Certification Practice Statement (CPS)

VR-Ident SSL-Certificates (WebTrust)

FIDUCIA GAD
ZUKUNFTSERFAHREN

IT-Partner der FinanzGruppe
Volksbanken Raiffeisenbanken

Certification Practice Statement (CPS)

VR-Ident SSL-Certificates (WebTrust)

Version:	Version 3.02.00, Approved
Zielgruppe:	Users and owners of VR-Ident SSL-Certificates
Datum/Uhrzeit:	26.01.2018 / 10:12 Uhr

Revision History

Nummer	Datum	Inhalt / Änderungen
3.1.0	06.09.2017	Amendment Chapter 4.2.4 "Certification Authority Authorization (CAA)"
3.2.0	10.01.2018	Translation to English and updates and improvements

Zusammenfassung
This document is the "Certification Practice Statement" (CPS) for the Certification Service VR-Ident for VR-Ident SSL-Certificates (WebTrust). Because of technical reasons some terms on this title page are still in German language.

Öffentlich (C1) - Users and owners of VR-Ident SSL-Certificates

Table of Contents

List of Figures

List of Tables

Chapter 1. Introduction

1.1. Overview

Fiducia & GAD IT AG is an IT service provider and software developer for more than 1.100 banks. The company's objective is commercial promotion and support of its members in the area of information technology.

Among its services *Fiducia & GAD IT AG* also offers certification services for the issuance, dissemination, and management of electronic certificates. This service is called "Certification Service VR-Ident".

SSL server certificates are offered under the product name "VR-Ident SSL-Certificate".

Fiducia & GAD IT AG also issues extended validation (EV) certificates that fulfill additional requirements.

This document is the "*Certification Practice Statement*" (*CPS*) for the *Certification Service* VR-Ident for VR-Ident SSL-Certificates.

All SSL certificates are issued in the following CA hierarchy:

- end-entity certificates are issued from subordinate CAs operated by *Fiducia & GAD IT AG*
- subordinate CA certificates are issued from the external Root CA operated by QuoVadis.

All services have been assessed and certified by an independent external auditor according to the following requirements:

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

If updated versions of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" are published (see www.cabforum.org) and if this updated version introduces deviations from this document, the requirements defined in the updated version of the Baseline Requirements have priority over the requirements defined in this document. The certification service "*Certification Service* VR-Ident" will, if necessary, amend its CPS as well as the processes for the issuance of VR-Ident SSL certificates.

In addition the following requirements are fulfilled:

- Mozilla CA Certificate Inclusion Policy.

The certification service ensures adherence to the current version of the Baseline Requirements "CA Browser Forum" (https://www.cabforum.org) regarding application, generation, dissemination, and management of VR-Ident SSL Certificates. If there are discrepancies between the "*Certification Practice Statement*" (*CPS*) for the certification service for VR-Ident SSL Certificates and the Baseline Requirements of the "CA Browser Forum" the Baseline Requirements of the "CA Browser Forum" have priority.

Details and references to these documents can be found in appendix A Bibliography with general and common international documents.

1.1.1. Purpose of the Document

According to *RFC* 3647 a "*Certification Practice Statement*“ (*CPS*) describes the practices followed by the CA in issuing and managing the certificates. Accordingly, this document describes the practices of the Certification Service "*Certification Service* VR-Ident" for application, generation, dissemination, and management of VR-Ident certificates.

This *CPS* describes the current status of the certification processes and the security measures implemented by the certification service VR-Ident and allows an estimation of the quality of the certification service.

In particular, this CPS describes:

- the meaning and use of VR-Ident certificates,
- the application for and issuance of VR-Ident certificates,
- the renewal of VR-Ident certificates,
- the revocation of VR-Ident certificates,
- the repository and revocation status services,
- the technical and organizational security,
- details regarding the content of VR-Ident certificates and *CRL*s (certificate revocation lists), and
- other business and legal matters.

This document is structured according to *RFC* 3647.

CAs issuing VR-Ident SSL certificates conform to the current version of the CA/Browser Forum (CABF) requirements including:

- Guidelines for the Issuance and Management of Extended Validation (EV) Certificates,
- Guidelines for the Issuance and Management of Extended Validation (EV) Code-Signing Certificates, and,
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates,

published at www.cabforum.org.

In the event of any inconsistency between this document and those requirements, those requirements take precedence over this document

This *CPS* (*Certification Practice Statement*) is applicable only for the products mentioned in Chapter 1.1 [1].

Guidelines for the applicability and use of VR-Ident certificates are provided in the document "VR-Ident Certificate Policy (CP) for VR-Ident Certificates (WebTrust)" (cf. Appendix with VR-Ident References) and in the document "CA-Certificate Policy of QuoVadis" (Appendix with General References).

1.1.2. VR-Ident Certificates

Certificates are "electronic IDs" for secure communication in the internet enabling users to prove their identity and to authenticate their content. With certificates persons, organizations, and IT-systems can obtain their own unique and unforgeable security identification. For this purpose VR-Ident offers several different solutions:

- VR-Ident SSL (for devices)
- VR-Ident mail (for individuals)
- VR-Ident SMIME (for individuals)
- VR-Ident privat (for individuals)

VR-Ident SSL-Certificates are the digital ID for web servers. They allow the unique identification of servers and bind the identity of an organization to that specific server. The certificate consists of validated data of the certificate owner, the public key of the server, information about the issuer of the certificate, and the electronic signature of the *Certification Service* Provider *Fiducia & GAD IT AG*. A certificate also permits encrypted communication between a server and a user's browser. The cryptographic strength of the encryption depends on the technical capabilities of server and browser. Technically the encryption is implemented as hybrid encryption; the key exchange can be performed based on SSL-Server-Certificates using *asymmetric cryptography* and the encryption of the communication is done by symmetric cryptographic techniques.

By issuing a VR-Ident SSL-Certificate the *Certification Service* VR-Ident assures that the web-presence of an organization belongs to the organization named in the certificate. The validation of the organization's identity is based on the verification of the organization's real existence, the organization's approval of the certificate application, and the verification that the individual submitting the application on behalf of the organization has been authorized to do so. In addition, the certificate assures that the domain name in the certificate is assigned to the organization or the organization has been authorized by the domain owner to use the domain name.

VR-Ident SSL-Certificates can be used by components capable of interpreting and processing certificates as specified in *X.509*, version 3. A description of certificate profiles is provided in Chapter 7.1 [38].

1.2. Document Name and Identification

The titles of relevant documents related to the *Certification Service* VR-Ident are composed as follows:

- Name of the product family "VR-Ident"
- "Certification Practice Statement (CPS)" or "Certificate Policy (CP)"
- "for"
- Name of the product

Version number of this document: 3.02.00

Date of release of this document: 23.01.2018

The number "17696" has been reserved for publications of "*Fiducia & GAD IT AG*".

According to the OID description {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1)} the first positions of the *Object Identifier* (OID) of documents owned by "*Fiducia & GAD IT AG*" related to the *Certification Service* VR-Ident are: 1.3.6.1.4.1.17696.

Details can be found in all public OID repositories, e.g. http://www.oid-info.com/get/1.3.6.1.4.1.17696)[1]

The ASN.1 *Object Identifier* (OID) for this document is: 1.3.6.1.4.1.17696.4.1.2.5.3.2

The document name of this CPS is: "VR-Ident Certification Practice Statement (CPS) für VR-Ident SSL-Certificatee (WebTrust)".

The ASN.1 *Object Identifier* (OID) for the associated "*Certificate Policy*" (*CP*) ("VR-Ident Certificate Policy (CP) for VR-Ident Certificates (WebTrust)"): 1.3.6.1.4.1.17696.4.1.2.9.3.2.

1.3. Participants of the Public Key Infrastructure (PKI)

1.3.1. Certification Authorities and PKI

The following paragraphs describe the Certification Authorities (CAs) and other participants of the certification hierarchy of the VR-Ident PKI of the *Certification Service* VR-Ident.

The *Certification Service* VR-Ident is the *Certification Authority* which issues the VR-Ident certificates. For the certificate types named in Chapter 1.1 [1] the CA uses several certification instances. These are logical units using their own key pairs for signing the certificates.

The certification instances issuing the VR-Ident certificates for end-entities obtain their certificates from a superior CA. The *Certification Service* VR-Ident consists of the following entities in the certification hierarchy:

[1] http://www.oid-info.com/get/1.3.6.1.4.1.17696

- The CA certificates used for issuing the VR-Ident end-entity certificates have been issued via Root Signing from an external *Root-CA* operated by the company Quo Vadis ("QuoVadis Root CA 2").

The Common Name (CN) of CAs used by the *Certification Service* VR-Ident includes as suffix the year of their creation. In this document the suffix is often omitted if not explicitly required. It is only included if required by the context. In some cases the information about the year is noted as "[JJJJ]" instead of the real date.

Certificate Hierarchy with"QuoVadis Root CA 2"

The *Certification Service* VR-Ident for the issuance of "VR-Ident SSL-Certificates" under the "QuoVadis Root CA 2" consist of the following hierarchy elements:

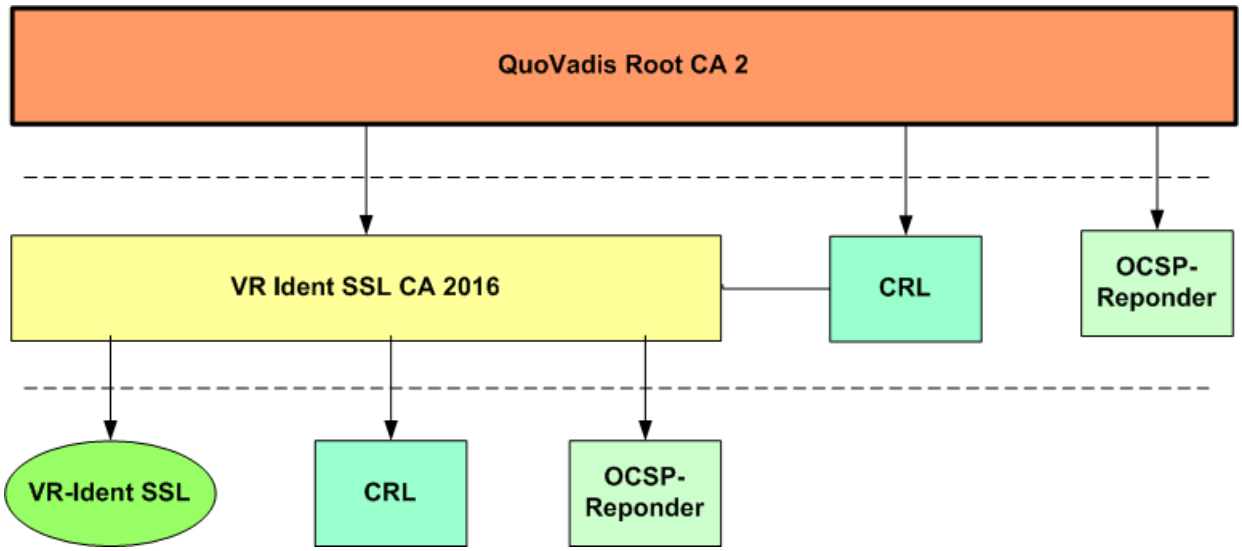

Figure 1.1. Certification hierarchy for VR-Ident SSL-Certificates using the "QuoVadis Root CA 2"

Description of the hierarchy:

The CA hierarchy consists of three hierarchy levels:

- The top level consists of the "QuoVadis Root CA 2". This Root CA issued the subordinate CA certificate "VR IDENT SSL CA 2016", signs its own Certificate Revocation Lists (*CRL*s), and signs the associated QuoVadis OCSP Responder certificates.
- The second level consists of the "VR IDENT SSL CA 2016", which signs
  - the "VR-Ident SSL-Certificates", i.e the customer's SSL-Server end-entity certificates,
  - the *OCSP-Responder* certificates used for signing responses to certificate status requests for "VR-Ident SSL-Certificates", and
  - the *CRL*s with revocation status information for "VR-Ident SSL-Certificates",

The "VR IDENT SSL CA 2016" acts as a Certification Authority (*CA*); it generates and signs the SSL-Server certificates for the customers.

- The third level consists of the customer's "VR-Ident SSL-Certificates", the *OCSP-Responder* certificates, and the CRLs.

1.3.2. Registration Authorities

A Registration Authority is the organizational unit in a PKI infrastructure responsible for the identification and authentication of applicants, arranges certificate renewal, and receives certificate revocation requests.

The RA is the point of contact for persons and organizations for obtaining electronic certificates from the CA.

The *RA* (*Registration Authority*) for VR-Ident certificates is located in the premises of *Fiducia & GAD IT AG*. The *Certification Service* Provider *Fiducia & GAD IT AG* acts as *RA* (*Registration Authority*). The RA receives and validates applications for the issuance, revocation, or renewal of certificates. The *RA* (*Registration Authority*) may authorize applications or reject them.

1.3.3. Applicants

1.3.3.1. Subscribers

Subscribers for VR-Ident SSL-Certificates are juristic persons applying for the issuance of VR-Ident SSL-Certificates through the *Certification Service* VR-Ident. The *Certification Service* VR-Ident issues VR-Ident SSL-Certificates to legal entities (e..g. banks, commercial enterprises, etc.).

The *Certification Service* VR-Ident distinguishes between the following subscribers:

- *Fiducia & GAD IT AG* (or affiliates of *Fiducia & GAD IT AG*) for applications of VR-Ident SSL-Certificates for subdomains of domains exclusively used by *Fiducia & GAD IT AG* (e.g. www.fiduciagad.de),
- *VR-Banks* for applications of VR-Ident SSL-Certificates for their own domains,
- *Fiducia & GAD IT AG* affiliates or partners for applications of VR-Ident SSL-Certificates for their own domains.

1.3.3.2. Subscribers

The Subscriber of a VR-Ident SSL-Certificate is the entity for which the certificate is issued. The Subscriber is included in the certificate as "Subject". Typically, the Subscriber is identical to the Applicant, but this is not mandatory.

1.3.4. Relying Parties

Relying Parties are natural persons or legal entities that rely on the validity of a VR-Ident certificate issued by the *Certification Service* VR-Ident of *Fiducia & GAD IT AG*.

1.3.5. Other Participants

None.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

VR-Ident certificates may be used only according to the following restrictions. VR-Ident certificates shall be used only to the extent consistent with applicable law.

VR-Ident SSL-Certificates may be used for the authentification of the web server named in the certificate. Secure communication is established through SSL or TLS. If the certificate is used for a high-traffic FQDN the operator of this website must activate OCSP stapling.

1.4.2. Prohibited Certificate Usage

For all VR-Ident certificates the following restrictions apply:

- VR-Ident certificates are not designed and intended for use or resale as control equipment in hazardous circumstances or for uses where fail-safe performance is required. In addition, VR-Ident certificates may not be used for the operation of nuclear facilities, aircraft navigation or communication systems, air traffic

control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage. Certificate usage for the purposes mentioned above is explicitly excluded.

- VR-Ident certificates may only be used according to the key usage extension included in the certificates (Chapter 4.5 [18]).
- Additional information regarding prohibited certificate usage is published at http://www.vr-ident.de.

For VR-Ident SSL-Certificates the following restrictions on certificate usage apply:

- A VR-Ident SSL-Certificate may not be used in the name of an organization not named in the certificate.
- It is prohibited to use VR-Ident SSL-Certificates for domain names and organization names different from those included in the certificates.
- A VR-Ident SSL-Certificate may be used only for the contractually agreed number of servers or services.
- After expiry or revocation the private keys associated with the VR-Ident SSL-Certificates may not be used.
- It is prohibited to use VR-Ident SSL-Certificates for so-called „Man in the Middle“ attacks. Using VR-Ident SSL-Certificates for domains which are not owned or under control of the Subscriber is prohibited; this also applies for closed, internal environments.

1.5. Policy Administration

1.5.1. Organisation Administering the CPS

Responsible for administration and approval of this document is:
Fiducia & GAD IT AG
Department: PPMASK
GAD Straße 2-6
48163 Münster
Internet: http://www.vr-ident.de

1.5.2. Contact Person

Contact Person for questions related to this document is:
Fiducia & GAD IT AG
Department: PPMASK
GAD Straße 2-6
48163 Münster
E-Mail: IND_Zertifikatsverwaltung@fiduciagad.de[2]

1.5.3. Person Determining CPS Suitability for the Policy

Responsible for the approval of this document is the manager of the department named in Chapter 1.5.1 [6]. The document remains effective until it is withdrawn by this instance or replaced by an amended version.

1.5.4. CPS Approval Procedures

This document is amended if required. If substantial changes are made the version number is incremented. New versions are approved by the entity named in Chapter 1.5.1 [6]. The contents of CP (*Certificate Policy*) and *CPS* (*Certification Practice Statement*) are coordinated during this process.

[2] mailto:IND_Zertifikatsverwaltung@fiduciagad.de

1.6. Definitions and Acronyms

Definitions and acronyms can be found in the glossary.

Chapter 2. Publication and Repository Responsibilities

2.1. Repositories

The *Certification Service* VR-Ident publishes information related to the VR-Ident PKI at its website https://www.vr-ident.de. Internally (access only for employees of *Fiducia & GAD IT AG* and employees of *Fiducia & GAD IT AG*'s partner banks) additional information is available.

The *Certification Service* VR-Ident operates the following repositories for publishing certificate information:

- VR-Ident certificates can be retrieved from a public directory. Certificates for individuals can be retrieved from the directory only if the certificate owner has declared its consent to the publication. The VR-Ident Repository is available at the following address: ldap://www.vr-ident.de
- For online revocation checking the *Certification Service* VR-Ident operates an *OCSP-Responder*. Via this validation service the status of all certificates can be requested. The OCSP service is available at: http://ocsp.vr-ident.de/gtnocsp/OCSPResponder/<name of the CA>
- The *Certification Service* VR-Ident also publishes certificate revocation lists (*CRL*s) with revocation information of certificates. CRLs can be downloaded from:
  http://www.vr-ident.de/gtncrl/CRLResponder/<name of the CA>
  and
  ldap://www.vr-ident.de (the *CRL* is stored in the attribute of the CA object).

The CA-Certificates of the *Certification Service* VR-Ident are published at the website http://www.vr-ident.de. Additionally, the *Certification Service* VR-Ident publishes on this website the *fingerprint*s (*hash value*)s of the VR-Ident CA-Certificates; they can be used to verify the correctness and authenticity of the CA-Certificates before they are installed on the user's systems. The website also provides information how the fingerprints can be verified.

2.2. Publication of Certificate Information

The *Certification Service* VR-Ident publishes

- Issued VR-Ident certificates (certificates for individuals only if the owner declared his/her consent) in the repositories mentioned in Chapter 2.1 [8],
- *CRL*s, at the address stated in Chapter 2.1 [8],
- This *CPS* (*Certification Practice Statement*), available for download from http://www.vr-ident.de,
- General Terms and Conditions (Allgemeine Geschäftsbedingungen) for Participants and Relying Parties, available for download from http://www.fiduciagad.de.

Other business and legal matters are listed in Chapter 9 [46] of this CPS.

2.3. Time or Frequency of Publication

VR-Ident certificates (for individuals only if the owner declared his/her consent) are published immediately after they have been issued. The certificates are retained in the VR-Ident repositories for a period of at least seven years after the certificates have expired.

*CRL*s are published immediately after generation; they can be downloaded from the VR-Ident repository. CRLs are generated according to the following schedule:

- *CRL*s for VR-Ident SSL-Certificates are published 7 days before the current CRL expires.
- *CRL*s for CA-Certificates are generated and published at least once per year and after a CA-Certificate has been revoked.

CP and CPS are reviewed at least annually. Updates and amendments of CP and CPS are published according to the stipulations in Chapter 9.12. *CP* (Certificate Policies) and *CPS* (*Certification Practice Statement*) are published after their creation or after amendments have been made.

Amendments to the General Terms and Conditions and other documents are made as necessary.

2.4. Access Controls on Repositories

All information in the VR-Ident repository is publicly and internationally available. Read access to the repository is unrestricted.

Changing the information stored in the repository is restricted to authorized personnel.

The *Certification Service* VR-Ident has implemented appropriate security mechanisms to prevent unauthorized modifications, or adding, or removing of data.

Chapter 3. Identification and Authentication

3.1. Naming

3.1.1. Types of Names

All certificates issued by the *Certification Service* VR-Ident contain unique names (DistinguishedName) in the fields "Issuer" and "Subject" according to *X.501*.

In VR-Ident SSL-Certificates the Issuer field includes the attributes:

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

The Subject fields of VR-Ident SSL-Certificates contain the attributes:

- CommonName (CN) = Domain name or URL of the organization, according to the registration with the domain name registrar of the applicable Top-Level Domain
- Organization (O) = Name of the organization, according to the records in the applicable commercial register
  - if the name of the organization does not uniquely identify the organization the locality of the organization may be added, e.g. if the record in the register is "Volksbank eG" and this organization has more than one office, then the locality may be added and the O-field contains "Volksbank eG Musterstadt"
  - if the commercial register contains a record about a local branch of the organization and the name of this local branch differs from the mother organization (assumed name) then this local name may be included in the O-field. In this case the O-field consists of the assumed name followed by the name of the organization in parenthesis e.g. "Bürgerbank Musterstadt (Volksbank Musterstadt eG)"
- Organizational Unit (OU) = "VR-Ident" (default value), the applicant may submit and alternative value for the OU-field, e.g. a department or subdivision of the organization. Not permitted are names of other organizations, trade-marks, toponyms, DBA names, or similar
- Locality (L) = Place of residence of the organization, as stated in the record of the applicable commercial register
- State (ST) = State or Province where the organization is located, as stated in the record of the applicable commercial register
- Country (C) = DE for organizations located in Germany.

The attributes Locality (L) and State (ST) may be shortened or abbreviated as long as the pair L and S together are a reasonable combination identifying the organizations place of residence.

The certificate extension SubjectAltName contains at least the CommonName (CN) as defined above. Optional additional alternative names may be added as DNS-Names. All alternative domain names must undergo the same validation process as the domain name in the CN-field.

Wildcard-Certificates are issued only after consulting the responsible instance in the *Certification Service* VR-Ident. The wildcard character "*" may be used only in the leftmost position of a subdomain.

3.1.2. Need for Names to be Meaningful

CA-Certificates contain in the attribute "CommonName" in the field "Subject" the name of the CA which allows the identification of the CA.

VR-Ident SSL-Certificates contain the attribute "Organization" in the field "Subject" the name of an organization which makes the organization identifiable as the owner of the certificate.

The attributes Locality and State identify where the organization is located.

The attribute OrganizationalUnit contains the name of a department, subdivision or similar of the organization. Not permitted are names of other organizations, trade-marks, toponyms, DBA names, or similar. Alternatively, the term "VR-Ident" may be used.

The attribute CommonName contains the domain-name as assigned to the organization by the domain registrar of the Top-Level Domain.[1]The certificate extension SubjectAltName contains at least the CommonName and optional additional alternative domain names as DNS-Names. All alternative domain names must undergo the same validation process as the domain name in the CN-field.

CommonName attributes and SubjectAltNames may not include internationalised Domain Names (i.e. umlaut-characters or special characters are not permitted except as stated in Chapter 3.1.4).

3.1.3. Anonymity or Pseudonymity of Subscribers

Pseudonyms and anonymous VR-Ident certificates are not supported by the *Certification Service* VR-Ident.

3.1.4. Rules for Interpreting Various Name Forms

In names only the following characters are permitted:

A-Z, a-z, 0-9, blank symbol, ', (,), +, -, , (comma), . (dot), /, :, ?.

Optional the following "German" umlauts may be used:

Ä, Ö , Ü , ä , ö, ü , ß.

German characters may be substituted according to the following rules:

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

Accents are removed from characters. In general, a given character or symbol will be substituted by one or more characters from the set a-z and A-Z using commonly applied substitution rules to represent the correspondent phoneme.

In general, it is recommended to abstain from special characters and umlauts.

3.1.5. Uniqueness of Names

Subject Distinguished Names (DNs) are unique.

3.1.6. Recognition, Authentication, and Role of Trademarks

The names of organizations in VR-Ident SSL-Certificates are identical to the registered names in the applicable registers. Therefore, the right to use the name is guaranteed.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

The Applicant must prove the authenticity of the public key submitted for certification. For that purpose the Applicant must prove to be in possession of the private key associated with the public key to be certified. For this purpose suitable asymmetric cryptographic techniques are used. Evidence of possession of the private key is typically provided through a self-signed certificate request in *PKCS*#10 format during the certificate application.

[1]VR-Ident SSL-Certificates are not issued for IP addresses and not for internal server names.

For all domains where *Fiducia & GAD IT AG* is registered as domain owner the proof of possession is omitted. *Fiducia & GAD IT AG* reserves the right to apply for certificates for its own domains directly. In such cases the keys and certificate requests are generated in the secure environment of *Fiducia & GAD IT AG*'s secure data center.

3.2.2. Authentication of Organizations

The *Certification Service* VR-Ident distinguishes between personal certificates and certificates issued to devices. Accordingly, the authentication of natural persons is different from the authentication for devices. The authentication of organizations is required only for certificates issued to devices. Mandatory for authenticating an organization is a valid record (not deleted, not invalid, not marked as inactive or deprecated) in an official public register. The name of the organization on the certificate application form must be identical to the name of the organization in the register.

The *Certification Service* VR-Ident accepts only evidences and applications in Latin script.

It accepts organizations only if they are registered in one of the following registers:

- official German Commercial Register (HRB)
- official German Register of Cooperatives (GnR).

Records in the above registers must mark the organization as "active".

In order to validate the identity of the Applicant the *Certification Service* VR-Ident verifies the existence of the organization submitting the certificate application and the domain-ownership or the right to use the domain name (by requesting a Domain Authorization document).

Employees of *Fiducia & GAD IT AG* or employees of *Fiducia & GAD IT AG* affiliates may apply for VR-Ident SSL-Certificates for subdomains of domains exclusively used by *Fiducia & GAD IT AG* (e.g.www.fiduciagad.de) if appropriately authorized to submit such applications. The following checks are performed directly or indirectly:

- The identification of the Requester is done through a secure login process at the VR-Ident Workflow Management System,
- Applications originating from employees of *Fiducia & GAD IT AG* affiliates must be approved by an authorized employee of *Fiducia & GAD IT AG*,
- The department and the Requester must be authorized to apply for VR-Ident SSL-Certificates for subdomains of domains exclusively used by *Fiducia & GAD IT AG* (e.g.www.fiduciagad.de),
- Control over the private key is in the department of the Requester,
- Applications are possible only for subdomains of domains exclusively used by *Fiducia & GAD IT AG* (i.e.*Fiducia & GAD IT AG* is registered by the registrar of the applicable Top-Level Domain (in this case DENIC) as the domain owner, e.g. www.fiduciagad.de) and this domain must match with the CommonName (CN) in the certificate application and request,
- The entry in the certificate request for "Country" must be "DE",
- The entry in the certificate request for "Organization" must be "*Fiducia & GAD IT AG*",
- The entry in the certificate request for "Organizational Unit" must be either "VR-Ident" or the name of the department of the Requester,
- The entry in the certificate request for "Locality" and "State" must match the values for *Fiducia & GAD IT AG* ("L=FRANKFURT AM MAIN", "ST=HESSEN").

VR-Banks can apply for VR-Ident SSL-Certificates at the GAD Service-Portal. The following checks are performed directly or indirectly:

- The identification of the Requester is done at the GAD Service-Portal based on the host identification and the Requester's RACF password,
- Check whether *Fiducia & GAD IT AG* is listed as the domain registrant of the domain or URL provided in the "Common Name" of the certificate application,
  - If this is not the case the Applicant must present a document proving its right to use the domain name (Domain Authorization document), signed by the legitimate domain owner,
- Online-verification with the applicable official register whether the data in the field "Organization" match with the data in the register,
  - if the name of the organization is longer than 64 bytes it must be appropriately shortened, if the record in the register is not unique the locality of the organization may be added as a suffix to the name of the organization. For example if the record in the register is "Volksbank eG" and there are more registers with such an entry, then "Volksbank eG Musterstadt" may be entered as name of the organization,
- Data in the certificate request in the OU-field (Organizational Unit) are checked against documents at *Fiducia & GAD IT AG* (alternatively the term "VR-Ident" may be used),
- Data in the L-field ("Locality") must match the data in the record obtained from the official commercial register,
- Data in the S-field ("State or Province") must match the data in the record obtained from the official commercial register
- Data in the C-field ("Country") must be equal to "DE" for organizations located in Germany.

After the application for a VR-Ident SSL-Certificate has been received from *Fiducia & GAD IT AG* affiliates or partners but before the certificate is issued the following checks are performed:

- Verification whether the Applicant is registered at the relevant domain registrar as the legitimate owner of the domain named in the field "Common Name",
- Verification of the domain record obtained from the domain registrar (or comparable documents) for
  - authenticity and completeness,
- Data in the field "Organization" must match with the data obtained from the official commercial register
  - if the name of the organization is longer than 64 bytes it must be shortened appropriately,
  - The organization must exist since at least 3 years,
    - or it must be a financial institute under governmental supervision,
    - or the Applicant must provide confirmed evidence that the organization has an active bank account at a regular bank,
  - The organization must be affiliated with *Fiducia & GAD IT AG* or the organization must be a known organization in the corporative association,
  - DBA names are not supported,
- Data in the certificate request in the OU-field (Organizational Unit) is checked against documents at *Fiducia & GAD IT AG*; the department or subdivision must be existent in the organization and the certificate Requester must be part of that organizational unit (alternatively the term "VR-Ident" may be used),
- Data in the S-field ("State or Province") must match the data in the record obtained from the official commercial register,
- Data in the S-field ("State or Province") must match the data in the record obtained from the official commercial register
- Only request from German organizations are accepted, therefore, the value in the Country field is predefined and equals "DE",

- The verification of the Requester's authority to apply for a certificate is performed through the Requester's secure login at the *VR-Ident Workflow Management* system.
- The verification whether the individuals named in the certificate application are authorized to request certificates on behalf of the organization is based on the written authorization of these persons signed by an authorized representative of the organization or through a telephone call to an authorized representative of the organization using a confirmed communication channel.

3.2.3. Authentification of Individuals

The *Certification Service* VR-Ident distinguishes between personal certificates and certificates issued to devices. Accordingly, the authentication of natural persons is different from the authentication for devices. The authentication of organizations is required only for certificates issued to devices. Individuals are identified only for certificate issued to individuals.

Documents are accepted only in they are in Latin script and German language.

The authentification of individuals as certificate owners of VR-Ident SSL-Certificates is not required because certificates are issued to organizations only.

3.2.4. Non-verified Subscriber Information

For the issuance of a certificate and in order to ensure trust in VR-Ident SSL-Certificates the identity of the certificate owner is verified and recorded. These verifications include only the identity of the certificate owner but not its financial status or trustworthiness .

Validation according to the prevention of money laundering act or checks of embargo lists are not performed because these checks have already been completed during the identification of the customer in "bank21" by means of the program GenoSonar. *Fiducia & GAD IT AG* itself and all *VR-Banks* are publicly recognized as well known and trustworthy. This also applies to *Fiducia & GAD IT AG* and its affiliates and partners.

All required data is validated at the time of registration. Whether this data is still correct at a later point in time can not be assured. The certificate owner is obliged to revoke its certificate if relevant data regarding the ownership structure (i.e. domain ownership, company ownership, company name) have changed.

3.2.5. Verification of Authority

Documents declaring a person as "authorized agent" must be signed by an authorized person named in the official register. For validating the signature of the authorized person named in the official register a qualified independent information source (QIIS) is used to determine the contact information of this person. This contact data is then used to obtain direct confirmation from the signer that he/she has signed the document.

3.2.6. Criteria for Interoperation

The certificate of the issuing CA "VR IDENT SSL CA 2016" has been signed by the Root CA "QuoVadis Root CA 2".

The interoperation is regulated by a contract with the operator of the Root-CA (Quo Vadis).

3.3. Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-key

For routine re-key requests of VR-Ident SSL-Certificates it is assumed that customer data is still valid. Customer data is regularly checked for being up-to-date (Chapter 3.2.2 [12]).

For VR-Ident EV SSL-Certificates it is ensured that these checks are performed immediately before the certificates are issued. Re-key of VR-Ident EV SSL-Certificates is handled identical to initial certificate issuance.

3.3.2. Identification and Authentication for Routine Re-key after Revocation

For routine re-key requests of VR-Ident SSL-Certificates after revocation it is assumed that customer data is still valid. Customer data is regularly checked for being up-to-date (cf. Chapter 3.2.2 [12]) - preferably directly before VR-Ident SSL-Certificates are re-keyed.

For VR-Ident EV SSL-Certificates it is ensured that these checks are performed immediately before the certificates are issued. Re-key of VR-Ident EV SSL-Certificates is handled identical to initial certificate issuance.

3.4. Identification and Authentication for Revocation Request

VR-Ident SSL-Certificates can be revoked only after the individual submitting the revocation request has been successfully identified. The revocation request (in writing, by e-mail, or by fax) must contain the reference number of the certificate (serial number) and the signature of the requester of the revocation. Revocation requests for internal VR-Ident SSL-Certificates used by *Fiducia & GAD IT AG* are authenticated through secure login of the person submitting the revocation request to the VR-Ident Workflow Management.

Chapter 4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application?

The following parties can apply for VR-Ident SSL-Certificates:

- *VR-Banks* and special institutes of *Fiducia & GAD IT AG*,
- *Fiducia & GAD IT AG*,
- *Fiducia & GAD IT AG* affiliates,
- Partners of *Fiducia & GAD IT AG*.

4.1.2. Enrollment Process and Responsibilities

Depending on the entity requesting a certificate the following enrollment processes are supported:

Authorized *Fiducia & GAD IT AG* employees may apply for VR-Ident SSL-Certificates for subdomains of domains exclusively used by *Fiducia & GAD IT AG* (e.g. www.fiduciagad.de) through the *VR-Ident Workflow Management*.

VR-Banks can apply for VR-Ident SSL-Certificates at the GAD Service-Portal.

Fiducia & GAD IT AG affiliates and partners: The application is carried out electronically by submitting an online order form (PDF). The Certificate Requester or another person authorized to apply fills out the online order form, it may be submitted in advance by e-mail. Additionally, the order form must be printed out on paper and it must be signed by the Requester. Together with an additional document serving as evidence for the name of the Requester's organization the order form must be submitted in paper form or by fax (0251 7133 - 91500) to *Fiducia & GAD IT AG*'s Registration Authority (department Auftragsmanagement).

As evidence for the name of the Requester's organization the following documents are required:

- Current excerpt from the official commercial register (Handelsregisterauszug)
- Proof that the Requester is authorized to apply for certificates. If the Requester is not authorized to apply for a certificate another person with such authority must be named in the order form.

The online order form is available for *Fiducia & GAD IT AG* affiliates and partners from "GAD Zertifikatsverwaltung" on request.

Certificate applications for VR-Ident EV SSL-Certificates must be in written form. The *Certification Service* VR-Ident provides suitable means for the submission of applications. The order forms must be signed by the Certificate Approver and the Contract Signer. The order form must be submitted in paper form or by fax (0251 7133 - 91500) to *Fiducia & GAD IT AG*'s Registration Authority (department Auftragsmanagement). This process applies for initial certificate applications as well as for renewal requests.

A natural person with authorization to order VR-Ident SSL-Certificates in the name of an organization may authorize one or more other persons to act in the name of the organization as Applicants (Chapter 1.3.3 [5]) and to request VR-Ident SSL-Certificates for domains registered by the organization. Such an authorization document must be signed by an authorized member of the organization and be marked with the organization's stamp or seal.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

The *Certification Service* VR-Ident performs identification and authentication as described in Chapter 3.2.2 [12]. All registration data is validated using dual control. Only if all data has been successfully validated the registration data is further processed and forwarded to the CA system as a certification order.

4.2.2. Approval or Rejection of Certificate Applications

Certificate applications are accepted only if identification and authentification of all required Applicant information in terms of Chapter 3.2.2 [12] and Chapter 3.2.3 [14]has been successfully completed.

Approval of certificate requests can not be claimed. In the following cases applications will be rejected:

- The Applicant or Requester can not be identified free of doubt,
- The Appplicant has violated the prevention of money laundering act or is on a list of denied persons or organizations,
- Relevant documents are not available e.g. the excerpt from the commercial register,
- There are doubts about the authenticity of submitted documents,
- The Applicant fails to respond to notices of *Fiducia & GAD IT AG* within a specified time,
- The *Certification Service* VR-Ident has other reasons to reject the application.

4.2.3. Time to Process Certificate Applications

Processing certificate applications begins within a reasonable time of receipt during the common business hours of *Fiducia & GAD IT AG*. There is no time stipulation to complete the processing of an application unless explicitly agreed upon in individual agreements

VR-Ident SSL-Certificates are issued immediately after the enrollment process has been successfully completed.

4.2.4. Certification Authority Authorization (CAA)

In January 2013 RFC 6844 „DNS Certification Authority Authorization“ (CAA) was published. The CAA DNS Resource Record allows a domain name holder to specify the Certification Authorities authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate mis-issue.

The *Certification Service* VR-Ident supports this mechanism since September 2017.

Before VR-Ident SSL-Certificates are issued the CAA Records are checked for each DNS name in the CommonName and in the SubjectAltNames fields. Certificates are issued at most 8 hours after the CAA Records have been validated.

The Property Tags "issue", "issuewild" and "iodef" are handled as specified in RFC 6844.

Excluded from this rule are domains where Fiducia & GAD IT AG is the operator of the domain's DNS Server according to RFC 7719.

The CAA domain for the *Certification Service* VR-Ident is "vr-ident.de".

4.3. Certificate Issuance

4.3.1. CA Actions During Certificate Issuance

A certificate is created and issued following the approval of a certificate application by the *RA* (*Registration Authority*) based on the information in the certificate application.

4.3.2. Notifications to Subscriber by the CA of Issuance of Certificate

The VR-Ident SSL-Certificate and the complete certificate chain is automatically sent to the Subscriber by e-mail. Attention should be paid to the fact that the file extension "cer" is used which could be disallowed by some firewalls or e-mail programs.

In the certificate application optional additional e-mail addresses can be specified. Notification of certificate issuance is automatically sent to these addresses, too.

4.4. Certificate Acceptance

4.4.1. Subscriber Conduct Constituting Certificate Acceptance

Issued VR-Ident SSL-Certificates and the entire certificate chain are sent by e-mail to the Subscriber. The certificate chain is specified in Chapter 1.3.1 [10].

By downloading and receiving the VR-Ident SSL-Certificate the certificate owner accepts the certificate. The Subscriber is obliged to check the certificate and its content for correctness.

4.4.2. Publication of the Certificate by the Certification Service

The *Certification Service* VR-Ident publishes issued VR-Ident certificates in its repository.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

There is no notification of other entities. Certificates are available from the VR-Ident repository as specified in Chapter 2.1 [8].

4.5. Key Pair and Certificate Usage

Usage of the key pair and the VR-Ident certificate by the owner and Relying Parties is permitted only according to the following conditions.

4.5.1. Subscriber Private Key and Certificate Usage

Using the Subscriber's private key is possible only after the associated VR-Ident certificate has been successfully integrated into the Subscriber's system.

Usage of the private key and the VR-Ident certificate is permitted only for the purposes specified in Chapter 1.4.1 [5]. The VR-Ident certificate may be used only pursuant to the stipulations in this *CPS* (*Certification Practice Statement*). Usage of the private key and the VR-Ident certificate is prohibited in the cases specified in Chapter 1.4.2 [5].

4.5.2. *Relying Party* Public Key and Certificate Usage

Usage of VR-Ident certificates by Relying Parties must follow the stipulations made in this CPS. Before relying on a VR-Ident certificate relying parties must verify that:

- using the certificate for a specific purpose is not prohibited or otherwise restricted by this CPS,
- using the certificate is in accordance with the keyUsage extensions in the certificate,
- the certificate is not revoked or has expired,
- at the time of validation the signature of the certificate can be successfully validated and the signature is based on a then valid CA-Certificate issued by the *Certification Service* Provider *Fiducia & GAD IT AG*.

Checking the revocation status may be based on a valid CRL or on a current OCSP request at the *Certification Service* VR-Ident. Furthermore, Relying Parties should use certificates only in suitable and approved software applications.

The validity of the VR-Ident CA-Certificate is checked analogously based on the validity of the Root-CA-Certificate.

4.6. Certificate Renewal

Certificate renewal is the issuance of a new certificate to the Subscriber with new validity period but without changing the public key or any other information in the certificate.

Certificate Renewal is not supported.

4.7. Certificate Re-Key

Certificate re-key is the replacement of a certificate with a new certificate with new validity period and a new public key while all other certificate data remains unchanged.

4.7.1. Circumstances for Certificate Re-Key

Prior to the expiration of an existing VR-Ident certificate it is necessary for the Subscriber to re-key the certificate to maintain continuity of certificate usage. A certificate may also be re-keyed after expiration. Certificate re-key may also be required if the old certificate has been revoked.

Because the content of a certificate can not be changed after issuance (Chapter 4.8 [19]) the extension of the validity period can only be achieved by issuing a new certificate with new validity period.

VR-Ident SSL-Certificates are valid for 13 months or 37 months.

To maintain the continuity of VR-Ident SSL-Certificate usage the certificate must be re-keyed before expiry. The upcoming option for certificate re-key is announced for the first time by e-mail to the Subscriber and to the GAD certificate management 60 days prior to the expiration of the certificate.

4.7.2. Who May Request Certification of a New Public Key

See Chapter 4.1.1.

4.7.3. Processing Certificate Re-Keying Requests

The processes for application processing and certificate issuance are identical to the processes for initial certificate application as described in Chapter 4.2 and in Chapter 4.3.

All customer data is regularly checked and re-validated. Routine re-key and re-key after revocation of VR-Ident SSL-Certificates are performed using current customer data.

For VR-Ident EV SSL-Certificates it is ensured that all validation steps are performed immediately prior to the issuance of the certificate. Certificate re-key is handled identical to initial certificate application and issuance.

4.7.4. Notification of New Certificate Issuance to Subscriber

Notification of Subscribers about re-keyed certificates is identical to the notification for initial certificate issuance as described in Chapter 4.3.2.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

Certificate acceptance for re-keyed certificates is identical to certificate acceptance for initial certificates (cf. Chapter 4.4.1).

4.7.6. Publication of the Re-Keyed Certificate by the CA

See Chapter 4.4.2 [18].

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

See Chapter 4.4.3 [18].

4.8. Certificate Modification

Certificate modification refers to the replacement of an existing certificate with a new certificate with changed information in the new certificate (other than the subscriber's public key) with unchanged validity period.

Certificate modification is not supported.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

The *Certification Service* VR-Ident reserves the right to revoke a CA-Certificate or VR-Ident-Certificate without delay for the following reasons:

- The *Certification Service* VR-Ident has a reasonable suspicion that a VR-Ident certificate has been misused,
- Information in the certificate are not or no longer in accordance with the facts, in particular, if continued use of the certificate violates legal provisions,
- It is strongly suspected or there is certainty that the private key corresponding to the certificate has been compromised or is not appropriately protected,
- The cryptographic algorithms and parameters used in certificates or for certificate signing are no longer considered suitable due to technological progress or new developments in cryptography,
- The *Certification Service* VR-Ident becomes aware that a certificate has not been issued in accordance with the provisions made in this CPS,
- The *Certification Service* VR-Ident terminates its *Certification Service* (Chapter 5.8 [31]),
- The certificate owner has breached the contractual obligations related to the *Certification Service* VR-Ident, e.g. the Subscriber has not submitted payment when due,
- The customer requests revocation of its certificate by fax or by e-mail,
- Another reason for revocation exists.

Furthermore, the *Certification Service* VR-Ident reserves the right to revoke a VR-Ident certificate if:

- The contract with the Subscriber ends.

In any case the *Certification Service* VR-Ident notifies the certificate owner about the revocation of the VR-Ident certificate by email.

Subscribers must request revocation of their own VR-Ident SSL-Certificates under the following circumstances:

- The Subscriber is aware or has reason to suspect that unauthorized persons have access to the private key corresponding to the certificate or can manipulate that key,
- The original certificate request was not authorized and the Subscriber does not retroactively grant authorization,
- Information in the certificate is incorrect or has changed, the organization's name has changed, or the domain registration has changed,
- The Subscriber is no longer authorized to use the domain name or the legitimate domain owner has not extended the Subscriber's authorization to use the domain name.

In these cases the Subscriber is obliged to notify the *Certification Service* VR-Ident without undue delay.

4.9.2. Who Can Request Revocation

The following parties are authorized to request revocation of VR-Ident certificates:

- The certificate owner or an authorized agent of the certificate owner may request the revocation of its own VR-Ident certificate,

- The*Certification Service* VR-Ident may request and execute the revocation of VR-Ident certificates and VR-Ident CA certificates,
- The *Certification Service* VR-Ident may request the revocation of the CA certificate "VR IDENT SSL CA 2016" from Quo Vadis.
- Der *Certification Service* VR-Ident may request the revocation of the CA certificate "VR IDENT GENERAL CA 2016" from Quo Vadis.

4.9.3. Procedure for Revocation Request

The *Certification Service* VR-Ident revokes VR-Ident SSL-Certificates on customer's request and after the requester has been identified. The following procedures for revocations are implemented:

- In writing: in this case the revocation request must include the certificate serial number and the signature of the requesting person,
- By e-mail: in this case the revocation request must include the certificate serial number and the signature of the requesting person,
- By fax: in this case the revocation request must include the certificate serial number and the signature of the requesting person.

The responsible person for the certificate and the GAD Certificate Management (GAD Zertifikatsverwaltung) are informed by e-mail about the revocation.

When the *Certification Service* VR-Ident has a reason to revoke a VR-Ident SSL-Certificate the manager of the *Certification Service* VR-Ident submits the revocation request to a Revocation Officer.

The revocation of the CA certificate "VR IDENT SSL CA 2016" on request of the *Certification Service* VR-Ident will be initiated by the management of *Certification Service* VR-Ident. According to the provisions of this CPS the request will be submitted to the operator of the Root-CA "QuoVadis Root CA 2".

The revocation of the CA certificate "VR IDENT SSL CA 2016" by QuoVadis is processed according to the applicable CPS of the Root-CA "QuoVadis Root CA 2".

4.9.4. Revocation Request Grace Period

Revocation requests shall be submitted without delay if a private key is compromised, suspected to be compromised, or compromise is imminent.

4.9.5. Time within which CA Must Process the Revocation Request

The CA begins investigation of a Certificate Problem Report within twenty-four hours of receipt, and decides whether revocation or other appropriate action is required.

VR-Ident SSL-Certificates are usually revoked within one or two workdays after the revocation request has been received. In urgent cases, for example if a private key is compromised, the revocation request is processed without delay.

Revocation requests for VR-Ident SSL-Certificates can be submitted 24x7 in writing, by e-mail (IND_Zertifikatssperre@fiduciagad.de), or by fax (0251 7133 - 91500). At most 4 days after receipt of a revocation request the revocation is processed and after one more day the revocation status information on the OCSP responder is updated. The time and frequency for the issuance and publication of CRLs is described in Chapter 2.3 [8].

4.9.6. Revocation Checking Requirements for Relying Parties

Third parties shall rely on a VR-Ident Certificate only after they have successfully validated the revocation status of the certificate.

Relying Parties can rely on a VR-Ident certificate when the certificate has not expired, is not revoked, and the certificate's signature is based on a valid (at the time of verification) CA-certificate of the *Certification*

Service Provider *Fiducia & GAD IT AG*. The revocation status can be checked through a valid CRL, by requesting the certificate from the LDAP directory, or by requesting the status from the *Certification Service* VR-Ident OCSP responder.

4.9.7. CRL Issuance Frequency

The time and frequency for the issuance and publication of CRLs is described in Chapter 2.3 [8].

4.9.8. Maximum Latency for CRLs

*CRL*s are added to the database immediately after issuance. They can be downloaded from the VR-Ident Repository.

4.9.9. On-Line Revocation/Status Checking Availability

Certificate revocation status information is available online. All revoked certificates of *Certification Service* VR-Ident are included. The OCSP service as well as the Repository are available 24x7.

4.9.10. On-Line Revocation Checking Requirements

Relying Parties are required to check the VR-Ident Repository of issued and revoked certificates before relying on a certificate. Revocation status information is available via the standard protocols *OCSP* and *LDAP*.

4.9.11. Other Forms of Revocation Advertisements Available

There are no other forms of revocation advertisement.

4.9.12. Special Requirements Regarding Key Compromise

There are no special requirements regarding key compromise. When a private key is compromised the corresponding certificate must be revoked without delay.

4.9.13. Circumstances for Suspension

Suspension of VR-Ident certificates is not supported.

4.10. Certificate Status Services

The Certificate Status Service is based on the "Online Certificate Status Protocol" (*OCSP*), Version 1, according to *RFC* 6960. It provides online status information for VR-Ident certificates.

4.10.1. Operational Characteristics

The OCSP responder is available at the URL given in Chapter 2.1 [8]. The OCSP responder uses the transport protocol *HTTP* and implements the"Online Certificate Status Protocol" (*OCSP*) with the following characteristics:

- Requests (OCSP-Requests) need not to be signed; signed requests are also supported,
- The responses of the *OCSP-Responder* are positive information; if the response to a request delivers the status "good" this means that the requested certificate is available in the VR-Ident directory and that it is currently valid,
- The *OCSP-Responder*s use a continuously updated database. The field "NextUpdate" contains the time of the next scheduled update to certificate status information. Responses should not be stored and used beyond the value of the "NextUpdate" field,
- Certificate status information is available for at least 7 years after the expiry of the certificate,

- The extensions (OCSP-Extensions) which are supported and used are provided in Chapter 7.3 [42].

Each *CA* issues a CRL responsible for the certificates it issues with the following characteristics:

- The *CRL* is conform with the standards *X.509*, *RFC* 5280, and Common *PKI* (cf. Appendix with general References),
- The *CRL* is signed by the CA, it is a direct CRL,
- The *CRL*s are stored in the VR-Ident *Directory Service* (Chapter 2.1 [8]) in the attribute of the relevant CA-object,
- The *CRL*s are valid until the next scheduled CRL is issued. The frequency for CRL issuance is defined in Chapter 2.3 [8],
- The *CRL*s contain the serial numbers of all revoked certificates issued by the respective CA, even for those where the certificate owner has not declared consent to the publication of the certificate,
- Revoked Certificates remain on the CRL for at least 7 years after the expiry of the Certificate,
- The CRL extensions are provided in Chapter 7.2 [41].

For the Certification Service VR-Ident the following provisions regarding *OCSP-Responder*s for VR-Ident SSL-Certificates apply:

- For the "VR IDENT SSL CA 2016" an OCSP-Responder is set-up which is available at a dedicated URL.
- The *OCSP-Responder* of the "VR IDENT SSL CA 2016" provides revocation status information for VR-Ident SSL-Certificates.

4.10.2. Revocation Status Service Availability

The *OCSP-Responder*s of the *Certification Service* VR-Ident are available 24x7. The OCSP response time is less than 10 seconds under normal operating conditions.

The *Certification Service* VR-Ident maintains a continuous 24x7 ability to respond internally to high-priority certificate problem reports. Where appropriate such a complaint is forwarded to law enforcement authorities and/or the certificate that is subject to the complaint is revoked.

4.10.3. Optional Features

Requests submitted to the *OCSP-Responder*s may include the extension "Nonce". This extension is a preventive mechanism against attacks sending old responses (Replay-Attacks). The OCSP-Responder encodes the value of the nonce submitted in the request and returns the encoded value in the extension "Nonce" of the response.

All OCSP responses include the hash value of the requested certificate.

In addition, the certificate can be included in the OCSP response – provided that the certificate owner has declared consent to the publication of the certificate – by using the extension "RetrieveIfAllowed" in the request.

4.11. End of Subscription

A Subscriber or customer ends its subscription to the *Certification Service* VR-Ident if all its certificates have expired or been revoked and no new certificates have been ordered. This is the case if

- the Subscriber requested the revocation of all of its certificates,
- the Subscriber terminates the contractual agreements with the *Certification Service* Provider *Fiducia & GAD IT AG* or with its VR-Bank,

- the *Certification Service* VR-Ident initiates the revocation of all certificates of the Subscriber, and this is not done in the course of replacing these certificates with new ones, or
- the VR-Ident certificates expire and no new certificates are requested and issued.

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

The *Certification Service* VR-Ident neither offers key escrow nor performs it.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

The *Certification Service* VR-Ident neither offers nor performs key escrow.

Chapter 5. Facility, Management, and Operational Controls

5.1. Physical Controls

5.1.1. Site Location and Construction

Fiducia & GAD IT AG's *Certification Service* VR-Ident is operated in a physically protected environment in the secure data center of *Fiducia & GAD IT AG* in the GAD Straße 2-6 in 48163 Münster. The construction meets high security standards related to physical security and protection. It is designed to provide a high level of protection against intrusion. In addition, precautionary provisions are made against fire, water, and lightning. The IT-systems of the *Certification Service* VR-Ident are located in a secure area inside *Fiducia & GAD IT AG*'s premises. In order to ensure uninterrupted service in case of an emergency the *Certification Service* VR-Ident maintains redundant hardware and backups of its CA and infrastructure system software. The redundant systems are located in separate rooms in a disaster recovery data center.

5.1.2. Physical Access

Appropriate measures for access control provide a high level of protection against unauthorized intrusion into the rooms and against unauthorized access to security relevant systems and data. Access control is token-based for rooms with IT-systems of the *Certification Service* VR-Ident. Most parts of the premises and the data center, in particular, entrance areas, corridors, and rooms where IT-systems are located are under video surveillance at all times.

5.1.3. Power and Air Conditioning

The data center of *Fiducia & GAD IT AG*, where the *Certification Service* VR-Ident is operated, is equipped with power systems to ensure continuous, uninterrupted access to electric power supply.

Industry standard heating/ventilation/air conditioning systems control temperature and relative humidity of the IT-rooms and IT-systems of the *Certification Service* VR-Ident. Correct functioning of the heating/ventilation/air conditioning systems is continuously monitored..

5.1.4. Water Exposures

The data center of *Fiducia & GAD IT AG* and especially the rooms with technical equipment are protected against water exposure by constructional measures.

5.1.5. Fire Prevention and Protection

For the data center of *Fiducia & GAD IT AG* appropriate fire protection measures have been implemented to prevent fire and other damages by fire. The fire protection measures are implemented in compliance with the German fire protection regulations.

5.1.6. Media Storage

All media containing critical data (e.g. backups) is stored within *Fiducia & GAD IT AG* facilities protected against unauthorized access and accidental damage (fire, water, and electromagnetic). Media containing very critical data are stored in a safe.

5.1.7. Waste Disposal

Media used to collect or transmit sensitive information are physically destroyed (e.g. by cutting the chip in pieces or shredding) prior to disposal. Paper documents containing sensitive information are shredded prior to disposal.

5.1.8. Backup

Data of the *Certification Service* VR-Ident is regularly backed up. The backup includes all data collected during the certification process, log and audit files, and other relevant data. Backup media are securely handled and stored (cf. Chapter 5.1.6 [25]).

5.2. Procedural Controls

5.2.1. Trusted Roles

Functions in the certification service may be performed exclusively by authorized personnel in trusted roles. These are employees which have been assigned to the roles. In particular, trusted roles are:

- personnel performing system administration,
- PKI operators,
- security staff,
- responsible technical personnel,
- auditors or revisers, and
- roles with senior management functions.

Persons in trusted roles must be trustworthy and sufficiently qualified for their roles.
Roles and their duties are described in detail in the role concept of *Fiducia & GAD IT AG*'s security policy .

5.2.2. Number of Persons Required per Task

For security critical activities requiring a high level of protection regarding confidentiality, like access to the Hardware Security Modules (*HSM*) and the associated cryptographic keys and its management, dual control is required. Existing policies and controls enforce that physical and logical access to critical devices requires co-operation of at least two employees in trusted roles. Access to other security relevant systems of the *Certification Service* VR-Ident and their backup data is also performed under dual control. For the following activities dual control is enforced:

- Administrative or operative access to Hardware Security Modules (*HSM*),
- Initial exchange of cryptographic system keys,
- Key Ceremonies.

5.2.3. Identification and Authentication for Each Role

Identification and authentication of persons in trusted roles in the secure areas of the data center and when logging into IT-systems is achieved by the use of access cards or by using username and password. Login of *PKI* operators at the VR-Ident *PKI* systems is based on authentication certificates.

5.2.4. Roles Requiring Separation of Duties

The role concept regulates which roles require separation of duties. The following rules apply:

- The management personnel of *Fiducia & GAD IT AG* may not perform operative or administrative tasks,
- Auditors and Revisers may not perform operative or administrative tasks,
- System administrators may not perform operative tasks,

- Persons in trusted roles administering the access rights to the premises of *Certification Service* VR-Ident may not perform other operative or administrative tasks.

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

The *Certification Service* VR-Ident employs only personnel with the required expertise, experience, and qualification.

5.3.2. Background Check Procedures

All employees of the *Certification Service* VR-Ident are checked for reliability. Persons in trusted roles must present a clearance certificate issued by the responsible governmental agency before being assigned to their roles. Background checks for persons in trusted roles are repeated in regular intervals.

5.3.3. Training Requirements

All personnel concerned with duties in the certification service are appropriately trained and sensitized prior to beginning their occupation. Among others, training covers the following topics:

- Basic knowledge about PKI,
- Awareness for IT security,
- Incident reporting and handling,
- Emergency handling,
- Handling of passwords, PINs, and smart cards,
- Handling of person related data,
- Data backup and creating backups.

5.3.4. Retraining Frequency and Requirements

For maintaining the qualification of personnel retrainings are conducted. Depending on the job description trainings are repeated regularly or as needed.

5.3.5. Job Rotation Frequency and Sequence

Regular job rotation is not required because of separation of roles and duties and the implementation of dual control for security relevant tasks.

5.3.6. Sanctions for Unauthorized Actions

If an employee acts against instructions and/or provisions steps are taken to prevent such irregularities in the future. In severe cases this can include consequences according to German labor law or criminal law.

5.3.7. Independent Contractor Requirements

Employees of the *Certification Service* Provider *Fiducia & GAD IT AG* are obliged to observe instructions and legal provisions. This includes the obligation to keep person related data in confidence.

If external persons (independent contractors or consultants) are appointed to trustworthy positions they underlie the same functional and security criteria as regular employees of the *Certification Service* Provider *Fiducia & GAD IT AG* in comparable positions.

5.3.8. Documentation Supplied to Personnel

The *Certification Service* VR-Ident makes available for its employees all documentation required to perform their tasks. The following documents are handed out to the employees:

- Informationen regarding relevant laws and legal regulations,
- Technical norms and specifications,
- This *CPS* (*Certification Practice Statement*) ,
- Internal security concepts, operating concepts, operating manuals,
- Instructions for use of systems and software.

5.4. Audit Logging Procedures

5.4.1. Types of Events Recorded

The *Certification Service* VR-Ident records (automatically in electronic form or in paper form) the following relevant events:

- Events in the life-cycle of VR-Ident certificates, including:
  - Collection of customer master data for VR-Ident certificates,
  - Enrollment for VR-Ident certificates,
  - Issuance of VR-Ident certificates,
  - Dissemination of VR-Ident certificates,
  - Revocations,
  - Generation and publication of CRLs.
- Application data and validation of authorizations
  - Acceptance of "Certification Practice Statement" (CPS) as agreement to special conditions,
  - Identity of the entity accepting the application,
  - Method used for validating submitted authorizations (if applicable).
- Registration data
  - Enrollment data for VR-Ident SSL-Certificates in the Key Management Workflow (internal VR-Ident SSL-Certificates) and in the GAD Service-Portal (*VR-Banks*),
  - Application forms in paper form or in electronic form in the order management system of Fiducia & GAD IT AG.
- Events in the life-cycle of CA certificates and key pairs:
  - Key generation, archival, and destruction of CA keys,
  - Issuance of CA-certificates,
  - Publication of CA-certificates,
  - Revocations of CA-certificates,

  - Issuance and publication of *CRL*s.
- Security relevant events, including:
  - Login to PKI systems,
  - Assignment and revocation of access rights,
  - Access and access attempts to networks,
  - Performing individual process steps in the Key Management Workflow, bank21, and in the GAD Service-Portal,
  - Events in the life-cycle of HSMs.
- Events related to the access control system, including:
  - Entering and leaving secured rooms,
  - Failed access attempts and alarms,
  - Assignment and revocation of access rights,
  - Application for, issuance of, and revocation of access cards.

All records include:

- Type of entry,
- Time and date of entry (synchronization is carried out through an internal NTP server receiving time information from an official time signal),
- Identification of the entity making the entry.

5.4.2. Frequency of Processing Log

Log files are reviewed in regular intervals. In case of suspected irregularities they are reviewed immediately.

5.4.3. Retention Period for Audit Log

Audit log files documenting events in the life-cycle of certificates, (especially audit files of the CA-systems) are retained for at least 7 years beyond the expiry date of the certificates.

5.4.4. Protection of Audit Log

Audit logs are protected against unauthorized access and manipulation by access control mechanisms. It is clearly defined which roles may access which data.

5.4.5. Audit Log Backup Procedures

All electronic audit data is regularly transferred to backup media.

5.4.6. Audit Collection System (Internal vs. External)

All audit logs are stored in the secure area of the data center. There are no external audit collection systems.

5.4.7. Notification to Event-Causing Subject

All employees of the *Certification Service* Provider *Fiducia & GAD IT AG* are aware of the extent of the collection of records about their activities.

5.4.8. Vulnerability Assessments

Possible vulnerabilities are assessed by continuous monitoring, by security audits carried out by the Information Security Officer of the *Certification Service* Provider *Fiducia & GAD IT AG*, and by regular vulnerability assessments performed by external auditors.

An overall risk assessment covering all PKI services is performed once per month.

5.5. Records Archival

5.5.1. Types of Records Archived

The *Certification Service* VR-Ident has implemented systems and processes to ensure the integrity of stored data. Regular routine backups are produced. The archive includes the entire PKI database.

5.5.2. Retention Period for Archive

Certificates and related data are archived for a period of at least 7 years after expiry of the respective certificate.

Paper documents (e.g. application forms) are also archived for at least 7 years.

5.5.3. Protection of Archive

Archived data is protected by technical measures against intentional or accidental manipulations or deletion. Access to this data is restricted to authorized personnel in trusted roles. Archived data is secured against damage by fire, water, or other environmental influences. During the retention period the readability of archived data is ensured.

5.5.4. Archive Backup Procedures

All electronic archive data is included in the regular backup process.

5.5.5. Requirements for Time-Stamping of Records

Archived data is not secured with cryptographic time-stamps. However, every record includes date and time of the event causing the generation of the record.

5.5.6. Archive Collection System (Internal or External)

All archive data is stored in the secure area of the data center. There are no external archive collection systems.

5.5.7. Procedures to Obtain and Verify Archive Information

The procedures to collect and verify archive data are defined in internal operating instructions.

5.6. Key Changeover

Key pairs used by the *Certification Service* VR-Ident for the provision of *Certification Service*s have a limited validity period which is specified in the corresponding certificate. CA key pairs are replaced prior to expiry. CA keys are replaced at an early stage such that the validity period of end-entity VR-Ident certificates does not exceed the validity period of the CA-Certificate. This routine key changeover does not require the revocation of the old CA-Certificate.

A non-routine key changeover for CA-keys is performed in the following cases:

- The certificate of the Certification Service VR-Ident is revoked,
- It was noticed or it is suspected that the private CA-key is compromised,

- The cryptographic algorithm or key length of the CA-key is no longer considered secure for the scheduled life-time of the key,
- The superior CA-Certificate is revoked.

In case of non-routine key changeover the corresponding CA-Certificate will be revoked. The revocation of a CA-Certificate invalidates all certificates issued by that CA-Certificate.

If a CA-Certificate is revoked this fact will be immediately published on website of the *Certification Service* VR-Ident. The persons responsible for the invalidated VR-Ident certificates are notified by e-mail without delay.

On key changeover the VR-Ident CA generates a new key pair and for the new key pair a new certificate is issued. After key changeover the private key of the old key pair is destroyed.

In case of a known or suspected key compromise the regulations of Chapter 5.7.3 [31] apply.

If the VR-Ident CA-Certificate has been issued by an external *Root-CA* the operator of the external Root-CA is responsible for the Root-CA's key changeover.

5.7. Business Continuity Management and Incident Handling

5.7.1. Incident Handling and Emergency Procedures

Fiducia & GAD IT AG has established an Incident Management System allowing a timely and effective reaction to incidents. For the data center internal emergency plans exist determining procedures and responsibilities for emergencies and disasters. Objective of these emergency procedures is minimizing outages of the services and at the same time maintaining security.

All systems involved in the provision of PKI services are installed in two distinct data centers in a redundant way. In case of an outage of one of the data centers the continuous operation of the PKI is ensured. An outage of up to one day is considered acceptable. The recovery time objective is one workday.

5.7.2. Computing Resources, Software, and/or Data are Corrupted

After suspected or real compromise of resources, software, or data the emergency procedures are invoked. For recovery of compromised resources, software, or data the latest backups of system configurations and data that have not been corrupted are used. The procedures for recovery from corruption of resources are determined in an internal recovery concept.

5.7.3. CA Private Key Compromise Procedures

If the private key of a CA of the *Certification Service* Provider *Fiducia & GAD IT AG* is compromised the corresponding certificate and all certificates issued from the CA-key are revoked.

Furthermore, the circumstances causing the key compromise are investigated. In particular, it is examined whether the algorithms, parameters, and devices used for generating and operating the private key have become insecure.

All affected subscribers and organizations are notified by e-mail that the CA-Certificate is revoked.

5.7.4. Business Continuity Capabilities after a Disaster

After a disaster operation is continued by the redundant infrastructure. Business continuity procedures are included in the internal emergency concept and in the emergency manual of the data center..

5.8. Termination of Certification Service

In case of termination of the*Certification Service* VR-Ident all participants are notified.

In the event of termination of the *Certification Service* VR-Ident the following measures are taken:

- The *Certification Service* VR-Ident notifies (in writing or by e-mail) Subscribers and other contract partners three months in advance of the termination and informs them whether another *Certification Service* Provider will adopt the services and the certificates.
- If no other *Certification Service* Provider continues the VR-Ident revocation service, directory service, and revocation status service for the VR-Ident certificates the *Certification Service* VR-Ident is authorized to revoke all certificates prior to termination of services. At the time of termination the CA-Certificates will be revoked and the corresponding private keys will be destroyed.
- The termination will be announced on the website http://www.vr-ident.de.
- If needed the *Certification Service* VR-Ident will also notify third parties (e.g. VR-Banks) of the termination.
- If required the *Certification Service* VR-Ident notifies the applicable third party auditing firm.

Chapter 6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

Key pairs for certificate signing (CA-keys) and for OCSP-signing are generated in Hardware Security Modules (HSM) certified according to *FIPS 140-2* Level 4 (cf. Appendix with general References). CA key generation follows a Key Ceremony Policy, is performed by authorized persons in trusted roles, and witnessed by an independent qualified auditor. The HSMs are located in the physically secure area of the data center. Access is strictly restricted to authorized personnel. All activities related to key generation are recorded.

End-entity key pairs are usually generated by the applicant itself. The *Certification Service* VR-Ident recommends to use *Hardware Security Module*s (*HSM*s) certified according to *FIPS 140-2* Level 2 or a comparable standard (like *CC* (*Common Criteria*)) for key generation.

For all domains where *Fiducia & GAD IT AG* is registered as the domain owner key pairs are generated in the secure environment of *Fiducia & GAD IT AG*'s data center. For this purpose *FIPS 140-2* Level 4 evaluated HSMs are used. On request *Fiducia & GAD IT AG* offers this key generation service also for other organizations.

6.1.2. Private Key Delivery to Subscriber

If the subscriber generates its key pair private key delivery is not required.

If key pairs are generated by *Fiducia & GAD IT AG*, as described in Chapter 6.1.1 [33], private keys are transmitted to subscribers in PIN-protected files (e.g. *PKCS*#12, JKS, PEM).

6.1.3. Public Key Delivery to Certificate Issuer

Public keys are submitted in a self-signed Certificate Signing Request.

6.1.4. CA Public Key Delivery to Relying Parties

The CA public keys can be downloaded from the public repository (cf. Chapter 2.1) [8] or from the website http://www.vr-ident.de. The associated fingerprints are available at these locations as well.

6.1.5. Key Sizes

The *Certification Service* VR-Ident uses RSA keys with key length

- 2048 bit for the superior external Root CA,
- 2048 bit for the VR-Ident CAs,
- at least 2048 bit for subscribers.

6.1.6. Public Key Parameters Generation and Quality Checking

The VR-Ident CAs perform public key quality checking as required by clause 6.1.6 of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates as published by the CA/Browser Forum.

6.1.7. Key Usage Purposes

Using private keys of VR-Ident Certificates is permitted only according to the provisions made in Chapter 1.4.1 [5].

The specific key usage purpose depends on the key and is specified in the certificate extensions "keyUsage" and "extendedKeyUsage" (Chapter 7.1 [38]).

The key usage of CA private keys is specified in the certificate extension "keyUsage" in the CA certificate (Chapter 7.1 [38]).

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

The *Certification Service* VR-Ident uses *Hardware Security Module*s which are certified according to the standard *FIPS 140-2* Level 4. The HSMs are operated according to the provisions made in the HSM's certification.

6.2.2. Private Key (m out of n) Multi-Person Control

Administrative or operational access to HSMs requires the participation of at least two persons in trusted roles. After the HSMs have been initialized (and before keys are generated) dual control is implemented and technically enforced by generating credentials (passphrases or smart cards) for the persons in trusted roles among which the control is to be shared.

6.2.3. Private Key Escrow

Key escrow is not supported.

6.2.4. Private Key Backup

The *Certification Service* VR-Ident creates backup copies of CA private keys for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form in a database.

Subscriber private keys are not backed-up by the *Certification Service* VR-Ident.

6.2.5. Private Key Archival

CA private keys are not archived. After expiry of the key usage period CA private keys can not be used any more.

6.2.6. Private Key Transfer into or from a Cryptographic Module

Private CA keys are protected by Hardware Security Modules (*HSM*s) and stored in encrypted form. If a private key must be transferred from one HSM to another HSM (e.g. for recovery) such a transport between modules is in encrypted form.

Subscriber private keys are not transferred if generated by the subscriber. Chapter 6.1.1 [33] describes how private keys are transferred from *Fiducia & GAD IT AG* to subscribers if keys are generated by *Fiducia & GAD IT AG*.

6.2.7. Private Key Storage on Cryptographic Module

CA private keys are either stored on the Hardware Security Modules or in the database in encrypted form.

The *Certification Service* VR-Ident does not store subscriber private keys.

6.2.8. Method of Activating Private Key

CA private keys are activated by two Key Managers under dual control. Both of them must authenticate at the system with the HSM using their individual usernames and passwords.

Subscriber private keys are activated by installing them on the webserver and entering the PIN. The PIN is chosen by the subscriber during key generation.

If the key pair is generated by *Fiducia & GAD IT AG* the PIN is sent to the subscriber on a separate communication channel.

6.2.9. Method of Deactivating Private Key

CA private keys are automatically deactivated when the CA application using the private key on the HSM terminates.

CA private keys that are no longer used are deactivated permanently on the HSM by the key managers.

Subscriber private keys are deactivated by logging off from the system or by shutting down the webserver application.

6.2.10. Method of Destroying Private Key

CA private keys are securely erased from the HSM before the HSM is removed from its secure environment (e.g. for repair or disposal). CA private keys can not be used beyond the key usage expiry date. CA private keys which have expired or otherwise became invalid and are not used anymore are erased from the systems.

For subscriber private keys it is the responsibility of the webserver administrator to erase the private key if it is no longer needed.

6.2.11. Cryptographic Module Rating

See Chapter 6.2.1 [34].

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

Public keys are included in the certificates. They are archived in the VR-Ident directory for at least 7 years.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

CA private keys are not used beyond the expiry of the corresponding certificates (Chapter 6.2.1 [34]). The validity period of CA certificates is at most 20 years.

The validity period of VR-Ident SSL-Certificates is 13 months or 37 months, VR-Ident EV SSL-Certificates are valid for 27 months.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

Activation data for private CA keys is generated according to Chapter 6.2.2 [34] and the provisions of the Key Ceremony either randomly by the Hardware Security Module or by the responsible trusted role. Persons in trusted roles are obliged to choose strong passwords to protect CA private keys from unauthorized access. The generation of activation data is logged and recorded.

For activation data of Subscriber keys the *Certification Service* VR-Ident recommends using strong passwords.

6.4.2. Activation Data Protection

The *Certification Service* VR-Ident has implemented the following security measures for CA private key activation data protection:

- Every employee of the *Certification Service* VR-Ident is obliged to handle its passwords and PINs confidentially and not to note them somewhere,

- Every employee of the *Certification Service* VR-Ident is obliged to protect its activation data for HSMs from misuse and to store hem securely after use,
- If an employee of the *Certification Service* VR-Ident is terminated its access rights are removed. Shared credentials (e.g. role based passwords) are removed and replaced by new credentials.

Subscriber activation data must be protected against unauthorized access.

6.4.3. Other Aspects of Activation Data

Removal of activation data is carried out in a manner that prevents loss, theft, disclosure, or unauthorized use of keys protected by this activation data.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

The IT-systems used for the provision of crucial *Certification Service*s, in particular, the CA-system, the *OCSP-Responder*s, and the RA systems, as well as other systems protecting the Certification Service facilities meet the following security requirements:

- Only necessary applications are installed,
- Only necessary communication interfaces are enabled. In particular, systems are integrated only in those network segments which are necessary for their functionality,
- Systems are located in locked cabinets in the *Fiducia & GAD IT AG* data center,
- Access to systems is restricted to the minimum needed for proper operations. System administration is carried out by authorized administrators only,
- Access to critical systems and components like Hardware Security Modules is based on separation of duties (for eyes principle),
- Systems with high availability demands (e.g. the VR-Ident revocation status service) are installed redundantly such that service availability is maintained even in case of system failure,
- Uninterruptable power supply units compensate fluctuation of current and are capable of bypassing power outages for several hours,
- Data storage media are checked for malicious software before use,
- IT systems are continuously monitored,
- Security relevant incidents are reported and recorded.

6.5.2. Computer Security Rating

A formal evaluation of system security has been carried out for the *Hardware Security Module*s, see Chapter 6.2.1 [34]).

The *Certification Service* VR-Ident has implemented technical security mechanisms and measures. Their suitability is ensured by continuous monitoring and assessed through security audits performed by the *Certification Service* VR-Ident Information Security Officer and external auditors.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

Applications are developed and implemented by *Fiducia & GAD IT AG* in accordance with *Fiducia & GAD IT AG*'s systems development and change management standards.

The security measures implemented in the development of of the HSMs which are evaluated and certified according to FIPS-140-2 or CC (Common Criteria) are in compliance with the strict provisions of the certification or evaluation procedures.

6.6.2. Security Management Controls

Security Management Controls are defined in the security concept of *Fiducia & GAD IT AG*.

6.6.3. Life Cycle Security Controls

The *Certification Service* VR-Ident ensures that software used for the *Certification Service*s is developed, tested, delivered, installed, configured, operated, and maintained in a manner that its authenticity, integrity, and intended functionality is preserved.

6.7. Network Security Controls

The *Certification Service* VR-Ident has implemented the following measures regarding network security:

- The PKI systems are separated from the internet by firewalls;
- Security relevant systems which must be accessible from the internet (e.g. *OCSP-Responder*s and the VR-Ident *Directory Service*) are located in a *DMZ* which is separated from the internet and from internal networks by firewalls. All other security relevant systems are located in internal network segments;
- Communication ports are enabled only if necessary for the provision of services;
- Network security is continuously monitored. If security breaches are detected appropriate responsive actions are initiated;
- Attacks on systems exposed to the internet are monitored and stopped where necessary.

6.8. Time-Stamping

The *Certification Service* VR-Ident does not operate a time-stamping service. All log and audit data include time and date of creation.

Chapter 7. Certificate, CRL, and OCSP Profiles

7.1. Certificate Profile

Certificates in the VR-Ident PKI conform to the standard X.509. As applicable, VR-Ident certificates conform to the current versions of the CA/Browser Forum "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" and the "Guidelines for the Issuance and Management of Extended Validation (EV) SSL Certificates". Certificates include data about their validity period, the signature algorithm used, the key size, the subscriber, and the issuer. Using the certificate extensions defined in the X.509 standard additional information may be included in certificates.

"QuoVadis Root CA 2" Certificate

The "QuoVadis Root CA 2" certificate contains the following basic data:

Table 7.1. "QuoVadis Root CA 2" Certificate

Certificate field	Content
Version	V 3
Serial number	05 09
Signature algorithm	sha1RSA
Issuer DN	CN = QuoVadis Root CA 2 O = QuoVadis Limited C = BM
Valid not before	Friday, November 24 2006 19:27:00
Valid not after	Monday November 24 2031 19:23:33
Subject DN	CN = QuoVadis Root CA 2 O = QuoVadis Limited C = BM
Public key	Encoded value of the key, RSA 4096 bit
Signature	Digital signature of the QuoVadis Root CA 2
Fingerprint algorithm	sha1
Fingerprint (sha1)	ca 3a fb cf 12 40 36 4b 44 b2 16 20 88 80 48 39 19 93 7c f7

"VR IDENT SSL CA 2016" Certificate

The "VR IDENT SSL CA 2016" Certificate contains the following basic data:

Table 7.2. "VR IDENT SSL CA 2016" Certificate

Certificate field	Content
Version	V 3
Serial number	4d 14 49 94 d4 f1 f2 7e dc 42 f3 5e 84 ce fa 07 e9 88 fe 02
Signature algorithm	sha256RSA
Issuer DN	CN = QuoVadis Root CA 2 O = QuoVadis Limited C = BM
Valid not before	Tuesday, January 12, 2016 16:53:00
Valid not after	Monday, January 12, 2026 16:53:00
Subject DN	CN = VR IDENT SSL CA 2016 O = FIDUCIA & GAD IT AG

	OU = VR IDENT C = DE
Public key	Encoded value of the key, RSA 2048 bit
Signature	Digital signature of the QuoVadis Root CA 2
Fingerprint algorithm	sha1
Fingerprint (sha1)	29 ef 54 e6 a0 4a b1 9a 0d d6 87 e9 ee c0 5b 16 3d b5 96 25

VR-Ident SSL-Certificates

The *Certification Service* VR-Ident issues VR-Ident SSL-Certificates according to *X.509* Version 3, *RFC* 5280, and Common *PKI*. In the basic fields the certificates contain the following data:

Table 7.3. VR-Ident SSL-Certificates

Certificate field	Content
Version	V 3
Serial number	Unique value, non-zero, non-sequential, with at least 64 bit of randomness
Signature algorithm	sha256RSA
Issuer DN	CN = VR IDENT SSL CA 2016 O = FIDUCIA & GAD IT AG OU = VR IDENT C = DE
Valid not before	Date and time
Valid not after	Date and time
Subject DN	CN = URL or Domain of the organization OU = VR-IDENT (example) O = Name of the organization/company L = Frankfurt am Main (example) ST = Hessen (example) C = DE
Public key	Encoded value of the key
Signature	Digital signature of the VR IDENT SSL CA 2016
Fingerprint algorithm	sha1
Fingerprint (sha1)	SHA-1 value of the certificate

7.1.1. Version Number(s)

VR-Ident certificates are *X.509* Version 3 certificates.

The certificate of the "QuoVadis Root CA 2" is a *X.509* Version 3 certificate.

7.1.2. Certificate Extensions

"QuoVadis Root CA 2" Certificate

The extension fields of the "QuoVadis Root CA 2" are shown in the following table:

Table 7.4. Extensions of the "QuoVadis Root CA 2" Certificate

Extensions	
KeyUsage	Certificate Sign, CRL Sign (06)
SubjectKeyIdentifier	1a 84 62 bc 48 4c 33 25 04 d4 ee d0 f6 03 c4 19 46 d1 94 6b

AuthorityKeyIdentifier	Key-ID=1a 84 62 bc 48 4c 33 25 04 d4 ee d0 f6 03 c4 19 46 d1 94 6b DirName: CN=QuoVadis Root CA 2 O=QuoVadis Limited C=BM SerialNumber=05 09
Critical Extensions	
BasicConstraints	CA:TRUE PathLen Restriction: none

"VR IDENT SSL CA 2016" Certificate

The extensions of the "VR IDENT SSL CA 2016" Certificate are shown in the following table:

Table 7.5. Extensions of the "VR IDENT SSL CA 2016" Certificate

Extensions	
CertificatePolicies	Policy=2.23.140.1.2.2 Policy=1.3.6.1.4.1.8024.0.2.1600.0.1 CPS qualifier: http://www.quovadisglobal.com/repository Policy=1.3.6.1.4.1.17696.4.1.1.9 CPS qualifier: http://www.vr-ident.de
AuthorityInfoAccess	OCSP - URL=http://ocsp.quovadisglobal.com CA Issuers - URL=http://trust.quovadisglobal.com/qvrca2.crt
ExtendedKeyUsage	serverAuth, clientAuth, OCSPSigning
AuthorityKeyIdentifie	KeyID=1a 84 62 bc 48 4c 33 25 04 d4 ee d0 f6 03 c4 19 46 d1 94 6b
CRLDistributionPoints	Full Name: URL=http://crl.quovadisglobal.com/qvrca2.crl
SubjectKeyIdentifier	50 52 4f 44 2e 47 54 4e 2e 45 58 53 53 4c 43 41 2e 53 49 47 47 45 4e 52 53 2e 30 30 30 30 32 37 30 30
Critical Extensions	
BasicConstraints	CA:TRUE PathLen Restriction=0
KeyUsage	Digital Signature, Certificate Sign, CRL Sign (86)

VR-Ident SSL-Certificates

The extensions of VR-Ident SSL-Certificates are shown in the table below:

Table 7.6. Extensions of VR-Ident SSL-Certificates

Extensions	
BasicConstraints	CA:FALSE PathLen Restriction: none
AuthorityInfoAccess	OCSP - URL=http://ocsp.vr-ident.de/gtnocsp/OCSPResponder/VR%20IDENT%20SSL%20CA%202016
SubjectAltName	DNS-Name = <Content of Subject DN> plus <optional additional FQDNs>
SubjectKeyIdentifier	individual hash value
ExtendedKeyUsage	serverAuth, clientAuth
AuthorityKeyIdentifier	KeyID=50 52 4f 44 2e 47 54 4e 2e 45 58 53 53 4c 43 41 2e 53 49 47 47 45 4e 52 53 2e 30 30 30 30 32 37 30 30
CertificatePolicies	Policy: 1.3.6.1.4.1.17696.4.1.1.9

	CPS Qualifier: http://www.vr-ident.de Policy: 1.3.6.1.4.1.8024.0.2.1600.0.1 CPS Qualifier: http://www.quovadisglobal.com/repository Policy: 2.23.140.1.2.2
CRLDistributionPoints	Full Name: URL=http://www.vr-ident.de/gtncrl/CRLResponder/VR%20IDENT%20SSL%20CA%202016
Critical Extensions	
KeyUsage	Digital Signature, Key Encipherment (a0)

7.1.3. Algorithm Object Identifiers

The algorithm object identifiers are conform to common standards. Compare tables above.

7.1.4. Name Forms

See Chapter 3.1.1.

7.1.5. Name Constraints

Name constraints are not used.

7.1.6. Certificate Policy Object Identifier

Where the Certificate Policies extension is used certificates contain the object identifier for the certificate policy corresponding to the appropriate type of the certificate according to Chapter 1.2 of this CPS.

7.1.7. PolicyConstraints

Policy constraints are not used.

7.1.8. Policy Qualifiers Syntax and Semantics

The Policy Qualifier in the extension Certificate Policies contains a text which can be displayed to the user and the URL of the applicable *CPS* (*Certification Practice Statement*).

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation. The certificate policy extensions of VR-Ident EV SSL certificates are not marked as critical.

7.2. CRL Profile

The VR-Ident PKI issues CRLs according to the standard X.509. CRLs contain information about the validity period, the signature algorithm used, the serial numbers of revoked certificates, the revocation reasons, and the issuer of the CRL.

7.2.1. Version number(s)

CRLs issued by the VR-Ident PKI conform to the standards *X.509* Version 2, *RFC* 5280, and Common *PKI* (cf. Appendix with general references).

7.2.2. CRL and CRL Entry Extensions

The *CRL*s contain the following fields and extensions:

Table 7.7. Extensions of CRLs (Certificate Revocation List)

CRL Content	
Version	V 2
Issuer	The issuer of the CRL is identical to the CA issuing the certificates. For every CA there is a valid certificate revocation list signed by the same private key which has been used for signing the certificates on the CRL. CN = <Name of CA> OU = VR IDENT O = FIDUCIA & GAD IT AG C = DE
Last Update	Date and time
NextUpdate	Date and time
Signature algorithm	sha1RSA
Extensions	
AuthorityKeyIdentifier	individual hash value of signing key
CRL Number	increasing serial number, incremented for each new CRL

The entries on the list consist of:

Table 7.8. Extensions of CRL Entries

Content of entry	
Serial Number	Serial number of revoked certificate
Revocation Date	Date and time of revocation
Reason Code	Reason for revocation. This value is identical to "revocationReason" in OCSP responses. The following revocation reasons may be used: • "Unspecified", no reason specified (not for SSL certificates) • "Cessation of Operation", certificate no longer needed (not for SSL certificates) • "Superseded", certificate has been replaced by new certificate (for SSL certificates)
Certificate Issuer	Name of the issuer of the certificate, identical to the issuer of the CRL.
No critical extensions	

7.2.3. Additional Properties of CRLs

CRLs are always signed by the issuer of the certificates on the CRL. Only direct CRLs are supported.

7.3. OCSP Profile

The OCSP profiles used in the VR-Ident PKI conform to the standard RFC 6960 and are intended to validate the revocation status of VR-Ident certificates according to X.509.

7.3.1. Version Number(s)

The *OCSP-Responder*s of the VR-Ident revocation status service support OCSP pursuant to *RFC* 6960 in version 1 and are conform to the Common *PKI* standard (see cf. Appendix with general references).

7.3.2. OCSP Extensions

The *OCSP-Responder*s support the following OCSP extensions for requests:

Table 7.9. Extensions in OCSP-Requests

Extension	
Nonce	Number which cryptographically binds the response to the request (optional)

The *OCSP-Responder*s support the following extensions in responses:

Table 7.10. Extensions in OCSP-Responses

Extension	
Cert Hash	Hash value of the certificate being requested.
Nonce	Same value as in the request. Not present in response if not present in request.

7.3.3. Additional Properties of OCSP Requests and Responses

OCSP Requests:

- Signed OCSP requests are supported but OCSP requests are not required to be signed. The signature is ignored.
- The field "requestorName" can be set at will (even empty).
- The field "CertID" must be a *SHA*-1 hash value.

OCSP Responses:

- The field "NextUpdate" contains the time of the next scheduled update, i.e. the time at or before which newer information will be available about the status of the certificates.
- The field "ResponderID" in "ResponseData" contains the *Distinguished Name* (*DN*) of the OCSP responder's certificate.
- The field "Certs" contains the certificate of the OCSP responder and the CA certificate that issued the OCSP responder certificate.
- The OCSP responder returns the status "unknown" only if the requested certificate has not been issued by the corresponding CA of the *Certification Service* VR-Ident.

Chapter 8. Compliance Audit and Other Assessments

8.1. Frequency and Circumstances of Assessment

The processes for issuing VR-Ident SSL-Certificates are assessed annually by an external auditor according to IDW PS 951.

Additional audits for compliance with the security requirements are conducted in a four-year-cycle.

There may be more than one audit in theses four years, e.g. if a previous audit did not prove satisfactory results of if security relevant incidents occurred.

Management personnel and administrators regularly check whether processes are followed and meet the requirements.

The *CA* is assessed and certified by an independent external auditor according to the requirements mentioned in Chapter 1.1 [1]:

- WebTrust Service Principles and Criteria for Certification Authorities
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
- Extended validation audit criteria
- Guidelines for the Issuance and Management of Extended Validation Certificate

Conformity with these requirements is demonstrated by Fiducia & GAD IT AG and assessed annually by external auditors.

8.2. Identity/Qualifications of Assessor

The *Certification Service* VR-Ident decides whether audits are conducted by external auditors or by an employee of *Fiducia & GAD IT AG* (internal audit).

Auditors must possess the following qualifications:

- Technical know-how of *PKI*.
- Familiarity with the applicable norms and standards (ISO 27001, ETSI EN 319 401, ETSI EN 319 411-1, IDW PS 951, and others).

8.3. Assessor's Relationship to Assessed Entity

Auditors are contractually bound to *Fiducia & GAD IT AG*, either as employees or as independent contractors.

Auditors are in no way involved in the management, administration, or operation of the *Certification Service* VR-Ident. Furthermore, auditors neither directly nor indirectly depend on the *Certification Service* VR-Ident or its employees.

8.4. Topics Covered by Assessment

Objective of the assessment is the inspection of the implementation of defined measures, processes, and procedures. The scope of the assessment is chosen by the assessor based on the applicable standards, requirements, and legal provisions. The assessment includes all systems, facilities, procedures, and information which are relevant for the implementation of the measures. In particular, the inspection covers the following topics:

- equipment for constructional and physical security (e.g. fire protection, access control, etc.),
- configuration of security relevant systems,
- log files of security relevant systems,

- log data of security relevant procedures (e.g. key ceremony, emergency procedures, modifications of systems),
- documentation of personal security measures (like records about trainings, duty roster, or similar),
- documentation of procedures and systems (e.g. emergency plans, system manuals),
- keys and authentication smart cards (e.g. for access control or access to HSMs),
- archive data.

8.5. Actions Taken as a Result of Deficiency

Depending on the severity and urgency the findings of an assessment are considered as incidents or problems and follow-up procedures are invoked. Severe deficiencies are reported to the management of *Fiducia & GAD IT AG*.

The *Certification Service* VR-Ident ensures that all findings are followed and remedied without unnecessary delay.

8.6. Communications of Results

Results are documented by the assessor in an audit report. Audit reports of WebTrust audits for compliance with the CA/Browser Forum Baseline Requirements and EV Guidelines are published on *Fiducia & GAD IT AG*'s website.

8.7. Self-Audits

The *Certification Service* VR-Ident monitors adherence to its Certificate Policy, Certification Practice Statement, the Baseline Requirements, and the EV Guidelines and strictly controls its service quality by performing self audits.

On a quarterly basis a randomly selected sample of 10 percent of the SSL certificates issued by the *Certification Service* VR-Ident during the previous quarter is checked for compliance with the requirements.

Chapter 9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

The *Fiducia & GAD IT AG* is entitled to charge end-user subscribers for the issuance, management, and renewal of VR-Ident SSL-Certificates. The fees for internal VR-Ident SSL-Certificates are internally visible in *Fiducia & GAD IT AG*'s schedule of prices. Fees for VR-Ident SSL-Certificates for *Fiducia & GAD IT AG*'s affiliates and partners can be requested from the contact person named in Chapter 1.5.2 [6].

9.1.2. Certificate Access Fees

Fiducia & GAD IT AG does not charge a fee for certificate access.

9.1.3. Revocation or Status Information Access Fees

Fiducia & GAD IT AG does not charge a fee for certificate revocation or status access.

9.1.4. Fees for Other Services

Fiducia & GAD IT AG does not charge fees for other services related to VR-Ident certificates.

Fiducia & GAD IT AG does not charge a fee for access to this CPS

9.1.5. Refund Policy

When a valid VR-Ident certificate is revoked the subscriber is not eligible for refund or compensation of expenses, provided that the revocation by the *Certification Service* VR-Ident was legitimate.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

The *Fiducia & GAD IT AG* operating the *Certification Service* VR-Ident maintains a Commercial General Liability insurance (Vermögensschaden - Haftpflicht Versicherung) with policy limits of 5 million Euro to cover legal obligations regarding indemnity if products or technical security mechanisms fail.

Organizations and companies using VR-Ident SSL-Certificates as subscribers are recommended to maintain similar insurances to be able to indemnify their customers for damages.

9.2.2. Other Assets

Not applicable.

9.2.3. Extended Warranty Coverage

No additional insurance or warranties.

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

All information not included in certificates is considered confidential, in particular, business secrets and industrial secrets of customers and subscribers.

9.3.2. Information Not Within the Scope of Confidential Information

All information contained in issued and published certificates is considered public information. All CRLs issued, all CPS, and all CP documents are considered public..

9.3.3. Responsibility to Protect Confidential Information

The *Certification Service* VR-Ident is responsible for the protection of all confidential information named in Chapter 9.3.1 against manipulation and unauthorized access.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

The *Certification Service* VR-Ident observes the legal requirements regarding the privacy of personal information, in particular, the German Federal Data Protection Act and other data protection regulations.

9.4.2. Information Treated as Private

All personal information not included in certificates or CRLs is considered confidential.

9.4.3. Information Not Deemed Private

All information included in certificates is deemed non-confidential.

9.4.4. Responsibility to Protect Private Information

The *Certification Service* VR-Ident protects person related subscriber information in compliance with the local privacy laws. Information is processed solely for the purpose of certificate issuance and certificate management.

9.4.5. Notice and Consent to Use Private Information

Where necessary the Subscriber declares its consent to the use of personal data by the *Certification Service* VR-Ident for the purpose of certification services. The Subscriber may withdraw its consent at any time.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

On request the *Certification Service* VR-Ident is obliged to disclose private information about the identity of a Subscriber to law courts or other governmental agencies, provided that the preconditions are fulfilled.

At least one of the following preconditions must be met:

- disclosure is necessary for the prosecution of judicial, administrative, or other legal offenses or crimes, or for the defense of public safety or public order;
- disclosure is necessary for the realization of the lawful duties of either the federal or a state Office for the Protection of the Constitution, the Federal Intelligence Service, the Military Counter-Intelligence Service, or the Revenue Department;
- if it has been court-ordered in accordance with the applicable regulations over the course of pending proceedings.

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5. Intellectual Property Rights

Existence and content of copyright or other intangible property rights is governed by the applicable legal regulations.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

VR-Ident warrants that issued VR-Ident certificates fulfill the requirements of this CPS.

9.6.2. RA Representations and Warranties

As Registration Authority for VR-Ident certificates *Fiducia & GAD IT AG* warrants that issued VR-Ident certificates fulfill the requirements of the CPS.

9.6.3. Subscriber Representations and Warranties

Subscribers warrant that they:

- pay the agreed upon fees in due time,
- use VR-Ident certificates according to the regulations of this CPS and prevent improper use,
- observe national and international export regulations and terms of use when using VR-Ident certificates internationally,
- keep the private key corresponding to the VR-Ident certificate secret and protect it from unauthorized access,
- report defects, damages, or other disruptions promptly to the *Certification Service* VR-Ident,
- initiate the revocation of the VR-Ident certificate if the corresponding private key is lost or suspected to be compromised,
- initiate the revocation of the VR-Ident certificate if data in the certificate is no longer correct,
- regularly check the website http://www.vr-ident.de for new information about recent changes regarding security relevant aspects or methods.

9.6.4. Relying Party Representations and Warranties

Relying parties are obliged to follow the provisions made in Chapter 4.5.2 [18] and Chapter 4.9.6.

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7. Disclaimers of Warranties

In spite of maximum carefulness in the creation of this document *Fiducia & GAD IT AG* cannot exclude unwanted errors in the procedures described. In this case *Fiducia & GAD IT AG* expressly disclaims any and all express or implied warranties of any type.

9.8. Limitations of Liability

9.8.1. Liability of the *Certification Service* VR-Ident

The following stipulations regarding liability apply:

- In cases of wilful intent or gross negligence or if a warranted property is absent the liability of the *Certification Service* VR-Ident shall be unlimited for all damages caused by these facts.
- In cases of slight negligence the *Certification Service* VR-Ident shall be liable in cases of death and injury to body or health. In the event that the *Certification Service* VR-Ident defaults on delivery or performance, or in the event that irrespective of the reasons delivery or performance becomes impossible, or in the event that the *Certification Service* VR-Ident breaches material obligations the *Certification Service* VR-Ident is liable for all damages to property and economic losses caused by such an event up to a maximum of 2.500 EUR.
- The *Certification Service* VR-Ident is liable for the correctness of identity validation only to the extent of its available opportunities for identity validation. By issuing a certificate the *Certification Service* VR-Ident only assures that at the time of identity validation someone presented the required identity proofing documents and that this information has been included in the certificate.
- In the event of a failure of the certificate database the *Certification Service* VR-Ident is liable for damages caused by such non-availability only if the database is unavailable for more than 24 hours.
- The *Certification Service* VR-Ident is not liable for damages caused by subscribers or relying parties not observing the applicable regulations.
- Liability according to the Product Liability Law is applicable, for all other damages liability is excluded.

9.8.2. Subscriber Liability

Subscribers are liable for damages to the *Certification Service* VR-Ident due to erroneous information in certificates caused by the Subscriber and for damages caused by negligence of responsibilities originating in laws, contracts, the applicable CP (Certificate Policy), or this CPS.

9.9. Indemnities

See Chapter 9.8.1.

9.10. Term and Termination

9.10.1. Term

This CPS becomes effective upon publication. Amendments to this CPS become effective upon publication. The validity of this CPS ends when it is amended or when the Certification Service is terminated.(Chapter 5.8 [31]).

9.10.2. Termination

This document remains in force until it is replaced by an amended version.

9.10.3. Effect of Termination and Survival

Upon termination of this CPS participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11. Individual Notices and Communications with Participants

For individual notices and communications with participants the applicable contact information (address, e-mail, phone, etc.) are used.

9.12. Amendments

9.12.1. Procedure for Amendment

The *Certification Service* VR-Ident reserves the right to change or amend this CPS.

Typically, amendments to the CPS are made to improve performance or to adapt systems and services to new technological developments if such adaptions are considered necessary. Amendments, approval, and publication of amended documents is in the sole responsibility of the *Certification Service* VR-Ident.

9.12.2. Notification Mechanism and Period

When the Certification Service VR-Ident applies changes to security relevant aspects or procedures affecting Subscribers or Relying Parties, e.g. changes to the enrolment process, directory service, revocation service, contact information, or liability, the *Certification Service* VR-Ident informs Subscribers and Relying Parties by e-mail or by publication at:

http://www.vr-ident.de.

When notifying Subscribers about changes the *Certification Service* VR-Ident, respectively the Registration Authority of the *Certification Service* VR-Ident, includes information about the consequences of such changes in the notification.

Changes become effective six weeks after the *Certification Service* VR-Ident

- notified the Subscribers about the changes and
- informed the Subscribers that they are entitled to object to the planned changes within a defined period of time, and that the changes become effective after time limit for the filing of objections has expired and no objections have been filed.

When small changes are made, especially the correction of typing errors or adding explanatory text, the notification of Subscribers is not mandatory.

9.12.3. Circumstances under Which OID Must be Changed

The decision about the assignment of a new OID is part of the CPS review and update process. When the CPS is amended or modified the *Certification Service* VR-Ident determines whether these amendments or modifications result in significant changes to the security of the *Certification Service*s, the rights and obligations of participants, or the usability of the certificates. In this case the version number of the CPS is incremented to the next full number and the OID is adapted. Otherwise the OID remains unchanged.

9.13. Dispute Resolution Provisions

Disputes between the Certification Service VR-Ident and its customers shall be resolved as agreed upon in the contractual agreements. Other parties may contact the Certification Service using the email address IND_Zertifikatsverwaltung@fiduciagad.de.

9.14. Governing Law

Applicable is only German Law. The General Terms and Conditions of *Fiducia & GAD IT AG* apply.

9.15. Compliance with Applicable Law

No stipulation.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

All provisions made in this CPS apply to the Certification Service Provider Fiducia & GAD IT AG and its customers. The publication of a new version of the CPS replaces all previous versions. There are no verbal or subsidiary agreements.

9.16.2. Assignment

Not applicable.

9.16.3. Severability

If any of the provisions of this CPS is determined to be invalid or unenforceable this will not invalidate or affect the enforceability of the remaining provisions of this CPS. Instead of the invalid provision another provision meeting to a large extent the spirit and purpose of the invalid provision becomes effective. In the case of omissions it is considered to be agreed upon what would have reasonably been agreed upon in accordance with the spirit and purpose of this CPS.

9.16.4. Enforcement (Attorney's Fees and Waiver of Rights)

Legal disputes resulting from the operation of the VR-Ident PKI underlie German law. Place of jurisdiction is Münster.

9.16.5. Force Majeure

No stipulation.

9.17. Other Provisions

No stipulation.

Chapter 10. Other Provisions

10.1. Requirement of Written Form

The most recent version of this document replaces all previous versions. There are no verbal agreements.

10.2. Language

For this CP as well as for all legally binding documents like the CPS or General Terms and Conditions (Allgemeine Geschäftsbedingungen) the German version is authoritative.

Appendix A. References

A.1. Bibliography with general international documents

[Nr.]	Document	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.	https://csrc.nist.gov/publications/detail/fips/140/2/final[3]
[04]	PKCS#10: Certification Request Syntax Standard. RSA Laboratories. Version 1.7. 2000.	http://tools.ietf.org/html/rfc2986
[05]	RFC 6960, X.509 Internet Public Key Infrastructure – Online certificate Status Protocol – OCSP. S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, 2013.	http://www.ietf.org/rfc/rfc6960.txt[4]
[06]	RFC 3647, Internet X.509 Public Key Infrastructure certificate Policy and Certification Practices Framework. S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu, 2003 (obsoletes RFC 2527)	http://www.ietf.org/rfc/rfc3647.txt
[07]	RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.	http://www.ietf.org/rfc/rfc5280.txt
[08]	ETSI EN 319401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers, European Telecommunications Standards Institute (ETSI), Version 2.2.0, 08/2017	http://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.02.00_20/
[09]	ETSI EN 319411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, European Telecommunications Standards Institute (ETSI), Version 1.2.0, 08/2017	http://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.02.00_20/
[10]	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
[11]	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
[12]	CA-Certificate Policy for Cybertrust Certification Services	http://cybertrust.omniroot.com/repository/
[13]	WebTrust Principles and Criteria for Certification Authorities Version 2.1	http://www.webtrust.org/principles-and-criteria/docs/item85228.pdf
[14]	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, V.1.5.1	https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.5.1.pdf
[15]	Guidelines For The Issuance And Management Of Extended Validation Certificates Version 1.6.5	https://cabforum.org/wp-content/uploads/EV-V1_6_5.pdf
[16]	WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL, Version 1.6	http://www.webtrust.org/principles-and-criteria/docs/item83989.pdf
[17]	Mozilla CA Certificate Inclusion Policy (Version 2.1)	http://www.mozilla.org/projects/security/certs/policy/InclusionPolicy.html
[18]	"QuoVadis Root Certification Authority Certificate Policy/Certification Practice Statement", Version 4.21	https://www.quovadisglobal.com/~/media/Files/Repository/QV_RCA1_RCA3_CP-CPS_V4_21.ashx

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

A.2. Bibliography with VR-Ident Documents

[Nr.]	Document	Link
[01]	Certificate Policy (CP) for VR-Ident private-Certificates	http://www.vr-ident.de
[02]	Certification Practice Statement (CPS) for VR-Ident private-Certificates	http://www.vr-ident.de
[03]	Certification Practice Statement (CPS) for VR-Ident SSL-Certificates under external Root	http://www.vr-ident.de
[04]	Certificate Policy (CP) for VR-Ident Certificates (WebTrust)	http://www.vr-ident.de
[05]	Certification Practice Statement (CPS) for VR-Ident SSL-Certificates (WebTrust)	http://www.vr-ident.de
[06]	Certification Practice Statement (CPS) for VR-Ident mail-Certificates (WebTrust)	http://www.vr-ident.de
[07]	Certification Practice Statement (CPS) for VR-Ident private-Certificates (WebTrust)	http://www.vr-ident.de
[08]	Certification Practice Statement (CPS) for general VR-Ident Certificates (WebTrust)	http://www.vr-ident.de
[09]	Agreements for den *Certification Service* VR-Ident	http://www.vr-ident.de
[10]	Terms of Use for VR-Ident mail-Certificates for Banks in the *Certification Service* VR-Ident of *Fiducia & GAD IT AG*	http://www.vr-ident.de
[11]	Terms of Use VR-Ident SMIME-Certificates in the *Certification Service* VR-Ident of *Fiducia & GAD IT AG*	http://www.vr-ident.de
[12]	Agreements for the *Certification Service* VR-Ident for VR-Ident EV SSL-Certificates (WebTrust)	http://www.vr-ident.de

Glossary

Activation data	Confidential data which can be used by the legitimate user of a private key to authenticate at the system storing the private key (e.g. a smart card or a HSM) thus activating the private key..Typically, PINs or passphrases are used as activation data.
asymmetric cryptography	Cryptographic method based on two different keys where one of the keys is public and the other one is private (secret). In this way it is possible to encrypt a message using the public key; the message can be decrypted only by the owner of the private key.
CA	Certification Authority.
CC	Common Criteria.
Certificate Policy	Set of rules an provisions defining the applicability of specific types of certificates.
Certification Authority	Logical unit in a Public Key Infrastructure for issuing (signing) of certificates. A Certification Authority possesses one or more key pairs for signing certificates.
Certification Practice Statement	A document from a Certification Authority which describes their practice for issuing and managing public key certificates. It includes practices of: issuance, publication, archiving, revocation, and renewal. It allows judging the relative reliability of a given Certification Authority.
Certification Service	Service issuing certificates and providing other services related to certificates, e.g. directory services, time-stamping services, or key escrow services.
Common Criteria	An international standard (ISO/IEC 15408) for computer security certification of products and systems.
CP	Certificate Policy.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
Directory Service	In a PKI a service providing information about certificates (e.g. revocation information) or other information about the PKI. Access to the directory service in the VR-Ident PKI is via LDAP protocol.
Distinguished Name	Name form according to X.501. A DN allows the identification of an entity within a PKI. The most common attributes in a DN are CommonName (cn), Organization (o), Organizational Unit (ou), and Country (c).
DMZ	Demilitarized Zone – logical network zone between the public Internet and internal network zones.
DN	Distinguished Name.
Fiducia & GAD IT AG	The *Fiducia & GAD IT AG* is located in Münster and in Karlsruhe. It is an IT Service Provider, data center, and software house for more than 1.100 Volks- and Raiffeisen Banks and several Private Banks and Special Banks. Integrated into the cooperative Finace Group *Fiducia & GAD IT AG* possesses special strenth concerning offering qualified Bank services at the customer's location. The core competencies are the

	development and operation of modern and sustainable Core-Banking-Solutions and in the provision of high-quality and secure outsourcing services.
fingerprint	The fingerprint of a certificate is the hash value of the certificate.
FIPS 140-2	US-american standard for the assessment and evaluation of the sucurity of cryptographic software and hardware. FIPS 140-2 is the successor of FIPS 140-1. Both standards distinguish between 4 different levels of security, where Level 1 imposes the weakest and Level 4 the highest requirements on security. Both standards are comparable to the greatest possible extent.
Hardware Security Module	Device for the secure storage and application of cryptographic keys. In contrast to smart cards in most cases HSMs have their own üpower supply and implement extensive security mechanisms like secure key backup and logging of security relevant activities or role based access control.
hash value	A hash function computes from arbitrary data a (practically) unique string of constant length which can be used as check sum. This string is called hash value or fingerprint.
HSM	Hardware Security Module.
HTTP	Hypertext Transfer Protocol – communication protocol in the Internet.
LDAP	Lightweight Directory Access Protocol – Protocol for access to directory services; stadardized by IETF.
Object Identifier	Unique numerical identifier for objects; hierarchical structure.
OCSP	Online Certificate Status Protocol – Online Certificate-checking protocol for providing Relying Parties with real-time Certificate status information. Standardized by IETF.
OCSP-Responder	Online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See Also OCSP.
PKCS	Public Key Cryptography Standard – Standard for cryptographic processes, data formats, and interfaces in a PKI.
PKI	Public Key Infrastructure – technical environment for the use asymmetric cryptography. A PKI is based on certificates and a certification hierarchy. Relevant components are the CAs, Registration Authorities, and certificate status services. A PKI also includes the participants, client components for storing and using cryptographic keys and certificates, and technical and organizational processes.
RA	Registration Authority.
Registration Authority	Entity in a certification service responsible for validation of certificate applications, identification of applicants, managing certificates, and handling of revocations.
Relying Party	Entity (person or organization) who relies on the correctness of a certificate issued by VR-Ident. A Relying Party can be a certificate owner at the same time.
RFC	Request for Comment – Document type of the Internet Engineering Task Force (IETF). Proposes and publishes standards.

Root-CA	Top level of a certification hierarchy. The certificate of the Root-CA is signed by the Root-CA itself and must be made available for participants in a trustworthy manner. Subordinate CA certificates are signed by the Root-CA.
SHA	SHA (Secure Hash Algorithm) is a family of cryptographic hash function which takes an input and produces hash value known as a message digest. It was designed by the United States National Security Agency, and is a U.S. Federal Information Processing Standard. SHA-1 produces 160-bit (20-byte) hash values and is no longer considered secure. Algortims from the SHA-2 family (SHA-256, SHA-384, and SHA-512) are recommended - where the number in the suffix describes the length of the output value.
SSL	Secure Socket Layer, a protocol that allows mutual authentication of a client and a server for establishing encrypted communication between client and server.
VR-Banks	The term VR-Banks subsumes German Volks- and Raiffeisenbanks and private and special bank institutes serviced by *Fiducia & GAD IT AG*. In this document VR-Banks means those banks using the certificate download service of VR-Ident.
VR-Ident Workflow Management	Lotus Notes based Key Management Workflow Tool. The authentication is role oriented and is based on the Lotus Notes ID. Role assignment is defined internally.
X.501	Standard defined by ITU, defines the structure of directories and name forms for identifying objects in directories.
X.509	Standard defined by ITU, defines (among others) the commonly used data formats for Certificates and Certificate Revocation Lists.