelle 3: Erweiterungen der Sperrlisten*

| Feld | Wert | Bemerkung |
|---|---|---|
| **crlEntryExtensions** | | |
| reasonCode<br>(non-critical) | Grund der Revozierung; entspricht dem Wert in den Antworten des OCSP-Responders | Kodierung nach RFC 5280 |
| **crlExtensions** | | |
| authorityKeyIdentifier<br>(non-critical) | Hashwert über den öffentlichen Schlüssel der CA. | Identifiziert den öffentlichen Schlüssel der CA, die die CRL signiert hat. |
| CRLNumber<br>(non-critical) | Sperrlistennummer | Fortlaufende Seriennummer der Sperrliste |

## 7.3 OCSP-Profil

Der OCSP-Responder der Volksverschlüsselungs-PKI erfüllt die Anforderungen des [RFC6960] und ist konform zu Common PKI 2.0 [CommonPKI].

### 7.3.1 Versionsnummer(n)

Es wird die Version 1 gemäß [RFC6960] unterstützt.

### 7.3.2 OCSP-Erweiterungen

Der OCSP-Responder unterstützt bei Anfragen (OCSP Request) die im Folgenden angegeben Erweiterung:

*Tabelle 4: Erweiterungen der OCSP-Anfragen*

| Feld | Bedeutung |
|---|---|
| Nonce (optional) | Wert, der die Anfrage kryptographisch an die Antwort bindet (Abwehr von Replay Attacken). |

Der OCSP-Responder verwendet bei Antworten (OCSP Response) die im Folgenden angegeben Erweiterung:

*Tabelle 5: Erweiterungen der OCSP-Antworten*

| Feld | Bedeutung |
|---|---|
| *Nonce* | Gleicher Wert wie in der Anfrage. Nicht existent, falls in Anfrage nicht vorhanden. |

# 8 Audits und andere Prüfungen

## 8.1 Prüfungsintervall

Die Einhaltung der Richtlinien in diesem Dokument (VV-X509-CP/CPS) wird jährlich durch interne Audits geprüft. Besondere sicherheitskritische Ereignisse können eine außerplanmäßige Überprüfung erforderlich machen.

## 8.2 Identität und Qualifikation des Prüfers

Die internen Audits werden von einem qualifizierten Mitarbeiter durchgeführt, der über das notwendige Know-How in den Bereichen Public Key Infrastructure, Sicherheits-Auditing und Informationssicherheit verfügt.

## 8.3 Beziehung des Prüfers zur prüfenden Stelle

Die Prüfung wird von einem Mitarbeiter durchgeführt, der keine weiteren Aufgaben im operativen Betrieb der Volksverschlüsselungs-PKI wahrnimmt.

## 8.4 Abgedeckte Bereiche der Prüfung

Zielsetzung der internen Audits ist die Überprüfung der Konformität zu diesem Dokument und der Umsetzung der im Sicherheitskonzept definierten Maßnahmen. Die zu prüfenden Bereiche legt der Prüfer selbst fest. Die Ergebnisse der Prüfung sind in einem Auditbericht zu dokumentieren.

## 8.5 Maßnahmen zur Mängelbeseitigung

Werden bei einer Prüfung Mängel oder Fehler festgestellt, wird entschieden, welche Korrekturmaßnahmen zu treffen sind. Hierbei ist je nach Schwere und Dringlichkeit zu unterscheiden. Bei schweren sicherheitskritischen Mängeln wird an das Management des Fraunhofer SIT berichtet und dieses entscheidet auf Basis eines Korrekturplans, welche Maßnahmen in welchem Zeitraum zur Behebung durchgeführt werden.

## 8.6 Veröffentlichung der Ergebnisse

Eine Veröffentlichung der Prüfergebnisse ist nicht vorgesehen.

# 9 Sonstige finanzielle und rechtliche Regelungen

## 9.1 Entgelte

### 9.1.1 Gebühren für Zertifikate

Zertifikate von der „**Volksverschluesselung Private CA**“ und dazugehörige Schlüssel dürfen ausschließlich zu privaten Zwecken verwendet werden. Für die Ausstellung von Zertifikaten der „**Volksverschluesselung Private CA**“ und die Veröffentlichung im Verzeichnisdienst der Volksverschlüsselungs-PKI werden keine Gebühren erhoben. Zu den ggf. anfallenden Kosten beim Verfahren zum Nachweis der Identität siehe Abschnitt 9.1.4.

### 9.1.2 Gebühren für den Abruf von Zertifikaten

Der Abruf von Zertifikaten aus dem Verzeichnisdienst der Volksverschlüsselungs-PKI ist kostenlos.

### 9.1.3 Gebühren für Sperrungen oder Statusinformationen

Sperrungen und das Abrufen von Statusinformationen sind kostenlos.

### 9.1.4 Gebühren für andere Dienstleistungen

Falls im Zusammenhang mit dem vom Endteilnehmer gewählten Verfahren zum Nachweis der Identität bei einem Diensteanbieter Gebühren für den Endteilnehmer anfallen sollten, werden diese direkt vom Diensteanbieter erhoben.

## 9.2 Finanzielle Zuständigkeiten

Fraunhofer, ihre gesetzlichen Vertreter und Erfüllungsgehilfen haften nur für grobe Fahrlässigkeit sowie für Vorsatz. Diese Haftungsbeschränkung findet jedoch keine Anwendung bei Schäden gegen Körper, Leben oder Gesundheit oder in Fällen, in welchen das Produkthaftungsgesetz greift. Auf die Nutzungsbeschränkungen, welche in dieser Zertifizierungsrichtlinie unter Abschnitt 1.4 und Abschnitt 4.5 genannt werden, wird ausdrücklich hingewiesen.

## 9.3 Vertraulichkeit von Geschäftsinformationen

### 9.3.1 Vertraulich zu behandelnden Daten

Als vertraulich gelten alle persönlichen und unternehmensspezifischen Informationen, die im Rahmen der Zertifizierungsdienstleistung zugänglich gemacht werden und nicht Bestandteil eines Zertifikats sind.

### 9.3.2 Öffentliche Informationen

Als öffentlich gelten Zertifikate, die im Verzeichnisdienst veröffentlicht werden, Sperrlisten und OCSP-Responder-Anfragen/-Antworten sowie alle unter Abschnitt 2 genannten Informationen.

### 9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Das Fraunhofer SIT ist für den Schutz der vertraulichen Informationen und die Einhaltung der datenschutzrechtlichen Vorgaben verantwortlich.

## 9.4 Datenschutz von personenbezogenen Daten

### 9.4.1 Richtlinie zur Verarbeitung personenbezogener Daten

Die Volksverschlüsselungs-PKI muss zur Leistungserbringung personenbezogene Daten elektronisch speichern und verarbeiten. Dies geschieht in Übereinstimmung mit der Datenschutz-Grundverordnung (DS-GVO) und dem Bundesdatenschutzgesetz (BDSG).

Die Auftragsdatenverarbeitung zur Bereitstellung der eID-Schnittstelle für die VV-PKI zur Entgegennahme und Bearbeitung von Authentisierungsanfragen der Nutzer und zum Auslesen der Ausweisdaten entsprechend des Berechtigungszertifikates sowie zur Weitergabe der Ausweisdaten und des Pseudonyms an die Volksverschlüsselungs-PKI richtet sich nach Art. 28 DS-GVO, vgl. PAuswV § 29 Abs. 1.

Die Veröffentlichung von Zertifikaten im Verzeichnisdienst bedarf der Einwilligung des Zertifikatsinhabers.

### 9.4.2 Definition von personenbezogenen Daten

Für personenbezogene Daten gilt Art. 4 Abs. 1 DS-GVO.

### 9.4.3 Vertraulich zu behandelnde personenbezogene Daten

Für personenbezogene Daten gelten die Regelungen aus Abschnitt 9.3.1 analog.

### 9.4.4 Nicht vertraulich zu behandelnde Daten

Unter nicht vertraulichen personenbezogenen Daten werden alle Informationen eingestuft, die explizit in Zertifikaten, Sperrlisten, Statusinformationen und im Verzeichnisdienst enthalten sind.

### 9.4.5 Verantwortung für den Schutz personenbezogener Daten

Die Volksverschlüsselungs-PKI hält sich an den gesetzlich vorgeschriebenen Datenschutz. Alle Mitarbeiter der Volksverschlüsselungs-PKI sind auf die Einhaltung des Datenschutzes verpflichtet worden. Die interne Kontrolle erfolgt durch den betrieblichen Datenschutzbeauftragten.

### 9.4.6 Hinweis und Einwilligung zur Nutzung personenbezogener Daten

Der Zertifikatsinhaber wird bei Antragstellung darauf hingewiesen, welche persönlichen Daten erhoben und im Zertifikat enthalten sein werden.

Die Volksverschlüsselungs-PKI nutzt diese Daten allein zum Zweck der Erbringung der Zertifizierungsdienstleistungen. Eine weitergehende Nutzung dieser Daten durch Fraunhofer findet nicht statt.

Eine Veröffentlichung der E-Mail-Adresse und der öffentlichen Zertifikate erfolgt nur, wenn der Endteilnehmer der Veröffentlichung bei der Antragstellung ausdrücklich zugestimmt hat. Der Zertifikatsinhaber kann seine Einwilligung zur Veröffentlichung jederzeit widerrufen. Der Widerruf ist via E-Mail zu richten an:

widerruf@volksverschluesselung.de

### 9.4.7 Offenlegung gemäß gerichtlicher oder verwaltungsmäßiger Prozesse

Die Fraunhofer-Gesellschaft richtet sich bei der Speicherung und Verarbeitung von personenbezogenen Daten nach den gesetzlichen Datenschutzbestimmungen. Eine Offenlegung personenbezogener Daten gegenüber staatlichen Instanzen erfolgt nur auf Basis eines gerichtlichen Beschlusses.

### 9.4.8 Andere Gründe zur Offenlegung von Daten

Entfällt.

## 9.5 Urheberrechte

Alle Eigentumsrechte an diesem Dokument (VV-X.509-CP/CPS) an den Schlüsseln und Zertifikaten des Zertifizierungsdienstes, dem Veröffentlichungsdienst und den Sperrlisten liegen bei der Fraunhofer.

## 9.6 Zusicherungen und Gewährleistungen

### 9.6.1 Zusicherungen und Gewährleistungen der Zertifizierungsstelle (CA)

Das Fraunhofer SIT stellt sicher, dass die von der Volksverschlüsselungs-PKI erzeugten Zertifikate alle Anforderungen der vorliegenden Richtlinien erfüllen.

Die Volksverschlüsselungs-PKI wird von der Deutschen Telekom AG im Rahmen eines Kooperationsvertrages mit Auftragsdatenverarbeitung betrieben. Das Fraunhofer SIT nimmt die hieraus resultierenden Prüfpflichten wahr und stellt so sicher, dass die vereinbarten Vorgehensweisen umgesetzt werden.

Wenn weitere Auftragnehmer Aufgaben in der Volksverschlüsselungs-PKI wahrnehmen, so wird durch geeignete Verfahren und Prüfungen sichergestellt, dass die Aufgaben gemäß den Anforderungen aus dem vorliegenden Dokument erfüllt werden. Die Verantwortung für den Betrieb der Volksverschlüsselungs-PKI verbleibt beim Fraunhofer SIT.

Trotz größter Sorgfalt bei der Erstellung des vorliegenden Dokuments kann das Fraunhofer SIT nicht vollständig ausschließen, dass Fehler in den hier beschriebenen Richtlinien enthalten sind. Für diesen Fall lehnt die Fraunhofer Gesellschaft jegliche Haftung ab.

### 9.6.2 Zusicherungen und Gewährleistungen der Registrierungsstelle (RA)

Das Fraunhofer SIT stellt sicher, dass die RA-Aufgaben gemäß den Anforderungen des vorliegenden Dokuments durchgeführt werden.

Es wird zugesichert, dass die Identität der im Zertifikat benannten Person und die E-Mail-Adresse im Rahmen der Zertifikatsbeantragung verifiziert wurden.

### 9.6.3 Zusicherungen und Gewährleistungen der Zertifikatsinhaber

Die Zertifikatsinhaber sichern zu, die in den Abschnitten 1.4.1, 1.4.2 und 4.5.1 beschriebenen Regelungen einzuhalten.

### 9.6.4 Zusicherungen und Gewährleistungen der Zertifikatsnutzer

Die Zertifikatsnutzer sichern zu, die in den Abschnitten 1.4.1, 1.4.2 und 4.5.2 beschriebenen Regelungen einzuhalten.

## 9.7 Gewährleistung

Fraunhofer SIT wird Zertifikate mit der bei ihr üblichen Sorgfalt und unter Zugrundelegung des ihr bekannten Standes der Wissenschaft und Technik herstellen. Für Fehler, die bei Erstellung eines Zertifikats trotz der bei ihm üblichen Sorgfalt und unter Zugrundelegung des ihm bekannten Standes der Wissenschaft und Technik entstehen, haftet die Fraunhofer-Gesellschaft nicht. Darüber hinaus haftet die Fraunhofer-Gesellschaft auch nicht für Mängel, die aufgrund der fehlenden bzw. nicht lückenlosen Verfügbarkeit der Volksverschlüsselungs-PKI auftreten. Mängelansprüche – v.a. bei missbräuchlicher Verwendung des Zertifikats - sind ausgeschlossen.

Der Endteilnehmer hat keinen Anspruch auf unterbrechungsfreien Zugang zum System bzw. auf einen fehlerfreien Zertifizierungsvorgang.

Der Zertifikatsinhaber stellt die Fraunhofer-Gesellschaft von Schäden Dritter, die durch missbräuchliche Nutzung des Zertifikats seinerseits entstehen, frei.

## 9.8 Haftungsbeschränkungen

Die Fraunhofer-Gesellschaft haftet nur im Umfang nach den Abschnitten 9.2 und 9.7.

## 9.9 Schadenersatz

Siehe Abschnitt 9.2 und 9.7.

## 9.10 Gültigkeit und Beendigung der CP/CPS

### 9.10.1 Gültigkeit

Diese VV-X.509-CP/CPS gilt ab dem Zeitpunkt ihrer Veröffentlichung.

### 9.10.2 Beendigung

Diese VV-X.509-CP/CPS bleibt solange in Kraft, bis sie durch eine neue Version ersetzt wird.

### 9.10.3 Wirkung der Beendigung

Auch nach Beendigung der vorliegenden VV-X.509-CP/CPS bleibt diese solange gültig, bis das letzte Zertifikat, das auf Basis dieser VV-X.509-CP/CPS ausgestellt wurde, abgelaufen oder gesperrt wird. Von der Beendigung dieser Zertifizierungsrichtlinie bleibt die Verantwortung zum Schutz vertraulicher und personenbezogener Daten unberührt.

## 9.11 Individuelle Mitteilungen und Kommunikation mit den Teilnehmern

Für Endteilnehmer ist eine Kontaktaufnahme über die E-Mail-Adresse info@volksverschluesselung.de möglich.

## 9.12 Änderungen des Dokuments

### 9.12.1 Verfahren bei Änderungen

Das Fraunhofer SIT behält sich das Recht vor, Änderungen und Anpassungen an diesem Dokument vorzunehmen. Dies kann insbesondere durch eine Weiterentwicklung der technischen Gegebenheiten oder aufgrund sich ändernder Sicherheitsanforderungen erforderlich sein.

Bei Änderungen erhält dieses Dokument eine neue aufsteigende Versionsnummer und ein neues Datum, an welchem die Zertifizierungsrichtlinie aktualisiert wurde. Die Änderungen treten mit Veröffentlichung des Dokuments in Kraft.

### 9.12.2 Benachrichtigungsverfahren und –zeitraum

Eine neue Version wird neben der früheren Version auf der Web-Seite https://volksverschluesselung.de/dokumente.php veröffentlicht.

### 9.12.3 Änderung des Richtlinienbezeichners (OID)

Bei Änderungen entscheidet das Fraunhofer SIT, ob sich daraus signifikante Änderungen der Sicherheit der Zertifizierungsdienste, der Rechte und Pflichten der Teilnehmer oder der Anwendbarkeit der Zertifikate ergeben, die eine Änderung der zu der Richtlinie gehörenden OID (siehe 1.2) zur Folge haben.

## 9.13 Bestimmungen zur Beilegung von Streitigkeiten

Entfällt.

## 9.14 Geltendes Recht

Es gilt das Recht der Bundesrepublik Deutschland.

## 9.15 Einhaltung geltenden Rechts

Das vorliegende Dokument und der Betrieb der Volksverschlüsselungs-PKI unterliegen den geltenden deutschen Gesetzen, Richtlinien und Verordnungen zu Datenschutz und Datensicherheit.

## 9.16 Weitere Regelungen

### 9.16.1 Salvatorische Klausel

Sollte eine der Bestimmungen dieser Zertifizierungsrichtlinie unwirksam sein oder werden, so wird dadurch nicht die Wirksamkeit der übrigen Bestimmungen berührt. Unwirksame Bestimmungen werden durch solche wirksamen Bestimmungen ersetzt, die den angestrebten Zweck weitgehend erreichen.

### 9.16.2 Erfüllungsort

Erfüllungsort ist Darmstadt.

# 10 Referenzen


| | |
|---|---|
| [BSI TR-02012-1] | Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2014.01, 2014 |
| [BSI TR-03130] | BSI: Technische Richtlinie TR-03130. eID-Server |
| [CommonPKI] | T7 & Teletrust: Common PKI Specification, Version 2.0, Januar 2009 |
| [DS-GVO] | VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) |
| [eIDAS-VO] | Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG |
| [REST-API] | Volksverschlüsselung – REST API Documentation |
| [RFC2247] | Using Domains in LDAP/X.500 Distinguihed Names, January 1998 |
| [RFC3647] | X.509 Internet Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003 |
| [RFC4510] | Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map, June 2006 |
| [RFC4511] | Lightweight Directory Access Protocol (LDAP): The Protocol, June 2006 |
| [RFC5280] | X.509 Internet Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile, May 2008 |
| [RFC6960] | X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol - OCSP, June 2013 |
| [SigG] | Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG), Mai 2001, zuletzt geändert durch Art. 4 Abs. 111 G v. 7.8.2013 I 3154 |
| [X.501] | ITU-T Recommendation X.501 \| ISO/IEC 9594-2: Information Technology – Open System Interconnection – The Directory: Models, 10/2012 |
| [X.509] | ITU-T Recommendation \| ISO/IEC 9594-8: Information technology – Open Systems Interconnection – The Directory: Public.key and attribute certificate frameworks, 2005 |
| [x.520] | ITU-T Recommendation \| ISO/IEC 9594-8: Information technology – Open Systems Interconnection – The Directory: Selected attribute types, 10/2012 |

# Anhang A: Abkürzungen und Definitionen

## Abkürzungen

| | |
|---|---|
| BDSG | Bundesdatenschutzgesetz |
| BNetzA | Bundesnetzagentur |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| C | Country Name |
| CA | Certification Authority (Zertifizierungsstelle) |
| CC | Common Criteria |
| CN | Common Name |
| CP | Certificate Policy (Zertifizierungsrichtlinie) |
| CPS | Certificate Policy Statement (Regelungen zum Zertifizierungsbetrieb) |
| CRL | Certificate Revocation List (Sperrliste) |
| CSR | Certificate Signing Request |
| DN | Distinguished Name |
| EAL | Evaluation assurance level |
| eID | elektronischer IDentitätsnachweis |
| FhG | Fraunhofer-Gesellschaft |
| FIPS | Federal Information Processing Standard |
| DS-GVO | Datenschutz-Grundverordnung |
| HSM | Hardware Security Module |
| HTTP | Hypertext Transfer Protocol |
| ISO | International Organization for Standardization |
| ITSEC | Information Technology Security Evaluation Criteria |
| LDAP | Lightweight Directory Access Protocol |
| nPA | neuer Personalausweis |
| O | Organization Name |
| OCSP | Online Certificate Status Protocol |
| OID | Object identifier |
| OU | Organizational Unit Name |
| PKCS | Public Key Cryptography Standards |
| PKI | Public Key Infrastructure |
| RA | Registration Authority (siehe Registrierungsstelle) |
| RFC | Request For Comment |
| Root-CA | Wurzelzertifizierungsstelle |
| S/MIME | Secure Multipurpose Internet Mail Extension |
| SN | Serial Number |
| TLS | Transport Layer Security |
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator |
| UTC | Coordinated Universal Time |
| UTF8 | Unicode Transformation Format-8 |
| VV | Volksverschlüsselung |

# Definitionen

| | |
|---|---|
| Aktivierungsdaten | Vertrauliche Daten, mit denen sich ein Nutzer gegenüber einem System, das den privaten Schlüssel speichert (z.B. HSM, Smartcard, Key-Store), authentisiert und somit den Schlüssel aktiviert. Üblicherweise werden PINs und Passwörter als Aktivierungsdaten verwendet. |
| Asymmetrisches Kryptoverfahren | Kryptographisches Verfahren, dass auf einem Schlüsselpaar beruht, wobei einer öffentlich und einer privat (geheim) ist. |
| Authentisierung, Authentifizierung | Vorgang des Nachweises der Authentizität durch kryptographische Verfahren. Durch ein festgelegtes Verfahren wird festgestellt, ob jemand wirklich derjenige ist, der er vorgibt zu sein. Authentisierung bezeichnet dabei den Nachweis. Authentifizierung bezeichnet die Prüfung des Nachweises. |
| Class 3-Zertifikate | Die Vertrauenswürdigkeit von Zertifikaten ist abhängig von der Art der Überprüfung der Inhalte sowie der Identitätsfeststellung. Dazu werden Zertifikate in Klassen eingeteilt. Je höher die Zertifikatsklasse, desto umfangreichere Identitätsprüfungen liegen der Ausstellung eines Zertifikats zu Grunde.<br><br>Die von der Volksverschlüsselungs-PKI angebotene Zertifikate sind Class 3 Zertifikate.<br><br>Mit der Ausstellung eines Class 3-Zertifikats bestätigt die Volksverschlüsselungs-PKI , dass neben der Überprüfung der E-Mail-Adresse die Identität der im Zertifikat genannten Person in einem sicheren Verfahren festgestellt wurde, beispielsweise durch Nutzung der eID-Funktion des neuen Personalausweises. |
| eID-Funktion des neuen Personalausweises | eID steht für elektronische Identität. Die eID-Funktion des neuen Personalausweises, auch Online-Ausweisfunktion genannt, ermöglicht den sicheren Identitätsnachweis im Internet. |
| Endteilnehmer-Zertifikat | Zertifikat für eine natürliche Person, das nicht zum Zertifizieren anderer Zertifikate oder CRLs verwendet werden darf. |
| Fingerprint | Als Fingerprint eines Zertifikats bezeichnet man den über das gesamte Zertifikat erzeugten Hashwert. |
| Identitätsfeststellung | Überprüfung der Identität einer natürlichen Person. |
| Lightweight Directory Access Protocol (LDAP) | Von der IETF standardisiertes Protokoll zum Zugriff auf Verzeichnisse. |
| OCSP-Responder | Server für die Online-Abfrage von Statusinformationen von Zertifikaten. |
| Öffentlicher Schlüssel | Nicht-geheimer Teil eines Schlüsselpaares bei asymmetrischen Schlüsselpaaren |
| Online Certificate Status Protocol (OCSP) | Von der IETF standardisiertes Protokoll zur Online-Abfrage von Statusinformation von Zertifikaten. |

| | |
|---|---|
| PKCS#10 | Von RSA Security Inc. entwickelter Public-Key Cryptography Standard, um die Zertifizierung eines öffentlichen Schlüssels zu beantragen. |
| PKCS#12 | Von RSA Security Inc. entwickelter Public-Key Cryptography Standard, der ein Dateiformat definiert, um private Schlüssel zusammen mit dem dazugehörigen Zertifikat passwortgeschützt zu speichern. |
| PostIdent | Verfahren der Deutschen Post AG zur sicheren persönlichen Identifikation von Personen. |
| privater Schlüssel | Geheimer Teil eines Schlüsselpaares bei asymmetrischen Schlüsselpaaren |
| Registrierungsstelle (RA) | Komponente der Volksverschlüsselungs-PKI, mit der eine Person kommunizieren muss, um ein Zertifikat zu erhalten. Sie übernimmt die Identifizierung des Zertifikatsinhabers. |
| RSA | Asymmetrisches Kryptoverfahren für Verschlüsselung und elektronischer Signatur, benannt nach Rivest, Shamir, Adleman. |
| S/MIME | Der Standard S/MIME(Secure Multipurpose Internet Mail Extension) ist eine Erweiterung des E-Mail-Formats MIME um kryptographische Sicherheitseigenschaften zur Gewährleistung von Authentizität, Integrität und Vertraulichkeit von Nachrichten. |
| Sperrliste | Liste, in der die Volksverschlüsselungs-PKI Informationen zu gesperrten Zertifikate veröffentlicht. |
| Validierungscode | Zufällig gewählte Nummer zur Validierung der E-Mail-Adresse, die in das Zertifikat eingetragen werden soll. Nachdem der Antragsteller seine E-Mail-Adresse an die RA gesendet hat und diese durch das gewählte Authentifizierungsverfahren noch nicht validiert wurde, wird ihm an diese Adresse eine Bestätigungs-Mail mit dem Validierungscode zugeschickt, den er benötigt, um die Zertifikatsbeantragung fortsetzen zu können. |
| Verzeichnisdienst | Dienst, über den Zertifikate und Sperrlisten abgerufen werden können. |
| Volksverschlüsselungs-Software | Die Volksverschlüsselungs-Software ist eine Anwendung für den Endteilnehmer. Sie wird auf dem Rechner des Endteilnehmers installiert und unterstützt den Endteilnehmer bei der Zertifikatsbeantragung, der Konfiguration der Anwendungen und dem Zertifikatsmanagement. |
| Wurzelinstanz (Root-CA) | Oberste Zertifizierungsstelle einer CA-Hierarchie, deren Zertifikat nicht von einer anderen Zertifizierungsstelle ausgestellt ist, sondern selbst-signiert ist. |
| X.501 | Internationaler Standard, der die Struktur von Verzeichnissen und entsprechende Namensformen zur Identifizierung der Objekte in Verzeichnissen festlegt. |
| X.509 | Internationaler Standard, der ein Format für digitale Zertifikate und Sperrlisten definiert. X.509v3 Zertifikate werden in allen gängigen Public-Key-Infrastrukturen unterstützt. |

| | |
|---|---|
| Zertifikat | Eine elektronische Bescheinigung, die das Schlüsselpaar an die Identität des Zertifikatsinhabers bindet und von einer Zertifizierungsstelle digital unterschieben ist. |
| Zertifikatsinhaber | Natürliche Person, für die ein Zertifikat ausgestellt wird und die im Zertifikatsfeld *Subject* eingetragen ist. |
| Zertifizierungsstelle (CA) | Komponente der Volksverschlüsselungs-PKI, die Endteilnehmer-Zertifikate ausstellt und Sperrinformationen herausgibt. |