

***VALID ROOT CERTIFICATE AUTHORITY
CERTIFICATION PRACTICE STATEMENT***

***OID: 1.3.6.1.4.1.47402.2.1
Version 1.1 – 05/18/2018***

DOCUMENT HISTORY:

<i>Version</i>	<i>Release Date</i>	<i>Author(s)</i>	<i>Description</i>
v1.0	11/10/2017	Lucas Carvalho	VALID ROOT CERTIFICATE AUTHORITY creation.
v1.1	05/18/2018	Ana Carolina Volpe	Inclusion of Information Classification.

APPROVED BY:

SUMMARY

- 1. INTRODUCTION 9
 - 1.1 Overview 9
 - 1.2 Document Name and Identification 9
 - 1.3 PKI Participants 9
 - 1.4 Certificate Usage 9
 - 1.5 Policy Administration 10
 - 1.5.1 Organization Administering the Document 10
 - 1.5.2 Contact Person 10
 - 1.5.3 Person Determining CP Suitability for the Policy 10
 - 1.5.4 CPS Approval Procedure 10
 - 1.6 Definitions and Acronyms 10
 - 1.6.1 Definitions 10
 - 1.6.2 Acronyms 10
 - 1.6.3 References 10
 - 1.6.4 Conventions 10
- 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 10
 - 2.1 Repositories 10
 - 2.2 Publication of Certificate Information 10
 - 2.3 Time or Frequency of Publication 11
 - 2.4 Access Controls on Repositories 11
- 3. NAMING 11
 - 3.1 Type of Names 11
 - 3.1.1 CABF Naming Requirements 11
 - 3.1.2 Need for Names to be Meaningful 11
 - 3.1.3 Anonymity or Pseudonymity of Subscribers 11
 - 3.1.4 Rules for Interpreting Various Name Forms 11
 - 3.1.5 Uniqueness of Names 11
 - 3.1.6 Recognition, Authentication, and Role of Trademarks 11
 - 3.2 Initial Identity Validation 11
 - 3.2.1 Method to Prove Possession of Private Key 11
 - 3.2.2 Authentication of Organization and Domain Identity 12
 - 3.2.3 Authentication of Individual Identity 13
 - 3.2.4 Non-Verified Subscriber information 13
 - 3.2.5 Validation of Authority 13
 - 3.2.6 Criteria for Interoperation 13

3.3	Identification and Authentication for Re-key Requests	13
3.3.1	Identification and Authentication for Routine Re-key.....	14
3.3.1	Identification and Authentication for Re-key After Revocation	14
3.4	Identification and Authentication for Revocation Request.....	14
4.	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	14
4.1	Certificate Application	14
4.1.1	Who Can Submit a Certificate Application?.....	14
4.2	Certificate Application Processing	14
4.3	Certificate Issuance	14
4.3.1	CA Actions during Certificate Issuance	14
4.3.2	Notifications to Subscriber by a CA of Issuance of Certificate.....	14
4.4	Certificate Acceptance	14
4.4.1	Conduct Constituting Certificate Acceptance	14
4.4.2	Publication of the Certificate by the CA.....	15
4.4.3	Notification of Certificate Issuance by a CA to Other Entities.....	15
4.5	Key Pair and Certificate Usage.....	15
4.5.1	Subscriber Private Key and Certificate Usage	15
4.5.2	Relying Party Public Key and Certificate Usage.....	15
4.6	Certificate Renewal.....	15
4.7	Certificate Re-Key.....	15
4.8	Certificate Modification	15
4.9	Certificate Revocation and Suspension	16
4.9.1	Circumstances for Revocation	16
4.9.2	Who Can Request Revocation	16
4.9.3	Procedure for Revocation Request	16
4.9.4	Revocation Request Grace Period.....	16
4.9.5	Time within Which CA Must Process the Revocation Request	16
4.9.6	Revocation Checking Requirements for Relying Parties	16
4.9.7	CRL Issuance Frequency.....	17
4.9.8	Maximum Latency for CRLs	17
4.9.9	On-Line Revocation/Status Checking Availability.....	17
4.9.10	On-Line Revocation Checking Requirements	17
4.9.11	Other Forms.....	17
4.9.12	Special Requirements Regarding Key Compromise	17
4.9.13	Circumstances for Suspension	17
4.9.14	Who Can Request Suspension	17

4.9.15	Procedure for Suspension Request	17
4.9.16	Limits on Suspension Period	17
4.10	Certificate Status Service	17
4.10.1	Operational Characteristics	17
4.10.2	Service Availability	17
4.10.3	Optional Features	17
4.11	End of Subscription	17
4.12	Key Escrow and Recovery	17
5.	FACILITY, MANAGEMENT, ANDE OPERATIONAL CONTROLS	18
5.1	Physical Controls	18
5.2	Procedural Controls	18
5.3	Personnel Controls	18
5.4	Audit Logging Procedures	18
5.5	Records Archival.....	18
5.6	Key Changeover	18
5.7	Compromise and Disaster Recovery	18
5.8	CA or RA Termination.....	18
5.9	Data Security	18
6.	TECHNICAL SECURITY CONTROLS.....	18
6.1	Key Pair Generation and Installation	18
6.1.1	Key Pair Generation.....	18
6.1.2	Private Key Delivery to Subscriber	18
6.1.3	Public Key Delivery to Certificate Issuer.....	18
6.1.4	CA Public Key Delivery to Relying Parties	19
6.1.5	Key Sizes	19
6.1.6	Public Key Parameters Generation and Quality Checking	19
6.1.7	Key Usage Purposes (as per X.509 v3 Key Usage Field).....	19
6.2	Private Key Protection and Cryptographic Module Engineering Controls	19
6.2.1	Cryptographic Module Standards and Controls.....	19
6.2.2	Private Key (m out of n) Multi-Person Control	20
6.2.3	Private Key Escrow	20
6.2.4	Private Key Backup.....	20
6.2.5	Private Key Archival	20
6.2.6	Private Key Transfer Into or From a Cryptographic Module	20
6.2.7	Private Key Storage on Cryptographic Module	20
6.2.8	Method of Activating Private Key	20

6.2.9	Method of Deactivating Private Key	20
6.2.10	Method of Destroying Private Key.....	20
6.2.11	Cryptographic Module Rating	21
6.3	Other Aspects of Key Pair Management.....	21
6.3.1	Public Key Archival	21
6.3.2	Certificate Operational Periods and Key Pair Usage Periods.....	21
6.4	Activation Data.....	21
6.4.1	Activation Data Generation and Installation	21
6.4.2	Activation Data Protection	21
6.4.3	Other Aspects of Activation Data	21
6.5	Computer Security Controls.....	21
6.5.1	Specific Computer Security Technical Requirements	21
6.5.2	Computer Security Rating	22
6.6	Life Cycle Technical Controls	22
6.6.1	System Development Controls.....	22
6.6.2	Security Management Controls	22
6.6.3	Life Cycle Security Controls	22
6.7	Network Security Controls	22
6.8	Time-Stamping	22
7	CERTIFICATE, CRL, AND OCSP PROFILES	22
7.1	Certificate Profile	22
7.1.1	Version Number(s)	22
7.1.2	Certificate Extensions	22
7.1.3	Algorithm Object Identifiers	22
7.1.4	Name Forms	22
7.1.5	Name Constraints	22
7.1.6	Certificate Policy Object Identifier	22
7.1.7	Usage of Policy Constraints Extension	22
7.1.8	Policy Qualifiers Syntax and Semantics	22
7.1.9	Processing Semantics for the Critical Certificate Policies Extension.....	22
7.2	CRL Profile	23
7.2.1	Version Number(s)	23
7.2.2	CRL and CRL Entry Extensions	23
7.3	OCSP Profile	23
8	COMPLIANCE AUDIT AND OTHER ASSESSMENTS	23
8.1	Frequency and Circumstances of Assessment	23

8.2	Identity/Qualifications of Assessor.....	23
8.3	Assessor's Relationship to Assessed Entity	23
8.4	Topics Covered by Assessment	23
8.5	Actions Taken as a Result of Deficiency	23
8.6	Communications of Results.....	23
8.7	Self Audits	23
9.	OTHER BUSINESS AND LEGAL MATTERS	23
9.1	Fees.....	23
9.1.1	Certificate Issuance or Renewal Fees.....	23
9.1.2	Certificate Access Fees.....	23
9.1.3	Revocation or Status Information Access Fees.....	23
9.1.4	Fees for Other Services	23
9.1.5	Refund Policy	23
9.2	Financial Responsibility	23
9.2.1	Insurance Coverage.....	23
9.2.2	Other Assets	23
9.2.3	Extended Warranty Coverage	24
9.3	Confidentiality of Business Information.....	24
9.3.1	Scope of Confidential Information	24
9.3.2	Information Not Within the Scope of Confidential Information	24
9.3.3	Responsibility to Protect Confidential Information	24
9.4	Privacy of Personal Information.....	24
9.4.1	Privacy Plan	24
9.4.2	Information Treated as Private	24
9.4.3	Information Not Deemed Private	24
9.4.4	Responsibility to Protect Private Information.....	24
9.4.5	Notice and Consent to Use Private Information	24
9.4.6	Disclosure Pursuant to Judicial or Administrative Process.....	24
9.4.7	Other Information Disclosure Circumstances	24
9.4.8	Intellectual Property Rights	24
9.4.9	Property Rights in Certificates and Revocation Information	24
9.4.10	Property Rights in the CP	24
9.4.11	Property Rights in Names	24
9.4.12	Property Rights in Keys and Key Material.....	24
9.5	Representations and Warranties	24
9.5.1	CA Representations and Warranties.....	24

9.5.2	RA Representations and Warranties.....	24
9.5.3	Subscriber Representations and Warranties.....	24
9.5.4	Relying Party Representations and Warranties.....	25
9.5.5	Representations and Warranties of Other Participants	25
9.6	Disclaimers of Warranties.....	25
9.7	Limitations of Liability.....	25
9.7.1	Limitations of Liability for EV	25
9.8	Indemnities	25
9.8.1	Indemnification by Subscribers	25
9.8.2	Indemnification by Relying Parties	25
9.8.3	Indemnification of Application Software Suppliers.....	25
9.9	Term and Termination	25
9.9.1	Term.....	25
9.9.2	Termination	25
9.9.3	Effect of Termination and Survival	25
9.10	Individual Notices and Communications with Participants.....	25
9.11	Amendments	25
9.11.1	Procedure for Amendment.....	25
9.11.2	Notification Mechanism and Period.....	25
9.11.3	Circumstances under Which OID Must be Changed.....	25
9.12	Dispute Resolution Provisions.....	25
9.12.1	Disputes among VALID, Affiliates, and Customers.....	25
9.12.2	Disputes with End-User Subscribers or Relying Parties	25
9.13	Governing Law	26
9.14	Compliance with Applicable Law	26
9.15	Miscellaneous Provisions	26
9.15.1	Entire Agreement.....	26
9.15.2	Assignment	26
9.15.3	Severability	26
9.15.4	Enforcement (Attorney's Fees and Waiver of Rights)	26
9.15.5	Force Majeure.....	26
9.16	Other Provisions.....	26
	TABLE OF ACRONYMS AND DEFINITIONS.....	26
	REFERENCES	37

1. INTRODUCTION

This document is VALID ROOT CA Certification Practice Statement (CPS). It states the practices that VALID ROOT CA employs in providing certification services that include, but are not limited to, issuing, managing, revoking, and renewing certificates in accordance with the specific requirements of VALID CA Certificate Policies ("CP").

This document is targeted at:

- ✓ VALID CA PKI service providers who have to operate in terms of their own Certificate Practices (CP) that complies with the requirements laid down by the CPS.
- ✓ VALID ROOT CA certificate Subscribers who need to understand how they are authenticated and what their obligations are as VALID CA subscribers and how they are protected under VALID CA.
- ✓ Relying parties who need to understand how much trust to place in a VALID CA certificate, or a digital signature using that certificate.

This CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction.

VALID CA conforms to the current version of:

- a) CA/Browser Forum - Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates- version 1.5.1 (available at <https://cabforum.org/baseline-requirements-documents/>);
- b) CA/Browser Forum - Guidelines For The Issuance And Management Of Extended Validation Certificates – version 1.6.6 (available at <https://cabforum.org/extended-validation/>); and
- c) CA/Browser Forum - Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates – version 1.4 (available at <https://cabforum.org/ev-code-signing-certificate-guidelines/>) In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

1.1 Overview

This CPS is applicable to VALID ROOT CA.

VALID Subordinates CAs operate as CAs under VALID CA CP, issuing end-user subscriber certificates.

Registration Authorities (RAs) are entities that authenticate certificate requests under VALID CA.

VALID and Affiliates act as RAs for certificates they issue. VALID and Affiliates enter into contractual relationships with Enterprises who wish to manage their own certificate requests. These enterprise customers act as RAs, authenticating certificate requests for themselves and their affiliated individuals. VALID or the Affiliate will then issue these authenticated certificate requests.

Depending on the type of certificate, Digital Certificates MAY be used by Subscribers to secure websites, digitally sign code or other content, digitally sign documents and/or e-mails. The person who ultimately receives a signed document or communication, or accesses a secured website is referred to as a relying party, i.e., he/she is relying on the certificate and has to make a decision on whether to trust it.

A Relying Party MUST rely on a certificate in terms of the relevant Relying Party Agreement listed in VALID CA website.

1.2 Document Name and Identification

This document is VALID ROOT CA certification practice statement (CPS).

1.3 PKI Participants

As described at VALID CA CP, Section 1.3.

1.4 Certificate Usage

VALID ROOT CA issues certificate for others Certificate Authorities of VALID CA.

1.5 Policy Administration

1.5.1 Organization Administering the Document

VALID CERTIFICADORA DIGITAL

1000, Paulista Avenue – Ground floor – Bela Vista – São Paulo/SP – CEP 01310-100 – Brasil

1.5.2 Contact Person

VALID CERTIFICADORA DIGITAL

NORMAS & COMPLIANCE

1000, Paulista Avenue – Ground floor – Bela Vista – São Paulo/SP – CEP 01310-100 – Brasil

(55 - 11 - 2575-6800) / pki.compliance@valid.com

1.5.3 Person Determining CP Suitability for the Policy

VALID CA Policy Management Department (PMD), named as “Normas e Compliance” determines the suitability and applicability of this CPS.

1.5.4 CPS Approval Procedure

Approval of this CPS and subsequent amendments SHALL be made by the PMD. Amendments SHALL either be in the form of a document containing an amended form of the CPS or an update notice. Amended versions or updates SHALL be linked to the Practices Updates and Notices section of the VALID Repository located at:

<http://global.validcertificadora.com.br/ca-valid-root/cps-valid-root.pdf>

Updates supersede any designated or conflicting provisions of the referenced version of this CPS.

1.6 Definitions and Acronyms

1.6.1 Definitions

See Appendix A for a table of definitions.

1.6.2 Acronyms

See Appendix A for a table of acronyms.

1.6.3 References

See Appendix B for a list of References.

1.6.4 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in these Requirements SHALL be interpreted in accordance with RFC 2119.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

VALID is responsible for maintaining a publicly accessible online repository, as well as revocation information concerning Certificates it issues.

2.2 Publication of Certificate Information

VALID maintains a web-based repository that permits Relying Parties to make online inquiries regarding revocation and other Certificate status information. Any exception to this SHALL be approved by the PMD on a case by case basis and MUST be documented in the appropriate CP. VALID and Affiliates provide Relying Parties with information on how to find the appropriate repository to check Certificate status and, if OCSP (Online Certificate Status Protocol) is available, how to find the right OCSP responder.

VALID publishes the Certificates it issues on behalf of its own CAs, and the CAs in their Sub-domain. Upon revocation of an end-user Subscriber’s Certificate, VALID publishes notice of such revocation in the repository. In addition, VALID issues Certificate Revocation Lists (CRLs) and, if available, provide OCSP services (Online Certificate Status Protocol) for its own CAs and the CAs within their respective Sub-domains.

VALID will at all times publish a current version of the following documents in its repositories:

- ✓ This VALID ROOT CA CPS,
- ✓ VALID CA CP and CPS,
- ✓ Subscriber Agreements,
- ✓ Relying Party Agreements

VALID guarantees that its repository is accessible online on a 24x7 basis and that its CP and/or CPS disclose its VALID CA business practices as required by WebTrust for CAs and ETSI TS 102 042 and ETSI EN 319 411-1.

2.3 Time or Frequency of Publication

As described at VALID CA CP, Section 2.3.

2.4 Access Controls on Repositories

As described at VALID CA CP, Section 2.4.

3. NAMING

Names appearing in Certificates issued under VALID ROOT CA are authenticated.

3.1 Type of Names

VALID ROOT CA Certificates contains:

- ✓ an X.501 Distinguished Name (DN) in the Subject name field and in the Issuer Name field,
- ✓ MAY contain multiple OU attributes,
- ✓ its DN is formed as below:

<i>Version</i>	<i>Release Date</i>
Country (C) =	BR
Organization (O) =	Valid Certificadora Digital LTDA
Common Name (CN) =	VALID ROOT CA

3.1.1 CABF Naming Requirements

Not applicable.

3.1.2 Need for Names to be Meaningful

VALID ROOT CA Certificates contains names with commonly understood semantics permitting the determination of the identity of the CA that is the Subject of the Certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

VALID ROOT CA Subscribers are not permitted to use pseudonyms.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

VALID ROOT CA ensures that Subject Distinguished Name (DN) of the Subscriber is unique within the domain of a specific CA through automated components of the Subscriber enrollment process.

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificate Applicants SHALL NOT use names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. VALID SHALL be REQUIRED to determine whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark, and VALID SHALL be entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The certificate applicant MUST demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate.

The method to prove possession of a private key SHALL be PKCS #10, another cryptographically equivalent demonstration, or another VALID-approved method.

3.2.2.1 CABF Verification Requirements for EV

Not applicable.

3.2.2 Authentication of Organization and Domain Identity

Whenever a certificate contains an organization name, the identity of the organization and other enrollment information provided by Certificate Applicants (except for Non-verified Subscriber Information) is confirmed in accordance with the procedures set forth in this CPS and/or VALID internal documents.

If the Applicant requests a Certificate that will contain Subject Identity Information comprised only of the countryName field, then VALID SHALL verify the country associated with the Subject using a verification process meeting the requirements of Section 3.2.2.3 and that is described in this CP and/or VALID's internal documents. If the Applicant requests a Certificate that will contain the countryName field and other Subject Identity Information, VALID SHALL verify the identity of the Applicant, and the authenticity of the Applicant Representative's certificate request using a verification process meeting the requirements of this Section 3.2.2.1 and that is described in this CPS and/or VALID's internal documents.

VALID SHALL inspect any document relied upon under this Section for alteration or falsification.

3.2.2.1 Identity

VALID SHALL verify the identity and address of the Applicant using:

- a) Documentation provided by the Applicant and
- b) Determine that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government agency or recognized authority that confirms the existence of the organization.

VALID ROOT CA MAY use the same documentation or communication described above to verify both the Applicant's identity and address.

Alternatively, VALID ROOT CA MAY verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that VALID ROOT CA determines to be reliable.

3.2.2.2 DBA/Tradename

If the Subject Identity Information is to include a DBA or tradename, VALID ROOT CA SHALL verify the Applicant's right to use the DBA/tradename using at least one of the following:

- a) Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
- b) A Reliable Data Source;
- c) Communication with a government agency responsible for the management of such DBAs or tradenames;
- d) An Attestation Letter accompanied by documentary support; or
- e) A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that VALID ROOT CA determines to be reliable.

3.2.2.3 Verification of Country

VALID ROOT CA SHALL verify the country associated with the Subject using one of the following:

- a) Information provided by the Domain Name Registrar; or
- b) A method identified in Section 3.2.2.1.

3.2.2.4 Validation of Domain Authorization or Control

Not applicable.

3.2.2.5 Authentication for an IP Address

Not applicable.

3.2.2.6 Wildcard Domain Validation

Not applicable.

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, VALID ROOT CA SHALL evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. VALID ROOT CA SHOULD consider the following during its evaluation:

- a) The age of the information provided,
- b) The frequency of updates to the information source,
- c) The data provider and purpose of the data collection,
- d) The public accessibility of the data availability, and
- e) The relative difficulty in falsifying or altering the data.

Databases maintained by VALID ROOT CA, its owner, or its affiliated companies do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements under this Section 3.2.

3.2.2.8 CAA Records

Not applicable.

3.2.2.9 CABF Verification Requirements for Organization Applicants

Not applicable.

3.2.3 Authentication of Individual Identity

Not applicable.

3.2.4 Non-Verified Subscriber information

Non-verified subscriber information includes:

- ✓ Organization Unit (OU) with certain exceptions¹
- ✓ Any other information designated as non-verified in VALID CA CP

3.2.5 Validation of Authority

If the Applicant for a Certificate containing Subject Identity Information is an organization, VALID ROOT CA SHALL use a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request.

VALID ROOT CA MAY use the sources listed in section 3.2.2.1 to verify the Reliable Method of Communication.

Provided that VALID ROOT CA uses a Reliable Method of Communication, VALID ROOT CA MAY establish the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that VALID ROOT CA deems appropriate.

3.2.6 Criteria for Interoperation

VALID MAY provide interoperation services that allow any CA to be able to interoperate with VALID CA by unilaterally certifying that CA. CAs enabled to interoperate in this way will comply with VALID CA CP as supplemented by additional policies when required.

VALID SHALL only allow interoperation with VALID CA of any CA in circumstances where VALID CA SHALL at a minimum:

- ✓ Enters into a contractual agreement with VALID or an Affiliate
- ✓ Operates under a CPS that meets VALID CA requirements for the type of certificates it will issue
- ✓ Passes a compliance assessment before being allowed to interoperate
- ✓ Passes an annual compliance assessment for ongoing eligibility to interoperate.

VALID CA SHALL disclose all Cross Certificates that identify VALID CA as the Subject, provided that VALID CA arranged for or accepted the establishment of the trust relationship (i.e. the Cross Certificate at issue).

3.3 Identification and Authentication for Re-key Requests

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. VALID ROOT CA requires that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as "rekey").

¹ Domain-validated and organization-validated certificates MAY contain Organizational Unit values that are validated.

3.3.1 Identification and Authentication for Routine Re-key

Re-key procedures ensure that the person or organization seeking to rekey an end-user Subscriber Certificate is in fact the Subscriber of the previous Certificate.

VALID ROOT CA requires the same process as described at 4.1. section.

3.3.1 Identification and Authentication for Re-key After Revocation

VALID ROOT CA requires the same process as described at 4.1. section.

3.4 Identification and Authentication for Revocation Request

Revocation procedures ensure prior to any revocation of any Certificate that the revocation has in fact been requested by the Certificate's Subscriber, the entity that approved the Certificate Application, or the applicable CA.

Acceptable procedures for authenticating the revocation requests of a Subscriber include:

- ✓ Having the Subscriber for certain certificate types submit the Subscriber's Challenge Phrase (or the equivalent thereof), and revoking the Certificate automatically if it matches the Challenge Phrase (or the equivalent thereof) on record. (Note that this option MAY NOT be available to all customers.)
- ✓ Receiving a message from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked,
- ✓ Communication with the Subscriber providing reasonable assurances that the person or organization requesting revocation is, in fact the Subscriber. Such communication, depending on the circumstances, MAY include one or more of the following: telephone, e-mail, postal mail, or courier service.

The requests to revoke a CA Certificate SHALL be authenticated by the requesting entity's Superior entity to ensure that the CA has in fact requested the revocation.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application?

Below is a list of people who MAY submit certificate applications:

- ✓ Any authorized representative of an Organization or entity,
- ✓ Any authorized representative of a CA.

4.2 Certificate Application Processing

VALID ROOT CA SHALL perform identification and authentication of all required Subscriber information in terms of Section 3.2.

VALID ROOT CA begins processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application.

A certificate application remains active until rejected.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

A Certificate is created and issued following the approval of a Certificate Application by VALID ROOT CA. VALID ROOT CA creates and issues a Certificate based on the information in a Certificate Application following approval of such Certificate Application.

Certificate issuance by VALID ROOT CA SHALL require an individual authorized by VALID CA (i.e. VALID CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for VALID ROOT CA to perform a certificate signing operation.

4.3.2 Notifications to Subscriber by a CA of Issuance of Certificate

Not applicable.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The following conduct constitutes certificate acceptance:

- ✓ Downloading a Certificate or installing a Certificate from a message attaching it constitutes the Subscriber's acceptance of the Certificate.
- ✓ Failure of the Subscriber to object to the certificate or its content constitutes certificate acceptance.

4.4.2 Publication of the Certificate by the CA

VALID ROOT CA publishes the Certificates it issues in a publicly accessible repository.

4.4.3 Notification of Certificate Issuance by a CA to Other Entities

Not applicable.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Use of the Private Key corresponding to the public key in the certificate SHALL only be permitted once the Subscriber has agreed to the Subscriber Agreement and accepted the certificate. The certificate SHALL be used lawfully in accordance with VALID's Subscriber Agreement the terms of this CPS. Certificate use MUST be consistent with the KeyUsage field extensions included in the certificate.

Subscribers SHALL protect their private keys from unauthorized use and SHALL discontinue use of the private key following expiration or revocation of the certificate. Parties other than the Subscriber SHALL NOT archive the Subscriber Private Key except as set forth in section 4.12.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties SHALL assent to the terms of the applicable Relying Party Agreement as a condition of relying on the certificate.

Reliance on a certificate MUST be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party MUST obtain such assurances for such reliance to be deemed reasonable.

Before any act of reliance, Relying Parties SHALL independently assess:

- ✓ the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by this CPS.

VALID CA are not responsible for assessing the appropriateness of the use of a Certificate.

- ✓ that the certificate is being used in accordance with the Key Usage field extensions included in the certificate.
- ✓ the status of the certificate and all the CAs in the chain that issued the certificate. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to investigate whether reliance on a digital signature performed by an end-user Subscriber Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely at the risk of the Relying party.

Assuming that the use of the Certificate is appropriate, Relying Parties SHALL utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain.

4.6 Certificate Renewal

Certificate renewal is the issuance of a new certificate to the subscriber without changing the public key or any other information in the certificate.

VALID ROOT CA doesn't allow certificate renewal.

4.7 Certificate Re-Key

Certificate rekey is the application for the issuance of a new certificate that certifies the new public key.

VALID CA doesn't allows certificate re-Key, we ask for the subscriber start a new application.

4.8 Certificate Modification

Certificate modification refers to the application for the issuance of a new certificate due to changes in the information in an existing certificate (other than the subscriber's public key).

Certificate modification is considered a Certificate Application in terms of Section 4.1.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

VALID ROOT CA SHALL revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
4. The Issuing CA obtains evidence that the Certificate was misused;
5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this CP or the applicable CP or CPS;
6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by the Issuing CA's CP and/or CPS; or
10. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties².

4.9.2 Who Can Request Revocation

The Subscriber, RA, or Issuing CA can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties MAY submit Certificate Problem Reports informing VALID ROOT CA of reasonable cause to revoke the certificate.

Individual Subscribers can request the revocation of their own individual Certificates through an authorized representative of VALID or an RA.

In the case of organizational Certificates, a duly authorized representative of the organization SHALL be entitled to request the revocation of Certificates issued to the organization.

The entity that approved a Subscriber's Certificate Application SHALL also be entitled to revoke or request the revocation of the Subscriber's Certificate.

Only VALID is entitled to request or initiate the revocation of the Certificates issued to its own CAs.

4.9.3 Procedure for Revocation Request

4.9.3.1 Procedure for Requesting the Revocation of an End-User Subscriber Certificate

Not applicable.

4.9.4 Revocation Request Grace Period

Revocation requests SHALL be submitted as promptly as possible within a commercially reasonable time.

4.9.5 Time within Which CA Must Process the Revocation Request

Commercially reasonable steps are taken to process revocation requests immediately.

VALID ROOT CA begins investigation of a Certificate Problem Report within 24 hours of receipt, and decides whether revocation or other appropriate action is warranted based on at least the following criteria:

- ✓ The nature of the alleged problem;
- ✓ The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
- ✓ The entity making the complaint³; and
- ✓ Relevant legislation.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties SHALL check the status of Certificates on which they wish to rely. Relying Parties MAY check Certificate status by consulting the most recent CRL from VALID ROOT CA.

² e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates SHOULD be revoked and replaced by CAs within a given period of time.

³ for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered

4.9.7 CRL Issuance Frequency

VALID ROOT CA CRL SHALL be issued at least annually, but also within 24 hours whenever a CA Certificate is revoked.

4.9.8 Maximum Latency for CRLs

CRLs are posted to the VALID Repository within a commercially reasonable time after generation. This is generally done automatically within seconds of generation.

4.9.9 On-Line Revocation/Status Checking Availability

As described at VALID CA CP, Section 4.9.9.

4.9.10 On-Line Revocation Checking Requirements

Not applicable.

4.9.11 Other Forms

Not applicable.

4.9.12 Special Requirements Regarding Key Compromise

VALID CA Participants SHALL be notified of an actual or suspected CA private key Compromise using commercially reasonable efforts. VALID ROOT CA shall use commercially reasonable efforts to notify potential Relying Parties if they discover, or have reason to believe, that there has been a Compromise of the private key of one of their own CAs or one of the CAs within their sub-domain.

4.9.13 Circumstances for Suspension

Not applicable.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Service

4.10.1 Operational Characteristics

The status of public certificates is available via CRL through VALID ROOT CA (at a URL specified in AC's CPS).

Revocation entries on a CRL MUST NOT be removed until "Expiry Date" of the revoked Certificate.

4.10.2 Service Availability

VALID ROOT CA operates and maintains its CRL capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

VALID ROOT CA maintains an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by it.

VALID ROOT CA maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3 Optional Features

Not applicable.

4.11 End of Subscription

A subscriber MAY end a subscription for a VALID ROOT CA certificate by:

- ✓ Allowing his/her/its certificate to expire without renewing or re-keying that certificate
- ✓ Revoking of his/her/its certificate before certificate expiration without replacing the certificate.

4.12 Key Escrow and Recovery

No VALID CA participant MAY escrow CA, RA or end-user Subscriber private keys.

5. FACILITY, MANAGEMENT, ANDE OPERATIONAL CONTROLS

5.1 Physical Controls

VALID CA CP has documented detailed procedural control for CAs and RAs to adhere to.

5.2 Procedural Controls

VALID CA CP has documented detailed procedural control for CAs and RAs to adhere to.

5.3 Personnel Controls

VALID CA CP has documented detailed personnel control and security policies for CAs and RAs to adhere to.

5.4 Audit Logging Procedures

As described at VALID CA CP, Section 5.4.

5.5 Records Archival

As described at VALID CA CP, Section 5.5.

5.6 Key Changeover

As described at VALID CA CP, Section 5.6.

5.7 Compromise and Disaster Recovery

As described at VALID CA CP, Section 5.7.

5.8 CA or RA Termination

As described at VALID CA CP, Section 5.8.

5.9 Data Security

As described at VALID CA CP, Section 5.9.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Key pair generation SHALL be performed using Trustworthy Systems and processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, modification, or unauthorized use of private keys. This requirement applies to end-user Subscribers, Enterprise Customers, CAs pre-generating key pairs on end-user Subscriber hardware tokens.

CA key pair generation is performed by multiple pre-selected, trained and trusted individuals using Trustworthy Systems and processes that provide for the security and REQUIRED cryptographic strength for the generated keys.

For VALID ROOT CA and Issuing Root CAs, the cryptographic modules used for key generation meet the requirements of FIPS 140-1 level 3 or other similar standard used in Brazil.

All CA key pairs are generated in pre-planned Key Generation Ceremonies in accordance with VALID internal requirements. The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by VALID Management.

VALID CA maintains effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its CP and/or CPS and its Key Generation Script.

6.1.2 Private Key Delivery to Subscriber

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

When a public key is transferred to the issuing CA to be certified, it SHALL be delivered through a mechanism ensuring that the public key has not been altered during transit and that the Certificate Applicant possesses the private key corresponding to the transferred public key. The acceptable mechanism within VALID CA for public key delivery is a PKCS#10 Certificate signing request package or an equivalent method ensuring that:

- ✓ The public key has not been altered during transit; and
- ✓ The Certificate Applicant possesses the private key corresponding to the transferred public key.

VALID CA performing Key Generation Ceremonies transfer the public key from the cryptographic module where it was created to the cryptographic module of the superior CA (same cryptographic module if a CCA) by wrapping it in a PKCS #10 Certificate signing request.

6.1.4 CA Public Key Delivery to Relying Parties

As described at VALID CA CP, Section 6.1.4.

6.1.5 Key Sizes

Key pairs SHALL be of sufficient length to prevent others from determining the key pair’s private key using cryptanalysis during the period of expected utilization of such key pairs.

VALID ROOT CA Standard is:

- ✓ key sizes for end-users: 4096 bit RSA
- ✓ digital signature hash algorithm: SHA-512

6.1.5.1 CABF Requirements for Key Sizes

Root CA Certificates	Validity period beginning on or before 31 Dec 2010	Validity period beginning After 31 Dec 2010
Digest algorithm	MD5 (NOT RECOMMENDED), SHA-1, SHA-256, SHA-384 or HA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048**	2048
ECC curve	NIST P-256, P-384, or P-521	
Minimum DSA modulus and divisor size (bits) ***	L= 2048, N= 224 or L= 2048, N= 256	

Subordinate CA Certificates	Validity period beginning on or before 31 Dec 2010 and ending on or before 31 Dec 2013	Validity period beginning after 31 Dec 2010 or ending after 31 Dec 2013
Digest algorithm	SHA-1, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	1024	2048
ECC curve	NIST P-256, P-384, or P-521	
Minimum DSA modulus and divisor size (bits) ***	L= 2048, N= 224 or L= 2048, N= 256	

6.1.6 Public Key Parameters Generation and Quality Checking

As described at VALID CA CP, Section 6.1.6.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Private Keys corresponding to VALID ROOT CA MUST NOT be used to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and
4. Certificates for OCSP Response verification.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

VALID has implemented a combination of physical, logical, and procedural controls to ensure the security of VALID and Enterprise Customer CA private keys. Protection of VALID ROOT CA Private Key outside the validated system or device specified above MUST consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of VALID ROOT CA Private Key. VALID ROOT CA encrypts its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

Subscribers are required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.2.1 Cryptographic Module Standards and Controls

VALID ROOT CA private keys SHALL be protected using a Trustworthy System and private key holders SHALL take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such Private Keys in accordance with this CPS.

VALID ROOT CA performs all CA cryptographic operations on cryptographic modules rated at a minimum of FIPS 140-2 level 3 or other similar standard used in Brazil.

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

As described at VALID CA CP, Section 6.2.2.

6.2.3 Private Key Escrow

VALID ROOT CA private keys are not escrowed.

6.2.4 Private Key Backup

VALID creates backup copies of VALID ROOT CA private keys for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices. Cryptographic modules used for VALID ROOT CA private key storage meet the requirements of this CPS. VALID ROOT CA private keys are copied to backup hardware cryptographic modules in accordance with this CPS.

Modules containing onsite backup copies of VALID ROOT CA private keys are subject to the requirements of this CPS. Modules containing disaster recovery copies of VALID ROOT CA private keys are subject to the requirements of this CPS.

Private keys that are backed up are to be protected from unauthorized modification or disclosure through physical or cryptographic means. Backups are protected with a level of physical and cryptographic protection equal to or exceeding that for cryptographic modules within VALID site, such as at a disaster recovery site or at another secure off-site facility, such as a bank safe.

6.2.5 Private Key Archival

Upon expiration of VALID ROOT CA Certificate, the key pair associated with the certificate will be securely retained for a period of at least 5 years using hardware cryptographic modules that meet the requirements of this CPS. VALID ROOT CA key pairs SHALL NOT be used for any signing events after the expiration date of the corresponding VALID ROOT CA Certificate.

Parties other than the Subordinate CA SHALL NOT archive the Subordinate CA Private Keys without authorization by the Subordinate CA.

VALID does not archive copies of Subscriber private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

VALID generates CA key pairs on the hardware cryptographic modules in which the keys will be used. In addition, VALID makes copies of such CA key pairs for routine recovery and disaster recovery purposes. Where CA key pairs are backed up to another hardware cryptographic module, such key pairs are transported between modules in encrypted form.

If the Issuing CA generated the Private Key on behalf of the Subordinate CA, then the Issuing CA SHALL encrypt the Private Key for transport to the Subordinate CA. If the Issuing CA becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then the Issuing CA SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.

6.2.7 Private Key Storage on Cryptographic Module

Not applicable.

6.2.8 Method of Activating Private Key

VALID ROOT CA protects the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

When deactivated, private keys SHALL be kept in encrypted form only.

6.2.9 Method of Deactivating Private Key

VALID ROOT CA private keys are deactivated upon removal from the token reader.

When VALID ROOT CA is taken offline, VALID ROOT CA's personnel SHALL remove the token containing such private key from the reader in order to deactivate it.

6.2.10 Method of Destroying Private Key

Where required, all private keys MAY be destroyed in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key.

VALID utilizes the zeroization function of its hardware cryptographic modules and other appropriate means to ensure the complete destruction of CA private keys. When performed, CA key destruction activities are logged.

6.2.11 Cryptographic Module Rating

See Section 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

VALID ROOT CA SHALL archive their own public keys, as well as the public keys of all CAs within their Sub-domains, in accordance Section 5.5.

VALID ROOT CA Certificates are backed up and archived as part of VALID's routine backup procedures.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

As described at VALID CA CP, Section 6.3.2.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

As described at VALID CA CP, Section 6.4.1.

6.4.2 Activation Data Protection

As described at VALID CA CP, Section 6.4.2.

6.4.3 Other Aspects of Activation Data

6.4.3.1 Activation Data Transmission

When activation data for their private keys are transmitted, VALID CA Participants SHALL protect the transmission using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.4.3.2 Activation Data Destruction

Activation data for CA private keys SHALL be decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data.

6.5 Computer Security Controls

CA and RA functions take place on Trustworthy Systems in accordance with the standards documented in VALID CA's confidential security policies.

6.5.1 Specific Computer Security Technical Requirements

VALID ensures that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorized access. In addition, VALID limits access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers.

VALID's production network is logically separated from other components. This separation prevents network access except through defined application processes. VALID uses firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that MAY access production systems.

VALID requires the use of passwords that have a minimum character length and a combination of alphanumeric and special characters. VALID requires that passwords be changed on a periodic basis.

Direct access to VALID databases supporting VALID's CA Operations is limited to Trusted Persons in VALID's Production Operations group having a valid business reason for such access.

VALID enforces multi-factor authentication for all accounts capable of directly causing certificate issuance.

Gateway servers SHALL include the following functionality: access control to CA services, identification and authentication for launching of CA services, object re-use for CA random access memory, use of cryptography for session communication and database security, archival of CA and end-user Subscriber history and audit data, audit of security related events, self-test of security related CA services, and Trusted path for identification of PKI roles and associated identities.

RAs SHALL ensure that the systems maintaining RA software and data files are Trustworthy Systems secure from unauthorized access, which can be demonstrated by compliance with audit criteria.

RAs SHALL logically separate access to these systems and this information from other components. This separation prevents access except through defined processes. RAs SHALL use firewalls to protect the network from internal and external intrusion and limit the nature and source of activities that MAY access such systems and information. RAs SHALL require the use of passwords with a minimum character length and a combination of alphanumeric and special characters,

and SHALL require that passwords be changed on a periodic basis and as necessary. Direct access to the RA's database maintaining Subscriber information SHALL be limited to Trusted Persons in the RA's operations group having a valid business reason for such access.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Applications are developed and implemented by VALID in accordance with VALID systems development and change management standards. VALID also provides software to its Enterprise Customers for performing RA and certain CA functions. Such software is developed in accordance with VALID system development standards.

VALID developed software, when first loaded, provides a method to verify that the software on the system originated from VALID, has not been modified prior to installation, and is the version intended for use.

6.6.2 Security Management Controls

VALID has mechanisms and/or policies in place to control and monitor the configuration of its CA systems. VALID validates the integrity of its CA systems.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

CA and RA functions are performed using networks secured in accordance with the standards documented in VALID CA's confidential security policies (in the case of VALID and Affiliates) to prevent unauthorized access, tampering, and denial-of-service attacks. Communications of sensitive information SHALL be protected using point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication.

6.8 Time-Stamping

Certificates, CRLs, and other revocation database entries SHALL contain time and date information.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

As described at VALID CA CP, Section 7.1.

7.1.1 Version Number(s)

As described at VALID CA CP, Section 7.1.1.

7.1.2 Certificate Extensions

As described at VALID CA CP, Section 7.1.2.

7.1.3 Algorithm Object Identifiers

As described at VALID CA CP, Section 7.1.3.

7.1.4 Name Forms

As described at VALID CA CP, Section 7.1.4.

7.1.5 Name Constraints

As described at VALID CA CP, Section 7.1.5.

7.1.6 Certificate Policy Object Identifier

As described at VALID CA CP, Section 7.1.6.

7.1.7 Usage of Policy Constraints Extension

Not applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

As described at VALID CA CP, Section 7.1.8.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not applicable.

7.2 CRL Profile

As described at VALID CA CP, Section 7.2.

7.2.1 Version Number(s)

As described at VALID CA CP, Section 7.2.1.

7.2.2 CRL and CRL Entry Extensions

Not applicable.

7.3 OCSP Profile

As described at VALID CA CP, Section 7.3.

8. COMPLIANCE AUDIT AND OTHER ASSESMENTS

As described at VALID CA CP, Section 8.

8.1 Frequency and Circumstances of Assessment

As described at VALID CA CP, Section 8.1.

8.2 Identity/Qualifications of Assessor

As described at VALID CA CP, Section 8.2.

8.3 Assessor's Relationship to Assessed Entity

As described at VALID CA CP, Section 8.3.

8.4 Topics Covered by Assessment

As described at VALID CA CP, Section 8.4.

8.5 Actions Taken as a Result of Deficiency

As described at VALID CA CP, Section 8.5.

8.6 Communications of Results

As described at VALID CA CP, Section 8.6.

8.7 Self Audits

As described at VALID CA CP, Section 8.7

9. OTHER BUSINESS AND LEGAL MATTERS**9.1 Fees****9.1.1 Certificate Issuance or Renewal Fees**

As described at VALID CA CP, Section 9.1.1.

9.1.2 Certificate Access Fees

As described at VALID CA CP, Section 9.1.2.

9.1.3 Revocation or Status Information Access Fees

As described at VALID CA CP, Section 9.1.3.

9.1.4 Fees for Other Services

As described at VALID CA CP, Section 9.1.4.

9.1.5 Refund Policy

As described at VALID CA CP, Section 9.1.5.

9.2 Financial Responsibility**9.2.1 Insurance Coverage**

As described at VALID CA CP, Section 9.2.1.

9.2.2 Other Assets

As described at VALID CA CP, Section 9.2.2.

9.2.3 Extended Warranty Coverage

As described at VALID CA CP, Section 9.2.3.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

As described at VALID CA CP, Section 9.3.1.

9.3.2 Information Not Within the Scope of Confidential Information

As described at VALID CA CP, Section 9.3.2.

9.3.3 Responsibility to Protect Confidential Information

As described at VALID CA CP, Section 9.3.3.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

As described at VALID CA CP, Section 9.4.1.

9.4.2 Information Treated as Private

As described at VALID CA CP, Section 9.4.2.

9.4.3 Information Not Deemed Private

As described at VALID CA CP, Section 9.4.3.

9.4.4 Responsibility to Protect Private Information

As described at VALID CA CP, Section 9.4.4.

9.4.5 Notice and Consent to Use Private Information

As described at VALID CA CP, Section 9.4.5.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

As described at VALID CA CP, Section 9.4.6.

9.4.7 Other Information Disclosure Circumstances

As described at VALID CA CP, Section 9.4.7.

9.4.8 Intellectual Property Rights

As described at VALID CA CP, Section 9.5.

9.4.9 Property Rights in Certificates and Revocation Information

As described at VALID CA CP, Section 9.5.1.

9.4.10 Property Rights in the CP

As described at VALID CA CP, Section 9.5.2.

9.4.11 Property Rights in Names

As described at VALID CA CP, Section 9.5.3.

9.4.12 Property Rights in Keys and Key Material

As described at VALID CA CP, Section 9.5.4.

9.5 Representations and Warranties

9.5.1 CA Representations and Warranties

As described at VALID CA CP, Section 9.6.1.

9.5.2 RA Representations and Warranties

As described at VALID CA CP, Section 9.6.2.

9.5.3 Subscriber Representations and Warranties

As described at VALID CA CP, Section 9.6.3.

9.5.4 Relying Party Representations and Warranties

As described at VALID CA CP, Section 9.6.3.

9.5.5 Representations and Warranties of Other Participants

As described at VALID CA CP, Section 9.6.5.

9.6 Disclaimers of Warranties

As described at VALID CA CP, Section 9.7.

9.7 Limitations of Liability

As described at VALID CA CP, Section 9.8.

9.7.1 Limitations of Liability for EV

As described at VALID CA CP, Section 9.8.2.

9.8 Indemnities

9.8.1 Indemnification by Subscribers

As described at VALID CA CP, Section 9.9.1.

9.8.2 Indemnification by Relying Parties

As described at VALID CA CP, Section 9.9.2.

9.8.3 Indemnification of Application Software Suppliers

As described at VALID CA CP, Section 9.9.3.

9.9 Term and Termination

9.9.1 Term

As described at VALID CA CP, Section 9.10.1.

9.9.2 Termination

As described at VALID CA CP, Section 9.10.2.

9.9.3 Effect of Termination and Survival

As described at VALID CA CP, Section 9.10.3.

9.10 Individual Notices and Communications with Participants

As described at VALID CA CP.

9.11 Amendments

9.11.1 Procedure for Amendment

As described at VALID CA CP, Section 9.12.1.

9.11.2 Notification Mechanism and Period

As described at VALID CA CP, Section 9.12.2.

9.11.3 Circumstances under Which OID Must be Changed

As described at VALID CA CP, Section 9.12.3.

9.12 Dispute Resolution Provisions

9.12.1 Disputes among VALID, Affiliates, and Customers

As described at VALID CA CP, Section 9.13.1.

9.12.2 Disputes with End-User Subscribers or Relying Parties

As described at VALID CA CP, Section 9.13.2.

9.13 Governing Law

As described at VALID CA CP, Section 9.14.

9.14 Compliance with Applicable Law

As described at VALID CA CP, Section 9.15.

9.15 Miscellaneous Provisions

9.15.1 Entire Agreement

Not applicable.

9.15.2 Assignment

Not applicable.

9.15.3 Severability

As described at VALID CA CP, Section 9.16.3.

9.15.4 Enforcement (Attorney's Fees and Waiver of Rights)

Not applicable.

9.15.5 Force Majeure

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements SHALL include a force majeure clause protecting VALID and the applicable Affiliate.

9.16 Other Provisions

Not applicable.

TABLE OF ACRONYMS AND DEFINITIONS

Term	Definition
AC Digital Notarization Service	A service offered to Managed PKI SSL VALID Customers that provides a digitally signed assertion (a Digital Receipt) that a particular document or set of data existed at a particular point in time
AC Participant	An individual or organization that is one or more of the following within AC: VALID, an Affiliate, a Customer, a Reseller, a Subscriber, or a Relying Party
AC PKI	consists of systems that collaborate to provide and implement AC
AC Repository	VALID's database of Certificates and other relevant VALID SSL CERTIFICATION AUTHORITY information accessible on-line
AC Standards	The business, legal, and technical requirements for issuing, managing, revoking, renewing, and using Certificates within AC
Accounting Practitioner	A certified public accountant, chartered accountant, or a person with an equivalent license within the country of the Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility; provided that an accounting standards body in the jurisdiction maintains full (not "suspended" or "associate") membership status with the International Federation of Accountants
ACS	Authenticated Content Signing
Administrator	A Trusted Person within the organization of a CA or AR that performs validation and other CA or RA functions
Administrator Certificate	A Certificate issued to an Administrator that MAY only be used to perform CA or RA functions
Affiliate	A trusted third party (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) that has entered into an agreement with VALID to be a CA distribution and services channel within a specific territory
Affiliated Individual	A natural person that is (i) as an officer, director, employee, partner, contractor, intern, or other person within the Affiliate;

	(ii) as a member of a VALID registered community of interest, or (iii) as a person maintaining a relationship with the entity where the entity has business or other records providing appropriate assurances of the identity of such person
AICPA	American Institute of Certified Public Accountants
ANSI	The American National Standards Institute
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 AC or is 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 Period	In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in section 8.1
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. AC 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 AC MUST remove all wildcard labels from the left most portion of requested FQDN. AC 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 (https), 115 (sftp), 25 (smtp), 22 (ssh).
Automated Administration	A procedure whereby Certificate Applications are approved automatically if enrollment information matches information contained in a database
Automated Administration Software Module	Software provided by VALID that performs Automated Administration
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 FQDNs where the right-most domain name node is a GTLD having ICANN Specification 13 in its registry agreement, the GTLD itself MAY be used as the Base Domain Name
BIPM	International Bureau of Weights and Measures
BIS	(US Government) Bureau of Industry and Security
Business Entity	Any entity that is not a Private Organization, Government Entity, or Non-Commercial Entity as defined herein. Examples include, but are not limited to, general partnerships, unincorporated associations, sole proprietorships, etc.
CA	Certification Authority
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CEO	Chief Executive Officer
Certificate	An electronic document that uses a digital signature to bind a public key and an identity. At least, it states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.

Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate
Certificate Approver	A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate
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 CA has access
Certificate Management Control Objectives	Criteria that an entity MUST meet in order to satisfy a Compliance Audit
Certificate Management Process	Processes, practices, and procedures associated with the use of keys, software, and hardware, by which AC verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates
Certificate Policy (CP)	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 Requester	A natural person who is either the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits an EV Certificate Request on behalf of the Applicant
Certificate Revocation List (CRL)	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates in accordance with CP Section 3.4. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation
Certificate Signing Request (CSR)	A message conveying a request to have a Certificate issued
Certification Authority (CA)	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 Authority Authorization (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 "misuse"
Certification Practice Statement (CPS)	One of several documents forming the governance framework in which Certificates are created, issued, managed, and used. A statement of the practices that VALID or an Affiliate employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates.
VALID	Means, with respect to each pertinent portion of this CPS, VALID Certificadora Digital Ltda. and/or any wholly owned VALID subsidiary responsible for the specific operations at issue
VALID SSL CERTIFICATION AUTHORITY	The Certificate-based Public Key Infrastructure governed by AC Certificate Policies, which enables the worldwide deployment and use of Certificates by VALID and its Affiliates, and their respective Customers, Subscribers, and Relying Parties
CFO	Chief Financial Officer
Challenge Phrase	A secret phrase chosen by a Certificate Applicant during enrollment for a Certificate. When issued a Certificate, the Certificate Applicant becomes a Subscriber and a CA or RA can use the Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke or renew the Subscriber's Certificate
CICA	Canadian Institute of Chartered Accountants
CIO	Chief Information Officer
CISO	Chief Information Security Officer
Compliance Audit	A periodic audit that a AC or AR undergoes to determine its conformance with AC Standards that apply to it

Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information MAY have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key
Confidential/Private Information	Information required to be kept confidential and private pursuant to CP Section 2.8.1
Confirmation Request	An appropriate out-of-band communication requesting verification or confirmation of the particular fact at issue
Confirming Person	A position within an Applicant’s organization that confirms the particular fact at issue
Contract Signer	A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements
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%.
COO	Chief Operating Officer
Country	Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.
CP	Certificate Policy
CPA	Chartered Professional Accountant
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CRL Usage Agreement	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used
Cross Certificate	A certificate that is used to establish a trust relationship between two Root CAs
CSO	Chief Security Officer
CSPRNG	A random number generator intended for use in cryptographic system
Customer	An organization that is either a Managed PKI SSL VALID Customer or Gateway Customer
DBA	Doing Business As
Delegated Third Party	A natural person or Legal Entity that is not the CA, and whose activities are not within the scope of the appropriate CA audits, 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
Demand Deposit Account	A deposit account held at a bank or other financial institution, the funds deposited in which are payable on demand. The primary purpose of demand accounts is to facilitate cashless payments by means of check, bank draft, direct debit, electronic funds transfer, etc. Usage varies among countries, but a demand deposit account is commonly known as a share draft account, a current account, or a checking account
DNS	Domain Name System
Domain Authorization	Correspondence or other documentation provided by a Domain Name Registrant attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace
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 contact (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 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)
Domain Namespace	The set of all possible Domain Names that are subordinate to a single node in the Domain Name System
Enterprise EV Certificate	An EV Certificate that an Enterprise RA authorizes the CA to issue at third and higher domain levels
Enterprise EV RA	An RA that is authorized by the CA to authorize the CA to issue EV Certificates at third and higher domain levels
Enterprise RA	An employee or agent of an organization unaffiliated with AC who authorizes issuance of Certificates to that organization
Entry Date	The “Not After” date in a Certificate that defines the end of a Certificate’s validity period
EV	Extended Validation
EV Authority	A source other than the Certificate Approver, through which verification occurs that the Certificate Approver is expressly authorized by the Applicant, as of the date of the EV Certificate Request, to take the Request actions described in these Guidelines
EV Certificate	A digital certificate that contains information specified in the EV Guidelines and that has been validated in accordance with the Guidelines
EV Certificate Beneficiaries	Persons to whom the CA and its Root CA make specified EV Certificate Warranties
EV Certificate Reissuance	The process whereby an Applicant who has a valid unexpired and non-revoked EV Certificate makes an application, to the CA that issued the original certificate, for a newly issued EV Certificate for the same organizational name and Domain Name prior to the expiration of the Applicant's existing EV Certificate but with a 'valid to' date that matches that of the current EV Certificate
EV Certificate Renewal	The process whereby an Applicant who has a valid unexpired and non-revoked EV Certificate makes an application, to the CA that issued the original certificate, for a newly issued EV Certificate for the same organizational name and Domain Name prior to the expiration of the Applicant's existing EV Certificate but with a new 'valid to' date beyond the expiry of the current EV Certificate
EV Certificate Request	A request from an Applicant to the CA requesting that the CA issue an EV Certificate to the Applicant, which request is validly authorized by the Applicant and signed by the Applicant Representative
EV Certificate Warranties	In conjunction with the CA issuing an EV Certificate, the CA and its Root CA, during the period when the EV Certificate is Valid, promise that the CA has followed the requirements of these Guidelines and the CA’s EV Policies in issuing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate
EV Code Signing Certificate	A certificate that contains subject information specified in these Guidelines and that has been validated in accordance with these Guidelines
EV Code Signing Certificate Issuer	A CA providing an EV Code Signing Certificate to a Subscriber or a Signing Authority that provides an EV signature for a Subscriber.
EV Code Signing Object	An EV Code Signing Certificate issued by a CA or an EV Signature provided by a Signing Authority.
EV OID	An identifying number, in the form of an “object identifier,” that is included in the certificate Policies field of a certificate that: (i) indicates which CA policy statement relates to that certificate, and (ii) is either the CA/Browser Forum EV policy identifier or a policy identifier that, by pre-agreement with one or more Application Software Supplier, marks the certificate as being an EV Certificate.
EV Policies	Auditable EV Certificate practices, policies and procedures, such as a certification practice statement and certificate policy, that are developed, implemented, and enforced by the CA and its Root CA
EV Processes	The keys, software, processes, and procedures by which the CA verifies Certificate Data under CA/Browser Forum EV Guidelines, issues EV Certificates, maintains a Repository, and revokes EV Certificates
EV Signature	An encrypted electronic data file which is attached to or logically associated with other electronic data and which (i) identifies and is uniquely linked to the signatory of the electronic data, (ii) is created using means that the signatory can maintain under its sole control, and (iii) is linked in a way so as to make any subsequent changes that have been made to the electronic data detectable.

EV Subscriber	The Subject of the EV Code Signing Certificate. A Subscriber is the entity responsible for distributing the software but does not necessarily hold the copyright to the software
Exigent Audit/Investigation	An audit or investigation by VALID where VALID has reason to believe that an entity's failure to meet AC Standards, an incident or Compromise relating to the entity, or an actual or potential threat to the security of AC posed by the entity has occurred
Extended Validation	Validation Procedures defined by the Guidelines for Extended Validation Certificates published by a forum consisting of major certification authorities and browser vendors
Extended Validation Certificate	EV Certificate
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully-Qualified Domain Name
Fully-Qualified Domain Name	A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System
Government Agency	<ul style="list-style-type: none"> . In the context of a Private Organization, the government agency is in the Jurisdiction of Incorporation under whose authority the legal existence of Private Organizations is established (e.g., the government agency that issued the Certificate of Incorporation) . In the context of Business Entities, the government agency in the jurisdiction of operation that registers business entities. . In the case of a Government Entity, is 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, country, etc.)
GTLD	Generic TopLevel Domain
High Risk Certificate Request	A Request that AC 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 AC identifies using its own risk-mitigation criteria
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IFAC	International Federation of Accountants
IM	Instant Messaging
Incorporating Agency	Government Agency
Independent Confirmation From Applicant	Confirmation of a particular fact received by the CA pursuant to the provisions of the Guidelines or binding upon the Applicant
Individual	A natural person
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights
Intermediate Certification Authority	A Certification Authority whose Certificate is located within a Certificate Chain between the Certificate of the root CA and the Certificate of the Certification Authority that issued the end-user Subscriber's Certificate
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.
Internal Server Name	A Server Name (which MAY or MAY NOT include an Unregistered Domain Name) that is not resolvable using the public DNS
International Organization	An organization founded by a constituent document, e.g., a charter, treaty, convention or similar document, signed by, or on behalf of, a minimum of two Sovereign State governments
IRS	Internal Revenue Service
ISO	International Organization for Standardization
ISP	Internet Service Provider
Issuing CA	In relation to a particular Certificate, AC that issued the Certificate. This could be either a Root CA or a

	Subordinate CA
Jurisdiction of Incorporation	In the context of a Private Organization, the country and (where applicable) the state or province or locality where the organization’s legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the context of a Government Entity, the country and (where applicable) the state or province where the Entity’s legal existence was created by law
Jurisdiction of Registration	In the case of a Business Entity, the state, province, or locality where the organization has registered its business presence by means of filings by a Principal Individual involved in the business
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 Ceremony	A procedure whereby a CA’s or RA’s key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
Key Generation Script	A documented plan of procedures for the generation of a CA Key Pair
Key Manager Administrator	An Administrator that performs key generation and recovery functions for a Managed PKI SSL
Key Pair	The Private Key and its associated Public Key
Key Recovery Block (KRB)	A data structure containing a Subscriber’s private key that is encrypted using an encryption key. KRBS are generated
Key Recovery Service	A VALID service that provides encryption keys needed to recover a Key Recovery Block as part of a Managed PKI SSL
KRB	Key Recovery Block.
Latin Notary	A person with legal training whose commission under applicable law not only includes authority to authenticate the execution of a signature on a document but also responsibility for the correctness and content of the document. A Latin Notary is sometimes referred to as a Civil Law Notary.
Legal Entity	An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country’s legal system
Legal Existence	A Private Organization, Government Entity, or Business Entity has Legal Existence if it has been validly formed and not otherwise terminated, dissolved, or abandoned.
Legal Practitioner	A person who is either a lawyer or a Latin Notary as described in these Guidelines and competent to render an opinion on factual claims of the Applicant.
LSVA	Logical security vulnerability assessment
Managed PKI SSL VALID	VALID’s fully integrated Managed PKI SSL VALID service that allows enterprise Customers of VALID and its Affiliates to distribute Certificates to individuals, such as employees, partners, suppliers, and customers, as well as devices, such as servers, routers, and firewalls. Managed PKI SSL VALID permits enterprises to secure messaging, intranet28, extranet, virtual private network, and e-commerce applications
Managed PKI SSL VALID Administrator	An Administrator that performs validation or other RA functions for a Managed PKI SSL VALID Customer
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface
NIST	(US Government) National Institute of Standards and Technology
Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only an adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a AC Certificate MAY provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation
Non-verified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by AC or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant

Notary	A person whose commission under applicable law includes authority to authenticate the execution of a signature on a document
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	Online Certificate Status Protocol
OCSP Responder	An online server operated under the authority of AC and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol
Offline CA	Issuing Root CAs and other designated intermediate CAs that are maintained offline for security reasons in order to protect them from possible attacks by intruders by way of the network. These CAs do not directly sign end user Subscriber Certificates
OID	Object Identifier
Online CA	CAs that sign end user Subscriber Certificates are maintained online so as to provide continuous signing services
Online Certificate Status Protocol	An online Certificate-checking protocol for providing Relying Parties with real-time Certificate status information
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked
Parent Company	A company that Controls a Subsidiary Company
PIN	Personal identification number
PKCS	Public-Key Cryptography Standard
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys
PKI	Public Key Infrastructure
Place of Business	The location of any facility (such as a factory, retail store, warehouse, etc) where the Applicant's business is conducted
PMD	Policy Management Department
Policy Management Authority (PMD)	The organization within VALID responsible for promulgating this policy throughout AC
Principal Individual	An individual of a Private Organization, Government Entity, or Business Entity that is either an owner, partner, managing member, director, or officer, as identified by their title of employment, or an employee, contractor or agent authorized by such entity or organization to conduct business related to the request, issuance, and use of EV Certificates
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
Private Organization	A non-governmental legal entity (whether ownership interests are privately held or publicly traded) whose existence was created by a filing with (or an act of) the Incorporating Agency or equivalent in its Jurisdiction of Incorporation
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	The architecture, organization, techniques, practices, procedures, hardware, software, people, rules, policies, and obligations that collectively support the implementation and operation of a Certificate-based public key cryptographic system.
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
QGIS	Qualified Government Information Source
QIIS	Qualified Independent Information Source
QTIS	Qualified Government Tax Information Source

Qualified Auditor	A natural person or Legal Entity that meets the requirements of Section 8.2 Identity/Qualifications of Assessor
Qualified Government Information Source	A database maintained by a Government Entity (e.g. SEC filings) that meets the requirements of Section 11.11.6
Qualified Government Tax Information Source	A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities, or Individuals
Qualified Independent Information Source	A regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information
RA	Registration Authority
Click-through	Process of a visitor clicking on a Web advertisement and going to the advertiser's Web site. Also called ad clicks or requests.
Registered Domain Name	A Domain Name that has been registered with a Domain Name Registrar
Registered Domain Name	A Domain Name that has been registered with a Domain Name Registrar. 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.
Registered Office	The official address of a company, as recorded with the Incorporating Agency, to which official documents are sent and at which legal notices are received.
Registration Agency	A Governmental Agency that registers business information in connection with an entity's business formation or authorization to conduct business under a license, charter or other certification. A Registration Agency MAY include, but is not limited to (i) a State Department of Corporations or a Secretary of State; (ii) a licensing agency, such as a State Department of Insurance; or (iii) a chartering agency, such as a state office or department of financial regulation, banking or finance, or a federal agency such as the Office of the Comptroller of the Currency or Office of Thrift Supervision.
Registration Authority	A 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.
Registration Number	The unique number assigned to a Private Organization by the Incorporating Agency in such entity's Jurisdiction of Incorporation
Regulated Financial Institution	A financial institution that is regulated, supervised, and examined by governmental, national, state or provincial, or local authorities
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.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party
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 AC 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 AC 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.
Required Website Content	Either a Click-through or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.
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
Retail Certificate	A Certificate issued by VALID or an Affiliate, acting as CA, to individuals or organizations applying one by one to VALID or an Affiliate on its web site
RFC	Request for comment
Root CA	Root Certification Authority
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
Root Certification Authority	A CA that acts as a root CA and issues Certificates to CAs subordinate to it
Root Key Generation Script	Key Generation Script of a Root CA Key Pair
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman
S/MIME	Secure MIME (multipurpose Internet mail extensions)
SAR	Security Audit Requirements
SEC	(US Government) Securities and Exchange Commission
Secure Sockets Layer	The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and OPTIONAL client authentication for a Transmission Control Protocol/Internet Protocol connection
Security and Practices Review	A review of an Affiliate performed by VALID before an Affiliate is permitted to become operational
Signing Authority	One or more Certificate Approvers designated to act on behalf of the Applicant.
SOC	Service Organization Control standard
Sovereign State	A state or country that administers its own government, and is not dependent upon, or subject to, another power.
SSL	Secure Sockets Layer
SSL Admin	A web-based interface that permits Managed PKI SSL VALID Administrators to perform Manual Authentication of Certificate Applications
Sub-domain	The portion of VALID AC PARTNERS under control of an entity and all entities subordinate to it within VALID AC PARTNERS hierarchy
Subject	The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject and holder of a private key corresponding to a public key. The Subject is either the Subscriber or a device under the control and operation of the Subscriber. The term "Subject" can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject's Certificate
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	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organizational Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate
Subscriber Agreement	An agreement between VALID AC PARTNERS or RA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties
Subsidiary Company	A company that is controlled by a Parent Company

Superior Entity	An entity above a certain entity within a VALID AC PARTNERS hierarchy
Superior Government Entity	Based on the structure of government in a political subdivision, the Government Entity or Entities that have the ability to manage direct and control the activities of the Applicant.
Supplemental Risk Management Review	A review of an entity by VALID following incomplete or exceptional findings in a Compliance Audit of the entity or as part of the overall risk management process in the ordinary course of business
Suspect code	Code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes
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 or is the CA.
Timestamp Authority	An organization that timestamps data, thereby asserting that the data existed at the specified time
TLD	Top-Level Domain
TLS	Transport Layer Security
Translator	An individual or Business Entity that possesses the requisite knowledge and expertise to accurately translate the words of a document written in one language to the native language of the CA.
Trusted Person	An employee, contractor, or consultant of an entity within VALID AC PARTNERS responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CP Section 5.2.1
Trusted Position	The positions within a VALID AC PARTNERS entity that MUST be held by a Trusted Person.
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. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature
TTL	Time To Live
Unregistered Domain Name	A Domain Name that is not a Registered Domain Name.
UTC(k)	National realization of Coordinated Universal Time
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
Verified Accountant Letter	A document meeting the requirements specified in Section 11.11.2 of these Guidelines
Verified Legal Opinion	A document meeting the requirements specified in Section 11.11.1 of these Guidelines
Verified Method of Communication	The use of a telephone number, a fax number, an email address, or postal delivery address, confirmed by the CA in accordance with Section 11.5 of the Guidelines as a reliable way of communicating with the Applicant.
Verified Professional Letter	A Verified Accountant Letter or Verified Legal Opinion
VOID	Voice Over Internet Protocol
WebTrust EV Program	The additional audit procedures specified for CAs that issue EV Certificates by the AICPA/CICA to be used in conjunction with its WebTrust Program for Certification Authorities
WebTrust Program for CAs	The then-current version of the AICPA/CICA WebTrust Program for Certification Authorities
WebTrust Seal of Assurance	An affirmation of compliance resulting from the WebTrust Program for CAs
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
CABF Baseline Requirements	CABF Baseline Requirements, v. 1.0.5, Effective 12-Sep-12, user-assigned as XX, based on ISO 3166-1 country code , was allowed

REFERENCES

- ✓ CA/Browser Forum - Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates- version 1.4.8 (available at <https://cabforum.org/baseline-requirements-documents/>)
- ✓ CA/Browser Forum - Guidelines For The Issuance And Management Of Extended Validation Certificates – version 1.6.5 (available at <https://cabforum.org/extended-validation/>)
- ✓ ETSI EN 319 403, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.
- ✓ ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ✓ 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. Network and Certificate System Security Requirements, v.1.0, 1/1/2013.
- ✓ 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.
- ✓ 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.
- ✓ RFC6844, Request for Comments: 6844, DNS Certification Authority Authorization (CAA) Resource Record, Hallam-Baker, Stradling, January 2013.
- ✓ RFC6960, Request for Comments: 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Santesson, Myers, Ankney, Malpani, Galperin, Adams, June 2013.
- ✓ WebTrust for Certification Authorities , SSL Baseline with Network Security, Version 2.0, available at <http://www.webtrust.org/homepage-documents/item79806.pdf>.
- ✓ X.509, Recommendation ITU-T X.509 (10/2012) | ISO/IEC 9594-8:2014 (E), Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.