Certification Practice Statement (CPS)

VR-Ident SSL-Zertifikate (Web-Trust)

FIDUCIA GAD
ZUKUNFTSERFAHREN

IT-Partner der FinanzGruppe
Volksbanken Raiffeisenbanken

Certification Practice Statement (CPS)

VR-Ident SSL-Zertifikate (WebTrust)

Version:	Version 3.02.04, Freigegeben
Zielgruppe:	Nutzer und Besitzer von VR-Ident SSL-Zertifikaten
Datum/Uhrzeit:	16.01.2019 / 09:47 Uhr

Gegenüber der vorherigen Ausgabe wurden folgende Änderungen vorgenommen:

Nummer	Datum	Inhalt / Änderungen
3.2.2	07.02.2018	Kapitel 0.0.0:
3.2.3	24.08.2018	Änderungen wegen neuer Baseline Requirements
3.2.4	14.12.2018	Hinweis auf Betriebseinstellung EV und OV eingefügt

Zusammenfassung
Das vorliegende Dokument ist ein "Certification Practice Statement" (CPS) für den Zertifizierungsdienst VR-Ident für VR-Ident SSL-Zertifikat (WebTrust).

Öffentlich (C1) - Nutzer und Besitzer von VR-Ident SSL-Zertifikaten

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Einleitung

1.1. Überblick

Wichtiger Hinweis: Einstellung des Betriebs
Der Betrieb der VR IDENT EV SSL CA und der VR IDENT OV SSL CA wird am 01.01.2019 beendet.
Nach deisem Datum werden keine VR Ident EV SSL oder OV SSL Zertifikate mehr ausgestellt.
Alle noch gültigen Zertifikate werden vorher durch inhaltlich äquivalente Zertifikate des Ausstellers Quo Vadis ersetzt.
Die Verzeichnisdienste zum Sperrstatus und die Sperrdienste werden noch bis zum 31.03.2019 weiter betrieben.
Nach diesem Datum werden auch diese Dienste eingestellt. Alle dann noch gültigen VR Ident EV SSL and OV SSL Zertifikate werden zu diesem Zeitpunkt gesperrt.
Alle archivierten Daten und Unterlagen sind bei der *Fiducia & GAD IT AG* noch für wenigstens 7 Jahre nach dem 31.03.2019 gemäß Kapitel 5.5 des CPS vefügbar.

Die *Fiducia & GAD IT AG* ist ein IT-Dienstleister und Softwarehaus für mehr als 1100 Banken. Zweck des Unternehmens ist die wirtschaftliche Förderung und Betreuung ihrer Mitglieder im Bereich der Informationstechnologie.

Im Rahmen dieser IT-Dienstleistungen bietet die *Fiducia & GAD IT AG* auch *Zertifizierungsdienste* für die Erzeugung, Ausgabe und Verwaltung von digitalen Zertifikaten an. Diese Dienstleistung wird im Folgenden mit "*Zertifizierungsdienst* VR-Ident" bezeichnet.

SSL-Server-Zertifikate werden von dem *Zertifizierungsdienst* VR-Ident unter dem Namen "VR-Ident SSL-Zertifikat" angeboten.

In Ausnahmen können auch Zertifikate gemäß dieser Richtlinien erstellt werden, die zusätzlich noch Bedingungen der Richtlinie "*Certification Practice Statement*" (*CPS*) für den *Zertifizierungsdienst* VR-Ident für VR-Ident EV SSL-Zertifikate (siehe Anhang mit VR-Ident Referenzen) erfüllen.

Das vorliegende Dokument ist ein "*Certification Practice Statement*" (*CPS*) für den *Zertifizierungsdienst* VR-Ident für VR-Ident SSL-Zertifikate.

Die hier beschriebenen Zertifikate werden wahlweise innerhalb folgender CA-Hierarchien erstellt:

- unterhalb einer *Root-CA* der *Fiducia & GAD IT AG*
- unterhalb einer externen *Root-CA*

Die *CA* wurden gemäß den folgenden Anforderungen durch einen externen Auditor geprüft und zertifiziert:

- Trust Service Principles and Criteria for Certification Authorities
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

Falls es eine neuere Version des Dokumentes "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" geben sollte (siehe www.cabforum.org) und falls es zu Abweichungen der Anforderungen in dieser aktuelleren Version gegenüber diesem Dokument kommen sollte, haben die Anforderungen in dieser aktuelleren Version höhere Priorität als die entsprechenden Ausführungen in diesem Dokument. Der "*Zertifizierungsdienst* VR-Ident" wird, falls notwendig, sowohl dieses Dokument in einer aktuelleren Version als auch die Prozesse zum Ausstellen der VR-Ident Zertifikate anpassen.

Die nachfolgenden Anforderungen werden von der *CA* erfüllt:

- Mozilla CA Certificate Inclusion Policy.

Der *Zertifizierungsdienst* VR-Ident gewährleistet die Einhaltung der Richtlinien des "CA Browser Forum" in der aktuellen Version (http://www.cabforum.org) für die Beantragung, Generierung, Auslieferung und Verwaltung der VR-Ident SSL Zertifikate. Im Falle eines Widerspruchs zwischen dem "*Certification Practice Statement*" (*CPS*) für den *Zertifizierungsdienst* VR-Ident für VR-Ident SSL Zertifikate und den Richtlinien des "CA Browser Forum", gelten die Richtlinien des "CA Browser Forum" vorrangig.

Details mit Verweisen zu den Dokumenten sind in dem Anhang mit allgemeinen Referenzen zu finden.

1.1.1. Zweck des Dokuments

Nach *RFC* 3647 legt das "*Certification Practice Statement*" (*CPS*) die Praktiken dar, die eine *Zertifizierungsstelle* VR-Ident bei der Ausgabe der Zertifikate anwendet. Dementsprechend beschreibt das vorliegende Dokument das Vorgehen des *Zertifizierungsdienst* VR-Ident bei der Beantragung, Generierung, Auslieferung und Verwaltung der VR-Ident Zertifikate. Das Dokument beschreibt im Einzelnen:

- Die Bedeutung und Verwendung von VR-Ident Zertifikaten,
- die Beantragung und Erstellung von VR-Ident Zertifikaten,
- die Erneuerung von VR-Ident Zertifikaten,
- die Sperrung von VR-Ident Zertifikaten,
- Verzeichnis- und Sperrinformationsdienste,
- die technische und organisatorische Sicherheit,
- Details zu den Inhalten der VR-Ident Zertifikate und *CRL* (Sperrlisten) sowie
- weitere geschäftliche und rechtliche Regelungen.

Die Dokumentenstruktur orientiert sich an dem *RFC* 3647.

Das vorliegende *CPS* (*Certification Practice Statement*) beschreibt den aktuellen Status der Zertifizierungsabläufe und der Sicherheitsmaßnahmen und ermöglicht somit eine qualitative Einschätzung des *Zertifizierungsdienst* VR-Ident.

Das *CPS* (*Certification Practice Statement*) gilt ausschließlich für die in Kapitel 1.1.2 genannten Produkte.

Vorgaben für die Bedeutung und Verwendung von VR-Ident Zertifikaten werden in dem Dokument "VR-Ident Certificate Policy (CP) für VR-Ident Zertifikate (WebTrust)" (siehe Anhang mit VR-Ident Referenzen) und in dem Dokument "QuoVadis Root Certification Authority Certificate Policy/Certification Practice Statement" (siehe Anhang mit allgemeinen Referenzen) definiert.

1.1.2. Das VR-Ident Zertifikat

Zertifikate sind jene "Ausweise" zur bestmöglich gesicherten Kommunikation im Internet, mit denen ein Nutzer sich selbst ausweisen und seine Inhalte authentifizieren kann. Mit Zertifikaten erhalten Personen, Organisationen oder IT-Systeme einen jeweils eigenen, eindeutigen und unverfälschbaren Sicherheitsausweis. VR-Ident bietet hierfür u.a. unterschiedliche Lösungen an:

- VR-Ident SSL (maschinengebunden)
- VR-Ident mail (personengebunden)
- VR-Ident SMIME (personengebunden)
- VR-Ident privat (personengebunden)

VR-Ident SSL-Zertifikate sind der digitale Ausweis für den Server. Sie machen einen Internetserver identifizierbar und binden eine Unternehmensidentität daran. Das *Zertifikat* setzt sich zusammen aus den geprüften Angaben des Zertifikatsinhabers, dem *öffentlichen Schlüssel* des Servers, Daten zum Aussteller des Zertifikats sowie aus der Signatur des *Zertifizierungsdienst*eanbieters *Fiducia & GAD IT AG*. Durch die Möglichkeit der Verschlüsselung über *SSL* beziehungsweise TLS wird für die Sicherheit der Kommunikation zwischen einem Browser und einem Server gesorgt. Die Verschlüsselungsstärke richtet sich nach den Möglichkeiten des Servers und des Browsers.

Mittels eines VR-Ident SSL-Zertifikats bescheinigt der *Zertifizierungsdienst* VR-Ident dem Webauftritt einer Organisation seine Identität. Die Sicherstellung der Identität basiert auf dem Nachweis, dass die Organisa-

tion tatsächlich existiert, dass die Organisation die Beantragung des Zertifikats genehmigt hat und dass die Person, welche den Antrag im Namen der Organisation gestellt hat, hierzu berechtigt war. Das *Zertifikat* bietet ebenfalls die Sicherstellung, dass die Nutzung des Domainnamens, der in dem Zertifikatsantrag genannt wurde, berechtigt ist.

VR-Ident SSL-Zertifikate können von Komponenten benutzt werden, welche Zertifikate nach *X.509* in der Version 3 korrekt interpretieren und verwenden können. Die Zertifikatsprofile sind in Kapitel 7.1 (S. 40) beschrieben.

1.2. Dokumentenname und Identifikation

Die Bezeichnung aller Richtliniendokumente des *Zertifizierungsdienst* VR-Ident setzen sich wie folgt zusammen:

- Name der Produktfamilie "VR-Ident"
- "Certification Practice Statement (CPS)" oder "Certificate Policy (CP)"
- "für"
- Name des Produktes

Version des vorliegenden Dokumentes: 3.02.04

Freigabedatum des vorliegenden Dokumentes: 12.2018

Der Bezeichner "17696" ist fest für Publikationen und weiteres der "*Fiducia & GAD IT AG*" vergeben. Die ersten Stellen der *Object Identifier* (OID) der Richtliniendokumente des *Zertifizierungsdienst* VR-Ident sind somit fest vergeben: 1.3.6.1.4.1.17696

Details hierzu sind in einem frei zugänglichen OID Repository einzusehen: http://www.oid-info.com/get/1.3.6.1.4.1.17696

Der ASN.1 *Object Identifier* (OID) für dieses Dokument lautet: 1.3.6.1.4.1.17696.4.1.1.5.3.2

Die Dokumentenbezeichnung für das vorliegende CPS lautet: "VR-Ident Certification Practice Statement (CPS) für VR-Ident SSL-Zertifikate (WebTrust)".

Der ASN.1 *Object Identifier* (OID) für die dazugehörige "*Certificate Policy*" (*CP*) ("VR-Ident Certificate Policy (CP) für VR-Ident Zertifikate (WebTrust)"): 1.3.6.1.4.1.17696.4.1.1.9.3.2

1.3. Teilnehmer der Zertifizierungsinfrastruktur (PKI)

1.3.1. Zertifizierungsstellen (CA) und Zertifizierungshierarchie

Im folgenden sind die Zertifizierungsstellen (*CA*) und die Zertifizierungshierarchie der VR-Ident PKI des *Zertifizierungsdienst* VR-Ident beschrieben.

Der *Zertifizierungsdienst* VR-Ident stellt im Sinne dieses Dokumentes die *Zertifizierungsstelle* VR-Ident dar, welche VR-Ident Zertifikate ausstellt. Für die in Kapitel 1 genannten Zertifikatstypen verwendet die *Zertifizierungsstelle* VR-Ident mehrere Zertifizierungsinstanzen. Hierbei handelt es sich um logische Einheiten, die jeweils einem oder mehreren Schlüsselpaaren zur Signierung der Zertifikate zugeordnet sind.

Die Zertifizierungsinstanzen, welche die VR-Ident Zertifikate für Endentitäten ausstellen, erhalten die Zertifikate zu ihren Signaturschlüsseln von einer übergeordneten Root *CA*. Hierzu wird vom *Zertifizierungsdienst* VR-Ident die folgende Hierarchie zur Verfügung gestellt:

- Die Zertifizierungsinstanzen, welche die VR-Ident Zertifikate für Endentitäten ausstellen wurden über ein Root Signing von einer externen *Root-CA* der Firma Quo Vadis ("QuoVadis Root CA 2") erstellt.

*CA*s, die von dem *Zertifizierungsdienst* VR-Ident erstellt werden, enthalten am Ende des Namens (CN) die Jahreszahl der Erstellung. Die Jahreszahl wird in diesem Dokument größtenteils weggelassen. Sie wird nur

explizit angegeben, falls das im jeweiligen Kontext notwendig ist. Teilweise wird die Jahreszahl bei dem Namen der *CA* mit "[JJJJ]" anstatt der konkreten Jahreszahl vermerkt werden.

Zertifizierungshierarchie mit "QuoVadis Root CA 2"

Der *Zertifizierungsdienst* VR-Ident verwendet für die Ausstellung der "VR-Ident SSL-Zertifikate", welche unterhalb der "QuoVadis Root CA 2" ausgestellt werden, die nachfolgende *Zertifizierungshierarchie*:

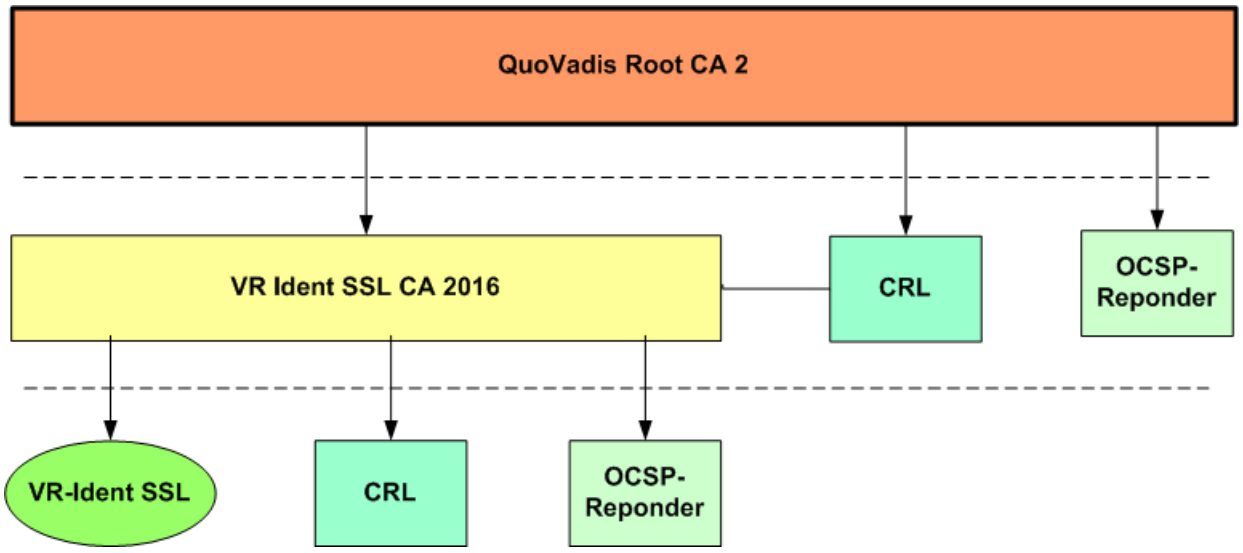

Abb. 1.1. Zertifizierungshierarchie für VR-Ident SSL-Zertifikate mit der "QuoVadis Root CA 2"

Beschreibung der Zertifizierungshierarchie:

Die *Zertifizierungshierarchie* besteht aus drei Hierarchieebenen, die im Folgenden kurz erläutert werden:

- Auf der obersten Ebene dieser *Zertifizierungshierarchie* befindet sich die "QuoVadis Root CA 2", die unter anderem das *Zertifikat* der "VR IDENT SSL CA 2016" sowie die entsprechende *CRL* (*Sperrliste*)signiert.
- Auf der zweiten Hierarchieebene befindet sich die "VR IDENT SSL CA 2016", die
  - die "VR-Ident SSL-Zertifikate", also die SSL-Server-Zertifikate der Kunden,
  - die Zertifikate des *OCSP-Responder* für Zertifikatsabfragen für "VR-Ident SSL-Zertifikate" und
  - die *CRL* (*Sperrliste*) mit den Informationen zum *Sperrstatus* für die "VR-Ident SSL-Zertifikate" ausstellt.
- Auf der dritten Hierarchieebene befinden die "VR-Ident SSL-Zertifikate" der Kunden, *OCSP-Responder* und *CRL* (*Sperrliste*).

1.3.2. Registrierungsinstanzen

Eine Registrierungsinstanz (RA) ist die Organisationseinheit einer PKI-Infrastruktur, welche die Identifizierung und *Authentisierung* des Antragstellers durchführt, Zertifikatserneuerungen veranlasst und Sperranträge entgegennimmt. Sie ist die Stelle, mit der eine Person oder ein System kommunizieren muss, um ein digitales *Zertifikat* zu erhalten. Die *RA* (*Registration Authority*) kann Aufträge autorisieren oder ablehnen.

Die *RA* (*Registration Authority*) für VR-Ident Zertifikate befindet sich in den Räumlichkeiten der *Fiducia & GAD IT AG*.

Die *RA* (*Registration Authority*) für VR-Ident Zertifikate befindet sich in den Räumlichkeiten der *Fiducia & GAD IT AG*. Der *Zertifizierungsdienst*eanbieter *Fiducia & GAD IT AG* handelt also als *RA* (*Registration Authority*). Von der *RA* (*Registration Authority*) werden Anträge zur Ausstellung, Sperrung und Erneuerung entgegen genommen und geprüft.

1.3.3. Antragsteller

1.3.3.1. Auftraggeber

Auftraggeber für VR-Ident SSL-Zertifikate sind juristische Personen, welche die Ausstellung eines VR-Ident SSL-Zertifikats durch den *Zertifizierungsdienst* VR-Ident beantragen. Der *Zertifizierungsdienst* VR-Ident stellt VR-Ident SSL-Zertifikate an juristische Personen (wie z. B. Banken, Industrieunternehmen usw.) aus.

Es wird zwischen folgenden Auftraggebern unterschieden:

- *Fiducia & GAD IT AG* (oder *Fiducia & GAD IT AG* Konzerntöchter) zur Beantragung von VR-Ident SSL-Zertifikaten für Subdomains von Domains, die von der *Fiducia & GAD IT AG* ausschließlich verwendet werden (beispielsweise: www.fiduciagad.de),
- *VR-Banken* zur Beantragung von VR-Ident SSL-Zertifikaten für ihre eigenen Domains,
- *Fiducia & GAD IT AG* Konzerntöchter und Verbundpartner zur Beantragung von VR-Ident SSL-Zertifikaten für ihre eigenen Domains.

1.3.3.2. Zertifikatseigentümer

Zertifikatseigentümer von VR-Ident SSL-Zertifikaten ist die Entität, für die das *Zertifikat* ausgestellt wird. Der *Zertifikatseigentümer* ist im *Zertifikat* als "Subject" eingetragen. Der *Zertifikatseigentümer* kann, muss aber nicht gleichzeitig Auftraggeber sein.

1.3.4. Vertrauende Dritte

Vertrauende Dritte sind Personen oder Organisationen, die sich auf die Ordnungsmäßigkeit der VR-Ident Zertifikate, die vom *Zertifizierungsdienst* VR-Ident der *Fiducia & GAD IT AG* ausgestellt wurden, verlassen.

1.3.5. Andere Teilnehmer

Keine.

1.4. Anwendung von Zertifikaten

1.4.1. Zulässige Anwendung von Zertifikaten

Die Anwendung von VR-Ident Zertifikaten darf nur gemäß den nachfolgenden Bedingungen erfolgen und darf nicht gegen gesetzliche Regelungen verstoßen.

VR-Ident SSL-Zertifikate dürfen nur zur *Authentifizierung* des entsprechenden Servers genutzt werden. Die sichere Kommunikation erfolgt mittels *SSL* beziehungsweise TLS Sicherheitsstandard. Wird das Zertifikat für eine hoch frequentierte FQDN (high-traffic FQDN) eingesetzt, so muss der Betreiber dieser Webseite OCSP stapling beim TLS Handshake aktivieren.

1.4.2. Unzulässige Anwendung von Zertifikaten

Für alle VR-Ident Zertifikate gelten folgende Nutzungsbeschränkungen und -verbote:

- VR-Ident Zertifikate sind nicht zur Verwendung oder zum Weitervertrieb als Kontroll- oder Steuerungsinstrumente in gefährlichen Umgebungen oder für Verwendungszwecke, bei denen ein ausfallsicherer Betrieb erforderlich ist, vorgesehen. Weiterhin dürfen VR-Ident Zertifikate nicht zum Betrieb von nuklearen Einrichtungen, Flugzeugnavigations- oder Flugkommunikationssystemen, Luftverkehrs-Kontrollsystemen oder Waffenkontrollsystemen, wobei ein Ausfall direkt zum Tode, zu Personenschäden oder zu schweren Umweltschäden führen kann, verwendet werden. Eine Verwendung zu den genannten Zwecken wird ausdrücklich ausgeschlossen.

- Die Anwendung der VR-Ident Zertifikate muss der Im *Zertifikat* angegebenen Schlüsselnutzung (siehe Kapitel 4.5 (S. 18)) entsprechen.
- Weitere Informationen zur unzulässigen Nutzung von VR-Ident Zertifikaten sind unter http://www.vr-ident.de veröffentlicht.
- Ein VR-Ident SSL-Zertifikat darf nicht im Namen einer anderen Organisation verwendet werden.
- Es ist untersagt, ein VR-Ident SSL-Zertifikat zur Durchführung von Verfahren mit privaten Schlüsseln oder *öffentlichen Schlüssel*n in Verbindung mit einem anderen Domänennamen oder Organisationsnamen, als den bei der Registrierung eingereichten Namen zu verwenden.
- Ein VR-Ident SSL-Zertifikat darf ausschließlich für die vertraglich vereinbarte Anzahl von Servern beziehungsweise Diensten eingesetzt werden.
- Nach Ablauf der Gültigkeitsdauer oder Sperrung des VR-Ident SSL-Zertifikats dürfen die zertifizierten Schlüssel nicht mehr verwendet werden.
- VR-Ident SSL-Zertifikate dürfen nicht für sogenannte „Man-in-the-Middle“-Angriffe missbraucht werden. Die Verwendung für Domänen, die nicht im Besitz oder Zugriff des Antragstellers sind, ist ausgeschlossen, das gilt auch für geschlossene, interne Umgebungen.

1.5. Policy Verwaltung

1.5.1. Organisation für die Verwaltung dieses Dokuments

Zuständig für die Verwaltung und Genehmigung dieses Dokumentes ist:
Fiducia & GAD IT AG
Abteilung: PPMASK
GAD Straße 2-6
48163 Münster
Internet: http://www.vr-ident.de

1.5.2. Kontaktperson

Ansprechpartner für Fragen bezüglich dieses Dokumentes ist:
Fiducia & GAD IT AG
Abteilung: PPMASK
GAD Straße 2-6
48163 Münster
E-Mail: IND_Zertifikatsverwaltung@fiduciagad.de[1]

1.5.3. Zuständigkeit für die Abnahme des CP/CPS

Für die Abnahme und Verabschiedung dieses Dokumentes ist die Leitung der in Kapitel 1.5.1 (S. 6) genannten Abteilung zuständig. Das Dokument behält seine Gültigkeit, solange es nicht von dieser Instanz widerrufen wird oder durch eine aktualisierte Version ersetzt wird.

1.5.4. Abnahmeverfahren des CP/CPS

Dieses Dokument wird bei Bedarf fortgeschrieben und erhält dann jeweils eine neue aufsteigende Versionsnummer. Es wird von der Leitung der in Kapitel 1.5.1 (S. 6) genannten Abteilung abgenommen. *CP* (*Certificate Policy*) und *CPS* (*Certification Practice Statement*) werden hierbei aufeinander abgestimmt. Es findet mindestens einmal jährlich ein Review von CP und CPS statt.

[1] mailto:IND_Zertifikatsverwaltung@fiduciagad.de

1.6. Definitionen und Abkürzungen

Definitionen und Abkürzungen siehe im Glossar.

2. Bekanntmachung und Verzeichnisdienst

2.1. Verzeichnisse

Der *Zertifizierungsdienst* VR-Ident stellt öffentliche Informationen zur VR-Ident PKI unter der Adresse http://www.vr-ident.de zur Verfügung. Im Intranet (Zugriff nur für Beschäftigten der *Fiducia & GAD IT AG* und die Mitarbeiter der *Fiducia & GAD IT AG* Mitgliedsbanken) werden weitere interne Informationen zur Verfügung gestellt.

Der *Zertifizierungsdienst* VR-Ident betreibt folgende Verzeichnisse zur Veröffentlichung von Zertifikatsinformationen:

- VR-Ident Zertifikate können über einen öffentlichen *Verzeichnisdienst* abgerufen werden. Personengebundene VR-Ident Zertifikate können nur im VR-Ident *Verzeichnisdienst* abgerufen werden, wenn der *Zertifikatseigentümer* diesem zugestimmt hat. Der VR-Ident *Verzeichnisdienst* ist unter der folgenden Adresse zu erreichen:
  ldap://www.vr-ident.de

- Zur Online-Abfrage steht ein *OCSP-Responder* zur Verfügung. Über diesen Verifikationsdienst kann der Status aller Zertifikate online abgerufen werden. Er ist unter der folgenden Adresse zu erreichen:
  http://ocsp.vr-ident.de/gtnocsp/OCSPResponder/<Name der CA>

- Der *Zertifizierungsdienst* VR-Ident erstellt zusätzlich *CRL* (Sperrlisten) mit Sperrinformationen von Zertifikaten. Die Sperrlisten können über die folgende Adresse eingesehen werden:
  http://www.vr-ident.de/gtncrl/CRLResponder/<Name der CA>
  und
  ldap://www.vr-ident.de (die *CRL* (*Sperrliste*) ist in dem Attribut des jeweiligen CA-Objektes gespeichert)

Die CA-Zertifikate des *Zertifizierungsdienst* VR-Ident werden über die Webseite http://www.vr-ident.de veröffentlicht. Zusätzlich werden auf dieser Webseite die *Fingerprints* (*Hashwerte*) der VR-Ident CA-Zertifikate veröffentlicht, die zur Prüfung der Korrektheit und *Authentizität* der Zertifikate vor ihrer Installation im System genutzt werden sollten. Die Webseite gibt Instruktionen, wie die Prüfung des *Fingerprints* vorgenommen werden kann.

2.2. Veröffentlichung von Zertifikatsinformationen

Der *Zertifizierungsdienst* VR-Ident veröffentlicht

- Ausgestellte VR-Ident Zertifikate (bei personengebundenen Zertifikaten, sofern der Inhaber der Veröffentlichung zugestimmt hat), in den in Kapitel 2.1 (S. 8) genannten Verzeichnissen,

- *CRL* (Sperrlisten), unter der in Kapitel 2.1 (S. 8) genannte Adresse,

- Das vorliegende *CPS* (*Certification Practice Statement*), das unter http://www.vr-ident.de herunter geladen werden kann,

- Allgemeine Geschäftsbedingungen für die Teilnehmer und vertrauende Dritte, die unter http://www.fiduciagad.de herunter geladen werden können.

Weitere geschäftliche und rechtliche Bestimmungen sind in Kapitel 9 (S. 49) des vorliegenden *CPS* (*Certification Practice Statement*) aufgeführt und werden somit veröffentlicht.

2.3. Häufigkeit und Zyklen für Veröffentlichungen

Die Veröffentlichung der VR-Ident Zertifikate (bei personengebundenen Zertifikaten, sofern der Inhaber der Veröffentlichung zugestimmt hat) erfolgt direkt nach ihrer Erstellung. Die Zertifikate verbleiben mindestens sieben Jahre nach ihrem Gültigkeitsablauf im VR-Ident *Verzeichnisdienst*.

Die *CRL* (Sperrlisten) werden unmittelbar nach der Erstellung veröffentlicht und sind aus dem VR-Ident *Verzeichnisdienst* abrufbar. Die Veröffentlichung von *CRL* (Sperrlisten) erfolgt regelmäßig mit folgenden Fristen:

- *CRL* (Sperrlisten) der CA-Zertifikate werden mindestens jährlich und nach jeder Sperrung eines CA-Zertifikats erstellt.
- *CRL* (Sperrlisten) für VR-Ident SSL-Zertifikate werden alle 7 Tage oder vor Gültigkeitsablauf der bestehenden *CRL* (*Sperrliste*) erstellt.

CP und CPS werden mindestens einmal jährlich einem Review unterzogen. Aktualisierungen des vorhandenen Dokuments werden gemäß Kapitel 9.12 (S. 53) veröffentlicht. Die Veröffentlichung der *CP* (*Certificate Policy*) und des *CPS* (*Certification Practice Statement*) erfolgt jeweils nach ihrer Erstellung oder ihrer Aktualisierung.

Aktualisierungen der allgemeinen Geschäftsbedingungen und weiterer Sonderbedingungen für den *Zertifizierungsdienst* VR-Ident erfolgen nach Bedarf.

2.4. Zugriffskontrolle auf Verzeichnisse

Die in dem VR-Ident *Verzeichnisdienst* veröffentlichte Information ist öffentlich zugänglich. Der Lesezugriff auf den VR-Ident *Verzeichnisdienst* ist nicht beschränkt.

Dagegen haben nur berechtigte *Rollenträger* von VR-Ident Änderungsrechte für den VR-Ident *Verzeichnisdienst*.

Der *Zertifizierungsdienst* VR-Ident hat entsprechende Sicherheitsmaßnahmen implementiert, um ein unbefugtes Ändern von Einträgen im VR-Ident *Verzeichnisdienst* zu verhindern.

3. Identifizierung und Authentisierung

3.1. Namensgebung

3.1.1. Namenstypen

Die vom *Zertifizierungsdienst* VR-Ident erstellten Zertifikate erhalten eindeutige Namen (DistinguishedName) in den Feldern issuer und subject nach *X.501*.

Im Feld issuer erhalten die VR-Ident SSL-Zertifikate die Attribute:

- CommonName (CN) = VR IDENT SSL CA 2016
- Organization (O) = FIDUCIA & GAD IT AG
- Organizational Unit (OU) = VR IDENT
- Country (C) = DE

Im Feld subject erhalten die VR-Ident SSL-Zertifikate die Attribute:

- CommonName (CN) = Domainname oder URL der Organisation, gemäß Registrierung durch den Registrar der entsprechenden Top-Level Domain
- Organization (O) = Name der Organisation oder der Firma, gemäß des Eintrags in dem entsprechenden Register
  - falls der Registereintrag nicht eindeutig ist, kann hier auch der Sitz des Unternehmens ergänzt werden, wie beispielsweise: Eintrag im Genossenschaftsregister "Volksbank eG", dann kann "Volksbank eG Musterstadt" in Organization übernommen werden
  - falls im Handelsregister eine Zweigstelle/Zweigniederlassung (assumed name) mit abweichendem Firmennamen eingetragen ist, kann diese als Organisationsname eingetragen werden. In diesem Fall folgt in Klammern der Name der Organisation oder der Firma, gemäß des Eintrags in dem entsprechenden Register, wie beispielsweise "Bürgerbank Musterstadt (Volksbank Musterstadt eG)"
- Organizational Unit (OU) = "VR-Ident" (Standardeinstellung), es kann optional vom *Antragsteller* eine alternative OU angegeben werden, diese kann eine Abteilung, ein Bereich oder eine andere Unterteilung der Organisation oder Firma sein. Es dürfen hier keine fremden Organisationsnamen, Markennamen, Ortsbezeichnungen, fiktive bzw. angenommene Geschäftsnamen (amerikanisch DBA) oder ähnliches verwendet werden.
- Locality (L) = Sitz der Organisation oder der Firma, gemäß des Eintrags in dem entsprechenden Register
- State (ST) = Bundesland in welchem sich die Stadt mit dem Sitz der Organisation oder der Firma, gemäß des Eintrags in dem entsprechenden Register, befindet
- Country (C) = DE für Organisationen, die in Deutschland ansässig sind

Die Attribute Locality (L) und State (ST) können gekürzt werden, müssen aber als Wertepaar eine sinnvolle Kombination ergeben, das dem Sitz der Organisation entspricht.

Außerdem enthalten die Zertifikate in der Erweiterung SubjectAltName mindestens den oben genannten CommonName (CN) und optional weitere alternative Domainnamen als DNS-Name. Für alle alternativen Domainnamen müssen alle weiteren Attribute gültig sein.

Wildcard-Zertifikate werden in VR-Ident SSL-Zertifikaten nur nach Rücksprache mit dem *Zertifizierungsdienst* VR-Ident unterstützt. Wildcard Zeichen "*" können nur unterhalb einer Subdomain vergeben werden.

3.1.2. Anforderung an die Bedeutung von Namen

CA-Zertifikate enthalten im Attribut CommonName im Feld subject Namen, welche die Identität der entsprechenden *CA* als Inhaber des Zertifikats erkennen lassen.

VR-Ident SSL-Zertifikate enthalten im Attribut Organization im Feld subject Namen, welche die Organisation oder die Firma als Inhaber des Zertifikats erkennen lassen.

Durch die Attribute Locality (Stadt) und State (Bundesland) wird eindeutig identifiziert, wo sich der Sitz der Organisation oder der Firma befindet.

Das Attribut OrganizationalUnit enthält den Namen einer Abteilung, einen Bereich oder eine andere Unterteilung dieser Organisation oder Firma, die dazu berechtigt ist, das Zertifikat zu verwenden. Es dürfen hier keine fremden Organisationsnamen, Markennamen, Ortsbezeichnungen, fiktive bzw. angenommene Geschäftsnamen (amerikanisch DBA) oder ähnliches verwendet werden. Alternativ kann hier der Begriff "VR-Ident" verwendet werden.

Das Attribut CommonName enthält den Namen der URL oder der Domain, der durch den Registrar der entsprechenden Top-Level Domain festgelegt wurde[1]. Außerdem enthalten die Zertifikate in der Erweiterung SubjectAltName mindestens den CommonName und optional weitere alternativen Domainnamen als DNS-Name, für welche die gleichen Bedingungen wie in dem Attribut CommonName gelten.

Desweiteren sind weder im CommonName noch in einem der SubjectAltName internationalisierte Domain Namen (Umlaut- oder Sonderzeichendomains) erlaubt.

3.1.3. Anonymität und Pseudonyme für Zertifikatseigentümer

Pseudonyme und anonyme VR-Ident Zertifikate werden vom *Zertifizierungsdienst* VR-Ident nicht unterstützt.

3.1.4. Regeln zur Interpretation verschiedener Namensformen

Im Namen dürfen ausschließlich die folgenden Zeichen verwendet werden:

A-Z, a-z, 0-9, Leerzeichen, ', (,), +, -, ,, ., /, :, ?.

Optional können die folgenden "deutschen" Sonderzeichen verwendet werden:

Ä, Ö , Ü , ä , ö, ü , ß

Für die Ersetzung deutscher Sonderzeichen gelten folgende Substitutionsregeln:

Ä -> Ae, Ö ->Oe, Ü -> Ue, ä -> ae, ö -> oe, ü -> ue, ß -> ss

Sonderzeichen mit Akzenten verlieren diese. Ansonsten wird eine für das betreffende Zeichen gemeinhin verwendete Schreibweise aus den Zeichen a-z und A-Z so zusammengesetzt, dass der entsprechende Laut entsteht.

Generell wird empfohlen auf Sonderzeichen und Umlaute zu verzichten.

3.1.5. Eindeutigkeit von Namen

Die Subject *Distinguished Name* (*DN*) sind eindeutig.

3.1.6. Erkennung, Authentisierung und Rolle von geschützten Namen

Die Namen der Organisationen in den VR-Ident SSL-Zertifikaten sind identisch mit dem Unternehmensnamen im entsprechenden Register. Somit ist der Namenschutz gegeben.

3.2. Erstmalige Identitätsprüfung

3.2.1. Methode zum Besitznachweis des privaten Schlüssels

Der Beantragende eines Zertifikats muss die *Authentizität* der verwendeten Schlüssel nachweisen. Er muss legitimieren, dass er den *privaten Schlüssel*, der dem im *Zertifikat* anzugebenden *öffentlichen Schlüssel*

[1] VR-Ident SSL-Zertifikate werden weder für IP Adressen noch für interne Servernamen ausgestellt.

entspricht, rechtmäßig besitzt. Hierzu werden geeignete *asymmetrische Kryptoverfahren* verwendet. Der Besitznachweis erfolgt in der Regel durch die Übermittlung eines selbst-signierten *PKCS*#10 Requests im Rahmen der Beantragung der Zertifikate.

Bei allen Domains, wo die *Fiducia & GAD IT AG* bei dem Registrar einer Top-Level-Domain als Inhaber registriert ist, entfällt der Besitznachweis des *privaten Schlüssel*s durch den *Antragsteller*. In diesem Fall hat die *Fiducia & GAD IT AG* das Recht, Zertifikate für diese Domains direkt zu beantragen. Die Schlüssel und Zertifikatsanfragen werden in einer gesicherten Umgebung im Rechenzentrum der *Fiducia & GAD IT AG* generiert.

3.2.2. Authentisierung von Organisationen

Der *Zertifizierungsdienst* VR-Ident unterscheidet zwischen personengebundenen und maschinengebundenen Zertifikaten. Dementsprechend findet auch die *Authentisierung* von Personen bzw. Maschinen statt. Organisationen werden somit nur für maschinengebundene Zertifikate authentisiert. Maßgeblich für die Authentisierung von Organisationen ist ein gültiger Eintrag (nicht als gelöscht, ungültig, inaktiv oder nicht aktuell gekennzeichnet) in einem öffentlichen Register. Der Name der Organisation in dem Antrag muss identisch sein mit dem Eintrag in dem jeweiligen Verzeichnis.

Es werden nur Nachweise und Antragsformulare in lateinischer Schrift und in deutscher Sprache akzeptiert.

Es werden nur Organisationen akzeptiert, die in einem der folgenden Verzeichnis eingetragen sind:

- Handelsregister (HRB)
- Genossenschaftsregister (GnR)

Der Eintrag in dem o.g. Verzeichnis muss den Status "aktuell" haben.

Zur Feststellung der Identität des Zertifikatseigentümers von VR-Ident SSL-Zertifikaten prüft der *Zertifizierungsdienst* VR-Ident die Existenz des beauftragenden Unternehmens und die Eigentumsverhältnisse seines Domainnamens.

Fiducia & GAD IT AG Mitarbeiter oder Mitarbeiter von *Fiducia & GAD IT AG* Konzerntöchtern, die dazu berechtigt sind, dürfen VR-Ident SSL-Zertifikate für Subdomains von Domains, die von der *Fiducia & GAD IT AG* ausschließlich verwendet werden (beispielsweise www.fiduciagad.de), beantragen. Folgende Prüfungen werden hier direkt oder indirekt durchgeführt:

- Die Identifizierung des Auftraggebers erfolgt durch ein sicheres Anmeldeverfahren am VR-Ident Workflow Management System,
- Anträge von Mitarbeitern von *Fiducia & GAD IT AG* Konzerntöchtern müssen von einem *Fiducia & GAD IT AG* Mitarbeiter, der dazu berechtigt ist, betätigt werden,
- Die Abteilung und der Auftraggeber müssen dazu berechtigt sein, VR-Ident SSL-Zertifikate für Subdomains von Domains, die von der *Fiducia & GAD IT AG* ausschließlich verwendet werden (beispielsweise www.fiduciagad.de) ausstellen zu lassen,
- Die Hoheit über den *privaten Schlüssel* liegt in der Abteilung des Auftraggebers,
- Es können nur Zertifikate für Subdomains von Domains, die von der *Fiducia & GAD IT AG* ausschließlich verwendet werden (das heißt, die *Fiducia & GAD IT AG* ist durch den Registrar der entsprechenden Top-Level Domain (hier: DENIC) als Domaininhaber eingetragen, beispielsweise www.fiduciagad.de) beantragt werden, dieses muss den Angaben im Zertifikat Request unter "Common Name" entsprechen,
- Der Eintrag im Zertifikat Request unter "Country" muss gleich "DE" sein,
- Der Eintrag im Zertifikat Request unter "Organization" muss gleich "*Fiducia & GAD IT AG*" sein,
- Der Eintrag im Zertifikat Request unter "Organizational Unit" muss gleich "VR-Ident" sein oder dem Abteilungsnamen des Antragstellers entsprechen,

- Die Einträge im Zertifikat Request unter "Locality" und "State" müssen den Angaben der *Fiducia & GAD IT AG* ("L=FRANKFURT AM MAIN", "ST=HESSEN") entsprechen.

VR-Banken können VR-Ident SSL-Zertifikate über das GAD Service-Portal bestellen. Folgende Prüfungen werden hier direkt oder indirekt durchgeführt:

- Die Identifizierung des Auftraggebers erfolgt im GAD Service-Portal anhand der Host Kennung und des RACF Passworts,

- Prüfung, ob *Fiducia & GAD IT AG* durch den Registrar der entsprechenden Top-Level Domain als Domaininhaber der angegeben URL oder der angegebenen Domäne eingetragen ist, die im Feld "Common Name" genannt wurde,
  - Falls das nicht der Fall ist, muss der Auftraggeber eine Abtrittserklärung an die *Fiducia & GAD IT AG* übergeben,

- Online-Prüfung anhand des entsprechenden Registers, ob die Angaben im Feld "Organization" identisch mit den Angaben in dem Register sind,
  - ist dieser größer 64 Byte muss eine entsprechende Abkürzung gewählt werden, falls der Registereintrag nicht eindeutig ist, kann hier auch der Sitz des Unternehmens ergänzt werden, wie beispielsweise: Eintrag im Genossenschaftsregister "Volksbank eG", dann kann "Volksbank eG Musterstadt" in Organization übernommen werden,

- Überprüfung der Angaben im Zertifikat Request unter den Feldnamen "Organizational Unit" anhand der bei der *Fiducia & GAD IT AG* vorhandenen Unterlagen (alternativ kann hier der Begriff "VR-Ident" verwendet werden),

- Überprüfung der Angaben im Zertifikat Request unter den Feldnamen "Locality" anhand des Handelsregisterauszugs,

- Überprüfung der Angaben im Zertifikat Request unter den Feldnamen "State", welches dem Bundesland entsprechen muss, in welchem sich die Stadt mit dem Sitz der Organisation oder der Firma, gemäß des Eintrags im Handelsregister, befindet

- Der Eintrag im Zertifikat Request unter "Country" muss für Organisationen, die in Deutschland ansässig sind, gleich "DE" sein.

Nach Erhalt des Antrags auf VR-Ident SSL-Zertifikate von *Fiducia & GAD IT AG* Konzerntöchtern und Verbundpartnern sowie vor der Zertifikatsausstellung werden die folgenden Prüfungen durchgeführt:

- Prüfung, ob der Auftraggeber durch den Registrar der entsprechenden Top-Level Domain als Domaininhaber der angegeben URL oder der angegebenen Domäne eingetragen ist, die im Feld "Common Name" genannt wurde,

- Prüfung des entsprechenden Registereintrages oder vergleichbarer Unterlagen (siehe Kapitel 4.1.2 (S. 16)) auf

  - Echtheit und Vollständigkeit,

  - Verifikation der Kontrolle über die Domain durch Rückfrage per E-Mail oder Telefon beim Domain-Kontakt, der im DNS-Registereintrag genannt ist

- Die Angaben im Feld "Organization" müssen identisch mit den Angaben in dem Register sein

  - Ist der Name der Firma größer 64 Byte muss eine entsprechende Abkürzung gewählt werden,

  - Die Firma muss mindestens 3 Jahre existent sein,
    - oder es muss sich um ein reguliertes Finanzinstitut handeln
    - oder der Antragsteller muss einen bestätigen Nachweis erbringen, dass die Firma oder Organisation ein Konto bei einem regulierten Finanzinstitut unterhält

- Die Firma muss eine *Fiducia & GAD IT AG*-Konzerntochter oder ein bekanntes Unternehmen im genossenschaftlichen Verbund sein,
- der sogenannte d/b/a Name ("geschäftstätig als ...", aus dem amerikanischen Rechtsraum) wird nicht unterstützt

- Überprüfung der Angaben im Zertifikat Request unter den Feldnamen "Organizational Unit" anhand der bei der *Fiducia & GAD IT AG* vorhandenen Unterlagen, diese Abteilung muss in der Organisation oder der Firma existent sein und der *Antragsteller* muss dieser angehören, alternativ kann hier der Begriff "VR-Ident" verwendet werden,
- Überprüfung der Angaben im Zertifikat Request unter dem Feldnamen "Locality" anhand des Handelsregisters,
- Überprüfung der Angaben im Zertifikat Request unter dem Feldnamen "State", welches dem Bundesland entsprechen muss, in welchem sich die Stadt mit dem Sitz der Organisation oder der Firma, gemäß des Eintrags im Handelsregisters, befindet
- Es werden nur Anträge von Auftraggebern aus Deutschland bearbeitet, wodurch der Eintrag bei Country (="DE") fest vorgegeben ist,
- Die Prüfung ob der Antragsteller dazu berechtigt ist den Zertifikatsantrag zu stellen erfolgt durch die sichere Anmeldung an den *VR-Ident Workflow Management* System.
- Prüfung, ob die im Zertifikatsantrag genannten Personen dazu berechtigt sind, VR-Ident SSL-Zertifikate im Namen der Organisation zu beauftragen erfolgt durch eine Handlungsvollmacht oder durch eine telefonische Nachfrage bei einem Zeichnungsberechtigten der Organisation über den bestätigten Kommunikationskanal.

3.2.3. Authentisierung von Personen

Der *Zertifizierungsdienst* VR-Ident unterscheidet zwischen personengebundenen und maschinengebundenen Zertifikaten. Dementsprechend findet auch die *Authentisierung* von Personen bzw. Maschinen statt. Personen werden somit nur für personengebundene Zertifikate authentisiert.

Es werden nur Nachweise und Antragsformulare in lateinischer Schrift und in deutscher Sprache akzeptiert.

Die *Authentisierung* von Personen (als *Zertifikatseigentümer*) für VR-Ident SSL-Zertifikate entfällt, da nur Zertifikate für Organisationen erstellt werden.

Die Überprüfung des Bestätigers des Antrags, des Vertragsunterzeichners und des Antragstellers (je nach Bedarf) erfolgt wie im vorherigen Kapitel beschrieben.

3.2.4. Nicht verifizierte Teilnehmerinformationen

Für die Zertifikatsausstellung und um das Vertrauen in ein ausgestelltes VR-Ident SSL-Zertifikat zu gewährleisten, werden u. a. Identitätsdaten des Zertifikatseigentümers erfasst und geprüft. Bei diesen Prüfungen wird nur die Identität des Zertifikatseigentümers, nicht jedoch die Liquidität und Kreditwürdigkeit festgestellt.

Überprüfungen nach dem Geldwäschegesetz und gegenüber Embargolisten entfallen, da diese bei der Identifikation des Kunden in bank21 über das Programm GenoSonar durchgeführt werden. *Fiducia & GAD IT AG* selbst und *VR-Banken* gelten als bekannt und vertrauenswürdig. Dieses gilt auch für *Fiducia & GAD IT AG* Konzerntöchter und Verbundpartner.

Zum Zeitpunkt der Registrierung werden die für den Dienst erforderlichen Daten überprüft. Eine Aktualität der Daten zu einem späteren Zeitpunkt kann nicht zugesichert werden. Bei Änderungen, die auf die Eigentumsverhältnisse der im ersten Absatz genannten Positionen abzielen, ist der *Zertifikatseigentümer* zu einer Sperrung des Zertifikats verpflichtet.

3.2.5. Überprüfung der Handlungsvollmacht

Eingehende Handlungsvollmachten müssen von zeichnungsberechtigten Personen laut Handelsregister unterzeichnet sein. Zur Unterschriftsprüfung werden qualifizierte unabhängige Quellen verwendet um die Kontaktdaten der unterzeichnenden Personen zu ermitteln. Diese Kontaktdaten werden verwendet, um eine Bestätigung der Vollmachtsunterzeichnung durch eine der unterzeichnenden Personen einzuholen.

3.2.6. Kriterien für Zusammenwirkung

Das *Zertifikat* der "VR IDENT SSL CA 2016" wurde von der "QuoVadis Root CA 2" signiert und das *Zertifikat* der "VR IDENT GENERAL CA 2016" wurde von der "QuoVadis Root CA 3" signiert.

Die Zusammenarbeit ist durch einen entsprechenden Vertrag mit dem Betreiber dieser *Root-CA* (Quo Vadis), geregelt.

3.3. Identifizierung und Authentifizierung bei Schlüsselerneuerung

3.3.1. Identifizierung und Authentifizierung bei turnusmäßiger Schlüsselerneuerung

Bei turnusmäßiger Erneuerung eines VR-Ident SSL-Zertifikats wird davon ausgegangen, dass die Kundenangaben weiterhin gültig sind. Es wird eine regelmäßige Prüfung der Kundenangaben (siehe Kapitel 3.2.2 (S. 12)) durchgeführt.

Bei VR-Ident EV SSL-Zertifikaten wird gewährleistet, dass diese Überprüfung vor jeder Ausstellung eines Zertifikats stattfindet. Die Erneuerung von Zertifikaten wird wie eine Erstausstellung von Zertifikaten behandelt.

3.3.2. Identifizierung und Authentifizierung bei Schlüsselerneuerung nach Sperrung

Bei einer Erneuerung eines VR-Ident SSL-Zertifikats nach einer Sperrung wird genau wie beiner erstmaligen Ausstellung eines Zertifikats vorgegangen. Sofern Kundenangaben weiterhin gültig sind, können diese Angaben erneut verwendet werden. Es wird eine regelmäßige Prüfung der Kundenangaben (siehe Kapitel 3.2.2 (S. 12)) - möglichst vor Erneuerung der VR-Ident SSL-Zertifikate - durchgeführt.

Bei VR-Ident EV SSL-Zertifikaten wird gewährleistet, dass diese Überprüfung vor jeder Ausstellung eines Zertifikats stattfindet. Die Erneuerung von Zertifikaten wird wie eine Erstausstellung von Zertifikaten behandelt.

3.4. Identifizierung und Authentifizierung bei Sperranträgen

VR-Ident SSL-Zertifikate können nur nach erfolgter Identifizierung des Sperrbeantragenden gesperrt werden. Im Sperrantrag (schriftlich, per Email oder per Fax) sind die Referenznummer des Zertifikats und die Unterschrift des Sperrbeantragenden auf dem Sperrantrag erforderlich. Bei Sperranträgen für *Fiducia & GAD IT AG* interne VR-Ident SSL-Zertifikate erfolgt die Identifizierung des Sperrbeantragenden im VR-Ident Workflow Management.

4. Anforderungen an den Lebenszyklus des Zertifikats

4.1. Antragstellung

4.1.1. Wer kann ein Zertifikat beantragen

Folgende Parteien können VR-Ident SSL-Zertifikate beantragen:

- *VR-Banken* und Spezialinstitute der *Fiducia & GAD IT AG*
- die *Fiducia & GAD IT AG*
- *Fiducia & GAD IT AG* Konzerntöchter
- Verbundpartner

4.1.2. Registrierungsprozess und Verantwortlichkeiten

Der Registrierungsprozess wird je nach beantragender Partei wie folgt unterschieden:

Fiducia & GAD IT AG Mitarbeiter, die dazu berechtigt sind, können VR-Ident SSL-Zertifikate für Subdomains von Domains, die von der *Fiducia & GAD IT AG* ausschließlich verwendet werden (beispielsweise www.fiduciagad.de) über den *VR-Ident Workflow Management* beantragen.

VR-Banken können VR-Ident SSL-Zertifikate über das GAD Service-Portal bestellen.

Fiducia & GAD IT AG Konzerntöchter und Verbundpartner: Die Antragstellung erfolgt elektronisch mittels eines Online-Bestellformulars (PDF). Der Auftraggeber oder die für die Antragstellung berechtigte Person füllt das Online-Bestellformular aus und kann es vorab per E-Mail übermitteln. Zusätzlich wird eine Papierversion des Bestellformulars erzeugt, die vom *Antragsteller* unterschrieben werden muss und zusammen mit einem weiteren Dokument, das als Nachweis des Organisationsnamens des Auftraggebers schriftlich oder per Fax (0251 7133 - 91500) an das Auftragsmanagement der *Fiducia & GAD IT AG* gesendet wird.

Als Nachweisdokumente kommen folgende in Frage:

- Aktueller Auszug aus dem Handelsregister,
- Nachweis der Zeichnungsberechtigung des Antragstellers. Sollte der Antragsteller nicht zeichnungsberechtigt sein, kann hier eine andere Person angegeben werden, die den Antrag unterschreibt.

Das Online-Bestellformular kann auf Anfrage den *Fiducia & GAD IT AG* Konzerntöchtern und Verbundpartnern von der Fiducia & GAD Zertifikatsverwaltung zur Verfügung gestellt werden.

VR-Ident EV SSL-Zertifikate müssen auf jeden Fall schriftlich beantragt werden. Der *Zertifizierungsdienst* VR-Ident stellt hierzu geeignete Verfahren zur Verfügung. Die Antragsformulare müssen durch den Bestätiger des Antrags und durch den Vertragsunterzeichner unterschrieben werden. Die Übermittlung des Antrags erfolgt entweder schriftlich oder per Fax (0251 7133 - 91500) an das Auftragsmanagement der *Fiducia & GAD IT AG*. Dieser Prozess muss sowohl für Erstanträge als auch für Erneuerungen eingehalten werden.

Eine natürlichen Person, die berechtigt ist, im Namen einer Organisation VR-Ident SSL-Zertifikate zu beantragen, hat durch ein schriftliches Bestellformular die Möglichkeit, einen oder mehrere Antragsteller (siehe Kapitel 1.3.3 (S. 5)) dazu zu bevollmächtigen, im Namen der Organisation VR-Ident SSL-Zertifikate für Domains zu beantragen, die auf diese Organisation registriert sind. Das Bestellformular muss von einem Zeichnungsberechtigten der Organisation unterschrieben und mit dem Stempel der Organisation versehen sein.

4.2. Antragsbearbeitung

4.2.1. Durchführung der Identifikation und Authentifizierung

Zertifizierungsdienst VR-Ident führt die Identifizierung und Authentifizierung wie in Kapitel 3.2.2 (S. 12) beschrieben durch. Der Registrierungsdatensatz wird im Vier-Augen-Prinzip geprüft. Erst nach erfolgreichem Prüfungsablauf wird der Registrierungsdatensatz weitergegeben und der Zertifizierungsauftrag erteilt.

4.2.2. Annahme beziehungsweise Ablehnung von Zertifikatsanträgen

Voraussetzung für die Annahme des Zertifikatsantrags ist, dass die Identifizierung und *Authentifizierung* aller erforderlichen Informationen zum *Antragsteller* oder zum Auftraggeber gemäß Kapitel 3.2.2 (S. 12) und Kapitel 3.2.3 (S. 14) erfolgreich war.

Ein Anspruch auf Annahme eines Antrags besteht nicht. In folgenden Fällen wird der Zertifikatsantrag abgelehnt:

- Der Auftraggeber beziehungsweise der *Antragsteller* kann nicht zweifelsfrei identifiziert werden.
- Der Auftraggeber hat gegen Geldwäschegesetz verstoßen oder steht auf Embargolisten.
- Der *Zertifizierungsdienst* VR-Ident hat weitere Ablehnungsgründe.
- Erforderliche Unterlagen, wie beispielsweise der Registerauszug fehlen.
- Es bestehen Zweifel an der Echtheit der eingereichten Unterlagen.
- Der Auftraggeber versäumt, auf Benachrichtigungen der *Fiducia & GAD IT AG* zu reagieren.

4.2.3. Bearbeitungsdauer von Zertifikatsanträgen

Die Bearbeitung des Zertifikatsauftrags beginnt in einem angemessenen Zeitrahmen nach Erhalt der Beauftragung zu den normalen Geschäftszeiten der *Fiducia & GAD IT AG*. Es gibt keine Maßgaben, wann ein Zertifikat erstellt sein muss, außer das ist in individuellen Sonderbedingungen explizit festgelegt.

VR-Ident SSL-Zertifikate werden unmittelbar nach Beendigung des Registrierungsprozesses erstellt.

4.2.4. Certification Authority Authorization (CAA)

Seit Anfang 2013 gibt es den RFC 6844 „Certification Authority Authorization“ (CAA). CAA spezifiziert einen gleichnamigen Resource Record zur Ablage im DNS, mit dem ein Domain-Inhaber festlegen kann, welche Zertifizierungsstelle (CA) für seine Domain Zertifikate ausgeben darf.

Der *Zertifizierungsdienst* VR-Ident unterstützt diesen Mechanismus seit September 2017.

Bevor VR-Ident SSL-Zertifikate ausgestellt werden, werden die CAA Records für jeden DNS Namen im CommonName und in der SubjectAltNames Erweiterung überprüft. Die Ausstellung der Zertifikate erfolgt maximal 8 Stunden nach Überprüfung der CAA Records.

Die Property Tags "issue", "issuewild" und "iodef" werden gemäß RFC 6844 behandelt.

Ausgenommen hiervon sind Domains, für welche die Fiducia & GAD IT AG als Betreiber der entsprechenden DNS Server gemäß RFC 7719 gilt.

Die CAA Domain für den *Zertifizierungsdienst* VR-Ident lautet "vr-ident.de".

4.3. Zertifikatserstellung

4.3.1. CA Prozesse während der Zertifikatserstellung

Nach erfolgreicher Prüfung des Antrags durch die *RA* (*Registration Authority*) wird anhand der im Registrierungsdatensatz enthaltenen Daten das entsprechende *Zertifikat* erzeugt.

4.3.2. Benachrichtigung des Antragstellers über die Zertifikatserstellung

Das VR-Ident SSL-Zertifikat wird nach erfolgreicher Erstellung inklusive der kompletten Zertifikatskette automatisiert an den *Antragsteller* per E-Mail versendet. Hierbei ist zu beachten, dass die Dateierweiterung "cer" verwendet wird, die von einigen Firewalls oder E-Mail Programmen abgewiesen werden kann.

Im Zertifikatsantrag können optional zusätzlich E-Mail Adressen angegeben werden, die automatisch benachrichtigt werden.

4.4. Zertifikatsakzeptanz

4.4.1. Annahme durch den Zertifikatsinhaber

Das ausgestellte VR-Ident SSL-Zertifikat wird zusammen mit der gesamten Zertifikatskette per E-Mail verschickt. Die komplette CA-Kette ist in Kapitel 3.1.1 (S. 10) dargestellt.

Der Zertifikatsinhaber ist dazu verpflichtet, den Inhalt des Zertifikats zu überprüfen. Mit dem Erhalt des VR-Ident SSL-Zertifikats akzeptiert der Inhaber das Zertifikat, es sei denn, er bemängelt das Zertifikat innerhalb einer gegebenen Frist.

4.4.2. Veröffentlichung der Zertifikate durch den Zertifizierungsdienst

Der *Zertifizierungsdienst* VR-Ident veröffentlicht die ausgestellten VR-Ident Zertifikate in dem VR-Ident *Verzeichnisdienst*.

4.4.3. Benachrichtigung weiterer Instanzen durch den Zertifizierungsdienst

Weitere Instanzen werden nicht benachrichtigt. Die Zertifikate sind in dem in Kapitel 2.1 (S. 8) genannten VR-Ident *Verzeichnisdienst* verfügbar.

4.5. Nutzung des Schlüsselpaares und des Zertifikats

Die Nutzung des Schlüsselpaares und des VR-Ident Zertifikats durch den Eigentümer und durch vertrauende Dritte darf nur gemäß den nachfolgenden Bedingungen erfolgen.

4.5.1. Nutzung durch den Eigentümer

Die Nutzung eines privaten Schlüssels durch den Eigentümer ist erst möglich, nachdem das zugehörige VR-Ident Zertifikat erfolgreich in seinem System integriert wurde.

Die Nutzung eines privaten Schlüssels und des zugehörigen VR-Ident Zertifikats ist nur zu den in Kapitel 1.4.1 (S. 5) beschrieben Zwecken zulässig. Das VR-Ident Zertifikat darf nur gemäß dem vorliegenden *CPS* (*Certification Practice Statement*) verwendet werden. In den in Kapitel 1.4.2 (S. 5) beschriebenen Fällen ist die Verwendung des Zertifikats unzulässig.

4.5.2. Nutzung durch vertrauende Dritte

Die Nutzung der VR-Ident Zertifikate durch *Vertrauende Dritte* muss diesem Richtliniendokument folgen. Vor dem Vertrauen auf ein VR-Ident *Zertifikat* hat der *Vertrauende Dritte* folgendes unabhängig zu prüfen:

- dass die Nutzung des Zertifikats für einen bestimmten Zweck durch das vorliegende Dokument nicht verboten oder anderweitig beschränkt ist,
- dass die Nutzung des Zertifikats den im *Zertifikat* enthaltenen KeyUsage-Felderweiterungen entspricht,
- dass das *Zertifikat* zum gegebenen Zeitpunkt nicht gesperrt oder dessen Gültigkeit abgelaufen ist,
- dass die Signatur des Zertifikats auf Basis eines zum Prüfzeitpunkt gültigen CA-Zertifikats des *Zertifizierungsdienst*eanbieters *Fiducia & GAD IT AG* geprüft werden kann.

Die Prüfung der Sperrinformation kann wahlweise auf Basis einer gültigen Sperrliste oder einer aktuellen Abfrage beim Auskunftsdienst des *Zertifizierungsdienst* VR-Ident erfolgen. Außerdem sollten vertrauende Dritte Zertifikate nur in dafür zugelassenen Anwendungen akzeptieren.

Die zulässige Anwendung von Schlüsselpaaren ist in Kapitel 1.4.1 (S. 5) beschrieben.

Das VR-Ident CA-Zertifikat ist in analoger Weise auf Basis des gültigen Root-CA-Zertifkats zu prüfen.

4.6. Zertifikatserneuerung unter Beibehaltung des alten Schlüssels

Bei der Zertifikatserneuerung unter Beibehaltung des alten Schlüssels handelt es sich um die Ersetzung eines Zertifikates durch ein *Zertifikat* mit neuer Gültigkeitsdauer, aber für den gleichen *öffentlichen Schlüssel* und sonst unveränderten Inhaltsdaten. In *RFC* 3647 wird dieser Vorgang "*Certificate Renewal*" genannt.

Eine Zertifikatserneuerung unter Beibehaltung des alten Schlüssels von VR-Ident Zertifikaten wird nicht unterstützt.

4.7. Schlüssel- und Zertifikatserneuerung

Bei der *Schlüssel- und Zertifikatserneuerung* handelt es sich um die Ersetzung eines Zertifikates durch ein *Zertifikat* mit neuer Gültigkeitsdauer und für einen neuen *öffentlichen Schlüssel* aber sonst unveränderten Inhaltsdaten. In *RFC* 3647 wird dieser Vorgang "Certificate Re-key" genannt.

4.7.1. Gründe für eine Schlüssel- und Zertifikatserneuerung

Vor Ablauf eines VR-Ident Zertifikats muss der Zertifikatseigentümer den Schlüssel und das VR-Ident Zertifikat erneuern, um es ohne Unterbrechung weiterhin verwenden zu können. Der Schlüssel eines Zertifikats kann auch nach seinem Ablauf erneuert werden. Eine Erneuerung des VR-Ident Zertifikats kann auch nach einer Sperrung des alten Zertifikats erforderlich sein.

Da ein ausgegebenes VR-Ident Zertifikat nachträglich nicht mehr verändert werden kann (siehe Kapitel 4.8 (S. 20)), muss die Verlängerung der Gültigkeit durch eine erneute Ausstellung (Erneuerung) mit neuem Gültigkeitszeitraum durchgeführt werden.

VR-Ident SSL-Zertifikate haben bis zum Februar 2018 eine Gültigkeit von 13 Monaten oder von 37 Monaten und danach, also ab März 2018, eine Gültigkeit von 27 Monaten.

Um eine lückenlose Funktion des VR-Ident SSL-Zertifikates zu gewährleisten, muss die Erneuerung vor Ablauf der Gültigkeit durchgeführt werden. Die bevorstehende Möglichkeit der Erneuerung wird erstmals ca. 60 Tage vor Ablauf des Zertifikates dem Verantwortlichen für das *Zertifikat* und der Fiducia & GAD Zertifikatsverwaltung per E-Mail mitgeteilt.

4.7.2. Wer kann eine Schlüssel- und Zertifikatserneuerung beantragen

Siehe Kapitel 4.1.1.

4.7.3. Ablauf der Schlüssel- und Zertifikatserneuerung

Die Prozesse der Antragsbearbeitung und Zertifikatserstellung sind analog zu den in Kapitel 4.2 und in Kapitel 4.3 beschriebenen Prozessen bei einem Erstantrag.

Die Kundenangaben werden regelmäßig überprüft. Sowohl die turnusmäßige Erneuerung des VR-Ident SSL-Zertifikats als auch die Erneuerung eines VR-Ident SSL-Zertifikats nach Sperrung werden somit mit aktuellen Kundendaten durchgeführt.

Bei VR-Ident EV SSL-Zertifikaten wird gewährleistet, dass diese Überprüfung vor jeder Ausstellung eines Zertifikats stattfindet. Die Erneuerung von Zertifikaten wird wie eine Erstausstellung von Zertifikaten behandelt.

4.7.4. Benachrichtigung des Zertifikatsinhabers nach Schlüssel- und Zertifikatserneuerung

Der Prozess der Benachrichtigung des Zertifikatsinhabers ist analog zum in Kapitel 4.3.2 beschriebenen Prozess bei Erstantrag.

4.7.5. Annahme der Schlüssel- und Zertifikatserneuerung

Der Prozess der Annahme ist analog zum in Kapitel 4.4.1 beschriebenen Prozess bei Erstantrag.

4.7.6. Veröffentlichung einer Zertifikatserneuerung durch den Zertifizierungsdienst

Siehe Kapitel 4.4.2 (S. 18).

4.7.7. Benachrichtigung weiterer Instanzen durch den Zertifizierungsdienst

Siehe Kapitel 4.4.3 (S. 18).

4.8. Zertifikatsmodifizierung

Bei der *Modifizierung eines Zertifikats* handelt es sich um die Ersetzung eines Zertifikates durch ein *Zertifikat* mit veränderten Inhaltsdaten und für den gleichen oder einen neuen *öffentlichen Schlüssel* und sonst unveränderter Gültigkeitsdauer. In *RFC* 3647 wird dieser Vorgang "Certificate Modification" genannt.

Eine Modifizierung von VR-Ident Zertifikaten wird nicht unterstützt. Die Modifizierung von VR-Ident Zertifikaten wird wie eine neue Antragsstellung behandelt.

4.9. Sperrung und Suspendierung von Zertifikaten

4.9.1. Gründe für die Sperrung

Der *Zertifizierungsdienst* VR-Ident behält sich das Recht vor, ein *Zertifikat* (CA-Zertifikat oder VR-Ident Zertifikat) unverzüglich in folgenden Fällen zu sperren:

- Der *Zertifizierungsdienst* VR-Ident hat den begründeten Verdacht eines Missbrauchs des VR-Ident Zertifikats.
- Die in einem *Zertifikat* enthaltenen Angaben entsprechen nicht oder nicht mehr den Tatsachen, insbesondere wenn eine Weiterverwendung gegen gesetzliche Bestimmungen verstoßen würde.
- Es besteht der begründete Verdacht oder die Gewissheit, dass der zum *Zertifikat* korrespondierende private Schlüssel kompromittiert oder nicht mehr ausreichend geschützt ist.
- Die verwendeten kryptographische Algorithmen oder zugehörige Parameter, mit denen die Zertifikate ausgestellt oder mit der die Schlüssel verwendet werden, können aufgrund technologischer Fortschritte oder neuen Entwicklungen in der Kryptologie nicht mehr die notwendige Sicherheit gewährleisten.
- Der *Zertifizierungsdienst* VR-Ident stellt fest, dass das Zertifikat nicht gemäß diesen Richtlinien erstellt wurde.
- Der *Zertifizierungsdienst* VR-Ident stellt den *Zertifizierungsdienst* ein (siehe Kapitel 5.8 (S. 33)).
- Der *Zertifikatseigentümer* versäumt es, seinen vertraglichen Verpflichtungen bezüglich des *Zertifizierungsdienst* VR-Ident nachzukommen, beispielsweise bei Zahlungsverzug des Zertifikatseigentümers in nicht unerheblicher Höhe.
- Der Kunde verlangt per Fax oder E-Mail, dass das Zertifikat gesperrt werden soll.
- Ein sonstiger Grund zur Sperrung besteht.

Weiterhin behält sich der *Zertifizierungsdienst* VR-Ident das Recht vor, ein VR-Ident Zertifikat auch in einem der folgenden Fälle zu sperren:

- Das Vertragsverhältnis endet.

In allen diesen Fällen benachrichtigt *Zertifizierungsdienst* VR-Ident die Auftraggeber beziehungsweise die Zertifikatseigentümer über die durchgeführte Sperrung des VR-Ident Zertifikates durch eine E-Mail.

Der Zertifikatsinhaber muss in folgenden Fällen eine Sperrung seines VR-Ident SSL-Zertifikates veranlassen:

- Der Zertifikatsinhaber stellt fest oder hat Grund zu der Annahme, dass unberechtigte Personen Zugriff auf den *privaten Schlüssel* hatten oder ihn manipulieren konnten,
- Der Zertifikatsinhaber erklärt, dass das Zertifikat nicht ordnungsgemäß autorisiert wurde und dass keine nachträgliche Autorisierung gewünscht wird.
- Die Informationen im *Zertifikat* sind nicht korrekt oder haben sich geändert oder der Name der Organisation und/oder Ihre Domainregistrierung hat sich geändert.
- Dem Zertifikatsinhaber wurde das Nutzungsrecht des Domainnamens entzogen oder das Nutzungsrecht wurde durch den Eigentümer des Zertifikats nicht verlängert.

4.9.2. Sperrberechtigte

Die folgenden Parteien sind berechtigt, die Sperrung von VR-Ident Zertifikaten zu beantragen oder auch durchzuführen:

- Der *Zertifikatseigentümer* oder ein durch ihn bevollmächtigter Dritter kann die Sperrung eigener VR-Ident Zertifikate beantragen.
- Der *Zertifizierungsdienst* VR-Ident kann die Sperrung von ausgestellten VR-Ident Zertifikaten und der VR-Ident CA-Zertifikate veranlassen und durchführen.
- Der *Zertifizierungsdienst* VR-Ident kann die Sperrung des Zertifikats der "VR IDENT SSL CA 2016" bei Quo Vadis beantragen.
- Der *Zertifizierungsdienst* VR-Ident kann die Sperrung des Zertifikats der "VR IDENT GENERAL CA 2016" bei Quo Vadis beantragen.

4.9.3. Verfahren zur Sperrung

Der *Zertifizierungsdienst* VR-Ident sperrt VR-Ident SSL-Zertifikate auf Wunsch des Kunden nach erfolgter Identifizierung. Es sind folgende Verfahren für die Sperrung definiert:

- Schriftlich: In diesem Fall sind die Referenznummer des Zertifikats und die Unterschrift des Sperrbeantragenden auf dem Sperrantrag erforderlich,
- Per Fax: In diesem Fall sind die Referenznummer des Zertifikats und die Unterschrift des Sperrbeantragenden auf dem Sperrantrag erforderlich.

Der Verantwortliche für das *Zertifikat* und die Fiducia & GAD Zertifikatsverwaltung werden per E-Mail über die erfolgte Sperrung informiert.

Sollte der *Zertifizierungsdienst* VR-Ident Gründe haben, VR-Ident SSL-Zertifikate zu sperren, erteilt der Leiter des *Zertifizierungsdienst* VR-Ident einen entsprechenden Sperrauftrag an einen *Sperrmitarbeiter*.

Die Sperrung des Zertifikats der "VR IDENT SSL CA 2016" auf Wunsch des *Zertifizierungsdienst* VR-Ident wird von dessen Leitung gemäß der Zertifizierungsrichtlinien der "QuoVadis Root CA 2" (siehe Anhang mit allgemeinen Referenzen) bei Quo Vadis beantragt.

Die Sperrung des Zertifikats der "VR IDENT GENERAL CA 2016 auf Wunsch des *Zertifizierungsdienst* VR-Ident wird von dessen Leitung gemäß der Zertifizierungsrichtlinien der "QuoVadis Root CA 3" (siehe Anhang mit allgemeinen Referenzen) bei Quo Vadis beantragt.

Die Sperrung des Zertifikats der "VR IDENT SSL CA 2016" durch Quo Vadis erfolgt gemäß der Zertifizierungsrichtlinien der "QuoVadis Root CA 2" (siehe Anhang mit allgemeinen Referenzen).

Die Sperrung des Zertifikats der "VR IDENT GENERAL CA 2016" durch Quo Vadis erfolgt gemäß der Zertifizierungsrichtlinien der "QuoVadis Root CA 3" (siehe Anhang mit allgemeinen Referenzen).

4.9.4. Fristen für die Beantragung einer Sperrung

Bei einer bekannten, vermuteten oder drohenden Kompromittierung der *privaten Schlüssel* ist die Sperrung der entsprechenden VR-Ident Zertifikate unverzüglich zu beantragen.

4.9.5. Bearbeitungszeit für Anträge auf Sperrung

Die Untersuchung von eingehenden Certificate Problem Reports durch den Zertifizierungsdienst VR-Ident beginnt innerhalb von 24 Stunden nach Eingang des Reports. Der Zertifizierungsdienst VR-Ident entscheidet dann, ob eine Sperrung des Zertifikates oder eine andere angemessene Reaktion erforderlich ist.

Die Sperrung von VR-Ident SSL-Zertifikaten erfolgt in der Regel ein bis zwei Werktage nach Eingang des Sperrantrags. In dringenden Fällen wie beispielsweise bei einer Schlüsselkompromittierung wird unverzüglich gesperrt.

Der Sperrantrag von VR-Ident SSL-Zertifikaten kann 24x7 schriftlich, per E-Mail (IND_Zertifikatssperre@fiduciagad.de) oder per Fax (0251 7133 - 91500) eingereicht werden. Spätestens vier Werktage nach Eingang des Sperrantrags wird die Sperrung durchgeführt und ist spätestens nach einem weiteren Tag im *OCSP-Responder* eingetragen. Die Häufigkeit und Zyklen für die Veröffentlichung und Erstellung von *CRL* (Sperrlisten) ist in Kapitel 2.3 (S. 8) beschrieben.

4.9.6. Prüfung des Zertifikatsstatus durch vertrauende Dritte

Vertrauende Dritte sollten sich auf den Inhalt eines VR-Ident Zertifikats des *Zertifizierungsdienst* VR-Ident nur dann verlassen, wenn sie zuvor den Zertifikatsstatus geprüft haben. Vertrauende Dritte können dem VR-Ident *Zertifikat* vertrauen, wenn dieses nicht abgelaufen oder gesperrt ist und seine Signatur auf Basis eines zum Prüfzeitpunkt gültigen CA-Zertifikats des *Zertifizierungsdienst*eanbieters *Fiducia & GAD IT AG* geprüft werden kann. Die Prüfung der Sperrinformation kann wahlweise auf Basis einer gültigen *CRL* (*Sperrliste*) über das LDAP-Verzeichnis oder einer aktuellen Abfrage beim *OCSP-Responder* des *Zertifizierungsdienst* VR-Ident erfolgen.

4.9.7. Periode für Erstellung von Sperrlisten

Die Häufigkeit und Zyklen für die Veröffentlichung und Erstellung von *CRL* (Sperrlisten) ist in Kapitel 2.3 (S. 8) beschrieben.

4.9.8. Maximale Latenzzeit für Sperrlisten

CRL (Sperrlisten) werden unmittelbar nach der Erstellung in die Datenbank gestellt und sind aus dem VR-Ident *Verzeichnisdienst* abrufbar.

4.9.9. Verfügbarkeit von Online-Sperrinformationen

Sperrinformationen werden online bereitgestellt. Es sind alle vom *Zertifizierungsdienst* VR-Ident gesperrten Zertifikate enthalten. Sowohl der *OCSP-Responder* als auch der VR-Ident *Verzeichnisdienst* sind hochverfügbar (24x7).

4.9.10. Anforderungen an Online-Sperrinformationen

Es bestehen keine besonderen Anforderungen. Die Online-Sperrinformationen sind über die Standardprotokolle *OCSP* und *LDAP* abrufbar.

4.9.11. Andere verfügbare Formen der Bekanntmachung von Sperrinformationen

Es gibt keine anderen Formen der Bekanntmachung von Sperrinformationen.

4.9.12. Spezielle Anforderungen bei Kompromittierung privater Schlüssel

Es gibt keine speziellen Anforderungen bei der Kompromittierung privater Schlüssel. Bei der Kompromittierung eines privaten Schlüssels ist generell das entsprechende *Zertifikat* unverzüglich zu sperren und die Nutzung der privaten und öffentlichen Schlüssels zu beenden.

4.9.13. Suspendierung

Eine Suspendierung (vorläufige Sperrung) von VR-Ident Zertifikaten wird nicht unterstützt, die Sperrung eines VR-Ident Zertifikates ist immer endgültig und kann nicht aufgehoben werden.

4.10. Auskunftsdienst über den Zertifikatsstatus

Der Auskunftsdienst für den Zertifikatsstatus basiert auf dem "Online Certificate Status Protocol" (*OCSP*) Version 1 nach *RFC* 2560 und stellt die Status der VR-Ident Zertifikate sowie der Zertifikate der VR-Ident Zertifizierungsinstanzen (siehe Kapitel 1.3.1 (S. 3) und Kapitel 2.1 (S. 8)) online zur Verfügung.

4.10.1. Betriebseigenschaften der Auskunftsdienste

Der *OCSP-Responder* ist über die in Kapitel 2.1 (S. 8) angegebene URL erreichbar. Der *OCSP-Responder* verwendet als Übertragungsprotokoll *HTTP* und implementiert das "Online Certificate Status Protocol" (*OCSP*) mit den folgenden Eigenschaften:

- Die Anfragen (OCSP-Requests) müssen nicht signiert sein; signierte Anfragen werden jedoch auch unterstützt.
- Die Auskünfte des *OCSP-Responder* sind Positivauskünfte, sofern die Antwort auf eine Anfrage den Status "good" liefert, bedeutet dies auch, dass das *Zertifikat* im VR-Ident *Verzeichnisdienst* vorhanden ist und dass dieses gültig ist.
- Die *OCSP-Responder* verwenden für ihre Auskünfte eine ständig aktualisierte Datenbasis. Das Feld "NextUpdate" enthält den Zeitpunkt, an dem spätestens aktuellere Informationen zum Status der Zertifikate über den *OCSP-Responder* verfügbar sind. Die Antworten (OCSP-Response) sollten daher nicht länger als zu dem Zeitpunkt in dem Feld "NextUpdate" zwischengespeichert und wiederverwendet werden.
- Auskünfte über den Status von Zertifikaten sind mehr als 7 Jahre über den Ablauf der Gültigkeit der Zertifikate hinaus verfügbar.
- Die unterstützten und die verwendeten Erweiterungen (OCSP-Extensions) sind im Kapitel 7.3 (S. 45) angegeben.

Jede *CA* stellt zu den von ihr ausgestellten Zertifikaten eine *CRL* (*Sperrliste*) mit folgenden Eigenschaften aus:

- Die *CRL* (*Sperrliste*) entspricht den Standards *X.509*, sowie *RFC* 5280 und Common *PKI* (siehe Anhang mit allgemeinen Referenzen).
- Die *CRL* (*Sperrliste*) wird durch die *CA* selbst signiert, es handelt sich um eine sogenannte direkte *CRL* (*Sperrliste*).
- Die *CRL* (Sperrlisten) sind im VR-Ident *Verzeichnisdienst* (siehe Kapitel 2.1 (S. 8)) in dem Attribut des jeweiligen CA-Objektes gespeichert.
- Die *CRL* (Sperrlisten) sind gültig bis zur Ausstellung der nächsten *CRL* (*Sperrliste*) bzw. bis zu dem im next-Update-Feld genannten Zeitpunkt. Die Frequenz für die Ausstellung der Sperrlisten ist in Kapitel 2.3 (S. 8) festgelegt.
- Die *CRL* (Sperrlisten) enthalten die Seriennummern aller gesperrten Zertifikate, auch jene, die auf Wunsch des Zertifikatseigentümers nicht veröffentlicht wurden.

- Gesperrte Zertifikate verbleiben auf der CRL für mehr als 7 Jahre über den Ablauf der Gültigkeit der Zertifikate hinaus.
- Die verwendeten CRL-Erweiterungen sind in Kapitel 7.2 (S. 44) angegeben.

Für die *Zertifizierungsstelle* VR-Ident gelten folgende spezielle Festlegungen bezüglich der *OCSP-Responder* für VR-Ident SSL-Zertifikate:

- Für die "VR IDENT SSL CA 2016" wird ein *OCSP-Responder* eingesetzt, der unter der entsprechenden URL erreicht werden kann.
- Der *OCSP-Responder* der "VR IDENT SSL CA 2016" stellt Sperrinformationen zu VR-Ident SSL-Zertifikaten zur Verfügung.

4.10.2. Verfügbarkeit des Auskunftsdienstes

Die *OCSP-Responder* des *Zertifizierungsdienst* VR-Ident sind hochverfügbar ausgelegt. Unter normalen Betriebsbedingungen beträgt die Antwortzeit der OCSP-Responder weniger als 10 Sekunden.

Der Zertifizierungsdienst VR-Ident nimmt Problemberichte über Zertifikate jederzeit (24x7) entgegen. Wenn es erforderlich ist, wird ein solcher Bericht an die zuständige staatliche Behörde weitergeleitet, und/oder das betroffene Zertifikat wird gesperrt.

4.10.3. Optionale Funktionen

Eine Anfrage an den *OCSP-Responder* für den Zertifikatsstatus kann die Erweiterung "Nonce" enthalten. Diese Extension dient der Vorbeugung gegen Angriffe durch Senden alter Antworten (Replay-Attacks). Der in der Anfrage übergebene Wert wird vom Auskunftsdienst in die Extension "Nonce" der Antwort kodiert.

Die Antworten des *OCSP-Responder* enthalten den *Hashwert* des angefragten Zertifikates.

Außerdem kann das *Zertifikat* – sofern der *Zertifikatseigentümer* der Veröffentlichung zugestimmt hat – durch Verwendung der Extension "RetrieveIfAllowed" in der Anfrage mit der Antwort abgerufen werden.

4.11. Austritt aus dem Zertifizierungsdienst

Ein *Zertifikatseigentümer* oder ein Kunde tritt aus dem *Zertifizierungsdienst* VR-Ident aus, wenn er über keine gültigen Zertifikate mehr verfügt und nicht unmittelbar Folgezertifikate erstellt werden. Dies ist der Fall, wenn

- die VR-Ident Zertifikate ablaufen und keine neuen Zertifikate ausgestellt werden,
- er die Sperrung aller Zertifikate beantragt,
- er das Vertragsverhältnis mit dem *Zertifizierungsdienst*eanbieter *Fiducia & GAD IT AG* oder seiner VR-Bank kündigt, oder
- der *Zertifizierungsdienst* VR-Ident die Sperrung aller seiner Zertifikate veranlasst, und dies nicht im Zuge der Ersetzung der Zertifikate erfolgt.

4.12. Schlüsselhinterlegung und -wiederherstellung

4.12.1. Richtlinien und Praktiken zur Schlüsselhinterlegung und -wiederherstellung

Der *Zertifizierungsdienst* VR-Ident bietet weder eine Schlüsselhinterlegung an noch führt die *Zertifizierungsstelle* VR-Ident diese durch.

4.12.2. Richtlinien und Praktiken zum Schutz und Wiederherstellung von Sitzungsschlüsseln

Der *Zertifizierungsdienst* VR-Ident bietet weder eine Schlüsselhinterlegung an noch führt die *Zertifizierungsstelle* VR-Ident diese durch.

5. Physikalische, organisatorische und personelle Sicherheitsmaßnahmen

5.1. Physikalische Sicherheitsmaßnahmen

5.1.1. Lage und Aufbau des Standortes

Die Zertifizierungstätigkeiten des *Zertifizierungsdienst* VR-Ident der *Fiducia & GAD IT AG* werden in einem baulich geschützten Bereich des Rechenzentrums der *Fiducia & GAD IT AG* betrieben. Die bauliche Infrastruktur unterliegt hohen Sicherheitsstandards bezüglich physikalischer Sicherheit. Sie ist derart gestaltet, dass ein hoher Schutz gegen Einbruch gewährleistet ist. Weiterhin wurden Vorkehrungen zum Schutz gegen Brand, Wasser und Blitzeinschlag getroffen. Die entsprechenden IT-Systeme des *Zertifizierungsdienst* VR-Ident befinden sich innerhalb des gesicherten Bereichs. Zur Aufrechterhaltung des Zertifizierungsbetriebs im Notfall werden die IT-Systeme redundant ausgelegt und betrieben. Die Unterbringung der redundanten Systeme erfolgt in örtlich getrennten Räumen in einem Backup-Rechenzentrum.

5.1.2. Zutrittskontrolle

Geeignete Maßnahmen zur Zutrittskontrolle gewährleisten einen hohen Schutz gegen unbefugtes Eindringen in die einzelnen Räume und unbefugten Zugriff auf die sicherheitskritischen Systeme und Daten. Der Zutritt zu den Räumen mit den IT-Systemen des *Zertifizierungsdienst* VR-Ident ist durch Zutrittskarten gesichert. Weite Teile des Rechenzentrums und der Gebäude, insbesondere Eingangsbereiche, Flure und Rechnerräume werden rund um die Uhr videoüberwacht.

5.1.3. Stromversorgung und Klimakontrolle

Das Rechenzentrum der *Fiducia & GAD IT AG*, in dem der *Zertifizierungsdienst* VR-Ident betrieben wird, ist mit durchgehender, unterbrechungsfreier Stromversorgung ausgestattet.

Leistungsfähige Klimaanlagen gewährleisten die Klimatisierung der IT-Räume und der IT-Systeme für den *Zertifizierungsdienst* VR-Ident. Die Funktionalität der Klimaanlage wird permanent überwacht.

5.1.4. Schutz vor Wasserschäden

Das Rechenzentrum der *Fiducia & GAD IT AG* und insbesondere die Technikräume sind durch bauliche Maßnahmen vor Wassereinbrüchen gesichert.

5.1.5. Brandschutz

Für das Rechenzentrum der *Fiducia & GAD IT AG* sind geeignete Sicherheitsmaßnahmen getroffen, um Brände oder andere Schäden durch Brand zu verhüten. Die Brandschutzmaßnahmen wurden unter Einhaltung der Brandschutzbestimmungen gestaltet.

5.1.6. Aufbewahrung von Datenträgern

Datenträger mit sicherheitskritischen Informationen (beispielsweise mit Backups) werden ausschließlich in gegen unbefugten Zutritt sowie Wasser und Brand geschützten Räumlichkeiten aufbewahrt. Datenträger mit besonders kritischen Informationen werden ausschließlich im Tresor aufbewahrt.

5.1.7. Entsorgung von Datenträgern

Nicht mehr benötigte Datenträger, die zur Erfassung oder Übertragung von schutzbedürftigen Informationen verwendet wurden, werden sorgfältig entsorgt. Sie werden beispielsweise durch Zerschneiden des Chips oder durch Schreddern des Datenträgers physikalisch unbrauchbar gemacht. Papierdokumente, die schutzbedürftige Informationen enthalten, werden vor ihrer Entsorgung geschreddert.

5.1.8. Datensicherung

Für den *Zertifizierungsdienst* VR-Ident wird regelmäßig eine Datensicherung durchgeführt. Die Datensicherung umfasst die Daten der Zertifizierungsprozesse, die Protokolldaten und weitere wichtige Daten. Die Backup-Datenträger werden sicher aufbewahrt (siehe Kapitel 5.1.6 (S. 26)).

5.2. Organisatorische Sicherheitsmaßnahmen

5.2.1. Sicherheitskritische Rollen

Zertifizierungstätigkeiten dürfen ausschließlich durch autorisierte *Rollenträger* durchgeführt werden. Das sind Mitarbeiter, denen durch das Management des Zertifizierungsdienstes VR-Ident die entsprechenden Rollen zugewiesen sind. Sicherheitskritische Rollen sind insbesondere:

- Mitarbeiter der Systemadministration,
- PKI-Operatoren,
- Sicherheitspersonal,
- zuständiges technisches Personal,
- Auditoren oder Revisoren und
- Rollen der Managementebene.

Alle diese Rollen sind durch vertrauenswürdige und qualifizierte Mitarbeiter besetzt.

Die Rollen und deren Aufgaben werden im Rollenkonzept der Sicherheitsleitlinie der *Fiducia & GAD IT AG* explizit beschrieben.

5.2.2. Anzahl benötigter Personen bei sicherheitskritischen Tätigkeiten

Sicherheitskritische Tätigkeiten mit hohem Schutzbedarf bezüglich der Vertraulichkeit, wie beispielsweise der Zugang zu den Hardware-Sicherheitsmodulen (*HSM*) und den zugehörigem Schlüsselmaterial sowie dessen Management, erfordern den Einsatz mehrerer vertrauenswürdiger *Rollenträger*. Vorhandene Richtlinien- und Kontrollverfahren sorgen dafür, dass für den räumlichen oder logischen Zugang zum Gerät mindestens zwei vertrauenswürdige Mitarbeiter erforderlich sind. Der Zugriff auf die sicherheitskritischen Systeme des *Zertifizierungsdienst* VR-Ident und deren Backup-Daten wird ebenfalls im Vier-Augen-Prinzip durchgeführt. Die folgenden Tätigkeiten werden ausschließlich im Vier-Augen-Prinzip durchgeführt:

- Administrativer oder operativer Zugriff auf *Hardware-Sicherheitsmodul*e (*HSM*),
- Initialer Austausch von Systemschlüsseln,
- Prozeduren der Key Ceremony,
- Konfiguration der CA-Systeme,
- administrativer Zugriff auf Benutzerrechte.

5.2.3. Identifizierung und Authentisierung von Rollen

Die Identifizierung und *Authentisierung* der Rollen beim Zutritt zu den Sicherheitsräumen im Rechenzentrum und beim Zugriff auf die IT-Systeme erfolgt mit Hilfe von Zutrittskarten sowie Benutzername und Passwort. Die Anmeldung der *PKI* Operatoren an den VR-Ident *PKI* Systemen erfolgt basierend auf individuellen *Authentisierungszertifikat*en.

5.2.4. Trennung von Rollen und Aufgaben

Das Rollenkonzept regelt auch, welche Rollen eine Funktionstrennung erfordern. Dabei liegen die folgenden Regeln zugrunde:

- Das Management der *Fiducia & GAD IT AG* darf keine operativen oder administrativen Tätigkeiten ausüben.
- Auditoren und Revisoren dürfen keine operativen oder administrativen Tätigkeiten ausüben.
- System-Administratoren dürfen keine operativen Aufgaben ausüben.
- *Rollenträger*, die für die Zutrittsrechte zu den Räumlichkeiten des *Zertifizierungsdienst* VR-Ident zuständig sind, dürfen keine sonstigen operativen oder administrativen Aufgaben ausüben.

5.3. Personelle Sicherheitsmaßnahmen

5.3.1. Anforderungen an Qualifikation und Erfahrung

Im *Zertifizierungsdienst* VR-Ident wird nur zuverlässiges Personal mit den erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen beschäftigt.

5.3.2. Überprüfung der Vertrauenswürdigkeit

Für alle Mitarbeiter, die bei dem *Zertifizierungsdienst* VR-Ident beschäftigt sind, werden Zuverlässigkeitsprüfungen durchgeführt. *Rollenträger*, die sicherheitskritische Aufgaben durchführen, müssen vor der Ernennung zum *Rollenträger* ein Führungszeugnis vorgelegt haben. Nach einer erfolgreichen Zuverlässigkeitsprüfung werden im Anschluss daran regelmäßige Background Checks dieser Mitarbeiter durchgeführt.

5.3.3. Anforderungen an Schulung und Fortbildung

Das für die Zertifizierungstätigkeiten eingesetzte Personal wird vor Aufnahme der Tätigkeit ausreichend geschult und sensibilisiert. Die Schulungsinhalte umfassen unter anderem die folgenden Themen:

- Grundlegende PKI-Kenntnisse,
- Sensibilisierung für IT-Sicherheit,
- Verhalten bei Verletzung der Sicherheitsvorgaben,
- Verhalten im Notfall,
- Umgang von Passwörtern, *PIN* und Chipkarten,
- Umgang mit personenbezogenen Daten,
- Datensicherung und deren Durchführung.

5.3.4. Nachschulungsintervalle und –anforderungen

Zur Aufrechterhaltung der Qualifikation des Personals werden Fortbildungsmaßnahmen eingeleitet. Je nach Aufgabe des Mitarbeiters werden die entsprechenden Schulungen regelmäßig oder bei Bedarf wiederholt.

5.3.5. Arbeitsplatzrotation / Rollenumverteilung

Eine regelmäßige Rollenumverteilung ist aufgrund der Trennung von Rollen und Aufgaben und die Durchführung sicherheitskritischer Aufgaben im Vier-Augen-Prinzip nicht erforderlich.

5.3.6. Sanktionen bei unbefugten Handlungen

Sollte ein Mitarbeiter gegen die Anweisungen und Vorschriften verstoßen, werden Maßnahmen zur Verhinderung zukünftiger Verletzungen ergriffen. In schweren Fällen beinhaltet dies auch arbeits- und strafrechtliche Maßnahmen.

5.3.7. Vertragsbedingungen mit dem Personal

Der *Zertifizierungsdienst*eanbieter *Fiducia & GAD IT AG* verpflichtet seine Mitarbeiter auf die Einhaltung von Anweisungen und gesetzlichen Vorschriften. Diese beinhalten insbesondere eine Verpflichtung, personenbezogene Daten vertraulich zu behandeln.

Werden unter Umständen externe Personen (unabhängige Auftragnehmer oder Berater) zur Besetzung vertrauenswürdiger Positionen eingesetzt, so unterliegen diese denselben Funktionsbeschränkungen und Sicherheitskriterien wie Mitarbeiter des *Zertifizierungsdienst*eanbieters *Fiducia & GAD IT AG* in vergleichbarer Position.

5.3.8. An das Personal ausgehändigte Dokumentation

Der *Zertifizierungsdienst* VR-Ident stellt den Mitarbeitern die zur Erfüllung ihrer Aufgaben erforderliche Dokumentation zur Verfügung. Folgende Dokumente werden den Mitarbeitern ausgehändigt:

- Informationen zu relevanten Gesetzen und Verordnungen,
- Technische Normen und Spezifikationen,
- Das vorliegende *CPS* (*Certification Practice Statement*) ,
- Interne Sicherheits- und Betriebskonzepte, Betriebshandbücher,
- Bedienungsanleitungen für Systeme und Software.

5.4. Protokollierung sicherheitskritischer Ereignisse

5.4.1. Zu protokollierende Ereignisse

Der *Zertifizierungsdienst* VR-Ident protokolliert (automatisch in elektronischer Form oder in Papierform) die folgenden wichtigen Ereignisse:

- Ereignisse im Lebenszyklus der VR-Ident Zertifikate, einschließlich:
  - Stammdatenerfassung für VR-Ident Zertifikate
  - Registrierung für VR-Ident Zertifikate,
  - Ausstellung von VR-Ident Zertifikaten,
  - Veröffentlichung von VR-Ident Zertifikaten,
  - Durchgeführte Sperrungen,
  - Erstellung und Veröffentlichung von *CRL* (Sperrlisten).
- Antragsdaten und Vollmachtsprüfung
  - Annahme der "Certification Practice Statement" (CPS) und der Sonderbedingungen,
  - Identität der Antragsannehmenden Instanz,
  - Methoden, die zur Prüfung der eingegangenen Vollmachten verwendet wurden (sofern anwendbar).

- Registrierungsdaten
  - Registrierungsdaten für VR-Ident SSL-Zertifikate im Key Management Workflow (interne VR-Ident SSL-Zertifikate) und im GAD Service-Portal (*VR-Banken*)
  - Antragsformulare in Papierform beziehungsweise in elektronischer Form im Auftragmanagement der *Fiducia & GAD IT AG*
- Ereignisse im Lebenszyklus der CA-Zertifikate und Schlüsselpaare,
  - Schlüsselgenerierung, Archivierung und Vernichtung von CA-Schlüsseln,
  - Ausstellung von CA-Zertifikaten,
  - Veröffentlichung von CA-Zertifikaten,
  - Durchgeführte Sperrungen von CA-Zertifikaten,
  - Erstellung und Veröffentlichung von *CRL* (Sperrlisten).
- Sicherheitsrelevante Ereignisse, einschließlich:
  - Anmeldung am PKI-System,
  - Vergabe und Entzug von Zugriffsberechtigungen,
  - Zugriffe und Zugriffsversuche auf das Netzwerk.
  - Durchführung der Arbeitsschritte im Key Management Workflow, bank21 und im GAD Service-Portal
  - Ereignisse im Lebenszyklus der *Hardware-Sicherheitsmodul*e (*HSM*)
- Ereignisse der Zutrittskontrollanlage, einschließlich:
  - Betreten und Verlassen von gesicherten Räumen,
  - Fehlgeschlagene Zutrittsversuche und Alarme,
  - Vergabe und Entzug von Zutrittsberechtigungen,
  - Beantragung, Ausgabe und Sperrung von Zutrittskarten.

Die Protokolleinträge enthalten die folgenden Daten:

- Typ des Eintrags,
- Uhrzeit und Datum des Eintrags (die Synchronisation der Uhren erfolgt über einen zentralen internen NTP Server, der wiederum seine Zeit von einer offiziellen Zeitquelle bezieht),
- Identifizierung der Stelle, die den Eintrag macht.

5.4.2. Häufigkeit der Auswertung von Protokolldaten

Protokolldaten werden bei Verdacht auf Unregelmäßigkeiten umgehend sowie im Rahmen von regelmäßigen Audits überprüft.

5.4.3. Aufbewahrungsfristen für Protokolldaten

Protokolldaten, die den Lebenszyklus der Zertifikate dokumentieren, (insbesondere Protokolldaten der CA-Systeme) werden vom *Zertifizierungsdienst* VR-Ident mindestens 7 Jahre nach Gültigkeitsablauf der Zertifikate aufbewahrt.

5.4.4. Schutz der Protokolldaten

Protokolldaten werden durch Zugriffskontrolle vor unbefugtem Zugriff und vor Manipulation geschützt. Es ist festgelegt, welche Rolle auf welche Protokolldaten zugreifen darf.

5.4.5. Sicherungsverfahren für Protokolldaten

Alle elektronischen Protokolldaten werden regelmäßig gesichert.

5.4.6. Internes/externes Protokollierungssystem

Sämtliche PKI-relevanten Log-Daten werden automatisch zu einem dedizierten Log-File-Server übertragen und dort gespeichert. Personen, die die Erzeugung von Log-Daten verursachen, haben dort keinen schreibenden Zugriff und können auf dem Log-File-Server gespeicherte Daten nicht verändern oder löschen.

Alle Protokolldaten werden innerhalb der gesicherten Bereiche des Rechenzentrums gespeichert. Es gibt keine externen Protokollierungssysteme.

5.4.7. Benachrichtigung des Auslösers eines Ereignisses

Alle Mitarbeiter des *Zertifizierungsdienst*eanbieters *Fiducia & GAD IT AG* sind über den Umfang der Protokollierung ihrer Tätigkeiten informiert.

Eine gesonderte Mitteilung über die Erzeugung von Log-Dateien erfolgt nicht.

5.4.8. Schwachstellenbewertung

Eventuelle Schwachstellen werden durch permanente Überwachung und durch Sicherheits-Audits durch den Information Security Officer des *Zertifizierungsdienst*eanbieters *Fiducia & GAD IT AG* und bei Bedarf durch externe Auditoren bewertet.

Eine Risikoanalyse und -Bewertung der Gesamtheit der angebotenen PKI-Dienste erfolgt monatlich.

5.5. Archivierung

5.5.1. Archivierte Daten und Aufbewahrungsfrist

Der *Zertifizierungsdienst* VR-Ident hat Systeme und Prozesse implementiert, um die Integrität der gespeicherten Daten gewährleisten zu können. Es werden turnusmäßig Sicherungskopien erstellt. Es wird die gesamte PKI-Datenbank archiviert.

5.5.2. Aufbewahrungsfrist

Die Zertifikate und zugehörigen Antragsunterlagen werden für einen Zeitraum von mindestens 7 Jahren nach Ablauf der angegebenen Gültigkeitsdauer der jeweiligen Zertifikate archiviert.

Papierhafte Daten (wie beispielsweise Antragsdaten) werden ebenfalls für einen Zeitraum von mindestens 7 Jahren archiviert.

5.5.3. Schutz der archivierten Daten

Die archivierten Daten sind durch technische Maßnahmen vor beabsichtigter oder unbeabsichtigter Manipulation und Löschung geschützt. Der Zugang zu diesen Daten ist nur berechtigten *Rollenträger*n möglich. Insbesondere sind archivierte Daten gegen Brand, Wasserschäden und andere Umwelteinflüsse gesichert. Innerhalb der Aufbewahrungsfristen ist die Lesbarkeit der archivierten Daten gewährleistet.

5.5.4. Sicherung der archivierten Daten

Alle elektronischen Archivdaten werden regelmäßig gesichert.

5.5.5. Anforderungen an den Zeitstempel der archivierten Daten

Archivierte Daten werden nicht mit elektronischen Zeitstempeln versehen. Archivierte Daten sind jedoch mit Datum und Uhrzeit versehen.

5.5.6. Internes/externes Archivierungssystem

Alle Daten werden innerhalb der Räumlichkeiten der *Fiducia & GAD IT AG* archiviert. Es gibt keine externen Archivierungssysteme.

5.5.7. Verfahren zum Einholen und Verifizierung von Archivdaten

Die Verfahren zum Einholen und zur Verifizierung von Archivdaten sind in internen Handlungsanweisungen festgelegt.

5.6. Schlüsselwechsel

Schlüsselpaare, die vom *Zertifizierungsdienst* VR-Ident für die Erbringung der *Zertifizierungsdienste* verwendet werden, besitzen eine beschränkte Gültigkeitsdauer, die im zugeordneten *Zertifikat* angegeben ist. Sie werden rechtzeitig vor Ablauf ihrer Gültigkeit gewechselt. Insbesondere werden CA-Schlüssel frühzeitig gewechselt, so dass die Gültigkeitsdauer der von der *CA* ausgestellten VR-Ident Zertifikate nicht die Gültigkeitsdauer des CA-Zertifikates übersteigt. Bei diesen regulären CA-Schlüsselwechseln erfolgt keine Sperrung des Zertifikates.

Ein außerordentlicher Wechsel eines Schlüssels der *Zertifizierungsstelle* VR-Ident findet in den folgenden Fällen statt:

- Das *Zertifikat* der *Zertifizierungsstelle* VR-Ident wird gesperrt,
- Es wurde bereits festgestellt oder es besteht der Verdacht, dass der private Schlüssel kompromittiert wurde.
- Die dem Schlüsselpaar zugeordneten Algorithmen oder die verwendete Schlüssellänge bieten nach aktuellem Wissensstand für die vorgesehene Nutzungsdauer keine ausreichende Sicherheit.
- Das darüber liegende CA-Zertifikat wurde gesperrt.

Bei einem außerordentlichen Schlüsselwechsel wird das zugehörige CA-Zertifikat gesperrt. Die Sperrung eines CA-Zertifikates hat die Sperrung aller damit ausgestellten Zertifikate zur Folge.

Im Fall einer Sperrung eines CA-Zertifikates wird die Sperrung durch den *Zertifizierungsdienst* VR-Ident unverzüglich auf ihrer Webseite bekannt gegeben. Die Verantwortlichen der hierdurch gesperrten VR-Ident Zertifikate werden unverzüglich per E-Mail benachrichtigt.

Bei einem Schlüsselwechsel der *Zertifizierungsstelle* VR-Ident wird ein entsprechendes neues Schlüsselpaar erzeugt und für das neue Schlüsselpaar wird ein neues *Zertifikat* erzeugt. Nach dem Schlüsselwechsel wird der private Schlüssel des alten Schlüsselpaares vernichtet.

Bei einer bekannten oder vermuteten Kompromittierung des privaten Schlüssels gelten die Regelungen in Kapitel 5.7.3 (S. 33).

5.7. Business Continuity Management und Incident Handling

5.7.1. Prozeduren zu Incident Handling und zu Notfällen

Die *Fiducia & GAD IT AG* hat ein Incident Management System etabliert, um im Fall eines Sicherheitsvorfalls rechtzeitig und effektiv zu reagieren. Für das Rechenzentrum sind darüber hinaus interne Notfallpläne vorhanden, in denen die Prozeduren und Verantwortlichkeiten bei Notfällen und Katastrophen geregelt sind. Zielsetzung dieser Notfallprozeduren ist die Minimierung von Ausfällen der Zertifizierungsdienstleistungen bei gleichzeitiger Aufrechterhaltung der Sicherheit.

Alle PKI Rechner sind in zwei Rechenzentren redundant ausgelegt. Im Falle des Ausfalls eines der Rechenzentren ist dadurch ein Weiterbetrieb der PKI gewährleistet. Im Notfall werden Ausfälle vom maximal einem Werktag akzeptiert. Die Wiederherstellung der Systeme erfolgt ebenfalls innerhalb eines Werktages.

5.7.2. Prozeduren bei Kompromittierung von Ressourcen

Nach einer vermuteten oder tatsächlichen Kompromittierung von Ressourcen, Software oder Daten finden die Notfallprozeduren Anwendung. Zur Wiederherstellung der kompromittierten Ressourcen, Software oder Daten werden insbesondere die letzten, von der Kompromittierung nicht betroffenen, Sicherungskopien der Systemkonfigurationen und Daten verwendet. Die Prozeduren zur Wiederherstellung nach einer Kompromittierung von Ressourcen sind in einem internen Recovery-Konzept festgelegt.

5.7.3. Prozeduren bei Kompromittierung von CA-Schlüsseln

Im Falle einer Kompromittierung des privaten Schlüssels einer *CA* des *Zertifizierungsdienst*eanbieters *Fiducia & GAD IT AG* wird das jeweilige CA-*Zertifikat* sowie alle mit diesem CA-Schlüssel unmittelbar oder mittelbar ausgestellten Zertifikate unverzüglich gesperrt.

Außerdem werden die Umstände der Kompromittierung genau untersucht. Insbesondere wird untersucht, ob die für die Erzeugung und Anwendung des privaten Schlüssels eingesetzten Algorithmen, Parameter oder Geräte unsicher sind.

Alle betroffenen *Zertifikatseigentümer* und Organisationen werden vom *Zertifizierungsdienst* VR-Ident per E-Mail über die Sperrung des Zertifikats benachrichtigt.

Nach Abschluss der Untersuchung der Umstände, die zur Kompromittierung des CA-Schlüssels führten, werden Maßnahmen ergriffen, die eine Wiederholung des Zwischenfalls verhindern sollen. Anschließend wird eine neuer CA-Schlüssel ausgestellt.

5.7.4. Notbetrieb im Katastrophenfall

Für den Katastrophenfall wird der Betrieb durch die redundante Infrastruktur aufrechterhalten. Der Weiterbetrieb der Rechenzentren ist in dem internen Notfallvorsorgekonzept und Notfallhandbuch geregelt.

Der Normalbetrieb wird sobald wie möglich wieder aufgenommen.

5.8. Einstellung der Zertifizierungsdienste

Im Fall, dass der *Zertifizierungsdienst* VR-Ident die *Zertifizierungsdienst*e einstellt, werden im Einzelnen die folgenden Maßnahmen ergriffen:

- Der *Zertifizierungsdienst* VR-Ident benachrichtigt (schriftlich oder per E-Mail) die Zertifikatsinhaber oder die Vertragspartner drei Monate im Voraus über die Tätigkeitseinstellung und teilt ihnen mit, ob ein anderer *Zertifizierungsdienst*eanbieter die Tätigkeit und die Zertifikate übernimmt.
- Soweit kein anderer *Zertifizierungsdienst*eanbieter den *Sperrdienst*, *Verzeichnisdienst* und Statusinformationsdienst für die VR-Ident Zertifikate übernimmt, ist der *Zertifizierungsdienst* VR-Ident zur Sperrung der Zertifikate zum Zeitpunkt der Einstellung der Zertifizierungstätigkeit berechtigt. Zum Zeitpunkt der Einstellung des Betriebs werden die CA-Zertifikate ebenfalls gesperrt und die zugehörigen Schlüssel vernichtet.
- Die Einstellung des Zertifizierungsbetriebes wird auf der Webseite http://www.vr-ident.de veröffentlicht.
- Soweit erforderlich, informiert der *Zertifizierungsdienst* VR-Ident Dritte (beispielsweise die VR-Banken) über die Einstellung der Tätigkeit.
- Der *Zertifizierungsdienst* VR-Ident benachrichtigt gegebenenfalls die *Zertifizierungsstelle* VR-Ident über die Einstellung der Tätigkeit.

6. Technische Sicherheitsmaßnahmen

6.1. Erzeugung und Installation von Schlüsselpaaren

6.1.1. Erzeugung von Schlüsselpaaren

Die CA-Signaturschlüsselpaare und Schlüsselpaare der *OCSP-Responder* werden in Hardware-Sicherheitsmodulen (*HSM*s) erzeugt, die nach *FIPS 140-2* Level 4 (siehe Anhang mit allgemeinen Referenzen) evaluiert sind. Die Schlüsselerzeugung erfolgt gemäß der Key Ceremony Policy und nur durch qualifizierte und autorisierte *Rollenträger* unter Aufsicht eines qualifizierten Auditors. Die *Hardware-Sicherheitsmodul*e (*HSM*) befinden sich in einer physikalisch gesicherten Umgebung des Rechenzentrums. Nur autorisiertes Personal hat Zugang zu den Hardware-Sicherheitsmodulen (*HSM*). Alle Aktivitäten in Bezug auf die Schlüsselerzeugung werden protokolliert.

Endbenutzer-Schlüsselpaare werden in der Regel beim *Antragsteller* selbst generiert. Der *Zertifizierungsdienst* VR-Ident empfiehlt Endbenutzern, zur Schlüsselgenerierung *Hardware-Sicherheitsmodul*e (*HSM*) zu verwenden die mindestens nach *FIPS 140-2* Level 2 oder einem vergleichbaren Standard (wie beispielsweise *CC* (*Common Criteria*)) evaluiert sind.

Bei allen Domains, wo die *Fiducia & GAD IT AG* bei dem Registrar einer Top-Level-Domain als Inhaber registriert ist, werden die Schlüsselpaare in der gesicherten Umgebung des Rechenzentrums der *Fiducia & GAD IT AG* generiert. Hierzu werden *Hardware-Sicherheitsmodul*e (*HSM*) verwendet, die nach *FIPS 140-2* Level 4 evaluiert sind. Die *Fiducia & GAD IT AG* bietet auch weiteren Unternehmen diese Dienstleitung an.

6.1.2. Übermittlung privater Schlüssel an den Zertifikatseigentümer

Falls der Endbenutzer das Schlüsselpaar selbst generiert, werden keine *privaten Schlüssel* übermittelt.

Falls die Schlüssel bei der *Fiducia & GAD IT AG* erzeugt werden, wie in Kapitel 6.1.1 (S. 34) beschrieben, werden die *privaten Schlüssel* in einer PIN-geschützen Datei (z. B. *PKCS*#12, JKS, PEM) übermittelt.

6.1.3. Übermittlung öffentlicher Schlüssel an den Zertifikatsaussteller

Die Übermittlung des *öffentlichen Schlüssel*s erfolgt über einen signierten Zertifikat Request.

6.1.4. Übermittlung öffentlicher CA-Schlüssel an vertrauende Dritte

Die öffentlichen CA-Schlüssel können über den in Kapitel 2.1 (S. 8) beschriebenen öffentlichen *Verzeichnisdienst* oder über die Webseite http://www.vr-ident.de abgerufen werden. Die zugehörigen *Fingerprints* befinden sich ebenfalls dort.

6.1.5. Schlüssellängen

Der *Zertifizierungsdienst* VR-Ident verwendet *RSA*-Schlüssel mit einer Länge von

- 2048 Bit für übergeordnete externe Root CA,
- 2048 Bit für die VR-Ident CA-Zertifizierungsinstanzen,
- mindestens 2048 Bit für Kunden.

6.1.6. Erzeugung und Prüfung der Schlüsselparameter

Die VR-Ident CAs führen eine Qualitätsprüfung von Schlüsselmaterial gemäß Klausel 6.1.6 der "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" durch.

6.1.7. Verwendungszweck der Schlüssel

Die Nutzung der *privaten Schlüssel* für VR-Ident Zertifikate muss den Vorgaben im Kapitel 1.4.1 (S. 5) entsprechen.

Die genaue Bezeichnung des Verwendungszweckes des Schlüssels ist schlüsselabhängig und wird in den Zertifikatserweiterungsfeldern "Schlüsselverwendung" und "Erweiterte Schlüsselverwendung" vermerkt (siehe auch Kapitel 7.1 (S. 40)).

Die genaue Bezeichnung des Verwendungszweckes des privaten Schlüssels für CA-Zertifikate wird im Zertifikatserweiterungsfeld "Schlüsselverwendung" vermerkt (siehe auch Kapitel 7.1 (S. 40)).

6.2. Schutz der privaten Schlüssels und der kryptographischen Module

6.2.1. Standards und Schutzmechanismen der kryptographischen Module

Die vom *Zertifizierungsdienst* VR-Ident verwendeten *Hardware-Sicherheitsmodul*e (*HSM*) sind nach dem Standard *FIPS 140-2* Level 4 (siehe Anhang mit allgemeinen Referenzen) zertifiziert und werden gemäß den Vorgaben der Zertifizierung betrieben.

6.2.2. Aufteilung der Kontrolle über private Schlüsseln auf mehrere Personen

Jeglicher administrativer oder operativer Zugriff auf die *Hardware-Sicherheitsmodul*e (*HSM*) wird im Vier-Augen-Prinzip durchgeführt. Nach der Initialisierung der Module (vor der Schlüsselgenerierung) werden entsprechende Authentisierungs-Token (Passwörter oder Chipkarten) für die *Rollenträger*, auf welche die Kontrolle aufgeteilt wird, erzeugt und somit das Vier-Augen-Prinzip technisch durchgesetzt.

6.2.3. Hinterlegung privater Schlüssel

Private Schlüssel werden nicht hinterlegt.

6.2.4. Backup privater Schlüssel

Der *Zertifizierungsdienst* VR-Ident erstellt Backup-Kopien von CA-Schlüsseln für Wiederherstellungszwecke. Die Schlüssel werden in verschlüsselter Form in einer Datenbank gespeichert.

Private Schlüssel der Kunden werden nicht vom *Zertifizierungsdienst* VR-Ident gesichert.

6.2.5. Archivierung privater Schlüssel

Private CA-Schlüssel werden nicht archiviert. Nach Ablauf ihrer Nutzungsdauer können die CA-Schlüssel nicht mehr verwendet werden.

6.2.6. Transfer privater Schlüssel

Private Schlüssel der *CA* sind in Hardware-Sicherheitsmodulen (*HSM*) in verschlüsselter Form gespeichert. Falls ein privater Schlüssel einer *CA* von einem Hardware-Sicherheitsmodul (*HSM*) zum anderen transportiert werden soll (beispielsweise zwecks Recovery), so erfolgt der Schlüsseltransport ausschließlich in verschlüsselter Form.

Private Schlüssel der Kunden werden nicht transferiert, falls sie bei dem Kunden generiert wurden. In Kapitel 6.1.1 (S. 34) ist beschrieben, wie der Transfer privater Schlüssel von der *Fiducia & GAD IT AG* zum *Antragsteller* erfolgt.

6.2.7. Speicherung privater Schlüssel

Private Schlüssel der *CA* sind entweder in den die Hardware-Sicherheitsmodulen (*HSM*) oder in verschlüsselter Form in der Datenbank gespeichert.

Private Schlüssel der Kunden werden vom *Zertifizierungsdienst* VR-Ident nicht gespeichert.

6.2.8. Methoden zur Aktivierung privater Schlüssel

Private Schlüssel der *CA* werden aktiviert, indem sich zwei Key Manager im Vier-Augen-Prinzip mittels Benutzerkennung und Passwort gegenüber dem Hardware-Sicherheitsmodul (*HSM*) auf den betreffenden Systemen authentisieren.

Private Schlüssel der Kunden werden aktiviert, indem sie auf dem entsprechenden Webserver installiert werden und die *PIN* eingegeben wird. Die PIN wurde vom Kunden selbst bei der Generierung des Schlüsselpaares festgelegt.

Falls das Schlüsselpaar bei der *Fiducia & GAD IT AG* erzeugt wird, wird dem *Antragsteller* auf separatem Weg die *PIN* übermittelt (siehe Kapitel 6.1.2).

6.2.9. Methoden zur Deaktivierung privater Schlüssel

Private Schlüssel der CA, die nicht mehr benötigt werden, werden durch die *Rollenträger* am Hardware-Sicherheitsmodul (*HSM*) des betreffenden Systems dauerhaft deaktiviert.

Private Schlüssel der Kunden werden durch das Abmelden vom entsprechenden System oder das Abmelden des Webservers deaktiviert.

6.2.10. Methoden zur Vernichtung privater Schlüssel

Private Schlüssel der *CA* werden sicher gelöscht, bevor das Hardware-Sicherheitsmodul (*HSM*) der sicheren Betriebsumgebung entnommen wird (beispielsweise für eine Reparatur oder Entsorgung). Sie können nach Ablauf der Gültigkeitsdauer des Schlüssels nicht mehr verwendet werden. Private Schlüssel der *CA*, die abgelaufen beziehungsweise ungültig geworden sind und daher keine Verwendung mehr finden, werden in den nutzenden Systemen gelöscht.

Es liegt in der Verantwortung des Webserver-Administrators, den *privaten Schlüssel* des Antragstellers sicher zu löschen, falls dieser nicht mehr benötigt wird.

6.2.11. Bewertung kryptographischer Module

Siehe Kapitel 6.2.1 (S. 35).

6.3. Weitere Aspekte des Schlüsselmanagements

6.3.1. Archivierung öffentlicher Schlüssel

Öffentliche Schlüssel sind in den Zertifikaten enthalten und werden für mindestens 7 Jahre im VR-Ident *Verzeichnisdienst* aufbewahrt.

6.3.2. Verwendungsdauern von Zertifikaten und Schlüsselpaaren

Private Schlüssel der *CA* werden nach Ablauf ihres Zertifikates nicht mehr verwendet (siehe Kapitel 6.2.1 (S. 35)). Die Gültigkeitsdauer der CA-Zertifikate beträgt maximal 20 Jahre.

VR-Ident SSL-Zertifikate haben bis zum Februar 2018 eine Gültigkeit von 13 Monaten oder von 37 Monaten und danach, also ab März 2018, eine Gültigkeit von 27 Monaten, VR-Ident EV SSL-Zertifikate haben eine Gültigkeit von 27 Monaten.

6.4. Aktivierungsdaten

6.4.1. Erzeugung und Installation von Aktivierungsdaten

Aktivierungsdaten für den Schutz der *privaten Schlüssel* der *CA* werden gemäß Kapitel 6.2.2 (S. 35) und den Vorgaben des Key Ceremony entweder zufällig durch das Hardware-Sicherheitsmodul (*HSM*) oder von dem verantwortlichen *Rollenträger* gewählt. Die *Rollenträger* sind verpflichtet, starke Passwörter zu wählen, um die *privaten Schlüssel* der *CA* vor unbefugtem Zugriff zu schützen. Die Erzeugung der *Aktivierungsdaten* wird protokolliert.

Für die *Aktivierungsdaten* der Schlüssel der Kunden empfiehlt der *Zertifizierungsdienst* VR-Ident ebenfalls starke Passwörter zu verwenden.

6.4.2. Schutz der Aktivierungsdaten

Für den Schutz der *Aktivierungsdaten* für private Schlüssel der *CA* hat der *Zertifizierungsdienst* VR-Ident die folgenden Sicherheitsmaßnahmen implementiert:

- Jeder Mitarbeiter des *Zertifizierungsdienst* VR-Ident ist verpflichtet, die von ihm gewählten Passwörter und *PIN* vertraulich zu behandeln und diese nicht aufzuschreiben.
- Jeder Mitarbeiter des *Zertifizierungsdienst* VR-Ident ist verpflichtet, die ihm zugeordneten Zugangsdaten für *Hardware-Sicherheitsmodul*e (*HSM*) vor Missbrauch zu schützen und nach Benutzung sicher zu verwahren.
- Falls ein Mitarbeiter aus dem *Zertifizierungsdienst* VR-Ident ausscheidet, werden seine Zugriffsrechte entnommen und durch neue ersetzt.

Für den Schutz von Endnutzer-Zertifikaten ist der Endnutzer selbst zuständig. Er muss jedoch seine Aktivierungsdaten vor unbefugten Zugriff und unbefugter Kenntnisnahme schützen.

Die *Aktivierungsdaten* für private Kunden-Schlüssel müssen ebenfalls vor unbefugten Zugriff geschützt werden.

6.4.3. Weitere Aspekte von Aktivierungsdaten

Die Ausmusterung von *Aktivierungsdaten* erfolgt mittels Methoden, die einen Verlust, Diebstahl oder eine unautorisierte Kenntnisnahme oder Nutzung der mit diesen *Aktivierungsdaten* geschützten *privaten Schlüssel* verhindern.

6.5. Sicherheitsmaßnahmen für Computer

6.5.1. Spezielle Anforderungen zur Computersicherheit

Die IT-Systeme, welche die wichtigsten *Zertifizierungsdienste* bereitstellen, insbesondere die IT-Systeme der CA, der *OCSP-Responder* und der RA, sowie weitere IT-Systeme, die dem Schutz der Einrichtungen der Zertifizierungsinfrastruktur dienen, unterliegen den folgenden Sicherheitsanforderungen:

- Auf den IT-Systemen sind nur die notwendigen Anwendungen installiert.
- Die IT-Systeme verfügen nur die für die entsprechende Aufgabe notwendigen Kommunikationsschnittstellen. Insbesondere sind die IT-Systeme nur in die für ihre Aufgabe notwendigen Netzwerkbereiche integriert.
- Die IT-Systeme sind in abschließbaren Serverschränken im Rechenzentrum der *Fiducia & GAD IT AG* untergebracht.
- Der Zugriff auf die IT-Systeme ist auf das für den Zertifizierungsbetrieb notwendige Maß beschränkt. Insbesondere werden IT-Systeme nur durch autorisierte Administratoren verwaltet.

- Der Zugriff zu den sicherheitskritischen IT-Systemen wie beispielsweise zu den Hardware-Sicherheitsmodulen (*HSM*) ist nur im 4-Augen-Prinzip möglich.
- IT-Systeme mit hohen Verfügbarkeitsanforderungen (wie beispielsweise der VR-Ident *Verzeichnisdienst*) sind redundant ausgelegt, so dass bei Ausfall eines IT-Systems der Dienst erhalten bleibt.
- Mittels unterbrechungsfreier Stromversorgungen werden Schwankungen in der Stromversorgung ausgeglichen und Stromausfälle bis zu einer Dauer von mehreren Stunden überbrückt.
- Auf den IT-Systemen dürfen nur auf Schadsoftware geprüfte Datenträger verwendet werden.
- Die IT-Systeme werden durch permanentes Monitoring überwacht.
- Sicherheitskritische Ereignisse auf den IT-Systemen werden protokolliert.

6.5.2. Bewertung der Computersicherheit

Eine formale Evaluierung der Systemsicherheit wurde für die *Hardware-Sicherheitsmodule* (*HSM*, siehe Kapitel 6.2.1 (S. 35)) durchgeführt.

Der *Zertifizierungsdienst* VR-Ident hat technische Sicherheitsmaßnahmen implementiert, deren Eignung durch permanente Überwachung und durch Sicherheits-Audits durch den *Zertifizierungsdienst* VR-Ident Information Security Officer und bei Bedarf durch externe Auditoren bewertet wird.

6.6. Technische Kontrollen des Software-Lebenszyklus

6.6.1. Systementwicklungsmaßnahmen

Die Entwicklung und Implementierung von Anwendungsprogrammen der *Fiducia & GAD IT AG* erfolgt im Einklang mit den Systementwicklungs- und Change Management-Richtlinien der *Fiducia & GAD IT AG*.

Die Sicherheitsmaßnahmen bei der Entwicklung der nach FIPS-140-2 (siehe Anhang mit allgemeinen Referenzen) zertifizierten oder nach CC (Common Criteria) evaluierten Komponenten (Hardware-Sicherheitsmodule, HSM) entsprechen den strengen Vorgaben der Zertifizierungs- und Evaluierungsverfahren.

6.6.2. Sicherheitsmanagement

Im Sicherheitskonzept der *Fiducia & GAD IT AG* sind die Verantwortlichkeiten und Prozesse des Sicherheitsmanagements klar definiert.

6.6.3. Maßnahmen zur Kontrolle des Software-Lebenszyklus

Der *Zertifizierungsdienst* VR-Ident stellt sicher, dass die für die *Zertifizierungsdienst*e eingesetzte Software in einer Weise entwickelt, getestet, ausgeliefert, installiert, konfiguriert, betrieben und gewartet wird, so dass ihre *Authentizität*, Integrität, und bestimmungsgemäßen Funktionsfähigkeit sichergestellt ist.

6.7. Maßnahmen zur Netzwerksicherheit

Der *Zertifizierungsdienst* VR-Ident hat folgende Sicherheitsvorkehrungen zur Netzwerksicherheit getroffen:

- Die PKI-Systeme sind durch ausreichende Sicherheits-Gateways (Firewalls) vom Internet getrennt.
- Sicherheitskritische IT-Systeme, die vom Internet aus erreichbar sein müssen (wie beispielsweise die *OCSP-Responder* oder der VR-Ident *Verzeichnisdienst*), sind in einer *DMZ* untergebracht, die vom Internet und dem internen CA-Netz durch Firewalls getrennt sind. Alle anderen sicherheitskritischen IT-Systeme befinden sich in internen Netzbereichen.
- Es werden nur Kommunikationswege (Ports) frei geschaltet, die zwingend erforderlich sind.
- Die Netzwerksicherheit wird regelmäßig geprüft. Bei entdeckten Sicherheitslücken werden entsprechende Sicherheitsmaßnahmen eingeleitet.

- Angriffe auf öffentlich verfügbare IT-Systeme werden durch das Monitoring System überwacht und gegebenenfalls abgewehrt.

6.8. Zeitstempel

Der *Zertifizierungsdienst* VR-Ident betreibt keinen Zeitstempeldienst als Dienstleistung. Alle Protokolldaten werden mit Zeitangaben versehen.

7. Profile

7.1. Zertifikatsprofile

Die von der VR-Ident PKI verwendeten Zertifikate entsprechen dem Standard X.509. Die Zertifikate enthalten unter anderem Daten über den Gültigkeitszeitraum, den verwendeten Signaturalgorithmus, die Schlüssellänge, den Zertifikatsinhaber und den Aussteller. Mit den im X.509 definierten Zertifikatserweiterungen kann der Informationsgehalt des Zertifikats um weitere Angaben ergänzt werden.

7.1.1. Versionsnummern und Basisdaten

"QuoVadis Root CA 2" Zertifikat

Das *Zertifikat* der "QuoVadis Root CA 2" entspricht dem Zertifikatsprofil *X.509* in der Version 3 (siehe Anhang mit allgemeinen Referenzen). In den Basisfeldern enthält es folgende Informationen:

Tabelle 7.1. "QuoVadis Root CA 2" Zertifikat

Zertifikatsfeld	Inhalt
Version	V 3
Seriennummer	05 09
Signaturalgorithmus	sha1RSA
Aussteller (Issuer DN)	CN = QuoVadis Root CA 2 O = QuoVadis Limited C = BM
Gültig ab (not before)	Freitag, 24. November 2006 19:27:00
Gültig bis (not after)	Montag, 24. November 2031 19:23:33
Antragsteller (Subject DN)	CN = QuoVadis Root CA 2 O = QuoVadis Limited C = BM
Öffentlicher Schlüssel	Kodierter Wert des Schlüssels, RSA 4096 bit
Signatur	Digitale Signatur der QuoVadis Root CA 2
Fingerprint-Algorithmus	sha1
Fingerprint (sha1)	ca 3a fb cf 12 40 36 4b 44 b2 16 20 88 80 48 39 19 93 7c f7

"VR IDENT SSL CA 2016" Zertifikat

Das "VR IDENT SSL CA 2016" *Zertifikat* entspricht dem Zertifikatsprofil *X.509* in der Version 3, sowie *RFC* 5280 und Common *PKI* (siehe Anhang mit allgemeinen Referenzen). In den Basisfeldern enthält es folgende Informationen:

Tabelle 7.2. "VR IDENT SSL CA 2016" Zertifikat

Zertifikatsfeld	Inhalt
Version	V 3
Seriennummer	Eindeutiger Wert, 4d 14 49 94 d4 f1 f2 7e dc 42 f3 5e 84 ce fa 07 e9 88 fe 02
Signaturalgorithmus	sha256RSA
Aussteller (Issuer DN)	CN = QuoVadis Root CA 2 O = QuoVadis Limited C = BM

Gültig ab (not before)	Dienstag, 12. Januar 2016 16:53:00
Gültig bis (not after)	Montag, 12. Januar 2026 16:53:00
Antragsteller (Subject DN)	CN = VR IDENT SSL CA 2016 O = FIDUCIA & GAD IT AG OU = VR IDENT C = DE
Öffentlicher Schlüssel	Kodierter Wert des Schlüssels, RSA 2048 bit
Signatur	Digitale Signatur der QuoVadis Root CA
Fingerprint-Algorithmus	sha1
Fingerprint (sha1)	29 ef 54 e6 a0 4a b1 9a 0d d6 87 e9 ee c0 5b 16 3d b5 96 25

VR-Ident SSL-Zertifikate

Der *Zertifizierungsdienst* VR-Ident stellt VR-Ident SSL-Zertifikate nach *X.509* in der Version 3, sowie gemäß *RFC* 5280 und Common *PKI* (siehe Anhang mit allgemeinen Referenzen) aus. In den Basisfeldern enthalten sie folgende Informationen:

Tabelle 7.3. VR-Ident SSL-Zertifikate

Zertifikatsfeld	Inhalt
Version	V 3
Seriennummer	Eindeutiger Wert > 0, nicht sequentiell, mindestens 64 Zufallsbits
Signaturalgorithmus	sha256RSA
Aussteller (Issuer DN)	CN = VR IDENT SSL CA 2016 O = FIDUCIA & GAD IT AG OU = VR IDENT C = DE
Gültig ab (not before)	Datum und Uhrzeit
Gültig bis (not after)	Datum und Uhrzeit
Antragsteller (Subject DN)	CN = URL oder Domain der Organisation OU = VR-IDENT (Beispiel) O = Name der Organisation/ Firma L = Frankfurt am Main (Beispiel) ST = Hessen (Beispiel) C = DE
Öffentlicher Schlüssel	Kodierter Wert des Schlüssels
Signatur	Digitale Signatur der VR IDENT SSL CA 2016

7.1.2. Zertifikatserweiterungen

"QuoVadis Root CA 2" Zertifikat

Die Erweiterungen des "QuoVadis Root CA 2" Zertifikats sind in der folgenden Tabelle dargestellt:

Tabelle 7.4. Erweiterungen des "QuoVadis Root CA 2"Zertifikats

Erweiterungen	
Schlüsselverwendung (KeyUsage)	Zertifikatsignatur, Offline Signieren der Zertifikatsperrliste, Signieren der Zertifikatsperrliste (06)
Schlüsselkennung des Antragstellers (SubjectKeyIdentifier)	1a 84 62 bc 48 4c 33 25 04 d4 ee d0 f6 03 c4 19 46 d1 94 6b

Stellenschlüsselkennung (AuthorityKeyIdentifier)	Schlüssel-ID=1a 84 62 bc 48 4c 33 25 04 d4 ee d0 f6 03 c4 19 46 d1 94 6b Zertifikataussteller: Verzeichnisadresse: CN=QuoVadis Root CA 2 O=QuoVadis Limited C=BM Seriennummer des Zertifikats=05 09
Kritische Erweiterungen	
Basiseinschränkungen (BasicConstraints)	CA:TRUE Einschränkung der Pfadlänge=Keine

"VR IDENT SSL CA 2016" Zertifikat

Die Erweiterungen des "VR IDENT SSL CA 2016" Zertifikats sind in der folgenden Tabelle dargestellt:

Tabelle 7.5. Erweiterungen des "VR IDENT SSL CA 2016" Zertifikats

Erweiterungen	
Zertifikatsrichtlinie (CertificatePolicies)	[1] Richtlinienbezeichner=2.23.140.1.2.2 [2] Richtlinienbezeichner=1.3.6.1.4.1.8024.0.2.1600.0.1 [2,1] Richtlinienkennzeichnerinformationen: Kennung des Richtlinienqualifizierers=CPS Qualifizierer: http://www.quovadisglobal.com/repository [3] Richtlinienbezeichner=1.3.6.1.4.1.17696.4.1.1.9 [3,1] Richtlinienkennzeichnerinformationen: Kennung des Richtlinienqualifizierers=CPS Qualifizierer: http://www.vr-ident.de
Stelleninformationszugriff (AuthorityInfoAccess)	Zugriffsmethode = Onlinestatusprotokoll des Zertifikats (1.3.6.1.5.5.7.48.1) Alternativer Name: URL=http://ocsp.quovadisglobal.com Zugriffsmethode = Zertifizierungsstellenaussteller (1.3.6.1.5.5.7.48.2) Alternativer Name: URL=http://trust.quovadisglobal.com/qvrca2.crt
Erweiterte Schlüsselverwendung (ExtendedKeyUsage)	serverAuth, clientAuth, OCSPSigning
Stellenschlüsselkennung (AuthorityKeyIdentifier)	Schlüssel-ID=1a 84 62 bc 48 4c 33 25 04 d4 ee d0 f6 03 c4 19 46 d1 94 6b
Sperrlistenverteilungspunkte (CRLDistributionPoints)	Vollständiger Name: URL=http://crl.quovadisglobal.com/qvrca2.crl
Schlüsselkennung des Antragstellers (SubjectKeyIdentifier)	50 52 4f 44 2e 47 54 4e 2e 45 58 53 53 4c 43 41 2e 53 49 47 47 45 4e 52 53 2e 30 30 30 30 32 37 30 30
Kritische Erweiterungen	
Basiseinschränkungen (BasicConstraints)	CA:TRUE Einschränkung der Pfadlänge=0
Schlüsselverwendung (KeyUsage)	Digitale Signatur, Zertifikatssignatur, Offline Signieren der Zertifikatssperrliste, Signieren der Zertifikatssperrliste (86)

VR-Ident SSL-Zertifikate

Die Erweiterungen der VR-Ident SSL-Zertifikate sind in der folgenden Tabelle dargestellt:

Tabelle 7.6. Erweiterungen der VR-Ident SSL-Zertifikate

Erweiterungen	
Basiseinschränkungen	Typ des Antragstellers=Endeinheit

(BasicConstraints)	Einschränkung der Pfadlänge=keine
Stelleninformationszugriff (AuthorityInfoAccess)	Zugriffsmethode = OCSP-Responder des Zertifikats (1.3.6.1.5.5.7.48.1) Alternativer Name: URL=http://ocsp.vr-ident.de/gtnocsp/OCSPResponder/VR%20IDENT%20SSL%20CA%202016
Alternativer Antragstellername (SubjectAltName), siehe auch Attribute	DNS-Name = <Inhalt des Attributs CN aus dem Subject DN> plus <weitere optionale Angaben>
Schlüsselkennung des Antragstellers (SubjectKeyIdentifier)	individuell
Erweiterte Schlüsselverwendung (ExtendedKeyUsage)	serverAuth, clientAuth
Stellenschlüsselkennung (AuthorityKeyIdentifier)	Schlüssel-ID=50 52 4f 44 2e 47 54 4e 2e 45 58 53 53 4c 43 41 2e 53 49 47 47 45 4e 52 53 2e 30 30 30 30 32 37 30 30
1.3.6.1.4.1.11129.2.4.2 ("CertificateTransparency")	Codierter Wert für die erfolgreiche Registrierung und Veröffentlichung an den Certificate Transparency Logservern
Zertifikatsrichtlinie (CertificatePolicies)	[1] Richtlinienbezeichner=1.3.6.1.4.1.17696.4.1.1.9 [1,1] Richtlinienkennzeichnerinformationen: Kennung des Richtlinienqualifizierers=CPS Qualifizierer: http://www.vr-ident.de [2] Richtlinienbezeichner=1.3.6.1.4.1.8024.0.2.1600.0.1 [2,1] Richtlinienkennzeichnerinformationen: Kennung des Richtlinienqualifizierers=CPS Qualifizierer: http://www.quovadisglobal.com/repository [3] Richtlinienbezeichner=2.23.140.1.2.2
Sperrlistenverteilungspunkte (CRLDistributionPoints)	Vollständiger Name: URL=http://www.vr-ident.de/gtncrl/CRLResponder/VR%20IDENT%20SSL%20CA%202016
Kritische Erweiterungen	
Schlüsselverwendung (KeyUsage)	Digitale Signatur, Schlüsselverschlüsselung (a0)

7.1.3. Algorithmus Bezeichner (OID)

Die eingesetzten Algorithmen Bezeichner entsprechen den gängigen Standards. Siehe auch in den entsprechenden Tabellen oben.

7.1.4. Namensformen

Siehe Kapitel 3.1.1.

7.1.5. Nutzung von Erweiterungen zur Namensbeschränkung (Name Constraints)

Erweiterungen zur Namensbeschränkung werden nicht verwendet.

7.1.6. Bezeichner für Zertifizierungsrichtlinien (OID)

Der *Object Identifier* (OID) für die vorliegende Policy ist in Kapitel 1.2 (S. 3) aufgeführt.

7.1.7. Nutzung von Erweiterungen zur Richtlinienbeschränkungen (PolicyConstraints)

Erweiterungen zur Richtlinienbeschränkungen werden nicht verwendet.

7.1.8. Syntax und Semantik von Policy Qualifiern

Die Policy Qualifier in der Erweiterung Certificate Policies enthalten einen Text, der dem Benutzer angezeigt werden kann, sowie eine URL zu dem entsprechenden *CPS* (*Certification Practice Statement*).

7.1.9. Verarbeitung von kritischen Erweiterungen für Zertifizierungsrichtlinien (CertificatePolicies)

Die Erweiterungen für Zertifizierungsrichtlinien in den VR-Ident Zertifikaten sind nicht kritisch.

7.2. Profil der Sperrlisten

Die von der VR-Ident PKI ausgestellten Sperrlisten entsprechen dem Standard X.509, die unter anderem Daten über den Gültigkeitszeitraum, den verwendeten Signaturalgorithmus, die Seriennummern der gesperrten Zertifikate, den Sperrgrund und den Aussteller der Sperrliste enthalten.

7.2.1. Versionsnummern

Die von VR-Ident ausgestellten *CRL* (Sperrlisten) entsprechen dem Standard *X.509* Version 2, sowie *RFC* 5280 und Common *PKI* (siehe Anhang mit allgemeinen Referenzen).

7.2.2. Erweiterungen der Sperrlisten

Die *CRL* (Sperrlisten) verwenden die nachfolgenden Erweiterungen (Extensions):

Tabelle 7.7. Erweiterungen der CRL (Sperrliste)

Erweiterungen	
Version	V 2
Aussteller (Issuer)	Der Aussteller einer Sperrliste ist identisch mit der *CA*, welche die Zertifikate herausgibt. Pro *CA* gibt es somit immer eine gültige Sperrliste, die mit dem gleichen Schlüssel signiert wurde, wie die dazugehörigen Zertifikate. CN = <Name der CA> OU = VR IDENT O = FIDUCIA & GAD IT AG C = DE
Gültig ab (not before)	Datum und Uhrzeit
Nächste Aktualisierung (nextUpdate)	Datum und Uhrzeit
Signaturalgorithmus	sha1RSA
Kritische Erweiterungen	
Stellenschlüsselkennung (AuthorityKeyIdentifier)	individuell
Sperrlistennummer (CRLNumber)	Laufende Nummer

Die Einträge der Sperrliste verwenden die nachfolgenden Erweiterungen (Extensions):

Tabelle 7.8. Erweiterungen der Einträge der CRL (Sperrliste)

Erweiterungen

Seriennummer (SerialNumber)	Seriennummer des gesperrten Zertifikats
Sperrdatum	Datum und Uhrzeit der Sperrung
SperrGrundCode (ReasonCode)	Grund der Sperrung. Dieser entspricht dem Wert revocationReason in den Antworten des OCSP-Responder. Folgende Sperrgründe können unter anderem verwendet werden: • "Unspecified", bei Kartensperre bei VR-Ident privat • "Cessation of Operation", sonstige Fälle bei VR-Ident privat • "Superseded", Zertifikat wurde abgelöst und wird erneuert bei VR-Ident SSL
CertificateIssuer	Name des Herausgebers des Zertifikats (siehe oben), der identisch ist mit dem Herausgeber der Sperrliste.
Keine kritischen Erweiterungen	

7.2.3. Weitere Eigenschaften der Sperrlisten

CRL (Sperrlisten) werden immer von dem Aussteller der Zertifikate signiert. Es werden somit nur direkte Sperrlisten unterstützt.

7.3. OCSP-Profile

Die von der VR-Ident PKI verwendeten OCSP Profile entsprechen RFC 6960 und dienen dazu den Status der VR-Ident Zertifikate gemäß X.509 zu ermitteln.

7.3.1. Versionsnummern

Der *OCSP-Responder* des VR-Ident Auskunftsdienstes über den Zertifikatsstatus unterstützt *OCSP* nach RFC 6960 in der Version 1 und ist konform zum Common *PKI* Standard (siehe Anhang mit allgemeinen Referenzen).

7.3.2. OCSP-Erweiterungen

Der *OCSP-Responder* unterstützt bei Anfragen die nachfolgenden Erweiterungen (OCSP-Extensions):

Tabelle 7.9. Zulässige Erweiterungen der Anfragen (OCSP-Requests)

Erweiterungen	
Nonce	Wert, der die Antwort kryptographisch an die Anfrage bindet (optional)

Der *OCSP-Responder* unterstützt bei Antworten die nachfolgenden Erweiterungen (OCSP-Extensions):

Tabelle 7.10. Zulässige Erweiterungen der Antworten (OCSP-Response)

Erweiterungen	
CertHash	Hashwert des Zertifikates, zu dem der Status abgefragt wurde.
Nonce	Gleicher Wert wie in der Anfrage. Nicht existent, falls dieser in der Anfrage nicht vorhanden war.

7.3.3. Weitere Eigenschaften der OCSP-Anfragen und Antworten

Anfragen (OCSP-Requests):

- Anfragen (OCSP-Requests) müssen nicht signiert sein, signierte Anfragen werden aber unterstützt. Die Signatur wird hierbei ignoriert.

- Das Feld "requestorName" kann beliebig gesetzt sein (auch leer).
- Das Feld "CertID" muss mit *SHA*-1 berechnet worden sein.

Antworten (OCSP-Response):

- as Feld "NextUpdate" enthält den Zeitpunkt, an dem spätestens aktuellere Informationen zum Status des Zertifikats verfügbar sind.
- Das Feld "ResponderID" in "ResponseData" enthält den *Distinguished Name* (*DN*) des *OCSP-Responder* aus seinem Zertifikat.
- Das Feld "Certs" enthält das *Zertifikat* des *OCSP-Responder* und das *Zertifikat* der CA, die das *Zertifikat* ausgestellt hat.
- Der Status "unknown" wird nur angegeben, wenn das *Zertifikat* nicht entsprechenden *CA* des *Zertifizierungsdienst* VR-Ident ausgestellt wurde.

8. Revisionen und andere Bewertungen

8.1. Häufigkeiten von Revisionen

Die Prozesse zur Erstellung der VR-Ident SSL-Zertifikate werden durch einen externen Auditor jährlich gemäß IDW PS 951 überprüft.

Weitere Audits werden mindestens im 4 Jahresrhythmus zur Einhaltung der Sicherheitsvorgaben durchgeführt.

Es kann aber mehr als ein Audit in diesen 4 Jahren durchgeführt werden, wenn beispielsweise ein vorangehendes Audit nicht zufrieden stellende Resultate ergeben hatte oder bei sicherheitsrelevanten Vorkommen.

Führungskräfte der Administratoren führen regelmäßig Überprüfungen durch, ob die Prozesse gemäß den Anforderungen eingehalten werden.

Die CA wurden weiterhin gegenüber den in der Einleitung genannten Anforderungen geprüft (Siehe Kapitel 1.1 (S. 1)). Die Überprüfung der Konformität gegenüber diesen Anforderungen wird jährlich durch einen externen Auditor nachgewiesen.

8.2. Identität und Qualifikation des Auditors

Für die interne PKI kann der *Zertifizierungsdienst* VR-Ident selbst entscheiden, ob die Audits durch einen externen Auditor durchgeführt werden oder durch einen Mitarbeiter der *Fiducia & GAD IT AG* (Innenrevision).

Für die Auditoren gelten folgende Qualifizierungsvoraussetzungen:

- Technisches und organisatorisches *PKI* Know-how.
- Vertraut sein mit den entsprechenden Normen und Standards (ISO 27001, ETSI EN 319401, ETSI EN 319411-1, IDW PS 951 und andere).

8.3. Beziehungen zwischen Auditor und zu untersuchender Partei

Für die interne PKI darf der Auditor ein Mitarbeiter der *Fiducia & GAD IT AG* sein, er darf aber nicht an der Leitung, Administration und dem Betrieb des Zertifizierungsdienstes VR-Ident beteiligt sein.

Bereiche, die durch einen externen Auditor bereits geprüft worden sind, können ausgelassen werden, sofern die Prüfergebnisse des externen Auditors in das interne Audit übernommen werden und keine Beanstandungen enthalten, die die Sicherheit der internen PKI betreffen.

8.4. Umfang der Prüfungen

Zielsetzung der Audits ist die Überprüfung der Umsetzung der definierten Maßnahmen. Der Auditor wählt den von der Beurteilung abzudeckenden Prüfumfang gemäß den Standards oder gemäß den gesetzlichen Vorschriften selbst aus. Dabei bezieht er alle Systeme, Einrichtungen, Verfahren und Informationen mit ein, die für die Umsetzung der Maßnahmen relevant sind. Die Prüfung umfasst insbesondere die folgenden Bereiche:

- Einrichtungen zur baulichen und physikalischen Sicherheit (z. B. Brandschutz, Zugangsschutz),
- Konfigurationen der sicherheitskritischen Systeme,
- Netzwerksicherheit,
- Protokolldaten sicherheitskritischer Systeme,
- Protokolle sicherheitskritischer Prozeduren (beispielsweise Prozeduren der Key Ceremony, Notfallprozeduren, Modifikationen der Systeme),
- Dokumentation der personellen Sicherheitsmaßnahmen (wie Schulungsnachweise, Dienstpläne oder ähnliches) ,
- Dokumentationen von Prozeduren und Systemen (z. B. Notfallpläne, Systemhandbücher),

- Schlüssel sowie Authentisierungs-Chipkarten (beispielsweise für die Zugangskontrolle oder den Zugriff auf *Hardware-Sicherheitsmodul*e (*HSM*)),
- Archivdaten.

8.5. Maßnahmen bei Mängeln

Die Mängel eines Audits werden je nach Schwere und Dringlichkeit entweder als Zwischenfall oder als Problem betrachtet und entsprechend weiterverfolgt. Bei schwerwiegenden Mängeln wird an das Management der *Fiducia & GAD IT AG* berichtet.

Der *Zertifizierungsdienst* VR-Ident stellt sicher, dass alle Sachverhalte verfolgt und zeitnah behoben werden.

8.6. Veröffentlichung der Ergebnisse

Die Ergebnisse dokumentiert der Auditor in einem Audit-Bericht. Eine Veröffentlichung der Ergebnisse findet in der Regel nicht statt.

8.7. Selbst-Audits

Der Zertifizierungsdienst VR-Ident überprüft durch Selbst-Audits laufend die Einhaltung der internen Certificate Policy und Certification Practice Statement und kontrolliert ständig die Qualität der angebotenen Dienste.

9. Weitere geschäftliche und rechtliche Regelungen

9.1. Gebühren

9.1.1. Gebühren für die Ausstellung und Erneuerung von Zertifikaten

Die *Fiducia & GAD IT AG* erhebt Gebühren für die Ausstellung und die Erneuerung von VR-Ident SSL-Zertifikaten. Die Gebühren für interne VR-Ident SSL-Zertifikate sind in den internen Preisverzeichnissen der *Fiducia & GAD IT AG* ersichtlich. Die Gebühren für VR-Ident SSL-Zertifikate für *Fiducia & GAD IT AG* Konzerntöchter und Verbundpartner erhalten Sie auf Anfrage bei der unter Kapitel 1.5.2 (S. 6) genannten Kontaktpersonen.

9.1.2. Gebühren für den Abruf von Zertifikaten

Es werden keine Gebühren für den Abruf von Zertifikaten erhoben.

9.1.3. Gebühren für die Abfrage von Zertifikatsstatusinformationen

Es werden keine Gebühren für die Abfrage von Zertifikatsstatusinformationen erhoben.

9.1.4. Gebühren für andere Dienstleistungen

Es werden keine Gebühren für sonstige Dienstleistungen in Bezug auf die VR-Ident Zertifikate erhoben.

Insbesondere werden keine Gebühren für den Zugriff auf das vorliegende Dokument erhoben.

9.1.5. Rückerstattungen

Bei einer Sperre eines gültigen VR-Ident Zertifikats hat der *Zertifikatseigentümer* keinen Anspruch auf Erstattung einer Vergütung oder sonstigen Ersatz von Kosten oder Aufwendungen, soweit der *Zertifizierungsdienst* VR-Ident die Sperrung berechtigterweise durchführt.

9.2. Finanzielle Verantwortung

9.2.1. Deckungsvorsorge

Die *Fiducia & GAD IT AG* als Betreiber des *Zertifizierungsdienst* VR-Ident verfügt über eine entsprechende Deckungsvorsorge (Vermögensschaden - Haftpflicht Versicherung in Höhe von 5 Millionen Euro), damit sie ihren gesetzlichen Verpflichtungen zum Schadenersatz nachkommen kann, die dadurch entstehen, dass ihre Produkte oder sonstige technische Sicherungseinrichtungen versagen.

Organisationen und Unternehmen als Inhaber von VR-Ident SSL-Zertifikatn wird geraten, ebenfalls entsprechende Maßnahmen zu treffen, um im Schadenfall ihre Kunden entschädigen zu können.

9.2.2. Weitere Vermögenswerte

Keine weiteren Vermögenswerte.

9.2.3. Erweiterte Versicherung oder Garantie

Keine weiteren Versicherungen oder Garantien.

9.3. Vertraulichkeit betrieblicher Informationen

9.3.1. Art der geheim zu haltenden Information

Als vertraulich gelten alle Informationen, die nicht Bestandteil des Zertifikats sind, insbesondere Geschäfts- und Betriebsgeheimnisse der Kunden und *Zertifikatseigentümer*.

9.3.2. Öffentliche Informationen

Als öffentlich gelten alle Informationen in den ausgestellten und veröffentlichten Zertifikaten, die *CRL* (Sperrlisten), sowie alle veröffentlichten *CPS* (*Certification Practice Statement*) und *CP* (*Certificate Policy*) Versionen.

9.3.3. Verantwortlichkeit für den Schutz von geheim zu haltenden Information

Der *Zertifizierungsdienst* VR-Ident sichert die in Kapitel 9.3.1 (S. 50) genannten vertraulichen Informationen vor Manipulation und unbefugter Kenntnisnahme durch Dritte.

9.4. Vertraulichkeit personenbezogener Informationen

9.4.1. Geheimhaltungsplan

Der *Zertifizierungsdienst* VR-Ident beachtet die gesetzlichen Anforderungen zur Geheimhaltung von vertraulichen, personenbezogenen Daten, insbesondere das Bundesdatenschutzgesetz sowie weitere Datenschutzvorschriften.

9.4.2. Vertraulich zu behandelnde Daten

Als vertraulich gelten alle personenbezogenen Daten, die nicht Bestandteil eines Zertifikats oder einer *CRL* (*Sperrliste*) sind.

9.4.3. Nicht vertraulich zu behandelnde Daten

Alle im *Zertifikat* enthaltenen Informationen gelten als nicht vertraulich.

9.4.4. Verantwortlichkeit für den Schutz privater Informationen

Der *Zertifizierungsdienst* VR-Ident wird Daten des Zertifikatsinhabers, soweit sie in personenbezogener oder personenbeziehbarer Form vorliegen, unter Einhaltung der einschlägigen Bestimmungen der Datenschutzvorschriften behandeln. Die Daten werden ausschließlich zum Zweck der Zertifikatserstellung verarbeitet.

9.4.5. Einverständniserklärung zur Nutzung privater Informationen

Soweit erforderlich, erteilt der *Antragsteller* sein jederzeit widerrufbares Einverständnis, dass der *Zertifizierungsdienst* VR-Ident seine personenbezogenen Daten zum Zweck der Zertifizierungsdienstleistungen verarbeiten darf.

9.4.6. Weitergabe von Informationen an Ermittlungsinstanzen oder Behörden

Der *Zertifizierungsdienst* VR-Ident ist zur Weitergabe von Informationen an ersuchende Gerichte oder andere Behörden verpflichtet, und hat Daten über die Identität des Zertifikatsinhabers auf Ersuchen an die zuständigen Stellen zu übermitteln, soweit die Voraussetzungen dazu erfüllt sind.

Mindestens eine der folgenden Voraussetzungen muss hierfür erfüllt sein:

- Es muss für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung erforderlich sein.
- Es muss für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder der Finanzbehörden erforderlich sein.
- Es muss durch Gerichte im Rahmen anhängiger Verfahren nach Maßgabe der hierfür geltenden Bestimmungen angeordnet worden sein.

9.4.7. Sonstige Offenlegungsgründe

Keine weiteren Offenlegungsgründe.

9.5. Geistiges Eigentum und dessen Rechte

Bestand und Inhalt von Urheber- und sonstigen Immaterialgüterrechten richten sich nach den allgemeinen gesetzlichen Vorschriften.

9.6. Gewährleistung, Sorgfalts- und Mitwirkungspflichten

9.6.1. Verpflichtung der Zertifizierungsstelle

VR-Ident sichert zu, dass die von ihm erzeugten VR-Ident Zertifikate alle Anforderungen des vorliegenden Dokumentes erfüllen.

9.6.2. Verpflichtung der Registrierungsstelle

Als *Registrierungsstelle* für VR-Ident Zertifikate sichert die *Fiducia & GAD IT AG* zu, dass die VR-Ident Zertifikate alle Anforderungen des vorliegenden Dokumentes erfüllen.

9.6.3. Verpflichtung des Zertifikatsinhabers

Der Kunde beziehungsweise der *Zertifikatseigentümer* haben insbesondere folgende Pflichten:

- Die vereinbarten Preise sind fristgerecht zu zahlen.
- Die VR-Ident Zertifikate sind nur bestimmungsgemäß und nicht missbräuchlich zu benutzen.
- Bei einer Nutzung eines VR-Ident Zertifikates mit Auslandsbezug sind die geltenden nationalen und internationalen Ausfuhr- und Nutzungsbestimmungen zu beachten.
- Die den VR-Ident Zertifikaten zugeordnenden *privaten Schlüssel* sind geheim zu halten und sicher vor unbefugten Zugriffen aufzubewahren.
- Mängel, Schäden oder sonstige Störungen sind unverzüglich dem *Zertifizierungsdienst* VR-Ident anzuzeigen.
- Bei Verlust oder Verdacht der Kompromittierung des dem VR-Ident *Zertifikat* zuzuordnenden privaten Schlüssels ist unverzüglich eine Sperrung des entsprechenden VR-Ident Zertifikates zu veranlassen.

- Ebenfalls hat der Kunde eine Sperrung seines VR-Ident Zertifikates zu veranlassen, wenn die im *Zertifikat* enthaltenden Daten nicht mehr den Daten zum Zertifizierungszeitpunkt übereinstimmen.
- Er muss sich regelmäßig über eventuelle Änderungen bezüglich sicherheitsrelevanter Aspekte oder-Verfahren auf der Webseite http://www.vr-ident.de informieren.

9.6.4. Verpflichtung vertrauender Dritter

Vertrauende Dritte sind dazu verpflichtet, Zertifikate und ihren Sperrstatus gemäß den in Kapitel 4.5.2 (S. 18) und Kapitel 4.9.6 beschriebenen Regeln zu überprüfen.

9.6.5. Verpflichtung anderer Teilnehmer

Keine Verpflichtungen für andere Teilnehmer.

9.7. Haftungsausschluss

Trotz größter Sorgfalt beim Betrieb der Zertifizierungsdienste und bei der Erstellung dieser Dokumentation kann die *Fiducia & GAD IT AG* die Möglichkeit nicht vollständig ausschließen, dass Fehler in den hier beschriebenen Prozeduren enthalten sind oder Systeme fehlerhaft arbeiten. Für diesen Fall lehnt die *Fiducia & GAD IT AG* jegliche Haftung ab.

Weiterhin schließt die *Fiducia & GAD IT AG* jegliche Haftung für Störungen aus, die sich aus Gegebenheiten außerhalb der Einflusssphäre der *Fiducia & GAD IT AG* ergeben.

9.8. Haftungsbeschränkungen

9.8.1. Haftung des *Zertifizierungsdienst* VR-Ident

Im Einzelnen gelten die folgenden Haftungsbestimmungen:

- Bei Vorsatz oder grober Fahrlässigkeit sowie bei Fehlen einer garantierten Eigenschaft haftet der *Zertifizierungsdienst* VR-Ident für alle darauf zurückzuführenden Schäden unbeschränkt.
- Bei leichter Fahrlässigkeit haftet der *Zertifizierungsdienst* VR-Ident im Fall der Verletzung des Lebens, des Körpers oder der Gesundheit unbeschränkt. Wenn der *Zertifizierungsdienst* VR-Ident durch leichte Fahrlässigkeit mit ihrer Leistung in Verzug geraten ist, wenn ihre Leistung unmöglich geworden ist oder wenn der *Zertifizierungsdienst* VR-Ident eine wesentliche Pflicht verletzt hat haftet sie für darauf zurückzuführende Sach- und Vermögensschäden, mit deren Eintritt bei Vertragsabschluss vernünftigerweise zu rechnen war, bis zu dem Höchstbetrag von 2 500 EUR.
- Für die Korrektheit der Identitätsprüfung haftet der *Zertifizierungsdienst* VR-Ident nur im Rahmen der zur Verfügung stehenden Prüfungsmöglichkeiten. Schließlich bestätigt der *Zertifizierungsdienst* VR-Ident daher mit dem VR-Ident Zertifikat nur, dass jemand zum angegebenen Zeitpunkt die geforderten Identifikationsnachweise vorgelegt hat und die entsprechenden Angaben im VR-Ident Zertifikat darauf gestützt aufgenommen wurden.
- Bei Ausfall der Zertifikatsdatenbank haftet der *Zertifizierungsdienst* VR-Ident erst ab einer Ausfallzeit von mehr als vierundzwanzig Stunden für Schäden, die dem Kunden durch die fehlende Verfügbarkeit entstehen.
- Der *Zertifizierungsdienst* VR-Ident haftet nicht für Schäden, welche dadurch verursacht werden, dass Zertifikatsinhaber oder Zertifikatsprüfer die anwendbaren Bestimmungen nicht einhalten
- Die Haftung für alle übrigen Schäden ist ausgeschlossen, wobei die Haftung nach dem Produkthaftungsgesetz unberührt bleibt.

9.8.2. Haftung des Zertifikatseigentümers, Zertifikatsinhabers beziehungsweise Kunden

Der *Zertifikatseigentümer* haftet für Schäden, die dem *Zertifizierungsdienst* VR-Ident durch von ihm verursachte fehlerhafte Angaben in einem *Zertifikat* sowie durch Verletzung seiner aus Gesetz, Vertrag oder der vorliegenden *CP* (*Certificate Policy*) oder dem vorliegendem *CPS* (*Certification Practice Statement*) resultierenden Verpflichtungen entstehen.

9.9. Schadensersatz

Siehe Kapitel 9.8.1.

9.10. Gültigkeit des Richtliniendokuments

9.10.1. Gültigkeitszeitraum

Das vorliegende Dokument ist vom Tag seiner Veröffentlichung an gültig. Seine Gültigkeit endet mit der Einstellung des Zertifizieriungsdienstes (siehe Kapitel 5.8 (S. 33)).

9.10.2. Vorzeitiger Ablauf der Gültigkeit

Die Gültigkeit dieses Dokumentes endet vorzeitig mit der Veröffentlichung einer neuen Version.

9.10.3. Konsequenzen der Aufhebung

Nach Gültigkeitsablauf des vorliegenden Dokumentes sind die Teilnehmer dennoch für den Gültigkeitszeitraum des Zertifikats an die Bestimmungen dieses Dokumentes gebunden.

9.11. Individuelle Mitteilungen und Absprachen mit den Teilnehmern

Für individuelle Mitteilungen und Absprachen mit den Teilnehmern werden die jeweils gültigen Kontaktinformationen (Anschrift, E-Mail, Telefon etc.) genutzt.

9.12. Änderungen beziehungsweise Ergänzungen des Dokuments

9.12.1. Verfahren für die Änderungen und Ergänzungen

Der *Zertifizierungsdienst* VR-Ident behält sich das Recht vor, dieses Dokument jederzeit zu ändern oder zu ergänzen.

Dies gilt insbesondere, um die Leistung zu verbessern oder an technische Entwicklungen anzupassen und wenn dies aufgrund von Veränderungen und/oder Ergänzungen notwendig erscheint. Die Revision und Veröffentlichung unterliegt der ausschließlichen Verantwortung *Zertifizierungsdienst* VR-Ident. Eine Revision erfolgt mindestens einmal jährlich.

9.12.2. Benachrichtigungsverfahren und Veröffentlichungsperioden

Bei Änderungen bezüglich sicherheitsrelevanter Aspekte oder sicherheitsrelevanter Verfahren hinsichtlich der Zertifikatsinhaber, wie beispielsweise Änderungen des Registrierungsablaufs, des Verzeichnis-, Widerrufs- und Sperrdienstes, der Kontaktinformationen oder der Haftung, wird der *Zertifizierungsdienst* VR-Ident die Zertifikatsinhaber per E-Mail oder durch die Veröffentlichung im Internet unter:

http://www.vr-ident.de

benachrichtigen. Der *Zertifizierungsdienst* VR-Ident beziehungsweise die *Registrierungsstelle* des *Zertifizierungsdienst* VR-Ident wird die Zertifikatsinhaber bei der Übermittlung der Änderung über die Konsequenzen der Änderung informieren.

Die Änderung tritt sechs Wochen, nachdem der *Zertifizierungsdienst* VR-Ident

- die Zertifikatsinhaber über die Änderung informiert hat und
- die Zertifikatsinhaber darauf hingewiesen hat, dass sie berechtigt ist, innerhalb des genannten Zeitraums der Änderung zu widersprechen, und dass die Änderung nach Ablauf der Frist für den Widerspruch wirksam wird, soweit der Zertifikatsinhaber keinen Widerspruch eingelegt hat, in Kraft.

Hinsichtlich sonstiger Änderungen, insbesondere der Verbesserung geringfügiger redaktioneller Versehen oder der Beifügung von Erläuterungen, kann eine Benachrichtigung der Zertifikatsinhaber unterbleiben.

9.12.3. Bedingungen für Änderungen der Objekt-Kennung (OID)

Die Entscheidung über die Zuweisung einer neuen OID ist Teil des Prozesses zur Aktualisierung der *CPS* (*Certification Practice Statement*). Bei Ergänzungen oder Modifikationen der *CPS* (*Certification Practice Statement*) entscheidet der *Zertifizierungsdienst* VR-Ident, ob sich daraus signifikante Änderungen der Sicherheit der *Zertifizierungsdienste*, der Rechte und Pflichten der Teilnehmer oder der Anwendbarkeit der Zertifikate ergeben. Falls dies der Fall ist, wird die Versionsnummer auf die nächste volle Nummer erhöht. In diesem Fall wird die OID des *CPS* (*Certification Practice Statement*) angepasst. Anderenfalls bleibt die OID unverändert.

9.13. Schiedsverfahren

Unstimmigkeiten zwischen dem Zertifizierungsdienst VR-Ident und Kunden sollen entsprechend den getroffenen vertraglichen Vereinbarungen gelöst werden. Andere Parteien können den Zertifizierungsdienst VR-Ident über die E-Mail Adresse IND_Zertifikatsverwaltung@fiduciagad.de erreichen.

9.14. Anwendbares Recht

Anwendbar ist ausschließlich deutsches Recht. Es gelten die Allgemeinen Geschäftsbedingungen der *Fiducia & GAD IT AG*.

9.15. Konformität mit anwendbarem Recht

Entfällt.

9.16. Weitere Regelungen

9.16.1. Vollständigkeit

Alle in diesem Dokument enthaltenen Regelungen gelten zwischen der *Zertifizierungsstelle* VR-Ident VR-Ident und deren Auftraggebern. Die Ausgabe einer neuen Version ersetzt alle vorherigen Versionen. Mündliche Vereinbarungen oder Nebenabreden bestehen nicht.

9.16.2. Abtretung der Rechte

Entfällt.

9.16.3. Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Dokumentes unwirksam sein oder Lücken enthalten, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Anstelle der unwirksamen Bestimmungen gilt diejenige wirksame Bestimmung als vereinbart, welche dem Sinn und Zweck der unwirksamen Bestimmung weitgehend entspricht. Im Falle von Lücken gilt dasjenige als vereinbart, was nach Sinn und Zweck dieses Dokumentes vernünftigerweise vereinbart worden wäre, hätte man die Angelegenheit von vornherein bedacht.

9.16.4. Rechtliche Auseinandersetzungen / Erfüllungsort

Rechtliche Auseinandersetzungen, die aus dem Betrieb der VR-Ident PKI herrühren, obliegen den Gesetzen der Bundesrepublik Deutschland. Erfüllungsort und ausschließlicher Gerichtsstand ist Münster.

9.16.5. Force Majeure

Entfällt.

9.17. Andere Regelungen

Entfällt.

10. Sonstige Bestimmungen

10.1. Schriftformgebot

Die jeweils aktuelle Schriftversion dieses Dokumentes ersetzt sämtliche vorhergehende Versionen. Mündliche Kundmachungen bestehen nicht.

10.2. Sprache

Für dieses Richtliniendokument, sowie rechtlich verbindliche Dokumente wie die Allgemeinen Geschäftsbedingungen, ist die deutsche Fassung dieser Dokumente maßgebend.

Anhang A. Referenzen

A.1. Literaturverzeichnis mit allgemeingültigen internationalen Dokumenten

[Nr.]	Dokument	Link
[01]	Common Criteria for Information Technology Security Evaluation. Version 2.1, August 1999.	part1.2003-12-31.pdf[1]
[02]	Common PKI Specifications for Interoperable Applications, T7 & TeleTrusT, Version 2.0, 20.1.2009.	common-pki-v20-spezifikation.html[2]
[03]	FIPS PUB 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology (NIST), 2001.	http://csrc.nist.gov/publications/fips/fips140-2/[3]
[04]	PKCS#10: Certification Request Syntax Standard. RSA Laboratories. Version 1.7. 2000.	http://tools.ietf.org/html/rfc2986
[05]	RFC 6960, X.509 Internet Public Key Infrastructure – Online certificate Status Protocol – OCSP. S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, 2013.	http://www.ietf.org/rfc/rfc6960.txt[4]
[06]	RFC 3647, Internet X.509 Public Key Infrastructure certificate Policy and Certification Practices Framework. S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu, 2003 (obsoletes RFC 2527)	http://www.ietf.org/rfc/rfc3647.txt
[07]	RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.	http://www.ietf.org/rfc/rfc5280.txt
[08]	ETSI EN 319401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers, European Telecommunications Standards Institute (ETSI), Version 2.2.0, 08/2017	http://www.etsi.org/deliver/etsi_en/319400_319499/319401/
[09]	ETSI EN 319411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, European Telecommunications Standards Institute (ETSI), Version 1.2.0, 08/2017	http://www.etsi.org/deliver/etsi_en/319400_319499/31941101/
[10]	ETSI TS 102 176-1: Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms; Version 2.1.1, 07/2011	http://www.etsi.org/deliver/etsi_ts/102100_102199/10217601
[11]	ITU-T Recommendation X.501 (2005), Information technology - Open Systems Interconnection - The Directory: Models, 2008.	http://www.itu.int/rec/T-REC-X.501/en
[12]	ITU-T Recommendation X.509 (2005), Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, 2005.	http://www.itu.int/rec/T-REC-X.509/en
[13]	CA-Certificate Policy for Cybertrust Certification Services	http://cybertrust.omniroot.com/repository/
[14]	WebTrust Principles and Criteria for Certification Authorities Version 2.1	http://www.webtrust.org/principles-and-criteria/docs/item85228.pdf
[15]	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, V.1.5.1	https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.5.1.pdf
[16]	Guidelines For The Issuance And Management Of Extended Validation Certificates Version 1.6.5	https://cabforum.org/wp-content/uploads/EV-V1_6_5.pdf
[17]	WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL, Version 1.6	http://www.webtrust.org/principles-and-criteria/docs/item83989.pdf
[18]	Mozilla CA Certificate Inclusion Policy (Version 2.1)	http://www.mozilla.org/projects/security/certs/policy/InclusionPolicy.html
[19]	"QuoVadis Root Certification Authority Certificate Policy/Certification Practice Statement", Version 4.21	https://www.quovadisglobal.com/QVRepository.aspx

[1] http://www.commoncriteriaportal.org/files//ccfiles/part1.2003-12-31.pdf
[2] http://www.t7ev.org/themen/entwickler/common-pki-v20-spezifikation.html
[3] http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
[4] http://www.ietf.org/rfc/rfc2560.txt

A.2. Literaturverzeichnis mit VR-Ident Dokumenten

[Nr.]	Dokument	Link
[01]	Certificate Policy (CP) für VR-Ident privat-Zertifikate	http://www.vr-ident.de
[02]	Certification Practice Statement (CPS) für VR-Ident privat-Zertifikate	http://www.vr-ident.de
[03]	Certification Practice Statement (CPS) für VR-Ident SSL-Zertifikate unter externer Root	http://www.vr-ident.de
[04]	Certificate Policy (CP) für VR-Ident Zertifikate (WebTrust)	http://www.vr-ident.de
[05]	Certification Practice Statement (CPS) für VR-Ident SSL-Zertifikate (WebTrust)	http://www.vr-ident.de
[06]	Certification Practice Statement (CPS) für VR-Ident mail-Zertifikate (WebTrust)	http://www.vr-ident.de
[07]	Certification Practice Statement (CPS) für VR-Ident privat-Zertifikate (WebTrust)	http://www.vr-ident.de
[08]	Certification Practice Statement (CPS) für allgemeine VR-Ident Zertifikate (WebTrust)	http://www.vr-ident.de
[09]	Sonderbedingungen für den *Zertifizierungsdienst* VR-Ident	http://www.vr-ident.de
[10]	Nutzungsbedingungen für VR-Ident mail-Zertifikate für Banken aus dem *Zertifizierungsdienst* VR-Ident der *Fiducia & GAD IT AG*	http://www.vr-ident.de
[11]	Nutzungsbedingungen für VR-Ident SMIME-Zertifikate aus dem *Zertifizierungsdienst* VR-Ident der *Fiducia & GAD IT AG*	http://www.vr-ident.de
[12]	Sonderbedingungen für den *Zertifizierungsdienst* VR-Ident für VR-Ident EV SSL-Zertifikate (WebTrust)	http://www.vr-ident.de
[13]	Certificate Policy" (CP)" für den *Zertifizierungsdienst* VR-Ident für VR-Ident interne Zertifikate	http://www.vr-ident.de
[14]	Certification Practice Statement" (CPS)" für den *Zertifizierungsdienst* VR-Ident für VR-Ident interne Zertifikate	http://www.vr-ident.de

Glossar

Aktivierungsdaten	Vertrauliche Daten, mit denen sich ein legitimierter Nutzer eines privaten Schlüssels gegenüber dem System, das den Schlüssel speichert, (beispielsweise einer Chipkarte oder einem HSM) authentisiert und somit den Schlüssel aktiviert. Üblicherweise werden PINs und Passwörter als Aktivierungsdaten verwendet.
Antragsteller	Antragsteller sind Individuen oder Organisationen, welche die Ausstellung von VR-Ident Zertifikaten bei dem Zertifizierungsdienst VR-Ident beantragen.
asymmetrische Kryptoverfahren	Kryptographische Verfahren, die auf zwei verschiedenen Schlüsseln basieren, wobei einer öffentlich und einer privat (geheim) ist. Dadurch ist es möglich, dass jemand mit dem öffentlichen Schlüssel eine Nachricht verschlüsselt, die nur der Besitzer des geheimen Schlüssels wieder entschlüsseln kann.
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 und dass die Daten wirklich von einer bestimmten Person stammen. Authentisierung bezeichnet dabei den Nachweis, Authentifizierung die Prüfung dieses Nachweises.
Authentisierung	Vorgang des Nachweises der Authentizität durch kryptographische Verfahren. Durch ein festgelegtes Verfahren wird festgestellt, ob jemand wirklich derjenige ist, der er vorgibt zu sein und dass die Daten wirklich von einer bestimmten Person stammen. Authentisierung bezeichnet dabei den Nachweis, Authentifizierung die Prüfung dieses Nachweises.
Authentisierungs-zertifikat	Zertifikat zu einem Schlüsselpaar mit dem eine sichere Authentisierung durchgeführt werden kann.
Authentizität	Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit von Daten und deren Urheberschaft.
CA	Certification Authority – englischer Begriff für eine Zertifizierungsinstanz.
CC	Abkürzung für Common Criteria.
Certificate Policy	Gesamtheit der Regeln und Vorgaben, welche die Anwendbarkeit eines Zertifikatstyps festlegen.
Certificate Renewal	Die Ersetzung eines Zertifikates durch ein Zertifikat mit neuer Gültigkeitsdauer, aber für den gleichen öffentlichen Schlüssel und sonst unveränderten Inhaltsdaten. In RFC 3647 "Certificate Renewal" genannt.
Certification Practice Statement	Darlegung der Praktiken, die ein *Zertifizierungsdienst*eanbieter bei der Ausgabe der Zertifikate anwendet.
Common Criteria	Internationaler Standard zur Bewertung der Informationssicherheit von Produkten und Systemen. CC unterscheidet verschiedene Evaluation Assurance Levels (EAL), die festlegen, was und wie geprüft wird. Die Prüfung erfolgt immer gegen die Sicherheitsvorgaben oder ein Schutzprofil (Protection Profile).
CP	Abkürzung für Certificate Policy.
CPS	Abkürzung für Certification Practice Statement.

CRL	Certificate Revocation List – Sperrliste.
Distinguished Name	Namensform nach X.501. Ein DN besteht aus verschiedenen Attributen und entsprechenden Werten und soll eine Entität eindeutig kennzeichnen. Die wichtigsten Attribute in dieser Richtlinie sind CommonName (cn), Organization (o), Organizational Unit (ou) und Country (c).
DMZ	Demilitarisierte Zone – logische Zone eines Netzwerkes zwischen dem öffentlichen Netz und dem internen Netz.
DN	Abkürzung für Distinguished Name.
Fiducia & GAD IT AG	Die *Fiducia & GAD IT AG* mit Firmensitz in Münster und Karlsruhe ist IT-Dienstleister, Rechenzentrum und Softwarehaus für über 1100 Volks- und Raiffeisenbanken sowie mehrere Privat- und Spezialbanken. Eingebunden in die genossenschaftliche FinanzGruppe verfügt die *Fiducia & GAD IT AG* über besondere Stärke, vor allem hinsichtlich des Angebots von qualifizierten Bankdienstleistungen vor Ort. Die Kernkompetenzen liegen in der Entwicklung und dem Betrieb von modernen und zukunftsfähigen Core-Banking-Lösungen sowie in der Bereitstellung hochwertiger und sicherer Outsourcing-Services.
Fingerprints	Als Fingerprint eines Zertifikats bezeichnet man den über das gesamte Zertifikat berechneten Hashwert.
FIPS 140-2	US-amerikanische Standards zur Prüfung und Bewertung der Sicherheit kryptographischer Soft- und Hardware. FIPS 140-2 ist der Nachfolger von FIPS 140-1. Beide Standards unterscheiden 4 Levels, wobei Level 1 die geringsten und Level 4 die höchsten Anforderungen an die Sicherheit stellt. Die Standards und ihre Levels sind weitestgehend vergleichbar.
Hardware-Sicherheitsmodul	Geräte zur sicheren Speicherung und Anwendung kryptographischer Schlüssel. Im Unterschied zu Chipkarten besitzen Hardware-Sicherheitsmodule (HSM) meist eine eigene Stromversorgung und implementieren oft aufwendige Sicherheitsmechanismen wie ein sicheres Key-Backup von Schlüsseln, die Protokollierung sicherheitsrelevanter Ereignisse oder ein rollenbasiertes Zugriffskonzept.
Hashwert	Mit Hilfe einer Hashfunktion, wird aus beliebigen Daten ein (praktisch) eindeutiger String konstanter Länge berechnet, der als Prüfsumme verwendet werden kann. Dieser String wird als Hashwert oder auch Fingerprint bezeichnet.
HSM	Abkürzung für Hardware Sicherheitsmodul .
HTTP	Hypertext Transfer Protocol – besonders im Internet verbreitetes Kommunikationsprotokoll.
LDAP	Lightweight Directory Access Protocol – Von der IETF standardisiertes Protokoll zum Zugriff auf Verzeichnisdienste.
Modifizierung eines Zertifikats	Die Ersetzung eines Zertifikates durch ein Zertifikat, bei dem (auch) andere Inhaltsdaten als der öffentliche Schlüssel geändert wurden. In RFC 3647 "certificate modification" genannt.
Object Identifier	Weltweit eindeutiger, hierarchisch ausgebauter, numerischer Bezeichner.
OCSP	Online Certificate Status Protocol – Von der IETF standardisiertes Protokoll zur Online-Abfrage von Statusinformationen von Zertifikaten.

OCSP-Responder	Server, der die Online-Abfrage von Statusinformationen von Zertifikaten unterstützt.. Siehe auch OCSP.
öffentlichen Schlüssel	Der öffentliche Schlüssel ist der nicht-geheime Teil eines Schlüsselpaares bei asymmetrischen Schlüsselpaaren.
PIN	Personal Identification Number – Geheimzahl zur Authentisierung eines Individuums beispielsweise gegenüber einer Chipkarte.
PKCS	Public Key Cryptography Standard – Standard für Kryptographische Verfahren, Datenformate und Schnittstellen in einer PKI.
PKI	Public Key Infrastruktur – technisches Umfeld für den Einsatz asymmetrischer Kryptoverfahren. Eine PKI basiert üblicherweise auf Zertifikaten und einer Zertifizierungshierarchie. Wichtige Komponenten einer PKI sind daher die Zertifizierungsinstanzen, Registrierungsinstanzen und Verzeichnisdienste. Darüber hinaus umfasst die PKI aber auch die Teilnehmer (Anwender), dezentrale Komponenten wie beispielsweise Client-Komponenten zur Speicherung und Anwendung der Schlüssel und Zertifikate sowie umfassende technische und organisatorische Prozesse.
privaten Schlüssel	Der private Schlüssel ist der geheime Teil eines Schlüsselpaares bei asymmetrischen Schlüsselpaaren.
RA	Registration Authority – englischer Begriff für eine Registrierungsstelle.
Registration Authority	Englischer Begriff für eine Registrierungsstelle.
Registrierungsstelle	Stelle eines Zertifizierungsdienstes, welche die Anträge zur Ausstellung oder Sperrung von Zertifikaten erfasst und die Antragsteller identifiziert werden.
RFC	Request for Comment – Dokumententyp der Internet Engineering Task Force (IETF), in der diese Standards vorschlägt und veröffentlicht.
Rollenträger	Mitarbeiter, die im Zertifizierungsdienst VR-Ident beschäftigt sind. Es werden Zuverlässigkeitsprüfungen durchgeführt. Rollenträger die sicherheitskritische Aufgaben durchführen, haben bei der Ernennung zum Rollenträger ein Führungszeugnis vorgelegt.
Root-CA	Oberste Zertifizierungsinstanz einer Zertifizierungshierarchie. Das Zertifikat der Root-CA wird von ihr selbst signiert und muss den Teilnehmern der PKI auf eine vertrauenswürdige Weise (beispielsweise offline) zugänglich gemacht werden. Man nennt diese Instanz auch "Wurzel-Zertifizierungsinstanz".
RSA	Asymmetrisches Kryptoverfahren für Verschlüsselung und digitale Signatur, benannt nach Rivest, Shamir, Adleman
Schlüssel- und Zertifikatserneuerung	Die Ersetzung eines Zertifikates durch ein Zertifikat mit neuer Gültigkeitsdauer und für einen neuen öffentlichen Schlüssel aber sonst unveränderten Inhaltsdaten. In RFC 3647 "certificate re-key" genannt.
SHA	Vom US-amerikanischen Standardisierungsinstitut normierte Hashfunktion. Der SHA-1 mit 160 Bit langen Hash- beziehungsweise Ausgabewerten gilt heute nicht mehr als sicher. Daher wird möglichst der Einsatz von Hashfunktionen der sogenannten SHA-2 Familie (SHA-256, SHA-384 und SHA-512 - wobei die angefügte Zahl jeweils die Länge des Hash- beziehungsweise des Ausgabewerts in bit angibt) empfohlen.

Sperrdienst	Dienst innerhalb der Zertifizierungsdienste über den Zertifikate gesperrt werden können.
Sperrliste	Liste, in der ein Anbieter eines Zertifizierungsdienstes die Sperrinformation der von ihm ausgestellten und noch nicht abgelaufenen Zertifikate veröffentlicht (siehe auch CRL).
Sperrmitarbeiter	Rolle der Person, welche die Sperrung von Zertifikaten in der PKI beziehungsweise der Karten im Bankensystem durchführt.
Sperrstatus	Status eines Zertifikates bezüglich Sperrung.
SSL	Secure Socket Layer, ein Protokoll, das die wechselseitige Authentifizierung zwischen einem Client und einem Server für den Aufbau einer verschlüsselten Verbindung ermöglicht. SSL läuft über TCP/IP und unter HTTP, LDAP, IMAP, NNTP und anderen Netzwerkprotokollen höherer Ebene.
SSL-Server-Zertifikate	Zertifikat eines Servers, das zum Schutz der Daten, die per http übertragen werden, dient. Durch das Zertifikat wird eine Verschlüsselung aktiviert, welche die übertragenen Daten schützt.
Vertrauende Dritte	Die Entität (Person oder Organisation), die sich auf ein von VR-Ident ausgestelltes VR-Ident privat-Zertifikat verlassen sollen. Ein Zertifikatsprüfer kann gleichzeitig auch Zertifikatsinhaber sein.
Verzeichnisdienst	In einer PKI: Dienst über den Zertifikate oder Informationen zur Zertifikaten (beispielsweise Sperrinformationen) oder der PKI abgerufen werden können. Der Zugriff auf den VR-Ident Verzeichnisdienst erfolgt über das LDAP Protokoll.
VR-Banken	Zu den VR-Banken zählen Volks- und Raiffeisenbanken sowie privat- und Spezialinstitute, die von der *Fiducia & GAD IT AG* betreut werden. In diesem Dokument werden als VR-Bank diejenigen dieser Banken bezeichnet, die an dem Downloadverfahren für VR-Ident privat Zertifikate teilnehmen.
VR-Ident Workflow Management	Lotus Notes basiertes Key Management Workflow Tool. Die Authentifizierung ist rollenorientiert und basiert auf der Lotus Notes ID. Die Besetzung der Rollen ist in Trusted Computing festgelegt.
Wildcard-Zertifikate	Wildcard-Zertifikate unterstützen eine beliebige Anzahl von Subdomains unterhalb einer Domain. Als "Platzhalter" für die Namen der Subdomains wird ein "*" verwendet. Das Wildcard-Zertifikat "*.fiduciagad.de" schützt beispielsweise alle Subdomains unterhalb der Domain fiduciagad.de, "*.agree21.fiduciagad.de" schützt alle Subdomains unter der Subdomain agree21.fiduciagad.de und so weiter. Theoretisch gibt es auch mehrstufige Wildcard-Zertifikate ("*.*.agree21.fiduciagad.de" oder *"*.test.*.fiduciagad.de"), hier sind allerdings Inkompatibilitäten bekannt, so dass deren Einsatz nicht empfohlen wird.
X.501	Von der ITU definierter Standard, der die Struktur von Verzeichnissen und entsprechende Namensformen zur Identifizierung der Objekte in Verzeichnissen festlegt.
X.509	Von der ITU definierter Standard, der unter anderem die heute überwiegend verwendeten Datenformate für Zertifikate und Sperrlisten definiert
Zertifikat	Eine elektronische Bescheinigung, mit der ein öffentlicher Signaturschlüssel dem Zertifikatseigentümer zugeordnet wird und dessen Identität bestätigt wird. Ein Zertifikat enthält Angaben zum Eigentümer, zum Aussteller und zur Nutzung des Zertifikates

	sowie den öffentlichen Schlüssel des Eigentümers. Außerdem enthält das Zertifikat eine digitale Signatur, welche die Authentizität und Integrität der im Zertifikat enthaltenen Daten sicherstellt. Eine Variante sind Attributzertifikate, die keinen öffentlichen Schlüssel des Eigentümers enthalten.
Zertifikatseigentümer	Entität, für die das Zertifikat ausgestellt wird. Der Zertifikatseigentümer ist im Zertifikat als "Subject" eingetragen.
Zertifizierungsdienst	Dienst, der Zertifikate ausstellt oder andere Dienstleistungen im Zusammenhang mit Zertifikaten erbringt, beispielsweise Verzeichnisdienste, Zeitstempeldienste, Schlüsselhinterlegungsdienste.
Zertifizierungshierarchie	Hierarchisch geordnete Struktur bestehend aus den Zertifizierungsinstanzen und den von ihnen ausgestellten Zertifikaten. Auf der untersten Hierarchiestufe stehen die Zertifikate der Endanwender. Unter jeder Zertifizierungsinstanz hängen an entsprechenden Ästen die Entitäten, für die sie Zertifikate ausstellen. Die oberste(n) Zertifizierungsinstanz(en) nennt man Root-CA(s) (Deutsch: Wurzel-CA).
Zertifizierungsstelle	Logische Einheit einer Zertifizierungsstelle zur Ausstellung (Signierung) von Zertifikaten. Jeder Zertifizierungsinstanz sind jeweils ein oder mehrere Schlüsselpaare zur Signierung der Zertifikate zugeordnet.