Certification Practice Statement (CPS)

VR-Ident privat-Zertifikate

GAD
IT für Banken

Certification Practice Statement (CPS)

VR-Ident privat-Zertifikate

Version:	Version 2.01.00, Freigegeben
Zielgruppe:	Nutzer und Besitzer von VR-Ident privat-Zertifikaten
Datum/Uhrzeit:	02.04.2014 / 13:30 Uhr

Gegenüber der vorherigen Ausgabe wurden folgende Änderungen vorgenommen:

Nummer	Datum	Inhalt / Änderungen
2.0	31.07.2012	Umwandlung der Winword Version 1.2 in DocBook Format
2.0	13.07.2012	Generell den Produktnamen VR-Ident privat (kleingeschrieben) verwendet
2.0	24.07.2012	Kapitel 1.4.2: Gefährliche Umgebungen hinzugefügt
2.0	24.07.2012	Kapitel 2.1.0: Adresse OCSP-Responder und CRL Distribution Point korrigiert
2.0	24.07.2012	Kapitel 2.3.0: Fristen für Sperrlistenaktualisierung angepasst
2.0	30.07.2012	Kapitel 4.2.3: Bearbeitungsdauer maximal 10 Arbeitstage angepasst
2.0	31.07.2012	Kapitel 4.9.1: Sperrgründe konkretisiert
2.0	01.08.2012	Kapitel 4.10.2: Die OCSP-Responder sind hochverfügbar ausgelegt
2.0	26.10.2012	Kapitel 7.1.x: Die Jahreszahl für die CAs anstatt JJJJ angegeben oder herausgenommen (soweit notwendig)
2.0	07.11.2012	Kapitel 1.3.1: Die Darstellungen der Hierarchien mit SSL synchronisiert
2.0	13.11.2012	Kapitel 7.1.2: Erweiterungen aktualisiert
2.0	30.11.2012	Kapitel 9.9: Hinweis auf Kapitel 9.8.1Erweiterungen aktualisiert, Baltimore Root ergänzt
2.0	15.02.2013	Vereinheitlichung der Schreibweise: Bindestriche bei Begriffen wie CA, etc., komplette CA Namen in "Hochkomma"
2.0	18.02.2013	Kapitel 1.4.1: Hinweis auf VR-Ident personal
2.0	18.02.2013	Kapitel 1.2: VR-Ident mail hinzugefügt
2.0	25.02.2013	Glossar hinzugefügt
2.0	07.03.2013	Kapitel 1.4.1: Bezug auf "Sonderbedingungen für den Zertifizierungsdienst VR-Ident"
2.0	21.06.2013	GAD Marktplatz in GAD Service-Portal geändert

Öffentlich - Nutzer und Besitzer von VR-Ident privat-Zertifikaten

Zusammenfassung

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

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Einleitung

1.1. Überblick

Die *GAD* eG ist ein IT-Dienstleister und Softwarehaus für mehr als 450 Banken (*GAD* Mitgliedsbanken). Zweck des Unternehmens ist die wirtschaftliche Förderung und Betreuung ihrer Mitglieder im Bereich der Informationstechnologie.

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

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.

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

1.1.1. Zweck des Dokuments

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

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

Die Dokumentenstruktur orientiert sich an dem *RFC* 3647.

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

Das *CPS* (*Certification Practice Statement*) gilt ausschließlich für das Produkt "VR-Ident privat".

Vorgaben für die Bedeutung und Verwendung von VR-Ident privat-Zertifikaten werden in dem Dokument "VR-Ident Certificate Policy für VR-Ident privat-Zertifikate" (siehe Anhang mit VR-Ident Referenzen) definiert.

1.1.2. Das VR-Ident Zertifikat

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

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

Mittels eines VR-Ident privat-Zertifikats auf der VR-Bankkarte bescheinigt der *Zertifizierungsdienst* VR-Ident, dass der Inhaber der VR-Bankkarte der Besitzer des zugehörigen Schlüsselpaares ist.

Im Einzelnen enthalten die *VR-Bankkarten* die folgenden Schlüsselpaare und dazugehörigen Zertifikate:

- **CSA:** Schlüsselpaar für Client-Server *Authentisierung*. Dieses Schlüsselpaar wird unter anderem für FinTS/HBCI-Funktionen genutzt. Mit einem zugehörigen *Authentisierungszertifikat* des Zertifizierungsdiensteanbieters *GAD* kann das CSA-Schlüsselpaar zusätzlich für die *Authentisierung* in weiteren Anwendungen, wie beispielsweise ein Windows-Logon oder eine SSL-Client-*Authentisierung*, genutzt werden.
- **DS:** Schlüsselpaar für elektronische Signaturen. In Verbindung mit einem zugehörigen *Zertifikat* des Zertifizierungsdiensteanbieters *GAD* kann dieses Schlüsselpaar unter anderem für die Generierung fortgeschrittener elektronischer Signaturen, beispielsweise zur Signierung von E-Mails, genutzt werden.
- **KE:** Schlüsselpaar für die Verschlüsselung. In Verbindung mit einem zugehörigen *Zertifikat* des Zertifizierungsdiensteanbieters *GAD* kann dieses Schlüsselpaar unter anderem für die Verschlüsselung von E-Mails genutzt werden.

Alle oben genannten Zertifikate werden in diesem Dokument unter dem Begriff "VR-Ident privat-Zertifikate" zusammengefasst.

Das VR-Ident privat-Zertifikat kann von Komponenten benutzt werden, welche Zertifikate nach *X.509* in der Version 3 korrekt interpretieren und verwenden können. Die Zertifikatsprofile sind in Kapitel 7.1 (S. 37) beschrieben.

1.2. Dokumentenname und Identifikation

Die Bezeichnung aller Richtliniendokumentes des Zertifizierungsdienstes 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: 2.01.00

Freigabedatum des vorliegenden Dokumentes: 25.03.2014

Die "17696" ist fest für Publikationen etc der "GAD IT für Banken eG" vergeben. Die ersten Stellen der *Object Identifier* (OID) der Richtliniendokumente des Zertifizierungsdienstes 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: 1.3.6.1.4.1.17696.4.1.1.4.2

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

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 Zertifizierungsdienstes VR-Ident beschrieben.

Der *Zertifizierungsdienst* VR-Ident verwendet für die Ausstellung der "VR-Ident privat-Zertifikate" folgende *Zertifizierungshierarchie*:

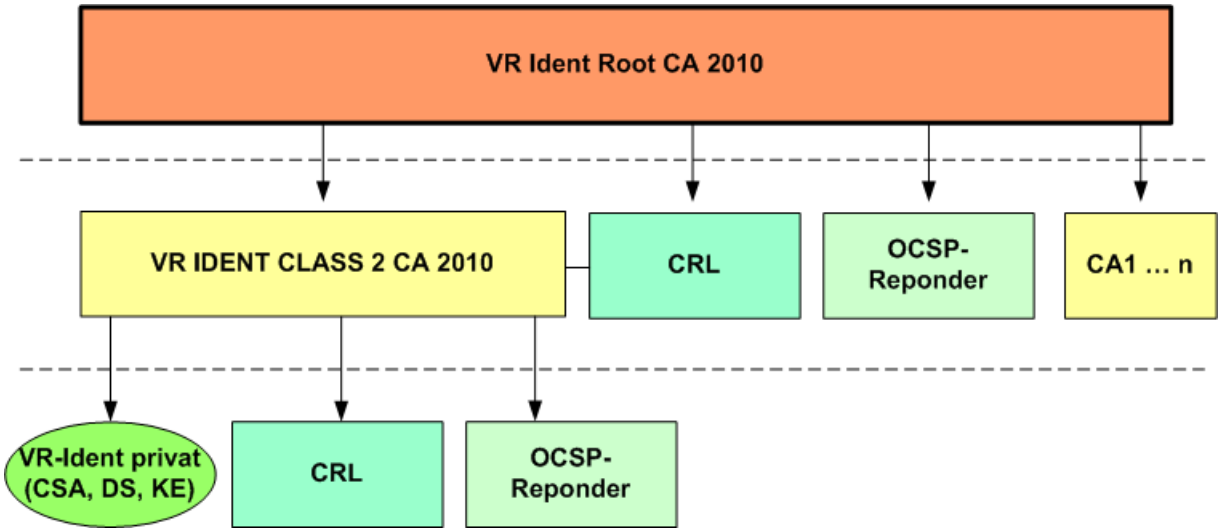

Abb. 1.1. Zertifizierungshierarchie für VR-Ident privat-Zertifikate

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

- Auf der obersten Ebene dieser *Zertifizierungshierarchie* befindet sich die "VR Ident Root CA 2010", die unter anderem das *Zertifikat* der "VR Ident Class 2 CA" signiert.
- Auf der zweiten Hierarchieebene befindet sich die "VR Ident Class 2 CA", die
  - die "VR-Ident privat-Zertifikate" in den Ausprägungen CSA-Zertifikate, DS-Zertifikate und KE-Zertifikate,
  - die Zertifikate des *OCSP-Responder* für Statusabfragen für "VR-Ident privat-Zertifikate" und
  - die *CRL* (*Sperrliste*) mit den Informationen zum *Sperrstatus* für die "VR-Ident privat-Zertifikate"

signiert.

Die "VR Ident Class 2 CA" handelt als Certification Authority (*CA*) und generiert und signiert "VR-Ident privat-Zertifikate" für die *Zertifikatseigentümer*.

- Auf der dritten Hierarchieebene befinden sich die "VR-Ident privat-Zertifikate" der *Zertifikatseigentümer*, *OCSP-Responder* und die *CRL* (*Sperrliste*).

1.3.2. Registrierungsinstanzen

Eine Registrierungsinstanz (RA) ist die Organisationseinheit einer PKI-Infrastruktur, welche die Identifizierung und *Authentisierung* des Antragstellers durchführt, Zertifikatserneuerungen veranlasst und Sperranträge

entgegennimmt. Sie ist die Stelle, mit der eine Person oder ein System kommunizieren muss, um ein digitales *Zertifikat* zu erhalten.

Die *VR-Banken* sind Registrierungsinstanzen. Sie nehmen die Anträge für VR-Ident privat-Zertifikate in den Filialen der *VR-Banken* entgegen und sind Vertragspartner der *Zertifikatseigentümer*.

1.3.3. Antragsteller

Auftraggeber

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.

Zertifikatseigentümer

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.

1.3.4. Vertrauende Dritte

Vertrauende Dritte sind Personen oder Organisationen, die sich auf die Ordnungsmäßigkeit der VR-Ident Zertifikate des Zertifizierungsdienstes VR-Ident der *GAD* verlassen.

1.3.5. Andere Teilnehmer

Keine.

1.4. Anwendung von Zertifikaten

1.4.1. Zulässige Anwendung von Zertifikaten

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

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 *GAD* 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.

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 Steuerungsinstrument 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. 14)) entsprechen.
- Weitere Informationen zur unzulässigen Nutzung von VR-Ident Zertifikaten sind unter http://www.vr-ident.de veröffentlicht.

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.

1.5. Policy Verwaltung

1.5.1. Organisation für die Verwaltung dieses Dokuments

Zuständig für die Verwaltung und Genehmigung dieses Dokumentes ist:
GAD eG
Abteilung: KVB/VSK/SKR
GAD-Straße 2-6
48163 Münster
Internet: http://www.vr-ident.de

1.5.2. Kontaktperson

Ansprechpartner für Fragen bezüglich dieses Dokumentes ist:
GAD eG
Abteilung: KVB/VSK/SKR
GAD-Straße 2-6
48163 Münster
E-Mail: gad_zertifikatsverwaltung@gad.de

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. 5) genannten Abteilung zuständig. Das Dokument behält seine Gültigkeit, solange es nicht von dieser Instanz widerrufen 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. 5) genannten Abteilung abgenommen. *CP* (*Certificate Policy*) und *CPS* (*Certification Practice Statement*) werden hierbei aufeinander abgestimmt.

1.6. Definitionen und Abkürzungen

Definitionen und Abkürzungen siehe im Glossar.

2. Bekanntmachung und Verzeichnisdienst

2.1. Verzeichnisse

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

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

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

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

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

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

2.2. Veröffentlichung von Zertifikatsinformationen

Der *Zertifizierungsdienst* VR-Ident veröffentlicht

- Ausgestellte VR-Ident Zertifikate (bei personengebundenen Zertifikaten, sofern der Inhaber der Veröffentlichung zugestimmt hat), in den in Kapitel 2.1 (S. 6) genannten Verzeichnissen,

- *CRL* (Sperrlisten), unter der in Kapitel 2.1 (S. 6) genannte Adresse,

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

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

Weitere geschäftliche und rechtliche Bestimmungen sind in Kapitel 9 (S. 47) des vorliegenden *CPS* (*Certification Practice Statement*) aufgeführt und werden somit veröffentlicht.

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) für VR-Ident SSL-Zertifikate werden alle 7 Tage oder vor Gültigkeitsablauf der bestehenden *CRL* (*Sperrliste*) erstellt.
- *CRL* (Sperrlisten) für VR-Ident mail-Zertifikate werden alle 7 Tage oder vor Gültigkeitsablauf der bestehenden *CRL* (*Sperrliste*) erstellt.
- *CRL* (Sperrlisten) für VR-Ident privat-Zertifikate werden alle 4 Tage oder vor Gültigkeitsablauf der bestehenden *CRL* (*Sperrliste*) erstellt.
- *CRL* (Sperrlisten) der CA-Zertifikate werden mindestens jährlich und nach jeder Sperrung eines CA-Zertifikats erstellt.

Aktualisierungen des vorhandenen Dokuments werden gemäß Kapitel 9.12 (S. 51) veröffentlicht. Die Veröffentlichung der *CP* (*Certificate Policies*) und des *CPS* (*Certification Practice Statement*) erfolgt jeweils nach ihrer Erstellung oder ihrer Aktualisierung.

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

2.4. Zugriffskontrolle auf Verzeichnisse

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

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

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

3. Identifizierung und Authentisierung

3.1. Namensgebung

3.1.1. Namenstypen

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

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

- CommonName (CN)= VR IDENT CLASS 2 CA 2010
- Organization (O) = GAD EG
- Organizational Unit (OU) = VR IDENT
- Country (C) = DE

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

- CommonName (CN) = Name des Zertifikatsinhabers
- serialNumber (SN) = verschlüsselter Hinweis auf die im Bankverfahren verwendete VR-Bankkarte
- distinguishedNameQualifier (DNQ) = eindeutige VR-Ident interne Kennung
- Country (C) = DE

Außerdem enthalten die Zertifikate in der Erweiterung SubjectAltName optional einen alternativen Eigentümer-Namen als rfc822Name.

3.1.2. Anforderung an die Bedeutung von Namen

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

Das Attribut CommonName der VR-Ident privat-Zertifikate beinhaltet den natürlichen Namen (Vor- und Familienname) des Zertifikatsinhabers. Das Attribut SubjectAltName enthält optional die E-Mail Adresse eines Zertifikatseigentümers.

3.1.3. Anonymität und Pseudonyme für Zertifikatseigentümer

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

3.1.4. Regeln zur Interpretation verschiedener Namensformen

Im Namen dürfen ausschließlich die folgenden Zeichen verwendet werden:
A-Z, a-z, 0-9, Leerzeichen, ', (,), +, -, ,, ., /, :, ?

Optional können die folgenden "deutschen" Sonderzeichen verwendet werden:
Ä, Ö , Ü , ä , ö ü , ß
Für die Ersetzung deutscher Sonderzeichen gelten folgende Substitutionsregeln:
Ä -> Ae, Ö ->Oe, Ü -> Ue, ä -> ae, ö -> oe, ü -> ue, ß -> ss
Sonderzeichen mit Akzenten verlieren diese. Ansonsten wird eine für das betreffende Zeichen gemeinhin verwendete Schreibweise aus den Zeichen a-z und A-Z so zusammengesetzt, dass der entsprechende Laut entsteht.

3.1.5. Eindeutigkeit von Namen

Die Namen der vom *Zertifizierungsdienst* VR-Ident ausgestellten VR-Ident privat-Zertifikaten sind durch die Nummer im Attribut serialNumber stets eindeutig. Dadurch sind die Subject *Distinguished Name* (*DN*) eindeutig.

3.1.6. Erkennung, Authentisierung und Rolle von geschützten Namen

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

3.2. Erstmalige Identitätsprüfung

3.2.1. Methode zum Besitznachweis des privaten Schlüssels

Der Beantragende eines Zertifikats muss die *Authentizität* der verwendeten Schlüssel nachweisen. Der Besitznachweis der *privaten Schlüssel* erfolgt durch den *Zertifikats-Downloadserver* in der folgenden Weise:

- Der Server authentisiert die VR-Bankkarte in einem kryptographischen Authentisierungsprotokoll mit Schlüsseln, die bei der Kartenproduktion auf die Karte aufgebracht wurden. Damit wird verifiziert, dass es sich um eine authentische VR-Bankkarte handelt, die nicht gesperrt wurde.
- Im Zuge der *Authentisierung* wird ein sicherer kryptographischer Kanal zwischen dem Server und der VR-Bankkarte aufgebaut, die es dem Server ermöglicht, die *öffentlichen Schlüssel*, für die Zertifikate ausgestellt werden sollen, sicher auszulesen.
- Nach dem Auslesen der *öffentlichen Schlüssel*, muss der *Antragsteller* einen Certification Requests für die beantragten Zertifikate signieren. Falls ein *Zertifikat* für den DS-Schlüssel beantragt wurde, wird der Request mit diesem signiert, anderenfalls mit dem CSA-Schlüssel. Durch die Signatur wird sichergestellt, dass der *Antragsteller* auch im Besitz der *PIN* der Karte ist. Hierzu werden geeignete *asymmetrische Kryptoverfahren* verwendet.

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 maschinengebunden 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 identische sein mit dem Eintrag in dem jeweiligen Verzeichnis.

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

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

- Handelsregister (HRB)
- Genossenschaftsregister (GnR)

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

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 in lateinischer Schrift und in deutscher oder englischer Sprache akzeptiert.

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

Bezüglich der *Authentisierung* des Zertifikatseigentümers werden die folgenden Fälle unterschieden:

1. Initiale Identifizierung: Bei der Erstkontoeröffnung erfolgt eine Identifizierung des Kunden nach den gesetzlichen Regelungen durch die VR-Banken. Diese Identifizierung genügt den Vorgaben des Geldwäschegesetzes. Hierzu muss sich ein Kunde, sofern er dem Kundenberater der Filiale der VR-Bank nicht bereits bekannt ist, persönlich durch einen gültigen amtlichen Ausweis sowie durch eine Gegenprobe der im Ausweis abgebildeten Unterschrift identifizieren.

2. *Authentisierung* bei Beantragung der Zertifikate: Der *Antragsteller* authentisiert sich in einer Filiale der VR-Bank nach den gesetzlichen Regelungen gegenüber den VR-Banken. In der Regel erfolgt die *Authentisierung* dabei anhand seiner Kundenstammdaten.

3. *Authentisierung* bei der Kontaktierung des Zertifikats-Downloadservers: Der *Antragsteller* authentisiert sich gegenüber dem *Zertifikats-Downloadserver* mittels seiner VR-Bankkarte. Die *Authentisierung* erfolgt dabei mit starken kryptographischen Authentisierungsverfahren und der HBCI-PIN. Die verwendeten kryptographischen Schlüssel werden im Rahmen der Kartenproduktion auf die Karte aufgebracht.

4. Die *Authentisierung* von E-Mail Adressen, die optional in ein *Zertifikat* aufgenommen werden können erfolgt über einen zufälligen Aktivierungscode, der dem *Antragsteller* vor Aufnahme der E-Mail Adresse in das *Zertifikat* zugesendet wird.

3.2.4. Nicht verifizierte Teilnehmerinformationen

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.

3.2.5. Überprüfung der Handlungsvollmacht

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

3.2.6. Kriterien für Zusammenwirkung

Kriterien zur Zusammenwirkung entfallen.

3.3. Identifizierung und Authentifizierung bei Schlüsselerneuerung

3.3.1. Identifizierung und Authentifizierung bei turnusmäßiger Schlüsselerneuerung

Die Prozesse zur Identifizierung und *Authentifizierung* von VR-Ident privat-Zertifikaten bei Schlüsselerneuerung sind identisch zur initialen Identifizierung (siehe Kapitel 3.2.3 (S. 9)).

3.3.2. Identifizierung und Authentifizierung bei Schlüsselerneuerung nach Sperrung

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. 9)).

3.4. Identifizierung und Authentifizierung bei Sperranträgen

Bezüglich der *Authentisierung* beim Sperrantrag werden die folgenden Fälle unterschieden:

1. Sperrung in einer Filiale der VR-Bank: Der *Antragsteller* authentisiert sich in einer Filiale der VR-Bank entsprechend den gesetzlichen Regelungen gegenüber der VR-Banken. Das verwendete Authentisierungsverfahren entspricht dem bei der Beantragung der Zertifikate (siehe Kapitel 3.2.3 (S. 9)).

2. Sperrung über das Online-Banking: Der Karteninhaber authentisiert sich im Rahmen der Anmeldung beim Online-Banking mittels seines privaten CSA-Schlüssels.

4. Anforderungen an den Lebenszyklus des Zertifikats

4.1. Antragstellung

4.1.1. Wer kann ein Zertifikat beantragen

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

4.1.2. Registrierungsprozess und Verantwortlichkeiten

Die Antragstellung erfolgt durch den *Antragsteller* in einer Filiale der VR-Bank des Antragstellers durch Freischaltung seiner Signaturkarte für das Nachladen von Zertifikaten auf seine Signaturkarte. Dabei kann der *Zertifikatseigentümer* folgende Parameter festlegen:

- Der *Antragsteller* entscheidet, für welche Schlüsselpaare seiner Signaturkarte er Zertifikate erhalten will.
- Der *Antragsteller* kann eine E-Mail Adresse angeben.
- Der *Antragsteller* bestimmt, ob die Zertifikate veröffentlicht werden sollen.

Es wird zwischen zwei verschiedenen Anträgen unterschieden:

- Erstanträge: In diesem Fall besitzt der *Antragsteller* noch keine Zertifikate für seine Signaturkarte.
- Wiederholungsanträge: Hierbei handelt es sich um die Beantragung von neuen Zertifikaten für eine existierende Signaturkarte, welche die bereits auf der Karte befindlichen Zertifikate ersetzen sollen. Weitere Informationen hierzu sind in Kapitel 4.7 (S. 15) und in Kapitel 4.8 (S. 16) zu entnehmen.

Bei Folgekarten entfällt die Beantragung von Zertifikaten, sofern der *Antragsteller* bereits gültige VR-Ident privat-Zertifikate für die zu ersetzende Karte besitzt. In diesem Fall erfolgt die Freischaltung automatisch innerhalb der Systeme der *Zertifizierungsstelle* VR-Ident.

4.2. Antragsbearbeitung

4.2.1. Durchführung der Identifikation und Authentifizierung

Die Kundenberater der Filialen der *VR-Banken* führen die Identifizierung und Authentifizierung wie in Kapitel 3.2.3 (S. 9) beschrieben durch.

4.2.2. Annahme beziehungsweise Ablehnung von Zertifikatsanträgen

Voraussetzung für die Annahme des Zertifikatsantrags ist, dass die Identifizierung und *Authentifizierung* aller erforderlichen Informationen zum *Antragsteller* oder zum Auftraggeber gemäß Kapitel 3.2.2 (S. 9) und Kapitel 3.2.3 (S. 9) erfolgreich war.

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

- Der Auftraggeber beziehungsweise der *Antragsteller* kann nicht zweifelsfrei identifiziert werden,
- Der Auftraggeber hat gegen Geldwäschegesetz verstoßen oder steht auf Embargolisten,
- Der *Zertifizierungsdienst* VR-Ident hat weitere Ablehnungsgründe.
- Das Konto des Antragstellers weist nicht die erforderliche Deckung auf.
- Der *Antragsteller* besitzt eine VR-Bankkarte, die technisch nicht geeignet ist.

4.2.3. Bearbeitungsdauer von Zertifikatsanträgen

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

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

4.3. Zertifikatserstellung

4.3.1. CA Prozesse während der Zertifikatserstellung

Ein *Antragsteller* startet die Erstellung der Zertifikate über ein entsprechendes Webinterface des Zertifikats-Downloadservers des Zertifizierungsdienstes VR-Ident. Er muss dabei seine VR-Bankkarte in einen an den Rechner angeschlossen Chipkartenleser stecken. Der *Zertifikats-Downloadserver* authentisiert die VR-Bankkarte des Antragstellers über kryptographische Mechanismen und baut einen sicheren Kanal zur Karte auf. Für die Zertifizierung werden die *öffentlichen Schlüssel* aus der Signaturkarte des Zertifikatseigentümers ausgelesen und über den sicheren Kanal an den *Zertifizierungsdienst* VR-Ident übermittelt.

Danach erhält der *Antragsteller* die Möglichkeit, eine E-Mail Adresse anzugeben, die in das *Zertifikat* aufgenommen werden soll. Folgende Möglichkeiten bestehen:

- Er kann seine gegebenenfalls bereits bei der Antragstellung angegebene E-Mail Adresse übernehmen
- Er kann seine gegebenenfalls bereits bei der Antragstellung angegebene E-Mail Adresse ändern
- Er kann eine neue E-Mail Adresse eingeben
- Es soll keine E-Mail Adresse verwendet werden

Falls eine E-Mail Adresse in das *Zertifikat* aufgenommen werden soll, wird an diese Adresse ein zufälliger Aktivierungscode gesendet, den der *Antragsteller* im Webformular eingeben muss, um die Korrektheit der E-Mail Adresse nachzuweisen.

Im nächsten Schritt muss der *Antragsteller* festlegen, ob seine Zertifikate veröffentlicht werden sollen.

Dann wird für die beantragten Zertifikate ein Certification Request generiert, vom *Antragsteller* signiert, und an den *Zertifizierungsdienst* VR-Ident übermittelt. Gegebenenfalls muss sich der *Antragsteller* dafür seine Transport Signatur-PIN in eine gültige Wirk-PIN ändern (siehe Kapitel 3.2.1 (S. 9) und Kapitel 6.4.1 (S. 34)). Der *Zertifizierungsdienst* VR-Ident prüft die Signatur des Certification Requests und erstellt entsprechende Zertifikate. Sofern der *Antragsteller* dies so festgelegt hat, werden die Zertifikate unmittelbar nach ihrer Erstellung veröffentlicht.

4.3.2. Benachrichtigung des Antragstellers über die Zertifikatserstellung

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

4.4. Zertifikatsakzeptanz

4.4.1. Annahme durch den Zertifikatsinhaber

Nach ihrer Generierung werden die VR-Ident privat-Zertifikate automatisch durch den Download-Server auf das System des Antragstellers übertragen und dort auf die Karte geschrieben. Hierdurch akzeptiert der Inhaber das Zertifikat.

Sollte es bei der Übermittlung der Zertifikate zum *Antragsteller* zu einem Abbruch der Kommunikation kommen, so kann der *Antragsteller* sich erneut am Download-Server anmelden und den Prozess abschließen.

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. 6) 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

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 Zertifizierungsdiensteanbieters *GAD* geprüft werden kann.

Die Prüfung der Sperrinformation kann wahlweise auf Basis einer gültigen Sperrliste oder einer aktuellen Abfrage beim Auskunftsdienst des Zertifizierungsdienstes 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. 4) beschrieben.

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.

4.6.1. Gründe für eine Zertifikatserneuerung

Ein *Zertifikatseigentümer* hat die Möglichkeit, sich nach der Sperrung eines VR-Ident privat-Zertifikats für diesen Schlüssel ein neues VR-Ident privat-Zertifikat ausstellen zu lassen. Voraussetzung dafür ist, dass die Sicherheit des Schlüsselpaares gewährleistet ist, und dass die VR-Bankkarte noch gültig und im Besitz des Zertifikatseigentümers ist.

4.6.2. Wer kann eine Zertifikatserneuerung beantragen

Siehe Kapitel 4.1.1 (S. 12).

4.6.3. Ablauf der Zertifikatserneuerung

Für die *Zertifikatserneuerung unter Beibehaltung des alten Schlüssels* muss der *Zertifikatseigentümer* einen Wiederholungsantrag (siehe Kapitel 4.1.1 (S. 12)) stellen und anschließend die neuen VR-Ident privat-Zertifikate über das Webportal runterladen (siehe Kapitel 4.3.1 (S. 13)).

4.6.4. Benachrichtigung des Zertifikatsinhabers nach Zertifikatserneuerung

Siehe Kapitel 4.3.2 (S. 13).

4.6.5. Annahme einer Zertifikatserneuerung

Siehe Kapitel 4.4.1 (S. 13).

4.6.6. Veröffentlichung einer Zertifikatserneuerung durch den Zertifizierungsdienst

Siehe Kapitel 4.4.2 (S. 14).

4.6.7. Benachrichtigung weiterer Instanzen durch den Zertifizierungsdienst

Siehe Kapitel 4.4.3 (S. 14).

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

Nach Ablauf der Kartengültigkeit oder einer Kartensperre stellt die VR-Bank in der Regel automatisch Folgekarten für die *Zertifikatseigentümer* aus.

4.7.2. Wer kann eine Schlüssel- und Zertifikatserneuerung beantragen

Siehe Kapitel 4.1.1.

4.7.3. Ablauf der Schlüssel- und Zertifikatserneuerung

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

4.7.4. Benachrichtigung des Zertifikatsinhabers nach Schlüssel- und Zertifikatserneuerung

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

4.7.5. Annahme der Schlüssel- und Zertifikatserneuerung

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

4.7.6. Veröffentlichung einer Zertifikatserneuerung durch den Zertifizierungsdienst

Siehe Kapitel 4.4.2 (S. 14).

4.7.7. Benachrichtigung weiterer Instanzen durch den Zertifizierungsdienst

Siehe Kapitel 4.4.3 (S. 14).

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.

4.8.1. Gründe für eine Zertifikatsmodifizierung

Eine Modifizierung von VR-Ident privat-Zertifikaten wird unterstützt, es kann dabei beispielsweise die E-Mail Adresse geändert werden.

Die Änderung des im VR-Ident privat-Zertifikats eingetragenen Namens des Zertifikatseigentümers (beispielsweise nach einer Namensänderung) erfordert dagegen die Ausstellung einer neuen VR-Bankkarte und ist daher zwangsläufig mit einem Wechsel des Schlüsselpaares verbunden. In diesem Fall muss der *Zertifikatseigentümer* für seine neue VR-Bankkarte wie in Kapitel 4.1.1 (S. 12) bis Kapitel 4.4.1 (S. 13) beschrieben neue Zertifikate beantragen und erstellen lassen.

4.8.2. Wer kann eine Zertifikatsmodifizierung beantragen

Siehe Kapitel 4.1.1 (S. 12).

4.8.3. Ablauf der Zertifikatsmodifizierung

Zur *Zertifikatsmodifizierung* muss der *Zertifikatseigentümer* einen Wiederholungsantrag (siehe Kapitel 4.1.1 (S. 12)) stellen und anschließend die neuen Zertifikate über das Webportal herunterladen (siehe Kapitel 4.3.1 (S. 13)). Eine vorherige Sperrung der alten Zertifikate durch den Zertifikatseigentümern ist nicht erforderlich, diese werden im Zuge (aber vor) der Ausstellung der neuen Zertifikate automatisch

gesperrt. Der *Zertifikatseigentümer* kann aber alternativ auch nach einer Sperrung seiner Zertifikate eine Modifizierung vornehmen.

4.8.4. Benachrichtigung des Zertifikatsinhabers nach der Zertifikatsmodifizierung

Siehe Kapitel 4.3.2 (S. 13).

4.8.5. Annahme der Zertifikatsmodifizierung

Siehe Kapitel 4.4.1 (S. 13).

4.8.6. Veröffentlichung einer Zertifikatsmodifizierung durch den Zertifizierungsdienst

Siehe Kapitel 4.4.2 (S. 14).

4.8.7. Benachrichtigung weiterer Instanzen durch den Zertifizierungsdienst

Siehe Kapitel 4.4.3 (S. 14).

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 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 Zertifizierungsdienstes 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 privat-Zertifikat zu sperren, wenn das *Zertifikat* des CA-Schlüssels oder deren *Root-CA*, mit dem das betreffende *Zertifikat* ausgestellt wurde, gesperrt wurde.

Weiterhin behält sich der *Zertifizierungsdienst* VR-Ident das Recht vor, ein 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. 16)) 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 folgenden Parteien sind berechtigt, die Sperrung von VR-Ident Zertifikaten zu beantragen oder auch durchzuführen:

- Der *Zertifikatseigentümer* oder ein durch ihn bevollmächtigter Dritter kann die Sperrung eigener VR-Ident Zertifikate beantragen.
- Der *Zertifizierungsdienst* VR-Ident kann die Sperrung von ausgestellten VR-Ident Zertifikaten und der VR-Ident CA-Zertifikate veranlassen und durchführen.
- *VR-Banken* können die Sperrung von VR-Ident privat-Zertifikaten zu den von ihnen ausgegebenen *VR-Bankkarten* veranlassen.

4.9.3. Verfahren zur Sperrung

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

- Über die Filiale der VR-Bank: Der *Zertifikatseigentümer* oder ein durch ihn bevollmächtigter Dritter kann einzelne oder alle Zertifikate telefonisch, schriftlich oder persönlich bei einer Filiale seiner VR-Bank sperren lassen. Die Identifizierung erfolgt in der für Bankgeschäfte vorgeschriebenen Weise. Ein Kundenberater der VR-Bank führt dann die Sperrung der VR-Ident privat-Zertifikate als *Sperrmitarbeiter* durch.
- Online: Über das Webportal des Zertifizierungsdienstes VR-Ident können VR-Ident privat-Zertifikate nach erfolgreicher *Authentisierung* im Online-Banking jederzeit gesperrt werden.
- Online: sofern der *Zertifikatseigentümer* noch im Besitz seiner VR-Bankkarte ist, kann er einzelne oder alle Zertifikate zu dieser Karte über das Webinterface sperren. Die *Authentisierung* erfolgt dabei wie beim Online-Banking.

- Durch Kartensperre: Ein *Zertifikatseigentümer* oder ein durch ihn bevollmächtigter Dritter kann seine Zertifikate durch Sperrung der VR-Bankkarte (beispielsweise über die Sperr-Hotline für *VR-Bankkarten* als *Sperrmitarbeiter*) sperren. Die Sperrung der Zertifikate ist dabei endgültig, auch wenn die Karte selbst wieder entsperrt werden kann.

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

Die Sperrung eines VR-Ident privat-Zertifikats bewirkt nicht die Sperrung oder Invalidierung der HBCI-Funktionalitäten einer VR-Bankkarte, der *Zertifikatseigentümer* kann also auch nach der Sperrung seiner Zertifikate das Online-Banking nutzen.

Die Sperrungen von "VR-Ident Root CA 2010" und von "VR-Ident Class 2 CA 2010" Zertifikaten werden ebenfalls vom Leiter des Zertifizierungsdienstes VR-Ident initiiert.

4.9.4. Fristen für die Beantragung einer Sperrung

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

Eine Sperrung von allgemeinen VR-Ident Zertifikaten erfolgt in der Regel unverzüglich nach Eingang eines Sperrantrags.

4.9.6. Prüfung des Zertifikatsstatus durch vertrauende Dritte

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

4.9.7. Periode für Erstellung von Sperrlisten

Die Häufigkeit und Zyklen für die Veröffentlichung und Erstellung von *CRL* (Sperrlisten) ist in Kapitel 2.3 (S. 7) 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 VR-Ident *Zertifizierungsdienst* 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* möglichst unverzüglich zu sperren.

4.9.13. Gründe für die 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.

4.9.14. Wer kann eine Suspendierung beantragen

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.

4.9.15. Verfahren zur 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.

4.9.16. Maximale Sperrdauer bei Suspendierung

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

4.10. Auskunftsdienst über den Zertifikatsstatus

Der Auskunftsdienst für den Zertifikatsstatus basiert auf dem "Online Certificate Status Protocol" (*OCSP*) Version 1 nach *RFC* 2560 und stellt die Status der VR-Ident Zertifikate sowie der Zertifikate der VR-Ident Zertifizierungsinstanzen (siehe Kapitel 1.3.1 (S. 3) und Kapitel 2.1 (S. 6)) online zur Verfügung.

4.10.1. Betriebseigenschaften der Auskunftsdienste

Der *OCSP-Responder* ist über die in Kapitel 2.1 (S. 6) angegebene URL erreichbar. Der *OCSP-Responder* verwendet als Übertragungsprotokoll *HTTP* und implementiert das "Online Certificate Status Protocol" (*OCSP*) mit den folgenden Eigenschaften:

- Die Anfragen (OCSP-Requests) müssen nicht signiert sein; signierte Anfragen werden jedoch auch unterstützt.
- Die Auskünfte des *OCSP-Responder* sind Positivauskünfte, sofern die Antwort auf eine Anfrage den Status "good" liefert, bedeutet dies auch, dass das *Zertifikat* im VR-Ident *Verzeichnisdienst* vorhanden ist und dass dieses gültig ist.
- Die *OCSP-Responder* verwenden für ihre Auskünfte eine ständig aktualisierte Datenbasis. Das Feld "NextUpdate" enthält den Zeitpunkt, an dem spätestens aktuellere Informationen zum Status des Zertifikats über den *OCSP-Responder* verfügbar sind. Die Antworten (OCSP-Response) sollten daher nicht länger als zu dem Zeitpunkt in dem Feld "NextUpdate" zwischengespeichert und wiederverwendet werden.
- Die unterstützten und die verwendeten Erweiterungen (OCSP-Extensions) sind im Kapitel 7.3 (S. 43) angegeben.

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

- Die *CRL* (*Sperrliste*) entspricht den Standards *X.509*, sowie *RFC* 5280 und Common *PKI* (siehe Anhang mit allgemeinen Referenzen).
- Die *CRL* (*Sperrliste*) wird durch die *CA* selbst signiert, es handelt sich um eine sogenannte direkte *CRL* (*Sperrliste*).
- Die *CRL* (*Sperrliste*) wird durch die *CA* selbst signiert, es handelt sich um eine sogenannte direkte *CRL* (*Sperrliste*).
- Die *CRL* (Sperrlisten) sind im VR-Ident *Verzeichnisdienst* (siehe Kapitel 2.1 (S. 6)) im Knoten der entsprechenden *CA* abgelegt.
- Die *CRL* (Sperrlisten) sind gültig bis zur Ausstellung der nächsten planmäßigen *CRL* (*Sperrliste*). Die Frequenz für die Ausstellung der Sperrlisten ist in Kapitel 2.3 (S. 7) festgelegt.
- Die *CRL* (Sperrlisten) enthalten alle gesperrten Zertifikate, auch jene, die auf Wunsch des Zertifikatseigentümers nicht veröffentlicht wurden.
- Die verwendeten CRL-Erweiterungen sind in Kapitel 7.2 (S. 42) angegeben.

Für die Zertifizierungsstellen von VR-Ident privat-Zertifikaten gelten folgende spezielle Festlegungen bezüglich der *OCSP-Responder*:

- Für die "VR Ident Class 2 CA 2010" und die "VR Ident Root CA 2010" werden zwei unterschiedliche *OCSP-Responder* eingesetzt, die unter unterschiedlichen URLs erreicht werden können.
- Der *OCSP-Responder* der "VR Ident Root CA2010" stellt Sperrinformationen für alle *CA* der 2. Ebene und den zugeordneten OCSP-Respondern (insbesondere dem *OCSP-Responder* der "VR Ident Class 2 CA 2010") zur Verfügung.
- Der *OCSP-Responder* der "VR Ident Class 2 CA 2010" stellt Sperrinformationen zu allen VR-Ident privat-Zertifikaten zur Verfügung, auch für jene, die auf Wunsch des Zertifikatseigentümers nicht veröffentlicht wurden.

4.10.2. Verfügbarkeit des Auskunftsdienstes

Die *OCSP-Responder* des Zertifizierungsdienstes VR-Ident sind hochverfügbar ausgelegt.

4.10.3. Optionale Funktionen

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

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

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

4.11. Austritt aus dem Zertifizierungsdienst

Ein *Zertifikatseigentümer* oder ein Kunde tritt aus dem *Zertifizierungsdienst* VR-Ident aus, wenn alle seine Zertifikate ablaufen oder gesperrt werden, und nicht unmittelbar Folgezertifikate erstellt werden. Dies ist der Fall, wenn

- er die Sperrung aller Zertifikate beantragt,
- er das Vertragsverhältnis mit dem Zertifizierungsdiensteanbieter *GAD* oder seiner VR-Bank kündigt,

- der *Zertifizierungsdienst* VR-Ident die Sperrung aller seiner Zertifikate veranlasst, und dies nicht im Zuge der Ersetzung der Zertifikate erfolgt, oder
- die VR-Ident Zertifikate ablaufen und keine neuen Zertifikate ausgestellt werden.

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* 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* diese durch.

5. Physikalische, organisatorische und personelle Sicherheitsmaßnahmen

5.1. Physikalische Sicherheitsmaßnahmen

5.1.1. Lage und Aufbau des Standortes

Die Zertifizierungstätigkeiten des Zertifizierungsdienstes VR-Ident der *GAD* werden in einem baulich geschützten Bereich des Rechenzentrums der *GAD* eG in der GAD-Straße 2-6 in Münster betrieben. Die bauliche Infrastruktur unterliegt hohen Sicherheitsstandards bezüglich physikalischer Sicherheit. Sie ist derart gestaltet, dass ein hoher Schutz gegen Einbruch gewährleistet ist. Weiterhin wurden Vorkehrungen zum Schutz gegen Brand, Wasser und Blitzeinschlag getroffen. Die entsprechenden IT-Systeme des Zertifizierungsdienstes VR-Ident befinden sich innerhalb des gesicherten Bereichs. Zur Aufrechterhaltung des Zertifizierungsbetriebs im Notfall werden die IT-Systeme redundant ausgelegt und betrieben. Die Unterbringung der redundanten Systeme erfolgt in örtlich getrennten Räumen in einem Backup-Rechenzentrum.

5.1.2. Zugangskontrolle

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

5.1.3. Stromversorgung und Klimakontrolle

Das Rechenzentrum der *GAD* eG, in dem der *Zertifizierungsdienst* VR-Ident betrieben wird ist mit durchgehender, ununterbrochener Zufuhr elektrischer Stromversorgung ausgestattet.

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

5.1.4. Schutz vor Wasserschäden

Das Rechenzentrum der *GAD* eG und insbesondere die Technikräume sind durch bauliche Maßnahmen vor Wassereinbrüchen gesichert.

5.1.5. Brandschutz

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

5.1.6. Aufbewahrung von Datenträgern

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

5.1.7. Entsorgung von Datenträgern

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

5.1.8. Datensicherung

Für den *Zertifizierungsdienst* VR-Ident wird regelmäßig eine Datensicherung durchgeführt. Die Datensicherung umfasst die Daten der Zertifizierungsprozesse, die Protokolldaten und weitere wichtige Daten. Die Backup-Datenträger werden sicher aufbewahrt (siehe Kapitel 5.1.6 (S. 23)).

5.2. Organisatorische Sicherheitsmaßnahmen

5.2.1. Sicherheitskritische Rollen

Zertifizierungstätigkeiten dürfen ausschließlich durch autorisierte *Rollenträger* durchgeführt werden. Das sind Mitarbeiter, denen die entsprechenden Rollen zugewiesen sind. Sicherheitskritische Rollen sind insbesondere:

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

Alle diese Rollen sind durch vertrauenswürdige und qualifizierte Mitarbeiter besetzt.

Die Rollen und deren Aufgaben werden im Rollenkonzept der Sicherheitsleitlinie der GAD explizit beschrieben

5.2.2. Anzahl benötigter Personen bei sicherheitskritischen Tätigkeiten

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

- Administrativer oder operativer Zugriff auf *Hardware-Sicherheitsmodule* (*HSM*),
- Initialer Austausch von Systemschlüsseln,
- Prozeduren der Key Ceremony.

5.2.3. Identifizierung und Authentisierung von Rollen

Die Identifizierung und *Authentisierung* der Rollen bei den Sicherheitsräumen im Rechenzentrum und bei den IT-Systemen erfolgt mit Hilfe von Zutrittskarten sowie Benutzername und Passwort. Die Anmeldung der *PKI* Operatoren an den VR-Ident *PKI* Systemen erfolgt basierend auf einem *Authentisierungszertifikat*.

5.2.4. Trennung von Rollen und Aufgaben

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

- Das Management der *GAD* darf keine operativen oder administrativen Tätigkeiten ausüben.

- Auditoren und Revisoren dürfen keine operativen oder administrativen Tätigkeiten ausüben.
- System-Administratoren dürfen keine operativen Aufgaben ausüben.
- *Rollenträger*, die für die Zutrittsrechte zu den Räumlichkeiten des Zertifizierungsdienstes VR-Ident zuständig sind, dürfen keine sonstigen operativen oder administrativen Aufgaben ausüben.

5.3. Personelle Sicherheitsmaßnahmen

5.3.1. Anforderungen an Qualifikation und Erfahrung

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

5.3.2. Überprüfung der Vertrauenswürdigkeit

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

5.3.3. Anforderungen an Schulung und Fortbildung

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

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

5.3.4. Nachschulungsintervalle und –anforderungen

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

5.3.5. Arbeitsplatzrotation / Rollenumverteilung

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

5.3.6. Sanktionen bei unbefugten Handlungen

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

5.3.7. Vertragsbedingungen mit dem Personal

Der Zertifizierungsdiensteanbieter *GAD* verpflichtet seine Mitarbeiter auf die Einhaltung von Anweisungen und gesetzlichen Vorschriften. Diese beinhalten insbesondere eine Verpflichtung, personenbezogene Daten vertraulich zu behandeln.

Werden unter Umständen externe Personen (unabhängige Auftragnehmer oder Berater) zur Besetzung vertrauenswürdiger Positionen eingesetzt, so unterliegen diese denselben Funktions- und Sicherheitskriterien wie Mitarbeiter des Zertifizierungsdiensteanbieters *GAD* in vergleichbarer Position.

5.3.8. An das Personal ausgehändigte Dokumentation

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

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

5.4. Protokollierung sicherheitskritischer Ereignisse

5.4.1. Zu protokollierende Ereignisse

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

- Ereignisse im Lebenszyklus der VR-Ident Zertifikate, einschließlich:
  - Stammdatenerfassung für VR-Ident Zertifikate
  - Registrierung für VR-Ident Zertifikate,
  - Ausstellung von VR-Ident Zertifikaten,
  - Veröffentlichung von VR-Ident Zertifikaten,
  - Durchgeführte Sperrungen,
  - Erstellung und Veröffentlichung von *CRL* (Sperrlisten).
- Registrierungsdaten
  - Registrierungsdaten für VR-Ident SSL-Webserver-Zertifikate im Key Management Workflow und im *GAD* Service-Portal
  - Antragsformulare in Papierform beziehungsweise in elektronischer Form im Auftragmanagement der *GAD*
- Ereignisse im Lebenszyklus der CA-Zertifikate und Schlüsselpaare,
  - Schlüsselgenerierung, Archivierung und Vernichtung für CA-Schlüssel,
  - Ausstellung von CA-Zertifikaten,
  - Veröffentlichung von CA-Zertifikaten,

  - Durchgeführte Sperrungen von CA-Zertifikaten,
  - Erstellung und Veröffentlichung von *CRL* (Sperrlisten).
- Sicherheitsrelevante Ereignisse, einschließlich:
  - Anmeldung am PKI-System,
  - Vergabe und Entzug von Zugriffsberechtigungen,
  - Zugriffe und Zugriffsversuche per Netzwerk.
  - Durchführung der Arbeitschritte im Key Management Workflow, bank21 und im *GAD* Service-Portal
- Ereignisse der Zutrittskontrollanlage, einschließlich:
  - Betreten und Verlassen von gesicherten Räumen,
  - Fehlgeschlagene Zutrittsversuche und Alarme,
  - Vergabe und Entzug von Zutrittsberechtigungen,
  - Beantragung, Ausgabe und Sperrung von Zutrittskarten.

Die Protokolleinträge enthalten die folgenden Daten:

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

5.4.2. Häufigkeit der Auswertung von Protokolldaten

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

5.4.3. Aufbewahrungsfristen für Protokolldaten

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

5.4.4. Schutz der Protokolldaten

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

5.4.5. Sicherungsverfahren für Protokolldaten

Alle elektronischen Protokolldaten werden regelmäßig gesichert.

5.4.6. Internes/externes Protokollierungssystem

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

5.4.7. Benachrichtigung des Auslösers eines Ereignisses

Alle Mitarbeiter des Zertifizierungsdiensteanbieters *GAD* sind über den Umfang der Protokollierung ihrer Tätigkeiten informiert.

5.4.8. Schwachstellenbewertung

Eventuelle Schwachstellen werden durch permanente Überwachung und durch Sicherheits-Audits durch den Information Security Officer des Zertifizierungsdiensteanbieters *GAD* und bei Bedarf durch externe Auditoren bewertet.

5.5. Archivierung

5.5.1. Archivierte Daten und Aufbewahrungsfrist

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

5.5.2. Aufbewahrungsfrist

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

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

5.5.3. Schutz der archivierten Daten

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

5.5.4. Sicherung der archivierten Daten

Alle elektronischen Archivdaten werden regelmäßig gesichert.

5.5.5. Anforderungen an den Zeitstempel der archivierten Daten

Archivierte Daten werden nicht mit Zeitstempel versehen.

5.5.6. Internes/externes Archivierungssystem

Alle Daten werden innerhalb der Räumlichkeiten der *GAD* eG archiviert. Es gibt keine externen Archivierungssysteme.

5.5.7. Verfahren zum Einholen und Verifizierung von Archivdaten

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

5.6. Schlüsselwechsel

Die Schlüsselpaare, welche die *GAD* zur Erbringung ihrer Zertifizierungsdienste für VR-Ident Zertifikate einsetzt, besitzen eine beschränkte Gültigkeitsdauer, die im zugeordneten *Zertifikat* angegeben ist. Sie werden rechtzeitig vor Ablauf ihrer Gültigkeit gewechselt. Insbesondere werden CA-Schlüssel frühzeitig gewechselt, so dass die Gültigkeitsdauer der von der *CA* ausgestellten VR-Ident Zertifikate nicht die Gültig-

keitsdauer des CA-Zertifikates übersteigt. Bei diesen regulären CA-Schlüsselwechseln erfolgt keine Sperrung des Zertifikates.

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

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

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

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

Bei einem Schlüsselwechsel der *Zertifizierungsstelle* werden entsprechende neue Schlüsselpaare erzeugt und für das neue Schlüsselpaar wird ein neues *Zertifikat* erzeugt. Nach dem Schlüsselwechsel werden die *privaten Schlüssel* des alten Schlüsselpaares vernichtet.

Bei einer bekannten oder vermuteten Kompromittierung des privaten Schlüssels gelten die Regelungen in Kapitel 5.7.3 (S. 29).

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*. Ein außerordentlicher Schlüssel eines Schlüssels einer VR-Ident *Zertifizierungsstelle*, die von einer externen *Root-CA* ausgestellt wurde, findet auch statt, falls das darüberliegende externe Root-CA-Zertifikat gesperrt wurde.

5.7. Business Continuity Management und Incident Handling

5.7.1. Prozeduren zu Incident Handling und zu Notfällen

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

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

5.7.2. Prozeduren bei Kompromittierung von Ressourcen

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

5.7.3. Prozeduren bei Kompromittierung von CA-Schlüsseln

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

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

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

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.

5.8. Einstellung der Zertifizierungsdienste

Im Fall, dass der *Zertifizierungsdienst* VR-Ident die Zertifizierungsdienste einstellt, werden alle Beteiligten benachrichtigt.

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

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

6. Technische Sicherheitsmaßnahmen

6.1. Erzeugung und Installation von Schlüsselpaaren

6.1.1. Erzeugung von Schlüsselpaaren

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

Das DS-Schlüsselpaar wird auf der Chipkarte unter Verwendung des Zufallszahlengenerators der Chipkarte generiert.

Die CSA- und KE-Schlüsselpaare werden in Hardware-Sicherheitsmodulen (*HSM*) generiert, die nach *FIPS 140-2* Level 4 (siehe Anhang mit allgemeinen Referenzen) evaluiert sind und im Rahmen der Personalisierung durch den Kartenherausgeber (DG VERLAG) auf die Karte geschrieben. Unmittelbar nach der Generierung werden die Schlüsselpaare wieder aus dem Hardware-Sicherheitsmodul (*HSM*) gelöscht.

Die Chipkarten gewährleisten, dass private Schlüssel nicht ausgelesen werden können und somit die Karte nicht verlassen. Die Anwendung von privaten Schlüsseln ist erst nach einer erfolgreichen *Authentisierung* möglich.

6.1.2. Übermittlung privater Schlüssel an den Zertifikatseigentümer

Die Auslieferung der *privaten Schlüssel* erfolgt durch die Auslieferung der Chipkarten an den Zertifikatseigentümern.

6.1.3. Übermittlung öffentlicher Schlüssel an den Zertifikatsaussteller

Im Zuge der Zertifikatserstellung liest der Webserver der *CA* die *öffentlichen Schlüssel* sicher aus der Chipkarte aus.

6.1.4. Übermittlung öffentlicher CA-Schlüssel an vertrauende Dritte

Die öffentlichen CA-Schlüssel können über den in Kapitel 2.1 (S. 6) beschriebenen öffentlichen *Verzeichnisdienst* oder über die Webseite http://www.vr-ident.de abgerufen werden. Die zugehörigen *Fingerprints* befinden sich ebenfalls dort.

6.1.5. Schlüssellängen

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

- 2048 bit für die "VR Ident Root CA 2010",
- 2048 bit für die "VR Ident Class 2 CA 2010",

Die Schlüssel der VR-Ident privat-Zertifikate besitzen folgende Längen:

- Die DS-Schlüssel von Karten mit Gültigkeits-Ablaufdatum ab 2013 sind 2048 bit lang.
- Die DS-Schlüssel von Karten mit Gültigkeits-Ablaufdatum bis einschließlich 2012 sind 1536 bit lang.
- Die CSA- und KE-Schlüssel von Karten mit Gültigkeits-Ablaufdatum ab 2013 sind 1984 bit lang.
- Die CSA- und KE-Schlüssel von Karten mit Gültigkeits-Ablaufdatum bis einschließlich 2012 sind 1024 bit lang.

6.1.6. Erzeugung und Prüfung der Schlüsselparameter

Nicht relevant. Für *RSA*-Schlüssel gibt es keine Parameter.

6.1.7. Verwendungszweck der Schlüssel

Die Nutzung der *privaten Schlüssel* für VR-Ident Zertifikate muss den Vorgaben im Kapitel 1.4.1 (S. 4) entsprechen.

Die genaue Bezeichnung des Verwendungszweckes des Schlüssels ist schlüsselabhängig und wird in den Zertifikatserweiterungsfeldern "Schlüsselverwendung" und "Erweiterte Schlüsselverwendung" vermerkt (siehe auch Kapitel 7.1 (S. 37)).

Die genaue Bezeichnung des Verwendungszweckes des privaten Schlüssels für CA-Zertifikate wird im Zertifikatserweiterungsfeld "Schlüsselverwendung" vermerkt (siehe auch Kapitel 7.1 (S. 37))

6.2. Schutz der privaten Schlüssels und der kryptographischen Module

6.2.1. Standards und Schutzmechanismen der kryptographischen Module

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

Die Chipkarten, die für die *VR-Bankkarten* verwendet werden, sind nach den Vorgaben der DK (Deutsche Kreditwirtschaft) bestätigt.

6.2.2. Aufteilung der Kontrolle über private Schlüsseln auf mehrere Personen

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

6.2.3. Hinterlegung privater Schlüssel

Private Schlüssel werden nicht hinterlegt.

6.2.4. Backup privater Schlüssel

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

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

6.2.5. Archivierung privater Schlüssel

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

6.2.6. Transfer privater Schlüssel

Private Schlüssel der *CA* sind in Hardware-Sicherheitsmodulen (*HSM*) in verschlüsselter Form gespeichert. Falls ein privater Schlüssel einer *CA* von einem Hardware-Sicherheitsmodul (*HSM*) zum anderen transportiert

werden soll (beispielsweise zwecks Recovery), so erfolgt der Schlüsseltransport ausschließlich in verschlüsselter Form.

Private Schlüssel der *Zertifikatseigentümer* werden mit den Karten durch den Kartenherausgeber sicher an den Zertifikatseigentümern ausgeliefert.

6.2.7. Speicherung privater Schlüssel

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

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

6.2.8. Methoden zur Aktivierung privater Schlüssel

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

Private Schlüssel der *Zertifikatseigentümer* werden durch die Eingabe einer *PIN* aktiviert. Es existieren zwei *PIN*: Die HBCI-PIN, die den CSA-Schlüssel und den KE-Schlüssel schützt, und die Signatur-PIN, die den DS-Schlüssel schützt.

Für die Erzeugung einer Signatur muss die Signatur-PIN vor jeder Verwendung des privaten DS-Schlüssels eingegeben werden. Sie wird unmittelbar nach Erzeugung einer Signatur automatisch deaktiviert.

Die privaten CSA- und KE-Schlüssel werden durch die Eingabe der HBCI-PIN aktiviert.

6.2.9. Methoden zur Deaktivierung privater Schlüssel

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

Private Schlüssel der Chipkarte werden jeweils durch die Unterbrechung der Stromversorgung der Chipkarte (beispielsweise beim Entfernen aus dem Kartenleser) deaktiviert.

6.2.10. Methoden zur Vernichtung privater Schlüssel

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

Zertifikatseigentümern wird empfohlen, gesperrte oder abgelaufene *VR-Bankkarten* (soweit noch verfügbar) durch Zerstören des Chips zu vernichten.

6.2.11. Bewertung kryptographischer Module

Siehe Kapitel 6.2.1 (S. 32).

6.3. Weitere Aspekte des Schlüsselmanagements

6.3.1. Archivierung öffentlicher Schlüssel

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

6.3.2. Verwendungsdauern von Zertifikaten und Schlüsselpaaren

Private Schlüssel der *CA* werden nach Ablauf ihres Zertifikates nicht mehr verwendet (siehe Kapitel 6.2.1 (S. 32)). Die Gültigkeitsdauer der CA-Zertifikate beträgt maximal 20 Jahre.

Die Gültigkeit der VR-Ident privat-Zertifikate beträgt in der Regel bis zu 4 Jahre, in Abhängigkeit der Kartengültigkeit und des Zeitpunktes der Beantragung der Zertifikate.

6.4. Aktivierungsdaten

6.4.1. Erzeugung und Installation von Aktivierungsdaten

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

Im Auslieferungszustand einer Chipkarte ist der private DS-Schlüssel durch eine sogenannte Transport-PIN geschützt. Diese wird anhand von Masterkeys abgeleitet, die im Hardware-Sicherheitsmodul (*HSM*) gespeichert sind, und im Rahmen der Personalisierung durch den Kartenherausgeber (DG VERLAG) auf die Chipkarten aufgebracht. Dabei werden auch die Fehlbedienungszähler der *PIN* irreversibel konfiguriert. Die Transport-PIN kann nur zur initialen Änderung der *PIN* verwendet werden. Im Rahmen der Erstellung und des Downloads der Zertifikate auf die Karte wird dem *Zertifikatseigentümer* die Transport-PIN anzeigt, und er kann die *PIN* so in eine Wirk-PIN ändern.

Im Auslieferungszustand einer Chipkarte sind der private CSA-Schlüssel und der private KE-Schlüssel durch eine Transport-PIN geschützt. Diese wird im Rahmen der Personalisierung durch den Kartenherausgeber (DG VERLAG) auf die Chipkarten aufgebracht. Dabei werden auch die Fehlbedienungszähler der *PIN* irreversibel konfiguriert. Vor der Beantragung von VR-Ident privat-Zertifikaten muss bereits ein entsprechender PIN-Brief an den *Zertifikatseigentümer* verschickt worden sein und die Transport-PIN muss in eine Wirk-PIN geändert worden sein, so dass er diese beiden Schlüssel nutzen kann. Der PIN-Brief wird separat zur Chipkarte versendet.

6.4.2. Schutz der Aktivierungsdaten

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

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

Die Signatur-PIN wird durch die folgenden Maßnahmen geschützt:

- Die *PIN* besteht aus mindestens 6 Stellen.
- Die Transport-PIN für die Nutzung des DS-Schlüssels muss vor der ersten Nutzung in eine Wirk-PIN geändert werden.
- Die Signatur-PIN kann nicht aus der Chipkarte ausgelesen werden.
- Für die Signatur-PIN ist auf der Chipkarte ein Fehlbedienungszähler installiert, der sicherstellt, dass der private DS-Schlüssel nach 3 aufeinanderfolgenden fehlerhaften Eingaben der *PIN* (ohne zwischenzeitliche

korrekte Eingabe) für die Benutzung gesperrt wird. Der Fehlbedienungszähler kann nicht mehr rückgesetzt werden.

Die HBCI-PIN wird durch die folgenden Maßnahmen geschützt:

- Die HBCI-PIN ist 6-stellig.
- Die Transport-PIN für die Nutzung des CSA- und des KE-Schlüssels muss vor der ersten Nutzung in eine Wirk-PIN geändert werden.
- Die HBCI-PIN kann nicht aus der Chipkarte ausgelesen werden.
- Für die HBCI-PIN ist auf der Chipkarte ein Fehlbedienungszähler installiert, der sicherstellt, dass der private CSA und der private KE-Schlüssel nach 3 aufeinanderfolgenden fehlerhaften Eingaben der *PIN* (ohne zwischenzeitliche korrekte Eingabe) für die Benutzung gesperrt wird. Der Fehlbedienungszähler kann nicht mehr rückgesetzt werden.

Darüber hinaus hat der Eigentümer einer VR-Bankkarte die Pflicht

- die *PIN* vertraulich und mit großer Sorgfalt zu behandeln,
- die Signatur-PIN unterschiedlich zur HBCI-PIN zu setzen,
- die *PIN* sofort zu ändern, sobald der Verdacht besteht, dass diese Dritten bekannt geworden sein könnten.

Zu keiner Zeit werden Mitarbeiter des Zertifizierungsdienstes VR-Ident oder der VR-Bank den Zertifikatseigentümern nach seiner HBCI- oder Signatur-PIN fragen.

6.4.3. Weitere Aspekte von Aktivierungsdaten

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

6.5. Sicherheitsmaßnahmen für Computer

6.5.1. Spezielle Anforderungen zur Computersicherheit

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

- Auf den IT-Systemen sind nur die notwendigen Anwendungen installiert.
- Die IT-Systeme verfügen nur die für die entsprechende Aufgabe notwendigen Kommunikationsschnittstellen. Insbesondere sind die IT-Systeme nur in die für ihre Aufgabe notwendigen Netzwerkbereiche integriert.
- Die IT-Systeme sind in abschließbaren Serverschränken im Rechenzentrum der *GAD* eG untergebracht.
- Der Zugriff auf die IT-Systeme ist auf das für den Zertifizierungsbetrieb notwendige Maß beschränkt. Insbesondere werden IT-Systeme nur durch autorisierte Administratoren verwaltet.
- Der Zugriff zu den sicherheitskritischen IT-Systemen wie beispielsweise zu den Hardware-Sicherheitsmodulen (*HSM*) ist nur im 4-Augen-Prinzip möglich.
- IT-Systeme mit hohen Verfügbarkeitsanforderungen (wie beispielsweise der VR-Ident *Verzeichnisdienst*) sind redundant ausgelegt, so dass bei Ausfall eines IT-Systems der Dienst erhalten bleibt.
- Mittels unterbrechungsfreier Stromversorgungen werden Schwankungen in der Stromversorgung ausgeglichen und Stromausfälle bis zu einer Dauer von mehreren Stunden überbrückt.

- Auf den IT-Systemen dürfen nur nach Viren geprüfte Datenträger verwendet werden.
- Die IT-Systeme werden durch permanentes Monitoring überwacht.
- Sicherheitskritische Ereignisse auf den IT-Systemen werden protokolliert.

6.5.2. Bewertung der Computersicherheit

Eine formale Evaluierung der Systemsicherheit wurde für die *Hardware-Sicherheitsmodule* (*HSM*, siehe Kapitel 6.2.1 (S. 32)) durchgeführt.

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

6.6. Technische Kontrollen des Software-Lebenszyklus

6.6.1. Systementwicklungsmaßnahmen

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

6.6.2. Sicherheitsmanagement

Im Sicherheitskonzept der *GAD* sind die Verantwortlichkeiten und Prozesse des Sicherheitsmanagements klar definiert.

6.6.3. Maßnahmen zur Kontrolle des Software-Lebenszyklus

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

6.7. Maßnahmen zur Netzwerksicherheit

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

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

6.8. Zeitstempel

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

7. Profile

7.1. Zertifikatsprofile

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

7.1.1. Versionsnummern

"VR Ident Root CA 2010" Zertifikat

Das "VR Ident Root CA 2010" *Zertifikat* entspricht dem Zertifikatsprofil *X.509* in der Version 3, sowie *RFC* 5280 und Common *PKI* (siehe Anhang mit allgemeinen Referenzen). In den Basisfeldern enthält es folgende Informationen:

Tabelle 7.1. "VR Ident Root CA 2010" Zertifikat

Zertifikatsfeld	Inhalt
Version	V 3
Seriennummer	Eindeutiger Wert, 01
Signaturalgorithmus	sha1RSA
Aussteller (Issuer DN)	CN = VR IDENT ROOT CA 2010 OU = VR IDENT O = GAD EG C = DE
Gültig ab (not before)	Dienstag, 20. Oktober 2009 13:05:18
Gültig bis (not after)	Mittwoch, 1. Januar 2031 00:59:59
Antragsteller (Subject DN)	CN = VR IDENT ROOT CA 2010 OU = VR IDENT O = GAD EG C = DE
Öffentlicher Schlüssel	Kodierter Wert des Schlüssels, RSA 2048 bit
Fingerprint-Algorithmus	sha1
Fingerprint (sha1)	1e a6 4c cb f6 05 42 7e 99 64 65 08 48 e4 5e e5 2c 11 bd 6d

"VR Ident Class 2 CA 2010" Zertifikat

Das "VR Ident Class 2 CA 2010" *Zertifikat* entspricht dem Zertifikatsprofil *X.509* in der Version 3, sowie *RFC* 5280 und Common *PKI* (siehe Anhang mit allgemeinen Referenzen). In den Basisfeldern enthält es folgende Informationen:

Tabelle 7.2. "VR Ident Class 2 CA 2010" Zertifikat

Zertifikatsfeld	Inhalt
Version	V 3
Seriennummer	Eindeutiger Wert, 03
Signaturalgorithmus	sha1RSA
Aussteller (Issuer DN)	CN = VR IDENT ROOT CA 2010 OU = VR IDENT O = GAD EG

	C = DE
Gültig ab (not before)	Donnerstag, 22. Oktober 2009 14:24:08
Gültig bis (not after)	Dienstag, 1. Januar 2019 00:59:59
Antragsteller (Subject DN)	CN = VR IDENT CLASS 2 CA 2010 OU = VR IDENT O = GAD EG C = DE
Öffentlicher Schlüssel	Kodierter Wert des Schlüssels, RSA 2048 bit
Fingerprint-Algorithmus	sha1
Fingerprint (sha1)	9f fd 24 40 a1 1b 55 c9 2a 8f ac 1e 21 aa b1 92 6c 7c d9 20

VR-Ident privat-Zertifikate

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

Tabelle 7.3. VR-Ident privat-Zertifikate

Zertifikatsfeld	Inhalt
Version	V 3
Seriennummer	Eindeutiger Wert
Signaturalgorithmus	sha1RSA
Aussteller (Issuer)	CN = VR IDENT CLASS 2 CA 2010 OU = VR IDENT O = GAD EG C = DE
Gültig ab (not before)	Datum und Uhrzeit
Gültig bis (not after)	Datum und Uhrzeit
Antragsteller (Subject DN)	Subject DN: CN = <Titel/Grad Vorname Name> serialNumber= <Eindeutige Referenznummer der Signaturkarte> distinuishedNameQualifier = <Eindeutige PKI-interne Identifikationsnummer des Zertifikatseigentümern> C = DE
Öffentlicher Schlüssel	Kodierter Wert des Schlüssels

7.1.2. Zertifikatserweiterungen

"VR Ident Root CA 2010" Zertifikat

Die Erweiterungen des "VR Ident Root CA 2010" Zertifikats sind in der folgenden Tabelle dargestellt:

Tabelle 7.4. Erweiterungen des "VR Ident Root CA 2010" Zertifikats

Erweiterungen	
Stelleninformationszugriff (AuthorityInfoAccess)	Zugriffsmethode = OCSP-Responder des Zertifikats (1.3.6.1.5.5.7.48.1) URL=http://ocsp.vr-ident.de/gtnocsp/OCSPResponder/VR%20Ident%20Root%20CA%202010
Stellenschlüsselkennung (AuthorityKeyIdentifier)	50 52 4f 44 2e 47 54 4e 2e 56 52 52 4f 4f 54 43 41 2e 53 49 47 47 45 4e 52 53 2e 30 30 30 30 33 30 30 30

Aktuellste Sperrliste (FreshestCRL)	Vollständiger Name: URL=http://www.vr-ident.de/gtndlt/DeltaCRLResponder/VR%20Ident%20Root%20CA%202010
Sperrlistenverteilungspunkte (CRLDistributionPoints)	Vollständiger Name: http://www.vr-ident.de/gtncrl/CRLResponder/VR%20Ident%20Root%20CA%202010
Schlüsselkennung des Antragstellers (SubjectKeyIdentifier)	50 52 4f 44 2e 47 54 4e 2e 56 52 52 4f 4f 54 43 41 2e 53 49 47 47 45 4e 52 53 2e 30 30 30 30 33 30 30 30
Kritische Erweiterungen	
Schlüsselverwendung (KeyUsage)	Digitale Signatur, Zertifikatssignatur, Offline Signieren der Zertifikatssperrliste, Signieren der Zertifikatssperrliste (86)
Basiseinschränkungen (BasicConstraints)	CA:TRUE Einschränkung der Pfadlänge=Keine

"VR Ident Class 2 CA 2010" Zertifikat

Die Erweiterungen des "VR Ident Class 2 CA 2010" Zertifikats sind in der folgenden Tabelle dargestellt:

Tabelle 7.5. Erweiterungen des "VR Ident Class 2 CA 2010" Zertifikats

Erweiterungen	
Stelleninformationszugriff (AuthorityInfoAccess)	Zugriffsmethode = OCSP-Responder des Zertifikats (1.3.6.1.5.5.7.48.1) Alternativer Name: URL=http://ocsp.vr-ident.de/gtnocsp/OCSPResponder/VR%20Ident%20ROOT%20CA%202010
Stellenschlüsselkennung (AuthorityKeyIdentifier)	50 52 4f 44 2e 47 54 4e 2e 56 52 52 4f 4f 54 43 41 2e 53 49 47 47 45 4e 52 53 2e 30 30 30 30 33 30 30 30
Aktuellste Sperrliste (FreshestCRL)	Vollständiger Name: URL=http://www.vr-ident.de/gtndlt/DeltaCRLResponder/VR%20Ident%20ROOT%20CA%202010
Sperrlistenverteilungspunkte (CRLDistributionPoints)	Vollständiger Name: http://www.vr-ident.de/gtncrl/CRLResponder/VR%20Ident%20ROOT%20CA%202010
Schlüsselkennung des Antragstellers (SubjectKeyIdentifier)	50 52 4f 44 2e 47 54 4e 2e 43 4c 41 53 53 32 43 41 2e 53 49 47 47 45 4e 52 53 2e 30 30 30 30 31 38 30 30
Kritische Erweiterungen	
Schlüsselverwendung (KeyUsage)	Digitale Signatur, Zertifikatssignatur, Offline Signieren der Zertifikatssperrliste, Signieren der Zertifikatssperrliste (86)
Basiseinschränkungen (BasicConstraints)	CA:TRUE Einschränkung der Pfadlänge=Keine

VR-Ident privat-Zertifikate

Die verwendeten Erweiterungen unterscheiden sich je nach Generation der Karte, für die sie ausgestellt wird. Ein Hinweis hierzu ist an den jeweiligen Stellen zu finden.

CSA-Zertifikate

Die Erweiterungen der CSA-Zertifikate sind in der folgenden Tabelle dargestellt:

Tabelle 7.6. : Erweiterungen der CSA-Zertifikate

Erweiterungen	
Stelleninformationszugriff (AuthorityInfoAccess)	Bei Karten, die bis mindestens 2013 gültig sind: Zugriffsmethode = OCSP-Responder des Zertifikats (1.3.6.1.5.5.7.48.1)

	Alternativer Name: URL=http://ocsp.vr-ident.de/gtnocsp/OCSPResponder/VR%20Ident%20Class%202%20CA%202010 Bei Karten, die bis spätestens 2012 gültig sind, ist diese Erweiterung nicht vorhanden
Stellenschlüsselkennung (AuthorityKeyIdentifier)	54 45 53 54 2e 47 54 4e 2e 43 4c 41 53 53 32 43 41 2e 53 49 47 47 45 4e 52 53 2e 30 30 30 30 31 38 30 30
Zertifikatsrichtlinie (CertificatePolicies)	Bei Karten, die bis mindestens 2013 gültig sind, die OID der CP: 1.3.6.1.4.1.17696.4.1 Bei Karten, die bis spätestens 2012 gültig sind, ist diese Erweiterung nicht vorhanden
Sperrlistenverteilungspunkte (CRLDistributionPoints)	Vollständiger Name: URL=http://www.vr-ident.de/gtncrl/CRLResponder/VR%20Ident%20Class%202%20CA%202010
Alternativer Antragstellername (SubjectAltNames)	rfc822Name: E-Mail Adresse des Zertifikatseigentümers (optional)
Erweiterte Schlüsselverwendung (ExtendedKeyUsage)	clientAuth
Kritische Erweiterungen	
Schlüsselverwendung (KeyUsage)	digitalSignature

DS-Zertifikate

Die Erweiterungen der DS-Zertifikate sind in der folgenden Tabelle dargestellt:

Tabelle 7.7. : Erweiterungen der DS-Zertifikate

Erweiterungen	
Stelleninformationszugriff (AuthorityInfoAccess)	Zugriffsmethode = OCSP-Responder des Zertifikats (1.3.6.1.5.5.7.48.1) Alternativer Name: URL=http://ocsp.vr-ident.de/gtnocsp/OCSPResponder/VR%20Ident%20Class%202%20CA%202010
Stellenschlüsselkennung (AuthorityKeyIdentifier)	54 45 53 54 2e 47 54 4e 2e 43 4c 41 53 53 32 43 41 2e 53 49 47 47 45 4e 52 53 2e 30 30 30 30 31 38 30 30
Zertifikatsrichtlinie (CertificatePolicies)	OID der CP: 1.3.6.1.4.1.17696.4.1
Sperrlistenverteilungspunkte (CRLDistributionPoints)	Vollständiger Name: URL=http://www.vr-ident.de/gtncrl/CRLResponder/VR%20Ident%20Class%202%20CA%202010
Alternativer Antragstellername (SubjectAltNames)	rfc822Name: E-Mail Adresse des Zertifikatseigentümers (optional)
Erweiterte Schlüsselverwendung (ExtendedKeyUsage)	eMailProtection
Kritische Erweiterungen	
Schlüsselverwendung (KeyUsage)	nonRepudiation, digitalSignature

KE-Zertifikate

Die Erweiterungen der KE-Zertifikate sind in der folgenden Tabelle dargestellt:

Tabelle 7.8. : Erweiterungen der KE-Zertifikate

Erweiterungen	
Stelleninformationszugriff (AuthorityInfoAccess)	Bei Karten, die bis mindestens 2013 gültig sind: Zugriffsmethode = OCSP-Responder des Zertifikats (1.3.6.1.5.5.7.48.1) Alternativer Name: URL=http://ocsp.vr-ident.de/gtnocsp/OCSPResponder/VR%20Ident%20Class%202%20CA%202010 Bei Karten, die bis spätestens 2012 gültig sind, ist diese Erweiterung nicht vorhanden
Stellenschlüsselkennung (AuthorityKeyIdentifier)	54 45 53 54 2e 47 54 4e 2e 43 4c 41 53 53 32 43 41 2e 53 49 47 47 45 4e 52 53 2e 30 30 30 30 31 38 30 30
Zertifikatsrichtlinie (CertificatePolicies)	Bei Karten, die bis mindestens 2013 gültig sind, die OID der CP: 1.3.6.1.4.1.17696.4.1 Bei Karten, die bis spätestens 2012 gültig sind, ist diese Erweiterung nicht vorhanden
Sperrlistenverteilungspunkte (CRLDistributionPoints)	Vollständiger Name: URL=http://www.vr-ident.de/gtncrl/CRLResponder/VR%20Ident%20Class%202%20CA%202010
Alternativer Antragstellername (SubjectAltNames)	rfc822Name: E-Mail Adresse des Zertifikatseigentümers (optional)
Erweiterte Schlüsselverwendung (ExtendedKeyUsage)	eMailProtection
Kritische Erweiterungen	
Schlüsselverwendung (KeyUsage)	keyEncipherment, dataEncipherment

7.1.3. Algorithmus Bezeichner (OID)

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

7.1.4. Namensformen

Siehe Kapitel 3.1.1.

7.1.5. Nutzung von Erweiterungen zur Namensbeschränkung (Name Constraints)

Erweiterungen zur Namensbeschränkung werden nicht verwendet.

7.1.6. Bezeichner für Zertifizierungsrichtlinien (OID)

Der *Object Identifier* (OID) für die vorliegende Policy ist in Kapitel 1.2 (S. 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 *CRL* (Sperrlisten) verwenden die nachfolgenden Erweiterungen (Extensions):

Tabelle 7.9. : Erweiterungen der CRL (Sperrliste)

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

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

Tabelle 7.10. : Erweiterungen der Einträge der CRL (Sperrliste)

Erweiterungen	
Seriennummer (SerialNumber)	Seriennummer des gesperrten Zertifikats
Sperrdatum	Datum und Uhrzeit der Sperrung

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

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

Tabelle 7.11. : Erweiterungen der Einträge der CRL (Sperrliste)

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

7.2.3. Weitere Eigenschaften der Sperrlisten

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

7.3. OCSP-Profile

Die von der VR-Ident PKI verwendeten OCSP Profile entsprechen dem Standard RFC 2560 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* 2560 in der Version 1 und ist konform zum Common *PKI* Standard (siehe Anhang mit allgemeinen Referenzen).

7.3.2. OCSP-Erweiterungen

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

Tabelle 7.12. : Zulässige Erweiterungen der Anfragen (OCSP-Requests)

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

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

Tabelle 7.13. : Zulässige Erweiterungen der Antworten (OCSP-Response)

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

7.3.3. Weitere Eigenschaften der OCSP-Anfragen und Antworten

Anfragen (OCSP-Requests):

- Anfragen (OCSP-Requests) müssen nicht signiert sein, signierte Anfragen werden aber unterstützt. Die Signatur wird hierbei ignoriert.
- Das Feld "requestorName" kann beliebig gesetzt sein (auch leer).
- Das Feld "CertID" muss mit *SHA*-1 berechnet worden sein.

Antworten (OCSP-Response):

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

8. Revisionen und andere Bewertungen

8.1. Häufigkeiten von Revisionen

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

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

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

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

8.2. Identität und Qualifikation des Auditors

Der *Zertifizierungsdienst* VR-Ident wird entscheiden, ob die Audits durch einen externen Auditor durchgeführt werden oder durch einen Mitarbeiter der *GAD* eG (Innenrevision).

Für die Auditoren gelten folgende Qualifizierungsvoraussetzungen:

- Technisches *PKI* Know-how.
- Vertraut sein mit den entsprechenden Normen und Standards (ISO 27001, ETSI 102 042, IDW PS 951 und andere).

8.3. Beziehungen zwischen Auditor und zu untersuchender Partei

Der Auditor ist vertraglich an die *GAD* eG gebunden, entweder als Mitarbeiter oder durch einen Vertrag.

Der Auditor ist in keiner Weise an der Leitung, Administration und Betrieb des Zertifizierungsdienstes VR-Ident beteiligt. Außerdem ist der Auditor weder direkt oder indirekt vom *Zertifizierungsdienst* VR-Ident oder seinen Mitarbeitern abhängig.

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,
- 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 *GAD* eG berichtet.

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

8.6. Veröffentlichung der Ergebnisse

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

9. Weitere geschäftliche und rechtliche Regelungen

9.1. Gebühren

9.1.1. Gebühren für die Ausstellung und Erneuerung von Zertifikaten

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

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.

Die Gebühren für andere Dienstleistungen ergeben sich aus dem Preisverzeichnis der VR-Bank.

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 *GAD* als Betreiber des VR-Ident verfügt über eine entsprechende Deckungsvorsorge (Versicherung), damit sie ihren gesetzlichen Verpflichtungen zum Ersatz von Schäden nachkommen kann, die dadurch entstehen, dass ihre Produkte oder sonstige technische Sicherungseinrichtungen versagen.

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. 47) 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 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 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 widerrufliches Einverständnis, dass der *Zertifizierungsdienst* VR-Ident seine personenbezogenen Daten zum Zweck der Zertifizierungsdienstleistungen verarbeitet.

9.4.6. Weitergabe von Informationen an Ermittlungsinstanzen oder Behörden

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

Mindestens eine der folgenden Voraussetzungen muss hierfür erfüllt sein:

- Es muss für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung erforderlich sein.
- Es muss für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder der Finanzbehörden erforderlich sein.

- Es muss durch Gerichte im Rahmen anhängiger Verfahren nach Maßgabe der hierfür geltenden Bestimmungen angeordnet worden sein.

9.4.7. Sonstige Offenlegungsgründe

Keine weiteren Offenlegungsgründe.

9.5. Geistiges Eigentum und dessen Rechte

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

9.6. Gewährleistung, Sorgfalts- und Mitwirkungspflichten

9.6.1. Verpflichtung der Zertifizierungsstelle

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

9.6.2. Verpflichtung der Registrierungsstelle

Als *Registrierungsstelle* für VR-Ident Zertifikate sichert die *GAD* eG 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 Kunde beziehungsweise der *Zertifikatseigentümer* haben insbesondere folgende Pflichten:

- Die vereinbarten Preise sind fristgerecht zu zahlen.
- Die VR-Ident Zertifikate sind nur bestimmungsgemäß und nicht missbräuchlich zu benutzen.
- Bei einer Nutzung eines VR-Ident Zertifikates mit Auslandsbezug sind die geltenden nationalen und internationalen Ausfuhr- und Nutzungsbestimmungen zu beachten.
- Die den VR-Ident Zertifikaten zuzuordnenden *privaten Schlüssel* sind geheim zu halten und sicher vor unbefugten Zugriffen aufzubewahren.
- Mängel, Schäden oder sonstige Störungen sind unverzüglich dem *Zertifizierungsdienst* VR-Ident anzuzeigen.
- Bei Verlust oder Verdacht der Kompromittierung des dem VR-Ident *Zertifikat* zuzuordnenden privaten Schlüssels ist unverzüglich eine Sperrung des entsprechenden VR-Ident Zertifikates zu veranlassen.
- Ebenfalls hat der Kunde eine Sperrung seines VR-Ident Zertifikates zu veranlassen, wenn die im *Zertifikat* enthaltenden Daten nicht mehr den Daten zum Zertifizierungszeitpunkt übereinstimmen.
- Er muss sich regelmäßig über eventuelle Änderungen bezüglich sicherheitsrelevanter Aspekte oder-Verfahren auf der Webseite http://www.vr-ident.de informieren.

9.6.4. Verpflichtung vertrauender Dritte

Vertrauende Dritte sind dazu verpflichtet, gemäß den in Kapitel 4.5.2 (S. 14) und Kapitel 4.9.6 beschriebenen Regeln vorzugehen.

9.6.5. Verpflichtung anderer Teilnehmer

Keine Verpflichtungen für andere Teilnehmer.

9.7. Haftungsausschluss

Trotz größter Sorgfalt bei der Erstellung dieser Dokumentation kann die *GAD* eG die Möglichkeit nicht vollständig ausschließen, dass Fehler in den hier beschriebenen Prozeduren enthalten sind. Für diesen Fall lehnt die *GAD* eG jegliche Haftung ab.

9.8. Haftungsbeschränkungen

9.8.1. Haftung des Zertifizierungsdienstes VR-Ident

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

So bestätigt der *Zertifizierungsdienst* VR-Ident daher mit den VR-Ident privat-Zertifikaten nur, dass jemand zum angegebenen Zeitpunkt die geforderten Identifikationsnachweise vorgelegt hat und die entsprechenden Angaben in den VR-Ident privat-Zertifikaten darauf gestützt aufgenommen wurden.

Im Übrigen gelten die Allgemeinen Geschäftsbedingungen der VR-Bank und die "Sonderbedingungen für den *Zertifizierungsdienst* VR-Ident".

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 Zertifizierungsdienstes (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 des 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, das Dokument jederzeit zu ändern oder zu ergänzen.

Dies gilt insbesondere, um die Leistung zu verbessern oder an technische Entwicklungen anzupassen und wenn dies aufgrund von Veränderungen und/oder Ergänzungen notwendig erscheint. Die Revision und Veröffentlichung unterliegt der ausschließlichen Verantwortung des Zertifizierungsdienstes VR-Ident.

9.12.2. Benachrichtigungsverfahren und Veröffentlichungsperioden

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

http://www.vr-ident.de

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

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

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

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

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

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

9.13. Schiedsverfahren

Entfällt.

9.14. Anwendbares Recht

Anwendbar ist ausschließlich deutsches Recht. Es gelten die Allgemeinen Geschäftsbedingungen der *GAD* eG.

9.15. Konformität mit anwendbarem Recht

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, 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

Entfällt.

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/fips1402.pdf
[04]	PKCS#10: Certification Request Syntax Standard. RSA Laboratories. Version 1.7. 2000.	http://tools.ietf.org/html/rfc2986
[05]	RFC 2560, X.509 Internet Public Key Infrastructure – Online certificate Status Protocol – OCSP. M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, 1999.	http://www.ietf.org/rfc/rfc2560.txt
[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]	TS 102 042: Policy requirements for certification authorities issuing public key certificates, European Telecommunications Standards Institute (ETSI), Version 2.1.2, 2010	ts_102042v020102p.pdf[3]
[09]	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
[10]	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
[11]	CA-Certificate Policy for Cybertrust Certification Services	http://cybertrust.omniroot.com/repository/
[12]	Trust Service Principles and Criteria for Certification Authorities Version 2.0	http://www.webtrust.org/homepage-documents/item54279.pdf
[13]	BASELINE REQUIREMENTS FOR THE ISSUANCE AND MANAGEMENT OF PUBLICLY-TRUSTED CERTIFICATES, V.1.0	http://http://www.webtrust.org/homepage-documents/item69267.pdf
[14]	BASELINE REQUIREMENTS FOR THE ISSUANCE AND MANAGEMENT OF PUBLICLY-TRUSTED CERTIFICATES, V.1.1	http://www.webtrust.org/homepage-documents/item72056.pdf
[15]	GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES Version 1.3	http://www.webtrust.org/homepage-documents/item54281.pdf
[16]	WEBTRUST® FOR CERTIFICATION AUTHORITIES – EXTENDED VALIDATION AUDIT CRITERIA Version 1.4	http://www.webtrust.org/homepage-documents/item72055.pdf
[17]	GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES	https://www.cabforum.org/EV_Certificate_Guidelines.pdf
[18]	Mozilla CA Certificate Inclusion Policy (Version 2.1)	http://www.mozilla.org/projects/security/certs/policy/InclusionPolicy.html

A.2. Literaturverzeichnis mit VR-Ident Dokumenten

[Nr.]	Dokument	Link
[01]	Certificate Policy (CP) für VR-Ident privat-Zertifikate	http://www.vr-ident.de

[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://www.etsi.org/deliver/etsi_ts/102000_102099/102042/02.01.02_60/ts_102042v020102p.pdf

Referenzen

[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 GAD	http://www.vr-ident.de
[11]	Nutzungsbedingungen für VR-Ident SMIME-Zertifikate aus dem Zertifizierungsdienst VR-Ident der GAD	http://www.vr-ident.de

Glossar

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

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.
Distinguished Name	Namensform nach X.501. Ein DN besteht aus verschiedenen Attributen und entsprechenden Werten und soll eine Entität eindeutig kennzeichnen. Die wichtigsten Attribute in dieser Richtlinie sind CommonName (cn), Organization (o), Organizational Unit (ou) und Country (c).
DMZ	Demilitarisierte Zone – logische Zone eines Netzwerkes zwischen dem öffentlichen Netz und dem internen Netz.
DN	Abkürzung für Distinguished Name.
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.
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.
GAD	Die GAD mit Firmensitz in Münster ist IT-Dienstleister, Rechenzentrum und Softwarehaus für 430 Volks- und Raiffeisenbanken sowie rund 20 Privat- und Spezialbanken. Eingebunden in die genossenschaftliche FinanzGruppe verfügt die GAD 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.
Hardware-Sicherheitsmodule	Geräte zur sicheren Speicherung und Anwendung kryptographischer Schlüssel. Im Unterschied zu Chipkarten besitzen Hardware-Sicherheitsmodule (HSM) meist eine eigene Stromversorgung und implementieren oft aufwendige Sicherheitsmechanismen wie ein sicheres Key-Backup von Schlüsseln, die Protokollierung sicherheitsrelevanter Ereignisse oder ein rollenbasiertes Zugriffskonzept.
Hashwert	Mit Hilfe einer Hashfunktion, wird aus beliebigen Daten ein (praktisch) eindeutiger String konstanter Länge berechnet, der als Prüfsumme verwendet werden kann. Dieser String wird als Hashwert oder auch Fingerprint bezeichnet.
HSM	Abkürzung für Hardware Sicherheitsmodul .
HTTP	Hypertext Transfer Protocol – besonders im Internet verbreitetes Kommunikationsprotokoll.
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..
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.
Registrierungsstelle	Stelle eines Zertifizierungsdienstes, welche die Anträge zur Ausstellung oder Sperrung von Zertifikaten erfasst und die Antragsteller identifiziert werden.
RFC	Request for Comment – Dokumententyp der Internet Engineering Task Force (IETF), in der diese Standards vorschlägt und veröffentlicht.
Rollenträger	Mitarbeiter, die im Zertifizierungsdienst VR-Ident beschäftigt sind. Es werden Zuverlässigkeitsprüfungen durchgeführt. Rollenträger die sicherheitskritische Aufgaben durchführen, haben bei der Ernennung zum Rollenträger ein Führungszeugnis vorgelegt.
Root-CA	Oberste Zertifizierungsinstanz einer Zertifizierungshierarchie. Das Zertifikat der Root-CA wird von ihr selbst signiert und muss den Teilnehmern der PKI auf eine vertrauenswürdige Weise (beispielsweise offline) zugänglich gemacht werden. Man nennt diese Instanz auch "Wurzel-Zertifizierungsinstanz".
RSA	Asymmetrisches Kryptoverfahren für Verschlüsselung und digitale Signatur, benannt nach Rivest, Shamir, Adleman
Schlüssel- und Zertifikatserneuerung	Die Ersetzung eines Zertifikates durch ein Zertifikat mit neuer Gültigkeitsdauer und für einen neuen öffentlichen Schlüssel aber sonst unveränderten Inhaltsdaten. In RFC 3647 "certificate re-key" genannt.
SHA	Vom US-amerikanischen Standardisierungsinstitut normierte Hashfunktion. Der SHA-1 mit 160 Bit langen Hash- beziehungsweise Ausgabewerten gilt heute nicht mehr

	als sicher. Daher wird möglichst der Einsatz von Hashfunktionen der sogenannten SHA-2 Familie (SHA-256, SHA-384 und SHA-512 - wobei die angefügte Zahl jeweils die Länge des Hash- beziehungsweise des Ausgabewerts in bit angibt) empfohlen.
Sperrdienst	Dienst innerhalb der Zertifizierungsdienste über den Zertifikate gesperrt werden können.
Sperrliste	Liste, in der ein Anbieter eines Zertifizierungsdienstes die Sperrinformation der von ihm ausgestellten und noch nicht abgelaufenen Zertifikate veröffentlicht (siehe auch CRL).
Sperrmitarbeiter	Rolle der Person, welche die Sperrung von Zertifikaten in der PKI beziehungsweise der Karten im Bankensystem durchführt.
Sperrstatus	Status eines Zertifikates bezüglich Sperrung.
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 GAD eG 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.
X.501	Von der ITU definierter Standard, der die Struktur von Verzeichnissen und entsprechende Namensformen zur Identifizierung der Objekte in Verzeichnissen festlegt.
X.509	Von der ITU definierter Standard, der unter anderem die heute überwiegend verwendeten Datenformate für Zertifikate und Sperrlisten definiert
Zertifikat	Eine elektronische Bescheinigung, mit der ein öffentlicher Signaturschlüssel dem Zertifikatseigentümer zugeordnet wird und dessen Identität bestätigt wird. Ein Zertifikat enthält Angaben zum Eigentümer, zum Aussteller und zur Nutzung des Zertifikates sowie den öffentlichen Schlüssel des Eigentümers. Außerdem enthält das Zertifikat eine digitale Signatur, welche die Authentizität und Integrität der im Zertifikat enthaltenen Daten sicherstellt. Eine Variante sind Attributzertifikate, die keinen öffentlichen Schlüssel des Eigentümers enthalten.
Zertifikats-Downloadserver	Server, bei dem die Zertifikatserstellung über ein Webinterface angestoßen wird. Der Zertifikats-Downloadserver authentisiert die VR-Bankkarte und den Antragsteller, liest die öffentlichen Schlüssel aus, stellt die Zertifikatsdaten zusammen, lässt das Zertifikat durch die CA ausstellen, und schreibt es auf die VR-Bankkarte.
Zertifikatseigentümer	Entität, für die das Zertifikat ausgestellt wird. Der Zertifikatseigentümer ist im Zertifikat als "Subject" eingetragen.
Zertifikatsmodifizierung	Die Ersetzung eines Zertifikates durch ein Zertifikat mit veränderten Inhaltsdaten und für einen neuen öffentlichen Schlüssel. In RFC 3647 "certificate update" genannt.

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.