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: 1.0
Datum: 29.06.2016

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	Initiale Version 1.0 veröffentlicht

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Das Fraunhofer–Institut für Sichere Informationstechnologie SIT (kurz Fraunhofer SIT), eine Einrichtung 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 bietet Fraunhofer SIT die Public Key Infrastruktur *Volksverschlüsselungs-PKI für X.509-Zertifikate* zur Erzeugung, Ausgabe und Verwaltung von X.509-Zertifikaten, 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 oder akkreditierten Zertifikate nach 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) für die 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	1.0
Objektbezeichnung (Object Identifier, OID):	1.3.36.15.9.1.1.1

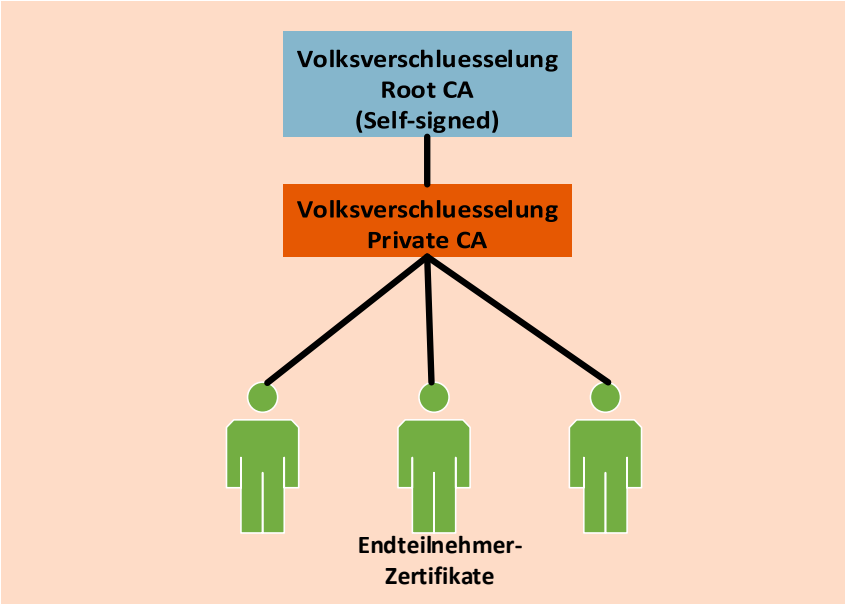
Der OID ist wie folgt zusammengesetzt:
{iso(1) identified-organization(3) teletrust(36) identified organization(15) Fraunhofer Institute for Secure Information Technology SIT (9) Volksverschlüsselung(1) cp/cps(1) Versionsnummer (1)}
Die Versionsnummer kennzeichnet die Hauptversionsnummer (major version).

1.3 Teilnehmer der Volksverschlüsselungs-PKI

1.3.1 Zertifizierungsstellen (Certification Authority, CA)

Die Abbildung 1 zeigt die Zertifizierungshierarchie der Volksverschlüsselungs-PKI. Die Rolle der Instanzen wird im Folgenden genauer erläutert.

Abbildung 1: Zertifizierungshierarchie der Volksverschlüsselungs-PKI



Die Volksverschlüsselungs-PKI folgt einer zweistufigen Zertifizierungshierarchie.

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 (SubCAs) aus.

Die „***Volksverschluesselung Private CA“*** wird unterhalb der „Volksverschluesselung Root CA“ betrieben. Sie stellt nur Zertifikate an natürliche Personen (Endteilnehmer-Zertifikate) zur privaten Nutzung aus. Die private Nutzung der Zertifikate und der zugehörigen Schlüssel ist gegeben, wenn diese an ausschließlich private 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)

Die Registrierungsstelle der Volksverschlüsselungs-PKI nimmt die Zertifikats- und Sperraufträge für Endteilnehmer-Zertifikate entgegen und führt die Identifizierung und Authentifizierung der Antragsteller durch. Als Identitätsnachweis kann unter anderem die Online-Ausweisfunktion des neuen Personalausweises (nPA) bzw. des elektronischen Aufenthaltstitels (eAT) genutzt werden. (vgl. Abschnitt 3.2.2).

Nach erfolgreicher Prüfung leitet die RA den Antrag zur Bearbeitung an die „Volksverschluesselung Private CA“ weiter.

1.3.3 Endteilnehmer (Antragsteller / Zertifikatsinhaber)

Ein Zertifikat der „**Volksverschluesselung Private CA“** kann nur auf eine natürliche Person ausgestellt werden, die im Besitz des privaten Schlüssels ist. Die im Zertifikat genannte Person muss Ihre Identität gegenüber der Registrierungsstelle (RA) nachweisen.

Auf Grund der Identitätsprüfung des Zertifikatsinhabers kann eine Person ein Zertifikat nur für sich selbst beantragen. Antragsteller und Zertifikatsinhaber sind somit identisch.

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.

1.3.5 Weitere Teilnehmer

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

1.4 Zertifikatsverwendung

1.4.1 Zulässige Verwendung von Zertifikaten

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

Endteilnehmer-Zertifikate von der „***Volksverschluesselung Private CA"*** und die zugehörigen Schlüssel dürfen zur Verschlüsselung und zum Signieren von E-Mails und anderen Daten (Schlüssel, Dateien, Nachrichten, etc.) sowie zur Authentisierung (Client-Authentifizierung) bei Anwendungen eingesetzt werden.

Der Zertifikatsinhaber entscheidet, für welche Anwendungen seine Schlüssel und Zertifikate verwendet werden sollen.

Die Endteilnehmer-Zertifikate von der „***Volksverschluesselung Private CA"*** und die zugehörigen Schlüssel dürfen ausschließlich nur zu privaten Zwecken verwendet werden. Private Nutzung der Zertifikate und der zugehörigen Schlüssel ist gegeben, wenn diese an ausschließlich private 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.

Dem Zertifikatsnutzer obliegt es zu prüfen, ob die 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

Endteilnehmer-Zertifikate dürfen nicht als Root-CA- oder CA-Zertifikate verwendet werden. Die Verwendung eines Zertifikats muss den im Zertifikat festgelegten Schlüsselverwendungszwecken (vgl. Abschnitt 7.1.2 KeyUsage) entsprechen.

Eine kommerzielle Nutzung der Zertifikate von der „***Volksverschluesselung Private CA"*** und der zugehörigen Schlüssel 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://www.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

- Endteilnehmer-Zertifikate werden in einem öffentlichen Verzeichnis der Volksverschlüsselungs-PKI veröffentlicht und können über LDAP abgefragt werden, sofern der Zertifikatsinhaber im Rahmen der Zertifikatsbeantragung der Veröffentlichung zugestimmt hat. Eine Zertifikatssuche ist nur nach Eingabe der E-Mail-Adresse möglich. Wird die E-Mail-Adresse nicht vollständig angegeben (Wildcard-Anfrage), erfolgt nur dann eine Antwort, wenn genau ein Eintrag gefunden wird.

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

- Die CA-Zertifikate der Volksverschlüsselungs-PKI und deren Fingerprint werden über die Web-Seite http(s)://volksverschluesselung.de/ veröffentlicht. Zusätzlich werden auf dieser Webseite die Fingerprints der CA-Zertifikate zur Prüfung der Korrektheit und der Authentizität der Zertifikate veröffentlicht.

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

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

  http(s)://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 7.1) vermerkt.

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

2.2 Veröffentlichung von Informationen

Für die Volksverschlüsselungs-PKI werden die in Abschnitt 2.1 genannten Informationen wie dort beschrieben veröffentlicht.

2.3 Aktualisierung der Informationen

Für die in Abschnitt 2.2 genannten Informationen gelten folgende Veröffentlichungsintervalle:

Root-CA-/CA-Zertifikat:	Root-CA- und CA-Zertifikate werden nach der Erzeugung veröffentlicht; eine erneute Publikation erfolgt nur bei Ablauf bzw. Erneuerung.
Endteilnehmer-Zertifikate:	Endteilnehmer-Zertifikate werden nach Erzeugung in den Verzeichnisdienst eingestellt, sofern der Zertifikatsinhaber der Veröffentlichung zugestimmt

	hat. Veröffentlichte Endteilnehmer-Zertifikate werden nach Ablauf ihrer Gültigkeit aus dem Verzeichnisdienst gelöscht.
CRL für CA-Zertifikate:	Die CRL (Sperrliste) für CA-Zertifikate wird turnusmäßig alle 4 Monate aktualisiert und veröffentlicht. Bei Sperrung der CA wird umgehend eine CRL erstellt und veröffentlicht.
CRL für Endteilnehmer-Zertifikate:	Die Sperrliste für Endteilnehmer-Zertifikate wird an den regulären Arbeitstagen (Mo.– Fr.) einmal täglich erzeugt und veröffentlicht, auch wenn keine Sperrungen erfolgten.
OCSP	Die OCSP-Datenquelle wird unmittelbar nach Ausstellung der CRL aktualisiert.
VV-X.509-CP/CPS	Die Veröffentlichung der VV-X.509-CPS/CPS erfolgt jeweils nach ihrer Erstellung oder Aktualisierung.

2.4 Zugang zu den Verzeichnissen

Für die in Abschnitt 2.1 aufgeführten Informationen sowie das Suchen nach Zertifikaten über den Verzeichnisdienst und die Nutzung des OCSP-Responder gibt es keine Zugriffsbeschränkung für lesenden Zugriff. Die Informationen sind öffentlich und unentgeltlich 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 7.1.3) und im Feld „Subject" Angaben zum Zertifikatsinhaber. Diese Namen werden entsprechend dem Standard [X.501] und dem [RFC5280] als DistinguishedNames (DN) vergeben. Ein DN enthält eine Folge von 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)
- emailAddress (E)

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 *eMailAddress* enthält (zusätzlich zur Angabe in der X.509-Extension *SubjectAltName)* die E-Mail-Adresse des Zertifikatsinhabers.

Beispiel:
CN = Erika Anna-Maria Mustermann
SN = Mustermann
G = Erika Anna-Maria
E = erika01@name.de

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 Registrierung 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 verwendete Name des Zertifikatsinhabers im Feld *SubjectDN* ist durch das Attribut eMailAdresse 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 vom Endteilnehmer generiert.

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 von natürlichen Personen

Die vom Zertifizierungsdienst „Volksverschluesselung Private CA" ausgestellten Zertifikate sind an natürliche Personen gebunden. Die Authentifizierung der Identität von Endteilnehmern 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 mittels 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 ein Festnetz-Account bei der Deutschen Telekom AG. Der Antragsteller authentifiziert sich gegenüber der Volksverschlüsselung mit seinem Telekom-Login.

3. Registrierungscode: Der Antragsteller authentifiziert sich gegenüber der Volksverschlüsselung mit seinem Registrierungscode, den er vorab im Rahmen einer Vor-Ort-Registrierung erhalten hat. Hierzu muss sich der Endteilnehmer persönlich durch ein gültiges Ausweisdokument ausweisen.

Nach erfolgreicher Identitätsfeststellung werden im Rahmen der Zertifikatsbeantragung folgende Daten erhoben, geprüft und in das Zertifikat übernommen

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

3.2.3 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.

3.2.4 Prüfung der Berechtigung zur Antragsstellung

Entfällt, da Zertifikate von der „Volksverschluesselung Private CA“ ausschließlich für natürliche Personen ausgestellt werden.

3.2.5 Kriterien für Interoperation (Cross-Zertifizierung)

Entfällt. Eine Cross-Zertifizierung mit anderen Zertifizierungsstellen ist nicht geplant.

3.3 Identifizierung und Authentifizierung bei Zertifikatserneuerung

3.3.1 Routinemäßige Zertifikatserneuerung

Es liegt in der Verantwortung des Zertifikatsinhabers, sich rechtzeitig vor Ablauf der Gültigkeit eines Zertifikats ein neues Zertifikat für ein neues Schlüsselpaar zu beschaffen. Es gilt das in Abschnitt 3.2 beschriebene Verfahren.

3.3.2 Zertifikatserneuerung nach Sperrung

Nach der Sperrung eines Zertifikats muss ein neues Zertifikat gemäß Abschnitt 3.2 beantragt werden.

3.4 Identifizierung und Authentifizierung bei Zertifikatssperrung

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

Zur Authentifizierung einer Sperrung muss der Zertifikatsinhaber das Sperrkennwort eingeben, das ihm im Rahmen der Zertifikatsbeauftragung per E-Mail sicher übermittelt wurde.

4 Betriebliche Anforderungen im Lebenszyklus von Zertifikaten

4.1 Zertifikatsbeantragung

4.1.1 Wer kann ein Zertifikat beantragen

Zertifikate können alle Personen gemäß Abschnitt 1.3.3 beantragen. Die Antragstellung erfolgt online über die auf dem Rechner des Endteilnehmers installierte Volksverschlüsselungs-Software.

4.1.2 Registrierungsprozess

Ein Zertifikat kann erst ausgestellt werden, wenn der Registrierungsprozess erfolgreich abgeschlossen wurde und von der Registrierungsinstanz (RA) ein geprüfter Zertifizierungsantrag an die CA übermittelt wurde.

Im Rahmen der Beantragung werden mittels der auf dem Rechner des Endteilnehmers installierten Volksverschlüsselungs-Software folgende Schritte durchlaufen:

- Die Identität des Endteilnehmers wird entsprechend dem ausgewählten Authentifizierungsverfahren (siehe Abschnitt 3.2.2) festgestellt.

- Die angegebene E-Mail-Adresse, die in das Zertifikat übernommen werden soll, wird validiert. In diesem Fall wird an die angegebene E-Mail-Adresse eine Bestätigungsmail mit einem Validierungscode gesendet, der eine begrenzte Gültigkeit (maximal 8 Tage) besitzt. Wird innerhalb dieser Frist der Validierungscode nicht an die Registrierungsstelle gesendet oder nach 3-maliger Falscheingabe des Validierungscode, wird der Registrierungsprozess 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 (vgl. Abschnitt 3.2.1). Außerdem wird vom Endteilnehmer die Einwilligung zur Veröffentlichung seiner Zertifikate im Verzeichnisdienst (vgl. Abschnitt 2.1) eingeholt.

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

- Nach erfolgreicher Überprüfung der Authentizität der Zertifikats-Requests 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 Ausstellung der Endteilnehmer-Zertifikate basiert auf einer erfolgreichen Authentifizierung der Identität des Zertifikatsinhabers gemäß Abschnitt 3.2, die von der Registrierungsstelle durchgeführt wird (vgl. Abschnitt 4.1.2).

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Zertifikatsanträge werden an die Registrierungsinstanz der Volksverschlüsselungs-PKI gerichtet.

Ein Anspruch auf Annahme eines Antrags besteht nicht. Ein Zertifikatsantrag kann in folgenden Fällen abgelehnt werden:

- Die angegebene Mailadresse erscheint anstößig.
- Die Identität des Antragstellers kann nicht festgestellt werden.
- Der Validierungscode ist ungültig.
- Für die angegebene E-Mail-Adresse wurden bereits Zertifikate ausgestellt, die noch gültig sind.

Nach erfolgreicher Prüfung des Zertifikatsantrags wird dieser an die Zertifizierungsstelle „Volksverschluesselung Private CA“ weitergeleitet.

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 Zertifikatsanträge an die Zertifizierungsstelle übermittelt. Auf Basis der Zertifikatsanträge werden die entsprechenden Zertifikate erstellt. Die ausgestellten Zertifikate werden persistent gespeichert und an die Registrierungsstelle der Volksverschlüsselungs-PKI 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 von Zertifikaten

4.4.1 Übergabe und Annahme der Zertifikate

Nachdem die Zertifikate erzeugt wurden, stehen diese auf dem Download-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 Endteilneh-

mers 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 einer Woche nicht abgeholt, werden sie gesperrt und aus dem Verzeichnisdienst gelöscht, falls der Endnutzer bei der Zertifikatsbeantragung der Veröffentlichung zugestimmt hatte.

4.4.2 Veröffentlichung der Zertifikate

Die Volksverschlüsselungs-PKI veröffentlicht die ausgestellten Endteilnehmer-Zertifikate gemäß Abschnitt 2.1 im Verzeichnisdienst, 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 „Volksverschlüsselung Private CA“ darf nur in Anwendungen benutzt werden, die in Übereinstimmung mit dem 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.

Wenn der private Schlüssel abhandenkommt, gestohlen wird oder eine Kompromittierung nicht ausgeschlossen werden kann, sollte der Zertifikatsinhaber 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 von der Volksverschlüsselungs-PKI **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 Volksverschlüsselungs-PKI erfolgt nicht.

Die durchzuführenden Prozessschritte entsprechen denen derr 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, ändern, sollte der Zertifikatsinhaber neue Zertifikate für neue Schlüsselpaare beantragen. Die durchzuführenden Prozessschritte entsprechen denen der Erstbeantragung und es gelten die Regelungen unter Abschnitt 3.2 und 4.1ff. Noch gültige Zertifikate sollten vom Zertifikatsinhaber gesperrt werden.

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 nicht mehr korrekt (z.B. Namensänderung bei Heirat),

4. das Zertifikat wird nicht mehr benötigt.

Der Zertifizierungsdienst 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. Des Weiteren muss er denn Sperrcode eingeben, der ihm an die E-Mail-Adresse im Rahmen der Zertifikatsbeantragung zugesendet wurde. Es werden immer alle drei Zertifikate des Zertifikatsinhabers mit gleicher E-Mail-Adresse gesperrt.

Die Authentifizierung des Zertifikatsinhabers gegenüber der Registrierungsstelle 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

Siehe Abschnitt 2.3.

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.

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

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.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

Die Volksverschlüsslungs-PKI wird im Auftrag des Fraunhofer SIT von der Deutschen Telekom AG betrieben. Die Infrastruktur wird von der Deutschen Telekom AG in einem gem. ISO 27001 zertifiziertem Rechenzentrum in Deutschland betrieben.

Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen sind im CPS der Volksverschlüsselungs-PKI beschrieben.

6 Technische Sicherheitsmaßnahmen

Technische Sicherheitsmaßnahmen sind im CPS der Volksverschlüsselungs-PKI beschrieben.

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)	Die von der Volksverschlüsselungs-PKI ausgestellten X.509-Zertifikate entsprechen der Version v3. Der codierte Wert im Zertifikatsfeld ist 2
SerialNumber	71:fb:32:04:bf:fa:8c:17	Eindeutiger Wert zur Identifikation des Zertifikats innerhalb der Volksverschlüsselungs-PKI
Signature	sha256WithRSAEncryption (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	Datum und Uhrzeit	Gültigkeitszeitraum des Zertifikats (von – bis); UTC-kodiert gemäß RFC 5280
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 (OID = 1.2.840.113549.1.1.1)	

Public Key	RSA 4096 Bit	Schlüssel und Schlüssellänge
Extensions - Zertifikatserweiterungen		
AuthorityKeyIdentifier (non-critical)	Identisch mit SubjectKeyIdentifier	Informationen zur Identifizierung des öffentlichen Schlüssels des Ausstellers.
SubjectKeyIdentifier (non-critical)	Hashwert über den SubjectPublicKey im Feld SubjectPublicKeyInfo	Informationen zur Identifizierung des öffentlichen Schlüssels des Zertifikats
KeyUsage (critical)	keyCertSign crlSign	Verwendungszweck des Schlüssels
BasicConstraints (critical)	CA=TRUE	Informationen zum Zertifikatstyp
signatureAlgorithm	sha256WithRSAEncryption (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)	Die von der Volksverschlüsselungs-PKI ausgestellten X.509-Zertifikate entsprechen der Version v3. Der codierte Wert im Zertifikatsfeld ist 2
SerialNumber	0e:cf:8a:22:c5:9e:c7:87	Eindeutiger Wert zur Identifikation des Zertifikats innerhalb der Volksverschlüsselungs-PKI
Signature	sha256WithRSAEncryption (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	Datum und Uhrzeit	Gültigkeitszeitraum des Zertifikats (von – bis); UTC-kodiert gemäß RFC 5280
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 (OID = 1.2.840.113549.1.1.1)	
Public Key	RSA 4096 Bit	Schlüssel und Schlüssellänge
Extensions - Zertifikatserweiterungen		
AuthorityKeyIdentifier (non-critical)	KeyIdentifier des Schlüssel der Volksverschlusselung Root CA	Informationen zur Identifizierung des öffentlichen Schlüssels des Ausstellers.
SubjectKeyIdentifier (non-critical)	Hashwert über den SubjectPublicKey im Feld SubjectPublicKeyInfo	Informationen zur Identifizierung des öffentlichen Schlüssels des Zertifikats
KeyUsage (critical)	keyCertSign crlSign	Verwendungszweck des Schlüssels
BasicConstraints (critical)	CA=TRUE Pathlen=0	Informationen zum Zertifikatstyp
Certificates Policies (non-critical)	X.509v3 Any Policy (OID: 2.5.29.32.0)	Referenz auf die Policies (CP/CPS)
CRLDistributionPoints (Non-critical)	http://volksverschluesselung.de/crl/rootca.crl	CRL-Issuer and URL zur Sperrliste
AuthorithyInfoAccess	http://volksverschluesselung.de/ca/rootca.crt	Angaben über die Quelle von Statusinformationen für die Validierung des Zertifikats
signatureAlgorithm	sha256WithRSAEncryption (OID=1.2.840.113549.1.1.11)	Hash- und Signaturalgorithmus der Zertifizierungsstelle „Volksverschluesselung Root

		CA“
SignatureValue	Signatur	Signatur der Zertifizierungsstelle

7.1.3 Zertifikatsprofil des OCSP-Signaturertifikats der „Volksverschluesselung Private CA“

Zertifikatsfeld	Wert	Bemerkung
Version	V3 (0x2)	Die von der Volksverschlüsselungs-PKI ausgestellten X.509-Zertifikate entsprechen der Version v3. Der codierte Wert im Zertifikatsfeld ist 2
SerialNumber	Seriennummer	Eindeutiger Wert zur Identifikation des Zertifikats innerhalb der Volksverschlüsselungs-PKI
Signature	sha256WithRSAEncryption (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		
CountryName	DE	
OrganisationName	Fraunhofer SIT	
CommonName	Domain-Name	
SubjectPublicKeyInfo – Öffentlicher Schlüssel des Zertifikatsinhabers gemäß RFC 5280		
Algorithm	RsaEncryption (OID = 1.2.840.113549.1.1.1)	
Public Key	RSA 2048 Bit	Schlüssel und Schlüssellänge

Extensions - Zertifikatserweiterungen		
AuthorityKeyIdentifier (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 (critical)	digitalSignature	Verwendungszweck des Schlüssels
BasicConstraints (critical)	CA=FALSE	Informationen zum Zertifikatstyp
Certificates Policies (non-critical)	VV-X509-CP/CPS (OID: 1.3.36.15.9.1.1.1)	Referenz auf die Policies (CP/CPS)
ExtendedKeyUsage	OCSPSigning	Erweiterte Nutzung des Schlüssels
signatureAlgorithm	sha256WithRSAEncryption (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)	Die von der Volksverschlüsselungs-PKI ausgestellten X.509-Zertifikate entsprechen der Version v3. Der codierte Wert im Zertifikatsfeld ist 2
SerialNumber	Seriennummer	Eindeutiger Wert zur Identifikation des Zertifikats innerhalb der Volksverschlüsselungs-PKI
Signature	sha256WithRSAEncryption	Hash- und Signaturalgorith-

	(OID=1.2.840.113549.1.1.11)	mus 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	
eMailAddress	Private E-Mail-Adresse des Zertifikatsinhabers	
Title (optional)	Titel	
surName	Name	
givenName	Vorname(n)	
SubjectPublicKeyInfo – Öffentlicher Schlüssel des Zertifikatsinhabers gemäß RFC 5280		
Algorithm	RsaEncryption (OID = 1.2.840.113549.1.1.1)	
Public Key	RSA 2048 Bit	Schlüssel und Schlüssellänge
Extensions - Zertifikatserweiterungen		
AuthorityKeyIdentifier (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 (critical)	keyEncipher dataEncipher	Verwendungszweck des Schlüssels
BasicConstraints (critical)	CA=FALSE	Informationen zum Zertifikatstyp
Certificates Policies (non-critical)	VV-X509-CP/CPS (OID: 1.3.36.15.9.1.1.1)	Referenz auf die Policies (CP/CPS)
ExtendedKeyUsage	eMailProtection	Erweiterte Nutzung des

	Microsoft EFS	Schlüssels
SubjectAltNames (non-critical)	Private E-Mail-Adresse des Zertifikatsinhabers	Weitergehende Informationen zu Subject
CRLDistributionPoints (Non-critical)	http://volksverschluesselung.de/crl/privateca.crl	CRL-Issuer and URL zur Sperrliste
AuthorithyInfoAccess	http://volksverschluesselung.de/ca/privateca.crt http://ocsp.volksverschluesslung.de	Angaben über die Quelle von Statusinformationen für die Validierung des Zertifikats
signatureAlgorithm	sha256WithRSAEncryption (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)	Die von der Volksverschlüsselungs-PKI ausgestellten X.509-Zertifikate entsprechen der Version v3. Der codierte Wert im Zertifikatsfeld ist 2
SerialNumber	Seriennummer	Eindeutiger Wert zur Identifikation des Zertifikats innerhalb der Volksverschlüsselungs-PKI
Signature	sha256WithRSAEncryption (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	
eMailAddress	Private E-Mail-Adresse des Zertifikatsinhabers	
Title (optional)	Titel	
surName	Name	
givenName	Vorname(n)	
SubjectPublicKeyInfo – Öffentlicher Schlüssel des Zertifikatsinhabers gemäß RFC 5280		
Algorithm	RsaEncryption (OID = 1.2.840.113549.1.1.1)	
Public Key	RSA 2048 Bit	Schlüssel und Schlüssellänge
Extensions - Zertifikatserweiterungen		
AuthorityKeyIdentifier (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 (critical)	digitalSignature nonReputiation	Verwendungszweck des Schlüssels
BasicConstraints (critical)	CA=FALSE	Informationen zum Zertifikatstyp
Certificates Policies (non-critical)	VV-X509-CP/CPS (OID: 1.3.36.15.9.1.1.1)	Referenz auf die Policies (CP/CPS)
ExtendedKeyUsage	eMailProtection	Erweiterte Nutzung des Schlüssels
SubjectAltNames (non-critical)	Private E-Mail-Adresse des Zertifikatsinhabers	Weitergehende Informationen zu Subject
CRLDistributionPoints (Non-critical)	http://volksverschluesselung.de/crl/privateca.crl	CRL-Issuer and URL zur Sperrliste
AuthorithyInfoAccess	http://volksverschluesselung.de/ca/privateca.crt http://ocsp.volksverschluesslung.de	Angaben über die Quelle von Statusinformationen für die Validierung des Zertifikats

signatureAlgorithm	sha256WithRSAEncryption (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)	Die von der Volksverschlüsselungs-PKI ausgestellten X.509-Zertifikate entsprechen der Version v3. Der codierte Wert im Zertifikatsfeld ist 2
SerialNumber	Seriennummer	Eindeutiger Wert zur Identifikation des Zertifikats innerhalb der Volksverschlüsselungs-PKI
Signature	sha256WithRSAEncryption (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	
eMailAddress	Private E-Mail-Adresse des Zertifikatsinhabers	
Title (optional)	Titel	
surName	Name	
givenName	Vorname(n)	
SubjectPublicKeyInfo – Öffentlicher Schlüssel des Zertifikatsinhabers gemäß RFC 5280		
Algorithm	RsaEncryption	

	(OID = 1.2.840.113549.1.1.1)	
Public Key	RSA 2048 Bit	Schlüssel und Schlüssellänge
Extensions - Zertifikatserweiterungen		
AuthorityKeyIdentifier (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 (critical)	digitalSignature	Verwendungszweck des Schlüssels
BasicConstraints (critical)	CA=FALSE	Informationen zum Zertifikatstyp
Certificates Policies (non-critical)	VV-X509-CP/CPS (OID: 1.3.36.15.9.1.1.1)	Referenz auf die Policies (CP/CPS)
ExtendedKeyUsage	clientAuth	Erweiterte Nutzung des Schlüssels
SubjectAltNames (non-critical)	Private E-Mail-Adresse des Zertifikatsinhabers	Weitergehende Informationen zu Subject
CRLDistributionPoints (Non-critical)	http://volksverschluesselung.de/crl/privateca.crl	CRL-Issuer and URL zur Sperrliste
AuthorithyInfoAccess	http://volksverschluesselung.de/ca/privateca.crt http://ocsp.volsverschluesslung.de	Angaben über die Quelle von Statusinformationen für die Validierung des Zertifikats
signatureAlgorithm	sha256WithRSAEncryption (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 der CA 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 1 zeigt das Profil der Sperrlisten, die von der Volksverschlüsselungs-PKI ausgestellt werden:

Tabelle 1: Profil der Sperrlisten

Zertifikatsfeld	**Bedeutung**	**Inhalt**
TBSCertList		
Version	Zertifikatsversion	Abschnitt 7.2.1
Signature	OID des verwendeten Signaturalgorithmus der Zertifizierungsstelle	Abschnitt 7.1.3
Issuer	DName der Zertifizierungsstelle (Aussteller)	Abschnitt 7.1.4
ThisUpdate	Gültig ab (creation time)	UTCTime kodiert gemäß RFC 5280
NextUpdate	Nächste Aktualisierung	UTCTime kodiert gemäß RFC 5280
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	Verwendeter Signaturalgorithmus der Zertifizierungsstelle	Abschnitt 7.1.3
SignatureValue	Signatur der Zertifizierungsstelle	

7.2.1 Versionsnummer(n)

Die von der Volksverschlüsselungs-PKI ausgestellten X.509-Zertifikatssperrlisten entsprechen der Version 2 gemäß [RFC2580]. Delta-CRLs sind nicht vorgesehen.

7.2.2 Erweiterungen der Sperrliste

Die Sperrlisten der Volksverschlüsselungs-PKI unterstützen die folgenden Erweiterungen:

Tabelle 2: Erweiterungen der Sperrlisten

Feld	Bedeutung	Inhalt	Kritikalität
crlEntryExtensions			
reasonCode	Grund der Revozierung; entspricht dem Wert in den Antworten des OCSP-Responders	Kodierung nach RFC 5289	nicht kritisch
crlExtensions			
authorityKeyIdentifier	Identifiziert den öffentlichen Schlüssel der CA, die die CRL signiert hat.	Hashwert über den öffentlichen Schlüssel der CA.	nicht kritisch
CRLNumber	Sperrlistennummer	Fortlaufende Seriennummer der Sperrliste	kritisch

7.3 OCSP-Profil

Der OCSP-Responder der Volksverschlüsselungs-PKI erfüllt die Anforderungen des RFC 6960[1] [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 verwendet bei Anfragen (OCSP Request) die folgenden Erweiterungen:

Tabelle 3: Zulässige Erweiterungen der OCSP-Anfragen

Feld	Bedeutung	Kritikalität
Nonce	Wert, der die Anfrage kryptographisch an die Antwort bindet (Abwehr von	nicht kritisch

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

	Replay Attacken, optional ???)	
AcceptableResponses	Der Client kann in einer Anfrage angeben, welche OCSP-Antwort-Typen er versteht.	nicht kritisch
ServiceLocator	Weiterleitung der Anfrage an einen anderen OCSP-Server, der für das Zertifikat zuständig ist.	nicht kritisch

Der OCSP-Responder verwendet bei Antworten (OCSP Response) die folgenden Erweiterungen:

Tabelle 4: Erweiterungen der OCSP-Antworten

Feld	**Bedeutung**	**Kritikalität**
Nonce	Gleicher Wert wie in der Anfrage. Nicht existent, fall in Anfrage nicht vorhanden	nicht kritisch
CrlID	Referenz auf CRL auf Basis derer der OCSP-Responder den Status eines Zertifikats ermittelt.	nicht kritisch
ArchiveCutoff	Zeitdifferenz zwischen Aufbewahrungsfrist für Statusinformationen und dem Zeitpunkt der Statusauskunft.	nicht kritisch
CrlEntryExtensions	vgl. Abschnitt 7.2.2	nicht kritisch / kritisch

8 Audits und andere Prüfungen

8.1 Prüfungsintervall

Die Einhaltung der VV-X509-CP/CPSVV-X509-CP/CPS wird in regelmäßigen Abständen 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

Der Prüfer ist in keiner Weise an der Leitung, der Administration und dem Betrieb der Volksverschlüsselungs-PKI beteiligt. Außerdem ist der Prüfer weder direkt noch indirekt von der Volksverschlüsselungs-PKI oder seinen Mitarbeitern abhängig.

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 zur Identitätsfeststellung 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. Hierzu wurde ein Datenschutzkonzept erstellt, das den Schutz der vertraulichen personenbezogenen Daten regelt. Technische und organisatorische Maßnahmen gemäß § 9 BDSG und der Anlage zu § 9 BDSG sind sichergestellt.

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 VV-PKI richtet sich nach § 11 BDSG, 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 § 3 Abs. 1 BDSG.

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 nach § 5 BDSG 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.

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)

Die VV-PKI sichert zu, dass die von ihr erzeugten Zertifikate alle Anforderungen der vorliegenden CP/CPS 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 die Haftung – außer in Fällen von Vorsatz oder grober Fahrlässigkeit - ab.

9.6.2 Zusicherungen und Gewährleistungen der Registrierungsstelle (RA)

Die Volksverschlüsselungs-PKI verpflichtet sich, die RA-Aufgaben gemäß den Anforderungen des vorliegenden Dokuments nach bestem Wissen und Gewissen durchzuführen.
Die Zertifizierungsstelle „Volksverschluesselung Private CA“ stellt sicher, 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 ihm üblichen Sorgfalt und unter Zugrundelegung des ihm bekannten Standes der Wissenschaft und Technik erstellen. 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

Der Zertifizierungsdienst Volksverschlüsselungs-PKI 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 jeder Änderung 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

Über signifikante Änderungen der VV-X.509-CP/CPS, wie beispielsweise Änderungen des Registrierungsablaufs, des Verzeichnis- oder Sperrdienstes, werden Zertifikatsinhaber durch Veröffentlichung auf der Webseite https.//www.volksverschluesselung.de informiert.

9.12.3 Änderung des Richtlinienbezeichners (OID)

Die Entscheidung über die Zuweisung einer neuen OID für die VV-X.509-CP/CPS ist Teil des Aktualisierungsprozesses. Bei signifikanten Änderungen hinsichtlich beispielsweise der Sicherheit, der Verfahrensabläufe und / oder der Rechte und Pflichten wird die Hauptversionsnummer (vgl. Abschnitt 1.2) um 1 erhöht. In diesem Fall wird die OID der aktualisierten VV-X.509-CP/CPS angepasst. Anderenfalls bleibt die OID unverändert.

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
[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, Version 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

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
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
VV-CLASS3-PKI	Volksverschlüsselung-PKI für Class 3 Zertifikate

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	Kryptografisches 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 Zertifikat zu Grunde. Die von der Volksverschlüsselungs-PKI angebotene Zertifikate sind Class 3 Zertifikate. Mit der Ausstellung eines Class 3-Zertifikats bestätigt die VV-CLASS3-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 VV-CLASS3-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, 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 Zertifi-

	katsfeld *Subject* eingetragen ist.
Zertifizierungsstelle (CA)	Komponente der VV-CLASS3-PKI , die Endteilnehmer-Zertifikate ausstellt und Sperrinformationen herausgibt.