Certificate Policy (CP)

VR-Ident Certificates (WebTrust)

FIDUCIA GAD
ZUKUNFTSERFAHREN

IT-Partner der FinanzGruppe
Volksbanken Raiffeisenbanken

Certificate Policy (CP)

VR-Ident Certificates (WebTrust)

Version:	Version 3.02.04, Approved
Zielgruppe:	Users and owners of VR-Ident Certificates
Datum/Uhrzeit:	16.01.2019 / 09:51 Uhr

Revision History

Nummer	Datum	Inhalt / Änderungen
3.2.2	07.02.2018	Chapter 0.0.0:
3.2.4	14.12.2018	Included note about termination of EV and OV

Zusammenfassung

This document is the "Certificate Policy" (CP) for the Certification Service VR-Ident for VR-Ident 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 Certificates

Table of Contents

Chapter 1. Introduction

1.1. Overview

Important Notice: Cessation of Operation
The VR IDENT EV SSL CA and the VR IDENT OV SSL CA are terminated 01.01.2019.
After this date the issuance of VR Ident EV SSL and OV SSL certificates is discontinued.
All valid certificates will be replaced by equivalent certificates issued by Quo Vadis.
The revocation status services and the revocation management services will remain operational until 31.03.2019.
After this date these services will be terminated, too. All valid VR Ident EV SSL and OV SSL certificates will be revoked at 31.03.2019.
All archived data will be available at *Fiducia & GAD IT AG* for at least 7 years after 31.03.2019 as specified in chapter 5.5.

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.

Extended Validation (*EV*) *SSL-Server-Certificate*s are issued by the *Certification Service* VR-Ident under the product name "VR-Ident EV SSL-Certificate".

The "VR IDENT EV SSL CA" is operated as a subordinate CA chained to the Root CA of the external validation partner QuoVadis.

This document is a "*Certificate Policy*" (*CP*) for the *Certification Service* VR-Ident for VR-Ident certificates issued under a *Root-CA* which has been assessed and certified by an external auditor.

This *CP* (*Certificate Policy*) is structured according to *RFC* 3647. The "*Certification Practice Statement*"s (*CPS*) of the Sub-CAs include detailed information regarding the implementation of the provisions of this CP (cf. Appendix with VR-Ident references).

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

VR-Ident Certificates issued under the external *Root-CA* "QuoVadis Root CA 2" also underlie the provisions made in the "QouVadis Root Certification Authority Certificate Policy/ Certification Practice Statement" (Appendix with general references).

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: 3.02.04

Date of release of this document: 31.12.2018

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 : 1.3.6.1.4.1.17696.4.1.2.9.3.2.

The document name for this CP is : "VR-Ident Certificate Policy (CP) for VR-Ident Certificates (WebTrust)".

The following *CPS*' (*Certification Practice Statement*)s are based on this CP:

- "VR-Ident Certification Practice Statement (CPS) for VR-Ident SSL-Certificates (WebTrust)" with the ASN.1 *Object Identifier* (OID): 1.3.6.1.4.1.17696.4.1.2.5.3.2.
- "VR-Ident Certification Practice Statement (CPS) for VR-Ident EV SSL-Certificates" with the ASN.1 *Object Identifier* (OID): 1.3.6.1.4.1.17696.4.1.2.10.3.2.
- "VR-Ident Certification Practice Statement (CPS) for VR-Ident mail-Certificates (WebTrust)" with the ASN.1 *Object Identifier* (OID): 1.3.6.1.4.1.17696.4.1.1.6.3
- "VR-Ident Certification Practice Statement (CPS) for VR-Ident private-Certificates (WebTrust)" with the ASN.1 *Object Identifier* (OID): 1.3.6.1.4.1.17696.4.1.1.7.3
- "VR-Ident Certification Practice Statement (CPS) for general VR-Ident Certificates (WebTrust)" with the ASN.1 *Object Identifier* (OID): 1.3.6.1.4.1.17696.4.1.1.8.3

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:

- 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").

Details about the certification hierarchy of the Certification Authority VR-Ident and the certificates issued by its CAs are documented in the applicable CPS (Certification Practice Statement) for VR-Ident Certificates (*WebTrust*) (Appendix with VR-Ident references).

1.3.2. Registration Authorities

A Registration Authority (RA) is the organizational unit in a PKI infrastructure responsible for the identification and authentication of applicants, certificate management, and receives certificate revocation requests. The RA is the point of contact for persons and organizations for obtaining electronic certificates from the CA. The Registration Authority for VR-Ident SSL-Certificates and for general VR-Ident Certificates is represented by VR-Ident. VR-Ident registers and identifies certificate applicants, receives certificate applications, and initiates (under specific circumstances) certificate revocations.

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

The Registration Authority for VR-Ident mail-Certificates is represented by contract partners of VR-Ident and by VR-Ident itself. Contract partners identify certificate applicants and initiate enrolment. VR-Ident receives certificate applications. Contract partners and VR-Ident initiate certificate revocations under specific circumstances.

The Registration Authority for VR-Ident private-Certificates is represented by VR-Bank affiliate offices and systems. They register and identify certificate applicants, receive certificate applications, and initiate certificate revocations under specific circumstances.

Detailed provisions are made in the applicable CPS (Certification Practice Statement) for VR-Ident Certificates (WebTrust) (cf. Appendix with VR-Ident references).

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.

The following roles can be involved in the application process for VR-Ident EV SSL-Certificates:

- Applicant
  The entity for which a certificate is requested. The applicant orders the certificate request and authorizes representatives to perform detailed duties.
- Representative of the Applicant:
  The Representative of the Applicant is a combined role including the following roles:
  - Certificate Requester
    The Certificate Requester may be an employee of the Applicant or a third party authorized by the Applicant to request certificates on behalf of the Applicant's organization.
  - Certificate Approver
    The Certificate Approver may be the Applicant, an employee of the Applicant, or an authorized person authorized to act on behalf or in the name of the Applicant. Certificate Approvers are authorized to authorize other persons as Certificate Requesters. Certificate Approvers must be authorized to approve certificate requests and to accept the requirements of the CPS for the *Certification Service* VR-Ident for VR-Ident EV SSL-Certificates.
  - Contract Signer
    The Contract Signer may be the Applicant, an employee of the Applicant, or an authorized third party authorized by the Applicant to sign the certificate request and to accept the CPS for VR-Ident EV SSL-Certificates.

    If the Applicant is *Fiducia & GAD IT AG* the authority of the Contract Signer is verified against the company's employee data base, otherwise the Contract Signer must be named in the organization's record in the official register of companies.
- Applicant Representative:
  An Applicant Representative is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to acknowledge and agree to the Terms of Use.

In this document all roles are subsumed under the term "Applicant". If a distinction must be made this is explicitly stated.

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 using VR-Ident certificates for secure communication with the owner of the certificate or to validate an electronic signature of the owner of the certificate.

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 [13]).
- 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 [5]. 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 [5]. The contents of CP (*Certificate Policy*) and *CPS* (*Certification Practice Statement*) are coordinated during this process.

1.6. Definitions and Acronyms

Definitions and acronyms can be found in the glossary.

[2] mailto:IND_Zertifikatsverwaltung@fiduciagad.de

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 VR-Ident directory service available at ldap://www.vr-ident.de
  and
- *OCSP-Responder*s for online revocation status requests available at http://ocsp.vr-ident.de/gtnocsp/OCSPResponder/<Name of CA>.

The *Certification Service* VR-Ident also issues *CRL*s with revocation information of certificates; CRLs are available from http://www.vr-ident.de/gtncrl/CRLResponder/<Name of CA> and ldap://www.vr-ident.de.

Detailed provisions are made in the applicable CPS (Certification Practice Statement) for VR-Ident Certificates (WebTrust) (cf. Appendix with VR-Ident references).

2.2. Publication of Certificate Information

The *Certification Service* VR-Ident publishes all VR-Ident Certificates (individual certificates only if the certificate owner declares its consent). The *Certification Service* VR-Ident publishes certificate revocation status information for all VR-Ident Certificates via online status services (OCSP) and *CRL*s (Certificate Revocation Lists). Certificates and revocation status information is published in the internet over standard communication protocols and ports. Detailed provisions are made in the applicable CPS (Certification Practice Statement) for VR-Ident Certificates (cf. Appendix with VR-Ident References).

The *Certification Service* VR-Ident publishes the applicable Root-CA-Certificate(s) and their *fingerprint*s (*hash value*s).

This CP is published ion the internet.

The *Certification Service* VR-Ident also publishes its General Terms and Conditions ("Allgemeine Geschäftsbedingungen") for participants and Relying Parties at http://www.fiduciagad.de.

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

The names of the certificate owners in the VR-Ident Certificates issued by the *Certification Service* VR-Ident are so-called DistinguishedNames according to *X.501*. They are included in the attribute "subject" of the certificate.

The wildcard character "*" may be used in a CommonName field only in the leftmost position of a subdomain and after approval by the responsible instance in the *Certification Service* VR-Ident. Wildcard characters are not permitted in EV SSL Certificates.

Detailed provisions are made in the applicable CPS (Certification Practice Statement) for VR-Ident Certificates (cf. Appendix with VR-Ident References).

3.1.2. Need for Names to be Meaningful

Names in VR-Ident SSL-Certificates must uniquely identify the URL or the domain name. Names shall be chosen identical to the name at the applicable Top-Level Domain Registrar. IP adresses are not supported as FQDNs.

The company or organization owning the certificate shall be uniquely identifiable based on the registered name and locality in the applicable official register. In addition the state or province of the locality shall be added to the certificate data. The organizational unit of the responsible person may be added, otherwise the term "VR-Ident" shall be used.

Detailed provisions are made in the applicable CPS (Certification Practice Statement) for VR-Ident SSL-Certificates or VR-Ident EV SSL-Certificates (cf. Appendix with VR-Ident References).

In EV-certificates the company's or organization's place of jurisdiction shall be included in the certificates by adding unique information about locality, state or province, and state of the applicable court.

The unique registration number with which the company or organization has been registered at the applicable official register shall be included in the certificate.

Detailed provisions are made in the applicable CPS (Certification Practice Statement) for VR-Ident EV SSL-Certificates (cf. Appendix with VR-Ident References).

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), /, :, ?.

Details can be found in the relevant CPS (Certification Practice Statement).

3.1.5. Uniqueness of Names

The *Certification Service* VR-Ident ensures by suitable measures the uniqueness of names.

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 shall prove possession of the private key through suitable cryptographic mechanisms. This can be achieved by suitable *asymmetric cryptography*.

Detailed provisions are made in the applicable CPS (Certification Practice Statement) for VR-Ident Certificates (cf. Appendix with VR-Ident References).

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).

- The Applicant and the Subscriber shall be validated by *Fiducia & GAD IT AG* using available documents or based on an excerpt from the applicable official register
- Departments or subdivisions are validated by *Fiducia & GAD IT AG* based on available documents
- Names of companies and organizations, their locality, and the state where they are located shall be validated by a lookup in the applicable official register
- A validation whether the applicant is actively engaged in doing business is not required because *Fiducia & GAD IT AG* has active business relations with the Applicant

Detailed provisions are made in the applicable CPS (Certification Practice Statement) for VR-Ident SSL-Certificates (Appendix with VR-Ident References).

For EV-Certificates

- The place of jurisdiction shall be validated through a current excerpt from the applicable official register.
- The registration number shall be validated through a current excerpt from the applicable official register.
- The Certificate Approver, the Contract Signer, and the Requester shall be validated as necessary.
- When an VR-Ident EV SSL-Certificate is requested the Certificate Approver must confirm the legitimacy of the certificate request.

Detailed provisions are made in the applicable CPS (Certification Practice Statement) for VR-Ident EV SSL-Certificates (Appendix with VR-Ident References).

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).

The certificate of the issuing CA "VR IDENT EV 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 [9]).

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 [9]) - 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

Only organizations can apply for VR-Ident SSL-Certificates at the Registration Authority VR-Ident. During the registration process the Applicant must provide information about the domain for which the VR-Ident SSL-Certificate is to be issued.

Initial applications as well as request for certificate renewal are supported for VR-Ident SSL-Certificates.

Only written applications are accepted for VR-Ident EV SSL-Certificates.

Detailed provisions are made in the applicable CPS (Certification Practice Statement) for VR-Ident SSL-Certificates respectively for VR-Ident EV SSL-Certificates (cf. Appendix with VR-Ident References).

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

Applicants for VR-Ident SSL-Certificates are securely identified and authenticated according to a documented procedure (see also Chapter 3.2.2 [9]).

Detailed provisions are made in the applicable CPS (Certification Practice Statement) for VR-Ident SSL-Certificates or VR-Ident EV SSL-Certificates (cf. Appendix with VR-Ident References).

4.2.2. Approval or Rejection of Certificate Applications

Certificate applications are accepted only if the Applicant can be successfully identified and authenticated.

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.

For the following products CAA Records are checked according to the CA/Broser Forum Baseline Requirements:

- VR-Ident SSL-Certificate
- VR-Ident EV SSL-Certificate

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

Details are specified in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

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 [6].

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 [4]. 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 [4].

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.

Certificate re-key shall be handled identical to initial certificate application.

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 [22]),

- 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.

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 revocation of VR-Ident Certificates can be applied for by persons or entities authorized to such an action. Authorized are

- *Certification Service* VR-Ident.
- The certificate owner or an authorized third party.

4.9.3. Procedure for Revocation Request

The procedure for the revocation of VR-Ident Certificates is defined in the applicable CPS (Certification Practice Statement) (Appendix with VR-Ident References).

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

Processing a revocation request for a VR-Ident Certificate shall start immediately after the revocation request has been received.

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 [6].

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.

4.9.7. CRL Issuance Frequency

The time and frequency for the issuance and publication of CRLs is described in Chapter 2.3 [6].

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 *Certification Service* VR-Ident shall provide an *OCSP-Responder* for requesting the revocation status of VR-Ident Certificates via the "Online Certificate Status Protocol" (*OCSP*). From this certificate status service current revocation status information can be requested.

In addition *CRL* s (Certificate Revocation Lists) according to *X.509* are issued and published.

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

4.10.1. Operational Characteristics

Information about the operational characteristics of the revocation status service are included in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

4.10.2. Revocation Status Service Availability

The revocation status information shall be available 24x7.

Details about the operational features of the certificate revocation status service are given in the applicable CPS.

4.10.3. Optional Features

Details about the operational features of the certificate revocation status service are given in the applicable CPS.

4.11. End of Subscription

Details are laid down in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

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

The implemented physical security controls ensure a very high protection of the critical facilities of the *Certification Service* VR-Ident. In particular, these measures ensure that

- access to the facilities of the *Certification Service* and physical access to sensible information is restricted to authorized employees,
- critical information and systems can not be destroyed or damaged by disasters, environmental conditions, or impairment of the infrastructure (e.g. fire, water, overvoltage, power outage, or other incidents.

5.1.1. Site Location and Construction

Detailed provisions are included in the applicable CPS (Certification Practice Statement) (cf. Appendix withVR-Ident References).

5.1.2. Physical Access

Detailed provisions are included in the applicable CPS (Certification Practice Statement) (cf. Appendix withVR-Ident References).

5.1.3. Power and Air Conditioning

Detailed provisions are included in the applicable CPS (Certification Practice Statement) (cf. Appendix withVR-Ident References).

5.1.4. Water Exposures

Detailed provisions are included in the applicable CPS (Certification Practice Statement) (cf. Appendix withVR-Ident References)

5.1.5. Fire Prevention and Protection

Detailed provisions are included in the applicable CPS (Certification Practice Statement) (cf. Appendix withVR-Ident References).

5.1.6. Media Storage

Detailed provisions are included in the applicable CPS (Certification Practice Statement) (cf. Appendix withVR-Ident References).

5.1.7. Waste Disposal

Detailed provisions are included in the applicable CPS (Certification Practice Statement) (cf. Appendix withVR-Ident References).

5.1.8. Backup

Detailed provisions are included in the applicable CPS (Certification Practice Statement) (cf. Appendix withVR-Ident References).

5.2. Procedural Controls

The security measures implemented are based on the security analysis and ensure a very high security standard of the *Certification Service* VR-Ident

- the responsibilities for the roles for the operation of the Certification Service VR-Ident and the security management are regulated,
- a comprehensive security management shall be established,
- critical processes and procedures of the Certification Service VR-Ident and the security management must be documented and implemented,
- objects and information deserving protection shall be identified and classified.

5.2.1. Trusted Roles

Detailed provisions are made in the applicable CPS (Certification Practice Statement) for VR-Ident Certificates (WebTrust) (cf. Appendix with VR-Ident references).

5.2.2. Number of Persons Required per Task

Detailed provisions are made in the applicable CPS (Certification Practice Statement) for VR-Ident Certificates (WebTrust) (cf. Appendix with VR-Ident references).

5.2.3. Identification and Authentication for Each Role

Detailed provisions are made in the applicable CPS (Certification Practice Statement) for VR-Ident Certificates (WebTrust) (cf. Appendix with VR-Ident references).

5.2.4. Roles Requiring Separation of Duties

Detailed provisions are made in the applicable CPS (Certification Practice Statement) for VR-Ident Certificates (WebTrust) (cf. Appendix with VR-Ident references).

5.3. Personnel Controls

The implemented personnel controls ensure a very high level of security for the *Certification Service*. In particular, personnel of the *Certification Service*

- is assigned clearly defined roles in the *Certification Service*,
- is appropriately qualified for its tasks,
- has access to all required documentation required for performing the tasks,
- has undergone background checks for reliability.

5.3.1. Qualifications, Experience, and Clearance Requirements

Detailed provisions are made in the applicable CPS (Certification Practice Statement) for VR-Ident Certificates (WebTrust) (cf. Appendix with VR-Ident references).

5.3.2. Background Check Procedures

Detailed provisions are made in the applicable CPS (Certification Practice Statement) for VR-Ident Certificates (WebTrust) (cf. Appendix with VR-Ident references).

5.3.3. Training Requirements

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.3.4. Retraining Frequency and Requirements

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.3.5. Job Rotation Frequency and Sequence

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.3.6. Sanctions for Unauthorized Actions

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.3.7. Independent Contractor Requirements

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.3.8. Documentation Supplied to Personnel

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.4. Audit Logging Procedures

The event logging related to the issuance and management of certificates is based on a risk analysis and ensures a very high security standard of the *Certification Service*s.

5.4.1. Types of Events Recorded

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.4.2. Frequency of Processing Log

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.4.3. Retention Period for Audit Log

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.4.4. Protection of Audit Log

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.4.5. Audit Log Backup Procedures

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.4.6. Audit Collection System (Internal vs. External)

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.4.7. Notification to Event-Causing Subject

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.4.8. Vulnerability Assessments

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.5. Records Archival

The archival of relevant data must be in compliance with the applicable legal provisions. Archived data shall be protected from disclosure and unauthorized manipulation or destruction.

5.5.1. Types of Records Archived

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.5.2. Retention Period for Archive

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.5.3. Protection of Archive

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.5.4. Archive Backup Procedures

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.5.5. Requirements for Time-Stamping of Records

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.5.6. Archive Collection System (Internal or External)

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.5.7. Procedures to Obtain and Verify Archive Information

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.6. Key Changeover

Key pairs used by the *Certification Service* VR-Ident for the provision of *Certification Service*s shall be replaced prior to expiry. This routine key changeover does not require the revocation of the old CA-Certificate.

A non-routine key changeover of a CA-key shall be performed when the security of the private key or of the corresponding certificate cannot be guaranteed any longer. In such an event the corresponding CA-Certificate must be revoked. The revocation of a CA-Certificate invalidates all certificates issued by that CA-Certificate.

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. The same holds for Root-CA non-routine key changeover.

5.7. Business Continuity Management and Incident Handling

The *Certification Service* VR-Ident shall implement for its services suitable measures to maintain operations (Business Continuity Management) in cases of emergency or security relevant incidents.

5.7.1. Incident Handling and Emergency Procedures

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

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

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.7.3. CA Private Key Compromise Procedures

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.7.4. Business Continuity Capabilities after a Disaster

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

5.8. Termination of Certification Service

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

Detailed provisions are made in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

Chapter 6. Technical Security Controls

6.1. Key Pair Generation and Installation

Key pairs intended to be used by the *Certification Service* VR-Ident for the provision of *Certification Service*s shall be generated using defined procedures by authorized employees under multi-person control in a secure environment in Hardware Security Modules (*HSM*s).

6.1.1. Key Pair Generation

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.1.2. Private Key Delivery to Subscriber

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.1.3. Public Key Delivery to Certificate Issuer

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.1.4. CA Public Key Delivery to Relying Parties

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.1.5. Key Sizes

Details are provided in the applicable CPS (Certification Practice Statement) (Appendix with VR-Ident References).

6.1.6. Public Key Parameters Generation and Quality Checking

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.1.7. Key Usage Purposes

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.2. Private Key Protection and Cryptographic Module Engineering Controls

CA private keys of the Certification Service VR-Ident must be generated and stored in a secure environment in Hardware Security Modules (*HSM*s). Access to these CA-keys is permitted only in the course of defined procedures under multi-person control inside the secure environment. If high availability is required key backups may be created. Access to private keys, including backup and recovery, must be protected through technical means. Access to private keys shall require secure procedures and the participation of at least two authorized employees in trusted roles. Access must be in compliance with the provisions of the HSM's certification. Unused CA-keys shall be securely deactivated.

6.2.1. Cryptographic Module Standards and Controls

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

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

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.2.3. Private Key Escrow

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.2.4. Private Key Backup

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.2.5. Private Key Archival

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.2.6. Private Key Transfer into or from a Cryptographic Module

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.2.7. Private Key Storage on Cryptographic Module

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.2.8. Method of Activating Private Key

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.2.9. Method of Deactivating Private Key

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.2.10. Method of Destroying Private Key

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.2.11. Cryptographic Module Rating

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.3. Other Aspects of Key Pair Management

Public keys and the certificates are archived for an appropriate period of time. Details can be found in the applicable *CPS* (*Certification Practice Statement*).

6.3.1. Public Key Archival

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.4. Activation Data

CA private keys shall be protected by activation data which are known by authorized employees only.

6.4.1. Activation Data Generation and Installation

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.4.2. Activation Data Protection

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.4.3. Other Aspects of Activation Data

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.5. Computer Security Controls

The *Certification Service* VR-Ident implements extensive security measures for all systems in the *Certification Service*. These measures ensure:

- Protection against viruses and other malicious software
- Protection against unauthorized logical access to systems
- Regular backup of critical data
- Adequate safeguards against system failure
- Adequate tests before changes to systems or configurations are applied
- Realtime detection of disruptions or failures.

6.5.1. Specific Computer Security Technical Requirements

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.5.2. Computer Security Rating

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.6. Life Cycle Technical Controls

The *Certification Service* VR-Ident shall ensure that software used for the *Certification Service*s is developed, tested, delivered, installed, configured, operated, and maintained in such a manner that the authenticity, integrity, and appropriate function are preserved.

6.6.1. System Development Controls

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.6.2. Security Management Controls

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.6.3. Life Cycle Security Controls

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

6.7. Network Security Controls

The *Certification Service* VR-Ident shall implement extensive network security measures for the *Certification Service*s. These shall include:

- Implementation of separated network segments,
- Restriction of network communication to the necessary amount,
- Restriction of network access to necessary resources,
- Monitoring of network traffic,
- Regular examination of network security.

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

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.

7.1.1. Version Number(s)

The *Certification Service* VR-Ident issues VR-Ident Certificates compliant with *X.509* Version 3.

Details are provided in the applicable CPS (Certification Practice Statement) (Appendix with VR-Ident References).

7.1.2. Certificate Extensions

The certificate extensions shall be conform with the standards *X.509*, *RFC* 5280, and Common PKI. VR-Ident Certificates may include the following extensions:

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

Details are provided in the applicable CPS (Certification Practice Statement) (Appendix with VR-Ident References).

7.1.3. Algorithm Object Identifiers

Algorithm identifiers are compliant with common standards.

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

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 extensions of *CRL*s issued by the Certification Service VR-Ident are conform with the standards *X.509*, *RFC* 5280, and Common *PKI* (cf. Appendix with general references).

*CRL*s and CRL entries have the following extensions:

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

7.2.3. Additional Properties of CRLs

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

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

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

7.3.3. Additional Properties of OCSP Requests and Responses

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

Chapter 8. Compliance Audit and Other Assessments

The *Certification Service* VR-Ident performs extensive audits to assess the security of its services in regular intervals.

The auditor is appropriately qualified and independent from the *Certification Service* Provider *Fiducia & GAD IT AG*.

Severe deficits are reported to *Fiducia & GAD IT AG* management.

8.1. Frequency and Circumstances of Assessment

Details are provided in the applicable CPS (Certification Practice Statement) (Appendix with VR-Ident References).

8.2. Identity/Qualifications of Assessor

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

8.3. Assessor's Relationship to Assessed Entity

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

8.4. Topics Covered by Assessment

Detailed provisions are made in the applicable CPS (Certification Practice Statement) for VR-Ident Certificates (WebTrust) (cf. Appendix with VR-Ident references).

8.5. Actions Taken as a Result of Deficiency

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

8.6. Communications of Results

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

8.7. Self-Audits

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

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 [5].

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.

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.

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

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 CP.

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

Certificate owners shall be obliged to use certificates only as intended and to not mis-use the certificates.

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

9.6.4. Relying Party Representations and Warranties

Relying parties are obliged to follow the provisions made in Chapter 4.5.2 [13] 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

Details are provided in the applicable CPS (Certification Practice Statement) (cf. Appendix with VR-Ident References).

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 CP becomes effective upon publication. Amendments to this CP become effective upon publication. The validity of this CP ends when it is amended or when the Certification Service is terminated.(Chapter 5.8 [22]).

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 CP 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 CP.

Detailed provisions are made in the applicable CPS (Certification Practice Statement) for VR-Ident Certificates (WebTrust) (cf. Appendix with VR-Ident references).

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 shall inform Subscribers and Relying Parties.

Detailed provisions are made in the applicable CPS (Certification Practice Statement) for VR-Ident Certificates (cf. Appendix with VR-Ident references).

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

The Certification Service Provider *Fiducia & GAD IT AG* shall act in compliance with applicable law.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

All provisions made in this CP apply to the Certification Service Provider Fiducia & GAD IT AG and its customers. The publication of a new version of the CP 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 CP is determined to be invalid or unenforceable this will not invalidate or affect the enforceability of the remaining provisions of this CP. 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 CP.

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

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.
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.
CP	Certificate Policy.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
EV	See Extended Validation.
Extended Validation	Extended Validation SSL-Cerificates are X.509 SSL-Certificates that contain information specified in the EV Guidelines and that have been validated in accordance with the EV Guidelines.
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.
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.
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.
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.
SSL	Secure Socket Layer, a protocol that allows mutual authentication of a client and a server for establishing encrypted communication between client and server.
SSL-Server-Certificate	Certificate of a server used for protecting data transmitted via httpt. The certificate enables encryption of transmitted data thus protecting that data.
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.
WebTrust	WebTrust wurde als weltweit anerkannter Standard durch das American Institute of Certified Public Accountants (AICPA) und Canadian Institute of Chartered Accountants (CICA) für Zertifizierungsdienstanbieter geschaffen, um höchstmögliche Standards und Qualität international zu sichern. Bei der *Fiducia & GAD IT AG* sind unter dem Begriff "WebTrust" folgende Anforderungen zusammengefasst: • "Trust Service Principles and Criteria for Certification Authorities" (Webtrust.org): Stellen allgemeine Anforderungen zur WebTrust Zertifizierung • "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (cabforum.org): Stellen spezielle (technische) Anforderungen an eine CA • "Mozilla CA Certificate Policy" (mozilla.org): Beschreibt die Pflichten der Zertifizierungsdienstanbieter für die Aufnahme ihrer Stammzertifikate in Mozilla Produkte
X.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.