CP

Status: final

Version: 1.0

OID: 47934.6.1.2.2.01

2019-04-16

Contents

1 INTRODUCTION

The “TERACARA CA” is a root certification authority operated by WPIA - World privacy and Identity Association (WPIA).

The “TERACARA CA” only issues certificates to its subordinated issuing CAs and special purpose certificates for the operation of the CSP.

The “TERACARA CA” has six subordinate CAs: the “TERACARA Unverified Intermediate CA”, the “TERACARA Verified Intermediate CA”, the “TERACARA Codesign Intermediate CA” , the “TERACARA Orga Intermediate”, the “TERACARA OrgaSign Intermediate CA” and “TERACARA EV Intermediate CA”.

- “TERACARA Unverified Intermediate CA” issues certificates that support digital signing and/or encryption and/or client authorisation for individuals whose identity are not verified and server certificates.
- “TERACARA Verified Intermediate CA” issues certificates that support digital signing and/or encryption and/or client authorisation for individuals whose identity are verified and server certificates.
- “TERACARA Codesign Intermediate CA” issues certificates that support digital signing code for individuals whose identity are verified.
- “TERACARA Orga Intermediate CA” issues certificates that support digital signing and/or encryption and/or CLIENT AUTHORISATION for individuals belonging to a verified organisation and server certificates to domains owned by and verified to the organisation.
- “TERACARA OrgaSign Intermediate CA” issues certificates that support digital signing code for individuals belonging to a verified organisation.
- “TERACARA EV Intermediate CA” issues Extended Validation SSL certificates.

For the issuance of certificates intended to be used for authenticating servers accessible through the Internet, WPIA conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

For the issuance of Extended Validation SSL certificates, WPIA fully complies with all the rules and regulations published by the CA/Browser Forum (http://www.cabforum.org/):

- EV Guidelines: “Guidelines for the Issuance and Management of Extended Validation Certificates”.

WPIA complies with the following Austrian and European laws including the relevant international standards:

- Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG) BGBl I Nr. 190/1999 i.d.g.F. BGBl. I Nr. 50/2016
- Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG) BGBl I Nr. 50/2016
- Verordnung zum Signaturgesetz (SigV), BGBl II 30/2000 und BGBl II Nr. 527/2004
- Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (SigRL)
- REGULATION (EU) Nr. 910/2014 electronic identification and trust services for electronic transactions in the internal market ("eIDAS-Regulation")

Austrian and European laws refers to the standards listed below that are prerequisites for the issuance of qualified certificates:

- ETSI TS 101 456 v1.4.1: Electronic Signatures and Infrastructures (ESI) – Certificate Policy and Certification Practices Framework
- ETSI TS 101 861 v1.3.1: Time Stamping Profile
- IETF RFC 3647 (2003): Internet X.509 Public Key Infrastructure – Certificate Policy and Certi-fication Practices Framework
- IETF RFC 5280 (2002): Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

The "TERACARA Unverified Intermediate CA", the "TERACARA Verified Intermediate CA" , the "TERACARA Codesign Intermediate CA", the "TERACARA Orga Intermediate CA", the "TERACARA OrgaSign Intermediate CA" and "TERACARA EV Intermediate CA" have a subset of issuing CAs for certificates that meet the stipulations of the European Technical Specification ETSI TS 102 042 – "Normalized" Certificate Policy (NCP). Certificates issued by these CAs do not meet the requirements of the Austrian and European Digital Signature Law and are not governed by the Austrian and European digital signature laws listed above.

All the certificates issued by the "TERACARA Unverified Intermediate CA", the "TERACARA Verified Intermediate CA" , the "TERACARA Codesign Intermediate CA" are free of charge. All the certificates issued by the

"TERACARA Orga Intermediate CA", the "TERACARA OrgaSign Intermediate CA" and "TERACARA EV Intermediate CA" are only available for cooperative member of the WPIA Cooperative eG - Genossenschaft zur Förderung von sicheren Technologien und Grundrechten im Internet (https://wpia.coop).

In this CP/CPS, "this CA" refers to the "TERACARA CA" and all its subordinated CAs, unless stated differently.

1.1 Overview

The picture below shows the structure of the TERACA CA tree:

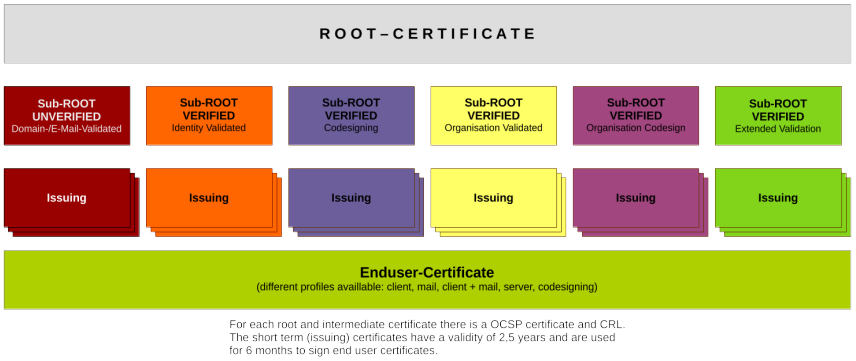

Figure 1: Figure 1: TERACARA CA Hierachy

This WPIA certificate policy and certification practice statement (CP/CPS) for the "TERACARA CA" and all its subordinate CAs describes:

- The certification and registration policy of this CA.
- Practices and procedures of this CA.
- Practices and procedures of the registration authorities for this CA.
- Terms and conditions under which this CA is made available.

This CP/CPS is applicable to all persons, including, without limitation, all requesters, subscribers, relying parties, registration authorities and any other persons, that have a relationship with TERACARA and WPIA with respect to certificates issued by this CA.

This CP/CPS also provides statements of the rights and obligations of SwissSign AG, authorized registration authorities, requesters, subscribers, relying parties, resellers, co-marketers and any other person, or organisation that may use or rely on certificates issued by this CA.

TERACARA provides a detailed product overview on their website (teracara.org) for certificates and for other services.

1.2 Document name and identification

This document is named "TERACARA Certificate Policy and Certification Practice Statement" as indicated on the cover page of this document.

The Object identification number (OID) for this document is:

OID 47934.6.1.2.2.01

Please note that the above OID identifies this document and this document only.

The OID of WPIA is based on the RDN issued by IANA and structured as follows:

PEN	SO	T	ST	DT	NN	-	LC	Description	Notice
47934								Private Enterprise Number (PEN)	as assigned by IANA
	6							Structural Organisation	
		1						Type	
			2					Sub-Type	
				2				Document-Type	
					1			Number (of the Document/Object)	Serial Number, starts with 2 digits

The above structure may be expanded without any problems, as long as already associated OIDs remain untouched.

1.2.1 Revisions

Ver.	Ballot	Description	Adopted	Effective*
1.0		Version 1.0 of the Baseline Requirements Adopted	2019-04-16	2019-04-16

- Effective Date and Additionally Relevant Compliance Date(s)

1.2.2 Relevant Dates

Compliance	Section(s)	Summary Description (See Full Text for Details)
xxx		

1.3 PKI participants

1.3.1 Certification authorities

The TERACARA CA and its subsidiary CAs (TERACARA Unverified Intermediate CA, TERACARA Verified Intermediate CA, TERACARA Codesign Intermediate CA, TERACARA Orga Intermediate CA, TERACARA OrgaSign Intermediate CA and TERACARA EV Intermediate CA) are the only public CAs operated by WPIA that issue certificates under this CP/CPS. WPIA may under this CP/CPS issue at any time additional subsidiary CAs for private or enterprise purposes.

1.3.2 Registration authorities

WPIA operates a registration authority, called TERACARA RA that registers subscribers of certificates issued by this CA.

1.3.3 Subscribers

In the context of this CP/CPS, the term “subscriber” or “Certificate Holder” encompasses all end users of certificates issued by this CA:

- Requesters are individuals that have requested (but not yet obtained) a certificate.
- Subscribers are individuals that have obtained a certificate.

Subscribers and requesters are responsible for:

- having a basic understanding of the proper use of public key cryptography and certificates;
- providing only correct information without errors, omissions or misrepresentations;
- substantiating information by providing a properly completed and personally signed registration form;
- supplementing such information with a proof of identity and the provision of the information as specified in chapter 3.1 and 3.2;
- verifying the content of a newly issued certificate before its first use and to refrain from using it, if it contains misleading or inaccurate information.
- reading and agreeing to all terms and conditions of this CP/CPS, other relevant regulations and agreements;
- the maintenance of their certificates using the tools provided by the RA;
- deciding on creation of a certificate or to a later time whether the respective certificate is to be published in the public directory: URL;
- using TERACARA certificates exclusively for legal and authorized intended purposes;
- ensuring that TERACARA certificates are exclusively used on behalf of the person specified as the subject of the certificate;
- protecting the private key from unauthorized access;
- using the private key only in secure computing environments that have been provided by trustworthy sources and that are protected by state-of-the-art security measures;
- ensuring complete control over the private key by not sharing private keys and passwords and not using easily guessable passwords;
- notifying the registration authority of any change to any of the information included in the certificate or any change of circumstances that would make the information in the certificate misleading or inaccurate;
- invalidating the certificate immediately if any information included in the certificate is misleading or inaccurate, or if any change of circumstances, makes the information in the cer-tificate misleading or inaccurate;
- notifying the registration authority immediately of any suspected or actual compromise of the private key and requesting that the certificate be revoked;

- immediately ceasing to use the certificate upon (a) expiration or revocation of such a certificate, or (b) any suspected or actual damage/corruption of the private key corresponding to the public key in such a certificate, and immediately removing such a certificate from the devices and/or software onto which it has been installed;
- refraining to use the subscriber's private key that corresponds to the public key certificate to sign other certificates;
- using their own judgment about whether it is appropriate, given the level of security and trust provided by a certificate issued by this CA, to use such a certificate in any given circumstance;
- using the certificate with due diligence and reasonable judgment;
- complying with all laws and regulations applicable to a subscriber's right to export, import, and/or use a certificate issued by this CA and/or related information. Subscribers shall be responsible for procuring all required licenses and permissions for any export, import, and/or use of a certificate issued by this CA and/or related information.

1.3.4 Relying parties

Relying parties are individuals or organisations that use certificates of this CA to validate the signatures and verify the identity of subscribers and/or to secure communication with these subscribers. Relying parties are allowed to use such certificates only in accordance with the terms and conditions set forth in this CP/CPS. It is in their sole responsibility to verify legal validity and applicable policies.

The Relying Party agrees to observe the following conditions:

- Orga and Orga Sign Certificates may only be used in accordance with the rules stipulated in the "Orga Certificate Policy and Certification Practice Statement".
- The Relying Party is obliged to have an appropriate understanding of the proper use of public key cryptography as well as an understanding of the associated risks.
- TERACARA Certificates may be used exclusively in accordance with applicable laws, rules, and regulations and only for authorized intended purposes.
- It is the sole responsibility of the Relying Party to always use the certificate with due diligence and reasonable judgment.
- It is in the sole responsibility of the Relying Party to verify revocation status, legal validity and applicable policies.

- The revocation status can be checked via OCSP or via CRL (Certificate Revocation List). The Relying Party must be aware, that the CRLs are valid 3 days, but updated second day. Therefore the Relying Party shall always check the newest available CRL to have the complete, up to date revocation information.
- Should the situation arise that for technical reasons an updated CRL is not available, it is the relying party's responsibility to decide how long a CRL is to be trusted for revocation checking. This decision may depend on the type of transaction being authorized and the damage potential. Under no circumstances should the trust be extended beyond the maximum life time of the CRL.

Relying parties can also be subscribers within this CA.

1.3.5 Other participants

Other participants are individuals or organisations that rely on the certificate of a subscriber, or are in some way involved with certificate manufacturing and may or may not wish to verify the identity of subscribers and/or to secure communication with this subscriber.

Other participants can be also subscribers within this CA.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The following certificates are issued under this CA:

All certificates issued by TERACARA CA's have the following key usage bits set: digitalSignature, keyEncipherment and keyAgreement

Personal SSl Certificates are issued by TERACARA CA's with the following extended key usage bit set: clientAuth

Personal mail Certificates are issued by TERACARA CA's with the following extended key usage bit set: emailProtection

Personal SSL and mail Certificates are issued by TERACARA CA's with the following extended key usage bits set: clientAuth and emailProtection

Codesigning Certificates are issued by TERACARA CA's with the following extended key usage bits set: codeSigning, msCodeInd and msCodeCom

Server Certificates are issued by the TERACARA CA's with the following extended key usage bit set: serverAuth

EV Certificates are issued by the TERACARA CA's with the following extended key usage bit set: serverAuth

1.4.2 Prohibited certificate uses

Any other use than defined in chapter 1.4.1 is prohibited.

This specifically includes the prohibition of using subordinate CAs chaining to this CA for MITM or "traffic management" of domain names or IPs that the certificate holder does not legitimately own or control, regardless of whether it is in a closed and controlled environment or not.

1.5 Policy administration

1.5.1 Organisation administering the document

The TERACARA CP/CPS is written and updated by WPIA.

World Privacy and Identity Association (WPIA) - Verein zur Förderung von sicheren Technologien und Grundrechten im Internet

c/o realraum

Brockmanngasse 15

8010 Graz

Österreich

E-Mail: info@wpia.club

Current versions of documents may be downloaded from the WPIA policy website: http://policy.wpia.club/

1.5.2 Contact person

The following persons are the main contacts for any questions or suggestions regarding the TERACARA CP/CPS.

Reinhard Mutz

President of WPIA

cps.feedback@wpia.club

All feedback, positive or negative, is welcome and should be submitted to the above email address to ensure that it is dealt with appropriately and in due time.

1.5.3 Person determining CPS suitability for the policy

Executive management of WPIA determines the suitability and applicability of this CP/CPS.

1.5.4 CPS approval procedures

Executive management of WPIA regularly evaluates this CP/CPS and its related documentation so that it adheres to applicable law, such as stipulated in chapter 1 of this CP/CPS.

1.6 Definitions and acronyms

1.6.1 Definitions

- **Affiliate** A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.
- **Applicant** The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.
- **Applicant Representative** A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA.
- **Application Software Supplier** A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.
- **Attestation Letter** A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.
- **Audit Report** A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.
- **Authorization Domain Name** The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then the CA MUST remove all wildcard labels from the left most portion

of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.

- **Authorized Port** One of the following ports: 80 (http), 443 (http), 115 (sftp), 25 (smtp), 22 (ssh).
- **Base Domain Name** The portion of an applied-for FQDN that is the first domain name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For gTLDs, the domain www.[gTLD] will be considered to be a Base Domain.
- **CAA** From RFC 6844 (http:tools.ietf.org/html/rfc6844): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) 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."
- **Certificate** An electronic document that uses a digital signature to bind a public key and an identity.
- **Certificate Data** Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.
- **Certificate Management Process** Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.
- **Certificate Policy** A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.
- **Certificate Problem Report** Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.
- **Certificate Revocation List** A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.
- **Certification Authority** An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.

- **Certification Practice Statement** One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.
- **Control** "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors ; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.
- **Country** Either a member of the United Nations OR a geographic region recognized as a sovereign nation by at least two UN member nations.
- **Credentials** Evidence or testimonials governing the user's right to access certain systems (e.g. User name, password, etc).
- **Cross Certificate** A certificate that is used to establish a trust relationship between two Root CAs.
- **Data Encryption Standard** A cipher developed by the United States government in the 1970s as the official encryption algorithm of the U.S.
- **Decryption** The process of transforming cipher text into readable plain text.
- **Delegated Third Party** A natural person or Legal Entity that is not the CA but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.
- **Domain Authorization Document** Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.
- **Domain Contact** The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record.
- **Domain Name** The label assigned to a node in the Domain Name System.
- **Domain Namespace** The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

- **Domain Name Registrant** Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.
- **Domain Name Registrar** A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).
- **Effective Date** TBD.
- **Encryption** Encryption is the process of using a formula, called an encryption algorithm, to transform plain text into an incomprehensible cipher text for transmission.
- **End Entity** Used to describe all end users of certificates, i.e. subscribers and relying parties.
- **End User Agreement** Contractual agreement between seller of certificates and the subscriber.
- **Enterprise RA** An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.
- **Enterprise EV Certificate** An EV certificate that an enterprise RA authorizes the CA to issue at third and higher domain levels that are contained within the domain that was included in an original valid EV certificate issued to the enterprise RA.
- **Entropy** A numerical measure of the uncertainty of an outcome. The entropy of a system is related to the amount of information it contains. In PKI and mathematics, a cryptographic key contains a certain amount of information and tends to lose a small amount of entropy each time it is used in a mathematical calculation. For this reason, one should not use a key too frequently or for too long a period.
- **EV Certificate** A digital certificate that contains information specific in the EV guidelines and that has been validated in accordance with the guidelines.
- **Extended Validation** Validation procedures defined by the guidelines for Extended Validation Certificates published by a forum consisting of major certification authorities and major browser vendors.
- **Expiry Date** The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

- **Fully-Qualified Domain Name** A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.
- **Government Entity** A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).
- **Hardware Security Module** Hardware Security Module is a device that physically protects key material against unauthorized parties.
- **High Risk Certificate Request** A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.
- **Internal Name** A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.
- **Issuing CA** In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.
- **Key Compromise** A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value. A Private Key is also considered compromised if methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys) or if there is clear evidence that the specific method used to generate the Private Key was flawed.
- **Key Generation Script** A documented plan of procedures for the generation of a CA Key Pair.
- **Key Pair** The Private Key and its associated Public Key.
- **Legal Entity** An association, corporation, partnership, proprietorship, trust, government entity or other entity with legalstandingin a country's legal system.
- **Lightweight Directory Access Protocol** LDAP is used to retrieve data from a public directory.

- **Object Identifier** A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.
- **OCSP Responder** An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.
- **Online Certificate Status Protocol** An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.
- **Parent Company** A company that Controls a Subsidiary Company.
- **Private Key** The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
- **Profile** A user profile is a personal area where end users can access and manage their digital identities and requests directly on the TERACARA web page. Access to this profile can be granted by means of user name and password.
- **Public Key** The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
- **Public Key Infrastructure** A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.
- **Publicly-Trusted Certificate** A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.
- **Qualified Auditor** A natural person or Legal Entity that meets the requirements of Section 8.3.
- **Random Value** A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.
- **Registered Domain Name** A Domain Name that has been registered with a Domain Name Registrar.

- **Registration Authority (RA)** Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.
- **Reliable Data Source** An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.
- **Reliable Method of Communication** A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.
- **Relying Party** Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.
- **Repository** An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
- **Request Token** A value derived in a method specified by the CA which binds this demonstration of control to the certificate request.

  The Request Token SHALL incorporate the key used in the certificate request.

  A Request Token MAY include a timestamp to indicate when it was created.

  A Request Token MAY include other information to ensure its uniqueness.

  A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation.

  A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future.

  A Request Token that does not include a timestamp is valid for a single use and the CA SHALL NOT re-use it for a subsequent validation.

  The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.
- **Requester** Requesters are individuals or organization that have requested, but not yet obtained a certificate.

- **Required Website Content** Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.
- **Requirements** The Baseline Requirements found in this document.
- **Reserved IP Address** An IPv4 or IPv6 address that the IANA has marked as reserved:

  http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

  http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
- **Root CA** The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.
- **Root Certificate** The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.
- **Secure Signature Creation Device** Signature-creation device which meets the requirements specified in annex III of Directive 1999/93/EC.
- **Signature** Cryptographic element that is used to identify the originator of the document and to verify the integrity of the document.
- **Sovereign State** A state or country that administers its own government, and is not dependent upon, or subject to, another power.
- **Subject** The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
- **Subject Identity Information** Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.
- **Subordinate CA** A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.
- **Subscriber** A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber or Terms of Use Agreement.
- **Subscriber Agreement** An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
- **Subsidiary Company** A company that is controlled by a Parent Company.

- **Technically Constrained Subordinate CA Certificate** A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.
- **Terms of Use** Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA.
- **Test Certificate** A Certificate with a maximum validity period of 30 days and which i) includes a critical extension with the specified Test Certificate CABF OID, or ii) which chains to a root certificate not subject to these Requirements.
- **Traffic management** Management and surveillance of network traffic with domain names or IPs owned or controlled by third parties.
- **Trustworthy System** Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.
- **Two-factor authentication** A two-factor authentication is any authentication protocol that requires two independent ways to establish identity and privileges.
- **Unregistered Domain Name** A Domain Name that is not a Registered Domain Name.
- **Valid Certificate** A Certificate that passes the validation procedure specified in RFC 5280.
- **Validation Specialists** Someone who performs the information verification duties specified by these Requirements.
- **Validity Period** The period of time measured from the date when the Certificate is issued until the Expiry Date.
- **Wildcard Certificate** A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

1.6.2 Acronyms

- **AICPA** American Institute of Certified Public Accountants
- **CA** Certification Authority

- **CAA** Certification Authority Authorization
- **CAO** Certification Authority Operator
- **ccTLD** Country Code Top-Level Domain
- **CICA** Canadian Institute of Chartered Accountants
- **CP** Certificate Policy
- **CPS** Certification Practice Statement
- **CRL** Certificate Revocation List
- **CT** Certificate Transparency
- **DBA** Doing Business As
- **DES** Data Encryption Standard. A cipher developed by the United States government in the 1970s as the official encryption algorithm of the U.S.
- **DN** Distinguished Name
- **DNS** Domain Name System
- **ETSI** European Telecommunications Standards Institute
- **EV** Extended Validation
- **FIPS(US Government)** Federal Information Processing Standard
- **FQDN** Fully-Qualified Domain Name
- **HSM** Hardware Security Module
- **HTTP** Hyper-Text Transfer Protocol used by the Internet. HTTP defines how data is retrieved or transmitted via the Internet and what actions should be taken by web servers and browsers.
- **HTTPS** Secure Hyper-Text Transfer Protocol using TLS/SSL
- **IANA** Internet Assigned Numbers Authority
- **ICANN** Internet Corporation for Assigned Names and Numbers
- **IETF** Internet Engineering Task Force
- **IM** Instant Messaging
- **IP** Internet Protocol number
- **ISO** International Organization for Standardization
- **ITIL** Information Technology Infrastructure Library

- **LDAP** Lightweight Directory Access Protocol
- **MITM** Man-in-the-middle, active eavesdropping of secure communications in which attacker/ third party relays and controls messages between sender and receiver.
- **NIST(US Government)** National Institute of Standards and Technology
- **OCSP** Online Certificate Status Protocol
- **OID** Object Identifier
- **PKD** Public Key Directory
- **PKI** Public Key Infrastructure
- **PKIX** Public Key Infrastructure Exchange
- **RA** Registration Authority
- **RAO** Registration Authority Operator
- **RFC** Request For Comments
- **S/MIME** Secure MIME (Multipurpose Internet Mail Extensions)
- **SCT** Signed Certificate Timestamp
- **SSCD** Secure Signature Creation Device
- **SSL** Secure Sockets Layer
- **TLD** Top-Level Domain
- **TLS** Transport Layer Security
- **TSA** Time-stamping Authority
- **TTP** Trusted Third Party
- **UTC** Coordinated Universal Time
- **VOIP** Voice Over Internet Protocol
- **WPIA** World Privacy and Identity Association (WPIA) - Verein zur Förderung von sicheren Technologien und Grundrechten im Internet

1.6.3 References

- ETSI TS 119 403, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - General Requirements and Guidance.
- ETSI TS 102 042, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.
- ISO 21188:2006, Public key infrastructure for financial services – Practices and policy framework.
- NIST SP 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications, http://csrc.nist.gov/publications/nistpubs/800-89/SP-800-89_November2006.pdf.
- RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner, March 1997.
- RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999.
- RFC2560, Request for Comments: 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP M. Myers, et al, June 1999.
- RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.
- RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake-Wilson, et al, April 2006.
- RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, A. Deacon, et al, September 2007.
- RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.
- WebTrust for Certification Authorities, SSL Baseline with Network Security, Version 2.0, available at http://www.webtrust.org/homepage-documents/item79806.pdf.

- X.509v3, ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

1.6.4 Conventions

The words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document shall be interpreted in accordance with IETF RFC 2119.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

WPIA will make its certificate(s), CP/CPS, CRL and related documents for this CA publicly available through the URL web sites. To ensure both integrity and authenticity, all documents must be digitally signed. To document the validity period of the document, a version history is included.

2.1 Repositories

TERACARA maintains the following services on a 24/7 basis:

- PKD address
- OCSP address
- CRL address

The PKD is an opt-in service under control of the certificate owner. The OCSP service offers the status of all issued certificates (revoked/not revoked) and the CRLs the revoked information of all revoked certificates.

2.2 Publication of certification information

TERACARA publishes the following information on website address:

- Information how to obtain a certificate
- Technical documentation of repository (OCSP responder, ???)
- Certificate profile

- Information about revocation service

A notification of certificate owners and related contracting parties will be sent in the event of

- revocation of any root or intermediate certificate
- compromise of any root or intermediate certificate, relevant keys or proper business operation
- security related changes to the CP/CPS

Notifications will be published at minimum on the website, including affected documents and certificates, or by email if such contact details are available.

TERACARA conforms to the current (1.6.2) version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

The data formats used for certificates issued by this CA and for certificate revocation lists in the URL web site are in accordance with the associated schema definitions as defined in the X.500 series of recommendations.

Certificate dissemination services are available 24 hours per day, 7 days per week with a guaranteed uptime of 99%.

2.3 Time or frequency of publication

New issued certificates, CRLs, Policies and if necessary other information will be published in a timely manner. These publish frequencies are used:

- Certificate will be published on the PKD immediately after issuance, but not later than 7 days given the certificate owner opts in to publication. Certificates will be kept available after their expiration for at least one year, but not longer than 2 years.
- CRL are renewed at least every 48 hours with a maximum validity of 72 hours
- Policies are renewed as neccessary, at least once a year.

2.4 Access controls on repositories

Published information quoted in 2.1 and 2.2 are publicly available in a read-only manner.

3 Identification and Authentication

This section describes the mechanisms used in the process of vetting, identification and authentication prior to certificate issuance:

- Applicant is personally identified in the RA
- Received forms are checked regarding completeness and plausibility of data
- Presented documents are checked for authentity
- The identification is done according to the Verification process with at least 2 meetings with RA authorised staff or affiliate

3.1 Naming

3.1.1 Types of names

The distinguished name (DN) in a certificate issued by the 'TERACARA CA' or one of its subsidiaries complies with the X.500 standard.

For the distinguished name a minimum of one field is required. This field must be /CN=.

For the common name (CN) WPIA allows several types of names to be specified:

- real names
- organisation names
- pseudonyms
- fully qualified domain names (FQDN)
- for unverified user accounts: 'TERACARA User' is used on unverifed user accounts and as placeholder for anonymous certificates

Real names are specified as /CN='First Name' optional 'Middle Names' 'Last Name' or /CN='Organisational Name'.

First, Middle and Last Name in the CN have to be absolutely identical to the names as they appear in the identifying documentation provided. Special characters are treated according to chapter 3.1.4. Abbreviations or nicknames without substantiating identifying documentation are prohibited. Names consisting of multiple words are permissible.

The organisational name in /CN or in /O MUST be spelled absolutely identical to the name as it appears in the documentation provided according to chapter 3.2.2.

If the CN is a organisational name, then the entries in the /O and /C field MUST also be inserted. In this case the /CN field MUST be identical to the /O field.

Pseudonyms are specified as /CN=‘identifier’: ‘arbitrary string’. The TERACARA RA recommends pseudonym certificates to use the string ‘pseudo’ as identifier. An example of a correctly formulated pseudonym is: ‘/CN=pseudo: John Doe’.

FQDNs MUST be well formed according to RFC 1035.

The use of names in the certificate attributes MUST be authorised. This means:

- The use of an organisational name MUST be authorised according to chapter 3.2.5.
- The use of a real name and its identifying information MUST be authenticated and authorised according to chapter 3.2.3.
- A pseudonym requires that the requester authenticates and authorises the request containing identifying information according to chapter 3.2.3.
- The use of a FQDN requires authorisation of the domain owner. For individuals the rules in chapter 3.2.3 and for organisations the rules in chapter 3.2.5 apply respectively.
- The use of a FQDN MAY be authorised through domain validation if an organisational name is part of the subject. Domain validation MUST be obtained by at least two of the following methods:
  - The requester proves control of an email to authoritative email addresses according to {&#3.2.2.4.4} or a subset thereof.
  - The requester proves control over the DNS RR from authoritative servers of that domain.
  - The requester proves control over the web server a specific content on the target domain using HTTP or HTTP over an TLS encrypted channel.
  - The requester proves control over the web server with an installed certificates issued under this CPS or containing a random challenge domain name.

SubjectAltName is a recommended field for certificates issued with real names or pseudonyms. If it is present, it contains at least an email address.

Additional attributes in the SubjectAltName are permissible in any certificate and MAY be supported by the RA at their own discretion:

- email: email address according to rfc 5322

- dNSName: FQDN, fully qualified domain name according to rfc 1035.

For Extended Validation Certificates the following, additional rules apply:

- The certificate subject MUST be conform to the EV guidelines.
- Wildcard certificates are not permissible.

3.1.2 Need for names to be meaningful

The subject and issuer name contained in a certificate MUST be meaningful in the sense that the RA has proper evidence of the existent association between these names or pseudonyms and the entities to which they belong. To achieve this goal, the use of a name MUST be authorised by the rightful owner or a legal representative of the rightful owner. The naming is done according to these requirements:

- The notation of the name MUST match the one found in an government issued ID document. The ID document MAY hold more data than the name but not less.
- The applicant MAY have more than one verified name.

3.1.3 Anonymity or pseudonymity of subscribers

The certificate owner MAY request an anonymised certificate. 'TERACARA user' will be used as name in the certificate. Each user has a specific account to which this certificate matches.

If a pseudonym is proved by the verification it can be used instead of the real name. In this case the subscribers have to clearly mark the certificate as a pseudonym. To this end the /CN= attribute in the subject MUST start with the following sequence:

- Identifier is a string that clearly indicates the nature of the CN. The TERACARA RA only allows the string 'pseudo'
- The identifier and the content of the /CN= attribute MUST be separated with a sequence.

A subscriber can use any string of characters after the identifier.

WPIA or TERACARA RAs reserve the right to reject certificate requests or revoke certificates containing offensive or misleading information or names protected by legislation and infringing rights of others.

3.1.4 Rules for interpreting various name forms

Allowed variations of various name forms are defined in Verification Policy (OID 47934.6.1.2.5.01) and its subpolicies.

3.1.5 Uniqueness of names

The CAs operating under this CP/CPS do enforce the uniqueness of certificate subject fields in such a manner that all valid certificates with identical subject fields MUST belong to the same in-dividual or organisation. The following rules are enforced:

- All actual valid certificates for individuals with identical subjects MUST belong to the same individual.
- All actual valid organisational certificates with identical subjects MUST belong to the same organisation.
- All actual valid server certificates with identical subjects MUST belong to the same domain owner.
- The uniqueness of names within certificates is guaranteed through a unique serial number.
- Each serial number maps with a unique account and therefore to a unique account owner.
- Domain names and email addresses can only be registered to one account. See also chapter “1.4.1, Appropriate certificate uses”.

3.1.6 Recognition, authentication, and role of trademarks

WPIA and its RAs reserve the right to reject certificate requests or revoke certificates containing offensive or misleading information or names protected by legislation and possibly infringing rights of others. WPIA is not obliged to verify lawful use of names. It is the sole responsibility of the subscriber to ensure lawful use of chosen names. WPIA will comply as quickly as possible with any court orders issued in accordance with Austrian Law that pertain to remedies for any infringements of third party rights by certificates issued under this CPS.

3.1.7 CAA (Certification Authority authorisation) Records

WPIA checks for CAA Records. If alerted to the presence of a CAA record not containg the CA information the issuing of a certificate will be declined..

3.2 Initial identity validation

The initial identity validation is part of the Certificate Application process as described in chapter 4.1. In conformance with a requirement of the Mozilla Foundation concerning SSL Server certificates, every RA operating under this CP/CPS MUST ascertain:

- NOT to issue certificates for SSL Servers with a lifetime exceeding 27 months.

3.2.1 Method to prove possession of private key

The Certificate Signing Request sent to the CA from the Subscriber is signed with the private key. Therefore the possession of the private key is proven.

3.2.2 Authentication of organisation identity

The DN of a certificate issued by one of the subsidiaries of this CA MAY contain one instance of the organisation field. Should the requester decide to make the organisation field part of the DN, the following rules MUST be adhered to:

- The use of the organisation field means that the use of the country field is mandatory.
- The registration process of any registration authority operating under this CP/CPS MUST contain provisions to determine the identity of an organisation and to authorise the use of its name.
- To validate the name of the organisation, the requester MUST provide official documentation about the organisation. Organisations with an entry in the federal commercial register MUST supply current excerpt. All other organisations MUST supply the European VAT ID or an equivalent information.
- The use of the organisation's name MUST be authorised by one or more legal representatives of the organisation, and handwritten personal signatures MUST be included on the registration form.
- The use of a domain name in an FQDN MUST be authorised by the domain owner or its representatives. The domain owner MAY be determined through the WHOIS information provided by the domain registrar. Should an organisation be listed as the domain owner, authorisation MUST be given by one or more legal representatives of the organisation with handwritten personal signatures on the registration form. Should an individual be listed as the owner, this individual MUST personally sign

the registration form. The RA will create a high-quality copy or scan of all required supporting documentation. Alternatively and only if an organisation name is present in the certificate subject, domain validation according to chapter 3.1.1 MAY be used to obtain authorisation of the use of the domain name in an FQDN. In this case the handwritten signatures of the authorisation of the organisational name are the only authorisation signatures required on the registration form.

- /DC= (Domain Components) fields are verified equivalent to domain validation.

An organisation MAY contractually define that all certificates using the name of the organisation in the /O= field MAY only contain email addresses in the /email= field that are in the domain of the organisation. Should such a contract exist, the organisation takes full responsibility for the proper management of email accounts. Therefore, the requirement to verify individual email addresses during the registration process is optional.

EV Certificates will only be issued in accordance with the EV Guidelines to the following types of organisations:

- Private organisations
- Government Entities
- Business Entities
- Non-commercial Entities

The authentication identity of an organisation MUST be verified by an Organisation RA Agent according to Verification Policy and the Policy On Organisation Verification.

3.2.3 Authentication of individual identity

Various individuals MAY need to authorise the use of names in different parts of the DN. The registration process of any registration authority operating under this CP/CPS MUST contain provisions to determine the identity of such individuals. The regulations defined in the registration forms MAY be summarized as follows:

- The registration form MUST carry original, personal handwritten signatures.
- The information on the identifying document MUST match both the name and signature on the registration form.

- The wording in the request has to be identical to the given name(s) and the family name of the identifying documents.
- The /email= field MUST be verified during the registration process. The requester MUST prove that they have access to the mailbox and that they can use it to receive mail.

The authentication identity of an individual MUST be verified by an RA Agent according to Verification Policy and the Policy On Verification By RA Agent.

3.2.4 Non-verified subscriber information

All subscriber information required has to be duly verified. Additional information given by the subscriber can be ignored.

3.2.5 Validation of authority

The requester provides current and valid documentation for the organisational or corporate name that SHOULD be included in the certificate, according to Chapter 3.2.2. The wording of the organisational or corporate name that SHOULD be included in the certificate MUST be exactly identical to the wording in the documentation provided.

The use of the organisational name MUST be authorised by top level representatives of this organisation.

- The use of the organisational name of an organisation with a commercial register entry MUST be authorised by representatives from the board of directors and/or executive management, which are listed in the excerpt of the Federal Commercial Registry.
- The use of the organisational name of a sole proprietorship MUST be authorised by the owner named in the current VAT invoice.
- The use of the organisational name of an organisation with a deed of partnership MUST be authorised by a partner named in the deed of partnership.
- The use of the organisational name of a community MUST be authorised by the corresponding civic agency and a copy of the directive of election.

These individuals MUST be identified according to the stipulations given in chapter 3.2.3.

3.2.6 Criteria for interoperation

TERACARA CA does not use Cross Certificates. TERACARA CA does not currently allow subordinate CA to act on behalf of TERACARA CA. Other CA MAY become organisational member but the certificate will be signed with certificate under full control of TERACARA CA.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and Authentication for Routine Re-key

TERACARA does not offer re-keying.

3.3.2 Identification and Authentication for Re-key After Revocation

TERACARA does not offer re-keying.

3.4 Identification and authentication for revocation request

Revocation of a certificate that is issued by one of the subsidiaries of this CA requires that the subscriber use one of the following methods:

- Successful login to the user profile.
- Providing proof of the possession of the private key on the web site of the registration authority.

The process how the revocation request can be submitted is described in chapter 4.9.3.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application

Applications can be submitted by anyone who complies with the provisions specified in the registration form, CP/CPS and relevant End-User Agreement.

4.1.2 Enrollment process and responsibilities

Certificate subscribers have to follow TERACARA registration formalities as specified in the relevant documents and provisions provided by the CA. The certificate is issued only after successful completion of the registration process. The main steps for a certificate registration are:

(I) Valid identification documentation is provided and complete registration forms have been signed, and the CP/CPS and End-User Agreement have been accepted by the subscriber,

(II) all documents and informations are approved by WPIA.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The TERACARA RA identifies the requester on the basis of the identifying documents that the requester presents, as stipulated in chapter 3.2 of this document.

Before issuing an EV certificate, TERACARA ensures that all subject organisation information in the EV certificate conforms to the requirements of, and has been verified in accordance with, the EV Guidelines and matches the information confirmed and documented by the CA pursuant to its verification processes. Such verification processes are intended to accomplish the following:

- Verify the organisation's existence and identity, including:
  - Verify the organisation's legal existence and identity (as established with an incorporating agency).
  - Verify the organisation's physical existence (business presence at a physical address).
  - Verify the organisation's operational existence (business activity).
- Verify that the organisation (or a corporate parent/subsidiary) is a registered holder or has exclusive control of the domain name to be included in the EV certificate.
- Verify the requester's authorization for the EV certificate, including:
  - Verify the name, title, and authority of the certificate requester.
  - Verify that the certificate requester signed the registration form.
  - Verify the authority to approve the EV certificate request ("certificate approver" role according to CA Browserforum)
  - Verify the authority to approve the Terms an Conditions ("contract signer" role according to CA Browserforum)

4.2.2 Approval or rejection of certificate applications

The TERACARA RA will approve a certificate request if all of the following criteria are met:

- all documentation has been received and verified successfully,
- all authorizations have been received and verified successfully,
- the information provided in the registration form is deemed adequate and complete,
- the verification of the Uniqueness of Names according to chapter 3.1.5 has not revealed any collisions.
- for EV certificates that all stipulations of the EV Guidelines have been met.

If the requester fails to adhere to any of the above, or in any other way violates the stipulations of this document, the TERACARA RA MUST reject the certificate signing request. WPIA reserves the right to decline certificate requests without giving reasons.

4.2.3 Time to process certificate applications

After receiving the registration form as well as the complete, accurate registration documentation, the time to process certificate applications is three working days.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Upon receipt of an approved certificate signing request, the TERACARA CA will verify

- the integrity of the request;
- the authenticity and authority of the RA operator;
- verify the contents of the certificate requests for compliance with the technical specification as outlined in chapter 7.1.2.

On successful verification, the TERACARA CA will then issue the requested certificate.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The CA notifies the requester in different ways:

- the certificate is presented to the subscriber immediately, special notification MAY not be necessary.
- email information permitting the subscriber to download the certificate from a website or repository.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Once the Certificate is issued by the CA, the subscriber receives an email with a link to download the certificate. If the subscriber utilise this link, then they have accepted the certificates.

4.4.2 Publication of the certificate by the CA

The requester agrees that TERACARA will publish certificate status information in accordance with applicable regulations. The requester decides in the course of the registration process whether or not the certificate will be published.

4.4.3 Notification of certificate issuance by the CA to other entities

The CA will not notify the TERACARA RA of the certificate issuance, since the certificate was issued immediately after authorization by the subscriber.

4.4.4 Certificate Transparency

TERACARA is supporting Certificate Transparency using OCSP. During the issuing of a SSL-EV certificate TERACARA provides the EV-SSL certificate to the required amount of CT log servers. For the EV-SSL certificate TERACARA returns the SCT within the OCSP status answer to the client. This method requires the server operator to enable OCSP stapling on the server who is hosting the EV-SSL certificate. Information on Certificate Transparency MAY be found in IETF RFC 6962.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The use of certificates by subscribers MUST adhere to the obligations stipulated in chapter 1.3.3. summarized as follows:

- Certificates issued by “TERACARA Unverified Intermediate CA”, “TERACARA Verified Intermediate CA”, “TERACARA Codesign Intermediate CA”, “TERACARA Orga Intermediate”, “TERACARA OrgaSign Intermediate CA” MAY only be used in accordance with the key usage declaration contained in the certificate.
- Subscribers MAY use TERACARA certificates exclusively for intended, legal, and authorised purposes;
- Subscribers MAY only use a TERACARA certificate on behalf of the person listed as the subject of such a certificate.

4.5.2 Relying party public key and certificate usage

Relying parties SHALL:

- be held responsible for the understanding of:
  - the proper use of public key cryptography and certificates;
  - the related risks;
- read and agree to all terms and conditions of this CP/CPS and End-User Agreement;
- verify certificates issued by this CA, including use of CRLs, in accordance with the certification path validation procedure, taking into account any critical certificate extensions;
- use their best judgement when relying on a certificate issued by this CA and assess if such reliance is reasonable under the circumstances:
  - determine whether such reliance is reasonable given the extent of the security and trust provided by a certificate issued by this CA;
- comply with all laws and regulations applicable to a relying party’s right to export, import, and/or use a certificate issued by this CA and/or related information. Relying parties SHALL be responsible for procuring all required licenses and permissions for any export, import, and/or use of a certificate issued by this CA and/or related information.

4.6 Certificate renewal

Certificate renewal is a process in which a new certificate is issued to a subscriber. The certificate contains new validity information, but retains subject and key information.

The process of certificate renewal is not supported by the TERACARA RA. TERACARA RA limits the validity period of certificates to ensure that keys are used only during a stipulated period of time.

4.6.1 Circumstance for certificate renewal

As indicated in chapter 4.6 TERACARA does not support renewal.

4.6.2 Who MAY request renewal

As indicated in chapter 4.6 TERACARA does not support renewal.

4.6.3 Processing certificate renewal requests

As indicated in chapter 4.6 TERACARA does not support renewal.

4.6.4 Notification of new certificate issuance to subscriber

As indicated in chapter 4.6 TERACARA does not support renewal.

4.6.5 Conduct constituting acceptance of a renewal certificate

As indicated in chapter 4.6 TERACARA does not support renewal.

4.6.6 Publication of the renewal certificate by the CA

As indicated in chapter 4.6 TERACARA does not support renewal.

4.6.7 Notification of certificate issuance by the CA to other entities

As indicated in chapter 4.6 TERACARA does not support renewal.

4.7 Certificate re-key

Certificate re-keying is a process where a subscriber automatically obtains a new certificate if proof of key possession of the old certificate can be provided. The resulting certificate contains new validity information, a new key pair but retains the same subject.

The TERACARA RA does not offer re-keying of certificates.

4.7.1 Circumstance for certificate re-key

As indicated in chapter 4.7 TERACARA does not support re-key.

4.7.2 Who MAY request certification of a new public key

As indicated in chapter 4.7 TERACARA does not support re-key.

4.7.3 Processing certificate re-keying requests

As indicated in chapter 4.7 TERACARA does not support re-key.

4.7.4 Notification of new certificate issuance to subscriber

As indicated in chapter 4.7 TERACARA does not support re-key.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

As indicated in chapter 4.7 TERACARA does not support re-key.

4.7.6 Publication of the re-keyed certificate by the CA

As indicated in chapter 4.7 TERACARA does not support re-key.

4.7.7 Notification of certificate issuance by the CA to other entities

As indicated in chapter 4.7 TERACARA does not support re-key.

4.8 Certificate modification

Certificate modification is the process through which a subscriber requests a certificate with modified subject information. The TERACARA RA treats these requests as initial registration requests. The requester is therefore required to start a new certificate request.

4.8.1 Circumstance for certificate modification

As indicated in chapter 4.8 TERACARA does not support certificate modification.

4.8.2 Who MAY request certificate modification

As indicated in chapter 4.8 TERACARA does not support certificate modification.

4.8.3 Processing certificate modification requests

As indicated in chapter 4.8 TERACARA does not support certificate modification.

4.8.4 Notification of new certificate issuance to subscriber

As indicated in chapter 4.8 TERACARA does not support certificate modification.

4.8.5 Conduct constituting acceptance of modified certificate

As indicated in chapter 4.8 TERACARA does not support certificate modification.

4.8.6 Publication of the modified certificate by the CA

As indicated in chapter 4.8 TERACARA does not support certificate modification.

4.8.7 Notification of certificate issuance by the CA to other entities

As indicated in chapter 4.8 TERACARA does not support certificate modification.

4.9 Certificate revocation and suspension

With regard to CRL, TERACARA will adhere to these general guidelines:

- Certificates that have been revoked can never be "un-revoked".
- Certificates that have once been published on a CRL will always remain on the CRL.

4.9.1 Circumstances for revocation

Subscribers MAY revoke their certificates at will.

The TERACARA RA will revoke a subscriber's certificate if one of the following conditions is met:

- The private key of the issuing CA or any of its superior CAs has been compromised.
- The subscriber's private key store (= cryptographic token) is lost.
- Any part of the certificate subject has changed.
- The certificate /O= field is no longer valid (lost of membership in WPIA COOP, in the case of legal persons by loss of legal personality or dissolution).
- The certificate /CN= field is no longer valid (e.g. name change due to change in marital status or omission of domain registration renewal).
- The certificate issued does not comply with the terms and conditions of this CP/CPS.
- A TERACARA private key in the trust chain of the customer's certificate has been compromised,
- The subscriber does not comply with the agreed conditions and/or other applicable laws, rules and regulations. In addition, WPIA MAY investigate any such incidents and take legal action if required.
- Any information included in the certificate is misleading or inaccurate, or if any change of circumstances, makes the information in the certificate misleading or inaccurate.
- The EV certificate issued does not comply with the terms and conditions of the EV Guidelines.

4.9.2 Who can request revocation

All subsidiaries of this CA accept certificate revocation requests from the following:

- the owner of the profile used to issue the initial registration request,
- the owner of the private key,
- an authorized representative of the organisation that has approved the content of the /O= field in the certificate,
- a properly authorised RAO,
- a properly authorised CAO,
- an Austrian court of law.

4.9.3 Procedures for revocation request

Any one of these procedures can be used to successfully revoke a certificate:

- The subscriber can use the ID management functions in the profile that issued the initial registration request.
- The owner of the private key can use a SSL session with strong authentication to revoke this certificate on line.
- By using a revocation form, the subscriber can issue an offline revocation request in writing. Such a request, in order to be authorized, MUST carry the personal signature of the original requester of the certificate as well as proof of identity (as described in chapter 3.2.3).
- The subscriber can personally visit the RA offices and request the revocation of a certificate offline. The subscriber MUST present a piece of identification. For identification purposes WPIA will accept any government-issued photo identification document. Offline revocation methods are typically several days slower than online revocations. The subscriber MUST take full responsibility for any and all delays that result from the chosen revocation method.

All registrations authorities operating under this CP/CPS MUST adhere to the following stipulations:

Online revocation management services MUST be available 24 hours per day, 7 days per week. The annual availability of the revocation management services MUST be guaranteed at no less than 97% for business hours only and a maximum

unplanned service interruption duration of 10 days. Outside of business hours the service is available without guarantees.

Offline revocation management services MUST be available and be able to receive revocation requests during business hours. The registration authorities operating under this CP/CPS MUST guarantee to process a revocation request until end of day of the next business day.

4.9.4 Revocation request grace period

After the formal requirements as detailed in chapters 4.9.1 and 4.9.2 have been fulfilled, TERACARA RA will process revocation requests within 24 hours after they have been received by TERACARA.

4.9.5 Time within which CA MUST process the revocation request

After proper authorisation has been demonstrated, the TERACARA CA will process revocation requests within two hours after receiving such requests from the RA.

4.9.6 Revocation checking requirement for relying parties

Relying parties MUST, when working with certificates issued by this CA, verify these certificates at all times. This includes the use of CRLs, in accordance with the certification path validation procedure specified in RFC 5280. Also, any and all critical extensions, key usage, and approved technical corrigenda as appropriate SHOULD be taken into account.

4.9.7 CRL issuance frequency (if applicable)

The CRL of the TERACARA CA and its subsidiaries are updated according to the following schedule:

CRL

At least once every 24 hours. At most, 24 hours MAY pass from the time a certificate is revoked until the revocation is reported on the CRL.

OCSP Information

Real-time. The OCSP responder will report a certificate's revocation immediately after the revocation has been completed.

4.9.8 Maximum latency for CRLs (if applicable)

The CRL of this CA and all its subsidiaries is issued according to chapter 4.9.7 and published without delay.

4.9.9 Online revocation/status checking availability

This CA and all its subsidiaries support the OCSP protocol for online revocation checking. The OCSP responder URL is stored in every certificate issued by one of the subsidiaries of the TERACARA CA (field “Authority Info Access”).

4.9.10 Online revocation checking requirements

Relying parties MUST, when working with certificates issued by this CA, at all times verify the certificates issued by this CA. This includes the use of CRLs in accordance with the certification path validation procedure specified in RFC 5280 and/or RFC 2560 or OCSP.

4.9.11 Other forms of revocation advertisements available

Currently no other forms of revocation advertisements are available.

4.9.12 Special requirements regarding key compromise

If a subscriber knows or suspects that the integrity of their certificate’s private key has been compromised, the subscriber SHALL:

- immediately cease using the certificate,
- immediately initiate revocation of the certificate,
- delete the certificate from all devices and systems,
- inform all relying parties that MAY depend on this certificate.

The compromise of the private key MAY have implications on the information protected with this key. The subscriber MUST decide how to deal with the affected information before deleting the compromised key.

4.9.13 Circumstances for suspension

Certificates MAY not be suspended.

4.9.14 Who can request suspension

Certificates MAY not be suspended.

4.9.15 Procedure for suspension request

Certificates MAY not be suspended.

4.9.16 Limits on suspension period

Certificates MAY not be suspended.

4.10 Certificate status services

4.10.1 Operational characteristics

The TERACARA certificate status services are CRL and OCSP. Access to these services is through the website "teracara.org". The certificate status services provide information on the status of valid certificates. The integrity and authenticity of the status information is protected by a digital signature of the respective CA.

4.10.2 Service availability

Certificate status services are available 24 hours per day, 7 days per week.

TERACARA RA provides customers with pre-filled revocation request forms during the registration process. TERACARA RA guarantees timely processing of revocation requests without undue delay if these forms are sent through registered mail and if all required signatures are present.

4.10.3 Optional features

The TERACARA certificate status services do not include or require any additional features.

4.11 End of subscription

End of subscription occurs after:

- successful revocation of the last certificate of a subscriber,

- expiration of the certificate of a subscriber.

For reasons of legal compliance, the TERACARA CA and TERACARA RA MUST keep all subscriber data and documentation for a minimum period of 11 years after termination of a subscription.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

TERACARA RA does not offer key escrow and key recovery.

4.12.2 Session key encapsulation and recovery policy and practices

This CA and its subsidiaries do not support session key encapsulation.

5 Facility, Management, and Operations Controls

5.1 Physical controls

Two identical clones of the TERACARA CA keys are stored offline in TBD bank safe deposit boxes. The TERACARA CA servers are located in a commercial data center that meets the highest security requirements:

- The data center complies with the TBD.
- The data center is ISO 27001 & ISO 22301 certified.
- The data center as well as its operation is annually reviewed.

5.1.1 Site location and construction

TBD bank: TBD

Data center: The TERACARA electronic data processing center is located in a data center TBD.

5.1.2 Physical access

TBD bank: Physical access is only granted to a group of three persons, where one must be a member of the board of WPIA. Identification documentation (Passport, ID) and the personal signature of every employee are checked by the personnel of the TBD Bank. TBD bank personnel does not have access to the safe deposit box.

Data center: Physical access is restricted to system administrators and authorized data center personnel. Biometric and electronic badge identification is required to enter the facility in which all movements are recorded by video and access control points.

5.1.3 Power and air-conditioning

TBD bank: Workspace with power facilities is available whenever needed.

Data center: The data center is air-conditioned so as to create an optimal environment for the system according to generally accepted best practices. Power relies on two independent local power suppliers as well as on independent emergency diesel generators and on emergency battery power.

5.1.4 Water exposure

TBD bank: The two TBD banks are not located in the same zone of exposure.

Data center: The data center has water sensors in all double floors. Adequate alarming is ensured. The data center is located in an area that has no special exposures.

5.1.5 Fire prevention and protection

TBD bank: Both TBD banks have fire prevention and protection.

Data center: The fire prevention system is an advanced VESDA (very early smoke detection system) and gas-type system. The data center has an Energen-based fire extinguishing system.

5.1.6 Media storage

All data relevant to CA services, whether offline or online in nature, is encrypted and stored.

The disposal of storage media is outsourced to a third party specializing in the destruction of data on storage media.

5.1.7 Waste disposal

The regular operations of the CA services does not create waste in the data center that would require any special action.

5.1.8 Off-site backup

The system periodically generates a backup of all digital information (data, code, configuration, etc.). The backup contains all information relevant for the CA service in encrypted form. A backup media is created and stored off-site in a bank safe deposit box. This process guarantees that the off-site storage of all data from the PKI environment is fully encrypted.

5.2 Procedural controls

5.2.1 Trusted roles

In order to guarantee a segregation of duties, the TERACARA CA and RA are operated by three separated authorisation groups, Access, Operations and Audit. Any one employee MAY only be part of one of these authorization groups. Within these authorisation groups, multiple roles are defined (see picture below). An employee assigned to one of the groups MAY have one or more roles within the same authorization group.

a) Access (AXS & CAM)

Network Administrators (NA) have full control over the network access to all the systems that, when combined, define the TERACARA PKI. The NA has no access to the application software. In other words, an NA neither “sees” the CA software, nor the CA defined in this software, nor the data in the CA.

The CA Manager (CAM) defines, creates, changes, deletes, and thus has full control over one or more of the actual CA and RA systems. The CAM uses the hardware and software provided by the SA.

b) Operations (OPS & RAO/CAO)

System Administrators (SA) have full control of the hardware, operating system and application software (like the CA server), but not of cryptographically relevant information such as the private key of the CA, or the CA itself. The SA is authorized to install, configure, and maintain the CA’s trustworthy systems for registration, certificate generation, subject-device provision and revocation management.

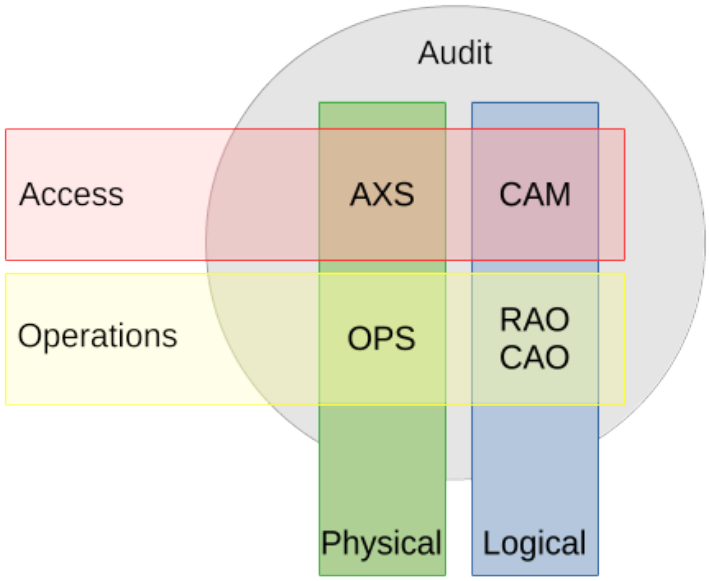

Figure 2: Figure 2: Segregation of duties

Certification Authority Operators (CAO) can manage all certificates, requests, and profiles as well as a subset of certificate authorities described by the operator access rules. The CAO works with the CA as defined by the CAM and cannot change the definition of the CA. The CAO is responsible for operating the CA's trustworthy systems on a day-to-day basis and is authorized to perform system backup and recovery.

Registration Authority Operators (RAO) can manage a subset of certificates and requests as described by the RA policies and the operator access rules. The RAO works with the RA as defined by the CAM and cannot change the definition of the RA. The RAO is responsible for operating the RA's trustworthy systems on a day-to-day basis and is authorized to perform system backup and recovery.

c) Audit

Auditors have read-only access to all components of the TERACARA CA to verify that the operation of these components complies with the rules and regulations of this CP/CPS. The TERACARA PKI system automatically notifies the auditor of all issues. The auditor is authorized to view and maintain archives and audit logs of all of the CA's trustworthy systems. The auditor has no direct operative abilities, but MUST inform WPIA executive management, after the fact, of any irregularities in the processes.

5.2.2 Number of persons required per task

The operation of the TERACARA CA and all its subsidiaries is entirely role-driven and therefore requires at least:

- Access: 2 employees for network access configuration and CA maintenance and management tasks
- Operations: 2 employees for system administration, RA and CA operation
- Audit: 1 auditor

The certificate store and all cryptographically relevant aspects of the CA (signing operations) can only be accessed by two persons working together (four-eye-principle).

5.2.3 Identification and authentication for each role

Identification and authentication for all roles is achieved using TERACARA certificates or SSH keys. Access to data facilities (including bank safe deposit box) requires requires national passport/ID card and/or biometric identification.

5.2.4 Roles requiring separation of duties

To guarantee a strict segregation of duties as described in section 5.2.1, roles related to access, operations, and audit MUST be held by separate individuals.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

WPIA has very high standards with regards to the skills of staff members.

To be assigned the role "Access", a staff member MUST prove that they have expert knowledge of TCP/IP networking, Unix operating systems, and PKI technology, concepts and applications.

To be assigned the role "Operations", a staff member MUST prove that they have expert knowledge of PKI technology and applications that use PKI. Also, they MUST have strong people skills and a good understanding of PKI processes.

To be assigned the role "Audit", a staff member MUST prove that they have expert knowledge of TCP/IP networking, Unix operating systems, PKI technology and applications using PKI, as well as a good understanding of PKI processes and strong people skills.

All TERACARA staff members MUST demonstrate understanding of security in general and expert knowledge of IT security in particular. TERACARA personnel SHALL be formally appointed to trusted roles by senior management members responsible for security.

Before starting work at WPIA, new staff members MUST sign confidentiality (non-disclosure) agreements and independence statements.

5.3.2 Background check procedures

WPIA verifies the background of its staff members and ensures that employees do not have a criminal record.

WPIA will not appoint any person who is known to have been convicted of a a serious crime or other offense which could effect his suitability for the position. Personnel SHALL not have access to the trusted functions until all necessary checks have been completed. WPIA will ask any candidate to provide such information and refuse an application if access to such information is denied.

5.3.3 Training requirements

Employees of WPIA MUST provide evidence that they have obtained the skills required for their position. Shortcomings will be addressed and alleviated by appropriate training.

During the year, there will be at least one meeting with the Chief Security Officer, the Human Resource Officer, and staff. The meeting will be similar in structure to the one on the first working day. Topics to be covered are information-security issues and the roles of staff members.

5.3.4 Retraining frequency and requirements

Retraining of staff members is done as necessity arises, depending on the needs of the organisation or the needs of the individual.

5.3.5 Job rotation frequency and sequence

Job rotation of staff members is done as necessity arises, depending on the needs of the organisation, or by request of an individual staff member.

5.3.6 Sanctions for unauthorized actions

WPIA reserves the right to prosecute unauthorized actions to the fullest extent of applicable Austrian law.

5.3.7 Independent contractor requirements

Above and beyond regular documentation, contractors that are candidates for an Access, Operations or Audit role MUST:

- provide proof of their qualifications in the same manner as internal personnel (see chapter 5.3.1),
- demonstrate a clean criminal record,
- sign a separate confidentiality statement (non-disclosure agreement) in addition to the confidentiality agreement covering the contractual relations with third-party contractors.

5.3.8 Documentation supplied to personnel

On their first day of work, all WPIA staff members receive a staff member handbook and access to the WPIA security policy, security concept, personal workspace security, and risk management documentation. Every staff member is expected to read and understand all of this documentation during the first week of engagement with WPIA.

5.4 Audit logging procedures

The TERACARA CA software is built to journal all events that occur in the TERACARA CA. The journal is stored in the TERACARA CA database and is accessible through the TERACARA CA Web Interface.

5.4.1 Types of events recorded

The following events are recorded in the CA log:

- new certificate requests
- rejected certificate requests
- account violations
- certificate signing
- certificate revocation
- user account changes
- CRL signing
- CA rollover

The above list is non-conclusive, and it is limited to events that are directly related to certificate management or trust-related functions. In particular, it does not include technical events that are logged elsewhere.

5.4.2 Frequency of processing log

Logs are processed continuously and audited on a monthly basis by the Chief Security Officer (CSO). The audit report covers the following aspects:

- list of the audit accomplished with the results of the review of each individual item,
- list of open audit issues including status, escalation, deadline, responsible person/organisation,
- prioritized list of actions to be taken.

5.4.3 Retention period for audit log

The journal information in the TERACARA CA database is kept for the period defined in 5.5.2.

5.4.4 Protection of audit log

Read access to the journal information is granted to personnel requiring this access as part of their duties. The following roles can obtain this access:

- Auditor
- RAO
- CAO
- CAM

The journal is stored in the database and access to the database is protected against unauthorised access by the CA application and through special security measures on the operating system level.

5.4.5 Audit log backup procedures

The journal is an integral part of the WPIA database and is therefore part of the daily backup. The entire database is encrypted on the disk as well as on the backup media. Only staff member with the role OPS have access to the backup media.

5.4.6 Audit collection system (internal vs. external)

The audit log or journal is an integral part of the TERACARA CA software.

5.4.7 Notification to event-causing subject

Depending on the severity of the log entry, WPIA reserves the right to notify the subscriber of the event, the log entry and/or the results of the event.

5.4.8 Vulnerability assessments

This CA and all its subsidiaries are constantly (24x7) monitored, and all attempts to gain unauthorised access to any of the services are logged and analyzed. WPIA reserves the right to inform the Austrian authorities of such successful or unsuccessful attempts.

5.5 Records archival

5.5.1 Types of records archived

The following records are archived:

- a daily backup of any information that this CA and its subsidiaries produce
- registration information of end entities

5.5.2 Retention period for archive

Archived information is kept at least 11 years beyond the end of subscription, as specified in chapter 4.11.

5.5.3 Protection of archive

Protection of the archive is as follows:

- Archived information is only accessible to authorized TERACARA employees according to the role model as presented in 5.2.
- Protection against modification: Archives of digital data are digitally signed to prevent unknown modification.
- ???? Protection against deletion: The RA archive (physical documents) is stored in a safe deposit box of a major TBD bank and can only be accessed by authorised WPIA staff members as detailed in the role model presented in 5.2.
- Protection against the deterioration of the media on which the archive is stored: Digital data is to be migrated periodically to fresh media.
- Protection against obsolescence of hardware, operating systems, and other software: As part of the archive, the hardware (if necessary), operating systems, and/or other software is archived in order to permit access to and use of archived records over time.

5.5.4 Archive backup procedures

Archived information is stored off-site in safe deposit boxes at a major TBD bank.

5.5.5 Requirements for time-stamping of records

All records in the database and in log files are time-stamped using the system time of the system where the event is recorded.

The system time of all servers is synchronized with the time source of the TBD Time-Stamping Authority.

5.5.6 Archive collection system (internal or external)

This CA and all its subsidiaries use a TERACARA-internal archiving system.

5.5.7 Procedures to obtain and verify archived information

In the event of a court order, a high-quality copy is made of the archived information and the original is temporarily made available to the court. When the original information is returned, the high-quality copy is destroyed. This process is logged and audited.

5.6 Key changeover

WPIA MAY change over all keys of intermediate CAs on a regular basis. All certificates of such intermediate CAs are available for download on the teracara.org website and in the public directory ??????. These CA certificates are directly signed by the long-living trust anchors of the TERACARA PKI.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

To manage all operational processes, WPIA has adopted the ITIL best practices model:

- A service desk receives all incoming service calls and assesses them according to severity.
- Incident management has the goal to restore normal operation as quickly as possible.
- Recurring incidents or incidents with major impact are entered into the problem management process. The goal here is to find the ultimate cause of the problem and to prevent further issues.

To manage a crisis or catastrophe, WPIA has a Business Continuity Management plan. Once this plan goes into action, the Task Force Business Continuity (TFBC) assumes managerial duties of WPIA until the crisis is dealt with and the TFBC is disbanded.

The TFBC has a charted course of action for the following events:

- Loss of one computing facility
- System or server compromise
- CA key compromise
- Algorithm compromise

If a crisis or catastrophe situation is declared, WPIA will communicate this state to the Board of WPIA, the Austrian authorities and the Austrian Recognition Body.

5.7.2 Computing resources, software and/or data are corrupted

This CA and its subsidiaries are implemented on fully redundant server systems. Any hardware defect will only affect one such system and allow a redundant system to take over and provide full functionality.

The master server of this CA and its subsidiaries is part of a daily backup process.

5.7.3 Entity private key compromise procedures

If the private key of the 'TERACARA CA' or one of its subsidiaries is suspected to be compromised, executive management of WPIA MUST be informed immediately. The following steps will be taken:

- The CA certificate will be revoked.
- WPIA will inform Austrian authorities of any trust-anchor compromise.
- All subscribers with certificates issued by either the revoked CA or one of its subsidiaries will be informed by email as soon as possible.
- All subscriber certificates will be revoked and new CRLs will be issued.
- The cause of the key compromise will be determined and the situation rectified.
- The revoked CA will generate a new key pair and the resulting certificate request will be signed by the superior CA.

- The new CA certificate will be published on the teracara.org web site.
- New CRLs will be issued.

5.7.4 Business continuity capabilities after a disaster

In case of a disaster, Executive Management and the Board of WPIA will assess the situation and take all decisions necessary to establish a new, fully redundant server location for the TERACARA CA servers.

A new server location will be chosen based on its ability to support the security requirements of WPIA with reference to the requirements as stipulated in this document. The off-site backups will be used to restore the CA, its data and its processes.

5.8 CA or RA termination

Before the WPIA CSP terminates its services, the following actions will be executed:

- TERACARA will report, without delay, any threat of bankruptcy to the Austrian Telekom Control Commision, the Austrian Recognition Body and any other governmental control agency or legal quality control organisation.
- When the decision to discontinue certification services has been taken, WPIA will inform, without delay, all its subscribers, relying parties and if applicable to other registration authorities and other CAs with which there are agreements or any other form of established relations. WPIA endeavors to give at least 30 days advance notice before revoking any certificates. This explicitly includes the Austraian Telekom Control Commision, the Austrian Recognition Body and any other governmental control agency or legal quality control organization.
- WPIA will immediately stop all registration services and if applicable will enforce this cessation of services for all other registration authorities.
- WPIA will immediately cancel all current and valid contracts. The cancellation is to be effective after the entire business termination process has been concluded. WPIA will also immediately revoke all rights of contracted parties to act on behalf of WPIA.

After a waiting period of at least 30 days, the following actions will be executed:

- WPIA will revoke all subscriber certificates. WPIA will issue a CRL. WPIA will revoke all root certificates.

- WPIA will transfer obligations for maintaining registration information, certificate status information, and event log archives that cover the respective time to the appropriate organization.
- WPIA will destroy all backup copies and escrow copies of the private signing keys of the “TERACARA Unverified Intermediate CA”, the “TERACARA Verified Intermediate CA”, the “TERACARA Codesign Intermediate CA” , the “TERACARA Orga Intermediate”, the “TERACARA OrgaSign Intermediate CA” and “TERACARA EV Intermediate CA” such that the private keys cannot be retrieved, retained, or put back into use.
- All copies of documents which are required to be saved according to the stipulations of any applicable law will be stored under the conditions and for the duration as stipulated in this TERACARA CP/CPS.

6 Technical Security Controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

The key pair for the TERACARA CA (Root CA Key) MUST be created in an off line SSCD that meets at least FIPS 140-2 level 3 requirements. The key pairs for the subsidiaries of the TERACRA CA (Issuing CA Keys) MUST be generated in an offline SSCD that meets at least FIPS 140-2 level 3 requirements. Subsequently, the Issuing CA keys MUST be cloned into an online SSCD meeting at least FIPS 140-2 level 4 requirements.

TSA key pairs are generated and managed in the same SSCD as the Issuing CA keys. The same rules apply.

6.1.2 Private key delivery to subscriber

Subscribers of the TERACARA RA have no choice, where the keys will be generated. TERACARA generates the keys on the TERACARA website.

Private keys are not generated by TERACARA.

6.1.3 Public key delivery to certificate issuer

The requester presents the public key as a PKCS#10-formatted certificate signing request to the signing CA using a secure SSL-encrypted communication channel.

If keys are generated online, no public key delivery method is required.

6.1.4 CA public key delivery to relying parties

Relying parties can download the issuing CA certificate from the TERACARA website by using the PKCS#7 format.

When a subscriber receives the certificate, the issuing CA public key is included. Also included is the complete chain of certificates of the hierarchical TERACARA PKI containing all public keys that are part of the trust chain.

6.1.5 Key sizes

TERACARA follows the recommendations on algorithms and key sizes as they are made available by the following institutions:

NIST: SP 800-57, http://csrc.nist.gov

Bundesnetzagentur: Übersicht über geeignete Algorithmen, http://www.bundesnetzagentur.de

TERACARA allows subscribers to use RSA keys with a size of at least 2048 bits, if the recommendations require 4096 bit key sizes.

For CA certificates TERACARA will use the following key sizes:

- The 'TERACARA CA' uses a 4096 bit RSA key.
- All issuing CAs use 4096 bit RSA key.

6.1.6 Public key parameters generation and quality checking

Parameters MAY be selected by requesters, but are verified by the RA and the CA.

For keys generated online, all TERACARA CAs use standard parameters.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

The signing key of this CA and its subsidiaries are the only keys permitted for signing certificates and CRLs and have the keyCertSign and CRLSign key usage bit set.

Parameters MAY be selected by requesters, but are verified by the RA and the CA.

- digitalSignature
- nonRepudiation

- keyAgreement
- keyEncipherment
- DataEncipherment

Subscribers MAY obtain certificates issued by this CA with the following extended key usages included:

- Server Authentication
- Client Authentication
- Code Signing
- Email Protection

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The following list shows how the requirements for the different users of SSCD are implemented:

Root CA keys: The SSCD used for CA keys MUST be kept offline at all times and MUST meet at least FIPS 140-2 level 3 requirements.

Issuing CA keys: The SSCD used for CA keys MUST meet at least FIPS 140-2 level 3 requirements. These keys are online and access MUST be controlled by using the '4-eye' principle.

Subscriber keys: The subscriber is fully responsible for the evaluation, implementation and protection of the cryptographic module, where the subscriber keys are generated and stored. TERACARA RECOMMENDS that the subscriber uses a SSCD.

6.2.2 Private key (n out of m) multi-person control

The following list shows how multi-person controls are implemented:

Root CA keys: Root CA keys MUST be accessed on the physical and on the logical level by adhering to '3 out of 5' control, meaning that 3 of the 5 persons are present.

Issuing CA keys: Management access to these keys MUST be only possible using '4-eyes' principle (2 out of m). Once the issuing CA is operable, signing operations can be authorized by a single RA operator.

Subscriber keys: The subscriber has single-person control of the subscriber keys.

6.2.3 Private key escrow

The following list shows how private key escrow is implemented:

Root CA keys: Root CA keys are not in escrow.

Issuing CA keys: The issuing CA keys are not in escrow.

Subscriber keys: Private key escrow is not offered by the TERACARA CA.

6.2.4 Private key backup

The following list shows how private key backup is implemented:

Root CA keys: Root CA keys MUST be backed up onto an SSCD so that they MAY be recovered if a major catastrophe destroys the productive set of keys. The recovery requires that 3 out of 5 persons be present in order to gain physical and logical access. At least one of these persons MUST be a member of the Board of WPIA.

Issuing CA keys: The Issuing CA keys MUST be put into backup SSCD, so that they MAY be recovered if a major catastrophe destroys the productive set of keys. The recovery requires that 3 out of 5 persons MUST be present in order to gain physical and logical access.

Subscriber keys: Private key backup is not offered by the TERACARA CA.

6.2.5 Private key archival

The following list shows how private key archival is implemented:

Root CA keys: The Root CA keys are not archived.

Issuing CA key: The Issuing CA keys are not archived.

Subscriber keys: Private key archival is not offered by the TERACARA CA.

6.2.6 Private key transfer into or from a cryptographic module

The following list shows how private key transfers are implemented:

Root CA keys: The Root CA keys MAY be cloned from the master SSCD to other SSCDs. This is achieved in a cloning ceremony. To protect the private key during the transport, the destination SSCD provides the public key of a key pair it has generated. The master SSCD encrypts the key to be cloned with this public key. Only the destination SSCD is therefore able to successfully decrypt the key pair from the master SSCD.

Issuing CA keys: The Issuing CA keys MAY be cloned in the same manner as Root keys.

Subscriber keys: Private key transfer is not available through TERACARA CA.

The controls on these processes are explained in chapter 6.2.4, Private Key Backup.

6.2.7 Private key storage on cryptographic module

Root CA keys: The Root CA keys MUST be stored on cryptographic modules so that they MAY be used only if properly activated.

Issuing CA keys: The Issuing CA keys MUST be stored on cryptographic modules so that they MAY be used only if properly activated.

Subscriber keys: Private key storage is not available through TERACARA CA.

6.2.8 Method of activating private key

The following list shows how private keys are activated:

Root CA keys: The Root CA keys MUST be activated with a user key (physical), a user pin (knowledge) and 3 authentication keys (physical).

Issuing CA keys: The Issuing CA keys MUST be activated with role-based access control requiring at least two persons and a SSCD PIN.

Subscriber keys: The subscriber of the TERACARA CA is solely responsible for the method of activating private keys.

6.2.9 Method of deactivating private key

The following list shows how private keys are deactivated:

Root CA keys: The Root CA keys MAY be deactivated either by logging out of the SSCD, by terminating the session with the SSCD, by removing the CA token from the computer or by powering down the system.

Issuing CA keys: The Issuing CA keys MAY be deactivated by terminating the key daemon process, by shutting down the CA server processes or by shutting down the server.

Subscriber keys: The subscriber is solely responsible for the deactivation of private key.

6.2.10 Method of destroying private key

The following list shows how private keys are destroyed:

Root CA keys: The Root CA keys MUST be destroyed by initializing the SSCD.

Issuing CA keys: The Issuing CA keys MUST be destroyed by initializing the SSCD.

Subscriber keys: The subscriber is solely responsible for the destroying of their subscriber keys.

6.2.11 Cryptographic Module Rating

Minimum standards for cryptographic modules have been specified in chapter 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

All certificates, and therefore the public keys of all subscribers and all CAs, MUST be stored online in a database. This database MUST be replicated to all servers in the CA cluster. This database is also part of the daily backup. To protect the data in the database, the database MUST be encrypted with a special backup key before it is put into the backup.

The encrypted daily backup MUST be copied onto a backup server and kept available online for one year.

6.3.2 Certificate operational periods and key pair usage periods

The usage periods for certificates issued by this CA are as follows:

- The 'TERACARA CA' as well as all trust-anchor certificates are valid approximately 30 years. Key changeover SHALL be performed every 15 years.
- Intermediate CA certificates SHALL be issued for a maximum life time of 15 years.
- Issuing CA certificates are issued for a maximum life time of 2.5 years.
- The Rollover of CA certificates SHALL be done manually after at most two thirds of the life time of the certificate.
- Enduser certificates MAY have a lifetime of up to the maximum remaining lifetime of the issuing CA certificate minus 5 days.
- For EV certificates the life time SHALL not exceed 24 months as specified in the EV Guidelines.

6.4 Activation data

6.4.1 Activation data generation and installation

The subscriber of the TERACARA CA is solely responsible to generate and install activation data.

6.4.2 Activation data protection

Root CA keys: The activation data MUST be distributed over multiple physical keys. The owners of a part MUST store this part in a private safe deposit of a TBD.

Issuing CA keys: The activation data MUST be known to trusted individuals at WPIA. An escrow copy MUST be stored in a safe deposit with dual controls access.

Subscribers keys: Subscribers MUST keep the activation data secret at all times.

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer security controls

The CA servers are protected by external firewalls that filter out all unwanted traffic. Additionally, the CA systems are hardened and equipped with a high-security operating system. SA access to the system is granted only over secure and restricted protocols using strong public-key authentication.

6.5.1 Specific computer security technical requirements

TERACARA uses a layered security approach to ensure the security and integrity of the computers used to run the TERACARA CA software.

The following controls ensure the security of WPIA-operated computer systems:

- Hardened operating system.
- Software packages are only installed from a trusted software repository.
- Minimal network connectivity.
- Authentication and authorization for all functions.
- Strong authentication and role-based access control for all vital functions.

- Disk and file encryption for all relevant data.
- Proactive patch management.
- Monitoring and auditing of all activities.

6.5.2 Computer security rating

WPIA has established a security framework which covers and governs the technical aspects of its computer security. The systems themselves and the services running on these systems are subject to thorough reviews and testing (including penetration testing). In order to make its environment more secure and to keep it on a state-of-the-art security level, WPIA operates a vulnerability management process which includes monitoring of supplier security alerts.

The technical aspects of computer security are subject to periodic audits under supervision of the Chief Security Officer (CSO).

6.6 Life cycle technical controls

6.6.1 System development controls

To ensure quality and availability of the WPIA software, WPIA implements the ITIL model and the development team adheres to the following principles:

- All software MUST be stored in the Source Code Control System to keep track of software versions.
- The software archive MUST be put onto backup regularly, and a copy MUST be stored externally.
- A Software Life Cycle Control based on separate environments for Development, Test and Production MUST be in place. This software life cycle control MUST ensure adherence to controls and checkpoints within the organisation.
- Internal software development policies MUST specify standards and principles for software engineering and related tasks.

6.6.2 Security management controls

Continuous monitoring MUST be used to ensure that systems and networks are operated in compliance with the specified security policy. All processes MUST be logged and audited according to applicable law and normative requirements.

6.6.3 Life cycle security controls

Development of software systems adheres to principles specified in the internal software development policies. These policies are part of a security management process covering life cycle aspects of security controls.

6.7 Network security controls

Network security MUST be based on a multi-level zoning concept using multiple redundant firewalls.

7 Certificate, CRL and OCSP Profiles

This section contains the rules and guidelines followed by this CA and all its subsidiaries in populating X.509 certificates and CRL extensions.

7.1 Certificate profile

The subsidiaries of this CA issue X.509 Version 3 certificates in accordance with PKIX. The structure of such a certificate is:

Certificate Field	Value	Comment
Version	X.509 Version 3	See Chapter 7.1.1
Serial number	Unique number	Will be used in CRL
Signature algorithm identifier	OID	See Chapter 7.1.3
Validity period	Start date, Expiration date	
Subject	According to X.500	See Definitions in Chapter 1.6
Subject Public Key Info	Public Key algorithm. Subject Public Key	See Chapter 7.1.3
Extensions	X509V3 Extensions	See Chapter 7.1.2
Signature	Certificate Signature	

For EV certificates the following fields MUST be included in the subject:

- Common Name (FQDN): /CN
- Organization: /O
- Locality: /L

- State or Province: /ST
- Country: /C

7.1.1 Version number(s)

Version of X.509 certificates: version 3.

7.1.2 Certificate Extensions

The Authority information Access extension is optional and it is derived from the issuing CA as follows:

- CA Issuers: URI: http://g2.crt.teracara.org/g2//
- OCSP: URI: http://g2.teracara.org

The Subject Alternative Name extension is optional. It is added in accordance with rfc 5280 and the content depends on the information provided by the subscriber.

TERACARA CA Certificates for Generation 2 (G2)

The generation 2 certificates of TERACARA are characterized by a self-signed root certificate with the SHA-2 hash algorithm.

Subject of the TERACARA CA certificates for Generation 2

CA Type	Subject	Issuer
Root CA	/CN=TERACARA CA Root Certificate /O=TERACARA /C=AT	/CN=TERACARA CA Root Certificate /O=TERACARA /C=AT
TERACARA Intermediate CA	/CN=TERACARA Intermediate CA /O=TERACARA /C=AT	/CN=TERACARA CA Root Certificate /O=TERACARA /C=AT
Issuing CA	/CN= -<1/2> /O=TERACARA /C=AT	/CN=TERACARA Intermediate CA /O=TERACARA /C=AT

key:

- Unverified
- Verified

- Codesign
- Orga
- OrgaSign
- EV

Common extensions of the TERACARA CA certificates for Generation 2

Extension	Root CA	Issuing CA	Critical
basic Constraints	CA: TRUE	CA:TRUE, pathlen: 0	Y
key Usage	Certificate Sign, CRL Sign	Certificate Sign, CRL Sign	Y
Subject Key Identifier		individual per CA	
Authority Key Identifier			
Certificate Policies	Policy: 47934.6.1.2.1.01 CPS: http://policy.wpia.club/	Policy: 47934.6.1.2.1.01 CPS: http://policy.wpia.club/	
CRL Distribution Points	not included in Root CA certificate	http://g2.crl.teracara.org/g2//	

Extension of the Root Certificate: TERACARA CA – G2

no exceptions

Extensions of the Issuing CA: TERACARA XXXX – G2

no exceptions

TERACARA Special Certificates for Generation 2 (G2)

Code-signing certificate issued by: TERACARA Codessign/Orgasign XXX – G2

Extension Attribute	Values	Comment
Subject	Data of Subscriber	See Definitions in Chapter 1.6
Issuer Name	/CN= -<1/2> /O=TERACARA /C=AT	

Extension Attribute	Values	Comment
Authority Key Identifier		See Chapter 7.1.3
CRL Distribution Points	http://g2.crl.interimca-tc.xyz/g2.crl	URLs of the CRL Distribution points (LDAP and/or HTTP)
Certificate Policies	Policy: 47934.6.1.2.1.01 CPS: http://policy.wpia.club/	
Authority Information Access		URL to OCSP responder and optional URL to CA issuer certificate
Subject Alternative Name		Alternative name of the subscriber: email address
Key Usage	digitalSignature	Critical extension
Extended Key Usage	CodeSigning	
NsComment		Optional

key:

- Codesign
- OrgaSign

7.1.3 Algorithm object identifiers

The algorithms with OIDs supported by this CA and its subsidiaries are:

Algorithm	Object Identifier
SHA2withRSAEncryption	1.2.840.113549.1.1.13
rsaEncryption	1.2.840.113549.1.1.1

7.1.4 Name forms

Certificates issued by the subsidiaries of this CA contain the full X.500 distinguished name of the certificate issuer and certificate subject in the issuer name and subject name fields. Distinguished names MUST be in the form of a X.501 printable string.

7.1.5 Name constraints

Not implemented.

7.1.6 Certificate policy object identifier

Each certificate MUST reference a policy OID, and MAY contain several as long as none of the policy constraints conflict.

For information see chapter 7.1.2 of this document.

7.1.7 Usage of Policy Constraints extension

Not implemented.

7.1.8 Policy qualifiers syntax and semantics

The subsidiaries of this CA do not currently issue certificates with policy qualifiers.

7.1.9 Processing semantics for the critical Certificate Policies extension

PKI client applications MUST process extensions marked as critical.

7.2 CRL profile

This CA and its subsidiaries issue X.509 Version 2 CRLs in accordance with IETF PKIX RFC 5280.

7.2.1 Version number(s)

The CRL version is v2.

7.2.2 CRL and CRL entry extensions

Version 2 CRL and CRL extensions and their current status are specified below:

- CRLNumber: Populated by the CA application
- reasonCode: not populated
- authorityKeyIdentifier: Populated by CA application contains key id (SHA256) of issuer public key

7.3 OCSP profile

The TERACARA OCSP functionality is built according to IETF OCSP RFC 2560.

7.3.1 Version number(s)

The OCSP version is set to v1.

7.3.2 OCSP extensions

The OCSP extensions used are specified below:

- Nonce
- ServiceLocator

8 Compliance Audit and Other Assessments

The terms and conditions of this CP/CPS and all dependent rules and regulations SHALL be used to conduct compliance audits for: * The TERACARA CA and its subsidiaries * The TERACARA RA

8.1 Frequency or circumstances of assessment

The compliance audit SHALL be conducted annually.

More than one compliance audit per year MAY be possible if this is requested by the audited party or is a result of unsatisfactory results of a previous audit.

8.2 Identity/qualifications of assessor

The Chief Security Officer (CSO) of WPIA is the auditor chosen by WPIA.

SHOULD the CSO desire to outsource all or part of the execution of the audit, they MAY do so if the following conditions are met:

- The outsourcing partner MUST have a reputation in the market for conducting security related audits.
- The chosen auditor MUST be acceptable to the auditee.

8.3 Assessor's relationship to assessed entity

The assessed entity (WPIA) generates objective evidences that are presented to the assessor (CSO) for annual assessment.

8.4 Topics covered by assessment

The CSO will choose the control objectives that MUST be covered by the assessments in accordance with this CP/CPS.

8.5 Actions taken as a result of deficiency

WPIA implements the ITIL best practices model and the results of a compliance audit SHALL be handled within this framework. Depending on severity and urgency, all issues SHALL be entered into the ITIL system either as incidents or as problems and tracked accordingly. Through the use of a supporting tool, WPIA ensures that all issues MUST be tracked and resolved in due course. Management reporting and escalation SHALL be part of the system.

8.6 Communication of results

The results of the compliance audit SHALL be communicated to WPIA executive management in a timely manner.

9 Other Business and Legal Matters

9.1 Fees

WPIA provides a price list for certification and registration services on the website teracara.org.

9.2 Certificate issuance or renewal fees

WPIA MAY charge fees for issuing certificates according to the respective price list published on their website or made available upon request.

9.2.1 Certificate access fees

WPIA MAY charge a fee according to their pricing policy.

9.2.2 Revocation or status information access fees

There is no charge for certificate revocation and the provision of certificate status information.

9.2.3 Fees for other services

WPIA MAY reserve the right to charge an hourly rate or a fee, depending on the services rendered, additional to the fees mentioned above.

9.2.4 Refund Policy

WPIA MAY establish a refund policy.

9.3 Financial responsibility

9.3.1 Insurance coverage

TBD

9.3.2 Other assets

Not applicable.

9.3.3 Insurance or warranty coverage for end-entities

It is in the sole responsibility of subscribers and relying parties to ensure an adequate insurance, to cover risks using the certificate or rendering respective services, according to Austrian Digital Signature Law. Upon request, WPIA will give advice about adequate insurances to cover potential risks.

9.4 Confidentiality of business information

9.4.1 Scope of confidential information

Any information or data WPIA obtains in the course of business transactions SHALL be considered confidential, except for information defined in chapter 9.3.2. This includes, but is not limited to business plans, sales information, trade secrets, organisational names, registration information, and subscriber data.

9.4.2 Information not within the scope of confidential information

Any information that is already publicly available SHALL not be considered confidential, nor SHALL be any information considered confidential which WPIA is explicitly authorized to disclose (e.g. by written consent of involved party, by law or because it is part of the publicly available certificate information).

9.4.3 Responsibility to protect confidential information

WPIA is responsible to take all required measures to comply with the Austrian Data Protection Law and any other relevant regulations.

9.5 Privacy of personal information

WPIA fully complies with the Austrian Data Protection and other applicable legislation. Information and data MAY be used where needed for professional handling of the services provided herein. Subscribers and other third parties MUST comply with the privacy standards of WPIA.

9.5.1 Privacy Plan

WPIA SHALL have a non disclosure agreement (NDA) which SHALL be a contractual obligation and SHALL be signed between WPIA and participants. Further, all stipulations of 9.3.1 SHALL apply.

9.5.2 Information treated as private

Any information about subscribers and requesters that is not made public through the certificates issued by this CA, the CRL, or the LDAP directory's content MUST be considered private information.

9.5.3 Information not deemed private

Any and all information made public in a certificate issued by this CA, or its CRL, or by a publicly available service SHALL not be considered confidential.

9.5.4 Responsibility to protect private information

Participants that receive private information MUST secure it from compromise, and refrain from using it or disclosing it to third parties.

9.5.5 Notice and consent to use private information

WPIA MAY only use private information if a subscriber has given full consent in the course of the registration process.

9.5.6 Disclosure pursuant to judicial or administrative process

WPIA MAY release or disclose private information only on judicial or other authoritative order, and MUST inform the subscriber about the incident.

9.5.7 Other information disclosure circumstances

WPIA MAY solely disclose information protected by the Austrian Data Protection on judicial or other authoritative order, and MUST inform the subscriber about the incident.

9.6 Intellectual property rights

All WPIA intellectual property rights including all trademarks and copyrights of all WPIA documents MUST remain the sole property of WPIA.

Certain third party software SHALL be used by WPIA in accordance with applicable license provisions.

9.7 Representations and warranties

9.7.1 representations and warranties

WPIA warrants full compliance with all provisions stated in this CP/CPS. For EV certificates WPIA fully complies with the stipulations regarding EV Certificate Warranties as presented in the EV guidelines.

9.7.2 RA representations and warranties

TERACARA RA warrants full compliance with all provisions stated in this CP/CPS, related agreements and documents.

9.7.3 Subscriber representations and warranties

Subscribers warrant full compliance with all provisions stated in this CP/CPS and other related agreements and documentation.

9.7.4 Relying party representations and warranties

Relying parties warrant full compliance with the provisions of this CP/CPS and related agreements.

9.7.5 Representations and warranties of other participants

Any other participant warrants full compliance with the provisions set forth in this CP/CPS and related agreements.

9.8 Disclaimers of warranties

Except for the warranties stated herein including related agreements and to the extent permitted by applicable law, WPIA disclaims any and all other possible warranties, conditions, or representations (express, implied, oral or written), including any warranty of merchantability or fitness for a particular use.

9.9 Liability

9.9.1 Liability of WPIA

WPIA SHALL only be liable for damages which are the result of WPIA's failure to comply with this CP/CPS and which were provoked deliberately or wantonly negligent.

WPIA SHALL NOT in any event be liable for any loss of profits, indirect and consequential damages, or loss of data, to the extent permitted by applicable law. WPIA SHALL NOT be liable for any damages resulting from infringements by the Certificate Holder or the Relying Party on the applicable terms and conditions.

WPIA SHALL NOT in any event be liable for damages that result from force majeure events as detailed in chapter 9.16.4. WPIA SHALL take commercially reasonable measures to mitigate the effects of force majeure in due time. Any damages resulting of any delay caused by force majeure will not be covered by WPIA.

9.9.2 Liability of the Certificate Holder

The Certificate Holder SHALL be liable to WPIA and Relying Parties for any damages resulting from misuse, willful misconduct, failure to meet regulatory obligations, or noncompliance with other provisions for using the certificate.

9.10 Indemnities

Indemnities are already defined in the provisions stated in this CP/CPS and other related documents.

9.11 Term and termination

9.11.1 Term

This Certificate Policy and Certification Practice Statement and respective amendments become effective as they are published on the WPIA website at http://policy.wpia.club/.

9.11.2 Termination

This CP/CPS will cease to have effect when a new version is published on the WPIA website.

9.11.3 Effect of termination and survival

After termination, the certificate MAY no longer be used. However, all provisions regarding confidentiality of personal and other data will continue to apply without restriction after termination. Also, the termination SHALL NOT affect any rights of action or remedy that MAY have accrued to any of the parties up to and including the date of termination.

9.12 Individual notices and communications with participants

WPIA MAY provide notices by email, postal mail or on web pages unless specified otherwise in this CP/CPS.

9.13 Amendments

9.13.1 Procedure for amendment

WPIA MAY implement changes with little or no impact for subscribers and relying parties to this Certificate Policy & Certificate Practice Statement upon the approval of the executive board of WPIA.

Updated CP/CPS become final and effective by publication on the WPIA website and will supersede all prior versions of this CP/CPS.

9.13.2 Notification mechanism and period

The WPIA executive board MAY decide to amend this CP/CPS without notification for amendments that are non-material (with little or no impact). The WPIA executive board, at its sole discretion, decides whether amendments have any impact on the subscriber and/or relying parties.

All changes to the CP/CPS SHALL be published according to chapter 2 of this CP/CPS. Material changes for the subscriber SHALL be sent to the respective parties via email 30 days before the changes become effective.

9.13.3 Circumstances under which OID MUST be changed

Changes of this CP/CPS that do affect subscribers and/or relying parties MUST NOT change the OID of this CP/CPS.

9.14 Dispute resolution provisions

In case of any dispute or controversy in connection with the performance, execution or interpretation of this agreement, the parties will endeavor to reach amicable settlement.

9.15 Governing law and place of jurisdiction

The laws of Austria and the European Union SHALL govern the validity, interpretation and enforcement of this contract, without regard to its conflicts of law. The application of the United Nations Convention on Contracts for International Sale of Goods SHALL be excluded. Exclusive place of jurisdiction SHALL be the commercial court of Graz (Handelsgericht Graz), Austria.

9.16 Compliance with applicable law

This Certificate Policy & Certification Practice Statement and rights or obligations related here to are in accordance with Austrian and European Union Law.

9.17 Miscellaneous provisions

9.17.1 Entire agreement

This CP/CPS MAY not be the only document which comprises the agreement between the parties involved. Any other agreements MAY further restrict this

CP/CPS, but no document or agreement SHALL lessen the rules and stipulations of this CP/CPS. Any document which serves as an annex to this CP/CPS MUST be made available to all parties involved. The relationship between the documents MUST be documented and communicated.

9.17.2 Assignment

The Certificate Holder SHALL NOT assign this agreement or its rights or obligations arising hereunder, in whole or in part.

WPIA MAY fully or partially assign this agreement and/or its rights or obligations hereunder.

9.17.3 Severability Clause

Invalidity or non-enforceability of one or more provisions of this agreement and its related documents SHALL not affect any other provision of this agreement, provided that only non-material provisions are severed.

9.17.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable.

9.17.5 Force Majeure

WPIA SHALL NOT be in default and the customer cannot hold WPIA responsible and/or liable for any damages that result from (but are not limited to) the following type of events: any delay, breach of warranty, or cessation in performance caused by any natural disaster, power or telecommunication outage, fire, unpreventable third-party interactions such as virus or hacker attacks, governmental actions, or labor strikes.

WPIA SHALL take commercially reasonable measures to mitigate the effects of force majeur in due time.

9.18 Other provisions

9.18.1 Language

If legal documents like the CP/CPS, the End-User-Agreement, or registration forms are provided in additional languages to English, the English version of these documents SHALL prevail.