Certificate Policy (CP)

VR-Ident privat-Zertifikate

GAD
IT für Banken

Certificate Policy (CP)

VR-Ident privat-Zertifikate

Version:	Version 2.01.00, Freigegeben
Zielgruppe:	Nutzer und Besitzer von VR-Ident privat-Zertifikaten
Datum/Uhrzeit:	02.04.2014 / 13:29 Uhr

Gegenüber der vorherigen Ausgabe wurden folgende Änderungen vorgenommen:

Nummer	Datum	Inhalt / Änderungen
2.0	31.07.2012	Umwandlung der Winword Version 1.4 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	26.10.2012	Kapitel 6.3.x, 6.4.x: Unterkapitel mit Hinweis auf CPS aufgenommen
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 1.2: 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

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

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

Inhaltsverzeichnis

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 eine "*Certificate Policy*" (*CP*) für den *Zertifizierungsdienst* VR-Ident für VR-Ident privat-Zertifikate.

Inhalt und Aufbau der dieser *CP* (*Certificate Policy*) orientieren sich an der *RFC* 3647. Im Dokument "VR-Ident Certification Practice Statement für VR-Ident privat-Zertifikate" sind detaillierte Informationen zur Umsetzung der Vorgaben des vorliegenden Dokuments enthalten (siehe Anhang mit VR-Ident Referenzen).

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: 1.3.6.1.4.1.17696.4.1.1.3.2

Die Dokumentenbezeichnung für die vorliegende CP lautet: "VR-Ident Certificate Policy (CP) 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 stellt im Sinne dieser *CP* (*Certificate Policy*) die *Zertifizierungsstelle* dar, welche VR-Ident privat-Zertifikate für die *VR-Bankkarten* (für CSA-, DS- und KE-Schlüssel) ausstellt. Für die genannten Zertifikatstypen verwendet die *Zertifizierungsstelle* eine Zertifizierungsinstanz. Hierbei handelt es sich um eine logische Einheit, die jeweils einem oder mehreren Schlüsselpaaren zur Signierung der Zertifikate zugeordnet ist.

Die Zertifizierungsinstanz, welche die VR-Ident privat-Zertifikate ausstellt, erhält die Zertifikate zu ihren Signaturschlüsseln wiederum von einer übergeordneten *Root-CA*, welche ebenfalls vom *Zertifizierungsdienst* VR-Ident betrieben wird.

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

1.3.2. Registrierungsinstanzen

Die *Registrierungsstelle* für VR-Ident privat-Zertifikate wird durch die VR-Bank Filialen und Systeme der *VR-Banken* dargestellt. Diese registrieren und identifizieren die Zertifikatsbewerber, nehmen Zertifizierungsanträge entgegen und veranlassen unter bestimmten Umständen die Sperrung der Zertifikate. Details sind im CPS (Certification Practice Statement) für VR-Ident privat-Zertifikate festgelegt (Anhang mit VR-Ident Referenzen).

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

1.3.5. Andere Teilnehmer

Keine.

1.4. Anwendung von Zertifikaten

1.4.1. Zulässige Anwendung von Zertifikaten

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

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. 11)) 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. 3) 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. 3) 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

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

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

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

2.2. Veröffentlichung von Zertifikatsinformationen

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

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

Das vorliegende Richtliniendokument wird im Internet veröffentlicht.

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

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. 35) 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 Namen der *Zertifikatseigentümer* in den von der *Zertifizierungsdienst* VR-Ident ausgestellten VR-Ident Zertifikate sind sogenannte DistinguishedNames nach *X.501* und im Attribut subject des Zertifikats enthalten.

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

3.1.2. Anforderung an die Bedeutung von Namen

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

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

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

3.1.3. Anonymität und Pseudonyme für Zertifikatseigentümer

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

3.1.4. Regeln zur Interpretation verschiedener Namensformen

Im Namen dürfen ausschließlich die folgenden Zeichen verwendet werden:

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

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

3.1.5. Eindeutigkeit von Namen

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

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

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

3.2.2. Authentisierung von Organisationen

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

sierung 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*.

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

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

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

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. 8)).

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. 8)).

3.4. Identifizierung und Authentifizierung bei Sperranträgen

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

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

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

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

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

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

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

4.2. Antragsbearbeitung

4.2.1. Durchführung der Identifikation und Authentifizierung

Antragsteller werden zuverlässig nach einem dokumentierten Verfahren identifiziert und authentifiziert (siehe auch Kapitel 3.2.3 (S. 8)).

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

4.2.2. Annahme beziehungsweise Ablehnung von Zertifikatsanträgen

Voraussetzung für die Annahme eines Antrags ist eine erfolgreiche Identifikation und *Authentifizierung* des Antragstellers.

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

4.2.3. Bearbeitungsdauer von Zertifikatsanträgen

Die Bearbeitung des Zertifikatsauftrags beginnt in einem angemessenen Zeitrahmen nach Erhalt der Beauftragung zu den normalen Geschäftszeiten der *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

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

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

4.3.2. Benachrichtigung des Antragstellers über die Zertifikatserstellung

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

4.4. Zertifikatsakzeptanz

4.4.1. Annahme durch den Zertifikatsinhaber

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

4.4.2. Veröffentlichung der Zertifikate durch den Zertifizierungsdienst

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

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

4.4.3. Benachrichtigung weiterer Instanzen durch den Zertifizierungsdienst

Weitere Instanzen werden nicht benachrichtigt. Die Zertifikate sind in dem in Kapitel 2.1 (S. 5) 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. 3) 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

Die Re-Zertifizierung eines Schlüssels ist möglich, wenn der *Zertifikatseigentümer* sein VR-Ident privat-Zertifikat gesperrt hat, die VR-Bankkarte noch gültig und einsatzfähig ist, und der *Zertifikatseigentümer* keine Kompromittierung der VR-Bankkarte, der *privaten Schlüssel* oder der *PIN* vermutet. Der *Zertifikatseigentümer* kann in einem solchen Fall ein neues VR-Ident privat-Zertifikat beantragen.

4.6.2. Wer kann eine Zertifikatserneuerung beantragen

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

4.6.3. Ablauf der Zertifikatserneuerung

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

4.6.4. Benachrichtigung des Zertifikatsinhabers nach Zertifikatserneuerung

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

4.6.5. Annahme einer Zertifikatserneuerung

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

4.6.6. Veröffentlichung einer Zertifikatserneuerung durch den Zertifizierungsdienst

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

4.6.7. Benachrichtigung weiterer Instanzen durch den Zertifizierungsdienst

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

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

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

4.7.2. Wer kann eine Schlüssel- und Zertifikatserneuerung beantragen

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

4.7.3. Ablauf der Schlüssel- und Zertifikatserneuerung

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

4.7.4. Benachrichtigung des Zertifikatsinhabers nach Schlüssel- und Zertifikatserneuerung

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

4.7.5. Annahme der Schlüssel- und Zertifikatserneuerung

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

4.7.6. Veröffentlichung einer Zertifikatserneuerung durch den Zertifizierungsdienst

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

4.7.7. Benachrichtigung weiterer Instanzen durch den Zertifizierungsdienst

Siehe Kapitel 4.4.3 (S. 11).

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. Details bezüglich der änderbaren Inhalte und dem Verfahren sind im CPS (Certification Practice Statement) für VR-Ident privat-Zertifikate festgelegt (siehe Anhang mit VR-Ident Referenzen).

4.8.2. Wer kann eine Zertifikatsmodifizierung beantragen

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

4.8.3. Ablauf der Zertifikatsmodifizierung

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

4.8.4. Benachrichtigung des Zertifikatsinhabers nach der Zertifikatsmodifizierung

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

4.8.5. Annahme der Zertifikatsmodifizierung

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

4.8.6. Veröffentlichung einer Zertifikatsmodifizierung durch den Zertifizierungsdienst

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

4.8.7. Benachrichtigung weiterer Instanzen durch den Zertifizierungsdienst

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

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. 23)).
- 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. 13)) und hat die Erstellung des neuen Zertifikats am Zertifikats-Download-Server angestoßen.
- Die VR-Bankkarte, welche die zum *Zertifikat* korrespondierenden Schlüssel enthält, wurde gesperrt.
- Die VR-Bank, welche die VR-Bankkarte des Zertifikatseigentümers ausgegeben hat, nimmt nicht mehr am *Zertifizierungsdienst* VR-Ident teil.

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

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

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

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

4.9.2. Sperrberechtigte

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

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

4.9.3. Verfahren zur Sperrung

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

4.9.4. Fristen für die Beantragung einer Sperrung

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

4.9.7. Periode für Erstellung von Sperrlisten

Die Häufigkeit und Zyklen für die Veröffentlichung und Erstellung von *CRL* (Sperrlisten) ist in Kapitel 2.3 (S. 5) 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 *Zertifizierungsdienst* VR-Ident bietet einen *OCSP-Responder* für die Abfrage des *Sperrstatus* von VR-Ident Zertifikaten mittels dem "Online Certificate Status Protocol" (*OCSP*) an. Über diesen können aktuelle Sperrinformationen abgefragt werden, die Sperrinformationen werden vom Auskunftsdienst zum Zeitpunkt der Abfrage ermittelt.

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

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

4.10.1. Betriebseigenschaften der Auskunftsdienste

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

4.10.2. Verfügbarkeit des Auskunftsdienstes

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

4.10.3. Optionale Funktionen

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

4.11. Austritt aus dem Zertifizierungsdienst

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

- Bei Ablauf eines VR-Ident privat-Zertifikats ohne Zertifikatserneuerung. Dies ist der Fall, wenn eine VR-Bankkarte abläuft, aber die VR-Bank keine Folgekarte ausstellt.
- Im Fall einer Sperrung aller Zertifikate des Zertifikatseigentümers, sofern nicht unmittelbar danach neue Zertifikate ausgestellt werden (siehe Kapitel 4.7 (S. 13) und Kapitel 4.8 (S. 13)).

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

4.12. Schlüsselhinterlegung und -wiederherstellung

4.12.1. Richtlinien und Praktiken zur Schlüsselhinterlegung und -wiederherstellung

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

Die eingesetzten physikalischen Sicherheitsmaßnahmen gewährleisten einen sehr hohen Schutz der kritischen Einrichtungen des Zertifizierungsdienstes VR-Ident. Insbesondere stellen diese Maßnahmen sicher, dass

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

5.1.1. Lage und Aufbau des Standortes

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

5.1.2. Zugangskontrolle

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

5.1.3. Stromversorgung und Klimakontrolle

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

5.1.4. Schutz vor Wasserschäden

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

5.1.5. Brandschutz

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

5.1.6. Aufbewahrung von Datenträgern

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

5.1.7. Entsorgung von Datenträgern

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

5.1.8. Datensicherung

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

5.2. Organisatorische Sicherheitsmaßnahmen

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

- die Zuständigkeiten und Rollen für den Betrieb der *Zertifizierungsstelle* und das Sicherheitsmanagement klar geregelt,
- ein umfassendes Sicherheitsmanagement etabliert,

- kritische Prozesse und Prozeduren der *Zertifizierungsstelle* und des Sicherheitsmanagements dokumentiert und implementiert,
- schützenswerte Objekte und Informationen identifiziert und klassifiziert.

5.2.1. Sicherheitskritische Rollen

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

5.2.2. Anzahl benötigter Personen bei sicherheitskritischen Tätigkeiten

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

5.2.3. Identifizierung und Authentisierung von Rollen

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

5.2.4. Trennung von Rollen und Aufgaben

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

5.3. Personelle Sicherheitsmaßnahmen

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

- klar den definierten Rollen im *Zertifizierungsdienst* zugewiesen,
- für ihre Aufgaben ausreichend qualifiziert,
- mit den für ihre Aufgaben erforderlichen Dokumentation ausgestattet,
- auf ihre Zuverlässigkeit hin überprüft.

5.3.1. Anforderungen an Qualifikation und Erfahrung

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

5.3.2. Überprüfung der Vertrauenswürdigkeit

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

5.3.3. Anforderungen an Schulung und Fortbildung

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

5.3.4. Nachschulungsintervalle und –anforderungen

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

5.3.5. Arbeitsplatzrotation / Rollenumverteilung

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

5.3.6. Sanktionen bei unbefugten Handlungen

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

5.3.7. Vertragsbedingungen mit dem Personal

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

5.3.8. An das Personal ausgehändigte Dokumentation

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

5.4. Protokollierung sicherheitskritischer Ereignisse

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

5.4.1. Zu protokollierende Ereignisse

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

5.4.2. Häufigkeit der Auswertung von Protokolldaten

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

5.4.3. Aufbewahrungsfristen für Protokolldaten

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

5.4.4. Schutz der Protokolldaten

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

5.4.5. Sicherungsverfahren für Protokolldaten

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

5.4.6. Internes/externes Protokollierungssystem

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

5.4.7. Benachrichtigung des Auslösers eines Ereignisses

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

5.4.8. Schwachstellenbewertung

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

5.5. Archivierung

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

5.5.1. Archivierte Daten und Aufbewahrungsfrist

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

5.5.2. Aufbewahrungsfrist

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

5.5.3. Schutz der archivierten Daten

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

5.5.4. Sicherung der archivierten Daten

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

5.5.5. Anforderungen an den Zeitstempel der archivierten Daten

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

5.5.6. Internes/externes Archivierungssystem

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

5.5.7. Verfahren zum Einholen und Verifizierung von Archivdaten

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

5.6. Schlüsselwechsel

Die Schlüsselpaare, die der *Zertifizierungsdienst* VR-Ident zur Erbringung ihrer Zertifizierungsdienste für VR-Ident Zertifikate einsetzt, werden rechtzeitig vor Ablauf ihrer Gültigkeit gewechselt. In diesem Fall wird das entsprechende *Zertifikat* nicht gesperrt.

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

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

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

5.7. Business Continuity Management und Incident Handling

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

5.7.1. Prozeduren zu Incident Handling und zu Notfällen

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

5.7.2. Prozeduren bei Kompromittierung von Ressourcen

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

5.7.3. Prozeduren bei Kompromittierung von CA-Schlüsseln

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

5.7.4. Notbetrieb im Katastrophenfall

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

5.8. Einstellung der Zertifizierungsdienste

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

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

6. Technische Sicherheitsmaßnahmen

6.1. Erzeugung und Installation von Schlüsselpaaren

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

6.1.1. Erzeugung von Schlüsselpaaren

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

6.1.2. Übermittlung privater Schlüssel an den Zertifikatseigentümer

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

6.1.3. Übermittlung öffentlicher Schlüssel an den Zertifikatsaussteller

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

6.1.4. Übermittlung öffentlicher CA-Schlüssel an vertrauende Dritte

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

6.1.5. Schlüssellängen

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

6.1.6. Erzeugung und Prüfung der Schlüsselparameter

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

6.1.7. Verwendungszweck der Schlüssel

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

6.2. Schutz der privaten Schlüssels und der kryptographischen Module

Private Schlüssel der *CA* der *Zertifizierungsstelle* werden ausschließlich einer sicheren Umgebung in Hardware-Sicherheitsmodulen (*HSM*) gespeichert und verwendet. Der Zugriff auf diese Schlüssel erfolgt ausschließlich im Rahmen festgelegter Prozeduren, unter Mitwirkung mehrerer berechtigter Mitarbeiter, und in der vorgesehenen sicheren Umgebung. Zum Zweck einer hohen Verfügbarkeit können sichere Schlüsselbackups angefertigt werden. Der Zugriff auf die *privaten Schlüssel*, insbesondere auch das Backup und Recovery, ist durch technische Maßnahmen geschützt, und erfolgt ausschließlich in sicheren Prozeduren unter Mitwirkung mehrerer berechtigter Mitarbeiter, und in Übereinstimmung mit den Vorgaben der Zertifi-

zierung der *Hardware-Sicherheitsmodule* (*HSM*). Nicht mehr benötigte Schlüssel der *Zertifizierungsstelle* werden sicher deaktiviert.

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

6.2.1. Standards und Schutzmechanismen der kryptographischen Module

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

6.2.2. Aufteilung der Kontrolle über private Schlüsseln auf mehrere Personen

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

6.2.3. Hinterlegung privater Schlüssel

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

6.2.4. Backup privater Schlüssel

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

6.2.5. Archivierung privater Schlüssel

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

6.2.6. Transfer privater Schlüssel

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

6.2.7. Speicherung privater Schlüssel

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

6.2.8. Methoden zur Aktivierung privater Schlüssel

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

6.2.9. Methoden zur Deaktivierung privater Schlüssel

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

6.2.10. Methoden zur Vernichtung privater Schlüssel

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

6.2.11. Bewertung kryptographischer Module

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

6.3. Weitere Aspekte des Schlüsselmanagements

Öffentliche Schlüssel werden mit den Zertifikaten für eine im *CPS* (*Certification Practice Statement*) angemessene Zeitdauer archiviert und verwendet.

6.3.1. Archivierung öffentlicher Schlüssel

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

6.3.2. Verwendungsdauern von Zertifikaten und Schlüsselpaaren

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

6.4. Aktivierungsdaten

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

6.4.1. Erzeugung und Installation von Aktivierungsdaten

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

6.4.2. Schutz der Aktivierungsdaten

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

6.4.3. Weitere Aspekte von Aktivierungsdaten

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

6.5. Sicherheitsmaßnahmen für Computer

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

- Schutz vor Viren und anderer bösartiger Software
- Schutz vor unbefugten logischen Zugriff auf die Systeme
- Regelmäßige Sicherung kritischer Daten
- Angemessene Ausfallsicherheit der kritischen Systeme

- Ausreichende Prüfung vor jeder Änderung der Konfiguration und Systemkomponenten
- Zeitnahe Erkennung von Störungen und Ausfällen

6.5.1. Spezielle Anforderungen zur Computersicherheit

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

6.5.2. Bewertung der Computersicherheit

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

6.6. Technische Kontrollen des Software-Lebenszyklus

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

6.6.1. Systementwicklungsmaßnahmen

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

6.6.2. Sicherheitsmanagement

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

6.6.3. Maßnahmen zur Kontrolle des Software-Lebenszyklus

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

6.7. Maßnahmen zur Netzwerksicherheit

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

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

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

6.8. Zeitstempel

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

7. Profile

7.1. Zertifikatsprofile

Die von der VR-Ident PKI verwendeten Zertifikate entsprechen dem Standard X.509, die 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

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

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

7.1.2. Zertifikatserweiterungen

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

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

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

7.1.3. Algorithmus Bezeichner (OID)

Die eingesetzten Algorithmen Bezeichner entsprechen den gängigen Standards.

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

7.1.4. Namensformen

Siehe Kapitel 3.1.1.

7.1.5. Nutzung von Erweiterungen zur Namensbeschränkung (Name Constraints)

Erweiterungen zur Namensbeschränkung werden nicht verwendet.

7.1.6. Bezeichner für Zertifizierungsrichtlinien (OID)

Der *Object Identifier* (OID) für die vorliegende Policy ist in Kapitel 1.2 (S. 1) aufgeführt.

7.1.7. Nutzung von Erweiterungen zur Richtlinienbeschränkungen (PolicyConstraints)

Erweiterungen zur Richtlinienbeschränkungen werden nicht verwendet.

7.1.8. Syntax und Semantik von Policy Qualifiern

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

7.1.9. Verarbeitung von kritischen Erweiterungen für Zertifizierungsrichtlinien (certificatePolicies)

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

7.2. Profil der Sperrlisten

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

7.2.1. Versionsnummern

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

7.2.2. Erweiterungen der Sperrlisten

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

CRL (Sperrlisten) und Sperrlisteneinträge haben die folgenden Erweiterungen:

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

7.2.3. Weitere Eigenschaften der Sperrlisten

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

7.3. OCSP-Profile

Die von der VR-Ident PKI verwendeten OCSP Profile entsprechen 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

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

7.3.3. Weitere Eigenschaften der OCSP-Anfragen und Antworten

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

8. Revisionen und andere Bewertungen

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

Der Auditor ist ausreichend qualifiziert und von dem Zertifizierungsdiensteanbieter *GAD* unabhängig.

Schwerwiegende Mängel, die bei einem Audit entdeckt werden, werden an das Management der *GAD* eG berichtet.

8.1. Häufigkeiten von Revisionen

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

8.2. Identität und Qualifikation des Auditors

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

8.3. Beziehungen zwischen Auditor und zu untersuchender Partei

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

8.4. Umfang der Prüfungen

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

8.5. Maßnahmen bei Mängeln

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

8.6. Veröffentlichung der Ergebnisse

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

9. Weitere geschäftliche und rechtliche Regelungen

9.1. Gebühren

9.1.1. Gebühren für die Ausstellung und Erneuerung von Zertifikaten

Die 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.

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 Schadenersatz nachkommen kann.

9.2.2. Weitere Vermögenswerte

Keine weiteren Vermögenswerte.

9.2.3. Erweiterte Versicherung oder Garantie

Keine weiteren Versicherungen oder Garantien.

9.3. Vertraulichkeit betrieblicher Informationen

9.3.1. Art der geheim zu haltenden Information

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

9.3.2. Öffentliche Informationen

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

9.3.3. Verantwortlichkeit für den Schutz von geheim zu haltenden Information

Der *Zertifizierungsdienst* VR-Ident sichert die in Kapitel 9.3.1 (S. 32) 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.

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

9.4.7. Sonstige Offenlegungsgründe

Keine weiteren Offenlegungsgründe.

9.5. Geistiges Eigentum und dessen Rechte

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

9.6. Gewährleistung, Sorgfalts- und Mitwirkungspflichten

9.6.1. Verpflichtung der Zertifizierungsstelle

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

9.6.2. Verpflichtung der Registrierungsstelle

Als *Registrierungsstelle* für VR-Ident Zertifikate sichert die *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 *Zertifikatseigentümer* ist verpflichtet, die VR-Ident Zertifikate sind nur bestimmungsgemäß und nicht missbräuchlich zu benutzen.

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

9.6.4. Verpflichtung vertrauender Dritte

Vertrauende Dritte sind dazu verpflichtet, gemäß den in Kapitel 4.5.2 (S. 11) 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.

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

9.8.2. Haftung des Zertifikatseigentümers, Zertifikatsinhabers beziehungsweise Kunden

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

9.9. Schadensersatz

Siehe Kapitel 9.8.1.

9.10. Gültigkeit des Richtliniendokuments

9.10.1. Gültigkeitszeitraum

Das vorliegende Dokument ist vom Tag seiner Veröffentlichung an gültig. Seine Gültigkeit endet mit der Einstellung des Zertifizierungsdienstes (siehe Kapitel 5.8 (S. 23)).

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.

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

9.12.2. Benachrichtigungsverfahren und Veröffentlichungsperioden

Bei Änderungen bezüglich sicherheitsrelevanter Aspekte oder sicherheitsrelevanter Verfahren hinsichtlich der Zertifikatsinhaber, wie beispielsweise Änderungen des Registrierungsablaufs, des Verzeichnis-, Widerrufs- und Sperrdienstes, der Kontaktinformationen oder der Haftung, wird der *Zertifizierungsdienst* VR-Ident die Zertifikatsinhaber benachrichtigen.

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

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

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

9.13. Schiedsverfahren

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.
Authentizität	Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit von Daten und deren Urheberschaft.
CA	Certification Authority – englischer Begriff für eine Zertifizierungsinstanz.
Certificate Policy	Gesamtheit der Regeln und Vorgaben, welche die Anwendbarkeit eines Zertifikatstyps festlegen.
Certification Practice Statement	Darlegung der Praktiken, die ein Zertifizierungsdiensteanbieter bei der Ausgabe der Zertifikate anwendet.
CP	Abkürzung für Certificate Policy.
CPS	Abkürzung für Certification Practice Statement.
CRL	Certificate Revocation List – Sperrliste.
CSA	CSA steht für „Client-Server-Authentisierung“, durch die beispielsweise die Authentisierung gegenüber Serveranwendungen technisch realisiert wird. Dieser Schlüssel wird während der Personalisierung der VR-Bankkarte generiert und dann während der Produktion auf die Karte gebracht.
DS	DS steht für „digitale Signatur“, durch welche die elektronische Signatur technisch realisiert ist. Dieser Schlüssel wird auf der VR-Bankkarte während der Produktion generiert.
Fingerprints	Als Fingerprint eines Zertifikats bezeichnet man den über das gesamte Zertifikat berechneten Hashwert.

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 .
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.

RA	Registration Authority – englischer Begriff für eine Registrierungsstelle.
Registrierungsstelle	Stelle eines Zertifizierungsdienstes, welche die Anträge zur Ausstellung oder Sperrung von Zertifikaten erfasst und die Antragsteller identifiziert werden.
RFC	Request for Comment – Dokumententyp der Internet Engineering Task Force (IETF), in der diese Standards vorschlägt und veröffentlicht.
Rollenträger	Mitarbeiter, die im Zertifizierungsdienst VR-Ident beschäftigt sind. Es werden Zuverlässigkeitsprüfungen durchgeführt. Rollenträger die sicherheitskritische Aufgaben durchführen, haben bei der Ernennung zum Rollenträger ein Führungszeugnis vorgelegt.
Root-CA	Oberste Zertifizierungsinstanz einer Zertifizierungshierarchie. Das Zertifikat der Root-CA wird von ihr selbst signiert und muss den Teilnehmern der PKI auf eine vertrauenswürdige Weise (beispielsweise offline) zugänglich gemacht werden. Man nennt diese Instanz auch "Wurzel-Zertifizierungsinstanz".
Schlüssel- und Zertifikatserneuerung	Die Ersetzung eines Zertifikates durch ein Zertifikat mit neuer Gültigkeitsdauer und für einen neuen öffentlichen Schlüssel aber sonst unveränderten Inhaltsdaten. In RFC 3647 "certificate re-key" genannt.
Sperrliste	Liste, in der ein Anbieter eines Zertifizierungsdienstes die Sperrinformation der von ihm ausgestellten und noch nicht abgelaufenen Zertifikate veröffentlicht (siehe auch CRL).
Sperrstatus	Status eines Zertifikates bezüglich Sperrung.
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 enthal-

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