Certificate Policy (CP)

VR-Ident Zertifikate (WebTrust)

FIDUCIA GAD
ZUKUNFTSERFAHREN

IT-Partner der FinanzGruppe
Volksbanken Raiffeisenbanken

Certificate Policy (CP)

VR-Ident Zertifikate (WebTrust)

Version:	Version 3.02.04, Freigegeben
Zielgruppe:	Nutzer und Besitzer von VR-Ident Zertifikaten
Datum/Uhrzeit:	16.01.2019 / 09:46 Uhr

Gegenüber der vorherigen Ausgabe wurden folgende Änderungen vorgenommen:

Nummer	Datum	Inhalt / Änderungen
3.2.2	07.02.2018	Kapitel 0.0.0:
3.2.4	14.12.2018	Hinweis wegen Beendigung EV und OV eingefügt

Zusammenfassung
Das vorliegende Dokument ist eine "Certificate Policy" (CP) für den Zertifizierungsdienst VR-Ident für VR-Ident Zertifikate (WebTrust).

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

Inhaltsverzeichnis

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.

Extended Validation (*EV*) *SSL-Server-Zertifikate* werden von dem *Zertifizierungsdienst* VR-Ident unter dem Namen "VR-Ident EV SSL-Zertifikat" angeboten.

Die "VR IDENT EV SSL CA" wird unterhalb einer Root CA eines externen Extended Validation Partners angelegt. Da zum Zeitpunkt der Erstellung dieses Dokumentes dieser Partner noch nicht feststeht wird an des Stellen des Dokumentes, wo unbekannte Parameter verwendet werden "ExEVPartner" als Platzhalter für das Unternehmen und Root-CA Name des ExEVPartner als Platzhalter für den Namen der CA verwendet.

Die *SMIME-Zertifikat*e werden unter den folgenden Produktnamen angeboten:

- "VR-Ident mail-Zertifikate": *SMIME-Zertifikat*e für *VR-Banken* und Spezialinstitute der *Fiducia & GAD IT AG* sowie die *Fiducia & GAD IT AG* selbst
- "VR-Ident SMIME-Zertifikate": *SMIME-Zertifikat*e für Konzerntöchter der *Fiducia & GAD IT AG* und Verbundpartner

Soweit eine Unterscheidung der obigen Produkttypen nicht erforderlich ist, wird im weiteren Verlauf des Dokuments der Einfachheit halber der Name "VR-Ident mail-Zertifikat" verwendet.

Die Zertifikate werden für folgende Schlüssel der VR-BankCards und VR-Networld-Cards (im Folgenden kurz mit "*VR-Bankkarten*" bezeichnet) ausgestellt:

- *CSA*
- *DS*
- *KE*

Diese Zertifikate werden im Folgenden unter dem Begriff "VR-Ident privat-Zertifikate" zusammengefasst.

Die allgemeinen Zertifikate werden unter den folgenden Produktnamen angeboten:

- momentan werden keine weiteren allgemeinen VR-Ident Zertifikate angeboten

Das vorliegende Dokument ist eine "*Certificate Policy*" (*CP*) für den *Zertifizierungsdienst* VR-Ident für VR-Ident Zertifikate, die unterhalb der durch einen externen Auditor geprüften und zertifizierten *Root-CA* erstellt wurden.

Inhalt und Aufbau der dieser *CP* (*Certificate Policy*) orientieren sich an der *RFC* 3647. In den einzelnen "*Certification Practice Statement*" (*CPS*) der Sub-CA sind detaillierte Informationen zur Umsetzung der Vorgaben des vorliegenden Dokuments enthalten (siehe Anhang mit VR-Ident Referenzen).

VR-Ident Zertifikate, die unterhalb der externen *Root-CA* "QuoVadis Root CA 2" erstellt wurden, unterliegen zusätzlich den Richtlinien der "CA-Certificate Policy des ExEVPartner ergänzen" (siehe Anhang mit allgemeinen Referenzen).

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: 1.3.6.1.4.1.17696.4.1.1.9.3.2

Die Dokumentenbezeichnung für die vorliegende CP lautet: "VR-Ident Certificate Policy (CP) für VR-Ident Zertifikate (WebTrust)".

Folgende *CPS* (*Certification Practice Statement*) sind auf diesem Dokument aufgebaut:

- "VR-Ident Certification Practice Statement (CPS) für VR-Ident SSL-Zertifikate (WebTrust)" mit folgender ASN.1 *Object Identifier* (OID): 1.3.6.1.4.1.17696.4.1.1.5.3.2
- "VR-Ident Certification Practice Statement (CPS) für VR-Ident EV SSL-Zertifikate" mit folgender ASN.1 *Object Identifier* (OID): 1.3.6.1.4.1.17696.4.1.1.10.3.2
- "VR-Ident Certification Practice Statement (CPS) für VR-Ident mail-Zertifikate (WebTrust)" mit folgender ASN.1 *Object Identifier* (OID): 1.3.6.1.4.1.17696.4.1.1.6.3
- "VR-Ident Certification Practice Statement (CPS) für VR-Ident privat-Zertifikate"e (WebTrust)" mit folgender ASN.1 *Object Identifier* (OID): 1.3.6.1.4.1.17696.4.1.1.7.3
- "VR-Ident Certification Practice Statement (CPS) für allgemeine VR-Ident Zertifikate (WebTrust)" mit folgender ASN.1 *Object Identifier* (OID): 1.3.6.1.4.1.17696.4.1.1.8.3

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.

Details zur *Zertifizierungshierarchie* der *Zertifizierungsstelle* VR-Ident, die durch ihre Zertifizierungsinstanzen und die von ihnen ausgestellten Zertifikate definiert wird, sind in den jeweiligen CPS (Certification Practice Statement) für VR-Ident Zertifikate (*WebTrust*) festgelegt (siehe Anhang mit VR-Ident Referenzen).

1.3.2. Registrierungsinstanzen

Die *Registrierungsstelle* für VR-Ident SSL-Zertifikate und für allgemeine VR-Ident Zertifikate wird durch VR-Ident dargestellt. VR-Ident registriert und identifiziert die Zertifikatsbewerber, nimmt Zertifizierungsanträge entgegen und veranlasst unter bestimmten Umständen die Sperrung der Zertifikate.

Die *Registrierungsstelle* für VR-Ident mail-Zertifikate wird durch die Vertragspartner von VR-Ident und VR-Ident selbst dargestellt. Der Vertragspartner identifiziert die Zertifikatsbewerber und veranlasst die Registrierung. VR-Ident nimmt Zertifizierungsanträge entgegen. Der Vertragspartner oder VR-Ident veranlasst unter bestimmten Umständen die Sperrung der Zertifikate.

Die *Registrierungsstelle* für VR-Ident privat-Zertifikate wird durch die VR-Bank Filialen und Systeme der *VR-Banken* dargestellt. Diese registrieren und identifizieren die Zertifikatsbewerber, nehmen Zertifizierungsanträge entgegen und veranlassen unter bestimmten Umständen die Sperrung der Zertifikate.

Details sind in dem jeweiligen CPS (Certification Practice Statement) für VR-Ident Zertifikate (WebTrust) festgelegt (Anhang mit VR-Ident Referenzen).

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.

Bei der Anforderung von VR-Ident EV SSL-Zertifikaten können folgende Rollen besetzt werden:

- Auftraggeber

Entität, für die ein Zertifikat beantragt wird. Diese erteilt den Auftrag zur Zertifikatsbeantragung oder bestimmt Repräsentanten, die diese Aufgaben übernehmen.

- Auftraggebervertreter:
  Der Auftraggebervertreter ist eine kombinierte Rolle, die folgende Rollen umfasst:
  - Antragsteller (Certificate Requester)
    Der Antragsteller kann ein Mitarbeiter des Auftraggebers oder auch ein Dritter sein, der vom Auftraggeber dazu berechtigt wurde, Zertifikate im Namen der Firma oder Organisation zu beantragen.
  - Bestätiger des Antrags (Certificate Approver)
    Der Bestätiger kann der Auftraggeber, Mitarbeiter des Auftraggebers oder eine vom Auftraggeber berechtigte Person sein, die berechtigt ist als Antragsteller zu agieren oder Dritte dazu zu berechtigen als Antragsteller zu agieren. Der Bestätiger des Antrags muss sowohl dazu berechtigt sein den Zertifikatsantrag als auch die Sonderbedingungen für den *Zertifizierungsdienst* VR-Ident für VR-Ident EV SSL-Zertifikate (WebTrust) gegenüber dem *Zertifizierungsdienst*eanbieter zu bestätigen.
  - Vertragsunterzeichner (Contract Signer)
    Der Vertragsunterzeichner kann der Auftraggeber, ein Mitarbeiter des Auftraggebers oder eine vom Auftraggeber berechtigter Dritter sein, der im Namen des Auftraggebers sowohl den Zertifikatsantrag als auch die Sonderbedingungen für den *Zertifizierungsdienst* VR-Ident für VR-Ident EV SSL-Zertifikate (WebTrust) gegenüber dem *Zertifizierungsdienst*eanbieter unterschreibt.

    Ist der Auftraggeber die *Fiducia & GAD IT AG*, wird die Zeichnungberechtigung des Vertragsunterzeichners aufgrund des Eintrags in der Mitarbeiter Informationsdatenbank (mindestens "HANDL.V.(I.V.)") festgestellt, ansonsten muss der Vertragsunterzeichner im entsprechenden Register eingetragen sein.
- Repräsentant des Auftraggebers (Applicant Representative):
  Der Repräsentant des Auftragsgebers kann der Auftraggeber, ein Mitarbeiter des Auftraggebers oder eine Dritte Person sein, die berechtigt ist die Nutzungsbedingungen im Namen des Antragstellers zur Kenntnis zu nehmen und anzuerkennen.

In dem Dokument werden alle diese Rollen mit Antragsteller bezeichnet, wenn eine Unterscheidung notwendig ist, wird das explizit erwähnt.

Auftraggeber für VR-Ident mail-Zertifikate sind juristische Personen, welche die Ausstellung von VR-Ident mail-Zertifikaten durch den *Zertifizierungsdienst* VR-Ident beantragen. Der *Zertifizierungsdienst* VR-Ident stellt VR-Ident mail-Zertifikate an natürliche Personen (Mitarbeiter des Auftraggebers) sowie für Sammelpostfächer aus.

Auftraggeber für VR-Ident privat-Zertifikate sind ausschließlich natürliche Personen (Kunden der VR-Banken), die im Besitz einer VR-Bankkarte sind und die Ausstellung eines VR-Ident privat-Zertifikats durch den *Zertifizierungsdienst* VR-Ident beantragen.

Auftraggeber für allgemeine VR-Ident Zertifikate sind abhängig vom jeweiligen Zertifikatstyp.

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.

Zertifikatseigentümer von VR-Ident mail-Zertifikaten ist die Entität, für die das *Zertifikat* ausgestellt wird. Der *Zertifikatseigentümer* ist im *Zertifikat* als "Subject" eingetragen. Der *Zertifikatseigentümer* ist Mitarbeiter des Auftraggebers.

Zertifikatseigentümer von VR-Ident privat-Zertifikaten sind die Inhaber von *VR-Bankkarten*, für die VR-Ident privat-Zertifikate ausgestellt worden sind. Der *Zertifikatseigentümer* ist im *Zertifikat* als "Subject" eingetragen.

Zertifikatseigentümer für allgemeine VR-Ident Zertifikate sind abhängig vom jeweiligen Zertifikatstyp.

1.3.4. Vertrauende Dritte

Vertrauende Dritte im Sinne dieser *CP* (*Certificate Policy*) sind alle Personen und Systeme, die VR-Ident Zertifikate nutzen, um mit deren Inhabern sicher zu kommunizieren beziehungsweise diese Zertifikate nutzen, um die Gültigkeit einer elektronischen Signatur der Inhaber zu verifizieren.

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.

Bei der Nutzung der VR-Ident mail-Zertifikate und Schlüsselpaare muss der *Zertifikatseigentümer* seine in den "Sonderbedingungen für den *Zertifizierungsdienst* VR-Ident" definierten Pflichten erfüllen (siehe Anhang mit VR-Ident Referenzen).

VR-Ident mail-Zertifikate dürfen nur zur Verschlüsselung und Entschlüsselung sowie zur Signatur und Verifizierung der Signatur von E-Mail verwendet werden. Die sichere Kommunikation erfolgt mittels *SMIME* Sicherheitsstandard.

Bei der Nutzung der VR-Ident privat-Zertifikate und Schlüsselpaare muss der *Zertifikatseigentümer* seine in den "Sonderbedingungen für den *Zertifizierungsdienst* VR-Ident" (siehe Anhang mit VR-Ident Referenzen) definierten Pflichten erfüllen.

Die VR-Ident privat-Zertifikate beziehungsweise die zugehörigen Schlüssel dürfen zur *Authentisierung*, Erzeugung fortgeschrittener elektronischer Signaturen und zur Schlüssel- und Datenverschlüsselung eingesetzt werden. Die Nutzung der Schlüssel und Zertifikate muss der im *Zertifikat* spezifizierten Schlüsselverwendung (Key Usage) entsprechen.

Die *Fiducia & GAD IT AG* bietet die kryptographische Mittelware VR-Ident personal an, damit VR-Ident privat-Zertifikate in Standardanwendungen verwendet werden können. Mit dem Erwerb eines VR-Ident privat-Zertifikats hat der *Zertifikatseigentümer* eine Lizenz zur Nutzung der VR-Ident personal-Sofware erhalten. Weitere Details hierzu und eine Liste der unterstützten Anwendungen sind unter http://www.vr-ident.de veröffentlicht.

Allgemeine bzw. interne VR-Ident Zertifikate dürfen nur zum Zweck der hierfür bestimmten Anwendung verwendet werden.

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.

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

- Die Zertifikate beziehungsweise Schlüssel dürfen nicht in Anwendungen eingesetzt werden, die eine qualifizierte elektronische Signatur erfordern.
- Nach Ablauf der Gültigkeitsdauer oder Sperrung des VR-Ident privat-Zertifikats dürfen die zertifizierten Schlüssel nur noch zur Entschlüsselung verwendet werden.

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

- Die Zertifikate beziehungsweise Schlüssel dürfen nicht in Anwendungen eingesetzt werden, die eine qualifizierte elektronische Signatur erfordern.
- Nach Ablauf der Gültigkeitsdauer oder Sperrung des VR-Ident privat-Zertifikats dürfen die zertifizierten Schlüssel nur noch zur Entschlüsselung verwendet werden.

Für allgemeine VR-Ident Zertifikate gelten momentan keine weiteren Nutzungsbeschränkungen und -verbote:

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.

1.6. Definitionen und Abkürzungen

Definitionen und Abkürzungen siehe im Glossar.

[1] mailto:IND_Zertifikatsverwaltung@fiduciagad.de

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

- einen VR-Ident *Verzeichnisdienst*, der unter der Adresse ldap://www.vr-ident.de zu erreichen ist und
- einen *OCSP-Responder* zur Online-Abfrage des Zertifikatsstatus, der unter der Adresse http://ocsp.vr-ident.de/gtnocsp/OCSPResponder/<Name der CA> zu erreichen ist.

Der *Zertifizierungsdienst* VR-Ident erstellt zusätzlich *CRL* (Sperrlisten) mit Sperrinformationen von Zertifikaten, die unter den Adressen http://www.vr-ident.de/gtncrl/CRLResponder/<Name der CA> und ldap://www.vr-ident.de eingesehen werden können.

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

2.2. Veröffentlichung von Zertifikatsinformationen

Der *Zertifizierungsdienst* VR-Ident veröffentlicht alle VR-Ident Zertifikate (bei personengebundenen Zertifikaten, sofern der Inhaber der Veröffentlichung zugestimmt hat). Außerdem veröffentlicht der *Zertifizierungsdienst* VR-Ident Sperrinformationen für alle VR-Ident Zertifikate über Auskunftsdienste und *CRL* (Sperrlisten). Die Veröffentlichung der Zertifikate und Sperrinformationen erfolgt im Internet über standardisierte Kommunikationsprotokolle und Schnittstellen. Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

Der *Zertifizierungsdienst* VR-Ident veröffentlicht die Root-CA-Zertifikate und CA-Zertifikate und deren *Fingerprints* (*Hashwert*).

Das vorliegende Richtliniendokument wird im Internet veröffentlicht.

Der *Zertifizierungsdienst* VR-Ident veröffentlicht außerdem die "Allgemeine Geschäftsbedingungen für die Teilnehmer und *Vertrauende Dritte*", die unter http://www.fiduciagad.de herunter geladen werden können.

Für VR-Ident mail-Zertifikate gelten zusätzlich die Allgemeinen Geschäftsbedingungen der Vertragspartner von VR-Ident, ergänzt durch

- "Nutzungsbedingungen für VR-Ident mail-Zertifikate für Banken aus dem *Zertifizierungsdienst* VR-Ident der *Fiducia & GAD IT AG*" für Kunden von "VR-Ident mail-Zertifikaten" (*VR-Banken* und Spezialinstitute der *Fiducia & GAD IT AG* sowie die *Fiducia & GAD IT AG* selbst)
- "Nutzungsbedingungen für VR-Ident SMIME-Zertifikate aus dem *Zertifizierungsdienst* VR-Ident der *Fiducia & GAD IT AG*" für Kunden von "VR-Ident SMIME-Zertifikaten" (*Fiducia & GAD IT AG* Konzerntöchter und Verbundpartner)

In diesem Dokument werden diese Nutzungsbedingungen als "Sonderbedingungen für den *Zertifizierungsdienst* VR-Ident" bezeichnet (siehe Anhang mit VR-Ident Referenzen).

Für VR-Ident privat-Zertifikate gelten zusätzlich die Allgemeinen Geschäftsbedingungen der teilnehmenden VR-Banken, ergänzt durch die "Sonderbedingungen für den *Zertifizierungsdienst* VR-Ident" (siehe Anhang mit VR-Ident Referenzen).

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. 44) 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 Namen der *Zertifikatseigentümer* in den von der *Zertifizierungsdienst* VR-Ident ausgestellten VR-Ident Zertifikaten sind sogenannte DistinguishedNames nach *X.509* und im Attribut "Subject" des Zertifikats enthalten.

Details sind im jeweiligen CPS (Certification Practice Statement) für VR-Ident Zertifikate festgelegt (siehe Anhang mit VR-Ident Referenzen).

3.1.2. Anforderung an die Bedeutung von Namen

Namen in VR-Ident SSL-Zertifikaten müssen die zu schützende URL oder den zu schützenden Domainnamen eindeutig identifizieren. Bei der Namensvergabe wird daher der Name verwendet, der durch den Registrar der entsprechenden Top-Level Domain vergeben wurde. IP-Adresssen sind als CommonName und SubjectAltName nicht zugelassen.

Die Firma oder die Organisation, welche Inhaber des Zertifikats ist, ist eindeutig aufgrund der Eintragung in einem entsprechenden Register aufgrund des hier registrierten Namens und Sitzes erkennbar. Weiterhin wird hier das Bundesland des Sitzes zugeordnet. Die Abteilung der Verantwortlichen für das Zertifikat kann angegeben werden, ansonsten wird hier "VR-Ident" eingetragen.

Details sind im CPS (Certification Practice Statement) für VR-Ident SSL-Zertifikate beziehungsweise für VR-Ident EV SSL-Zertifikate festgelegt (siehe Anhang mit VR-Ident Referenzen).

Der Gerichtsstand der Firma oder die Organisation, welche Inhaber des Zertifikats ist, wird durch die eindeutige Angabe des Ortes, des Bundeslandes und des Landes des Gerichts angegeben.

Die eindeutige Registernummer unter dem die Firma oder die Organisation in dem entsprechenden Register registriert wurde wird mit in das Zertifikat aufgenommen.

Details sind im CPS (Certification Practice Statement) für VR-Ident EV SSL-Zertifikate festgelegt (siehe Anhang mit VR-Ident Referenzen).

Namen in VR-Ident mail-Zertifikaten müssen den *Zertifikatseigentümer* eindeutig identifizieren. Bei der Namensvergabe werden daher die gesetzlichen Namen der natürlichen Person oder dessen E-Mail Adresse verwendet, die von dem Vertragspartner von VR-Ident weitergegeben wurden.

E-Mail Adressen, die in VR-Ident mail-Zertifikaten eingetragen werden sollen, müssen zu einem E-Mail-Postfach des Zertifikatseigentümers gehören. Die Angabe von fremden E-Mail Adressen ist unzulässig.

Details sind im CPS (Certification Practice Statement) für VR-Ident mail-Zertifikate festgelegt (siehe Anhang mit VR-Ident Referenzen).

Namen in VR-Ident privat-Zertifikaten müssen den *Zertifikatseigentümer* eindeutig identifizieren. Bei der Namensvergabe werden daher die gesetzlichen Namen der natürlichen Person verwendet, die von der VR-Bank erfasst wurde.

E-Mail Adressen, die in VR-Ident privat-Zertifikaten eingetragen werden sollen, müssen zu einem E-Mail-Postfach des Zertifikatseigentümers gehören. Die Angabe von fremden E-Mail Adressen ist unzulässig.

Details sind im CPS (Certification Practice Statement) für VR-Ident privat-Zertifikate festgelegt (siehe Anhang mit VR-Ident Referenzen).

Der Zertifikatsinhaber von allgemeinen VR-Ident Zertifikaten muss über geeignete Namensbestandteile eindeutig identifizierbar sein.

Details sind im CPS (Certification Practice Statement) für VR-Ident mail-Zertifikate festgelegt (siehe Anhang mit VR-Ident Referenzen).

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, ', (,), +, -, ,, ., /, :, ?.

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

3.1.5. Eindeutigkeit von Namen

Der *Zertifizierungsdienst* VR-Ident soll durch geeignete Maßnahmen die Eindeutigkeit von Namen gewährleisten.

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.

Die Namen in den VR-Ident mail-Zertifikaten sind identisch mit dem Namen des Zertifikatsinhabers in seinem Personalausweis. Die Vertragspartner von VR-Ident müssen hierfür sorgen. Somit ist der Namenschutz gegeben.

Die Namen in den VR-Ident privat-Zertifikaten sind identisch mit dem Namen des Zertifikatsinhabers in seinem Personalausweis. Somit ist der Namenschutz gegeben.

Momentan werden keine weiteren allgemeinen VR-Ident Zertifikate angeboten.

3.2. Erstmalige Identitätsprüfung

3.2.1. Methode zum Besitznachweis des privaten Schlüssels

Der *Antragsteller* muss durch ein geeignetes kryptographisches Verfahren den Besitz des *privaten Schlüssel*s nachweisen. Hierzu werden geeignete *asymmetrische Kryptoverfahren* verwendet.

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

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.

- Der *Antragsteller* und der Zertifikatseigentümer werden anhand der bei der *Fiducia & GAD IT AG* vorhandenen Unterlagen oder anhand des eingereichten Registerauszugs überprüft
- Die Abteilungen des Antragstellers und des Zertifikatseigentümers werden anhand der bei der *Fiducia & GAD IT AG* vorhandenen Unterlagen überprüft
- Der Name der Firma oder der Organisation, sowie deren Sitz und das jeweilige Bundesland werden anhand des Eintrags in ein entsprechendes Register überprüft
- Eine Überprüfung der aktiven Geschäftstätigkeit des Antragstellers entfällt, da die *Fiducia & GAD IT AG* aktive Geschäftsbeziehungen zu diesen pflegt

Details sind im CPS (Certification Practice Statement) für VR-Ident SSL-Zertifikate festgelegt (siehe Anhang mit VR-Ident Referenzen).

- Der Gerichtsstand wird anhand eines aktuellen Registerauszugs überprüft.
- Die Registernummer wird anhand eines aktuellen Registerauszugs überprüft.
- Der Bestätiger des Antrags, der Vertragsunterzeichner und der Antragsteller (je nach Bedarf) werden überprüft.
- Bei der Anforderung von VR-Ident EV SSL-Zertifikaten muss der Bestätiger des Antrags die Zertifikatsanträge gegenüber dem *Zertifizierungsdienst* VR-Ident bestätigen.

Details sind im CPS (Certification Practice Statement) für VR-Ident EV SSL-Zertifikate festgelegt (siehe Anhang mit VR-Ident Referenzen).

Zwischen VR-Ident und dem Auftraggeber wird vereinbart, dass durch den Auftraggeber nur VR-Ident mail-Zertifikate für Domains ausgestellt werden dürfen, bei welcher der Auftraggeber durch den Registrar der entsprechenden Top-Level-Domain als Inhaber dieser registriert ist. Details hierzu sind in den "Sonderbedingungen für den *Zertifizierungsdienst* VR-Ident" festgelegt (siehe Anhang mit VR-Ident Referenzen).

Die *Authentisierung* von Organisationen entfällt für VR-Ident privat-Zertifikate, da diese ausschließlich an natürliche Personen ausgestellt werden.

Momentan werden keine weiteren allgemeinen VR-Ident Zertifikate angeboten.

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.

Zwischen VR-Ident und dem Auftraggeber wird vereinbart, dass VR-Ident mail-Zertifikate nur für E-Mail Adressen unterhalb vorher festgelegter für welche Top-Level Domains ausgestellt werden dürfen. Der Vertragspartner von VR-Ident ist dafür verantwortlich, dass die Zertifikatseigentümer, die aus dem Personalsystem des Auftraggebers übernommen werden, vorher hinreichend überprüft wurden. Details hierzu

sind in den "Sonderbedingungen für den *Zertifizierungsdienst* VR-Ident" festgelegt (siehe Anhang mit VR-Ident Referenzen).

Zur Feststellung der Identität des Zertifikatseigentümers von VR-Ident privat-Zertifikaten identifiziert und authentifiziert die VR-Bank die *Antragsteller*.

Die Identifizierung der *Antragsteller* von VR-Ident privat-Zertifikaten erfolgt nach den Vorgaben aus dem Geldwäschegesetz.

Die *Authentisierung* des Zertifikatseigentümers bei der Erstellung der VR-Ident privat-Zertifikate und der Übergabe seiner *öffentlichen Schlüssel* erfolgt durch seine VR-Bankkarte und geeignete kryptographische Verfahren.

Die in VR-Ident privat-Zertifikaten angegebenen E-Mail Adressen werden vom *Zertifizierungsdienst* VR-Ident durch das Zusenden der zur Zertifikatsausstellung erforderlichen Daten verifiziert.

Momentan werden keine weiteren allgemeinen VR-Ident Zertifikate angeboten.

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.

Zwischen VR-Ident und dem Auftraggeber wird vereinbart, dass der Vertragspartner von VR-Ident dafür verantwortlich ist , alle Informationen des Zertifikatseigentümers, die in das VR-Ident mail-Zertifikat übernommen werden sollen, verifiziert werden. Details hierzu sind in den "Sonderbedingungen für den *Zertifizierungsdienst* VR-Ident" festgelegt (siehe Anhang mit VR-Ident Referenzen).

Bei der Erstkontoeröffnung werden unter anderem alle Informationen des Zertifikatseigentümers, die in das VR-Ident privat-Zertifikat übernommen werden sollen, verifiziert. Der Kunde ist verpflichtet. Änderungen dieser Daten unverzüglich seiner VR-Bank mitzuteilen.

Momentan werden keine weiteren allgemeinen VR-Ident Zertifikate angeboten.

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.

Zwischen VR-Ident und dem Auftraggeber wird vereinbart, dass der Vertragspartner von VR-Ident dazu berechtigt ist , VR-Ident mail-Zertifikate für die Zertifikatseigentümer anzufordern. Details hierzu sind in den "Sonderbedingungen für den *Zertifizierungsdienst* VR-Ident" festgelegt (siehe Anhang mit VR-Ident Referenzen).

Die Prüfung der Handlungsvollmacht entfällt, da VR-Ident privat-Zertifikate ausschließlich für natürliche Personen ausgestellt werden.

Momentan werden keine weiteren allgemeinen VR-Ident Zertifikate angeboten.

3.2.6. Kriterien für Zusammenwirkung

Kriterien zur Zusammenwirkung entfallen.

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.

Das *Zertifikat* der "VR IDENT EV SSL CA 2016" wurde von der "QuoVadis Root CA 2" 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. 11)) 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.

Zwischen VR-Ident und dem Auftraggeber wird vereinbart, dass der Vertragspartner von VR-Ident auch bei einer turnusmäßigen Schlüsselerneuerung von VR-Ident mail-Zertifikaten dafür sorgen muss, dass die Identifizierung und *Authentifizierung* aller Kundendaten aktuell ist. Details hierzu sind in den "Sonderbedingungen für den *Zertifizierungsdienst* VR-Ident" festgelegt (siehe Anhang mit VR-Ident Referenzen).

Die Prozesse zur Identifizierung und *Authentifizierung* von VR-Ident privat-Zertifikaten bei Schlüsselerneuerung sind identisch zur initialen Identifizierung (siehe Kapitel 3.2.3 (S. 12)).

Momentan werden keine weiteren allgemeinen VR-Ident Zertifikate angeboten.

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. 11)) - 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.

Zwischen VR-Ident und dem Auftraggeber wird vereinbart, dass der Vertragspartner von VR-Ident auch bei einer Schlüsselerneuerung von VR-Ident mail-Zertifikaten nach einer Sperrung dafür sorgen muss, dass die Identifizierung und *Authentifizierung* aller Kundendaten aktuell ist. Details hierzu sind in den "Sonderbedingungen für den *Zertifizierungsdienst* VR-Ident" festgelegt (siehe Anhang mit VR-Ident Referenzen).

Die Prozesse zur Identifizierung und *Authentifizierung* von VR-Ident privat-Zertifikaten bei Schlüsselerneuerung nach einer Sperrung sind identisch zur initialen Identifizierung (siehe Kapitel 3.2.3 (S. 12)).

Momentan werden keine weiteren allgemeinen VR-Ident Zertifikate angeboten.

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.

Sperranträge für VR-Ident mail-Zertifikate werden automatisiert über Mail Gateways angefragt. Zwischen VR-Ident und dem Auftraggeber wird vereinbart, dass der Vertragspartner von VR-Ident nur berechtigte Sperranträge an VR-Ident übermitteln darf. Details hierzu sind in den "Sonderbedingungen für den *Zertifizierungsdienst* VR-Ident" festgelegt (siehe Anhang mit VR-Ident Referenzen).

Die *Authentifizierung* beim Sperrantrag von VR-Ident privat-Zertifikaten kann auf folgende Weisen erfolgen:

- Handschriftliche Unterschrift.
- Prüfung der Identität durch einen Kundenberater der VR-Bank.
- Festgelegte kryptographische Verfahren.

Details sind im CPS (Certification Practice Statement) für VR-Ident privat-Zertifikate festgelegt (siehe Anhang mit VR-Ident Referenzen).

Momentan werden keine weiteren allgemeinen VR-Ident Zertifikate angeboten.

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

Die Vertragspartner von VR-Ident können VR-Ident mail-Zertifikate für deren Mitarbeiter beantragen.

VR-Ident privat-Zertifikate können alle Personen beantragen, die im Besitz einer VR-BankCard oder VR-Networld-Card sind (in diesem Dokument kurz mit "VR-Bankkarte" bezeichnet).

Momentan werden keine weiteren allgemeinen VR-Ident Zertifikate angeboten.

4.1.2. Registrierungsprozess und Verantwortlichkeiten

VR-Ident SSL-Zertifikate können nur von Organisationen bei der Registrierungsstelle VR-Ident beantragt werden. Bei der Antragstellung muss angegeben werden, für welche Domain das VR-Ident SSL-Zertifikat ausgestellt werden sollen.

Es werden sowohl Erstanträge als auch Wiederholungsanträge für eine Erneuerung von VR-Ident SSL-Zertifikatn unterstützt.

VR-Ident EV SSL-Zertifikate müssen auf jeden Fall schriftlich beantragt werden.

Details sind im CPS (Certification Practice Statement) für VR-Ident SSL-Zertifikate beziehungsweise für VR-Ident EV SSL-Zertifikate festgelegt (siehe Anhang mit VR-Ident Referenzen).

Der Vertragspartner von VR-Ident kann automatisiert VR-Ident mail-Zertifikate über eine vereinbarte Schnittstelle beantragen. Der Auftraggeber ist verantwortlich dafür, dass nur korrekte Registrierungsdaten an VR-Ident übermittelt werden. Details hierzu sind in den "Sonderbedingungen für den *Zertifizierungsdienst* VR-Ident" festgelegt (siehe Anhang mit VR-Ident Referenzen).

VR-Ident privat-Zertifikate können nur persönlich von natürlichen Personen bei einer zuständigen *Registrierungsstelle* beantragt werden. Bei der Antragstellung muss angegeben werden, für welche Schlüssel (CSA, DS oder KE) Zertifikate ausgestellt werden sollen.

Es werden sowohl Erstanträge als auch Wiederholungsanträge für eine Erneuerung von Zertifikaten unterstützt.

Details sind im CPS (Certification Practice Statement) für VR-Ident privat-Zertifikate festgelegt (siehe Anhang mit VR-Ident Referenzen).

Momentan werden keine weiteren allgemeinen VR-Ident Zertifikate angeboten.

4.2. Antragsbearbeitung

4.2.1. Durchführung der Identifikation und Authentifizierung

Antragsteller von VR-Ident SSL-Zertifikaten werden zuverlässig nach einem dokumentierten Verfahren identifiziert und authentifiziert (siehe auch Kapitel 3.2.2 (S. 11)).

Details sind im CPS (Certification Practice Statement) für VR-Ident SSL-Zertifikate beziehungsweise für VR-Ident EV SSL-Zertifikate festgelegt (siehe Anhang mit VR-Ident Referenzen).

Der Vertragspartner von VR-Ident ist dafür verantwortlich, dass die Zertifikatseigentümer von VR-Ident mail-Zertifikaten, die aus dem Personalsystem des Auftraggebers übernommen werden, vorher hinreichend identifiziert und authentifiziert wurden. Details hierzu sind in den "Sonderbedingungen für den *Zertifizierungsdienst* VR-Ident" festgelegt (siehe Anhang mit VR-Ident Referenzen).

Antragsteller werden zuverlässig nach einem dokumentierten Verfahren identifiziert und authentifiziert (siehe auch Kapitel 3.2.3 (S. 12)).

Details sind im CPS (Certification Practice Statement) für VR-Ident privat-Zertifikate festgelegt (siehe Anhang mit VR-Ident Referenzen).

Momentan werden keine weiteren allgemeinen VR-Ident Zertifikate angeboten.

4.2.2. Annahme beziehungsweise Ablehnung von Zertifikatsanträgen

Voraussetzung für die Annahme eines Antrags ist eine erfolgreiche Identifizierung und *Authentifizierung* des Antragstellers und das Vorliegen der entsprechenden Vollmachten.

Eine Ablehnung des Antrags für VR-Ident privat-Zertifikate kann auch erfolgen, wenn der *Antragsteller* hinsichtlich seiner VR-Bankkarte nicht die technischen Voraussetzungen erfüllt. Außerdem kann die VR-Bank weitere Gründe für die Ablehnung eines Antrages festlegen.

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.

VR-Ident mail-Zertifikate werden unmittelbar nach Beendigung des Registrierungsprozesses und somit nach Eingang des Auftrags erstellt.

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

Momentan werden keine weiteren allgemeinen VR-Ident Zertifikate angeboten.

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.

Für folgende Produkte werden die CAA Records gemäß den Vorgaben der Baseline Requirements geprüft:

- VR-Ident SSL-Zertifikat
- VR-Ident EV SSL-Zertifikat

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.

Nach erfolgreicher Prüfung des Antrags für ein VR-Ident privat-Zertifikat durch die *RA* (*Registration Authority*) wird das VR-Ident privat-Zertifikat durch den *Zertifizierungsdienst* VR-Ident erstellt. Der *Antragsteller* kann den Zertifikats-Download auf seine VR-Bankkarte über ein Online-Interface im Online-Banking anstoßen. Dabei wird anhand der im Registrierungsdatensatz enthaltenen Daten das entsprechende *Zertifikat* erzeugt und auf die Karte des Antragstellers geschrieben.

Details sind im CPS (Certification Practice Statement) für VR-Ident privat-Zertifikate festgelegt (siehe Anhang mit VR-Ident Referenzen).

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.

Der Vertragspartner von VR-Ident informiert den Zertifikatseigentümer über die erfolgreiche Erstellung des VR-Ident mail-Zertifikats. Details hierzu sind in den "Sonderbedingungen für den *Zertifizierungsdienst* VR-Ident" festgelegt (siehe Anhang mit VR-Ident Referenzen).

Der *Antragsteller* erhält die VR-Ident privat-Zertifikate automatisch direkt nach der Generierung.

Momentan werden keine weiteren allgemeinen VR-Ident Zertifikate angeboten.

4.4. Zertifikatsakzeptanz

4.4.1. Annahme durch den Zertifikatsinhaber

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

4.4.2. Veröffentlichung der Zertifikate durch den Zertifizierungsdienst

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

Die Veröffentlichung von VR-Ident privat-Zertifikaten erfolgt nur, wenn der *Zertifikatseigentümer* dem zugestimmt hat.

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.

Der *Zertifikatseigentümer* von VR-Ident privat-Zertifikaten ist verpflichtet, seine Schlüsselpaare mit einer angemessenen Sorgfalt zu nutzen. Insbesondere muss er sicherstellen, dass seine Schlüssel nicht ohne sein Wissen und nur in der von ihm gewünschten Weise eingesetzt werden. Um dies zu erreichen, sollte er seine VR-Bankkarte und Schlüssel nur mit Software und auf Systemen nutzten, denen er vertraut und seine *PIN* nicht im System wie einem Passwort-Manager dauerhaft speichern. Außerdem dürfen *Zertifikatseigentümer* ihre Schlüssel nur in dafür zugelassenen Anwendungen einsetzen.

Für die Nutzung der VR-Ident privat-Zertifikate durch den Eigentümer gelten insbesondere die "Sonderbedingungen für den *Zertifizierungsdienst* VR-Ident" (siehe Anhang mit VR-Ident Referenzen).

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.

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

Das VR-Ident Root-CA-Zertifikat stellt den Vertrauensanker der VR-Ident *PKI* dar und sollte daher mit besonderer Sorgfalt behandelt werden. Insbesondere sollte es

- ausschließlich aus einer vertrauenswürdigen Quelle bezogen werden,
- vor dem Import ins System anhand des durch den *Zertifizierungsdienst* VR-Ident veröffentlichten Fingerabdruckes geprüft werden, und
- im System gegen Manipulationen geschützt sein.

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.

Die Erneuerung eines VR-Ident privat-Zertifikats wird nach Ausstellung einer Folgekarte unterstützt.

4.7.2. Wer kann eine Schlüssel- und Zertifikatserneuerung beantragen

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

4.7.3. Ablauf der Schlüssel- und Zertifikatserneuerung

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

4.7.4. Benachrichtigung des Zertifikatsinhabers nach Schlüssel- und Zertifikatserneuerung

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

4.7.5. Annahme der Schlüssel- und Zertifikatserneuerung

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

4.7.6. Veröffentlichung einer Zertifikatserneuerung durch den Zertifizierungsdienst

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

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. 30)).
- 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.

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

- Der Inhaber der Root CA "QuoVadis Root CA 2" kündigt die Sperrung der "VR IDENT EV SSL CA 2016" an.
- 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.

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

- Der *Zertifikatseigentümer* beantragt die Ausstellung eines Zertifikates beispielsweise mit geänderter E-Mail Adresse (Modifizierung des Zertifikates, siehe Kapitel 4.8 (S. 20)) und hat die Erstellung des neuen Zertifikats am Zertifikats-Download-Server angestoßen.
- Die VR-Bankkarte, welche die zum *Zertifikat* korrespondierenden Schlüssel enthält, wurde gesperrt.
- Die VR-Bank, welche die VR-Bankkarte des Zertifikatseigentümers ausgegeben hat, nimmt nicht mehr am *Zertifizierungsdienst* VR-Ident teil.

Zertifikatseigentümer müssen die Änderung von in einem VR-Ident privat-Zertifikat enthaltenen Angaben unverzüglich ihrer VR-Bank anzeigen.

Der *Zertifikatseigentümer***muss** eine Sperrung seines VR-Ident privat-Zertifikates in den folgenden Fällen veranlassen:

- Im Fall einer bekannten, vermuteten oder drohenden Kompromittierung der *privaten Schlüssel*. In diesem Fall muss er seine VR-Bankkarte unverzüglich sperren lassen.
- Falls der *Zertifikatseigentümer* den *privaten Schlüssel* nicht mehr nutzen kann, weil er die *PIN* vergessen hat oder wegen eines Defektes der Karte.

In diesen Fällen muss der *Zertifizierungsdienst* VR-Ident unverzüglich davon in Kenntnis gesetzt werden.

4.9.2. Sperrberechtigte

Die Sperrung von VR-Ident Zertifikaten kann von zur Sperrung berechtigten Personen oder Stellen beantragt werden. Berechtigt zur Sperrung sind:

- *Zertifizierungsdienst* VR-Ident.
- Der *Zertifikatseigentümer* oder ein von ihm bevollmächtigter Dritter.
- Die VR-Bank, welche die VR-Bankkarte ausgestellt hat(*Registrierungsstelle*) für VR-Ident privat-Zertifikate.

4.9.3. Verfahren zur Sperrung

Das Verfahren für die Sperrung von VR-Ident Zertifikaten ist im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen) beschrieben.

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.

Im Fall einer bekannten, vermuteten oder drohenden Kompromittierung der *privaten Schlüssel* muss die Sperrung der VR-Bankkarte oder der entsprechenden VR-Ident privat-Zertifikate unverzüglich beantragt werden.

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. 9) beschrieben.

4.9.6. Prüfung des Zertifikatsstatus durch vertrauende Dritte

Vertrauende Dritte dürfen sich nur dann auf den Inhalt eines VR-Ident Zertifikats verlassen, wenn sie zuvor den Zertifikatsstatus geprüft haben.

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. 9) 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 *Zertifizierungsdienst* VR-Ident bietet einen *OCSP-Responder* für die Abfrage des *Sperrstatus* von VR-Ident Zertifikaten mittels dem "Online Certificate Status Protocol" (*OCSP*) an. Über diesen können aktuelle Sperrinformationen abgefragt werden, die Sperrinformationen werden vom Auskunftsdienst zum Zeitpunkt der Abfrage ermittelt.

Außerdem werden regelmäßig *CRL* (Sperrlisten) nach *X.509* ausgestellt und veröffentlicht.

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

4.10.1. Betriebseigenschaften der Auskunftsdienste

Informationen zu den Betriebseigenschaften der Auskunftsdienste sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

4.10.2. Verfügbarkeit des Auskunftsdienstes

Informationen zu der Verfügbarkeit der Auskunftsdienste sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

4.10.3. Optionale Funktionen

Informationen zu den optionalen Funktionen der Auskunftsdienste sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

4.11. Austritt aus dem Zertifizierungsdienst

In folgenden Fällen endet das Vertragsverhältnis zwischen der VR-Bank und dem Eigentümer von VR-Ident privat-Zertifikaten:

- Bei Ablauf eines VR-Ident privat-Zertifikats ohne Zertifikatserneuerung. Dies ist der Fall, wenn eine VR-Bankkarte abläuft, aber die VR-Bank keine Folgekarte ausstellt.
- Im Fall einer Sperrung aller Zertifikate des Zertifikatseigentümers, sofern nicht unmittelbar danach neue Zertifikate ausgestellt werden (siehe Kapitel 4.7 (S. 20) und Kapitel 4.8 (S. 20)).

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

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

Die eingesetzten physikalischen Sicherheitsmaßnahmen sollen einen sehr hohen Schutz der kritischen Einrichtungen des *Zertifizierungsdienst* VR-Ident gewährleisten. Insbesondere sollen diese Maßnahmen sicherstellen, dass

- der Zutritt zu den Einrichtungen des *Zertifizierungsdienst*es und der physikalische Zugriff auf sensible Informationen und kritische Systeme nur durch dazu befugte Mitarbeiter möglich ist,
- kritische Informationen und Systeme nicht durch Katastrophen, Umwelteinflüsse oder Beeinträchtigungen der Infrastruktur (wie bei Feuer, Wasser, Staub, Überspannung, Stromausfall oder anderen Zwischenfällen) zerstört oder beeinträchtigt werden.

5.1.1. Lage und Aufbau des Standortes

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

5.1.2. Zutrittskontrolle

Geeignete Maßnahmen zur Zutrittskontrolle sollen einen hohen Schutz gegen unbefugtes Eindringen in die einzelnen Räume und unbefugten Zugriff auf die sicherheitskritischen Systeme und Daten gewährleisten. Der Zutritt zu den Räumen mit den IT-Systemen des *Zertifizierungsdienst* VR-Ident wird 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, soll mit durchgehender, unterbrechungsfreier Stromversorgung ausgestattet sein.

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

5.1.4. Schutz vor Wasserschäden

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

5.1.5. Brandschutz

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

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 muss 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. 25)).

5.2. Organisatorische Sicherheitsmaßnahmen

Die eingesetzten organisatorischen Sicherheitsmaßnahmen basieren auf einer Risikoanalyse und gewährleisten einen sehr hohen Sicherheitsstandard der *Zertifizierungsdienste*. Insbesondere sollen

- die Zuständigkeiten und Rollen für den Betrieb der *Zertifizierungsstelle* VR-Ident und das Sicherheitsmanagement klar geregelt sein,
- ein umfassendes Sicherheitsmanagement etabliert sein,
- kritische Prozesse und Prozeduren der *Zertifizierungsstelle* VR-Ident und des Sicherheitsmanagements dokumentiert und implementiert sein,
- schützenswerte Objekte und Informationen identifiziert und klassifiziert sein.

5.2.1. Sicherheitskritische Rollen

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

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 soll ebenfalls im Vier-Augen-Prinzip durchgeführt werden.

5.2.3. Identifizierung und Authentisierung von Rollen

Die Identifizierung und *Authentisierung* der Rollen in den Sicherheitsräumen im Rechenzentrum und bei den IT-Systemen soll mit Hilfe von Zutrittskarten sowie Benutzername und Passwort erfolgen. 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

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

5.3. Personelle Sicherheitsmaßnahmen

Die eingesetzten personellen Sicherheitsmaßnahmen müssen einen sehr hohen Sicherheitsstandard der *Zertifizierungsdienste* gewährleisten. Insbesondere müssen die Mitarbeiter des *Zertifizierungsdienstes*

- klar den definierten Rollen im *Zertifizierungsdienst* zugewiesen werden,
- für ihre Aufgaben ausreichend qualifiziert sein,
- mit den für ihre Aufgaben erforderlichen Dokumentation ausgestattet sein,

- auf ihre Zuverlässigkeit hin überprüft worden sein.

5.3.1. Anforderungen an Qualifikation und Erfahrung

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

5.3.2. Überprüfung der Vertrauenswürdigkeit

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

5.3.3. Anforderungen an Schulung und Fortbildung

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

5.3.4. Nachschulungsintervalle und –anforderungen

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

5.3.5. Arbeitsplatzrotation / Rollenumverteilung

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

5.3.6. Sanktionen bei unbefugten Handlungen

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

5.3.7. Vertragsbedingungen mit dem Personal

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

5.3.8. An das Personal ausgehändigte Dokumentation

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

5.4. Protokollierung sicherheitskritischer Ereignisse

Die Protokollierung sicherheitskritischer Ereignisse im Zusammenhang mit der Ausstellung und Verwaltung der Zertifikate basieren auf einer Risikoanalyse und gewährleisten einen sehr hohen Sicherheitsstandard der *Zertifizierungsdienst*e.

5.4.1. Zu protokollierende Ereignisse

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

- Ereignisse im Lebenszyklus der VR-Ident Zertifikate,
- Antragsdaten und Vollmachtsprüfung,
- Registrierungsdaten
- Ereignisse im Lebenszyklus der CA-Zertifikate und Schlüsselpaare,
- Sicherheitsrelevante Ereignisse,
- Ereignisse der Zutrittskontrollanlage,

Die Protokolleinträge sollen die folgenden Daten enthalten:

- Typ des Eintrags,
- Uhrzeit und Datum des Eintrags,
- Identifizierung der Stelle, die den Eintrag macht.

5.4.2. Häufigkeit der Auswertung von Protokolldaten

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

5.4.3. Aufbewahrungsfristen für Protokolldaten

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

5.4.4. Schutz der Protokolldaten

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

5.4.5. Sicherungsverfahren für Protokolldaten

Alle elektronischen Protokolldaten müssen regelmäßig gesichert werden.

5.4.6. Internes/externes Protokollierungssystem

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

5.4.7. Benachrichtigung des Auslösers eines Ereignisses

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

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.

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

5.5. Archivierung

Die Archivierung relevanter Daten soll in Übereinstimmung mit den gesetzlichen Regelungen erfolgen. Archivierte Daten sollen vor unbefugter Einsichtnahme, Manipulation und Vernichtung geschützt werden.

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. Die Aufbewahrungsfrist beträgt mindestens 7 Jahre.

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

5.5.4. Sicherung der archivierten Daten

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

5.5.5. Anforderungen an den Zeitstempel der archivierten Daten

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

5.5.6. Internes/externes Archivierungssystem

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

5.5.7. Verfahren zum Einholen und Verifizierung von Archivdaten

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

5.6. Schlüsselwechsel

Schlüsselpaare, die vom *Zertifizierungsdienst* VR-Ident für die Erbringung der *Zertifizierungsdienst*e verwendet werden, müssen rechtzeitig vor Ablauf ihrer Gültigkeit gewechselt werden. In diesem Fall wird das entsprechende *Zertifikat* nicht gesperrt.

Ein außerordentlicher Wechsel eines Schlüssels einer *Zertifizierungsstelle* VR-Ident wird durchgeführt, wenn die Sicherheit des privaten Schlüssels oder des korrespondierenden Zertifikates nicht mehr gewährleistet ist. In einem solchen Fall wird das korrespondierende *Zertifikat* gesperrt. Im Fall einer Sperrung eines CA-Zertifikates werden auch alle mit diesem CA-Schlüssel unmittelbar oder mittelbar ausgestellten Zertifikate gesperrt.

Die Sperrung eines Zertifikates der VR-Ident *Root-CA* wird von der *Zertifizierungsdienst* VR-Ident unverzüglich auf geeignete Weise bekannt gegeben.

Falls die VR-Ident CA-Zertifikate von einer externen *Root-CA* erzeugt wurden, werden die Schlüsselwechsel der *Root-CA* von dem jeweiligen Eigentümer durchgeführt, da dieser die *Root-CA* betreibt. Das gleiche gilt für außerordentliche Schlüsselwechsel dieser *Root-CA*.

5.7. Business Continuity Management und Incident Handling

Der *Zertifizierungsdienst* VR-Ident soll für die *Zertifizierungsdienst*e für VR-Ident Zertifikate angemessene Maßnahmen zur Aufrechterhaltung des Betriebes (Business Continuity Management) in Notfällen und zur Behandlung von Sicherheitsvorfällen (Incident Handling) implementieren.

5.7.1. Prozeduren zu Incident Handling und zu Notfällen

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

5.7.2. Prozeduren bei Kompromittierung von Ressourcen

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

5.7.3. Prozeduren bei Kompromittierung von CA-Schlüsseln

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

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 *Zertifizierungsdienste* einstellt, werden alle Beteiligten benachrichtigt.

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (Anhang mit VR-Ident Referenzen).

6. Technische Sicherheitsmaßnahmen

6.1. Erzeugung und Installation von Schlüsselpaaren

Schlüsselpaare, die vom *Zertifizierungsdienst* VR-Ident für die Erbringung der *Zertifizierungsdienste* verwendet werden, sollen im Rahmen festgelegter Prozeduren, unter Mitwirkung mehrerer berechtigter Mitarbeiter, in einer sicheren Umgebung in Hardware-Sicherheitsmodulen (*HSM*) erzeugt werden.

6.1.1. Erzeugung von Schlüsselpaaren

Die CA-Signaturschlüsselpaare und Schlüsselpaare der *OCSP-Responder* sollen in Hardware-Sicherheitsmodulen (*HSM*s) erzeugt werden, die nach *FIPS 140-2* mindestens nach Level 3 oder vergleichbaren Standards (siehe Anhang mit allgemeinen Referenzen) evaluiert sind. Die Schlüsselerzeugung soll gemäß der Key Ceremony Policy und nur durch qualifizierte und autorisierte *Rollenträger* unter Aufsicht eines qualifizierten Auditors erfolgen.

6.1.2. Übermittlung privater Schlüssel an den Zertifikatseigentümer

Sofern private Schlüssel von der Fiducia & GAD IT AG generiert werden, muss die Übermittlung dieser Schlüssel an den Zertifikatseigentümer durch kryptographische Methoden gesichert werden.

6.1.3. Übermittlung öffentlicher Schlüssel an den Zertifikatsaussteller

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

6.1.4. Übermittlung öffentlicher CA-Schlüssel an vertrauende Dritte

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

6.1.5. Schlüssellängen

Der *Zertifizierungsdienst* VR-Ident soll Schlüssellängen verwenden, die von den einschlägigen Standards empfohlen werden. Es dürfen keinesfalls Schlüssel verwendet werden, die als unsicher angesehen werden.

6.1.6. Erzeugung und Prüfung der Schlüsselparameter

Keinesfalls dürfen Schlüssel mit ungeeigneten Parametern verwendet werden. Geeignete Algorithmen können z.B. ETSI TS 102 176-1, Algorithms and Parameters for Secure Electronic Signatures (siehe Anhang mit allgemeinen Referenzen), entnommern werden.

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.

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

6.2. Schutz der privaten Schlüssels und der kryptographischen Module

Private Schlüssel der *CA* der *Zertifizierungsstelle* VR-Ident werden ausschließlich einer sicheren Umgebung in Hardware-Sicherheitsmodulen (*HSM*) gespeichert und verwendet. Der Zugriff auf diese Schlüssel erfolgt ausschließlich im Rahmen festgelegter Prozeduren, unter Mitwirkung mehrerer berechtigter Mitarbeiter, und in der vorgesehenen sicheren Umgebung. Zum Zweck einer hohen Verfügbarkeit können sichere

Schlüsselbackups angefertigt werden. Der Zugriff auf die *privaten Schlüssel*, insbesondere auch das Backup und Recovery, ist durch technische Maßnahmen geschützt, und erfolgt ausschließlich in sicheren Prozeduren unter Mitwirkung mehrerer berechtigter Mitarbeiter, und in Übereinstimmung mit den Vorgaben der Zertifizierung der *Hardware-Sicherheitsmodule* (*HSM*). Nicht mehr benötigte Schlüssel der *Zertifizierungsstelle* VR-Ident werden sicher deaktiviert.

Private Schlüssel für VR-Ident privat-Zertifikate können nicht aus der Chipkarte ausgelesen werden. Ihre Verwendung ist durch entsprechende *PIN* geschützt. Es wird kein Schlüsselbackup für die Schlüssel der Kunden durchgeführt.

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* (mindestens Level 3, siehe Anhang mit allgemeinen Referenzen) zertifiziert und müssen gemäß den Vorgaben der Zertifizierung betrieben werden.

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

6.2.2. Aufteilung der Kontrolle über private Schlüsseln auf mehrere Personen

Jeglicher administrativer oder operativer Zugriff auf die *Hardware-Sicherheitsmodul*e (*HSM*) muss im Vier-Augen-Prinzip durchgeführt werden. 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 dürfen nicht hinterlegt werden.

6.2.4. Backup privater Schlüssel

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

6.2.5. Archivierung privater Schlüssel

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

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 und nach den Vorgaben des Herstellers des HSM.

6.2.7. Speicherung privater Schlüssel

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

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.

6.2.9. Methoden zur Deaktivierung privater Schlüssel

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

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).

Private Schlüssel der *CA*, die abgelaufen beziehungsweise ungültig geworden sind und daher keine Verwendung mehr finden, werden vom HSM durch Eingabe eines Löschbefehls sicher gelöscht.

Falls der Dienst VR-Ident die privaten Schlüssel im Namen des Antragstellers generiert hat, werden diese sicher gelöscht, sobald der Antragsteller im Besitz des privaten Schlüssels ist.

6.2.11. Bewertung kryptographischer Module

Siehe Kapitel 6.2.1 (S. 32).

6.3. Weitere Aspekte des Schlüsselmanagements

Öffentliche Schlüssel sollen mit den Zertifikaten für eine angemessene Zeitdauer archiviert und werden.

6.3.1. Archivierung öffentlicher Schlüssel

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

6.3.2. Verwendungsdauern von Zertifikaten und Schlüsselpaaren

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

6.4. Aktivierungsdaten

Private Schlüssel der *CA* der *Zertifizierungsstelle* VR-Ident werden durch *Aktivierungsdaten* geschützt, die nur berechtigten Mitarbeitern bekannt sind.

6.4.1. Erzeugung und Installation von Aktivierungsdaten

Aktivierungsdaten für den Schutz der *privaten Schlüssel* der *CA* werden gemäß Kapitel 6.2.2 (S. 32) 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* muss protokolliert werden.

6.4.2. Schutz der Aktivierungsdaten

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

6.4.3. Weitere Aspekte von Aktivierungsdaten

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

6.5. Sicherheitsmaßnahmen für Computer

Der *Zertifizierungsdienst* VR-Ident implementiert umfassende Maßnahmen für die Sicherheit der im *Zertifizierungsdienst* verwendeten Computer. Diese gewährleisten:

- Schutz vor Viren und anderer bösartiger Software
- Schutz vor unbefugten logischen Zugriff auf die Systeme
- Regelmäßige Sicherung kritischer Daten
- Angemessene Ausfallsicherheit der kritischen Systeme
- Ausreichende Prüfung vor jeder Änderung der Konfiguration und Systemkomponenten
- Zeitnahe Erkennung von Störungen und Ausfällen

6.5.1. Spezielle Anforderungen zur Computersicherheit

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

6.5.2. Bewertung der Computersicherheit

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

6.6. Technische Kontrollen des Software-Lebenszyklus

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

6.6.1. Systementwicklungsmaßnahmen

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

6.6.2. Sicherheitsmanagement

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

6.6.3. Maßnahmen zur Kontrolle des Software-Lebenszyklus

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

6.7. Maßnahmen zur Netzwerksicherheit

Der *Zertifizierungsdienst* VR-Ident implementiert umfassende Maßnahmen für die Sicherheit ihrer für den *Zertifizierungsdienst* verwendeten Netzwerke. Diese umfassen:

- Implementierung getrennter Netzwerksegmente,

- Beschränkung der Netzwerkkommunikation auf das erforderliche Maß,
- Beschränkung von Zugriffen auf Netzwerkressourcen auf das notwendige Maß,
- Überwachung des Netzwerkverkehrs,
- Regelmäßige Überprüfung der Netzwerksicherheit

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

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

Der *Zertifizierungsdienst* VR-Ident stellt VR-Ident Zertifikate nach *X.509* in der Version 3 aus.

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

7.1.2. Zertifikatserweiterungen

Die verwendeten Zertifikatserweiterungen sind konform zu den Standards *X.509*, *RFC* 5280 und Common PKI. VR-Ident Zertifikate können die folgenden Erweiterungen beinhalten:

- AuthorityKeyIdentifier
- SubjectKeyIdentifier
- KeyUsage
- ExtendedKeyUsage
- CRLDistributionPoints
- AuthorityInfoAccess
- CertificatePolicies (optional)
- AuthorityInfoAccess (optional)
- SubjectAltNames (optional)
- BasicConstraints

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

7.1.3. Algorithmus Bezeichner (OID)

Die eingesetzten Algorithmen Bezeichner entsprechen den gängigen Standards.

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

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. 2) 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 von VR-Ident in *CRL* (Sperrlisten) verwendeten Erweiterungen sind konform zu den Standards *X.509*, *RFC* 5280 und Common *PKI* (siehe Anhang mit allgemeinen Referenzen).

CRL (Sperrlisten) und Sperrlisteneinträge haben die folgenden Erweiterungen:

- AuthorityKeyIdentifier
- CRLNumber
- DeltaCRLIndicator
- IssuingDistributionPoint
- ReasonCode
- CertificateIssuer

7.2.3. Weitere Eigenschaften der Sperrlisten

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

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

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

7.3.3. Weitere Eigenschaften der OCSP-Anfragen und Antworten

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

8. Revisionen und andere Bewertungen

Der *Zertifizierungsdienst* VR-Ident führt regelmäßig umfassende Audits zur Bewertung der Sicherheit der *Zertifizierungsdienste* durch.

Der Auditor ist ausreichend qualifiziert und von dem *Zertifizierungsdienste*anbieter *Fiducia & GAD IT AG* unabhängig.

Schwerwiegende Mängel, die bei einem Audit entdeckt werden, werden an das Management der *Fiducia & GAD IT AG* berichtet.

8.1. Häufigkeiten von Revisionen

Die Prozesse und Systeme zur Erstellung und zum Management der internen Zertifikate sollen mindestens einmal jährlich durch einen internen Auditor überprüft werden.

Ein Review dieses Dokuments erfolgt ebenfalls mindestens einmal jährlich durch einen internen Auditor.

Eine Prüfung durch externe Auditoren ist nicht erforderlich, weil die internen Zertifikate nur internen Zwecken dienen und keine Außenwirkung entfalten.

8.2. Identität und Qualifikation des Auditors

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

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-Sicherheitsmodule* (*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

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

8.7. Selbst-Audits

Details sind im entsprechenden CPS (Certification Practice Statement) aufgeführt (siehe Anhang mit VR-Ident Referenzen).

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.

Die *Fiducia & GAD IT AG* vereinbart mit dem Vertragspartner von VR-Ident einen Projektpreis.

Die Gebühren für die Ausstellung und Erneuerung von Zertifikaten ergeben sich aus dem Preisverzeichnis der VR-Bank.

Momentan werden keine weiteren allgemeinen VR-Ident Zertifikate angeboten.

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.

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. 42) 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.

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

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.

Die *VR-Banken* sind verpflichtet, gemäß dem vorliegenden Dokument zu handeln.

9.6.3. Verpflichtung des Zertifikatsinhabers

Der *Zertifikatseigentümer* ist verpflichtet, die VR-Ident Zertifikate sind nur bestimmungsgemäß und nicht missbräuchlich zu benutzen.

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

9.6.4. Verpflichtung vertrauender Dritter

Vertrauende Dritte sind dazu verpflichtet, Zertifikate und ihren Sperrstatus gemäß den in Kapitel 4.5.2 (S. 19) 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

Für die Korrektheit der Identitätsprüfung von VR-Ident privat-Zertifikaten haftet die VR-Bank nur im Rahmen der zur Verfügung stehenden Prüfungsmöglichkeiten.

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

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. 30)).

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.

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

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 benachrichtigen.

Details sind im jeweiligen CPS (Certification Practice Statement) festgelegt (siehe Anhang mit VR-Ident Referenzen).

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

Der *Zertifizierungsdienst* VR-Ident stellt VR-Ident mail-Zertifikate aus, mit denen fortgeschrittene elektronische Signaturen gemäß dem deutschen Signaturgesetz erzeugt werden können.

Der *Zertifizierungsdienst* VR-Ident stellt VR-Ident privat-Zertifikate aus, mit denen fortgeschrittene elektronische Signaturen gemäß dem deutschen Signaturgesetz erzeugt werden können.

9.16. Weitere Regelungen

9.16.1. Vollständigkeit

Alle in diesem Dokument enthaltenen Regelungen gelten zwischen der *Zertifizierungsstelle* VR-Ident VR-Ident, der VR-Bank 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.
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.
CP	Abkürzung für Certificate Policy.
CPS	Abkürzung für Certification Practice Statement.
CRL	Certificate Revocation List – Sperrliste.
CSA	CSA steht für „Client-Server-Authentisierung“, durch die beispielsweise die Authentisierung gegenüber Serveranwendungen technisch realisiert wird. Dieser Schlüssel wird während der Personalisierung der VR-Bankkarte generiert und dann während der Produktion auf die Karte gebracht.

DS	DS steht für „digitale Signatur“, durch welche die elektronische Signatur technisch realisiert ist. Dieser Schlüssel wird auf der VR-Bankkarte während der Produktion generiert.
EV	Siehe Extended Validation.
Extended Validation	Extended Validation SSL-Zertifikate (etwa "Zertifikate mit erweiterter Überprüfung") sind X.509 SSL-Zertifikate, deren Ausgabe an strengere Vergabekriterien gebunden ist. Dies bezieht sich vor allem auf eine detaillierte Überprüfung des Antragstellers durch die Zertifizierungsstelle.
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 .
KE	KE steht für „Key Encryption“, durch welche die Entschlüsselung von Verschlüsselungsschlüsseln technisch realisiert wird. Dieser Schlüssel wird während der Personalisierung der VR-Bankkarte generiert und dann während der Produktion auf die Karte gebracht.
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.
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".
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.
SMIME-Zertifikat	Zertifikat eines Individuums, das zum Schutz der Emails, die per SMTP übertragen werden, dient. Durch das Zertifikat kann eine Verschlüsselung aktiviert werden, welche die Vertraulichkeit der übertragenen Emails schützt oder es kann eine Signatur aktiviert.
Sperrliste	Liste, in der ein Anbieter eines Zertifizierungsdienstes die Sperrinformation der von ihm ausgestellten und noch nicht abgelaufenen Zertifikate veröffentlicht (siehe auch CRL).

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-Bankkarten	Kurzbezeichnung für VR-BankCards und VR-Networld-Cards. Die VR-Bankkarten werden im Vorfeld durch den Kartenherausgeber (DG VERLAG) personalisiert.
WebTrust	WebTrust wurde als weltweit anerkannter Standard durch das American Institute of Certified Public Accountants (AICPA) und Canadian Institute of Chartered Accountants (CICA) für Zertifizierungsdienstanbieter geschaffen, um höchstmögliche Standards und Qualität international zu sichern. Bei der *Fiducia & GAD IT AG* sind unter dem Begriff "WebTrust" folgende Anforderungen zusammengefasst: • "Trust Service Principles and Criteria for Certification Authorities" (Webtrust.org): Stellen allgemeine Anforderungen zur WebTrust Zertifizierung • "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (cabforum.org): Stellen spezielle (technische) Anforderungen an eine CA • "Mozilla CA Certificate Policy" (mozilla.org): Beschreibt die Pflichten der Zertifizierungsdienstanbieter für die Aufnahme ihrer Stammzertifikate in Mozilla Produkte
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.

Zertifizierungs-dienst	Dienst, der Zertifikate ausstellt oder andere Dienstleistungen im Zusammenhang mit Zertifikaten erbringt, beispielsweise Verzeichnisdienste, Zeitstempeldienste, Schlüsselhinterlegungsdienste.
Zertifizierungshier-archie	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).
Zertifizierungsstel-le	Logische Einheit einer Zertifizierungsstelle zur Ausstellung (Signierung) von Zertifikaten. Jeder Zertifizierungsinstanz sind jeweils ein oder mehrere Schlüsselpaare zur Signierung der Zertifikate zugeordnet.