CA TECNISIGN

CERTIFICATION PRACTICES STATEMENT

OID: 1.3.6.1.4.1.47402.2.7

Version 1.0
September 13, 2018

Update History:

Version	*Date*	*Created by*	*Item Changed*	*Change Description*
v1.0	09/13/2018	Standards & Compliance	Not applicable	Creation of CA TECNISIGN

APPROVED BY:

_____

Table of Contents

1. INTROCTION 12
1.1 Overview 12
1.2 Document name and ID 13
1.2.1 CABF Policy Identifier 13
1.3 Community (PKI participants) 13
1.3.1 Certification Authority 13
1.3.2 Registry Authorities 13
1.3.3 Candidate 14
1.3.4 Subscribers 14
1.3.5 Trusted Parties 15
1.3.6 Accrediting Entity 15
1.3.7 Other participants 15
1.4 Certificate Owners 15
1.4.1 Applicability 15
1.4.1.1 Appropriate uses of the certificate 15
1.4.1.2 Certificates issued to individuals 15
1.4.1.3 Certificates issued to organizations 16
1.5 Policy Management 16
1.5.1 Organization that manages the document 16
1.5.2 Contact Information 16
1.5.3 Person who determines the adequacy of CPS as a policy 16
1.5.4 CDS approval procedure 16
1.6 Definitions and Acronyms 16
1.6.1 Definitions 16
1.6.2 Acronyms 16
1.6.3. References 17
1.6.4. Conventions 17
2. Publication and Repository Responsibilities 17
2.1 Repository 17
2.3 Publication time and frequency 17
2.4 Access Controls in Repositories 18

3. Identification and Authentication 18
3.1 CERTIFICATE ORDER VALIDATION 18
3.1.2 CERTIFICATE ORDER VERIFICATION 18
3.2. Authentication of an Individual Identity 19
3.2.1. Documents for the purpose of identifying an individual 19
3.2.2. Information included in the certificate issued to an individual 19
3.3 Authentication of an organization identity 19
3.3.1. Documents for the purpose of identifying an organization 20
3.3.2 Information included in the certificate issued to an organizationo 20
3.4 Identification and Authentication for new key order 20
3.4.1. Identification and Authentication for Renewal 20
3.4.1.2. Identification and Authentication for Renewal after Revocation 20
4. Operational Requirements of the Certificate Life Cycle 21
4.1. Certificate Order 21
4.1.1 Who can submit a certificate order 21
4.2 Certificate Order Process 21
4.2.1 Processing Time for Certificate Orders 21
4.3 Certificate Issuance 21
4.4 Certificate Acceptance 21
4.5 Pair of Keys and the use of the Certificate 22
4.5.1 Use of Trusted Parties' public key and certificate 22
4.6 Certificate Re-certification 23
4.7 Certificate Renewal 23
4.7.1 Circumstances for Certificate Renewal 23
4.8 Certificate Modification 23
4.8.1 Circumstances for Certificate Modification 23
4.9 Certificate Suspension and Revocation 23
4.9.1 Circumstances for Revocation 23
4.9.1.1. Reasons to Revoke a Subscriber Certificate 23
4.9.1.1.1 CABF Requirements 25
4.9.1.2. Reasons to revoke a Subordinate CA certificate 25
4.9.2 Who can order revocation 25
4.9.2.1 Procedure for Ordering Revocation of an End User Certificate 26

4.9.2.1.1 CABF Requirements 26
4.9.3 Grace Period of the Revocation Order 27
4.9.4 Term in which CA must process the revocation order 27
4.9.5 Revocation Verification Requirements for Trusting Parties 27
4.9.6 CRL Issue Frequency 27
4.9.6.1 Subscriber Certificate Status Requirements 27
4.9.6.2 Subordinate CA Certificate Status Requirements 28
4.9.7 Maximum pulication for CRLs 28
4.9.8 CRL Retention Period 28
4.9.9 Online Revocation Availability / Status Verification 28
4.9.10 Requirements for online revocation verification 28
4.9.11 CABF Requirements for OCSP 29
4.9.11.1 Certificate Sttatus for Subscriber Certificates 29
4.9.11.2 Certificate Status for Subordinate CA Certificates 29
4.9.12 Other forms available for revocation disclosure 29
4.9.13 Special Requirements Related to Key Commitment 29
4.9.14 Circumstances for suspension 29
4.9.15 Who can order suspension 29
4.9.16 Procedure for Ordering Suspension 29
4.9.17 Limit Suspension Period 29
4.10 Certificate Status Services 30
4.10.1 Operational Characteristics 30
4.10.2 Service Availability 30
4.10.3 Optional Features 30
4.11 End of Subscription 30
4.12 Key Custody and Recovery 30
5. Facilities, Management and Operational Controls 30
5.1 Physical Controls 33
5.1.1 Facilities Construction and Location 33
5.1.2 Physical Access 33
5.1.2.1. CA Operating Sensitive Activities 33
5.1.3 Energy and Air Conditioning 34
5.1.4 Water Exposure 34

5.1.5 Prevention and Protection Against Fire 34
5.1.6 Media Storage 34
5.1.7 Disposal of paper documents and electronic devices 34
5.1.8 External (off-site) Security (backup) Facilities 34
5.2 Procedural Controls 34
5.2.1 Trust Functions 34
5.2.2 Personnel Controls 35
5.2.2.1 Number of persons required per task 35
5.2.3 Identification and Authentication for each profile 35
5.2.4 Functions requiring task segregation 36
5.3 Personnel Controls 36
5.3.1 Background, qualification, experience and idoneidade requirements 36
5.3.2 Background Check Procedures 36
5.3.3 Training Requirements 37
5.3.3.1 CABF Requirements for Training and Skill Level 37
5.3.4 Recycling Frequency and Requirements 37
5.3.5 Job/Work Rotation Frequency and Sequence 38
5.3.6 Sanctions for Unauthorized Actions 38
5.3.7 Requirements for independent third parties 38
5.3.7.1 Guidelines Compliance Obligation 38
5.3.7.1.2 Responsibility Assignments 38
5.3.8 Documentation Provided to Personnel 38
5.4 Security Audit Procedures 39
5.4.1 Types of Recorded Events 39
5.4.1.1 CABF Tipos de Eventos Requisitos Gravados 39
5.5 Archiving Records 40
5.5.1 Types of archived records 40
5.5.2 Retention Period for Archieve 40
5.5.3 File protection 40
5.5.4 File backup procedures 40
5.5.5 Record time-stamping requirements 40
5.5.6 File data collection system (internal or external) 40
5.5.7 Procedures for obtaining and verifying file information 40

5.6 Key Exchange 41
5.7 Commitment/Compromise and Disaster Recovery 41
5.7.1 Procedures for Incident Handling and Commitment/Compromise 41
5.7.2 Computer resources, software and/or data are corrupted 42
5.7.3 Entity private key commitment procedures 42
5.7.4 Business continuity capacity after a disaster 42
5.7.4.1 CABF requirements for Business Continuity Capacity after a Disaster 44
5.8 CA or RA extinction 44
5.9 Data security 44
5.9.1 Objectives 44
5.9.2 Risk assessment 45
5.9.3 Security Plan 45
6. Security Technical Controls 45
6.1 Generation of key pair and installation 45
6.1.1 Generation of key pair 45
6.1.1.1. CABF CA key pair generation requirements 46
6.1.2 Delivery of the key pair to the Signatory 46
6.1.3 Delivery of public key to certificate issuer 47
6.1.4 Delivery of CA Public Key to Trusting Parties 47
6.1.5 Key size 47
6.1.5.1 CABF Requirements for key sizes 48
6.1.6 Generation of public key parameters and quality verification 48
6.1.7 Key usage purposes (according to “key usage” field in X.509 v3) 49
6.1.8 Private Key Protection Controls and Cryptographic Modulus 49
6.1.9 Cryptographic Modulus Defaults/Standards and Controls 49
6.1.10 Private Key (m out of n) Multi-Person Control 50
6.1.11 Private Key Custody 50
6.1.12 Private Key Backup 50
6.1.13 Private Key Archiving 50
6.1.14 Private key transfer in cryptographic modulus 51
6.1.15 Private Key Storage in Cryptographic Modulus 51
6.1.16 Private key Activation Method 51
6.1.17 Private Key Deactivation Method 52

6.1.18 Private key destruction method 52
6.1.19 Criptographic Modulus Classification 52
6.2 Other aspects of key pair management 52
6.2.1 Public Key Archiving 52
6.2.2 Certificate Operating Periods and Key Pair Usage Periods 52
6.2.2.1 CABF Requirements of the Validity Period 53
6.3 Activation Data 54
6.3.1 Generation and installation of Activation Data 54
6.3.2 Activation Data Protection 54
6.3.2.1 Other aspects of the activatino date 54
6.4 Computer Security Controls 55
6.4.1 Specific Technical Requirements for Computer Security 55
6.4.1.1 CABF Requirements for Security Systems 56
6.4.2 Life Cycle Technical Controls 56
6.4.1 System Development Controls 56
6.4.3 Security Management Controls 56
6.4.4 Life Cycle Security Control 56
N/A 56
6.5 Network Security Controls 56
6.6 Time Stamp 56
7. CERTIFICATE PROFILES, CRL AND OCSP 56
7.1 Certificate Profile 56
7.1.1 Version(s) Number 57
7.1.2 Certificate Extensions 57
7.1.2.1 Subject Alternative Name 57
7.1.2.2. Application of RFC 5280 57
7.1.3 Algorithms identifiers 57
7.1.3.1 CABF Requirements for algorithms identifiers 57
7.1.4 Names formats 57
7.1.4.1 Issuer (Issuer) Information 57
7.1.4.2.Issuer (Subject) information – End User Certificates 57
7.1.4.2.1. CABF Requirements for Subject Alternative Name Extension 57
7.1.4.2.1.1. Reserved IP Address or Internal Name 58

7.1.4.2.2. CABF Requirements for the field Subject Distinguished Name Fields 58
7.1.4.3. Subject Information – for CA Root and CA Subordinate Certificates 58
7.1.4.3.1. Subject Distinguished Name Fields 58
7.1.5 CABF Requirement for Name Restrictins 58
7.1.6 Certificates Policy Object Identifier 58
7.1.6.1. Reserved CP Identifiers 58
7.1.6.2. Root CA Certificates 58
7.1.6.3. CASubordinate Certificates ertificados de AC Subordinadas 58
7.1.6.4. Ende User Certificates 58
7.1.6.5 CABF Requirements for CP Object Identifier 59
7.1.6.5.1 CABF Requirements for CP Object Identifier for EV 59
7.1.7 Policy Restrictions Extension Use 59
7.1.8 Policy Qualifiers Syntax and Semantics 59
7.1.9 Processing semantics for Critical Extensions 59
7.2 LCR PROFILE 59
7.2.1 Version 59
7.2.2 LCR extensions and their entries 59
7.3 OCSP Profile 59
7.3.1 Version(s) Number 59
7.3.2 OCSP Extensions 59
8. Compliance Audit and Other Evaluations 59
CABF Requirements for audits 60
CABF requirements for audits for EV 60
8.1 Evaluation Frequency and Circumstances 61
8.2 Identity / Evaluator's Qualifications 61
8.3 Assistant relationship with the evaluated entity 62
8.4 Topics covered by the evaluation 62
1. WebTrust for Certification Authorities v2.1; 62
8.4.1 RAs Audit 62
8.4.2 VALID and Affiliate Audit 62
8.5 Actions taken as a result of defficiency 63
8.6 Results Communication 63
8.7. Self-Audits 63

8.7.1. CABF Self-Audit Requirements 63
8.7.2. CABF Self-Audit Requirements for EV Certificates and EV Code Signature 64
9. Other commercialand legal subjects 64
9.1 Fees 64
9.1.1 Certificates Issuance or Renewal Fees 64
9.1.2 Certificate Access Fees 64
9.1.3 Fees for Certificate Revocation or Status 64
9.1.4 Fees for other services 65
9.1.5 Refund Policy 65
9.2 Financial Responsibility 65
9.2.1 Insurance Coverage 65
9.2.2 Other Assets 65
9.2.3 Extended Warranty Coverage 65
9.2.4 Insurances for EV Certificates and EV Code Signature 66
9.3 Confidentiality of business information 66
9.3.1 Scope of Confidential Information 66
9.3.2 Information outside the scope of Confidential Information 66
9.3.3 Responsibilty to Protect Confidential Information 66
9.4 privacy of personal information 66
9.4.1 Privacy Plan 66
9.4.2 Information deemed Confidential 67
9.4.3 Information not deemed Confidential 67
9.4.4 Responsibility to Protect confidential information 67
9.4.5 Notice and Consent to Use Confidential Information 67
9.4.6 Disclosure on request of judicial or administrative proceedings 67
9.4.7 Other Circunstances of Information Disclosure 67
9.5 Intellectual Property Rights 68
9.5.1 Property Rights in Certificates information and revocation 68
9.5.2 Property Rights of this CPS 68
9.5.3 Property Rights for names 68
9.5.4 Property Rights for Keys and similar Materials 68
9.6 Representations and Guarantees 69
9.6.1 AC representations and Guarantees 69

9.6.1.1 CABF Guarantees and Obligations 69
1. Right to use Domain Name or IP Address: that, at the time of issuance, CA TECNISIGN 69
9.6.1.2 EV CCCertificates Guarantees 70
9.6.1.3 Guaranteesfor Code Signing EV Certificate 70
9.6.2 AR Representations and Guarantees 70
9.6.3 Subscriber Representations and Guarantees 71
9.6.3.1 CABF Requirements for Subscriber Agreement 71
9.6.4 Representations and Guarantees of Trusted Parties 72
9.6.5 Representations and Guarantees of other Participants 73
9.7 Disclaimer of Guarantees 73
9.8 Limitations of Liability 73
9.8.1 CABF Limitation of Liability Requirements 74
9.8.2 Limitations ofLiability for EV 74
9.9 Indemnifications 74
9.9.1 Indemnifications by subscribers 74
9.9.2 Indemnification of Trusted Parties 75
9.9.3 Indemnification for Software Vendors 75
9.10 Validity and Termination of CPS 76
9.10.1 CPS Change 76
9.10.2 Validity of the CPS 76
9.10.3 Effect after CP termination 76
9.11 Individual notices and communications with participants 76
9.12 Changes 76
9.12.1 Change process 76
9.12.2 Notificatin Machanism and Frequency 76
9.12.2.1 Period for comment 77
9.12.2.2 Mechanism to deal with Comments 77
9.12.3 Circumstances in which OIDs must be changed 77
9.13 Provisions for Disputes Resolution 77
9.13.1 Disputes between VALID, AR, Affiliates and Clients 77
9.13.2 Disputes with Subscribers,end users or Trusted Parties 77
9.14 Applicable Law 78
9.15 Compliance with the applicable Law 78

9.15.1 Compliance with CABFORUM 78
9.16 Miscellaneous Provisions 78
9.16.1 Totality of the Agreement 78
9.16.2 Attribution 78
9.16.3 Disassociation 79
9.16.3.1 CABF Disassociation requirements 79
9.16.4 Application (Fees and Waiver of attorney rights) 79
9.16.5 Force Majeure 79
9.17 Other Provisions 79
Appendix A: Abbreviations and Acronyms Table 80
Appendix B: References 101

1. INTRODUCTION

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

This document is intended for:

- Service providers for PKI and CA TECNISIGN E-signature Official Infrastructure that must operate in terms of their own Certification Policies (CP) which meet the requirements established by CPS.
- CA TECNISIGN certificate signatories who need to understand how they are authenticated and what their obligations are as CA TECNISIGN signatories and how they are protected by CA TECNISIGN.
- Trusted parties who need to understand how reliable an CA TECNISIGN certificate is, or a digital signature by using this certificate.

This CPS complies with Internet Engineering Task Force (IETF) RFC 3647 for the construction of the Certification Practices Statement and Certification Policy.

CA TECNISIGN CPS complies with the current version of:
a) CA/Browser Forum - Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates- version 1.6.0 (available at https://cabforum.org/baseline-requirements-documents/).
b) CA/Browser Forum - Guidelines For The Issuance And Management Of Extended Validation Certificates – version 1.6.8 (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 inconsistency between this document and these Guidelines, this document prevails.

1.1 Overview

This CPS applies to CA TECNISIGN .

CA TECNISIGN Subordinate CAs operate their CAs under CA TECNISIGN DPC and CP, issuing end-user certificates.

Registry Authorities (RAs) are entities that authenticate CA TECNISIGN certificate orders.

CA TECNISIGN and Affiliates can act as RAs for the certificates they issue. VALID and Affiliates also enter into contractual relationships with companies wishing to manage their own certificate orders. These corporate clients act as RAs, authenticating certificate orders for themselves and their nominees. VALID or Affiliates shall issue these authenticated certificate orders.

Depending on the type of certificate, Digital Certificates MAY be used by Subscribers to protect websites, digitally sign codes or other content, digitally sign documents and/or emails. The person who ultimately receives a signed document or communication, or accesses a protected website is designated as a Trusted Party, i.e. he or she is relying on the certificate.

The Trusting Party MUST trust a certificate under the terms of the Trusting Party Agreement listed on CA TECNISIGN website.

1.2 Document name and ID

This document is CA TECNISIGN Certification Practices Statement (CPS).

1.2.1 CABF Policy Identifier

Not applicable.

1.3 Community (PKI participants)

CA TECNISIGN's e-signature certificate services are incorporated into a trusted infrastructure. Basically: Certification Authority (PSC), Registration Authorities (RA), Subscriber, third parties that depend on certificates and Accreditation Entity.

1.3.1 Certification Authority

CA or Certification Authority (CA) is the organization responsible for the Certificate creation, issuance, revocation and management.

The term also applies to Root CAs and Subordinate CAs.

The certification practices and procedures used by CA TECNISIGN are described in its Certification Practices Statement (CA TECNISIGN CPS), which is published at the following address:

http://www.tecnisign.net/ac_tecnisign/dpc-ac-tecnisignv1.pdf

1.3.2 Registry Authorities

A Registry Authority (RA) is an entity that performs identification and authentication for certificate applicants to end users, initiates or transfers end user certificate revocation orders, and approves renewal orders on behalf of CA TECNISIGN. In the case of a third party acting as a registrar, the activity must be carried out in full compliance with the mandate agreement and this Certification Practices Statement. VALID CAN act as a RA for issuing certificates.

Third Parties that establish a contractual relationship with VALID MAY operate their own RA and authorize the issuance of certificates by CA TECNISIGN. Third party RAs MUST comply

with all requirements of this CA TECNISIGN CPS, and the terms of their corporate service agreement with CA TECNISIGN. The RAs MAY, however, implement more restrictive practices based on their internal requirements.

With the exception of sections 3.2.2.4 and 3.2.2.5, CA TECNISIGN MAY delegate the performance of all or any part of Section 3.2 requirements to a Third Party, provided that the process complies with all Section 3.2 requirements.

Before VALID authorizes a Third Party to perform a RA function, VALID MUST contractually require that the Third Party:

(1) Meets Section 5.3.1 qualification requirements, when applicable to RA function;

(2) Saves the documentation according to Section 5.5.2;

(3) Complies with the other provisions of these Requirements applicable to the function; and

(4) Complies with CA TECNISIGN policies (CPS and CP).

VALID may designate a company as RA to verify certificate orders from this organization itself.

1.3.3 Candidate

The people who agree to order a digital certificate fill out the order form and provide all history required by law and this CPS to reliably prove their identity.

1.3.4 Subscribers

The subscribers (or Signatories or Owners) include all end-users (including entities) of the certificates issued by CA TECNISIGN. A subscriber is the entity named as the end user of a certificate. Subscribers MAY be individuals, organizations, or infrastructure components, such as firewalls, routers, trusted servers, or other devices used to secure communications within an organization.

In some cases, the certificates are issued directly to individuals or entities for their own use. However, there are usually other situations where the party requiring a certificate is different from the “subject” to whom the certificate applies. For example, an organization MAY demand certificates for its employees to allow them to represent the organization in electronic transactions/businesses. In such situations, the entity that subscribes the issuance of certificates (i.e. paid by them, whether through subscription of a specific service or the issuer itself) is different from the entity that is the “subject” of the certificate (generally, the certificate holder).

Two different terms are used in CA TECNISIGN Certificate Policy (CP) to distinguish between these two roles "Subscriber" is the entity that contracts VALID to issue credentials and; SUBJECT is the person to whom the credential is bound. The Subscriber undertakes ultimate responsibility for the use of the certificate, but the SUBJECT is the individual who is authenticated when the certificate is submitted.

When “SUBJECT” is used is to indicate a distinction of the Subscriber. When “Subject” is used, it may mean only the Subscriber as a distinct entity, but may also use the term to encompass both. The use context in CP shall invoke the correct understanding.

CAs are also technically certificate subscribers within CA TECNISIGN, either as a CA that issues a self-signed certificate for itself, or as a CA that issued a Certificate for a higher CA. The references to “end entities” and “subscribers” in CA TECNISIGN Certificate Policy (CP), however, apply only to end users.

1.3.5 Trusted Parties

The Trusted Party is an individual or legal entity that relies on a certificate and/or digital signature issued by CA TECNISIGN. The Trusted Third Party may or may not be a subscriber within CA TECNISIGN.

The party who trusts must have mechanisms that allow validating, is an authentic certificate, and if such certificate was valid at the time the signature on the document was produced.

1.3.6 Accrediting Entity

The General Directorate of Intellectual Property (DIGEPIH) that is within the Institute of Property (IP). The E-signature Law was approved by the National Congress under decree number 149-2013, dated July 30, 2013.

1.3.7 Other participants

Not applicable.

1.4 Certificate Owners

Individuals or legal entities, whether public or private, national or foreign, that meet the requirements of this CPS and the applicable Certificate Policies, may be Certificate Owners. The certificates can be used by individuals and legal entities in equipment or applications.

In the case of the certificate owner is a legal entity, an individual shall be designated as the responsible for the certificate, who shall be the private key holder.

The legal representative of the legal entity or one of its legal representatives shall be MANDATORILY designated as responsible for the certificate.

1.4.1 Applicability

1.4.1.1 Appropriate uses of the certificate

1.4.1.2 Certificates issued to individuals

Certificates issued to individuals are typically used to sign and encrypt emails and to authenticate applications (client authentication).

1.4.1.3 Certificates issued to organizations

Legal entity certificates are issued to organizations after authentication that the organization legally exists and that other Organization attributes included in the certificate (excluding unverified subscriber information) are authenticated, and its ownership of an internet or email domain.

1.5 Policy Management

1.5.1 Organization that manages the document

VALID CERTIFICADORA DIGITAL S.A

Avenida Paulista, 2064 – 15. Andar –

São Paulo/SP Brasil

1.5.2 Contact Information

Standards and Compliance

VALID CERTIFICADORA DIGITAL

Avenida Paulista, 2064 – 15. Andar –

São Paulo/SP Brasil

Telephone: (55) 11-2575-6800

Email: pki.compliance@valid.com

1.5.3 Person who determines the adequacy of CPS as a policy

CA TECNISIGN Policy Management Department (PMD), named as "Standards and Compliance" determines the adequacy and applicability of this CPS.

1.5.4 CDS approval procedure

Approval of this CPS and subsequent modifications shall be made by the Management Policy (PMD). The changes MUST appear in the form of a document that contains an altered form of the CPS or an update history.

The modified versions shall be available at: http://www.tecnisign.net/ac_tecnisign/dpc-ac-tecnisignv1.pdf

Updates replace any designated or conflicting layout of this version for CPS.

1.6 Definitions and Acronyms

1.6.1 Definitions

Refer to appendix A for a table of definitions.

1.6.2 Acronyms

Refer to appendix A for a table of Acronyms.

1.6.3. References

Refer to appendix B to consult the reference list.

1.6.4. Conventions

The keywords "MUST", "MUST NOT", "MANDATORY", "SHALL/SHOULD", "SHALL/SHOULD NOT", "RECOMMENDED", "MAY/CAN/COULD" and "OPTIONAL" in this requirements should be interpreted in accordance with RFC 2119.

2. Publication and Repository Responsibilities

2.1 Repository

CA TECNISIGN is responsible for maintaining an online public access repository, as well as revocation information on issued Certificates. CA TECNISIGN repository is available for consultation at: http://www.tecnisign.net

2.2 Publication of Certificate Information

CA TECNISIGN and Affiliates maintain a web-based repository that allows Third Parties to make online consultations on Certificate revocation and other status information. Any exception to this SHALL be approved by PMD on a case-by-case basis and MUST be documented in the appropriate CPS. VALID and Affiliates provide Trusted Parties with information on how to find the appropriate repository to verify the Certificate status and, if the Online Certificate Status Protocol (OCSP) is available, how to find the OCSP respondent.

CA TECNISIGN publishes the Certificates it issues on behalf of its own CAs and subordinate CAs. After the Certificate revocation of an end user, VALID publishes a notice of such revocation in the repository. In addition, VALID issues Lists of Certificate Revocation Lists (LCRs) and, if available, provides Online Certificate Status Protocol (OCSP) services for its own CAs and subordinate CAs.

VALID shall publish a current version of the following documents and its repositories:

- This CA TECNISIGN CPS;
- CA TECNISIGN CP;
- Subscriber agreements; and
- Trusted Party Agreements.

VALID ensures that its repository is accessed online 24 hours a day, 7 days a week (24X7), and that its CPS and/or CP disclose CA TECNISIGN business practices, as required by "WebTrust for CAs" and ETSI TS 102 042 and ETSI EN 319 411-1.

2.3 Publication time and frequency

CA TECNISIGN develops, implements, enforces and at least annually updates its policies (CPS and CP).

Updates of Subscriber Agreements and Trusted Third Party Agreements are published as required. The certificates are published after the issue. Certificate status information is published in accordance with the provisions of this CPS.

2.4 Access Controls in Repositories

VALID and Affiliates do not intentionally use technical means to limit access to their policies, status information or CRL. CA TECNISIGN and Affiliates, however, may require people to agree to a Third Party Agreement as a condition of accessing OCSP or CRL. CA TECNISIGN and Affiliates must implement controls to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3. Identification and Authentication

Identity authentication is carried out in the physical presence of the applicant at the Registry Authority (RA). The identification of the certificate applicants and owners is conducted in accordance with the rules and procedures included in this CPS section.

3.1 CERTIFICATE ORDER VALIDATION

The Registry Authorities (RA) bound to CA TECNISIGN shall use the following requirements and procedures to carry out the following procedures:

a) confirmation of an individual identity: proof that the person who presents himself/herself as the owner of the individual certificate is actually the person whose data is included in the submitted documentation and/or biometrics presented, and any type of power of attorney for that purpose shall be forbidden;

In the case of a legal entity, prove that the individual who presents himself/herself as its representative is actually the one whose data is included in the documentation presented, and the power of attorney shall only be allowed if the constitutive act expressly provides such possibility, and must, therefore invest publicly and with expiration of up to ninety (90) days. The person responsible for the use of the legal entity digital certificate must appear in person, and any kind of power of attorney for this purpose shall be forbidden;

b) confirmation of the organization identity: proof that the documents submitted effectively refer to the legal entity holding the certificate and that the person who presents himself/herself as legal representative of the legal entity actually has such attribution;. and

c) issuance of the certificate: verification of the certificate order data with those included in the documents presented and release of the certificate issuance in CA TECNISIGN system.

3.1.2 CERTIFICATE ORDER VERIFICATION

Confirmation of the validation made, observing that it must be mandatorily performed:

a) by a registry agent other than the one who performed the validation step;

b) in one of RA technical facilities duly authorized to operate; and

c) only after receiving in RA technical facility a copy of the documentation presented in the validation step.

3.2. Authentication of an Individual Identity

Confirmation of an Individual identity is carried out through the physical presence of the person concerned, based on legally accepted personal identification documents and the biometric identification process.

3.2.1. Documents for the purpose of identifying an individual

The identification and confirmation of an individual identity is carried out through the physical presence of the person concerned, based on legally accepted personal identification documents.

The following documentation in its original version shall be submitted for the purpose of identifying the individual ordering the certificate:

a) National identity document;
b) Passport; and
c) Photograph of applicant's face;
d) Fingerprints of the certificate applicant.
e) Proof of residence or domicile, issued no more than three (3) months from the date of validation in person
f) Other allowable by law.

3.2.2. Information included in the certificate issued to an individual

It is mandatory to fill in the following individual certificate fields with information included in the documents submitted:

a) full name, without abbreviations;

b) identification of the document presented

c) identification document number.

d) Full address

3.3 Authentication of an organization identity

Individual shall be designated as the person responsible for the certificate, who shall be the holder of the private key. Preferably, the legal representative of the legal entity or one of its legal representatives shall be designated as the responsible for the certificate.

The confirmation of the legal entity and individual identities is made in the following terms

a) physical presence of the person responsible for the use of the certificate and signature of the term of representativeness of the certificate

physical presence of the legal representative(s) of the legal entity and signature of the term of representativeness of the certificate.

3.3.1. Documents for the purpose of identifying an organization

Confirmation of an organization identity is made upon submission of at least the following documents:

a) Constitutive act duly registered with the competent body

b) Documents of its administrators' election, when applicable; and

c) proof of company's registration.

3.3.2 Information included in the certificate issued to an organization

It is mandatory to fill in the following fields of an organization's certificate, with the information included in the documents submitted:

a) Corporate name, without abbreviations

b) National Tax Registry (RTN)

c) Full name of the certificate holder, without abbreviations

d) Identification of the document presented by the person in charge

3.4 Identification and Authentication for new key order

Prior to the expiration of the existing Subscriber Certificate, the Subscriber must obtain a new Certificate to maintain the use continuity of the Certificate. CA TECNISIGN and RAs generally require the Subscriber to generate a new pair of keys to replace the expiring pair of keys (technically defined as "renewal"). Renewal occurs in the fact that the old certificate is being replaced with a new Certificate.

3.4.1. Identification and Authentication for Renewal

The renewal procedures ensure that the person or organization that wishes to renew an end-user Subscriber Certificate is, in fact, the previous Certificate Subscriber.

3.4.1.2. Identification and Authentication for Renewal after Revocation

Re-certification /Renewal after revocation is not allowed.

4. Operational Requirements of the Certificate Life Cycle

4.1. Certificate Order

4.1.1 Who can submit a certificate order

Below is a list of people who can submit certificate orders:

- Any person who is the subject of the certificate,
- Any authorized representative of an Organization or entity, and
- Any authorized representative of a CA.

4.2 Certificate Order Process

This CPS item describes the operational requirements and procedures established by CA TECNISIGN and RAs bound to the certificate issuance orders. RA shall carry out the identification and authentication of all digital certificate applicants' information. These requirements and procedures comprise:

a) the proof of identification attributes included in the certificate, according to item 3.1;

b) the authentication of the registrar responsible for the certificate issuance and revocation orders; e

c) the signature, on the term of representativeness of the certificate by the certificate owner and the person responsible for the certificate use, in the case of a legal entity.

4.2.1 Processing Time for Certificate Orders

CAs and RAs execute the process within a reasonable time from receipt. There is no stipulated time to complete the processing of an order.

A certificate order remains active until it is rejected.

4.3 Certificate Issuance

Accepts only the digital certificates when the applicant identity is reliably verified as indicated in this Certification Practice Statement. After the procedures described in item 4.2, CA TECNISIGN issues the certificate in its system and notifies the owner by email indicating the method for the certificate withdrawal.

4.4 Certificate Acceptance

The certificate owner or the responsible individual verifies the information included on the certificate and accepts it if the information is complete, correct and true. Otherwise, the certificate owner cannot use the certificate and must immediately order its revocation. Upon accepting the certificate, the certificate owner:

- agrees with the responsibilities, obligations and duties in this CPS and the corresponding CP;
- ensures that, with his/her knowledge, no unauthorized person had access to the private key associated with the certificate;
- states that all information included in the certificate, provided in the order, is true and is reproduced in the certificate correctly and fully.

Acceptance of all issued certificate is implicitly declared by the owner on the first use of the certificate.

4.5 Pair of Keys and the use of the Certificate

The Private Key usage corresponding to the public key in the certificate SHALL only be done when the Subscriber agrees to the Subscriber Agreement and accepts the certificate. The certificate SHALL be legally used in accordance with VALID Subscriber Agreement, the terms of this CPS. The use of the certificate MUST be consistent with the extensions of KeyUsage field included in the certificate.

The subscribers SHALL protect their private Keys from unauthorized usage and will no longer use the private key after the certificate expiration or revocation. Parties other than the Subscribers SHOULD NOT file the Subscriber's Private Key, except as set forth in section 4.12.

4.5.1 Use of Trusted Parties' public key and certificate

Trusting Parties MUST accept the applicable Trusting Parties Agreement terms as a condition for relying on the certificate.

Trust in a certificate MUST be reasonable under the present circumstances. If the circumstances indicate the need for additional guarantees, the Third Party MUST obtain such guarantees so that the trust is considered reasonable.

Before any act of trust, Trusted Parties shall independently assess:

- the adequacy of the use of the Certificate for each purpose and determine whether the Certificate will, in fact, be used for the appropriate purpose, which is not prohibited or limited by this CP. CA TECNISIGN, CAs e ARs are not responsible for assessing the adequacy of using a Certificate.
- that the certificate is being used in accordance with the KeyUsage extension included in the certificate.
- certificate status of all CAs of the certificate issuance chain. If any of the Certificates of the Certification Chain has been revoked, the Third Party is solely responsible for investigating whether the digital signature was performed by an end-user Certificate prior to the revocation of any certificate of the Certification Chain. Any assumption is at the sole risk of the trusted party.

Assuming that the use of the Certificate is appropriate, the Trusted Parties shall use the appropriate software and/or hardware to perform the digital signature verification or other cryptographic operations that they wish to perform, on the condition that they rely on the Certificates involved in each operation. Such operations include the identification of the Certification Chain and verification of digital signatures on all certificates in the certificate chain.

4.6 Certificate Re-certification

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

A CA TECNISIGN does not allow certificate renewal.

4.7 Certificate Renewal

Certificate renewal is the issuance of a new certificate using a new public key. CA TECNISIGN requests the Applicant to send a new certificate order to issue a new certificate.

4.7.1 Circumstances for Certificate Renewal

Prior to the expiration of the existing Subscriber Certificate, the Subscriber must renew the certificate to maintain the use continuity of the Certificate. A certificate can also be renewed after expiration.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

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

Certificate modification shall be deemed to be a certificate issuance pursuant to Section 4.1.

4.9 Certificate Suspension and Revocation

4.9.1 Circumstances for Revocation

4.9.1.1. Reasons to Revoke a Subscriber Certificate

Only under the circumstances listed, the subscriber certificate shall be revoked by CA TECNISIGN (on behalf of the Subscriber) and published in an LCR.

An end-user certificate shall be revoked if:

1. The Subscriber requests in writing that CA TECNISIGN revokes the Certificate;
2. The Subscriber notifies CA TECNISIGN that the original certificate order was not authorized by him, and that he did not grant authorization retroactively;

3. CA TECNISIGN, a RA, the Client or Subscriber obtains evidence that the Subscriber's Private Key corresponding to the Certificate Public Key has been compromised or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
4. CA TECNISIGN, a RA, the Client or Subscriber obtains evidence that the Certificate has been misused;
5. . CA TECNISIGN, a RA or the Client is informed that the Subscriber has violated one or more of its material obligations set forth in the Subscriber Agreement or Terms of Use;
6. CA TECNISIGN, a RA or the Client is informed that a material change in the information included in the Certificate;
7. CA TECNISIGN, a RA or the Client is informed that the Certificate has not been issued in accordance with the requirements of this CPS or CA TECNISIGN CP;
8. CA TECNISIGN determines that any information that appears on the Certificate is inaccurate or misleading;
9. CA TECNISIGN ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
10. CA TECNISIGN's right to issue Certificates under these Requirements has expired or has been revoked or terminated, unless CA TECNISIGN has entered into agreements to continue to maintain the LCR / OCSP Repository;
11. CA TECNISIGN is informed of a possible compromise of the Private Key of the Subordinate CA used to issue the Certificate;
12. Revocation is required by CA TECNISIGN CPS/CP;
13. The Certificate technical content or format presents an unacceptable risk to application Software Vendors or Trusting Parties[1];
14. The Subscriber Agreement with the Subscriber has been wound up;
15. Affiliation between a Corporate Client and a Subscriber is terminated or otherwise has been terminated;
16. The Subscriber has not send payment when due;
17. The Subscriber identity has not been verified successfully in accordance with section 3.3.2; or
18. The use of such certificate represents risks to CA TECNISIGN.

19. Upon death of the subscriber;
20. By court order or competent administrative authority; and
21. Any other legal cause provided in the certification practice statement.

If the subscriber does not order the certificate revocation in case of presenting the above situations, he/she shall be liable for losses or damages incurred by bona fide third parties who have relied on the certificate contents.

CA TECNISIGN and/or RA when considering whether the use of certificate is harmful evaluates, among other things, the following:

- The nature and number of the complaints received

- The identity of the author(s)
- The relevant legislation in force
- The responses to the alleged harmful use of the Subscriber

CA TECNISIGN and Subscriber Agreements require the final user to promptly notify CA TECNISIGN of a known or suspected compromise of its private key.

CA TECNISIGN or RA MAY revoke an Administrator Certificate if the Administrator authority to act as Administrator has been wound up or terminated.

The Subscriber Agreements require the end-user to immediately notify a RA of a known or suspected compromise of its private key.

4.9.1.1.1 CABF Requirements

CA TECNISIGN shall revoke a Certificate within 24 hours.

4.9.1.2. Reasons to revoke a Subordinate CA certificate

The issuing CA must revoke a Subordinate CA certificate within seven (7) days if one or more of the following events occurs:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies the Issuing CA that the original certificate order was not authorized by it and it did not grant authorization;
3. The issuing CA obtains evidence that the subordinate CA private key corresponding to the Certificate public has compromised 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 has been misused;
5. The issuing CA is informed that the Certificate has not been issued in accordance with or that the Subordinate CA has not complied with this CP or the applicable CPS;
6. The issuing CA determines that any information that appears on 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 or subordinate CA right to issue certificates under these requirements has expired or is revoked or terminated, unless the issuing CA has made arrangements to continue to maintain CRL / OCSP Repository;
9. The revocation is required by the Issuing CA CP or CPS; or

The Certificate technical content or format presents an unacceptable risk to application Software Vendors or Trusting Parties.

4.9.2 Who can order revocation

The Subscriber, RA or Issuing CA may initiate the revocation and MAY send Certificate Issue Reports, informing the issuing CA of the reasonable cause to revoke the certificate.

Individual subscribers may request revocation of their own individual certificates through an CA TECNISIGN authorized representative or a RA.

In the case of organization Certificates, a duly authorized representative of the organization SHALL have the right to order revocation of Certificates issued to the organization.

An CA TECNISIGN duly authorized representative, an Affiliate or an RA MUST have the right to order revocation of an RA Administrator Certificate.

The entity that approved the subscriber certificate application SHALL also have the right to revoke or order revocation of the subscriber's certificate.

Only CA TECNISIGN has the right to order or initiate the revocation of the Certificates issued for its own CAs.

4.9.2.1 Procedure for Ordering Revocation of an End User Certificate

Prior to revocation of a Certificate, VALID checks whether the revocation was requested by the Certificate Subscriber or by the entity that approved the Certificate Application. Acceptable procedures for authenticating Subscriber revocation orders include:

1. Having the Subscriber of certain types of certificate to present the Subscriber Challenge Phrase (or an equivalent) and revoke the Certificate automatically if it matches the Challenge Phrase (or equivalent) in the record,
2. Receiving a message allegedly from the Subscriber ordering revocation and containing a verifiable digital signature with reference to the Certificate to be revoked, and
3. Communication to the Subscriber providing reasonable assurances that the person or organization requesting the revocation is, in fact, the Subscriber. This communication, depending on the circumstances, may include one or more of the following: telephone or email. In both cases, a copy of the government photo ID of the domain owner or controller is required. In addition, the order confirmation can be made through telephone contact or other means.

CA/RA administrators have the right to order the revocation of Subscribers' Certificates in CA/RA Subdomain. CA TECNISIGN Affiliates SHALL authenticate the Administrators identity through access control using SSL and client authentication before allowing them to perform revocation functions.

CAs orders to revoke a CA Certificate must be authenticated by its Top Entities to ensure that CA has in fact ordered the revocation.

4.9.2.1.1 CABF Requirements

CA TECNISIGN MAINTAINS a continuous capacity of 24x7 to accept and Responding to revocation orders and related issues.

4.9.3 Grace Period of the Revocation Order

The revocation orders MUST be sent as soon as possible within a commercially reasonable time.

4.9.4 Term in which CA must process the revocation order

Commercially reasonable measures are taken to process the revocation orders without delay.

CA TECNISIGN begins investigating a Certificate Issue Report within 24 hours of receipt and decides whether revocation or other appropriate action is justifiable based on at least the following criteria:

1. The nature of the alleged problem;
2. The number of Issue Reports received regarding a particular certificate or signatory;
3. The entity that submitted the complaint; and
4. The relevant legislation.

4.9.5 Revocation Verification Requirements for Trusting Parties

Trusted Third Parties SHALL verify the Certificate status in which they wish to trust. Trusted Parties CAN verify the Certificate status by consulting the latest VALID CA CRL.

Trusted Parties can verify the Certificate status by consulting the most recent CRL of the CA that issued the Certificate on which the Trusted Party wishes to trust. Alternatively, Trusted Parties may meet this requirement by verifying the certificate status by using the applicable Web-based repository or using OCSP (if available). The CAs should provide Trusted Parties with information on how to find the appropriate CRL, web-based repository or OCSP respondent (when available) to check revocation status.

A "CRL Reference Table" is posted in CA TECNISIGN Repository to allow Trusted Parties to determine CRL location for the relevant CA.

4.9.6 CRL Issue Frequency

CA TECNISIGN CRLs must be issued at least once a year, but also within 24 hours whenever a CA Certificate is revoked. Any deviation from this general policy MUST obtain PMD approval and be published in the appropriate CPS.

4.9.6.1 Subscriber Certificate Status Requirements

CA TECNISIGN SHALL update and reissue the CRLs at least once every 7 days, and the amount of nextUpdate field MUST NOT be more than 10 days in addition to the amount of thisUpdate field.

4.9.6.2 Subordinate CA Certificate Status Requirements

VALID SHALL update and reissue the CRLs at least:

a) Once every 12 months and

b) Within 24 hours after revocation of a Subordinate CA Certificate, and the amount of nextUpdate field MUST NOT be higher than 12 months in addition to the amount of thisUpdate field.

4.9.7 Maximum publication for CRLs

The CRLs are posted to VALID repository within a commercially reasonable time after generation. This is usually done automatically within seconds after generation.

4.9.8 CRL Retention Period

a) CRLs and digital signature certificates issued by VALID ROOT CA are permanently retained for historical consultation purposes;
b) The copies of the identification documents submitted at the time of application and the revocation of the certificates and the terms of ownership and responsibility must be kept for at least ten days from the date of expiration or revocation of the certificate; and
c) the other information, including audit records, is retained for at least six (6) years.

4.9.9 Online Revocation Availability / Status Verification

Online revocation and other certificate status information are available through a web-based repository and, when offered, the OCSP. Processing Centers must have a web-based repository that allows Trusted Parties to make online revocation consultations and other Certificate status information. A Processing Center, as part of its agreement with a Service Center, must host such a repository on behalf of the Service Center. Processing Centers provide Trusted Parties with information on how to find the appropriate repository to verify the status of the Certificate and, if OCSP is available, how to find the correct OCSP respondent.

OCSP responses must comply with RFC6960 and/or RFC5019. OCSP responses should:
1. Be signed by VALID or
2. Be signed by an OCSP Respondent whose certificate is signed by CA TECNISIGN. OCSP signature certificate MUST contain an id-pkix-ocsp-nocheck type extension, as defined by RFC6960.

4.9.10 Requirements for online revocation verification

A confident party MUST check the status of a certificate on which he/she wishes to trust. If a Trust Party does not verify the status of a Certificate on which the Trusted Party wishes to trust by consulting the latest CRL, the Trusted Party SHALL check the status of the Certificate

by consulting the applicable repository or by requesting Certificate status using the applicable OCSP respondent (where OCSP services are available).

VALID supports an OCSP feature using GET method for Certificates issued in accordance with these Requirements.

If OCSP respondent receives a certificate status order that has not been issued, the respondent shall not respond with a "good" status.

VALID monitors the respondent for such orders as part of their security response procedures.

4.9.11 CABF Requirements for OCSP

4.9.11.1 Certificate Status for Subscriber Certificates

CA TECNISIGN shall update the information provided through an online Certificate Status Protocol at least every 4 days. OCSP responses from this service MUST have a maximum expiration time of 10 days.

4.9.11.2 Certificate Status for Subordinate CA Certificates

CA TECNISIGN shall update the information provided through an Online Certificate Status Protocol at least (i) every 4 days and (ii) within 1 hour after the revocation of a Certificate.

4.9.12 Other forms available for revocation disclosure

Not applicable.

4.9.13 Special Requirements Related to Key Commitment

Involved with CA TECNISIGN the Participating Trusted Parties MUST be notified of a real or suspected CA private key commitment using commercially reasonable efforts. VALID must notify potential trusting parties if it discovers, or has reason to believe, that there has been a private key commitment of one of its own CAs or one of the CAs within its subdomain.

4.9.14 Circumstances for suspension

Not applicable.

4.9.15 Who can order suspension

Not applicable.

4.9.16 Procedure for Ordering Suspension

Not applicable.

4.9.17 Limit Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The status of the public certificates is available through the CRL through CA TECNISIGN website (at a URL specified in the CA CPS) and through the OCSP response (where available).

The revocation entries in a CRL or OCSP Response SHOULD NOT be removed until the "Expiration Date" of the revoked Certificate.

4.10.2 Service Availability

CA TECNISIGN operates and maintains its CRL capacity and OCSP with sufficient features to provide a response time of ten seconds or less, under normal operating conditions.

CA TECNISIGN maintains a 24x7 online Repository to automatically check the current status of all non-expired certificates issued by it.

CA TECNISIGN maintains 24x7 availability to Respondent internally to a high priority Certificate Issue Report and, where appropriate, forward such claim to law enforcement authorities and/or revoke a Certificate that is the object of such claim.

4.10.3 Optional Features

OCSP is an OPTIONAL status service feature that is not available for all products and MUST be specifically activated for certain products.

4.11 End of Subscription

A subscriber to terminate a subscription of a certificate issued by CA TECNISIGN must:

- Allow its certificate to expire without renewing or re-certifying such certificate
- Revoke its certificate before the certificate expiration without replacing it.

4.12 Key Custody and Recovery

No CA TECNISIGN participant MAY keep copy of CA, RA or end-user private keys.

5. Facilities, Management and Operational Controls

CA TECNISIGN develops, implements and maintains a comprehensive security program designed to:

1. Protect the confidentiality, integrity and availability of data and Certificate Management processes;
2. Protect against threats or risks to the confidentiality, integrity and availability of the certificate data and Certificate Management processes;

3. Protect against unauthorized or illegal access, use, disclosure, change or destruction of any certificate data and Certificate Management processes;
4. Protect against accidental loss or destruction or damage to certificate data and Certificate Management processes; and
5. Comply with all other legal security requirements applicable to CA TECNISIGN.

The Certificate Management Process includes:

1. physical security and environmental controls;
2. integrity control system, including configuration management, integrity maintenance and code reliability, and malware detection/prevention;
3. network security and firewall management, including port restrictions and IP address filtering;
4. user management, assignments separated by trust functions, awareness, sensibilization and training; and activities and inactivity deadlines to provide individualized accountability; and
5. control of logical Accesses, activity log and inactivity deadlines to provide individualized accountability.

CA TECNISIGN security program includes an annual risk assessment to:

1. Identify predictable internal and external threats that may result in unauthorized access, disclosure, misuse, change or destruction of any certificate data and Certificate Management processes;
2. Evaluate the likelihood and potential damage of these threats, taking into account the sensitivity of the certificate data and Certificate Management processes; and
3. Evaluate the sufficiency of the policies, procedures, information systems, technology and others that CA TECNISIGN has in place to combat these threats.

Based on the risk assessment, CA TECNISIGN develops, implements and maintains a security plan consisting of security procedures, measures and products designed to achieve the objectives set out above and to manage and control the risks identified during the risk assessment, proportional to the sensitivity of the certificate data and Certificate Management processes.

The security plan necessarily includes administrative, organizational, technical and physical safeguards appropriate to the sensitivity of the certificate data and Certificate Management Processes.

The security plan shall also take into account the technology then available and the costs of implementing the specific measures, and implement a reasonable and adequate level of security for damage that may result from a breach of security and the nature of the data to be protect.

CA TECNISIGN develops, implements and maintains a comprehensive security program designed to:

6. Protect the confidentiality, integrity and availability of Certificate Management data and processes;
7. Protect against threats or risks to confidentiality, integrity and availability of certificate data and Certificate Management processes;
8. Protect against unauthorized or illegal access, use, disclosure, change or destruction of any certificate data and Certificate Management processes;
9. Protect against accidental loss or destruction or damage to certificate data and Certificate Management processes; and
10. Comply with all other legal security requirements applicable to CA TECNISIGN.

The Certificate Management Process includes:

6. physical security and environmental controls;
7. integrity control system, including configuration management, integrity maintenance and code reliability, and malware detection/prevention;
8. network security and firewall management, including port restrictions and IP address filtering;
9. user management, assignments separated by trust functions, awareness, sensibilization and training; and activities and inactivity deadlines to provide individualized accountability; and
10. control of logical Accesses, activity log and inactivity deadlines to provide individualized accountability.

CA TECNISIGN security program includes an annual risk assessment to:

4. Identify predictable internal and external threats that may result in unauthorized access, disclosure, misuse, change or destruction of any certificate data and Certificate Management processes;
5. Evaluate the likelihood and potential damage of these threats, taking into account the sensitivity of the certificate data and Certificate Management processes; and
6. Evaluate the sufficiency of the policies, procedures, information systems, technology and others that CA TECNISIGN has in place to combat these threats.

Based on the risk assessment, CA TECNISIGN develops, implements and maintains a security plan consisting of security procedures, measures and products designed to achieve the objectives set out above and to manage and control the risks identified during the risk assessment, proportional to the sensitivity of the certificate data and Certificate Management processes.

The security plan necessarily includes administrative, organizational, technical and physical safeguards appropriate to the sensitivity of the certificate data and Certificate Management Processes.

The security plan shall also take into account the technology then available and the costs of implementing the specific measures, and implement a reasonable and adequate level of security for damage that may result from a breach of security and the nature of the data to be protect.

5.1 Physical Controls

CA TECNISIGN implemented VALID GLOBAL physical security policy that supports the security requirements of this CPS. Compliance with these policies is included in CA TECNISIGN independent auditing requirements described in Section 8.

CA TECNISIGN Physical Security Policy contains sensitive security information and is only available upon agreement with VALID GLOBAL. An overview of the requirements is described in the following subsections.

5.1.1 Facilities Construction and Location

CA TECNISIGN operations are performed in a physically protected environment that prevents and detects the unauthorized use, access or disclosure of confidential information and systems, whether secret or public.

VALID also maintains disaster recovery facilities for its CA operations. CA TECNISIGN disaster recovery facilities are protected by physical security levels comparable to those of the main CA TECNISIGN facility.

5.1.2 Physical Access

CA TECNISIGN systems are protected by a minimum of 4 layers of physical security, with access to lower levels being prerequisites for access to higher levels.

Restrictive physical access privileges progressively control access to each layer.

5.1.2.1. CA Operating Sensitive Activities

Any activity related to the certificate process life cycle occurs within more restrictive physical levels. Access to each layer requires the use of an employee badge with proximity card. Physical access is automatically recorded and a video is recorded. Additional layers of individual access control are applied through the use of two authentication factors, including biometric factors. Unauthorized persons, including unauthenticated employees or visitors, are not permitted in such protected areas without escort.

The physical security system includes additional layers for key management security that protects both online and offline storage of the cryptographic hardware and key material of CA TECNISIGN. The areas used to create and store cryptographic material are provided with dual control through the use of two authentication factors, including biometric factors. CA cryptographic hardware in Online and Offline mode are protected through the use of locked safes, cabinets and containers.

Access to cryptographic hardware and key material of CA TECNISIGN is limited according to role segregation requirements. The opening and closing of cabinets or other layers of security is recorded for audit purposes.

5.1.3 Energy and Air Conditioning

CA TECNISIGN's secure facilities are equipped with primary and backup equipment of:

- Power systems to ensure continuous and uninterrupted access to electricity and
- Heating / cooling / air conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposure

CA TECNISIGN secure facilities minimize the impact of its systems to water exposure.

5.1.5 Prevention and Protection Against Fire

CA TECNISIGN has taken reasonable precautions to prevent and extinguish fires or other exposures that are harmful to flames or smoke. CA TECNISIGN's fire protection and fire prevention measures are designed to comply with local fire safety regulation.

5.1.6 Media Storage

All media containing production and data software, auditing, archiving, or backup information are stored at CA TECNISIGN facility or in a secure external storage facility with appropriate physical and logical access controls designed to limit access to authorized persons, and protect such media against accidental damage (e.g. water, fire and electromagnetic).

5.1.7 Disposal of paper documents and electronic devices

Sensitive documents and materials are shredded before being discarded. Media used to collect or transmit confidential information is made illegible prior to disposal. Cryptographic devices are physically destroyed or reset according to the manufacturer's orientation prior to disposal.

Other wastes are disposed of in accordance with CA TECNISIGN normal waste disposal requirements.

5.1.8 External (off-site) Security (backup) Facilities

CA TECNISIGN performs routine backups of critical system data, audit log data, and other confidential information. External backup media is physically securely stored using a Trusted third-party storage resource and CA TECNISIGN disaster recovery resource/feature.

5.2 Procedural Controls

5.2.1 Trust Functions

Trust persons include all employees, contractors, and consultants who have access to or control over authentication and cryptographic operations that may materially affect:

- the validation of information in Certificate Orders;
- acceptance, rejection, or other process on lost nodes certificate orders, revocation orders, renewal orders, or requisition information;

- the issuance or revocation of certificates, including persons having access to restricted partitions of CA TECNISIGN repository;
- the information processing or the Subscriber orders.

The following personnel is included among Trust Persons, but they are not limited to:

- cryptographic operations personnel,
- security personnel,
- system administration personnel,
- engineering personnel, and
- executives who are assigned to manage the reliability of the infrastructure.

CA TECNISIGN considers the categories of employees identified in this section as Trust Persons, who have a Trust Position. Persons who need to become Trust Persons must successfully complete the selection requirements set forth in this CPS.

5.2.2 Personnel Controls

5.2.2.1 Number of persons required per task

CA TECNISIGN has established, maintains, and enforces rigorous control procedures to ensure segregation of duties based on job responsibility and to ensure that more than one Trust Person is required to perform sensitive duties.

Control policies and procedures operate to ensure segregation of duties based on work responsibilities. More sensitive tasks, such as cryptographic hardware and CA key material access and management, require a number of Trust Persons.

These internal control procedures are designed to ensure that at least two (2) Trust Persons are required to have any physical or logical access to the devices. Access to CA's cryptographic hardware is rigorously required by multiple Trust Persons throughout their entire life cycle, from receipt of entry and inspection to logical and/or physical destruction. Once a module is activated with the operation keys, other access controls are invoked to maintain control segregation over physical and logical access to the device. Persons with physical access to the modules do not have "Shared Secrets" and vice versa.

Other manual operations require the participation of at least two (2) Trust Persons, or a combination of at least one Trust Person and an automated validation and issuance process. Manual operations for key recovery may optionally require the validation of two (2) authorized administrators.

5.2.3 Identification and Authentication for each profile

For all personnel who needs to become a Trust Person, verification of identity is performed through the physical presence of that person before a Trust Person in the HR or Security area and a reliable verification of their identification. Identity is confirmed through the background check procedures described in Section 5.3.1.

CA TECNISIGN ensures that personnel archives Trust Person status before the areas:

- issue Access credentials and gain access to the facilities;

- issue electronic credentials to access and perform specific functions in CA TECNISIGN, RA or other IT systems.

5.2.4 Functions requiring task segregation

Roles requiring task segregations include (but are not limited to):

- the validation of information in certificate orders;
- acceptance, rejection or other processing of Certificate Orders, revocation orders, key recovery orders or renewal orders or registration information;
- the issuance or revocation of Certificates, including personnel with access to restricted parts of the repository;
- information processing or Subscriber orders;
- the generation, issuance or destruction of a CA certificate; and
- CA loading to production environment.

5.3 Personnel Controls

Persons who need to become Trust Persons must provide proof of background, qualifications and experience necessary to perform competently and satisfactorily the job responsibilities. Background controls are repeated at least every 5 years for the personnel holding trust offices.

5.3.1 Background, qualification, experience and good-standing requirements

Prior to the involvement of any person in the Certificate Management Process, whether as an CA TECNISIGN employee, agent, or independent third party, it MUST verify the identity and reliability of such person. CA TECNISIGN requires personnel seeking to become a Trust Person to provide proof of the background, qualifications and experience necessary to perform their work responsibilities in a competent and satisfactory manner.

5.3.2 Background Check Procedures

Prior to commencement of employment on a Trustworthy Paper, CA TECNISIGN conducts background checks that include the following:

- confirmation of previous employment,
- professional reference check,
- confirmation of the highest or most relevant educational degree obtained,
- search for criminal records, and
- verification of credit/financial records.

Reports containing information on factors revealed in a background check are evaluated by human resources and security personnel, who determine the appropriate course of action in light of the type, magnitude and frequency of the behavior discovered by the background

check. Such actions MAY include measures up to and including cancellation of job vacancies made to candidates for positions of trust or termination of existing trustworthy persons.

5.3.3 Training Requirements

CA TECNISIGN provides training to its employees as well as the necessary training in the work required to perform their job responsibilities competently and satisfactorily.

CA TECNISIGN keeps records of such training. CA TECNISIGN periodically anticipates and enhances its training programs as needed.

CA TECNISIGN training programs are tailored to the individual's responsibilities and include the following topics:

- basic PKI concepts,
- work responsibilities,
- CA TECNISIGN security and operational policies and procedures,
- use and operations of implemented hardware and software,
- reports and handling of incidents and commitments, and
- disaster recovery and business continuity procedures.

5.3.3.1 CABF Requirements for Training and Skill Level

In addition to the requirements of Section 5.3.3, CA TECNISIGN MUST provide all personnel performing information verification tasks with skills training that include:

- authentication and evaluation policies and procedures (including CP and/or CPS),
- common threats to information verification process (including phishing and other social engineering tactics) and
- CABFORUM requirements.

CA TECNISIGN SHALL maintain records of such training and ensure that the staff performing the duties of the Validation Specialist maintains a level of skill that enables them to perform those tasks satisfactorily.

CA TECNISIGN MUST document that each Validation Specialist has the skills required by a task before allowing the Validation Specialist to accomplish this task.

CA TECNISIGN SHALL require that all Validation Specialists are approved in an examination provided by CA TECNISIGN regarding the information verification requirements described in ACBFORUM Requirements.

5.3.4 Recycling Frequency and Requirements

CA TECNISIGN provides refresher training and updates to its employees to the extent and frequency needed to ensure that they maintain the level of knowledge required to perform their job responsibilities competently and satisfactorily.

5.3.5 Work Rotation Frequency and Sequence

Not applicable.

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of CA TECNISIGN policies and procedures. Disciplinary actions MAY even include dismissal measures and are proportionate to the frequency and severity of the unauthorized actions.

5.3.7 Requirements for independent third parties

In limited circumstances, independent contractors or consultants may be used to fill trust offices. Any contractor or consultant is kept in the same functional and safety criteria that apply to CA TECNISIGN employees has a comparable position.

The CERTIFICATE SHALL verify that the Contracted Third Party personnel involved in issuing a Certificate meet the training and skill requirements of Section 5.3.3 and the document retention and logging requirements of Section 5.4.1.

Contractors and independent consultants who have failed to comply with or have not approved the background check procedures specified in Section 5.3.2 of the CPS are permitted access to CA TECNISIGN security facilities only to the extent that they are monitored and supervised directly by trust third parties in all the moments.

5.3.7.1 Guidelines Compliance Obligation

In all cases, CA TECNISIGN MUST contractually obligate each Affiliate, RA, subcontractor and company to comply with all applicable requirements in this CPS, its CP and to execute them as required by VALID itself. CA TECNISIGN SHALL enforce these obligations and internally audit each Affiliate, RA, subcontractor, and company compliance with these requirements annually.

5.3.7.1.2 Responsibility Assignments

As specified in Section 9.8.

5.3.8 Documentation Provided to Personnel

CA TECNISIGN provides its employees with the necessary training and other documentation necessary to perform their job responsibilities competently and satisfactorily.

5.4 Security Audit Procedures

5.4.1 Types of Recorded Events

CA TECNISIGN and each Contracted Third Party SHALL record details of the actions taken to process a certificate request and issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the staff involved. CA TECNISIGN SHALL make these records available to its Qualified Auditor as proof of compliance with CABFORUM requirements.

VALID manually and automatically records the following significant events:

CA key lifecycle management events, including:

- ✓ Generation, backup, storage, recovery, archiving and destruction of keys
- ✓ Cryptographic device lifecycle management events.

CA and Subscriber certificate lifecycle management events, including:

- ✓ Certificate and revocation orders
- ✓ Successful or unsuccessful order processing
- ✓ Generation and issuance of Certificates and CRSs.

Events related to security, including:

- ✓ Successful and unsuccessful attempts to access PKI system
- ✓ PKI actions and security system implemented by VALID CA personnel
- ✓ Read, written or deleted confidential security files or records
- ✓ Changes to the security profile
- ✓ System failure, hardware failure and other anomalies
- ✓ Firewall and router activity
- ✓ Visitor entrance/exit from CA facilities.

Log entries include the following elements:

- ✓ Input date and time
- ✓ Input sequence serial or number for automatic accounting entries
- ✓ Identity of the entity that did the entry in the journal
- ✓ Input description/type.

5.4.1.1 CABF Types of Recorded Requests Events

- ✓ In addition, VALID CA manually or automatically records the following significant events:
- ✓ All verification activities stipulated in CABFORUM requirements and in this CPS;
- ✓ Date, time, telephone number used, persons spoken and final results of verification telephone calls;
- ✓ OCSP responses.

5.5 Archiving Records

5.5.1 Types of archived records

CA TECNISIGN archives:

- All audit data collected under Section 5.4
- Certificate order information
- Certificate order support documentation
- Certificate lifecycle information such as revocation, renewal and application orders.

5.5.2 Retention Period for Archive

CA TECNISIGN retains all documentation related to certificate orders and their verification, certificates and their revocation for at least SEVEN (7) years after any certificate based on such documentation ceases to be valid.

5.5.3 File protection

CA TECNISIGN protects files so only authorized Trust Persons are able to gain access to the file. The file is protected from viewing, modifying, unauthorized deleting or other violation through storage within a Trusted System. The media containing the data file and the applications required to process the data file must be maintained to ensure that the given file can be accessed for the period of time set forth in this CPS.

5.5.4 File backup procedures

CA TECNISIGN makes daily incremental backup of the files of its Certificate issued information and performs full monthly backups. Copies of paper records should be kept in an off-site safe facility.

5.5.5 Record time-stamping requirements

Certificates, CRLs and other revocation bases must contain time and date information.

5.5.6 File data collection system (internal or external)

CA TECNISIGN's file collection systems are internal except for some corporate client RAs. CA TECNISIGN assists its RA of corporate clients by maintaining the audit trail. Therefore, the corporate client RA file collection systems are external.

5.5.7 Procedures for obtaining and verifying file information

Only authorized Trust Person is able to gain access to the files. Information integrity is checked when it is restored.

5.6 Key Exchange

Thirty days before the expiration of the digital certificate, CA TECNISIGN or the linked RA, through the email registered in the certificate order form, informs the owner of the expiration date and instructions for ordering a new certificate.

5.7 Compromise and Disaster Recovery

5.7.1 Procedures for Incident Handling and Compromise

Backups of the following CA information shall be kept in off-site storage and made available in the event of a compromise or disaster:

- certificate order data,
- audit data, and
- database of all certificates issued.

Backups of CA private keys shall be generated and maintained in accordance with Section 6.2.4. CA TECNISIGN maintains backups of previous information of its own CAs.

CA TECNISIGN has an Incident Response Plan and a Disaster Recovery Plan.

CA TECNISIGN documents business continuity and disaster recovery procedures designed to reasonably notify and protect suppliers, subscribers, and application software stakeholders in the event of a disaster, security compromise, or business failure.

CA TECNISIGN does not publicly disclose its business continuity plans, but makes its business continuity plans and security plans available to its auditors upon request.

CA TECNISIGN tests, reviews, and updates these procedures annually.

The business continuity plan includes:

1. The conditions for activating the plan;
2. Emergency procedures;
3. Fallback procedures;
4. Retrieval procedures;
5. A plan maintenance schedule;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery Time Purpose (RTP);
9. Regular tests of contingency plans;
10. CA TECNISIGN plans to maintain and restore its business operations in a timely manner after interruption of failure of critical business processes;
11. A requirement to store critical cryptographic materials in an alternate location;
12. What constitutes an acceptable system disruption and a recovery time;
13. How often backup copies of essential business information and software are taken;
14. The distance from the recovery facilities to the main site of CA TECNISIGN; and
15. Procedures to protect its facilities as much as possible during the time period after a disaster and before restoring a secure environment to the original or remote location.

5.7.2 Computer resources, software and/or data are corrupted

In the event of corruption of computing resources, software and/or data, such occurrence is reported for CA TECNISIGN CA Security incident handling procedures. Such procedures require proper referral, incident investigation, and incident response. If necessary, CA TECNISIGN key commitment procedures or disaster recovery shall be approved.

5.7.3 Entity private key commitment procedures

Following the suspected or proven compromise of CA TECNISIGN private keys, VALID key commitment response procedures are performed by the VALID Incident Response Security team. This team, which includes security, encryption staff, production services personnel, and other representatives of VALID management, evaluates the situation, develops and implements the action plan with the approval of VALID's executive board.

If revocation of CA certificate is required, the following procedures are performed:

- Certificate revocation status is communicated to Trusted Parties through CA TECNISIGN Repository in accordance with Section 4.9.7,
- Commercially reasonable efforts will be made to provide additional notice of revocation to all affected by the revocation of CA TECNISIGN certificate, and
- CA will generate a new key pair according to Section 5.6, except in the case where CA is being extinguished, according to Section 5.8.

5.7.4 Business continuity capacity after a disaster

VALID maintains business continuity plans so that, in case of business interruption, critical business functions can be resumed. VALID maintains a contingency site located in a facility geographically separate from the main site.

The contingency site is equipped to meet the security standards of this CPS.

In the event of a natural or man-made disaster requiring the permanent cessation of operations of VALID primary facilities, the Business Continuity Team and the Operations Incident Management Team shall coordinate with the functional cross management teams to make the decision to formally declare a disaster situation and to manage the incident. Once a disaster situation is declared, restoration of the VALID production services functionality on the contingency site shall begin.

CA TECNISIGN has developed a Business Continuity Plan (BCP) for its managed PKI services, including the CA TECNISIGN PKI service. BCP identifies the conditions for activating the plan and what constitutes an acceptable system interruption and recovery time. BCP defines procedures for teams to reconstitute CA TECNISIGN operations using backup data and backup copies of CA TECNISIGN's key.

Entities operating safe facilities for CA and RA operations develop, test, maintain and, if necessary, implement a Business Continuity Plan (BCP) designed to mitigate the effects of any

natural or man-made disaster. BCP must identify the conditions for activating the plan and what constitutes an acceptable system interruption and recovery time for the restoration of information systems services and key business functions within a defined recovery time objective (RTO).

In addition, BCP shall include:

- ✓ Frequency to make backup copies of essential business information and software,
- ✓ Requirement to store critical cryptographic materials (i.e. secure cryptographic device and activation materials) in an alternate location,
- ✓ Separation distance from the disaster recovery site to the main CA site, and
- ✓ Procedures to protect the facility against Disasters during the time period after a disaster and before restoring a secure environment in the original or remote location.

BCP should include administrative requirements, including:

- ✓ Plan maintenance schedule;
- ✓ Awareness and education requirements;
- ✓ Responsibilities of individuals; and
- ✓ Regular testes of contingency plans.

Disaster recovery sites have the equivalent physical security protections specified by CA TECNISIGN.

CA TECNISIGN may restore or recover essential operations within 48 hours after a disaster with, at least, support for the following functions:

- ✓ Issue of certificate,
- ✓ Revocation of certificate,
- ✓ Publication of revocation information and
- ✓ Providing key recovery information for corporate clients.

CA TECNISIGN disaster recovery database SHALL be synchronized with the production database within the time limits established in Security and Audit Requirements Guide. CA TECNISIGN disaster recovery equipment MUST have physical security protections documented in CA TECNISIGN confidential security policies, which include the application of physical security levels.

5.7.4.1 CABF requirements for Business Continuity Capacity after a Disaster

Not applicable.

5.8 CA or RA extinction

In the event that CA TECNISIGN is required to cease operation, CA TECNISIGN makes a commercially reasonable effort to notify Subscribers, Trusted Parties and other affected termination entities prior to the effective termination of CA. Where CA assignment is required, CA TECNISIGN shall develop an extinction plan to minimize disruption to Clients, Subscribers and Trusted Parties. Such closure plan may address the following, as the case may be:

- Notification to the parties affected by extinction, such as Subscribers, Trusted Parties and Clients, informing them of the CA status,
- Address the cost of such notification,
- Revocation of the Certificate issued to CA TECNISIGN,
- The preservation of CA files and records for the period of time required in this CP ,
- The continuation of Subscriber and Client Support Services,
- The continuation of revocation services, such as the issuance of CRL,
- Revocation of non-expired end-user certificates, if necessary,
- Reimbursement (if necessary) to Subscribers whose valid Certificates have been revoked under the extinction plan, or alternatively, the issuance of replacement certificates by the successor CA,
- Availability of CA private key and hardware tokens containing such private key, if applicable, and
- Procedures needed for the transition of CA services to its successor.

5.9 Data security

Both CAs and other Signatory Authorities are required to comply with the obligations set forth in this Section.

5.9.1 Objectives

VALID develops, implements and maintains a comprehensive security program designed to:

1. Protect the confidentiality, integrity and availability of Certificate Data and Certificate Management Processes;
2. Protect against threats or risks to the confidentiality, integrity and availability of Certificate Data and Certificate Management Processes;
3. Protect itself against unauthorized or illegal access, use, disclosure, change or destruction of any Certificate Data or Certificate Management Processes;
4. Protect against accidental loss or destruction or damage to Certificate Data and Certificate Management Processes; and

5. Comply with all other legal security requirements applicable to CA.

5.9.2 Risk assessment

VALID carries out an Annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that may result in unauthorized access, disclosure, misuse, change or destruction of any certificate data or Certificate Management Processes;
2. Evaluates the likelihood and possible harm of these threats, taking into account the sensitivity of Certificate Data Processes and Certificate Management; and
3. Evaluates the adequacy of the policies, procedures, information systems, technology and other arrangements that CA has in place to combat such threats.

5.9.3 Security Plan

Based on the results of the Annual Risk Assessment, VALID develops, implements and maintains a Security Plan consisting of procedures, measures and security products designed to achieve the established objectives and to manage and control the risks identified during the Risk Assessment, with the sensitivity of Certificate Data Processes and Certificate Management.

The Security Plan includes administrative, organizational, technical and physical safeguards appropriate to the sensitivity of Certificate Data Processes and Certificate Management. The Security Plan takes into account the technology available at the time and the cost of implementing the specific measures and implements a reasonable level of security appropriate to the damages that may result from a security breach and nature of the data to be protected.

6. Security Technical Controls

6.1 Generation of key pair and installation

6.1.1 Generation of key pair

Key pair generation MUST be performed using Trusted 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, corporate clients that use CAs that pre-generate key pairs in end-user Subscriber hardware tokens.

VALID recommends that the key pair generation of the Automated Administration server be performed using a FIPS 140-1 level 2 certified cryptographic module or another similar standard used in Brazil.

Generation of Subscriber key pairs is usually performed by the Subscriber. Subscriber generally uses a FIPS 140-1 level 1 certificate cryptographic module provided with its browser software for key generation. For server Certificates, the Subscriber generally uses the key generation utility provided with the web server software.

6.1.1.1. CABF CA key pair generation requirements

For root CA key pairs created that are (i) used as root CA key pairs, or (ii) key pair generated for a subordinate CA other than the root CA operator or an affiliate of the root CA,

1. prepare and follow a key generation script,

2.have a qualified auditor to witness the process of generating the root pair of the root CA or recording a video of the entire process of generating CA root key pair, and

3.have a Qualified Auditor issue a report stating that CA followed its key ceremony during the key and certificate generation process and the controls used to ensure the key pair's integrity and confidentiality.

For other CA key pairs that are for the root CA operator or an Affiliate of root CA, CA TECNISIGN must:

1. prepare and follow a key generation script; and

2. have a qualified auditor to witness the process of generating root CA key pair or recording a video of the entire process of generating the root CA key pair.

In all cases, CA TECNISIGN:

1.generates the Keys in a physically secure environment, as described in this CP and its CPS;

2.generates CA TECNISIGN keys using personnel in trust functions under the principles of control of several people and divide the knowledge;

3.generates CA TECNISIGN keys within cryptographic modules that meet the applicable technical and business requirements, as disclosed in this CPS and its CP.

4.records its CA key generation activities; and

5.maintains effective controls to provide reasonable assurance that the Private Key has been generated and protected in accordance with the procedures described in this CPS and its CP.

6.1.2 Delivery of the key pair to the Signatory

Subscriber private keys are generally generated by the end user, and therefore, the delivery of the private key to a Subscriber does not apply.

If CA TECNISIGN or any of its RAs becomes aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated to the Subscriber, CA TECNISIGN shall revoke all certificates that include the Public Key corresponding to the Private Key communicated.

If CA TECNISIGN or any of its RAs generated the Private Key on behalf of the Subscriber, CA TECNISIGN must encrypt the Private Key for transportation to the Subscriber.

6.1.3 Delivery of public key to certificate issuer

When a public key is transferred to the issuing CA to be inserted into a certificate, it must be delivered through a mechanism that ensures that the public key has not been changed during transit and that the certificate applicant has the private key corresponding to the transferred public key. The acceptable mechanism within CA TECNISIGN for public key delivery is a PKCS # 10 Certificate signing order pack or equivalent method, ensuring that:

- The public key was not changed during transit; and
- The Certificate Applicant has the private key corresponding to the transferred public key.

CA TECNISIGN when executing Key Generation Ceremonies transfers the public key of the cryptographic module in which it was created to the upper CA cryptographic module (the same cryptographic module, if it is a CCA), grouping it into a PKCS # 10 order.

6.1.4 Delivery of CA Public Key to Trusting Parties

CA TECNISIGN provides the complete certification chain (including CA TECNISIGN and any chain CAs) to the End User Subscriber upon issuance of the Certificate. The download of certificates MAY also be downloaded at: http://www.tecnisign.net

VALID will make a reasonable effort so that CA TECNISIGN public keys are included in Root Certificates that are already embedded in many popular software applications, making special root distribution mechanisms unnecessary. In addition, in many cases, a Trusting Party using the S/MIME protocol will automatically receive, in addition to the Subscriber Certificate, the Certificates (and hence the public keys) of all CAs subordinate to CA TECNISIGN.

6.1.5 Key size

Key pairs MUST be long enough to prevent others from determining the private key of the key pair using cryptographic analysis for the expected period of use of such key pairs.

CA TECNISIGN Standard is:

. for CA issued until 09/26/2018

- key sizes for end users: 2048 bits RSA

- digital signature algorithm: SHA-1

. for CA issued after 08/18/2011:

- key sizes for end users: 2048 bits RSA

- hash digital signature algorithm: sha-512

The generated key size follows the best practices described by WebTrust and CA/Browser Forum Baseline Requirements and an annual revision is performed in key lengths to determine the appropriate key usage period with recommendations followed.

After the CA certificate expires, the private key is destroyed correctly at the end of the archive period.

6.1.5.1 CABF Requirements for key sizes

Root CA Certificates	Validity period starting on December 31, 2010	Validity period starting on December 31, 2010
Digest Algorithm	MD5 (NOT RECOMMENDED), SHA-1, SHA-256, SHA-384 or SHA-51	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum DSA modulus and divisor 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 Certificate	Validity period starting on December 31, 2010	Validity period starting on December 31, 2010
Digest Algorithm	SHA-1, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum DSA modulus and divisor 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	

Subscriber Certificate	End of validity period on or before December 31, 2013	Validity period ending after December 31, 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	

* SHA-1 CAN be used with RSA Keys according to the criteria defined in Section 7.1.3.

** A Root CA Certificate issued prior to December 31, 2010 with an RSA key size of less than 2048 bits CAN still serve as a trust anchor for subscriber Certificates issued in accordance with these Requirements.

*** L and N (the bit lengths of the p modulus of q divisor, respectively) are described in the Standard Digital Signature, FIPS 186-4 (http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf).

6.1.6 Generation of public key parameters and quality verification

CA TECNISIGN participants must generate the necessary key parameters according to an equivalent standard approved by PMD.

The same standards must be used to verify the quality of the key parameters generated.

RSA: CA TECNISIGN must confirm that the public exponent value is an odd number equal to 3 or more. Also, the public exponent must be in the range between 216 + 1 and 2256-1. The modulus must also have the following characteristics: an odd number, not the power of a prime, and has no factors less than 752. [Source: Section 5.3.3, NIST SP 800-89].

DSA: Although FIPS 800-57 says domain parameters CAN be made available on some accessible site, the compatible DSA certificates must include all domain parameters. This is to ensure maximum interoperability between trusted third-party software. CA TECNISIGN must confirm that the public key value has the unique correct representation and range in the field, and that the key has the correct order in the subgroup. [Source: Section 5.3.1, NIST SP 800-89].

ECC: CA TECNISIGN must confirm the validity of all keys using ECC Full Public Key Validation Routine or ECC Partial Public Key Validation Routine. [Source: Sections 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 56A: Revision 2]].

6.1.7 Key usage purposes (according to "key usage" field in X.509 v3)

Private keys corresponding to end user Certificates MUST HAVE digitalSignature, nonRepudiation, AND keyEncipherment bits enabled.

Private Keys corresponding to Root Certificates 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 (certificates of administrative roles, internal certificates of CA operational devices); and
4. Certificates for OCSP response verification.

6.1.8 Private Key Protection Controls and Cryptographic Modulus

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

6.1.9 Cryptographic Modulus Standards and Controls

Private keys within CA TECNISIGN must be protected using a Trusted System and private key holders must take the necessary precautions to prevent the loss, disclosure, modification or unauthorized use of such Private Keys under this CP, contractual obligations and documented requirements in CA TECNISIGN Confidential Security Policies. End-user subscribers have the option of protecting their private keys on a smart card or other hardware token. CA TECNISIGN and RA clients must protect private key segments on these servers by using a Trusted System.

CA TECNISIGN recommends that RA clients perform all cryptographic operations from AR to Automated Administration on a FIPS 140-2 level 3 certified cryptographic modulus or another similar standard used in Brazil.

VALID recommends that SSL certificates perform cryptographic operations on a cryptographic modulus rated at least 140-2 level 3, certified cryptographic modulus, or other similar standard used in Brazil.

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

VALID has implemented technical and procedural mechanisms that require the participation of several trusted individuals to perform confidential CA cryptographic operations. VALID uses "Secret Share" to divide the activation data required to use a CA private key into separate parts called "Secret Share" that are only maintained by trained, trusted individuals called "Shareholders." A "Secret Share" threshold number (m) of the total number of Secret Shares created and distributed for a particular hardware cryptographic modulus (n) is NECESSARY to enable a CA private key stored in the modulus.

The threshold number of shares required to sign a CA certificate is It should be noted that the number of shares distributed to disaster recovery tokens CAN be less than the number distributed to operational tokens while the threshold number of shares remains the same. The Secret Shares are protected under this CPS.

6.1.11 Private Key Custody

CA private Keys are not guarded.

6.1.12 Private Key Backup

CA TECNISIGN creates CA private keys backup copies for routine recovery and disaster recovery purposes. These keys are encrypted stored in the hardware cryptographic modulus and associated key storage devices. The cryptographic modulus used for CA private key storage meet the requirements of this CPS. The CA private keys are copied to the backup hardware cryptographic modulus, according to this CPS.

The cryptographic modules used to store the CA's private keys in place are subject to the requirements of this CPS. Modulus containing disaster recovery copies of CA private keys are subject to the requirements of this CPS.

Private keys the backup of which is made must be protected from unauthorized modification or disclosure by physical or cryptographic means. Backup copies are protected with a level of physical and cryptographic protection equal to or higher than cryptographic modulus on CA TECNISIGN site, such as in a disaster recovery site or other secure external facility, such as a bank safe.

CA TECNISIGN recommends that Corporate Clients who have Automated Administration tokens not subject to service make back up of their private keys and protect them from unauthorized modification or disclosure by physical or cryptographic means.

CA TECNISIGN does not maintain a backup copy of the digital signature certificate's private keys issued by CA TECNISIGN.

6.1.13 Private Key Archiving

Upon expiration of CA TECNISIGN certificate, the key pair associated with the certificate shall be securely maintained for a period of at least 5 years using cryptographic module that meets

the requirements of this CPS. These CA key pairs should not be used for any signing events after the expiration date of the corresponding certificate.

CA TECNISIGN subordinate CAs perform the same controls established for CA TECNISIGN.

CA TECNISIGN does not archive Subscriber's private key copies.

6.1.14 Private key transfer in cryptographic modulus

CA TECNISIGN generates the CA key pair on the hardware cryptographic modulus on which the keys will be used. In addition, VALID makes copies of CA key pair for routine recovery and disaster recovery purposes. Where CA key pair is copied to another hardware cryptographic modulus, those key pairs are transported between the modulus in encrypted format.

If the Issuance CA generated the Private Key on behalf of the Subordinate CA, then the Issuing CA must encrypt the private key for transport to the subordinate CA. If the issuing CA knows that a subordinate CA private key has been communicated to an unauthorized person or to an organization that is not affiliated with the Subordinated CA, the Issuing CA will revoke all certificates that include the key corresponding to the communicated private key.

The entry of a private key into a cryptographic modulus must use mechanisms to prevent loss, theft, modification, unauthorized disclosure or unauthorized use of such private key.

CA TECNISIGN participants who pre-generate private keys and transfer them to a hardware token, for example, transfer the Subscribers generated private keys to a smart card, securely transfer those private keys to the token to the extent necessary to prevent loss, theft, modification, unauthorized disclosure or unauthorized use of such private keys.

6.1.15 Private Key Storage in Cryptographic Modulus

The entry of a private key into a cryptographic modulus must use mechanisms to prevent loss, theft, modification, unauthorized disclosure or unauthorized use of such private key.

6.1.16 Private key Activation Method

CA TECNISIGN protects activation data of its private keys from loss, theft, modification, unauthorized disclosure or unauthorized use.

CA TECNISIGN Standard for Subscribers to Private Key Protection is:
. Use a password according to Section 6.4.1 or equivalent strength security to authenticate the Subscriber prior to activation of the private key, which includes, for example, a password to operate the private key or a login password or Windows screen saver; and
. Take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent the use of the workstation and its associated private key without the Subscriber's authorization.

When deactivated, private Keys are only kept in encrypted form.

6.1.17 Private Key Deactivation Method

End-user subscribers MUST protect their private keys. These obligations extend to the protection of the private key after the occurrence of a private key operation. The private key can be deactivated after each operation, after the system logoff or after removal of a smart card from the smart card reader, depending on the authentication mechanism employed by the user.

The Subscriber's private keys can be deactivated after each operation, after logging off the system, or after removing a smart card from the smart card reader, depending on the authentication mechanism employed by the user. In all cases, end users are required to properly protect their private keys in accordance with their CPS.

6.1.18 Private key destruction method

If necessary, all private keys must be destroyed in a manner that reasonably ensures that there are no residual remnants of the key that could lead to rebuilding the key.

CA TECNISIGN uses the zeroing function of its hardware cryptographic modules and other appropriate means to ensure complete destruction of CA's private keys. When performed, CA key destruction activities are logged.

6.1.19 Cryptographic Modulus Classification

See Section 6.1.9.

6.2 Other aspects of key pair management

6.2.1 Public Key Archiving

CA TECNISIGN and end-user Subscriber Certificates store their own public keys in backup and archived as part of VALID routine backup procedures.

6.2.2 Certificate Operating Periods and Key Pair Usage Periods

The Certificate Operating Period MUST be defined according to the deadlines established in the Table below. End-user Subscriber Certificates that are renewals of existing subscriber certificates CAN have a longer validity period (up to 3 months).

The usage period for Subscriber key pairs is equal to the Operating Period of its Certificates, except that the private keys CAN continue to be used after the Operating Period for decryption and signature verification. The Operating Period of a Certificate ends with its expiration or revocation. A CA should not issue certificates if its Operating Periods extend beyond the period of usage of the CA's key pair. Therefore, CA's key pair usage period is necessarily shorter than CA Certificate's operating period. Specifically, the period of usage is the Operating Period of CA Certificate minus the Operating Period of the Certificates that CA issues. At the end of the

period of usage for a Subscriber or CA key pair, the Subscriber or CA SHALL, thereafter, discontinue all use of the key pair, except to the extent that a CA needs to sign revocation information to the end of the Operating Period of the last Certificate issued.

Certificate issued by validity period	*Validity period*
Self signed Root CA (4096 bit RSA)	Up to 20 years
ROOT CA for online CA	Up to 15 years
Off-line intermediary CA off-line for online CA	Up to 15 years
Online CA for individual subscriber of the user	Usually up to 3 years, but under the conditions described below, up to 6 years under the conditions described below, with no renewal or re-registration option. After 6 years, new registrations are REQUIRED.
Online CA for organizational subscriber of end entity	Normally up to 6 years30, under the conditions described below, with no renewal or re-typing option. After 6 years, new registrations are REQUIRED.
Subscriber certificates issued according to CABF Requirements	N/A.

Except as noted in this section, CA TECNISIGN candidates MUST discontinue all use of their key pairs after the termination of their usage periods.

Any exception to this procedure requires PMD approval and MUST be documented in the relevant CPS.

Certificates issued by CA TECNISIGN to end users MAY have Operating Periods greater than 1 (one) years, up to 5 (five) years if the following requirements are met:

- ✓ Protection of Subscriber key pairs against their operating environment for Organization Certificates, operation with enhanced data center protection, and Individual Certificates, Subscriber key pairs reside in a hardware token, such as a smart card,
- ✓ Subscribers are NECESSARY to undergo re-authentication procedures at least every 3 years under Section 3 of the CPS'.
- ✓ If a Subscriber is unable to successfully complete the new authentication procedures pursuant to Section 3 of the CPS successfully or is unable to prove ownership of such private key when NECESSARY as set forth above, CA will automatically revoke the Subscriber Certificate.

Any exception to this procedure requires PMD approval and MUST be documented in the relevant CPS and CP.

6.2.2.1 CABF Requirements of the Validity Period

Subscriber Certificates issued after March 1, 2018 MUST have a Validity Period not exceeding 825 days.

Subscriber Certificates issued after July 1, 2016, but before March 1, 2018, NEED to have a Valid Period greater than 39 months.

6.3 Activation Data

6.3.1 Generation and installation of Activation Data

CA TECNISIGN participants who generate and install activation data for their private keys must use methods that protect the activation data to the extent necessary to prevent loss, theft, tampering, unauthorized disclosure or unauthorized use of such private keys.

To the extent that passwords are used as activation data, Subscribers must generate passwords that cannot be easily guessed or broken by dictionary attacks.

The activation data (secret share) used to protect tokens containing private keys from CA TECNISIGN is generated according to the requirements of this CPS. The creation and distribution of secret shares is registered.

The VALID password selection guidelines require that passwords:

- ✓ be generated by the user;
- ✓ have at least fifteen characters;
- ✓ have at least one alphabetic character and one numeric character;
- ✓ have at least one lower case letter;
- ✓ does not contain many occurrences of the same character;
- ✓ is not the same as the operator profile name; and
- ✓ does not contain a long substring of the user profile name.

Valid also recommends the use of two factor authentication mechanisms (for example, token and password, biometric and token, or biometric and password) for private key activation.

6.3.2 Activation Data Protection

CA TECNISIGN participants must protect the activation data of their private keys using methods that protect against loss, theft, modification, unauthorized disclosure or unauthorized use of such private keys.

End-user subscribers must protect activation data from their private keys, to the extent necessary to prevent loss, theft, tampering, unauthorized disclosure or unauthorized use of such private keys.

VALID strongly recommends that all Subscribers store their private keys in an encrypted form and protect their private keys by using a strong and / or strong password. The use of two factor authentication mechanisms (for example, token and password, biometric and token, or biometric and password) is encouraged.

6.3.2.1 Other aspects of the activation date

6.3.2.1.1 Transmission of activation data

When private key activation data is transmitted, CA TECNISIGN shall protect the transmission using methods that protect against the loss, theft, modification, disclosure or unauthorized use of such private keys.

6.3.2.1.2 Destruction of activation data

Activation data for CA private keys must be destroyed using methods that protect against loss, theft, tampering, unauthorized disclosure or unauthorized use of the private keys protected by such activation data. After the retention periods determined in Section 5.5.2, CA TECNISIGN must disable activation data by physical substitution and/or destruction.

6.4 Computer Security Controls

AC and RA functions occur on Trusted Systems, according to the standards documented in CA TECNISIGN's confidential security policies.

6.4.1 Specific Technical Requirements for Computer Security

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

VALID requires the use of passwords with a minimum length of characters and a combination of alphanumeric and special characters. VALID requires that passwords be changed periodically.

Direct access to databases that support the operation of VALID is limited to People of Trust in the Production Operations team and who have a reason for such access. VALID applies multifactor authentication for all accounts that are capable of directly issuing certificates.

Gateway servers must include the following functionality: Control access to CC services, identification and authentication for initiating AC services, object reuse for AC random access memory, use of encryption for session communication, and bank security data archiving, CA archiving and end-user Subscriber history and audit data, security-related event auditing, self-testing of security-related CA services, and reliable path for identifying PKI functions and associated identities.

RAs should ensure systems that maintain RA software and data files are Trusted Systems, protected from unauthorized access.

RAs logically separate access to these systems and this information from other components. This separation prevents access, except through defined processes. ARs must use firewalls to protect the network from internal and external intrusions and limit the nature and source of activities that CAN access such systems and information. RAs require the use of passwords with a minimum character length and a combination of alphanumeric and special characters, and require passwords to be changed periodically and as required. Direct access to the databases that support the operation of the RA is limited to People of Trust in the Production Operations team *and who have a reason for such access.*

6.4.1.1 CABF Requirements for Security Systems

CA TECNISIGN must apply multifactor authentication for all accounts that are capable of directly issuing certificates.

6.4.2 Life Cycle Technical Controls

6.4.1 System Development Controls

Applications are developed and implemented by VALID in accordance with VALID's systems development and change management standards. VALID also provides software for its enterprise customers for running RA and certain CA functions. This software is developed according to the development standards of the VALID system.

Software developed by VALID, when loaded for the first time, provides a method to verify that the software on the system was originated by VALID, has not been modified before the installation and is the version that is intended to be used.

6.4.3 Security Management Controls

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

6.4.4 Life Cycle Security Control

N/A

6.5 Network Security Controls

AC and RA functions are performed using protected networks according to the standards documented in CA TECNISIGN's confidential security policies (in the case of VALID and Affiliates) to prevent unauthorized access, tampering, and denial of service attacks. Confidential information communications must be protected using point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication.

6.6 Time Stamp

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

7. CERTIFICATE PROFILES, CRL AND OCSP

7.1 Certificate Profile

As described in the CA TECNISIGN Certificate Policy.

7.1.1 Version(s) Number
As described in the CA TECNISIGN Certificate Policy.

7.1.2 Certificate Extensions
As described in the CA TECNISIGN Certificate Policy.

7.1.2.1 Subject Alternative Name
As described in the CA TECNISIGN Certificate Policy.

7.1.2.2. Application of RFC 5280
For clarification purposes, a Pre-Certificate, as described in RFC 6962 - Certificate Transparency, shall not be considered a "certificate" subject to the requirements described in RFC 5280 - Public Key Infrastructure - X.509 Internet and Certificate Revocation List) under these Policies.

7.1.3 Algorithms identifiers
As described in the CA TECNISIGN Certificate Policy .

7.1.3.1 CABF Requirements for algorithms identifiers
As described in the CA TECNISIGN Certificate Policy .

7.1.4 Names formats
CA TECNISIGN Certificates are filled in with the required Issuer Name and Subject Distinguished Name provided in section 7 of the Certificate Policy - CP.

In addition, end-user Subscriber Certificates generally include an additional Organizational Unit field that contains a warning stating that the terms of use of the Certificate are set to a URL, the URL must be an indicator of the applicable Trusted Party Agreement. Exceptions to the foregoing requirement shall be permitted where limitations of space, formatting or interoperability within the Certificates make it impossible to use the Organizational Unit in conjunction with the application for which the Certificates are intended or if an indication of the applicable Trusted Party Agreement is included in the certificate policy extension.

7.1.4.1 Issuer (Issuer) Information
As described in the CA TECNISIGN Certificate Policy .

7.1.4.2.Issuer (Subject) information – End User Certificates
As described in the CA TECNISIGN Certificate Policy .

7.1.4.2.1. CABF Requirements for Subject Alternative Name Extension
As described in the CA TECNISIGN Certificate Policy .

7.1.4.2.1.1. Reserved IP Address or Internal Name

As described in the CA TECNISIGN Certificate Policy .

7.1.4.2.2. CABF Requirements for the field Subject Distinguished Name Fields

As described in the CA TECNISIGN Certificate Policy .

7.1.4.3. Subject Information – for CA Root and CA Subordinate Certificates

As described in the CA TECNISIGN Certificate Policy .

7.1.4.3.1. Subject Distinguished Name Fields

As described in the CA TECNISIGN Certificate Policy .

7.1.5 CABF Requirement for Name Restrictions

As described in the CA TECNISIGN Certificate Policy.

7.1.6 Certificates Policy Object Identifier

As described in the CA TECNISIGN Certificate Policy.

7.1.6.1. Reserved CP Identifiers

As described in the CA TECNISIGN Certificate Policy .

7.1.6.2. Root CA Certificates

As described in the CA TECNISIGN Certificate Policy .

7.1.6.3. CA Subordinate Certificates

As described in the CA TECNISIGN Certificate Policy .

7.1.6.4. End User Certificates

As described in the CA TECNISIGN Certificate Policy .

7.1.6.5 CABF Requirements for CP Object Identifier

7.1.6.5.1 CABF Requirements for CP Object Identifier for EV

As described in the CA TECNISIGN Certificate Policy .

7.1.7 Policy Restrictions Extension Use

As described in the CA TECNISIGN Certificate Policy.

7.1.8 Policy Qualifiers Syntax and Semantics

As described in the CA TECNISIGN Certificate Policy.

7.1.9 Processing semantics for Critical Extensions

As described in the CA TECNISIGN Certificate Policy.

7.2 LCR PROFILE

As described in the CA TECNISIGN Certificate Policy.

7.2.1 Version

As described in the CA TECNISIGN Certificate Policy.

7.2.2 LCR extensions and their entries

As described in the CA TECNISIGN Certificate Policy.

7.3 OCSP Profile

As described in the CA TECNISIGN Certificate Policy.

7.3.1 Version(s) Number

As described in the CA TECNISIGN Certificate Policy.

7.3.2 OCSP Extensions

As described in the CA TECNISIGN Certificate Policy.

8. Compliance Audit and Other Evaluations

After the start of operations, VALID and Affiliates undergo a periodic compliance audit ("Compliance Audit") to ensure compliance with CA TECNISIGN Standards.

An annual review of **WebTrust for Certification Authorities v2.1** or later (or equivalent) is conducted for datacenter operations and VALID key management operations that support CA public services.

In addition to these compliance audits, VALID and Affiliates MUST undertake further reviews and investigations to ensure the reliability of CA TECNISIGN, which include, but is not limited to:

- An Affiliate “Security and Practice Review" before it is allowed to begin operations.
- A "Security and Practice Review" consists of a review of the secure facilities, security documents, CPS, CA TECNISIGN-related agreements, privacy policy and an Affiliate's validation plans to ensure that the Affiliate meets CA TECNISIGN Standards.
- VALID is entitled in its sole and exclusive discretion to perform at any time an "Audit / Supervision" on itself, an Affiliate in the event that VALID believes that the audited entity has not complied with the standards of CA TECNISIGN, has suffered an incident or commitment, or has acted or failed to act, such that the failure of the auditee, the incident or commitment, or the act or failure to constitute actual or potential threat to the safety or integrity of CA TECNISIGN.
- VALID has the right to conduct "Supplemental Risk Management Reviews" on itself, an Affiliate after incomplete or exceptional findings in a Compliance Audit or as part of the overall risk management process in the ordinary course of business.

VALID has the right to delegate the performance of such audits, reviews and investigations to the High Entity of the entity being audited, reviewed or investigated, or to a third party audit firm. Entities that are subject to an audit, review or investigation must provide full cooperation to VALID and the team conducting the audit, review or investigation.

CA TECNISIGN should always:

1. . Issue Certificates and operate its PKI in accordance with all laws applicable to its business and the Certificates it issues in all jurisdictions in which it operates;
2. Comply with these requirements;
3. Comply with the audit requirements set forth in this section; and
4. Be licensed as a CA in each jurisdiction where it operates, if licensing is required by law of such jurisdiction for the issuance of Certificates.

CABF Requirements for audits

N/A.

CABF requirements for audits for EV

N/A.

8.1 Evaluation Frequency and Circumstances

Compliance audits are conducted at least annually, at the expense of the audited entity. Audits should be conducted on uninterrupted sequences of audit periods with each period of no more than one year.

Certificates that can be used to issue new certificates must be:
. Technically in accordance with section 7.1.5 of the CP and audited only according to section 8.7, or
. Technically unrestricted and fully audited, in accordance with all remaining requirements of this section.

A certificate is considered capable of being used to issue new certificates if it contains an X.509v3 basicConstraints extension, with the set of Boolean values of CA TECNISIGN set to TRUE, and therefore by definition to be either a Root CA Certificate or a Subordinate CA Certificate.

(1)) If CA TECNISIGN has a valid Audit Report indicating compliance with one of the audit schemes listed in Section 8.1, then no pre-operational assessment is required.
(2) If CA TECNISIGN does not have an Audit Report indicating compliance with one of the audit schemes listed in Section 8.1, then, prior to issuing Publicly Trusted Certificates, CA TECNISIGN shall provide a point-in-time evaluation performed with the applicable standards under one of the audit schemes listed in Section 8.1. The point-in-time evaluation shall be completed not earlier than 12 months after the issuance of Publicly Trusted Certificates and shall be followed by a full audit under this scheme within 90 days of the issuance of the first Trusted Certificate.

8.2 Identity / Evaluator's Qualifications

CA TECNISIGN Audit must be performed by a Qualified Auditor.

A Qualified Auditor means a natural person or a legal entity or a group of natural or legal persons who collectively possess the following qualifications and abilities:

1. Independence from the object of the audit;
2. The ability to perform an audit that addresses the criteria specified in one of the Eligible audit schemes (see Section 8.1);
3. Employs people proficient in the examination of Public Key Infrastructure technology, information, tools and techniques of security, information technology and security auditing and ability to attest as a third party;
4. (for audits performed in accordance with any of the ETSI standards) are accredited in accordance with ISO 17065, applying the requirements specified in ETSI EN 319 403;
5. (for audits performed according to the WebTrust standard) licensed by WebTrust;
6. Bound by law, governmental regulation or code of professional ethics; and
7. Except in the case of an Internal Government Audit Agency, maintain Professional Liability/Errors and Omissions insurance with coverage of at least one million dollars.

8.3 Assistant relationship with the evaluated entity

Compliance audits of VALID's operations are performed by an independent public accounting firm of VALID.

8.4 Topics covered by the evaluation

CA TECNISIGN shall be audited in accordance with one of the following schemes:

1. **WebTrust for Certification Authorities v2.1**;
2. A national system that audits compliance with TSI TS 102 042 / ETSI EN 319 411-1; or
3. If a government CA is required by its Certificate Policy to use a different internal audit scheme, it may use such a scheme provided that the audit (a) covers all the requirements of either of the above schemes or (b) consists of comparable criteria that are available for public review.
4. Whichever scheme is chosen, it should incorporate periodic monitoring and / or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.
5. The audit should be conducted by a Qualified Auditor.
6. For non-ARS third parties, CA TECNISIGN shall receive an audit report, issued in accordance with the auditing standards that support the accepted audit schemes found in Section 8.1, which provides an opinion as to whether the performance of the Third Party is in compliance with the policies of the party or policies of VALID ALLIANCE. If the opinion is that the Third Party is not in compliance, CA TECNISIGN shall not allow the Third Party to continue to perform delegated functions.
7. The audit period for the Third Party should not exceed one year (ideally aligned with the audit of CA TECNISIGN). However, if CA TECNISIGN or Third Party is under the operation, control or supervision of a Government Entity and the audit scheme is completed over several years, the annual audit shall cover at least the main controls that are REQUIRED to be audited annually by such a scheme plus that part of all non-essential controls that can be performed less frequently, but under no circumstances can any non-essential control be audited less frequently than once every three years.

8.4.1 RAs Audit

It is RECOMMENDED that RAs authorizing the issuance of SSL certificates are subject to an annual audit of compliance of their obligations under VALID ALLIANCE. At the request of VALID, the ARs must undergo an audit observing any exceptions or irregularities to the policies of CA TECNISIGN and the measures taken to remedy the irregularities.

8.4.2 VALID and Affiliate Audit

VALID and each Affiliate MAY be audited in accordance with the guidelines provided by the American Institute of Certified Public Accounts for Service Organization Control (SOC) Reports on the risks associated with Service Organizations. Its Compliance Audits are WebTrust for

Certification Authorities or an equivalent auditing standard approved by VALID, which includes the Operational Effectiveness and Operational Testing Policy and Procedures Report.

8.5 Actions taken as a result of deficiency

After receiving a Compliance audit report, the Entity's Entity must contact the audited party to discuss any exceptions or deficiencies presented by the Compliance Audit. VALID has the right to discuss such exceptions or deficiencies with the audited party. The auditee and the Entity must, in good faith, use commercially reasonable efforts to reach agreement on a corrective action plan to correct the problems that cause the exceptions or deficiencies and implement the plan.

In the event of a failure of the auditee to develop such a corrective action plan or to implement it, or if the report reveals any exceptions or deficiencies that VALID and the Entity of the auditee reasonably believe represent an immediate threat to the safety or integrity of VALID ALLIANCE , then:

(a) VALID and/or the Senior Entity shall determine whether a revocation and a report of impairment are necessary,

(b) VALID and/or the Senior Entity has the right to suspend the services of an audited entity, and

(c)) If necessary, VALID and/or the Senior Entity may terminate their agreement with the audited entity on the basis of that CPS.

8.6 Results Communication

The Audit Report SHALL explicitly state that it covers the relevant systems and processes used in the issuance of all Certificates that have one or more of the OIDs listed in Section 7.1.6.1 of the CP.

After any Compliance Audit, the audited entity shall provide VALID with the annual report and attestations based on its audit or self-audit within 14 days after the completion of the audit and no later than 45 days after the date of commencement of operations.

CA TECNISIGN makes available its Annual Audit Report no later than three (3) months after the end of the audit period. In the event of a delay of more than three months, VALID ALIANCE must present an explanatory letter signed by the Qualified Auditor.

8.7. Self-Audits

8.7.1. CABF Self-Audit Requirements

During the period that the CA issues Certificates, CA TECNISIGN shall monitor adherence to this CPS, its CP and strictly control its quality of service, performing self audits at least quarterly against a randomly selected sample of at least one certificate or at least 3% of the

certificates issued by it during the period beginning immediately after the previous self-audit sample has been performed. Except for Third Parties who undergo an annual audit that meets the criteria specified in Section 8.1, CA TECNISIGN shall strictly control the quality of service of issued certificates containing information verified by a Third Party or by having a Validation Specialist employed by CA TECNISIGN. Quarterly audits against a randomly selected sample of at least one certificate or 3% of certificates verified by the Third Party in the period beginning immediately after the last sample was withdrawn. CA TECNISIGN shall review the practices and procedures of each Third Party to ensure that the Third Party is in compliance with the relevant SCP and CP.

CA TECNISIGN MUST internally audit the compliance of each Third Party with these Requirements annually.

During the period that a subordinate CA issues certificates, the CA that has signed the subordinate CA certificate must monitor the membership of your CA and the subordinate CA's CPS. The CA shall ensure that the CP requirements are being applied at least quarterly against a randomly selected sample of at least one certificate or at least 3% of the Certificates issued by the Subordinate CA during the period beginning immediately after the previous audit sample has been taken.

8.7.2. CABF Self-Audit Requirements for EV Certificates and EV Code Signature

N/A.

9. Other commercial and legal subjects

9.1 Fees

9.1.1 Certificates Issuance or Renewal Fees

CA TECNISIGN has the right to charge end users for the issuance, management and renewal of Certificates.

9.1.2 Certificate Access Fees

VALID does not charge fees as a condition for making CSFs available in a repository or otherwise for Trusted Parties.

9.1.3 Fees for Certificate Revocation or Status

VALID does not charge fees as a condition for making available the CSFs required by CPS in a repository or other forms available to Trusted Parties. However, VALID is entitled to charge a fee to provide customized LCRs, or other value-added revocation and certificate status information services. VALID does not allow access to revocation information, certificate status information, or timestamps in its repositories by third parties that provide products or services that use this Certificate status information without the prior written consent of VALID.

9.1.4 Fees for other services

CA TECNISIGN does not charge a fee for access to this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification or creation of derivative works, SHALL be subject to a license agreement with the copyright owner of the document. Issuing CAs may charge for additional services such as the timestamping service.

9.1.5 Refund Policy

In the sub-domain of VALID, the following reimbursement policy reproduced at: (http://www.validcertificadora.com.br/cancelamento) is in force:

VALID adheres to and complies with strict practices and policies in conducting certification and certificate issuance operations. However, if for any reason a subscriber is not completely satisfied with the certificate issued to him, the subscriber may request that VALID revoke the certificate within thirty (30) days of the issue and provide the subscriber with a refund. After the initial period of 30 (thirty) days, a subscriber may request that VALID revoke the certificate and provide a refund if VALID breaches a warranty or other material obligation under this CP relating to the subscriber's certificate. After VALID revokes the subscriber's certificate, VALID will immediately credit the subscriber.

To request a refund, call customer service at: (http://www.validcertificadora.com.br/faleconosco). This refund policy is not an exclusive feature and does not limit other features that are available to subscribers.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

VALID, Affiliates and ARs (when necessary) must maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an insurance program of errors and omissions with an insurer or a self-insured withholding. This insurance requirement does not apply to government entities.

9.2.2 Other Assets

VALID, Affiliates and ARs must have sufficient financial resources to maintain their operations and fulfill their obligations, and they must be reasonably capable of assuming the liability risks to Subscribers and Trusted Third Parties.

9.2.3 Extended Warranty Coverage

Some CA TECNISIGN participants offer extended warranty programs that offer SSL certificate subscribers protection against loss or damage due to a defect in the issuance of the certificate by the entrant or to other consequences caused by negligence or breach of their contractual obligations, provided that the subscriber the certificate has fulfilled its obligations under the applicable service contract. CA TECNISIGN participants who offer extended warranty programs are REQUIRED to include program information in this CPS.

9.2.4 Insurances for EV Certificates and EV Code Signature

N/A.

9.3 Confidentiality of business information

9.3.1 Scope of Confidential Information

The following subscriber records shall, subject to Section 9.3.2, be kept confidential and private ("Confidential / Private Information"):

- CA request records, approved or rejected;
- Certificate request records,
- Transactional records (transactions complete records and audit trail),
- Audit trail records created or retained by VALID,
- Audit reports created by VALID (to the extent such reports are maintained) or by their respective auditors (internal or public),
- Contingency planning and disaster recovery plans, and
- Security measures that control VALID hardware and software operations and administration of certificate services and request services.

9.3.2 Information outside the scope of Confidential Information

Certificates, revocation of certificates, and other status information, repositories, and information contained therein are not considered Confidential / Private Information.

Information not expressly considered Confidential / Confidential Information according to Section 9.3.1 shall be considered confidential or private.

This section is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

CA TECNISIGN participants who receive private information must protect it from compromise and disclosure to third parties.

9.4 privacy of personal information

9.4.1 Privacy Plan

VALID and Affiliates shall implement a privacy policy according to VALID's internal requirements. Such privacy policies SHALL comply with applicable local privacy laws. VALID and Affiliates shall not disclose or sell the names of certificate users or other identifying information about them, subject to Section 9.3.2 and the right of a CA to transfer such information to a successor CA pursuant to Section 5.8.

VALID has implemented a Privacy Policy, located at http://www.validcertificadora.com.br/politicadeprivacidade, in compliance with this section.

9.4.2 Information deemed Confidential

Any information about Subscribers that is not publicly available through the content of the issued certificate, certificate directory, and online LCRs is treated as private.

9.4.3 Information not deemed Confidential

Subject to local laws, all information made public on a certificate is not deemed private.

9.4.4 Responsibility to Protect confidential information

CA TECNISIGN participants who receive private information must protect them from compromise and disclosure to third parties and must comply with all local privacy laws in their jurisdiction.

9.4.5 Notice and Consent to Use Confidential Information

Unless otherwise indicated in this CPS, in the applicable Privacy Policy or by contract, private information will not be used without the consent of the party to whom such information applies.

This section is subject to applicable privacy laws.

9.4.6 Disclosure on request of judicial or administrative proceedings

VALID shall disclose Confidential / Private Information if, in good faith, VALID believes that:

- disclosure is required in response to subpoenas and search warrants;
- disclosure is necessary in response to legal, administrative or other legal proceedings during the process of discovery in a civil or administrative action, such as subpoenas, interrogations, requests for admission and requests for production of documents.

This section is subject to applicable privacy laws.

9.4.7 Other Circumstances of Information Disclosure

The privacy policies SHALL contain provisions regarding the disclosure of Confidential / Private Information to the person disclosing it to VALID or to the Affiliate.

This section is subject to applicable privacy laws.

9.5 Intellectual Property Rights

The allocation of Intellectual Property Rights among VALID Subdomain Participants other than Subscribers and Trusted Third Parties is governed by the applicable agreements between these VALID Subdomain Participants.

The following subsections of Section 9.5 apply to Intellectual Property Rights in relation to Subscribers and Trusted Third Parties.

9.5.1 Property Rights in Certificates information and revocation

CAs retain all Intellectual Property Rights over the Certificates and revocation information they issue. VALID grants permission to reproduce and distribute certificates on a non-exclusive, royalty-free basis provided they are fully reproduced and that the use of certificates is subject to the Trusted Party Agreement referenced in the Certificate.

VALID grants permission to use revocation information to perform the functions of the Trusted Party, subject to the applicable CRL Use Agreement, the Trusted Party Agreement, or any other applicable agreements.

9.5.2 Property Rights of this CPS

CA TECNISIGN and the participants acknowledge that VALID retains all Intellectual Property Rights in this CPS.

9.5.3 Property Rights for names

A Certificate Applicant retains all rights it holds (if any) in any trademark, service mark or trade name contained in any Certificate Request and distinguished name within any Certificate issued to such Certificate Applicant.

9.5.4 Property Rights for Keys and similar Materials

Key pairs corresponding to CA Certificates and End Users are owned by the CAs and end users which are the respective Objects of these Certificates, regardless of the physical medium in which they are stored and protected, and such persons hold all intellectual property rights to these key pairs.

Without limiting the foregoing, the public keys and certificates of the Root CA are owned by VALID. VALID licenses software and hardware manufacturers to reproduce such certificates from Root CA to place copies on trusted hardware or software devices.

Finally, Secret Shares of the private key of a CA is owned by the CA, and the CA retains all intellectual property rights of such Secret Shares, although they cannot obtain physical possession of these Secret Shares from CA TECNISIGN.

9.6 Representations and Guarantees

9.6.1 AC representations and Guarantees

CA TECNISIGN guarantees that

- There is no known material tampering with the Certificate data or from the entities that approved the Certificate Application or issued the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities that approved the Certificate Application or issued the Certificate as a result of a failure to exercise due care in the Management of the Certificate Application or creation of the Certificate,
- Its Certificates comply with all material requirements of this CPS and applicable PCs, and
- Revocation services and use of the repository meet all requirements of this CPS and applicable PCs in all material respects.

9.6.1.1 CABF Guarantees and Obligations

When issuing a certificate, CA TECNISIGN provides the guarantees listed here for the following Beneficiaries:

1. The Subscriber who is party to the Subscriber Agreement or the Certificate Terms of Use;
2. All Application Software Vendors with whom AC Root has entered into a contract for the inclusion of its Root CA Certificate in software distributed by such application Software vendor; and 3. All trusting parties who reasonably rely on a valid certificate.

CA TECNISIGN ensures to Certificate Beneficiaries that, during the period in which the Certificate is valid, CA TECNISIGN has fulfilled these Requirements in its CP and in the CPS, for issuing and managing the Certificate.

Certificate Warranties specifically include, but are not limited to, the following:

1. Right to use Domain Name or IP Address: that, at the time of issuance, CA TECNISIGN (i) implemented a procedure to verify that the Applicant was entitled to use, or had control of, the Domain Name (s). and IP addresses listed in the Subject field of the Certificate and subjectAltName extension (or, in the case of Domain Names only, was delegated such right or control by someone who had such a right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in its CPS and / or CP;

2. **Authorization for the Certificate:** that, at the time of issuance, CA TECNISIGN (i) implemented a procedure to verify that the Issue has authorized the issue of the Certificate and that the Representative Requester is authorized to request the Certificate on behalf of the object of the certificate; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in its CPS and / or CP;
3. **Accuracy of Information**: Accuracy of Information: That, at the time of issuance, CA TECNISIGN (i) implemented a procedure to verify the accuracy of all information contained in the Certificate (with the exception of the organizationalUnitName field); (ii) followed the

procedure when issuing the Certificate; and (iii) accurately described the procedure in its CPS and/or CP;

4. **No misleading information:** No misleading information: that at the time of issue, CA TECNISIGN (i) implemented a procedure to reduce the likelihood that the information contained in the organizationalUnitName field would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in its CPS and/or CP;

5. **Identity of the Applicant:** That, if the Certificate contains Identity Information of the applicant, CA TECNISIGN (i) has implemented a procedure to verify the identity of the Applicant in accordance with Section 3.2 of the CP; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in its CPS and/or CP;

6. **Subscriber Agreement:** If CA TECNISIGN and the Subscriber are not Affiliates, the Subscriber and CA TECNISIGN shall form part of a legally valid and enforceable Subscriber Agreement that meets these Requirements, or if CA TECNISIGN and Subscriber are the same entity or are Affiliates, the Representative of the Applicant has recognized the Terms of Use;

7. **Status:** CA TECNISIGN maintains a publicly accessible 24 x 7 Repository with current status information (valid or revoked) of all non-expired Certificates; and

8. **Revocation:** Revocation: CA TECNISIGN will revoke the Certificate for any of the reasons specified in its CPS and/or CP;

Root CA will be responsible for the performance and warranties of the Subordinate CA in accordance with this CPS and for all liabilities and indemnification obligations of the CA Subordinated with this CPS. If the root CA were the subordinate CA issuing the certificate subscriber agreements it may include additional representations and warranties.

9.6.1.2 EV Certificates Guarantees

N/A

9.6.1.3 Guarantees for Code Signing EV Certificate

N/A.

9.6.2 AR Representations and Guarantees

CA TECNISIGN and its ARs ensure that:

- There are no false statements in the Certificate known or originating in the entities that approve the Certificate Application or issue the Certificate,
- There are no errors in the information contained in the Certificate that were introduced by the entities that approve the Certificate Request as a result of a failure to exercise reasonable care in managing the Certificate Request,
- Your Certificates meet all material requirements of this CPS and the applicable CP and

- Revocation services (where applicable) and use of a repository meet all material requirements of this CPS and applicable CP in all material respects.

Subscriber agreements MAY include representations and additional warranties.

9.6.3 Subscriber Representations and Guarantees

Subscribers ensure that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate, and the Subscriber's digital signature and Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created;
- The private key is protected and no unauthorized person has access to the Subscriber's private key,
- All representations made by the Subscriber in the Certificate Request sent by the Subscriber are true;
- All information provided by the Subscriber and contained in the Certificate is true;
- The Certificate is being used exclusively for authorized and legal purposes, in accordance with all material requirements of this CP and the applicable CPS; and
- Subscriber is an end user and not an CA, and is not using the private key corresponding to any public key listed in the Certificate for the purpose of digitally signing any Certificate (or any other certified public key format) or LCR, such as a CA.

Subscriber agreements MAY include representations and additional warranties.

9.6.3.1 CABF Requirements for Subscriber Agreement

CA TECNISIGN requires, as part of the Subscription Agreement or Terms of Use, that the Applicant declare the commitments and warranties in this section for the benefit of CA TECNISIGN and the Certification Beneficiaries.

Before issuing a Certificate, CA TECNISIGN obtains, for the express benefit of CA TECNISIGN and the Certification Beneficiaries:
1. The Applicant's agreement to the Subscriber Agreement with CA TECNISIGN, or 2. 2. The Applicant's acknowledgment of the Terms of Use.

CA TECNISIGN implements a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In both cases, the Contract shall apply to the Certificate to be issued in accordance with the certificate application.

CA TECNISIGN may use an electronic or click-through agreement, provided VALID ALLIANCE has determined that such agreements are legally enforceable. A separate Agreement may be used for each certificate request, or a single Contract MAY be used to cover multiple future certificate requests and the resulting Certificates provided that each Certificate issued by CA

TECNISIGN to the Applicant is clearly covered by the Agreement or Terms of Use of the Subscriber.

The Subscription Agreement or the Terms of Use must contain provisions imposing upon the Applicant (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. **Accuracy of Information:** the obligation and guarantee to provide accurate and complete information at all times, both in the application for the certificate and as requested by CA TECNISIGN in connection with the issuance of the Certificate (s) by CA TECNISIGN;

2. **Private Key Protection:** The obligation and assurance of the Applicant to take all reasonable steps to ensure control, to maintain confidentiality, and to adequately protect the Private Key that corresponds to the Public Key to be included in the requested Certificate (s) any associated activation data or device, for example, password or token);

3. **Certificate Acceptance:** The obligation and assurance that the Subscriber will review and verify the contents of the Certificate for accuracy;

4. **Certificate use:**

i. EV Certificates: N/A.
ii. EV Code Signing Certificate: N/A.

5. Reporting and Revocation: the obligation and guarantee to promptly request the revocation of the Certificate, and cease to use it and its associated Private Key, in the event of:

a. have evidences that the certificate was used to sign the suspect code – for EV Code signature Certificate;
b. any information in the Certificate is, or becomes, incorrect or inaccurate; or
c. there is any actual or suspected abuse or compromise of the primary activation data or the Subscriber's private key associated with the Public Key included in the Certificate;

6. **End of Certificate Use:** End of Certificate Use: the obligation and guarantee to immediately cease all use of the Private Key corresponding to the Public Key included in the Certificate in the revocation of that Certificate for reasons of Key Commitment;
7. **Responsivity:** the obligation to respond to CA TECNISIGN's instructions regarding the Key Compromise or misuse of the Certificate within a specified period of time;
8. **Confirmation and Acceptance:** acknowledgment and acceptance that CA TECNISIGN has the right to revoke the certificate immediately if the Applicant violates the terms of the Subscription Agreement or Terms of Use or if CA TECNISIGN finds that the Certificate is being used to enable activities such as phishing attacks, fraud or the distribution of malware.

In the case of EV code signing certificate: N/A.

9.6.4 Representations and Guarantees of Trusted Parties

N/A.

9.6.5 Representations and Guarantees of other Participants

N/A.

9.7 Disclaimer of Guarantees

To the extent permitted by applicable law, Subscriber Agreements and Trusted Third Parties shall deny any possible warranties of VALID, including any commercial warranties or fitness for a particular purpose that is outside the context of CA TECNISIGN's CPS.

9.8 Limitations of Liability

To the extent that VALID has issued and managed the Certificate (s) in question in accordance with its Certificate Policy and its Certification Practice Statement, VALID has no responsibility to the Subscriber, any Trusted Party or any other third party for any damages or losses suffered as a result of the use or reliance on such Certificates. Limitations of liability shall include an exclusion of indirect, special, incidental and consequential damages. They must also observe the liability limits of one hundred US dollars ($ 100) limiting damages to VALID and the Affiliate.
The liability (and/or limitation thereof) of the Subscribers shall be as set forth in the applicable Subscription Agreements.

The liability (and/or limitation thereof) of the ARs and the applicable CA will be established in the contract (s) between them.

The liability (and/or limitation thereof) of the Relying Parties shall be as set forth in the applicable Trusted Parties Agreements.

For delegated tasks, CA TECNISIGN and any Third Party may allocate responsibility to each other contractually as they determine, but CA TECNISIGN remains fully responsible for the performance of all parties under this CPS and/or CP as if the tasks had not been delegated.

If CA TECNISIGN has issued and managed the Certificate in accordance with its CPS and CP, CA TECNISIGN disclaims liability to the Certification Beneficiaries or any other third parties for any losses incurred as a result of the use or reliance on such Certificate specified in CPS E CP of CA TECNISIGN.

If CA TECNISIGN has not issued or managed the Certificate in accordance with its CP and CPS, CA TECNISIGN seeks to limit its liability to the Subscriber and to the Trusted Parties, regardless of the cause of action or the legal theory involved, for any and all claims, losses or damages suffered as a result of use or reliance on such Certificate by any appropriate means you choose.
If CA TECNISIGN chooses to limit its liability for Certificates that are not issued or managed in accordance with its CP and CPS, CA TECNISIGN will include the limitations of liability in its CPS and CP of CA TECNISIGN.

9.8.1 CABF Limitation of Liability Requirements

For delegated tasks, CA TECNISIGN and other Third Parties may allocate responsibility for contractual performance, but the CA should be considered as having all obligations in accordance with these requirements, as if they had not been performed as having been delegated.

If CA TECNISIGN managed the Certificate in accordance with the CABF, CPS and CP Requirements, CA TECNISIGN disclaims liability to the Certification Beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such Certificates other than those specified in CPS and CP of CA TECNISIGN. If CA TECNISIGN has not issued or managed the Certificate in accordance with the requirements of the CABF and its CP and/or CPS, CA TECNISIGN may limit its liability to the Subscriber and to the Trusted Parties regardless of the cause of action or the legal theory involved, for any and all claims, losses or damages suffered as a result of the use or reliance on such Certificate by any appropriate means that CA TECNISIGN wishes. If CA TECNISIGN chooses to limit its liability for Certificates that are not issued or managed in accordance with the CABF, CPS and CP Requirements the CA shall include the limitations of liability in CPS and CP of CA TECNISIGN.

9.8.2 Limitations of Liability for EV

N/A.

9.9 Indemnifications

9.9.1 Indemnifications by subscribers

To the extent permitted by applicable law, Subscribers are required to indemnify VALID for:

- Truthful misrepresentation or misrepresentation by the Subscriber in the Subscriber Certificate Request,
- Subscriber's failure to disclose a material fact about the Certificate Request if the false statement or omission was made with negligence or intent to deceive any party,
- Subscriber's failure to protect the Subscriber's private key, to use a Trusted System, or to take reasonable precautions to prevent unauthorized committing, loss, disclosure, modification or unauthorized use of the Subscriber's private key, or
- use of a name by the Subscriber (including, without limitation, a common name, domain name or email address) that infringes on the Intellectual Property Rights of a third party.

The applicable Subscription Agreement may include additional indemnity obligations.

Notwithstanding any limitations to its responsibility to Subscribers and Relying Parties, CA TECNISIGN understands and acknowledges that Application Software Vendors that have a Root Certificate distribution agreement in effect with AC Root assume no obligation or liability of any kind CA TECNISIGN under these Requirements or that otherwise could exist due to the issuance or maintenance of Certificates or the trust deposited by Entrusting Parties or others. CA TECNISIGN hereby defends, indemnifies and exempts each Software Vendor from any and

all claims, damages and losses incurred by such Application Software Vendor in connection with a Certificate issued by CA TECNISIGN, regardless of the cause of the action or theory involved. This does not, however, apply to any claim, damage or loss suffered by such Application Software Vendor in connection with a Certificate issued by CA TECNISIGN when such claim, damage or loss was caused directly by the Software Vendor's software application displayed as unreliable. a Certificate that is still valid or is displayed as trusted: (1) the Certificate that has expired or (2) the Certificate that has been revoked (but only in cases where revocation status is available at the time of online CA TECNISIGN on- and the application software has not verified this status or ignored a revoked status indication).

9.9.2 Indemnification of Trusted Parties

To the extent permitted by applicable law, the Trusted Third Party Agreements shall require the Trustees to indemnify VALID for:

- Failure of the Trusted Third Parties to perform the obligations of a Trusted Third Parties,
- Trust of the Trusted Party in a Certificate that is unreasonable under the circumstances, or
- The failure of the Trusted Party to verify the status of such Certificate to determine if the Certificate has expired or has been revoked.

The applicable Trusted Party Agreement may include additional indemnity obligations.

9.9.3 Indemnification for Software Vendors

Notwithstanding any limitations on its liability to Subscribers and Trusted Third Parties, the AC understands and acknowledges that Software Vendors that have a Root Certificate distribution agreement in effect with the Root CA assume no liability or potential liability of CA under these Requirements or that otherwise may exist because of the issuance or maintenance of Certificates or to the trust deposited by Entrusted Parties or others.

Accordingly, AC shall defend, indemnify and hold harmless each Software Vendor from the application of any and all claims, damages and losses suffered by such Application Software Vendor in connection with a Certificate issued by CA regardless of the cause of action or legal theory involved. This does not, however, apply to any claim, damage or loss suffered by such Application Software Vendor in connection with a Certificate issued by the CA where such claim, damage or loss was caused directly by the Software Vendor's software application displayed as not trustworthy. a Certificate that is still valid or displayed as trusted: (1) a Certificate that has expired or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available in the online CA and the software failed to check this status or ignored a revoked status indication).

9.10 Validity and Termination of CPS

9.10.1 CPS Change

CPS becomes effective upon posting to the CA TECNISIGN Repository. Changes to this CPS take effect upon posting to the VALID Repository.

9.10.2 Validity of the CPS

This CPS is changed from time to time, it will remain in effect until it is replaced by a new version.

9.10.3 Effect after CP termination

Even after termination of this CPS, CA TECNISIGN participants are bound by these terms for all certificates issued for the remainder of the validity period of such certificates.

9.11 Individual notices and communications with participants

Unless otherwise provided by agreement between the parties, VALID Subdomain participants shall use commercially reasonable methods to communicate with each other, taking into account the importance and subject matter of the communication.

9.12 Changes

9.12.1 Change process

Changes to this CPS can be made by the Policy Management Authority of CA TECNISIGN Changes should be presented in the form of a document that contains a corrected version of the CPS or an update. Updates supersede any designated or conflicting provisions of the referenced version of CPS. The PMD must determine if the changes in the CPS require a change in the object identifiers (OID) of the Certificate policies corresponding to each type of Certificate.

9.12.2 Notification Mechanism and Frequency

VALID and PMD reserve the right to change the CPS without notice of changes that are not relevant, including but not limited to corrections of typographical errors, changes to URLs, and changes to contact information. The PMD's decision to designate changes as materials or non-materials is at the sole discretion of the PMD.

The PMD shall send to the Affiliates notice of material changes to the CP proposed by the PMD. The note should indicate the text of the proposed amendments and the comment period. Affiliates shall post or provide a link to the proposed changes in their own repositories within a reasonable time after receipt of notice of such changes.

The PMD requests proposed changes from the CPS of other CA TECNISIGN participants. If the PMD considers such a desirable amendment and proposes the implementation of the amendment, the PMD shall notify such amendment in accordance with this section.

Notwithstanding any provision of CP to the contrary, if the PMD believes that material changes to the CPS are necessary immediately to stop or prevent a breach of the security of CA TECNISIGN or any part thereof, VALID and PMD shall have the right to make such changes by publication in the VALID Repository. Such changes shall take effect immediately upon publication. Within a reasonable time after publication, VALID must notify Affiliates of such changes.

9.12.2.1 Period for comment

Except where otherwise indicated, the deadline for questioning about changes to the CP must be 15 days, from the date that the variables are published in the VALID Repository. Any of the participants of CA TECNISIGN have the right to submit comments from the PMD until the end of the comment period.

9.12.2.2 Mechanism to deal with Comments

The PMD MUST consider any comment on the proposed amendments. The PMD MUST:
(a) allow the proposed amendments to enter into force without modification,
(b) amend the proposed amendments and republish them as a new amendment when REQUIRED, or (c) withdraw the proposed amendments.

The PMD has the right to withdraw the proposed changes by notifying the Affiliates and providing a notice in the Updates and Practices Warnings section of the VALID Repository. Unless the proposed amendments are amended or withdrawn, they shall enter into force after the end of the comment period.

9.12.3 Circumstances in which OIDs must be changed

If the PMD determines that a change is required in the object identifier corresponding to a Certificate policy, the change MUST contain new object identifiers for the Certificate policies corresponding to each Certificate type. Otherwise, the changes SHOULD NOT require a change in the certificate policy object identifier.

9.13 Provisions for Disputes Resolution

9.13.1 Disputes between VALID, AR, Affiliates and Clients

Disputes between one or more of any involved MUST be resolved in accordance with the provisions of the applicable agreements between the parties.

9.13.2 Disputes with Subscribers, end users or Trusted Parties

To the extent permitted by applicable law, Subscriber Agreements and Trusted Party Agreements shall contain a dispute resolution clause. Disputes involving VALID require an initial negotiation period of sixty (60) days, followed by litigation in the city court of; City and Country name.

9.14 Applicable Law

Subject to any limitations contained in the applicable legislation, the laws of Brazil SHALL govern the applicability, construction, interpretation and validity of this CP, regardless of contract or other choice of legal provisions.
This choice of law is made to ensure uniform procedures and interpretation for all CA TECNISIGN Participants, no matter where they are located.

This provision of applicable law applies only to this CPS. Agreements incorporating the PSC by reference MAY have their own provisions of administrative law, provided that this Section regulates the applicability, construction, interpretation and validity of the terms of the PSC separately and independent of the other provisions of such agreements, subject to any limitations in the applicable law.

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, ordinances and orders, including, but not limited to, restrictions on the export or import of software, hardware, or technical information.

If a court or government body with jurisdiction over the activities covered by this CP and its SPC determines that compliance with any mandatory requirement is unlawful, such requirement shall be deemed to be retired to the extent necessary to make the requirement valid and lawful. This applies only to operations or issues of certificates that are subject to the laws of that jurisdiction. The parties involved must notify the CA / Browser Forum of the facts, circumstances and laws involved, so that the CA / Browser Forum can review its Guidelines accordingly.

9.15 Compliance with the applicable Law

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, ordinances and orders, including, but not limited to, restrictions on the export or import of software, hardware, or technical information.

9.15.1 Compliance with CABFORUM

N/A.

9.16 Miscellaneous Provisions

9.16.1 Totality of the Agreement

N/A.

9.16.2 Attribution

N/A.

9.16.3 Disassociation

In the event of a conflict between these Requirements and any law, regulation or governmental order (hereinafter referred to as "the Law") of any jurisdiction in which CA TECNISIGN operates or issues certificates, CA TECNISIGN MAY modify any conflicting requirement to the legal and valid requirement in the jurisdiction. This applies only to transactions or issues of certificates subject to this law. In this case, CA TECNISIGN shall immediately (and before issuing a certificate under the modified requirement) include in this Section a detailed reference to the Act that requires a modification of these Requirements under this section, and the specific modification of these Requirements implemented by CA TECNISIGN.

9.16.3.1 CABF Disassociation requirements

CA TECNISIGN MUST also (prior to issuing a certificate under the modified requirement) notify the CA / Browser Forum of the relevant information newly added to this CPS by sending a message to **questions@cabforum.org** and receiving confirmation that it has been posted on the Public Mailing List and indexed in the Public Message Archive available at**: https://cabforum.org/pipermail/public/** (or other e-mail addresses and links that the Forum MAY designate), so that CA / Browser Forum may consider revisions to these requirements accordingly.

Any modification to the **CA TECNISIGN** practice enabled in this section MUST be discontinued if and when the Act no longer applies, or these Requirements are modified to enable both and the Act to be complied with at the same time. An appropriate change in practice, modification in **CPS and CP**, and a notice in the **CA / Browser Forum**, as described above, MUST be made within 90 days.

9.16.4 Application (Fees and Waiver of attorney rights)

N/A.

9.16.5 Force Majeure

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

9.17 Other Provisions

N/A.

Appendix A: Abbreviations and Acronyms Table

Term in Portuguese	Term in English	Definition
Participante da AC	AC Participant	An individual or organization that has one or more of the following roles within the AC infrastructure: CA TECNISIGN, Affiliate, Customer, Subscriber or Trusted Party
PKI AC	AC PKI	consists of systems that collaborate to provide and implement AC
Repositório da AC	AC Repository	certificate database and other relevant information from the CA accessible online
Padrões da AC	AC Standards	Legal standards and technical requirements used by the CA for the issuance, administration, revocation, renewal and use of Certificates
Administrador	Administrator	A trusted person within the organization of an AC or AR performing AR or AC validation functions
Certificado de administrador	Administrator Certificate	A certificate issued to an administrator that can only be used to perform CA functions or AR
Afiliado	Affiliate	A trusted third party (a corporation, partnership, joint venture or other controlling entity, controlled or under common control with another entity) entered into an agreement with CA TECNISIGN to be a service or RA distributor within a specific territory
AICPA	AICPA	Instituto Americano de Contadores Públicos Certificados
ANSI	ANSI	American National Standards Institute
Requerente	Applicant	The natural or legal person who requires a certificate or renewal thereof. Once the certificate is issued, the Applicant is referred to as "Subscriber". For Certificates issued to devices, the applicant is the entity that controls or operates the device named on the certificate

Representante do Requerente	Applicant Representative	An individual representing the applicant, having express authority to represent the applicant: (i) applying for the certificate on behalf of the applicant, and / or (ii) signing and sending the Subscriber Agreement in the name of the Applicant, and / or (iii) which recognizes and agrees with the Certificate Terms of Use on behalf of the Applicant
Carta confirmatória	Attestation Letter	A letter certifying certain information in the process of requesting the certificate
Período de auditoria	Audit Period	the period from the first day (beginning) to the last (final) day of operation covered by the analysis. (which is different from the period of time auditors are conducting the audit).
Relatório de auditoria	Audit Report	A report of a qualified auditor stating qualified auditor's opinion on whether the processes and controls of an entity in accordance with the mandatory provisions of those requirements
Autorização de *Domain Name*	Authorization *Domain Name*	Authorization to use the Domain Name used to issue a certificate for a given
		FQDN.
Porta autorizada	Authorized Port	One of the following ports: 80 (http), 443 (http), 25 (SMTP), 22 (SSH).
Radical do *Domain Name*	Base *Domain Name*	The initial portion of the FQDN. This is the first node to the left of Domain Name (for example, "example.co.uk" or "example.com").
BIPM	BIPM	Bureau Internacional de Pesos e Medidas
BIS	BIS	(US Government) Bureau de Indústria e Segurança
Entidade de negócios	Business Entity	Any entity that is not a private organization, governmental entity or non-commercial entity as defined herein. Examples include, but are not limited to, general partnerships, unincorporated associations, individual name, etc.
AC	CA	Certification Authority
CAA	CAA	Certification Authority Authorization
ccTLD	ccTLD	Country Code Top-Level Domain

CEO	CEO	Chief Executive Officer
Certificado	Certificate	An electronic document that uses encryption to bind a public key to an identity. Contains at least the name of the issuing CA, Subscriber ID, subscriber public key, Certificate Validity Period, a certificate serial number and is digitally signed by the CA.
Solicitante de certificado	Certificate Applicant	An individual or organization requesting the issuance of a certificate by a CA
Solicitação de certificado	Certificate Application	A Request from a Claimant to a Certificate Authority for the Issuance of a Certificate
Aprovador do certificado	Certificate Approver	the individual of the applicant or an authorized agent who has express authority to represent the applicant: (i) act as a requestor for the certificate and authorize other officials or third parties to act as a requestor for the certificate, and (ii) approve EV submitted by other Certificate Applicants.
Cadeia de Certificados	Certificate Chain	An ordered list of Certificates containing at least: (i) End User Certificate, (ii) Issuing CA Certificate. If the issuing CA is not self-signed, it must contain the CA certificate that issued it
dados do certificado	Certificate Data	certificate requests and related data (if obtained from the Applicant or otherwise) in possession or control of the CA
Processo de Gestão dos Certificados	Certificate Management Process	Process, practice, and procedures related to the use of keys, software, and hardware, whereby CA verifies certificate data, issues certificates, maintains a repository, and revokes certificates
Política de Certificado (CP)	Certificate Policy (CP)	A set of rules that indicates the applicability of a named certificate to a particular community and / or PKI implementation with security requirements.

Relato de Problemas com Certificado	Certificate Problem Report	Complaint for suspected key liability, improper use of certificates, or other types of fraud, misconduct, misuse, or improper conduct related to certificates

Requerente do certificado	Certificate Requester	An individual who acts as the applicant, an authorized agent who has express authority to represent the applicant, or a third party (such as an ISP or hosting company) who completes and submits an EV Certificate request on behalf of the applicant.
Lista de Certificados Revogados (LCR)	Certificate Revocation List (CRL)	A periodically issued list digitally signed by a CA, identifying the Certificates that were revoked prior to the expiration date, in accordance with Section 3.4. The list generally indicates the name of the LCR issuer, the date of issue, the date of the next edition of the LCR, the serial numbers of the revoked certificates, the date of revocation and the specific reasons for revocation
Requisição de Assinatura de Certificado (CSR)	Certificate Signing Request (CSR)	A message containing an application for issuing a certificate
Autoridade de Certificação (AC)	Certification Authority (CA)	An organization that is responsible for creating, issuing, revoking, and managing certificates. The term also applies to Root CAs and subordinate CAs.
Autoridade de Certificação Autorizada (CAA)	Certification Authority Authorization (CAA)	As described in RFC 6844 (http: tools.ietf.org/html/rfc6844): "Authorized Authorization Authority (CAA) Lists for each DomainName the Certificate Authority (CA) authorized to issue certificates for that domain. The CAA publication allows a public CA to implement additional controls to reduce the risk of improper issuance of "
Declaração de Práticas de certificação (CPS)	Certification Practice Statement (CPS)	One of several documents that form the governance framework in which certificates are created, issued, managed, and used.
CA TECNISIGN	CA TECNISIGN	Means, in relation to each section of this CPS, CA TECNISIGN Certificado Digital SA
CA TECNISIGN AC PARCERIA	CA TECNISIGN AC PARCERIA	The certificate-based public key infrastructure governed by CA TECNISIGN
Diretor Financeiro	CFO	Financial Director

Frase de desafio	Challenge Phrase	A secret phrase chosen by the Applicant during enrollment for a certificate. When a certificate is issued, the Applicant becomes a Subscriber and an AC or AR may use the Identification Phrase to authenticate the Subscriber when the subscriber attempts to revoke or renew the Subscriber's Certificate
CICA	CICA	Canadian Institute of Chartered Accountants
CIO	CIO	Chief Information Officer

CISO	CISO	Chief Information Security Officer
Auditoria de conformidade	Compliance Audit	A periodic audit in a CA or RA to determine its compliance with applicable standards
Comprometimento	Compromise	A breach (or suspected breach) of a security policy, in which an unauthorized disclosure or loss of control over confidential information may have occurred. With respect to private keys, a Commitment is a loss, theft, disclosure, modification, unauthorized use, or other compromise of private key security
Informação Privada/Confidencial	Confidential/Private Information	Information to be kept confidential and private pursuant to Section 2.8.1
Pedido de confirmação	Confirmation Request	A verification using another means of communication than the one primarily used requesting the confirmation of the certain fact.
Pessoa confirmadora	Confirming Person	An individual within the organization of a candidate who determined fact
Assinante do contrato	Contract Signer	An individual who is 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.

Controle	Control	"Control" (and its correlative meanings, "controlled by" and "under control") means ownership, directly or indirectly, of the power of: (1) guide the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the administration; or (3) to vote that part of the voting actions necessary to "control" under the law of the jurisdiction of the merging or registration entity, but in no case less than 10%.
COO	COO	Director of Operations
País	Country	a member of the United Nations or a geographical region recognized as a sovereign state by at least two UN member countries.
CP	CP	Certification policy
CPA	CPA	Chartered Accountant Professional
CPS	CPS	Certification Practices Statement
LCR	CRL	List of Revoked Certificates
Contrato de Utilização de LCR	CRL Usage Agreement	An agreement establishing the terms and conditions under which an CSF can be used
Certificação cruzada	Cross Certificate	A certificate that is used to establish a trust relationship between two root CAs
CSO	CSO	Security Director
CSPRNG	CSPRNG	A random number generator used in the cryptographic system.
Cliente	Customer	An organization or individual that is a Client of CA TECNISIGN AC PARTNERSHIP
DBA	DBA	Known name of a company (“doing business as”
Terceiro Delegado	Delegated Third	A natural or legal person who is not a CA, and whose

	Party	activities are not within the scope of CA or AR audits but are authorized by the CA to assist in the certificate management process by performing or meeting one or more of the requirements found here.
Conta de depósitos	Demand Deposit Account	The deposit account held in a bank or other financial institution, the funds deposited in which are payable on

		demand.
DNS	DNS	Domain Name System
Autorização do domínio	Domain Authorization	Correspondence or other documentation provided by person / body attesting to the authority of a candidate to request a certificate for a specific domain name
Documento de Autorização de domínio	Domain Authorization Document	Documentation provided by the domain name holder or the person or entity listed on the WHOIS as the Domain Name Applicant (including any confidential and anonymous registration service, or proxy) attesting to the authority of a candidate to request a certificate for a specific domain name
Contato do domínio	Domain Contact	The Holder, technical contact or administrative contract (or
Nome de domínio	Domain Name	equivalent under the ccTLD) of the Domain Name as listed on the WHOIS database tab or in an SOA DNS record.
Proprietário do Nome de domínio	Domain Name Registrant	Sometimes referred to as the "owner" of a domain name, but rather the person (s) or entity (s) registered with having the right to control how a domain name is used; the individual or legal entity that is listed as the "Requester" by WHOIS or other national domain name administrator.
Registro de Dominio	Domain Name Registrar	The person or entity that registers domain names under the auspices or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name registrar or registrar, or (iii) an Information Network (including its subsidiaries, contractors, delegates, successors or assigns)
Namespace de domínio	Domain Namespace	The set of all possible domain names that are subordinate to a single node in the Domain Name System.
Data final	Entry Date	The date that defines the end of the validity period of a certificate.
EV	EV	extended Validation

EV Autoridade	EV Authority	A source other than the Certificate Approver where verification occurs and is expressly authorized to take the measures described in these Guidelines in relation to the EV certificate requests
Certificado EV	EV Certificate	A digital certificate containing information provided in the "EV" guidelines and which has been validated in accordance with the Guidelines

Beneficiários de Certificado EV	EV Certificate Beneficiaries	People to whom the CA and its Root CA establishes specific warranties for EV certificates
Reemissão de Certificado EV	EV Certificate Reissuance	The process by which a candidate who has a valid EV certificate (not expired and not revoked) makes a request to the CA that issued the original EV certificate, so that a new EV certificate is issued to the same organization name and domain name before the expiration of the existing EV Certificate but with the final validity coinciding with that of the current EV Certificate
Renovação de Certificados EV	EV Certificate Renewal	The process by which a candidate who has a valid EV certificate (not expired and not revoked) makes a request to the CA that issued the original EV certificate, so that a new EV certificate is issued to the same organization name and domain name before the expiration of the existing EV Certificate but with the final validity not coincident with that of the current EV Certificate
Pedido de Certificado EV	EV Certificate Request	A request from a CA applicant requesting the issuance of an EV certificate to the Applicant by application validly authorized by the applicant and signed by the Applicant's Representative.
Garantias de Certificado EV	EV Certificate Warranties	In conjunction with the certification authority issuing an EV certificate, the CA and its root AC assure, during the period when the EV Certificate is valid, that the CA follows the requirements of the CA's EV policies and guidelines to verify accuracy of the information contained in the EV Certificate and issue it

certificado de Assinatura de Código EV	EV Code Signing Certificate	A certificate that contains information specified for Code Signing and has been validated in accordance with the "EV for Codesign"
Emissor de certificado de Assinatura de Código EV	EV Code Signing Certificate Issuer	The CA that issued an EV Code Signing Certificate to a subscriber or a signing authority
Objeto de certificado de Assinatura de Código EV	EV Code Signing Object	An EV code signing certificate issued by a CA
EV OID	EV OID	An identification number, in the form of an "object identifier", that is included in the CertificatePolicies field of a certificate that: (i) indicates which CA policy statement was respected for that certificate, and (ii) is the policy identifier EV CA / Browser Forum or a policy identifier which, by pre-agreement with one or more applications, marks the certificate as being an EV certificate.
Políticas EV	EV Policies	Practices, policies and procedures for auditable EV Certificates with a CPS and / or CP that are developed, implemented, and executed by CA and its root CA
Processos EV	EV Processes	The keys, software, processes, and procedures by which the CA verifies the data under the CA / Browser Forum EV Guidelines, issues Certificates, maintains a repository, and revokes

		EV certificates
Assinatura EV	EV Signature	An electronic encrypted data file, which is linked to or logically associated with other electronic data, and which (i) identifies and is solely linked to the electronic data signer, (ii) is created with means that the signatory may maintain under its exclusive control and (iii) is connected in a manner so as to make any subsequent changes that may be made to the detectable electronic data.

Validação Extendida	Extended Validation	Validation procedures defined by the Extended Validation Certification Guidelines issued by a forum comprised of leading certification authorities and browser providers
FIPS	FIPS	Federal Information Processing Standard of the Unityed States Government
FQDN	FQDN	Fully Qualified Domain Name
Nome de domínio totalmente qualificado	Fully-Qualified Domain Name	A domain name that includes the labels of all the top nodes in the DNS
gTLD	gTLD	Generic TopLevel Domain
Solicitação de certificado de Alto Risco	High Risk Certificate Request	A request that CA identifies as requiring further examination based on internal criteria and databases maintained by CA, which may include names at increased risk of phishing or other fraudulent use, names contained in previously rejected or revoked certificate applications, Google Safe Browsing List, or names that CA identifies using its own risk mitigation criteria
IANA	IANA	Internet Assigned Numbers Authority
EU ENLATO	ICANN	Internet Corporation for Assigned Names and Numbers
IFAC	IFAC	International Federation of Accountants
IM	IM	Instant Message
confirmação independente do Requerente	Independent Confirmation From Applicant	Confirmation of a particular fact received by the CA in accordance with the Inquiries by the applicant.
Individual	Individual	An individual
Direito de propriedade intelectual	Intellectual Property Rights	Rights under one or more of the following: copyright, patents, trade secrets, trademarks and any other intellectual property rights
Autoridade de Certificação intermediária	Intermediate Certification Authority	The Certificate Authority whose Certificate is located within a Certificate Chain between the Root CA Certificate and the Certificate Authority Certificate that issued the Certificate of the Subscriber
Nome interno	Internal Name	The characters chain (not an IP address) in the Common Name or Subject Alternative Name fields of a Certificate that cannot be verified inside the public DNS at the time of issuance of the

		certificate, since it does not appear in domains registered in the IANA database.
Nome do servidor interno	Internal Server Name	A Name Server (which may or may not include an unregistered domain name) that cannot be resolved using public DNS

Organização Internacional	International Organization	An organization founded by a constituent document, for example, a charter, treaty, convention or similar document, signed by at least two sovereign states
ISO	ISO	International Organization for Standardization
ISP	ISP	Internet Service Provider
AC emitente	Issuing CA	In relation to a particular Certificate, the CA that issued the certificate. This could be a root CA or a subordinate CA
comprometimento de chave	Key Compromise	The private key is said to be compromised if its value has been disclosed to a non-authorized person, an unauthorized person has had access to it, or there is a technical possibility by which an unauthorized person can discover its value. The private key is also considered compromised if the methods have been created allowing you to easily calculate it based on the public key (such as a weak Debian 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.
Cerimônia de Geração de Chave	Key Generation Ceremony	A procedure where a CA AR key pair is generated, or your private key is transferred to a cryptographic module, your private key is backed up, and / or your public key receives a certificate.
Script de Geração de Chave	Key Generation Script	A documented procedure for generating a pair of keys
Administrador do Gerenciamento de Chaves	Key Manager Administrator	An administrator who performs key generation and recovery functions in a Public Key Infrastructure (PKI)
Par de Chaves	Key Pair	The private key and its associated public

		key
Entidade legal	Legal Entity	The private key and its associated public key An association, corporation, partnership, property, trust, government entity, or other entity with legal personality in a country
Existência Legal	Legal Existence	A private organization, governmental entity or business entity has legal existence if it has been validly constituted and not rescinded, dissolved, or abandoned
Praticante legal	Legal Practitioner	A person who is either a lawyer as described in these Guidelines and competent to give an opinion on the claims of the applicant
LSVA	LSVA	logical security vulnerability assessment
Autenticação manual	Manual Authentication	A procedure where Certificate Requests are evaluated and approved manually one by one by an Administrator using a web interface
NIST	NIST	Instituto Nacional de Padrões e Tecnologia - National Institute of Standards and Technology (USA Government)
Não-repúdio	Non-repudiation	An attribute of a communication that protects it against a disloyalty denying its origin, denying that it was submitted, or denying its delivery. Note: Except for ICPBRASIL certificates, only one sentence IN a court or arbitration committee or can definitely guarantee non-repudiation. For example, a digital signature may serve as evidence in a non-repudiation dispute by a court, but it does not in itself constitute proof of non-objection

Informações do Assinante não-verificadas	Non-verified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included in a Certificate, which has not been confirmed by CA or RA
Notário	Notary	A person legally constituted to authenticate the execution of a signature in a document.
Identificador de Objeto	Object Identifier	A unique alphanumeric or numeric identifier registered under the International Standardization Organization applicable to a specific

		object or object class
OCSP	OCSP	Online Certificate Status Protocol - Certificate Status Online Protocol
OCSP Responder	OCSP Responder	An online server operated under CA authority that responds to certificate status requests.
AC offline	Offline CA	Root CAs and other intermediate CAs that are kept out of the air for security reasons in order to protect them from possible attacks from intruders through the network. These CAs do not issue end-user certificates.
OID	OID	Object Identifier
AC on-line	Online CA	CAs that issue end-user certificates are maintained online, in order to provide services on an ongoing basis
Protocolo online de estado do certificado	Online Certificate Status Protocol	An online verification protocol for Certificates to provide real-time certificate status information to Trusted Parties
Período operacional	Operational Period	The period beginning with the date and time a certificate is issued (or at a date and time indicated on the certificate) and ending with the date and time the certificate expires, if it has not previously been revoked
controladora	Parent Company	A company that controls a subsidiary company
PIN	PIN	Personal Identification Number
PKCS	PKCS	Public-Key Cryptography Standard
PKCS # 10	PKCS #10	Public-Key Cryptography Standard # 10, developed by RSA Security Inc., which defines a framework for a Certificate Signing Request
PKCS # 12	PKCS #12	Public-Key Cryptography Standard # 12, developed by RSA Security Inc., which defines a secure medium for private key transfer
PKI	PKI	Public Key Infrastructure – Infraestrutura de Chaves Publicas

Local de negócios	Place of Business	The location of any facility (such as a factory, shop, warehouse, etc.) where the candidate's business is conducted
PMD	PMD	Policy Management Department
Departamento de Gestão de Políticas (PMD)	Policy Management Authority (PMD)	The area within CA TECNISIGN responsible for building and approving CA policies
chave privada	Private Key	The key of a key pair that is kept secret by the key pair holder, and which is used to create digital signatures and / or to decrypt electronic records or files that have been encrypted with the corresponding public key
Organização privada	Private Organization	A legal non-governmental entity whose existence was created by a registration (or act) in a Regulatory Agency or the equivalent in the territory
Chave pública	Public Key	The key of a key pair that can be publicly disclosed by the corresponding private key holder and which is used by a trusted party to verify digital signatures created with the corresponding private key holder and / or to encrypt messages so that they can be deciphered only with the holder's private key
Infraestrutura de Chaves Publicas	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 public key cryptographic system
Certificado publicamente confiável	Publicly-Trusted Certificate	A certificate that is trusted by virtue of the fact that the corresponding root CA certificate is distributed as a trusted anchor in widely available applications
QGIS	QGIS	Fonte de Informação Qualificado do Governo - Qualified Government Information Source
QIIS	QIIS	Fonte de Informação Independente Qualificada – Qualified Independent Information Source
QTIS	QTIS	Fonte de Informação Tributária Qualificada do Governo - Qualified Government Tax Information Source

Auditor qualificado	Qualified Auditor	The individual or legal entity that meets the requirements of Section 8.2 Advisor Identity / Qualifications
Fonte de Informação Qualificado do Governo	Qualified Government Information Source	A database maintained by a governmental entity (for example, SEC files) that meets the requirements of Section 11.11.6.
Fonte de Informação Tributária Qualificada do Governo	Qualified Government Tax Information Source	A database maintained by a government entity that specifically contains tax information relating to private organizations, business entities, or individuals
Fonte de Informação Independente Qualificada	Qualified Independent Information Source	database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a reliable source of such information.
AR	RA	Registration Authority

Valor aleatório	Random Value	A value specified by the CA for the Applicant, which displays at least 112 entropy bits.
Nome Registrado do Domínio	Registered Domain Name	A domain name that has been registered in a domain registration body.
fonte confiável de dados	Trusted Data Source	an identification document or source of data used to verify Identity Information which is generally recognized by commercial companies and governments as trustworthy, and which was created by a third party for purposes other than for the applicant to obtain a certificate.
Endereço oficial	Registered Office	The official address of a company, as registered in the competent organ, where the official documents are sent and in which legal notices are received.
Agência de registro	Registration Agency	The Government Agency that records business information regarding the business formation of an entity or authorization to conduct business under a license, license or other certification
Autoridade de registro	Registration Authority	a legal entity that is responsible for identifying and authenticating certificate data, but is not an CA and therefore does not sign or issue certificates. An AR can aid in the certificate request or revocation process, or both.

Número de registro	Registration Number	O número único atribuído a uma organização privada pelo orgão competente
Instituição financeira regulada	Regulated Financial Institution	a financial institution that is regulated, supervised, and examined by governmental, national, state or municipal body, central or local authorities.
Método confiável de Comunicação	Trusted Method of Communication	A method of communication, such as a postal address, telephone number, or e-mail address, which was verified using an alternate source to the Applicant.
Parte Confiável	Relying Party	Any individual or legal entity that is based on a valid certificate. An application software vendor is not considered a Trusted Party because the software distributed by such Vendors only displays information regarding a certificate.
Acordo de Parte Confiável	Relying Party Agreement	A contract used to establish the terms and conditions under which an individual or organization acts as a third party in relation to the certificates.
Repositório	Repository	An online database that contains publicly disclosed CA documents (such as Certification Policies and Certification Practices statements) and Certificate status information, whether in the form of an CRL or an OCSP response
solicitação de token	Request Token	A value derived in a method specified by the CA that demonstrates the control by the certificate request. The token request must incorporate the key used in the certificate request. The token request can include a timestamp

		to indicate when it was created. The token request may include other information to ensure its uniqueness. The token request that includes a timestamp will remain valid for no more than 30 days from the time of creation. The token request that includes a timestamp should be treated as invalid if its time is in the future. The token request that does not include a timestamp is valid for a single use and AC should not reuse it for later validation. The binding must use a digital signature algorithm or a cryptographic hash algorithm at least as strong as the one to be used in signing the certificate request.
conteúdo requisitado do site	Required Website Content	a random value, or a token request, together with additional information identifying the Subscriber as specified by the CA.
Endereço de IP Reservado	Reserved IP Address	An IPv4 or IPv6 address that IANA has marked as reserved: http://www.iana.org/assignments/ipv4-addressspace/ipv4-address-space.xml http://www.iana.org/assignments/ipv6-addressspace/ipv6-address-space.xml
Certificado de varejo	Retail Certificate	A certificate issued by CA TECNISIGN, to individuals or organizations who request one by one to CA TECNISIGN on their website.
RFC	RFC	Request for comments - Request for comment
AC raiz	Root CA	Root Certification Authority
Certificado raiz	Root Certificate	The self-signed certificate issued by the root CA to identify and facilitate the verification of certificates issued by its subordinate CAs
Autoridade Certificadora Raiz	Root Certification Authority	The CA, which acts as a root CA and issues CA certificates subordinate to it
Script de Geração de Chave Raiz	Root Key Generation Script	A documented procedures for generating a pair of root CA keys.
RSA	RSA	A public key cryptography system invented by Rivest, Shamir, and Adelman

S / MIME	S/MIME	Secure MIME (multipurpose Internet mail extensions - multipurpose Internet mail extensions)
SAR	SAR	Security Audit Requirements
SEC	SEC	Securities and Exchange Commission (US Government)
Segredo Compartilhado	Secret Share	A portion of a private key of the CA or a portion of the activation data required to operate a private key of CA on a secret sharing basis
Compartilhamento de segredo	Secret Sharing	The practice of separating the private key from the CA or the activation data to operate a CA private key in order to enforce multiple people's control over CA's private key operations under Section 6.2.2
Secure Sockets Layer	Secure Sockets Layer	Web Communications, developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP / IP connection

Revisão de Práticas de Segurança	Security and Practices Review	The review of an Affiliate, performed by CA TECNISIGN before the affiliate is authorized to operate
SOC	SOC	Standardized Organization Control Service - Standard Service Organization Control
Estado soberano	Sovereign State	A state or country that runs its own government, and is not dependent, or subject to, another power.
SSL	SSL	Secure Sockets Layer
Sujeito	Subject	The natural person, device, system, unit or legal entity identified in a Certificate as subject and holder of a private key corresponding to a public key. The subject (subject) is either the subscriber or a device under Subscriber control and operation. The term "Subject" may, in the case of a Corporate Certificate, refer to the device or device that contains a private key. A Holder is assigned a unique name, which is linked to a public key contained in the Holder's Certificate

Informação da Identidade do Assunto	Subject Identity Information	Information that identifies the subject of the certificate. Subject Identity Information includes a domain name listed in the subjectAltName extension or in the commonName field
AC subordinada	Subordinate CA	A certification authority whose certificate is signed by the root CA, or another subordinate CA
Assinante	Subscriber	in the case of an individual certificate, a person who is the subject of and for which a certificate has been issued. In the case of a Corporate Certificate, an organization that has the equipment or device that is the subject of the Certificate for which the Certificate was issued. A subscriber is able, and is authorized to use the private key that corresponds to the public key listed in the Certificate
Contrato de assinante	Subscriber Agreement	An agreement between CA TECNISIGN AC PARTNERSHIP or the AR and the Applicant / subscriber specifying the rights and responsibilities of the parties.
Empresa subsidiária	Subsidiary Company	A company that is controlled by a mother company.
Entidade Superior	Superior Entity	An entity above another entity within a PKI
Entidade Governamental Superior	Superior Government Entity	Based on the governance structure in a political subdivision, the entity or entities that have the ability to administer, direct and control the activities of the Government.
Revisão suplementar de Gerenciamento de Risco	Supplemental Risk Management Review	A review of an entity by CA TECNISIGN after the discovery of incomplete or exceptional data in an Entity Compliance Audit or as part of the overall risk management process

código suspeito	Suspect code	Code that contains malicious functionality or serious vulnerabilities, including spyware, malware, and other code that installs without user consent and / or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise reliability of the platforms on which it executes.

Certificado de AC subordinada tecnicamente limitado	Technically Constrained Subordinate CA Certificate	A subordinate CA certificate that uses a combination of extended key usage settings and name restriction settings to limit the scope at which the subordinate CA can issue additional CA or end user certificates.
Termos de uso	Terms of Use	Provisions relating to the safekeeping and acceptance of use of a certificate issued in accordance with those requirements when the applicant / Subscriber is a branch of the CA or is the CA.
Certificado do teste	Test Certificate	A certificate with a maximum validity period of 30 days, which: (i) includes a critical extension as specified in the OID (2.23.140.2.1), or (ii) is issued under a CA where there is no chain of certificate for a root CA certificate subject to these requirements.
timestamp Authority	Timestamp Authority	An organization that assigns date and time to data, thus asserting that the data existed at the specified time
TLD	TLD	Top-Level Domain
TLS	TLS	Transport Layer Security
Tradutor	Translator	An individual or business entity that has the knowledge and experience necessary to accurately translate the words of a document written in a language into the native language of the CA.
Pessoa de Confiança	Trusted Person	An employee, contractor or consultant in an area of CA TECNISIGN AC PARCERIA responsible for the management of the entity's infrastructure, its products, its services, its facilities, and / or its practices as provided in Section 5.2.1
Posição de Confiança	Trusted Position	Positions within an area of CA TECNISIGN AC PARTNERSHIP that must be owned by a trustworthy person.
Sistema confiável	Trustworthy System	Computer hardware, software and procedures that are reasonably safe from intrusion and abuse; providing a reasonable level of availability, reliability and correct operation; are suitable for performing the intended functions; and enforce the applicable security policy.
TTL	TTL	Tempo de Vida – Time to Live

Nome de Domínio não registrado	Unregistered Domain Name	A domain name that is not a registered domain name.
UTC (k)	UTC(k)	Coordinated Universal Time - National realization of Coordinated Universal Time
certificado válido	Valid Certificate	A certificate which has undergone the
		validation specified in RFC 5280
Especialistas de validação	Validation Specialists	Someone who performs the information validation functions specified by these requirements
Período de validade	Validity Period	The period of time measured from the date the certificate is issued until the expiry date
Parecer Legal Verificado	Verified Legal Opinion	A document that meets the requirements specified in section 11.11.1 of these Guidelines
Método de comunicação Verificada	Verified Method of Communication	The use of a CA-confirmed telephone number, fax number, e-mail address or delivery mailing address, pursuant to Section 11.5 as a reliable way to communicate with the Applicant.
Carta Professional Verificada	Verified Professional Letter	Verified Professional Letter
VOID	VOID	Voice Over Internet Protocol
Programa EV WebTrust	WebTrust EV Program	The additional auditing procedures specified for ACs issuing EV certificates by AICPA / CICA to be used in conjunction with its WebTrust Certification Authorities Program
Programa WebTrust para ACs	WebTrust Program for CAs	The current version of the AICPA / CICA WebTrust Program for Certification Authorities
Seal WebTrust de fiabilidade	WebTrust Seal of Assurance	A statement of compliance resulting from the WebTrust Program for CAs
Certificado Wildcard	Wildcard Certificate	A certificate containing an asterisk (*) in the leftmost position of the Subject field contained in the SSL certificate
Nome de Domínio Wildcard	Wildcard Domain Name	A domain name that consists of a single asterisk character followed by a single dot character ("*".) Followed by a fully qualified domain name

Table -Acronyms and Definitions

Appendix B: References

- CA/Browser Forum - Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates- version 1.6.7 (available at https://cabforum.org/baseline-requirementsdocuments/)
- CA/Browser Forum - Guidelines For The Issuance And Management Of Extended Validation Certificates – version 1.6.8 (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 2.1, available at http://www.webtrust.org/principles-and-criteria/docs/item85228.pdf
- X.509, Recommendation ITU-T X.509 (10/2012) | ISO/IEC 9594-8:2014 (E), Information technology – Open Systems Interconnection – The Diretory: Public-key and attribute certificate frameworks.
- Ley Sobre Firmas Electrónicas Decreto N°,149-2013 publicado en el Diario Oficial LA GACETA el 11 de diciembre del 2013
- ACUERDO EJECUTIVO № 41-2014, emitido el 12 de diciembre del 2014 (Oficio SECM №155-2015) y publicado en el Diario Oficial LA GACETA el 21 de mayo del 2015