# DIGITALSIGN – CERTIFICADORA DIGITAL, SA.

# CERTIFICATION PRACTICE STATEMENT

**VERSION 3.6 – 20/09/2019**

## VERSION HISTORY

| *Date* | *Edition nr* | *Content* |
|---|---|---|
| 20/07/2009 | 1.0 | Initial draft |
| 21/06/2010 | 1.1 | Revision |
| 07/01/2011 | 1.2 | Name Change |
| 22/02/2012 | 1.3 | Changing membership and creation of "Grupo de Gestão" |
| 28/03/2013 | 2.0 | Review and inclusion of the TimeStamp Certificate Profile |
| 23/10/2013 | 2.1 | Revision |
| 25/03/2015 | 2.2 | Revision |
| 01/07/2016 | 3.0 | Adaptation to thr Regulation (EU) n.º 910/2014 |
| 18/10/2016 | 3.1 | Revision |
| 20/07/2017 | 3.2 | Revision to include Remote Signature Solution |
| 21/12/2017 | 3.3 | Revision |
| 29/01/2018 | 3.4 | Revision |
| 19/09/2018 | 3.5 | Revision |
| 20/09/2019 | 3.6 | Revision |

## LEGAL NOTICE



Any question or request for information regarding the content of this document should be directed to suporte@digitalsign.pt.

## CONTENT

# 1. INTRODUCTION

On 31 October 2017, DigiCert Inc. completed the acquisition of Symantec Corporation's Website Security business unit. As a result, DigiCert is now the registered owner of the STN Certificate Policy and the PKI Services described within this document.

However a hybrid of references to both "VeriSign", "Symantec" and "DigiCert" shall be evident within this document for a period of time until it is operationally practical to complete the re-branding of the Certification Authorities and services. Any references to VeriSign or Symantec as a corporate entity should be strictly considered to be legacy language that solely reflects the history of ownership.

The purpose of this document is to define the practices and procedures used to support the certification activities by the Certification Authority DigitalSign – Certificadora Digital, SA ("EC DIGITALSIGN").

This document - Certification Practice Statement ("CPS") - is based on Certification Practice Statement of British Telecommunications plc and Certification Practice Statement of Symantec/Digicert/Quovadis (see https://www.trustwise.com/repository/CPS/cps.htm) complying with all National and European Community laws applicable, and to whom DigitalSign subcontracts electronic certification services according to established contracts between the parties, as the following table:

| ***Service*** | ***Subcontrated Entity*** |
|---|---|
| Certificates Generation | British Telecomunications, plc |
| Revocation Status | British Telecomunications, plc |
| Data Center | British Telecomunications, plc |

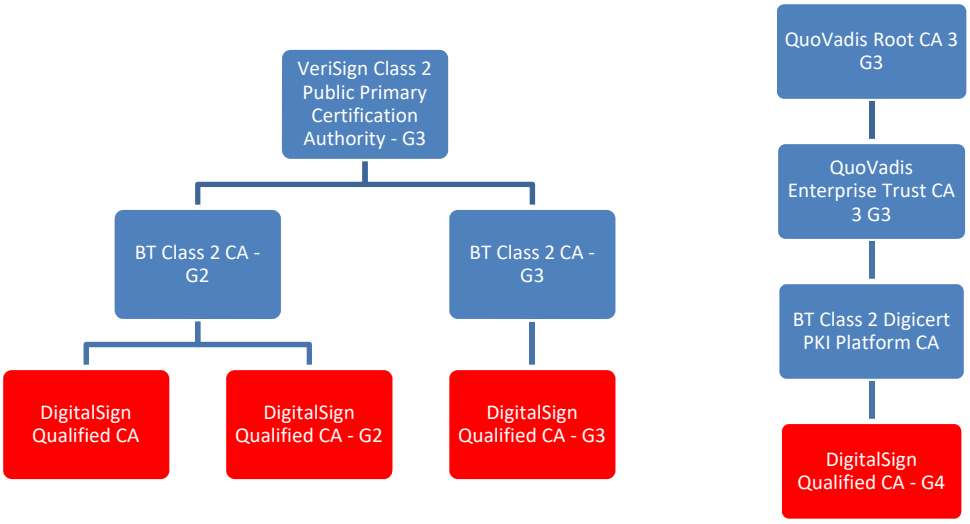
The subcontracted entities are responsible for implementing standards and procedures contained in this CPS, on the supply of outsourced services. The Management Group ("Grupo de Gestão"), as defined in paragraph 9.17.1 of this document, is responsible for ensuring the effective implementation of all processes and procedures of the management system and regularly review the need to readjust them in a logic of continuous improvement, through critical analysis of its effectiveness.

This group is also responsible for managing the regular monitoring of the relationship with subcontractors, in accordance with the appropriate procedure (PQ-06) for purchasing management and which is an integral part Quality Management System.

It establishes the practices that EC DIGITALSIGN employs in providing certification services that include, but are not limited to the issuance, management, revocation and renewal of qualified certificates, according to the requirements of the Symantec Trust Network Certificate Policies ("CP").

The CP is the principal statement of policy governing the STN. It establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates within the STN and providing associated trust services. These requirements, called the "STN Standards," protect the security and integrity of the STN, apply to all STN Participants, and thereby provide assurances of uniform trust throughout the STN. More information concerning the STN and STN Standards is available in the CP.

DigitalSign has authority over a portion of the STN, called its "Subdomain" of the STN. DigitalSign's subdomain DigitalSign includes entities subordinate to it, such as its Customers, End Users and Relying Parties.




The certificates issued under this intermediate certification authorities acquire the recognition obtained by ROOT in commercial applications (read: Browsers such as Internet Explorer, Google Chrome, Mozilla Firefox, etc.).

While the CP sets forth requirements that STN Participants must meet, this CPS describes how DigitalSign meets these requirements within DigitalSign's Subdomain of the STN. More specifically, this CPS describes the practices that DigitalSign employs for:

- Managing safely the core infrastructure that support the operations.
- Issue, manage, revoke and renew Qualified Digital Certificates.

For matters relating to the Time Stamping service, in conjunction with this CPS, should also be consulted the document "Políticas e Práticas de Certificação de Validação Cronológica", which is available in the repository of DigitalSign CA in: https://www.digitalsign.pt/ECDIGITALSIGN/cps.

This CPS is in compliance with the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policies and definition of Certification Practice Statement and may undergo regular updates.

## 1.1. OVERVIEW

Creation, signing and issuing certificates practices, as well as revocation of invalid certificates carried out by a Certification Authority ("CA") are essential to ensure the reliability and confidence of a Public Key Infrastructure ("PKI").

It respects and implements the following standards:

- RFC 3647: *Internet X.509 Public Key Infrastructure — Certificate Policy and Certification Practices Framework*
- RFC 3280: *Internet X.509 PKI - Certificate and CRL Profile*

This CPS complies with National and European legislation applicable to qualified certificates and specifies how to implement their procedures and controls, as well as the EC DIGITALSIGN reaches the specified requirements.

DigitalSign under this CA only offers qualified certificates. The CPS describes how DigitalSign meets the requirements of CP for this class of certificates, within its Subdomain.

DigitalSign may publish CPSs that are additional to this, in order to comply with specific policy requirements from the Government, or other industry standards and requirements.

This supplemental certificate policy, should be available to subscribers and relaying parties.

## 1.2. DOCUMENT NAME AND IDENTIFICATION

This document is the Certification Practice Statement of EC DIGITALSIGN. Certificates issued under the STN standard contain object identifier values corresponding to the applicable STN Class of Certificate, so DigitalSign did not associate any identifier to this CPS.

The Certificate Policy OID is used according to the explained in section 7.1.6.

This document is identified by the following information:

| ***Document Information*** | |
|---|---|
| Version/Edition | 3.6 |
| Date of Approval | 20/09/2019 |
| Expiration date | Non applicable |
| Location | https://www.digitalsign.pt/ECDIGITALSIGN/cps |

## 1.3. PKI PARTICIPANTS

### 1.3.1. CERTIFICATION AUTHORITIES

The term "Certification Authority" means the entity that issues and manages digital certificates.

EC DIGITALSIGN is part of the Symantec/Digicert/Quovadis and BT trust hierarchy. EC DIGITALSIGN issues qualified certificates to natural and legal persons and provides necessary services such as online OCSP validation.

EC DIGITALSIGN is signed by BT, which in turn is signed by Symantec/Digicert/Quovadis.

### 1.3.2. REGISTRATION AUTHORITIES

A Registration Authority (RA) is an entity that performs identification and authentication of certificate applicants for end-user certificates, initiates or passes along revocation requests for end-user certificates, and approves applications for renewal or re-keying of certificates on behalf of a STN CA. DIGITALSIGN may act as an RA for certificates it issues.

Third parties, who enter into a contractual relationship with DigitalSign, may operate their own RA and authorize the issuance of certificates by the EC DIGITALSIGN. Third party RAs must abide by all the requirements of this CPS and the terms of their Contract with DigitalSign. Third Party RAs may implement more restrictive practices based on their internal requirements

The RA identification, when distinct from CA, should be part of the information contained in the qualified digital certificate through an "OU" identifier in the "Subject" field (eg OU = ER - Entity Name).

### 1.3.3. SUBSCRIBERS

Subscribers are end users of certificates issued by a CA. A subscriber is the entity named as the end-user certificate subscriber. Subscribers can be individuals or organizations, as well as technological equipment as OCSP validation or TimeStamp Authority.

### 1.3.4. RELYING PARTIES

Relying parties are individuals, entities or devices that rely on the validity of the mechanisms and procedures used in the process of association of the name of the holder with its public key, that is, trust that the certificate corresponds in fact to whom claims to own it.

In this CPS, It is considered a relying party, one that relies on content, validity and applicability of the certificate issued by EC DIGITALSIGN.

Relying parties may or may not also be a subscriber in the trust hierarchy of Symantec/Digicert/Quovadis (STN).

### 1.3.5. OTHER PARTICIPANTS

None.

## 1.4. CERTIFICATE USAGE

The certificates issued by EC DIGITALSIGN are used by the various systems, applications, protocols and mechanisms, in order to ensure the following security services:

- Access control
- Integrity
- Authentication
- Non repudiation

These services are obtained by the use of public key cryptography, through their use in the trusting infrastructure that the EC DIGITALSIGN and STN / BT offer. Identification, authentication, integrity and non-repudiation services are achieved by using electronic signatures or electronic seals.

### 1.4.1. APPROPRIATE CERTIFICATE USES

Requirements and rules defined in this document apply to all certificates issued by EC DIGITALSIGN.

The licenses granted to natural persons, are intended to be used in any application for purposes of qualified electronic signature.

The licenses granted to legal persons, are intended to be used in any application for purposes of qualified electronic seal.

The certificates issued by EC DIGITALSIGN are also used by Relying Parties to verify its chain of trust, as well as to ensure the authenticity and identity of the sender of a electronic signature or electronic seal generated by the private key corresponding to the public key contained in this certificate.

### 1.4.2. PROHIBITED CERTIFICATE USES

Certificates shall be used only to the extent the use is consistent with applicable law.

The certificates issued by EC DIGITALSIGN are not designed, intended, or authorized for use or resale in equipment control in hazardous circumstances or for uses requiring a failsafe performance as nuclear plants, aviation, air traffic control system or gun control, where a failure could lead directly to death, personal injury, or severe environmental damage.

CA certificates cannot be used in any function other than the functions of the CA. Additionally, the end-user certificates cannot be used as CA certificates.

## 1.5. POLICY ADMINISTRATION

### 1.5.1. ORGANISATION ADMINISTERING THE DOCUMENT

DigitalSign – Certificadora Digital, SA.
Largo Padre Bernardino Ribeiro Fernandes, 26
4835-489 Nespereira – Guimarães
Portugal

### 1.5.2. CONTACT PERSON

Álvaro Matos
DigitalSign – Certificadora Digital, SA.
Largo Padre Bernardino Ribeiro Fernandes, 26
4835-489 Nespereira – Guimarães
Portugal
Email: suporte@digitalsign.pt
Telephone nr: +351 253560650
Fax: +351 253560639

### 1.5.3. COMPLIANCE DETERMINATION

The working group of this policy evaluates the compliance and internal applicability of this CPS (and / or their respective CPs), submitting it to the approval of DigitalSign's Administration, which is the competent body to determine its suitability to the applicable legislation.

### 1.5.4. APPROVAL PROCEDURES

The internal approval of this CPS (and / or their respective CPs) and following fixes and / or updates are made by the working group of this policy.

After internal approval, should be given their compliance, as described in the previous paragraph.

As part of a trust hierarchy, corrections and/or updates to this CPS shall be validated by the issuing CA (British Telecommunications Plc).

Corrections and / or updates shall be published in the form of new versions of the CPS (and / or their respective CPs), replacing any previous version.

## 1.6. DEFINITIONS AND ACRONYMS

See Appendix A.

# 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

## 2.1. REPOSITORIES

DigitalSign is responsible for the repository of its own EC DIGITALSIGN. DigitalSign publishes all certificates it issues in the repository, in accordance with Section 2.2.

After a certificate revocation, DigitalSign publishes notice of such revocation in the repository. DigitalSign issues Certificate Revocation Lists (CRLs) to its STN subdomain, under the provisions of this CPS. Additionally, for customers who have hired the Online Certificate Status Protocol (OCSP), DigitalSign OSCP provides the service, under the provisions of this CPS.

## 2.2. PUBLICATION OF CERTIFICATE INFORMATION

DigitalSign maintains a Web-based repository, which allows the relying parties to make online enquires regarding revocations and other information about the status of the certificates. DigitalSign provides information to relying parties on how to find the appropriate repository to check the status of certificates and, if the Online Certificate Status Protocol (OCSP) is available, how to find the corresponding OSCP.

DigitalSign publishes in its repository and the certificates it issues and, upon revocation of a certificate, publishes notice of such revocation. Additionally, DigitalSign issues Certificate Revocation Lists and, if available, provides OCSP services for EC DIGITALSIGN.

DigitalSign is responsible for the repository for EC DIGITALSIGN.

DigitalSign always publishes, at least, the following public information online:

- Electronic copy of this CPS (https://www.digitalsign.pt/ECDIGITALSIGN/cps)
- CRLs:
  - Certificates issued by EC "DigitalSign Qualified CA": (http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificate/LatestCRL.crl)
  - Certificates issued by EC "DigitalSign Qualified CA – G2": (http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG2/LatestCRL.crl)
  - Certificates issued by EC "DigitalSign Qualified CA – G3": (http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG3/LatestCRL.crl)
  - Certificates issued by EC "DigitalSign Qualified CA – G4": (http://onsitecrl.trustwise.com/DigitalSignCertificadoraDigitalQualifiedCertificateG4/LatestCRL.crl)

## 2.3. FREQUENCY OF PUBLICATION

Updates to this CPS and CP are published in accordance with Section 9.12.

Certificates are published after emission. The CRL is published daily.

Additional information about the status of the certificate is published in accordance with the provisions of this CPS.

## 2.4. ACCESS CONTROL ON REPOSITORIES

The information published in the DigitalSign repository is publicly available being guaranteed unrestricted access to read.

DigitalSign implemented measures regarding logical and physical security to prevent unauthorized persons from adding, erasing or modifying entries from the repositories.

# 3. IDENTIFICATION AND AUTHENTICATION

## 3.1. NAMING

The naming follows the applicable law. For certificates issued to individuals and organizations it is assigned its real name.

### 3.1.1. TYPES OF NAMES

The certificates issued by EC DIGITALSIGN are identified by a unique name in the Issuer and Subject fields, called Distinguished Name - DN, according to the X.501 standard.

DN consist of, as specified in the following table:

| *Attribute* | *Value* |
|---|---|
| Country – "C" | "PT", or other according to ISO 3166 table. |
| Organization – "O" | Name of organization to which belongs the signature holder (where applicable) |
| Organizational Unit – "OU" | Digital certificates can contain attributes OU, according to the corresponding PC |
| State or Province – "S" | The District of the signatory, or unused |
| Locality – "L" | The Location of the signatory, or unused |
| Common Name – "CN" | Certificate's Holder, service or organization represented by the holder |
| Email Address – "E" | Email address associated with the signature holder (where applicable) |
| First Name (Given Name – "G") | Holder's first name(s), when issued to natural persons, or unused |
| Last Name (Surname – "SN") | Holder's last name(s), when issued to natural persons, or unused |
| ID (SERIALNUMBER) | Holder's ID, when issued to natural persons, or unused |
| ID (Organization Identifier) | Organization's ID, or unused |
| Title – "T" | Professional title or another used by the certificate holder |

### 3.1.2. NEED FOR NAMES TO BE MEANINGFUL

EC DIGITALSIGN will ensure, within its subdomain of the STN:

- The uniqueness of the information contained in the DN.
- All data included in the DN field are properly validated and authenticated, and are easily identifiable by the Humans, allowing unequivocal determination of the respective holder.

### 3.1.3. ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

Qualified certificate subscribers can use pseudonyms (names other than their real name). In this case, an indication that a pseudonym is being used will be indicated in the "Observations" field.

It is not authorized anonymity.

Only when the technical constraints inherent to maximum sizes defined for each field are limiting to contain all of the information, may be authorized abbreviations, provided that they are easily identifiable by Humans.

### 3.1.4. RULES FOR INTERPRETING VARIOUS NAME FORMS

Not stipulated.

### 3.1.5. UNIQUENESS OF NAMES

DigitalSign ensures that the data in the DN are unique within their CA through automated components in the process of holders registration. It is possible for an owner to have two or more certificates with the same DN.

### 3.1.6. RECOGNITION, AUTHENTICATION AND ROLE OF TRADEMARKS

Entities requesting certificates must demonstrate the right to use of the requested name. The designations used on the certificates issued by EC DIGITALSIGN can not infringe intellectual property rights of others.

In the procedure of identification and authentication of the certificate holder, prior to the issuing of the same, the entity requesting the certificate will have to present legal documents that demonstrate the right to the use of the requested name.

DigitalSign does not arbitrate, mediate, or otherwise resolve any dispute relating to the ownership of any name or tag. DigitalSign reserves the right, without liability to any certificate subscriber, to reject any order due to such disputes.

## 3.2. INITIAL IDENTITY VALIDATION

For all certificates, it is mandatory that the initial registration be carried out in person or in an equivalent way, in order to ensure that the person who is going to be issued the certificate is who he actually says he is.

The process of identity validation can be achieved through three alternative ways:

a) in person at DigitalSign (or authorized RA); or

b) presentation of supporting documents which required physical presence to obtain, as is the case of ID or CC, complemented with appropriate signature recognition by Notary (or equivalent entity according to the law); or

c) through remote videoconferencing.

These practices are in accordance with the document ETSI EN 319 411-2 and in accordance with the legislation.

In this CPS are described all necessary steps, from the beginning of the certificate request until the issuance of the digital certificate to the holder.

### 3.2.1. METHOD TO PROVE POSSESSION OF PRIVATE KEY

DigitalSign uses various circuits for issuing certificates in which the private key is managed differently. Either the user or DigitalSign can create the private key.

The key creation method used is shown in the certificate, through the Policy ID and the Description attribute in the certificate DN field. These codes are described in the corresponding policies and in the certificate profile records.

a) Keys created by DigitalSign:
The keys can be delivered by DigitalSign to the Subject/Signatory, directly or through a registration authority on a qualified signature creation device (QSCD).

b) Keys created by the Signatory:
Proof of ownership of the private key in this case is the request that DigitalSign receives in **PKCS#10** format.

### 3.2.2. AUTHENTICATION OF ORGANIZATION IDENTITY

The process of authenticating the identity of a legal person shall ensure that the legal person who is going to be issued the certificate exists, and this verification is carried out by consulting the official documentation.

Any additional information included in the DN is verified and authenticated by the validation services.

### 3.2.3. AUTHENTICATION OF INDIVIDUAL IDENTITY

The process of identity authentication of a natural person ensures that the person who is going to be issued the certificate is who he actually says he is, through submission of documentation as well as the signature. This can be achieved by three distinct ways:

a) in person at DigitalSign (or authorized RA); or

b) presentation of supporting documents which required physical presence to obtain, as is the case of ID or CC, complemented with appropriate signature recognition by Notary (or equivalent entity according to the law); or

c) through remote videoconferencing.

The verification of the identity and powers of the representative/attorney (if applicable) is made indirectly through documental means by a notary or entity with legal authority for the recognition of signatures, in quality and empowered to act.

Any additional information included in the DN is verified and authenticated by the validation services.

### 3.2.4. NON-VERIFIED SUBSCRIBER INFORMATION

All the information included in the DN is checked and authenticated by the validation services.

### 3.2.5. VALIDATION OF AUTHORITY

All information relating to powers of attorney and / or affiliation of an individual to the corresponding company or organization is verified.

### 3.2.6. CRITERIA FOR INTEROPERATION

DigitalSign does not provide interoperation services that permit a non-STN CA to interoperate with the STN by unilaterally certifying that CA.

The interoperability between STN CAs is guaranteed by its own trust hierarchy, being the root (Symantec/Digicert/Quovadis) automatically available by the overwhelming majority of browsers, equipment and other software existing globally.

## 3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

Prior to the expiration of an existing certificate it is necessary to renew that certificate so that the holder maintains the continuity of its use.

DigitalSign requires for this purpose the creation of a new key pair to replace the expiring key pair (technically defined as "re-key", but in this document identified as 'renewal').

The process of creating a new key pair can be driven internally by DigitalSign, or directly by the owner (or representative) of the certificate, being guaranteed the creation of the same approved cryptographic device. In this case it is also required knowledge of "the Identification Phrase" defined by the holder during the initial request.

Verification of identity and other data contained in the DN is always checked by the validation services from DigitalSign in accordance with the following:

- If the information on the renewal process is identical to the information in the process of initial authentication, and that authentication has been performed in the least two years, the request is automatically approved without submission of documentation or proof of additional identity.
- If the information on the renewal process is not identical to the information in the initial authentication process, or that authentication has been performed for more than two years ago, the process is treated as an initial request and shall be applicable all authentication and validation rules described in section 3.2.

### 3.3.1. ROUTINE RE-KEY AND RENEWAL FOR CA CERTIFICATES

Not applicable.

### 3.3.2. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

It is not possible to renew a certificate after it has been revoked, being always applied the rules of authentication and validation described in section 3.2.

However, the documents and information contained in the initial request may be used for that purpose, as long as they remain valid.

## 3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Prior to the revocation of a Certificate, DigitalSign verifies that the revocation was requested by the certificate holder or by the entity that approved the request.

The accepted procedures to authenticate revocation requests include:

- To request the holder "the Identification Phrase" and revoke the certificate automatically if matches the existing records
- Receive a message, supposedly from its holder, that asks the revocation and contains a verifiable digital signature, with reference to the certificate to be revoked.
- Written request of the holder

Additionally, DigitalSign may proceed with the revocation of any certificate, since it is aware (after verification) that the information contained in the DN does not reflect the current reality.

# 4. OPERATIONAL REQUIREMENTS

## 4.1. CERTIFICATE APPLICATION

### 4.1.1. WHO CAN SUBMIT A CERTIFICATE APPLICATION

Requests for Certificates Applications may be submitted by:

- An individual who is the holder of the certificate
- A representative of the certificate holder, duly authorized and empowered to the effect
- A legal person who is the holder of the certificate
- A representative of EC DIGITALSIGN
- An authorized representative of an RA

### 4.1.2. ENROLMENT PROCESS AND RESPONSIBILITIES

#### 4.1.2.1. END-USER SUBSCRIBER CERTIFICATES

All end-user certificates must agree with the terms of the "Subscriber Agreement", which contains representations and warranties described in section 9.6.3. and undergo an enrolment process that consists of completing an application form and provide true and correct information, and all supporting documents required for the validation of the information contained in the certificate.

For renewal processes, it can:

- Create a key pair in an approved cryptographic device (as defined in section 3.3)
- Submit its public key using the tools provided by RA
- Demonstrate ownership and / or exclusive control of the private key corresponding to the public key delivered

#### 4.1.2.2. RA CERTIFICATES

Entities wishing to establish itself as RAs are subjected to the conclusion of a contract with DigitalSign.

RA must provide their credentials to prove their identity and to provide contact information during the hiring process. During this process, the candidate to RA must cooperate with DigitalSign to determine the content of the certificates to be issued by the candidate.

## 4.2. CERTIFICATE APPLICATION PROCESSING

### 4.2.1. PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

The DigitalSign, or a RA, must perform the identification and authentication of all requests, in accordance with Section 3.2.

### 4.2.2. APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

DigitalSign, or a RA , will approve the certificate requests if the following criteria are met:

- Successful identification and authentication of all information, in accordance with Section 3.2
- Once the payment is made or approved.

In the case of an initial process, RA will perform initialization and customizing (if applicable) of the approved cryptographic device, which will perform the generation of the key pair, and subsequent request to EC DIGITALSIGN for issuing the certificate.

Similarly, in renewal cases where the creation of the key pair is performed by RA, RA request to EC DIGITALSIGN for issuing the certificate.

In cases of renewal where the generation of the key pair is made by the holder of the certificate, the RA will carry out the approval of the request.

DigitalSign, or a RA, reject the request for a certificate if any of the following situations occur:

- The identification and authentication, in accordance with Section 3.2, is not complete
- The subscriber does not deliver any supporting documentation requested
- The subscriber does not respond to notification within a specified time
- Payment is not executed
- The RA believes that issuing a certificate to the subscriber may bring discredit to the STN and DigitalSign itself.

### 4.2.3. TIME TO PROCESS CERTIFICATE APPLICATIONS

DigitalSign begins processing requests after receipt of the required documentation. There is no stipulated time to complete the process, unless otherwise is stated in the relevant subscriber agreement, CPS or other agreement between the participants. A request remains active until it is rejected.

## 4.3. CERTIFICATE ISSUANCE

### 4.3.1. CA ACTIONS DURING CERTIFICATE ISSUANCE

A certificate is created and issued following the approval of a certificate request for any of the RA. DigitalSign creates and sends to the certificate applicant (or his representative) a certificate based on the information received, supported in legal documents and following the approval by the RA.

Each issued certificate begins its term (validity) at the time of issue.

### 4.3.2. NOTIFICATIONS TO SUBSCRIBERS BY THE CA OF ISSUANCE OF CERTIFICATE

The notification of certificate issuance to the certificate applicant (or his representative) is done by covering letter when sending it (and corresponding approved cryptographic device).

In cases of renewal (with the creation of key pairs by the certificate applicant) the certificate applicant is notified via e-mail message, which also includes installation instructions.

## 4.4. CERTIFICATE ACCEPTANCE

### 4.4.1. CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

Together with the notification of emission, according to Section 4.3.2, it is also sent to the certificate applicant the "Reception Term", which will be required to be signed by the certificate applicant himself, or it's representative(s).

Only when checked the compliance of the signature, will be sent an access code to the approved cryptographic device, necessary for using the corresponding private key.

This situation does not apply in cases of renewal with the creation of the key pair by the certificate applicant, when the certificate is intended for equipment, or when using a remote signature solution where the acceptance process is completed if the holder does not reject the certificate or its contents.

### 4.4.2. PUBLICATION OF THE CERTIFICATE BY THE CA

DigitalSign publishes the certificates issued in a publicly accessible repository.

### 4.4.3. NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

RA may receive notice of the issuance of certificates approved by them.

## 4.5. KEY PAIR AND CERTIFICATE USAGE

### 4.5.1. SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

The use of the private key corresponding to the public key in the certificate, should be allowed only when the holder agree to the subscriber agreement and accept the certificate. This should be used lawfully, in accordance with the subscriber agreement of DigitalSign under this CPS.

The certificate holders will use their private key only for the purpose for which they are intended (as stated in the certificate field "keyUsage") and always for legal purposes.

Time Stamp Certificates are used in Time Stamp servers.

Holders should protect their private key against unauthorized use, and must discontinue use of the private key following the expiration or revocation of the certificate.

### 4.5.2. RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

Relying Parties must agree to the terms stated in this CPS and in the relevant certification policy as a condition of trust in the certificate.

Before any act of trust, relying parties should independently evaluate:

- the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by this CPS. DigitalSign is not responsible for assessing the appropriateness of the use of a Certificate.
- that the certificate is being used as specified in the "KeyUsage" included in the certificate (eg, if the digital signature is not enabled, then the certificate cannot be trusted to validate the signature of the holder).
- the status of the certificate and all the CAs in the chain that issued the certificate. If any of the certificates in the certificate chain is revoked, the Relying Party is solely responsible for evaluating whether it is reasonable to trust a digital signature, made before the date of revocation. Any such reliance is made solely at the risk of the Relying party.
- Have knowledge and understand the use and functionality provided by public key cryptography and certificates.
- Read and understand the terms and conditions described in the policies and certification practices.

Assuming the use of the certificate is appropriate, relying parties must use the software and / or the appropriate hardware to perform electronic signature or electronic seal verification or other cryptographic operations that they wish to carry on the condition of trust certificates in connection with such operations. Such operations include identifying a Certificate Chain and verifying the digital signature on all certificates in the certificate chain.

## 4.6. CERTIFICATE RENEWAL

The renewal of a certificate using the same key pair is not acceptable by EC DIGITALSIGN.

## 4.7. CERTIFICATE RE-KEY

DigitalSign requires for this purpose the creation of a new key pair to replace the expiring key pair (technically defined as "re-key", but in this document identified as 'renewal').

### 4.7.1. CIRCUMSTANCES FOR CERTIFICATE RE-KEY

Prior to the expiration of an existing certificate, it is necessary to renew that certificate in order to the holder (or his representative) maintain the continuity of its use.

A certificate may be renewed after its expiration.

### 4.7.2. WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

See section 4.1.1.

### 4.7.3. PROCESSING CERTIFICATE RE-KEY REQUESTS

See section 4.1.2 e 4.2.

### 4.7.4. NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

See section 4.3.2.

### 4.7.5. CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE

See section 4.4.1.

### 4.7.6. PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA

See section 4.4.2.

### 4.7.7. NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

See section 4.4.3.

## 4.8. CERTIFICATE MODIFICATION

This is a practice not supported by EC DIGITALSIGN.

## 4.9. CERTIFICATE REVOCATION AND SUSPENSION

Revocation or suspension of certificate is only applicable if made within the period of validity of the certificate, meaning that it loses its operability.

The revoked certificates cannot be reactivated, ie, be valid again.

EC DIGITALSIGN does not support the certificate suspension.

### 4.9.1. CIRCUMSTANCES FOR REVOCATION

Only in the circumstances listed below, a certificate is revoked and published in the CRL:

- Compromise or suspected to have been compromised the private key.
- DigitalSign or the RA have reason to believe that a person has violated an obligation or warranty under the contract applied.
- The contract with the holder has terminated.
- The information contained in the DN does not reflect the current reality.
- There is reason to believe that the certificate was issued in an inconsistent manner with the procedures required and applicable by the CPS.
- The data contained in the DN is false.
- By legal or administrative resolution.
- Loss, destruction or deterioration of the support device of the private key.
- Revocation of the EC DIGITALSIGN or any other CA in the certificate chain.
- The continued use of the certificate can be harmful to the STN and DigitalSign.

When considered whether certificate usage is harmful to the STN, BT, Symantec and DigitalSign consider among other things:

- The nature and number of complaints received.
- The identity of the complainant.
- The relevant legislation in force.
- The responses to alleged harmful use from the Subscriber.

Certificate subscriber agreements with DigitalSign require that the holders (or its representatives) immediately notify DigitalSign (or corresponding RA) if they know, or suspect, that their private key is compromised.

### 4.9.2. WHO CAN REQUEST REVOCATION

Subscribers may request the revocation of their licenses. The entity that approved the Certificate (RA) can also apply for revocation of the certificate approved.

### 4.9.3. PROCEDURE FOR REVOCATION REQUEST

See section 3.4.

### 4.9.4. REVOCATION REQUEST GRACE PERIOD

Revocation requests must be submitted as soon as possible. After being performed all procedures and it is verified that the request is valid, the request cannot be canceled.

### 4.9.5. TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

DigitalSign (or RA) shall treat such requests as a priority. Updating the revocation status will be performed over a maximum period of 8 working hours.

### 4.9.6. REVOCATION CHECKING REQUIREMENTS FOR RELYING PARTIES

Relying Parties must check the status of Certificates on which they wish to rely. One method by which Relying Parties may check Certificate status is by consulting the most recent CRL published by the CA that issued the Certificate on which the Relying Party wishes to rely.

Alternatively, Relying Parties may meet this requirement either by checking Certificate status using the applicable web-based repository, or OCSP responder (where available) to check revocation status.

### 4.9.7. CRL ISSUANCE FREQUENCY

The CRL is issued at least once a day for end-user certificates. CRL for CA Certificates shall be issued at least annually, but also whenever a CA is revoked.

If a certificate listed in the CRL expires, it can be removed from the later-issued CRL after the expiry of the certificate.

### 4.9.8. MAXIMUM LATENCY FOR CRLS

After creating CRL, these are published in the repository within a very brief period. Typically this is accomplished automatically within minutes after creation.

### 4.9.9. ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

Revocations and other information about the status of the certificates are available through the web-based repository and, where provided, through the OCSP service. In addition to publishing the CRL, DigitalSign provides information on the status of the certificate through query functions in the DigitalSign repository.

The certificate status information is available via query functions, accessible via the DigitalSign repository at:

- Certificates issued by EC "DigitalSign Qualified CA":
  (https://onsite.trustwise.com/services/DigitalSignCertificadoraDigitalQualifiedCertificate/client/search.htm)
- Certificates issued by EC "DigitalSign Qualified CA – G2":
  (https://onsite.trustwise.com/services/DigitalSignCertificadoraDigitalQualifiedCertificateG2/client/search.htm)
- Certificates issued by EC "DigitalSign Qualified CA – G3":
  (https://onsite.trustwise.com/services/DigitalSignCertificadoraDigitalQualifiedCertificateG3/client/search.htm)
- Certificates issued by EC "DigitalSign Qualified CA – G4":
  (https://onsite.trustwise.com/services/DigitalSignCertificadoraDigitalQualifiedCertificateG4/client/search.htm)

DigitalSign also provides OCSP services. Customers who have contracted these services should check the status of the certificate by using OCSP. The URL for OCSP is communicated to the client.

### 4.9.10. ON-LINE REVOCATION CHECKING REQUIREMENTS

Relying parties must have software / hardware able to access the information provided about the revocation status of certificates.

### 4.9.11. OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

Non applicable.

#### 4.9.12. SPECIAL REQUIREMENTS REGARDING KEY COMPROMISE
DigitalSign will use all commercially reasonable efforts to notify potential relying parties, if it discovers, or have reason to believe that the private key of its own CA is compromised.

#### 4.9.13. CIRCUMSTANCES FOR SUSPENSION
Non applicable.

#### 4.9.14. WHO CAN REQUEST SUSPENSION
Non applicable.

#### 4.9.15. PROCEDURE FOR SUSPENSION REQUEST
Non applicable.

#### 4.9.16. LIMITS ON SUSPENSION PERIOD
Non applicable.

## 4.10. CERTIFICATE STATUS SERVICES

#### 4.10.1. OPERATIONAL CHARACTERISTICS
The state of public certificates is publicly available through the CRL and via OCSP respond (where available).

#### 4.10.2. SERVICE AVAILABILITY
The certificate status services are available 24 x 7 without any scheduled interruption.

#### 4.10.3. OPTIONAL FEATURES
The OSCP is an optional service that needs to be specifically enabled.

## 4.11. END OF SUBSCRIPTION
A subscriber may end a subscription of a certificate by:

- Allowing its certificate expire without renewing it.
- Revoking the certificate before the certificate expires, without replacing it.

## 4.12. KEY ESCROW AND RECOVERY
The escrow of CA, RA and end-user private keys is not permitted under this CPS.

DigitalSign does not in any way store or archive a Signatory's private key to create electronic signature/seal, except in the case of remote certification of a qualified certificate through the DigitalSign remote signature solution.

In this case, the private key is generated in a qualified signature creation device (QSCD) and encrypted in a reliable environment. The key encryption relies on a AES symmetric key (128 bits) wrapping key created by the QSCD and derived from the QSCD master wrapping key and the first authentication factor created/defined by the Signatory, which ensures that only he/she can access that private key

#### 4.12.1. KEY ESCROW AND RECOVERY POLICY AND PRACTICES

EC DIGITALSIGN's private key has been generated and is stored on Hardware Security Module (HSM) duly approved, being their protection guaranteed (backup) in identical device.

#### 4.12.2. SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

Non applicable.

# 5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

## 5.1. PHYSICAL CONTROLS

DigitalSign has implemented a Security Policy, which supports the security requirements of this CPS. The adequacy with these policies is included in the requirements for independent audit of DigitalSign described in section 8. The DigitalSign Security Policy contains sensitive security information and is only available through agreements with DigitalSign. An overview of the requirements is described below.

### 5.1.1. SITE LOCATION AND CONSTRUCTION

The operations DigitalSign's CA and RA are conducted within physically secure environments that dissuade, detect and prevent the use of unauthorized access or disclosure of sensitive information, whether hidden or evident.

DigitalSign also maintains facilities for the recovery of their CA operations in disaster situations. The facilities of DigitalSign for recovery in case of disaster are protected by multiple layers of physical security, comparable to the DigitalSign primary facilities.

### 5.1.2. PHYSICAL ACCESS

EC DIGITALSIGN systems are protected by a minimum of four hierarchical levels of physical security, with access requirements to access to the lower level before having access to the level in question.

Progressively restrictive physical access privileges control access to each level. The sensitive operational activities of the CA, ie, any activity on the life cycle of the certification process, such as authentication, verification and issuance, occur within very restricted access levels. Access to each level requires the use of a proximity card. Physical access is automatically logged and recorded in video. Additional levels require individual access controlled through the use of two authentication factors including biometrics. Personnel without escort, including non-accredited staff or visitors are not allowed in such security areas.

The physical security system includes additional tiers for key management security, which serves to protect both online and offline storage of Cryptographic Signing Units (CSUs) and keying material. Areas used to create and store cryptographic material enforce dual control, each through the use of two- factor authentication including biometrics. Online CSUs are protected through the use of locked cabinets. Offline CSUs are protected through the use of locked safes, cabinets and containers. Access to CSUs and keying material is restricted in accordance with BT's segregation of duties requirements. The opening and closing of cabinets or containers in these tiers is logged for audit purposes.

### 5.1.3. POWER AND AIR CONDITIONING

DigitalSign safety facilities are equipped with:

- Electricity systems to ensure continuous, uninterrupted access to electricity
- Heating / ventilation / air conditioning to control the temperature and relative humidity.

#### 5.1.4. WATER EXPOSURES
DigitalSign took precautions to minimize the impact of exposure to water, including flood detectors.

#### 5.1.5. FIRE PREVENTION AND PROTECTION
DigitalSign has taken the necessary precautions to prevent and extinguish fires or other exposure to flames or smoke that can be destructive. Preventive measures and protection of fires of DigitalSign are designed to comply with local safety regulations for fire.

#### 5.1.6. MEDIA STORAGE
All media containing production software and data, audit, archive or supporting information, are stored within the facility to control appropriate physical and logical access, designed to limit access to authorized personnel and protect such media information from possible accidental damage (eg, water, fire, and electromagnetic).

#### 5.1.7. WASTE DISPOSAL
Documents and paper materials containing sensitive information are shredded before disposal.

Brackets for electronic collection, storage or transmission of sensitive data are safely formatted or destroyed physically, according to the manufacturer's instructions.

Other wastes are treated according to the rules defined internally by DigitalSign.

#### 5.1.8. OFF-SITE BACKUP
Backups of critical data and routine audit logs are made. All backups are stored off-premises in safe environments.

## 5.2. PROCEDURAL CONTROLS

#### 5.2.1. TRUST ROLES
It are defined as Trusted Persons all officials, employees, contractors and consultants who have access or control authentication or encryption operations, which could materially affect:

- Validation of information for certificate issuance requests.
- The acceptance, rejection, or other processes for subscription of certificates, requests for revocation or renewal, or enrollment information.
- The issuance or revocation of certificates, including personnel having access to restricted portions of the repository.
- Handling of End User information or requests.

Trusted Persons include, but are not limited to:

- Personal of customer's service.
- Cryptographic operations Personnel.

- Security personnel.
- Management and operating systems Personnel.

DigitalSign considers the categories of personnel identification in this section as Trusted Persons having Positions of Trust. People seeking to become Trusted Persons by obtaining a position of Security, must successfully complete the requirements of this CPS.

### 5.2.2. NUMBER OF PEOPLE REQUIRED PER TASK

DigitalSign has established and maintains a policy of strict control procedures to ensure segregation of duties, based on the responsibilities of each task, and ensuring that multiple Trusted Persons are required to perform sensitive tasks.

Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (cryptographic signing unit or CSU) and associated key material, require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device. Persons with physical access to modules do not hold "Secret Shares" and vice versa.

Other manual operations such as the validation and issuance of qualified certificates, require the participation of at least two Trusted Persons, or a combination of at least one trusted person and automated process for validation and issuance.

### 5.2.3. IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing BT HR (or equivalent) or security functions and a check of well recognized forms of identification (e.g., passports and driver's licenses). Identity is further confirmed through the background checking procedures described in this CPS.

DigitalSign ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are granted access to:

- issued access devices and granted access to the required facilities.
- issued electronic credentials to access and perform specific functions on CA, RA, or other IT systems.

### 5.2.4. ROLES REQUIRING SEPARATION OF DUTIES

Roles requiring separation of duties include, but are not limited to:

- Validation of information in requests for issuing certificates, requests for renewal or revocation, or renewal of information.
- Issuance and revocation of certificates, including staff with access to restricted parts of the repository.
- handling information or requests from the subscriber.

- Creation, destruction or issuance of a CA Certificate.

## 5.3. PERSONNEL CONTROLS

Anyone who seeks to be a trusted person shall provide evidence of the requirements, qualifications and experience necessary to perform their possible liability tasks competently and satisfactorily. The verification of the data collected is repeated at least every 10 years for personnel holding Trusted Positions.

### 5.3.1. BACKGROUND, QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS

DigitalSign requires that staff try to be a Trusted Person, must provide evidence of background, qualifications, experience and clearance necessary to perform their possible liability tasks, competently and satisfactorily.

### 5.3.2. BACKGROUND CHECK PROCEDURES

Before granting the status of trusted person DigitalSign conducts background checks, which include but are not imitated to the following:

- Arrests for criminal offenses or criminal penalties associated with the nature of the job. As an example, crimes involving financial fraud (ie, embezzlement, theft, diversion).
- Any pattern of behavior that indicates personal irresponsibility, for example:
    - Arrests for driving under the influence of alcohol or drugs.
    - Bankruptcy declarations.
    - Recent credit problems (up to 3 years) (ie, missed mortgage or car payments).
- Any add on the resume or involving professional applications:
    - False employment statements (ie, claim to have worked for an employer particularly when it never did).
    - False statement on the academic qualifications (ie, claiming to be holder of a degree without ever having obtained it, or inflate the grade level that actually has as claiming to be the possessor of a degree having only obtained a Bachelor's degree).

To the extent that any of these requirements imposed by this section are not met due to prohibitions or limitations of local law or other circumstances, DigitalSign will use a surrogate research technique permitted by law, that provides substantially similar information, including, but not limited the respective background checks.

Factors revealed in the background check that could be considered for rejection of candidates for Trusting Positions or for developing actions against existing trusted person generally include (but are not limited to) the following:

- False presentation made by the candidate or trusted person.
- References highly adverse or unreliable.
- Certain criminal convictions.
- Indications of a lack financial responsibility.

Reports containing such information are evaluated by human resources and security personnel, which determine the appropriate action in the light of the type, magnitude and

frequency of the behavior, discovered by checking its past. Such actions may include measures covering the cancellation of offers of employment made to candidates for Trusting Positions or the end of the occupation of existing Trusted Persons.

The use of information revealed in the background check is subject to local law.

### 5.3.3. TRAINING REQUIREMENTS

DigitalSign provides its personnel with training upon hire as well as the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily. DigitalSign maintains records of such trainings in its Quality Management System ISO 9001 (QMS). DigitalSign periodically review and amend its program of training, if necessary.

The training programs / courses are tailored to the individual's responsibilities and include the following:

- Basic concepts of Public Key Infrastructures
- Job responsibilities
- Operational policies and safety procedures
- Use and operation of implemented hardware and software
- Report and handling incidents
- Recovery procedures and business continuity in the event of disaster

### 5.3.4. RETRAINING FREQUENCY AND REQUIREMENTS

DigitalSign provides refresher training and updates to its staff, to the extent and frequency required to ensure that staff maintain proficiency levels required to perform their duties with responsibility, competence and satisfaction. Periodic training of safety awareness is provided on a regular basis.

### 5.3.5. JOB ROTATION FREQUENCY AND SEQUENCE

Non stipulated.

### 5.3.6. SANCTIONS FOR UNAUTHORISED ACTIONS

Appropriate disciplinary sanctions are carried out due to unauthorized actions or other violations of the policies and procedures of DigitalSign. Disciplinary sanctions may include measures such as the end of the contract and are proportional to the frequency and severity of the unauthorized actions.

### 5.3.7. CONTRACTING PERSONNEL REQUIREMENTS

In exceptional situations, contractors or consultants may be used to fill positions of trust. To these subcontractors or consultants will be required the same security criteria that an employee of DigitalSign in equivalent role.

Subcontractors and independent consultants, who have not completed or passed the background check procedures specified in this CPS in section 5.3.2, only have access to the security facilities of DigitalSign in the extent they are escorted and directly supervised at all times by Trusted Persons.

#### 5.3.8. DOCUMENTATION SUPPLIED TO PERSONNEL

DigitalSign provides to its employees required training and other documents necessary to perform their work with responsibility and competence.

## 5.4. AUDIT LOGGING PROCEDURES

#### 5.4.1. TYPES OF EVENTS RECORDED

DigitalSign, manually or automatically records the following types of significant events:

- CA key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction
  - Cryptographic device life cycle management events
- CA and End User certificate life cycle management events, including:
  - Certificate request, renewal and revocation
  - Successful or unsuccessful processing of requests
  - Generation and issuance of certificates and CRLs
- Events related to security, including:
  - Attempts to access the PKI system, with or without success
  - Actions in the PKI and security systems performed by personnel of DigitalSign
  - Security sensitive files or records read, written or deleted
  - Changes to the security profiles
  - System and hardware failures and other anomalies
  - Activity of the firewall and routers
  - Entry and exit of visitors in the premises

Log entries include include the following:

- Date and time of entry
- Serial number or sequence of entry, for automatic daily entries
- Identity of the entity making the daily intake
- Input Type

The audit record for the RAs and MPKI Service Management Administrators includes:

- Type of identification documents presented by the applicant to the certificate
- Record of unique identification data, numbers, or a combination thereof (e.g., Certificate Applicant's drivers license number) of identification documents, if applicable
- Storage location of copies of candidates and identification documents
- Identity of entity accepting the request
- Method used to validate identification documents, if any

- Name of receiving CA or submitting RA, if appropriate

#### 5.4.2. FREQUENCY OF PROCESSING LOG

Audit logs are examined on at least a weekly basis for significant security and operational events. In addition, DigitalSign reviews its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within CA and RA systems.

Audit log processing consists of a review of the audit logs and documentation for all significant events in an audit log summary. Audit log reviews include a verification that the log has not been tampered with, an inspection of all log entries, and an investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews are also documented.

#### 5.4.3. RETENTION PERIOD FOR AUDIT LOG

Audit records are kept available until at least two months after the procedure and then filed in accordance with section 5.5.2.

#### 5.4.4. PROTECTION OF AUDIT LOG

Audit logs are protected by physical and logical access controls that include mechanisms to protect log files from unauthorized viewing, modification, deletion, or other tampering.

#### 5.4.5. AUDIT LOG BACKUP PROCEDURES

Incremental backups are created daily and full backups are performed weekly.

#### 5.4.6. AUDIT COLLECTION SYSTEM

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by DigitalSign personnel.

#### 5.4.7. NOTIFICATION TO EVENT-CAUSING SUBJECT

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

#### 5.4.8. VULNERABILITY ASSESSMENTS

Part of the audit records are used to monitor system vulnerabilities. Logical security vulnerability assessments ("LSVAs") are performed, as well as reviewed and analyzed.

The LSVAs are based on real-time automated records on a daily, monthly and annual basis.

### 5.5. RECORD ARCHIVAL

#### 5.5.1. TYPES OF EVENTS RECORDED

It is stored at least:

- All audit records collected under section 5.4

- Information on the life cycle of certificates, including requests and supporting documents

#### 5.5.2. RETENTION PERIOD FOR ARCHIVE

Archived data is retained for a period of time defined by applicable law, which is currently set at twenty (20) years.

#### 5.5.3. PROTECTION OF ARCHIVE

DigitalSign protects its archived records so that only authorized Trusted Persons are able to obtain access to the archive. The archive is protected against unauthorized viewing, modification, deletion, or other tampering by storage within a Trustworthy system. The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archived data can be accessed for the time period set forth in this CPS.

#### 5.5.4. ARCHIVE BACKUP PROCEDURES

Incremental backups are created daily and full backups are performed weekly

#### 5.5.5. REQUIREMENTS FOR TIME-STAMPING OF RECORDS

Some entries contain information about the time and date. Such information is generated in the cryptographic equipment.

#### 5.5.6. ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

The data file collection system is internal except for RA customers. DigitalSign supports its RA customers in the preservation of an audit record. This file collection system is therefore external.

#### 5.5.7. PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

Only authorized Trusted Persons can access the file. The integrity of the information is verified when it is restored.

### 5.6. KEY CHANGEOVER

Nothing to mention.

## 5.7. COMPROMISE AND DISASTER RECOVERY

### 5.7.1. INCIDENT AND COMPROMISE HANDLING PROCEDURES

The following backups should be maintained in outdoor installations, and available, in case of a compromise or disaster: Certification Application data, audit data and database records for all Certificates issued.

Backup copies of the CA private key shall be generated in accordance with Section 6.2.4.

DigitalSign will keep backup copies of the necessary data for the operation of the CA, as well as for the operation of the RAs.

### 5.7.2. COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to DigitalSign Security and DigitalSign's incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, DigitalSign's key compromise or disaster recovery procedures will be enacted.

### 5.7.3. END PRIVATE KEY COMPROMISE PROCEDURES

Given the suspicion or evidence of compromise of the CA private, the necessary actions will be taken in response to the incident.

If it is necessary the revocation of the CA certificate, it is set the following procedure:

- It is communicated to the relying parties the revocation status of the certificate through the repository, according to this CPS.
- There will be made commercially reasonable efforts to provide additional notification about the revocation to all affected STN participants.

### 5.7.4. BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

DigitalSign offers redundant secondary facilities, capable of reactivating the essential operations of EC DIGITALSIGN after disaster.

The recovery plan in case of disaster is regularly tested, verified and updated to be operational in case of any occurrence.

## 5.8. CA OR RA TERMINATION

In the event it is necessary to cease operations of the CA or any of the RAs, DigitalSign shall make commercially reasonable effort to notify in advance the end-users, relying parties and other entities affected by such termination.

When required the CA termination, DigitalSign will develop a termination plan to minimize the impact to its customers, end users and relying parties. Such a plan should contain the following, as applicable:

- Report the cessation of activity
- Notify the termination of the activity to the Autoridade Nacional de Segurança for the purposes of cancellation of security clearances
- Cease all contractual relationships with third parties authorized to act on its behalf in performing functions relating to the issuance of certificates

- Provide notice to the parties affected by the term, such as end users, relying parties and customers, informing them of the status of CA
- Support the costs of such notifications
- The revocation of the certificate issued to EC DIGITALSIGN
- The preservation of the file and records of CA during the imposed period in this CPS and applicable law
- Continued support services to end users and customers
- The continuation of revocation services, such as CRL issuance and maintenance of online status check service
- The revocation, if necessary, of all issued certificates that are not expired or revoked already
- Refund, if necessary, unexpired and unrevoked certificate holders which are revoked under the termination plan, or alternatively issue replacement certificates by a successor CA
- Destruction (or equivalent) of the private key of the CA and HSMs that contains them
- Plan for transition services for a successor CA, ensuring that the entity to which is transmitted all documentation undertakes its maintenance during the period of time required by law

# 6. TECHNICAL SECURITY CONTROLS

## 6.1. KEY PAIR GENERATION AND INSTALLATION

### 6.1.1. KEY PAIR GENERATION

The generation of cryptographic keys of EC DIGITALSIGN is made by authorized elements for such, at a security level 4 or higher, at a ceremony planned and audited in accordance with written procedures to perform operations, and using systems that ensure the requirements of cryptographic strength of keys. All activities developed in each key generation ceremony are recorded, dated and signed by all the elements involved. These records are retained for future audit purposes.

The cryptographic hardware used for the generation of CA keys, meets at least the requirements of FIPS 140-1 Level 3 and / or Common Criteria EAL 4 +.

The keys for end users are generated in qualified signature creation devices, duly approved.

### 6.1.2. PRIVATE KEY DELIVERY TO ENTITY

Subjects/Signatories keys of a qualified certificate for advanced electronic signature/Seal can be remotely generated in a secure environment as required by Regulation (EU) 910/2014. The keys are generated in secure signature creation devices, duly approved. The sole control of the private key is granted through the use of two factor authentication.

In the case of the key pair is generated in a smartcard or usb token by the RA, the delivery of the key pair and corresponding certificate is done in person or through registered postal mail or equivalent. The cryptographic device access codes are sent to the end user via email (to the address on the certificate) after receipt and verification of the "Statement of Reception", duly signed by the Subject/Signatory.

If subscribers create the keys on their own cryptographic device, DigitalSign verifies through technical process or an auditor declaration before a certificate with keys created on a hardware device is issued.

All keys are created using the RSA public key algorithm, with a minimum length of 2048 bits.

DigitalSign has controls to ensure that generated keys are aligned with the Certification Policies, and cannot issuing them otherwise.

### 6.1.3. PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

End-users and RAs submit public keys to EC DIGITALSIGN for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR).

### 6.1.4. CA PUBLIC KEY DELIVERY TO USERS

Digicert ensures that the root CA of the STN certificates is included in the overwhelming majority of web browsers, equipment and other existing software globally, including versions and upgrades.

Normally DigitalSign also provides the entire certificate chain to the end user, to be included in the available cryptographic device.

Additionally the certificate of EC DIGITALSIGN (and corresponding certificate chain) can be obtained in the directory.

#### 6.1.5. KEY SIZES

The length of the key pair of EC DIGITALSIGN is 2048 bit RSA.

The minimum length of the key pair to end users is 2048 bit RSA.

#### 6.1.6. PUBLIC KEY PARAMETERS GENERATION

Non applicable

#### 6.1.7. KEY USAGE PURPOSES

According to to section 7.1.2.1.

### 6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

DigitalSign has implemented a combination of monitoring procedures to ensure physical and logical security of its private key. It also requires the subscribers, by contract, to take reasonable precautions to prevent loss, disclosure, modification or unauthorized use of their private keys.

#### 6.2.1. STANDARDS FOR CRYPTOGRAPHIC MODULES

For the creation and storage of the DigitalSign private key is used hardware security modules that are certified or meet materially the requirements FIPS 140-1 Level 3 and / or Common Criteria EAL4+.

#### 6.2.2. PRIVATE KEY (M OUT OF N) MULTI-PERSON CONTROL

DigitalSign has implemented technical and procedural mechanisms that require the participation of several trusted employees to perform cryptographic operations of the CA. DigitalSign uses 'secret sharing' to share the information needed for the activation of the private key into separate parts, known as "secret shares", which are held by trained and trustworthy individuals, called 'Key Holders'. The limit number of Secret Shares (m), of a total number of Key Holders created and distributed for particular hardware cryptographic module (n), is required to enable the private key stored in the module.

The Secret Shares are protected in accordance with this CPS in Section 6.4.2.

#### 6.2.3. PRIVATE KEY ESCROW

Private key escrow is not used by DigitalSign.

DigitalSign does not in any way store or archive a Signatory's private key to create electronic signature/seal, except in the case of remote certification of a qualified certificate through the DigitalSign remote signature solution.

In this case, the private key is generated in a qualified signature creation device (QSCD) and encrypted in a reliable environment. The key encryption relies on a AES symmetric key (128 bits) wrapping key created by the QSCD and derived from the QSCD master wrapping key and the first authentication factor created/defined by the Signatory, which ensures that only he/she can access that private key.

### 6.2.4. PRIVATE KEY BACKUP

DigitalSign makes backups of CA private keys to allow their retrieval in the event of natural disaster, loss or damage. At least two people are required to create the copy and retrieve it. DigitalSign keeps records on CA private key management processes.

DigitalSign does not create copies of user's private keys, except in the case referred in the previous section 6.2.3.

### 6.2.5. PRIVATE KEY FILE

See section 6.2.3 and 4.1.2.

### 6.2.6. PRIVATE KEY ENTRY INTO CRYPTOGRAPHIC MODULE

DigitalSign creates key pairs directly in the cryptographic module in which they are used.

DigitalSign makes copies of these keys with the purpose of routine recoveries and in cases of disasters.

When keys are transferred to another cryptographic module (for backup purposes), such keys are transferred between cryptographic modules in encrypted form, and according to the manufacturer's specifications.

### 6.2.7. PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

The CA private key is stored in the cryptographic module in in encrypted form.

### 6.2.8. METHOD OF ACTIVATING PRIVATE KEY

DigitalSign private key is activated as defined in section 6.2.2. After the private key is activated, it can remain active indefinitely until being deactivated.

### 6.2.9. METHOD OF DEACTIVATING PRIVATE KEY

DigitalSign private key is disabled when the CA system is shut down.

### 6.2.10. METHOD OF DESTROYING PRIVATE KEY

When necessary, DigitalSign may destroy the CA private key, so as to ensure that there are key parts that may lead to its reconstruction. DigitalSign ensures formatting (zeroisation) of its cryptographic modules and other appropriate means to ensure the complete destruction of keys. When implemented, the key destruction activities are recorded.

### 6.2.11. CRYPTOGRAPHIC MODULE RATING

See section 6.2.1.

## 6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

### 6.3.1. PUBLIC KEY ARCHIVAL

Backup copies are made and all issued certificates are stored, as part of the routine procedures of DigitalSign.

### 6.3.2. USAGE PERIODS FOR THE PUBLIC AND PRIVATE KEYS

The usage period of a certificate expires upon its expiration or revocation. The usage period of the key pair is the same as the period defined for the associated certificates, except:

- Private keys can still be used to decode
- Public keys can still be used for signature verification

The EC DIGITALSIGN certificate has a validity period which can vary from five to ten years.

TSA certificates have a maximum validity period of six years.

End-user certificates have a maximum validity period of 40 months.

Certificates issued by EC DIGITALSIGN have a validity period not superior to its own certificate.

Furthermore, EC DIGITALSIGN stop issuing new Certificates at an appropriate date prior to the expiration of the CA's Certificate such that no Certificate issued by a Subordinate CA expires after the expiration of any Superior CA Certificates.

## 6.4. ACTIVATION DATA

### 6.4.1. ACTIVATION DATA GENERATION AND INSTALLATION

Activation data (Secret Shares) used for protection of cryptographic modules that contain the CA private key, are created in accordance with the requirements of section 6.2.2 and specifications for key generation ceremony. The creation and distribution of shared secrets is appropriately registered.

The activation data of the user's private key is generated differently depending on the type of certificate.

On the smartcards or usb tokens used by DigitalSign, keys are generated protected with a random-calculated PIN and PUK. This information is sent by the management platform to the Subject via the email address associated with the digital certificate. The Subject has software to change their card's PIN and PUK.

On a third party hardware devices, DigitalSign accredits third-party devices, even though they are managed separately.

The private keys stored on a HSM for remote signature/seal, the activation data is created/defined by the Signatory.

### 6.4.2. ACTIVATION DATA PROTECTION

It is required to holders of Secret Shares, to safeguard data and sign an agreement acknowledging their responsibilities.

Activation data are stored in secure vaults.

End-user private keys are protected through the use of secure-signature-creation-devices, and PIN (*Personal Identification Number*). In case of remote signature solution, two authentication factors are required.

### 6.4.3. OTHER ASPECTS OF ACTIVATION DATA

#### 6.4.3.1. ACTIVATION DATA TRANSMISSION

Whenever it is necessary to transmit activation data, it should be protected against loss, theft, modification, unauthorized use or viewing.

#### 6.4.3.2. ACTIVATION DATA DESTRUCTION

Activation data for CA private key must be destroyed using methods that protect against loss, theft, modification and viewing and unauthorized use of private keys protected by such activation data. After the record retention period, section 5.5.2, DigitalSign must destroy the activation data, rewriting them and / or destroying them physically.

## 6.5. COMPUTER SECURITY CONTROLS

DigitalSign performs all CA and RA functions using reliable systems that meet the requirements stipulated by DigitalSign. DigitalSign recommends that its RA clients follow the same guidelines.

### 6.5.1. SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

DigitalSign ensures systems maintaining CA activities are reliable and secure from unauthorized access. Furthermore, DigitalSign limits access to production servers only to individuals in need of such access effectively.

DigitalSign production network is logically separated from other components. This separation prevents network access except through well-defined applicational processes. DigitalSign uses firewall systems to protect the network from internal and external intrusion and limit the nature and origin of the network activities that may access production systems.

### 6.5.2. COMPUTER SECURITY RATING

No stipulation.

## 6.6. LIFE CYCLE TECHNICAL CONTROLS

### 6.6.1. SYSTEM DEVELOPMENT CONTROLS

The applications are developed and implemented by DigitalSign or others, according to systems development and maintenance change management standards. DigitalSign also provides software to its customers to perform RA functions.

The developed software, when loaded, provides methods to verify that the software has not been changed before installation and is the correct version to be used.

### 6.6.2. SECURITY MANAGEMENT CONTROLS

DigitalSign has mechanisms and / or policies to control or monitor the configuration of its CA systems. After installation and periodically DigitalSign validates the integrity of its CA system.

### 6.6.3. LIFE CYCLE SECURITY RATINGS

Update and maintenance operations of systems and products follows the same controls as the original equipment and is performed by authorized personnel with proper training to do so by following the procedures defined.

## 6.7. NETWORK SECURITY CONTROLS

DigitalSign performs all its CA and RA functions using secure networks, to prevent unauthorized access and other malicious activity. DigitalSign protects communication of sensitive information through the use of digital signatures and encryption.

## 6.8. TIME-STAMPING

Certificates, CRLs, and other revocation data contain information on the date and time. Such information is not based on cryptographic mechanisms.

# 7. CERTIFICATE AND CRL PROFILE

## 7.1. CERTIFICATE PROFILE

Certificates issued by CA DIGITALSIGN obey Recomendation *ITU-T Recomendation X.509 (1997): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework*, e *RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile*.

Issued certificates contain at least the fields and values described in the following table:

| ***Field*** | ***Value*** |
|---|---|
| Serial Number | Unique serial number assigned by the issuing CA |
| Signature Algorithm | Identification of the algorithm used to sign the certificates (see section 7.1.3) |
| Issuer DN | See section 7.1.4 |
| Valid From | Indicating the date and time in UTC format, properly synchronized through Network Time Protocol, and encoded according to RFC 3280 |
| Valid To | Indicating the date and time in UTC format, properly synchronized through Network Time Protocol, and encoded according to RFC 3280 |
| Subject | See section 7.1.4 |
| Subject Public Key | Encoded in accordance with RFC 3280 |
| Signature | Issuer signature generated and encoded in accordance with RFC 3280 |

### 7.1.1. VERSION NUMBER(S)

Both the CA and end-user certificates are X.509 version 3 (three) of the X.509 format.

### 7.1.2. CERTIFICATE EXTENSIONS

Certificates contain the extension described in sections 7.1.2.1 to 7.1.2.10.

#### 7.1.2.1. KEY USAGE

Certificates issued before 01/07/2016:

| ***Field*** | ***EC*** | ***Certificates*** | ***Time-Stamp*** |
|---|---|---|---|
| *Critical extension* | *YES* | *YES* | *YES* |
| Digital Signature (bit 0) | NO | YES | YES |
| Non Repudiation (bit 1) | NO | YES | YES |
| Key Encipherment (bit 2) | NO | NO | NO |
| Data Encipherment (bit 3) | NO | NO | NO |
| Key Agreement (bit 4) | NO | NO | NO |
| Key Certificate Signature (bit 5) | YES | NO | NO |
| CRL Signature (bit 6) | YES | NO | NO |
| Encipher Only (bit 7) | NO | NO | NO |
| Decipher Only (bit 8) | NO | NO | NO |

Certificates issued from 01/07/2016:

| *Field* | *EC* | *Certificates* | *Time-Stamp* |
|---|---|---|---|
| *Critical extension* | *YES* | *YES* | *YES* |
| Digital Signature (bit 0) | NO | NO | YES |
| Non Repudiation (bit 1) | NO | YES | YES |
| Key Encipherment (bit 2) | NO | NO | NO |
| Data Encipherment (bit 3) | NO | NO | NO |
| Key Agreement (bit 4) | NO | NO | NO |
| Key Certificate Signature (bit 5) | YES | NO | NO |
| CRL Signature (bit 6) | YES | NO | NO |
| Encipher Only (bit 7) | NO | NO | NO |
| Decipher Only (bit 8) | NO | NO | NO |

#### 7.1.2.2. CERTIFICATE POLICIES

| *Field* | *EC* | *Certificates* | *Time-Stamp* |
|---|---|---|---|
| *Critical extension* | *NO* | *NO* | *NO* |
| Cert Policy ID | 2.16.840.1.113733.1.7.23.2 | 2.16.840.1.113733.1.7.23.2 | 2.16.840.1.113733.1.7.23.2 |
| Cert Policy Qualifier ID | 1.3.6.1.5.5.7.2.1 (CPS Pointer) | 1.3.6.1.5.5.7.2.1 (CPS Pointer) | 1.3.6.1.5.5.7.2.1 (CPS Pointer) |
| Cert Qualifier | https://www.trustwise.com/cps | https://www.digitalsign.pt/ECDIGITALSIGN/cps | https://www.digitalsign.pt/ECDIGITALSIGN/cps |
| Cert Policy ID | | -- | |
| Cert Policy Qualifier ID | 1.3.6.1.5.5.7.2.2 (User Notice) | -- | -- |
| Cert Qualifier | https://www.trustwise.com/rpa | -- | -- |
| Cert Policy ID | -- | 2.16.840.1.113733.1.7.44.2 | -- |
| Cert Policy ID | -- | -- | -- |
| Cert Policy Qualifier ID | -- | -- | -- |
| Cert Policy ID **(1)** | -- | 0.4.0.194112.1.2 | -- |
| Cert Policy ID | -- | -- | -- |
| Cert Policy Qualifier ID | -- | -- | -- |
| Cert Policy ID **(2)** | -- | 0.4.0.194112.1.3 | -- |
| Cert Policy ID | -- | -- | -- |
| Cert Policy Qualifier ID | -- | -- | -- |

(1) Only present on Individual, Member, Professional and Representative certificate profiles, issued by EC "DigitalSign Qualified CA – G3".

(2) Only present on Organization certificate profile, issued by EC "DigitalSign Qualified CA – G3".

#### 7.1.2.3. SUBJECT ALTERNATIVE NAME

| *Field* | *EC* | *Certificates* | *Time-Stamp* |
|---|---|---|---|
| *Critical extension* | *NO* | *NO* | -- |
| | According to RFC 3280 | RFC822 Name/email address | -- |

#### 7.1.2.4. BASIC CONSTRAINTS

| *Field* | *EC* | *Certificates* | *Time-Stamp* |
|---|---|---|---|
| *Critinal Extension* | *YES* | *NO* | *YES* |
| Subject Type | CA | End Entity | End Entity |
| Path Length Constraint | 0 | None | None |

#### 7.1.2.5. EXTENDED KEY USAGE

| *Field* | *EC* | *Certificates* | *Time-Stamp* |
|---|---|---|---|
| *Critical extension* | -- | *NO* | *YES* |

| | | | |
|---|---|---|---|
| Server Authentication | -- | NO | NO |
| Client Authentication | -- | YES | NO |
| Code Signing | -- | NO | NO |
| Secure Email | -- | YES | NO |
| IPSEC End System | -- | NO | NO |
| IPSEC Tunnel | -- | NO | NO |
| IPSEC User | -- | NO | NO |
| Time Stamping | -- | NO | YES |
| OCSP Signing | -- | NO | NO |
| Microsoft Server Gated Crypto | -- | NO | NO |
| Netscape SGC | -- | NO | NO |
| Symantec SGC Identifier for CA Certificates | -- | NO | NO |

#### 7.1.2.6. CRL DISTRIBUTION POINTS

| *Field* | *EC* | *Certificates* | *Time-Stamp* |
|---|---|---|---|
| *Critical Extension* | *NO* | *NO* | *NO* |

#### 7.1.2.7. AUTHORITY KEY IDENTIFIER

This extension is filled with the hash of the public key of the issuer, through the algorithm 160-bit SHA-1. This extension is NOT marked as critical.

#### 7.1.2.8. SUBJECT KEY IDENTIFIER

This extension is filled with the hash of the public key of the certificate itself, through the algorithm 160-bit SHA-1, or by any other method described in RFC 3280. This extension is NOT marked as critical.

#### 7.1.2.9. AUTHORITY INFORMATION ACCESS

For certificates issued from 01/07/2015, this extension includes the URL where it can be found the certificate of issuing CA. This extension is NOT marked as critical.

#### 7.1.2.10. QUALIFIED CERTIFICATE STATEMENT

The certificates issued by DigitalSign have the extension "Qualified Certificate Statement" (OID 1.3.6.1.5.5.7.1.3), as stipulated in the document ETSI EN 319 412.

This extension is NOT marked as critical.

#### 7.1.2.11. PRIVATE EXTENSIONS

The end-user certificates may also have an additional extension - "Netscape Certificate Type" (OID 2.16.840.1.113730.1.1) - which has the active BIT 0 (SSL Client).

The CA certificate may also include this extension, possessing information "CA SSL" and "S / MIME CA" active.

This extension is NOT marked as critical.

### 7.1.3. ALGORITHM OBJECT IDENTIFIERS

Certificates are signed using the algorithm sha1WithRSAEncryption (OID 1.2.840.113549.1.1.5) or sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11).

### 7.1.4. NAME FORMS

DN Issuer (Issuer) and subject (Subject) fields follow the stipulations in section 3.1.1.

Although all the fields described in section 7.1.2 are common to all certificates issued to end users, DigitalSign subdivides its certificates in five (5) different types (nicknamed "Profile"), whose information in the DN of the Subject field has the meaning described in sections 7.1.4.1 to 7.1.4.5 below.

#### 7.1.4.1. INDIVIDUAL PROFILE

This certificate profile aims to identify an individual.

Certificates issued before 01/07/2016:

| *Type* | *required* | *Identifier* | *Description* |
|---|---|---|---|
| CN | YES | -- | Holder Full Name |
| E | YES | -- | Holder's email address, or to which he has access |
| T | NO | -- | Academic degree or another that the holder can use |
| OU | NO | ID | ID Number, ie ID card or Tax ID |
| OU | NO | Address1 | Postal address (line 1) |
| OU | NO | Address2 | Postal address (line 2) |
| OU | NO | Postal Code | Zip code |
| L | NO | -- | City ou Locality |
| C | YES | -- | Country |
| OU | NO | Limitation1 | Any limitations for use of signature (line 1) |
| OU | NO | Limitation2 | Any limitations for use of signature (line 2) |
| OU | NO | Limitation3 | Any limitations for use of signature (line 3) |
| OU | NO | Obs1 | Any comments (line 1) |
| OU | NO | Obs2 | Any comments (line 2) |
| OU | NO | Obs3 | Any comments (line 3) |
| OU | YES | -- | Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa |
| OU | YES | -- | Certificate Profile - Qualified Certificate - Individual |

Certificates issued from 01/07/2016:

| *Type* | *required* | *Identifier* | *Description* |
|---|---|---|---|
| CN | YES | -- | Holder Full Name |
| OU | NO | RemoteQSCDManagement | Only present on certificates issued for remote signature |
| G | YES | -- | Holder first name(s) |
| SN | YES | -- | Holder last name(s) |
| SERIALNUMBER | NO | -- | Holder ID, according to ETSI EN 319 412 |
| E | YES | -- | Holder's email address, or to which he has access |
| C | YES | -- | Country |
| OU | NO | Limitation1 | Any limitations for use of signature (line 1) |
| OU | NO | Limitation2 | Any limitations for use of signature (line 2) |
| OU | NO | Limitation3 | Any limitations for use of signature (line 3) |
| OU | NO | Obs1 | Any comments (line 1) |
| OU | NO | Obs2 | Any comments (line 2) |
| OU | NO | Obs3 | Any comments (line 3) |
| OU | YES | -- | Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa |
| OU | YES | -- | Certificate Profile - Qualified Certificate - Individual |

#### 7.1.4.2. PROFISSIONAL PROFILE

This certificate profile aims to identify an individual, and their ownership in the performance of their profession. Usually this type of certificate is issued to members of professional associations, where the ownership should be checked with this association.

Certificates issued before 01/07/2016:

| *Type* | *required* | *Identifier* | *Description* |
|---|---|---|---|
| CN | YES | -- | Holder Full Name |
| E | YES | -- | Holder's email address, or to which he has access |
| T | NO | -- | Academic degree or another that the holder can use |
| OU | YES | Entitlement | Professional title verified with the Professional Order |
| OU | NO | ID | ID Number, ie ID card or Tax ID |
| OU | NO | Address1 | Postal address (line 1) |
| OU | NO | Address2 | Postal address (line 2) |
| OU | NO | Postal Code | Zip code |
| L | NO | -- | City or Locality |
| C | YES | -- | Country |
| OU | NO | Limitation1 | Any limitations for use of signature (line 1) |
| OU | NO | Limitation2 | Any limitations for use of signature (line 2) |
| OU | NO | Limitation3 | Any limitations for use of signature (line 3) |
| OU | NO | Obs1 | Any comments (line 1) |
| OU | NO | Obs2 | Any comments (line 2) |
| OU | NO | Obs3 | Any comments (line 3) |
| OU | YES | -- | Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa |
| OU | YES | -- | Certificate Profile - Qualified Certificate - Professional |

Certificates issued from 01/07/2016:

| *Type* | *required* | *Identifier* | *Description* |
|---|---|---|---|
| CN | YES | -- | Holder Full Name |
| OU | NO | RemoteQSCDManagement | Only present on certificates issued for remote signature |
| G | YES | -- | Holder first name(s) |
| SN | YES | -- | Holder last name(s) |
| SERIALNUMBER | NO | -- | Holder ID, according to ETSI EN 319 412 |
| E | YES | -- | Holder's email address, or to which he has access |
| OU | YES | Entitlement | Professional title verified with the Professional Order |
| C | YES | -- | Country |
| OU | NO | Limitation1 | Any limitations for use of signature (line 1) |
| OU | NO | Limitation2 | Any limitations for use of signature (line 2) |
| OU | NO | Limitation3 | Any limitations for use of signature (line 3) |
| OU | NO | Obs1 | Any comments (line 1) |
| OU | NO | Obs2 | Any comments (line 2) |
| OU | NO | Obs3 | Any comments (line 3) |
| OU | YES | -- | Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa |
| OU | YES | -- | Certificate Profile - Qualified Certificate - Professional |

#### 7.1.4.3. MEMBER PROFILE

This certificate profile aims to identify an individual, and the position or function that takes / plays in a particular organization.

Certificates issued before 01/07/2016:

| *Type* | *required* | *Identifier* | *Description* |
|---|---|---|---|
| CN | YES | -- | Holder Full Name |
| E | YES | -- | Holder's email address, or to which he has access |
| T | NO | -- | Academic degree or another that the holder can use |
| OU | YES | Entitlement | Position or function that takes / plays in the organization (see field "O") |
| OU | NO | ID | ID Number, ie ID card or Tax ID |
| OU | NO | Address1 | Postal address |
| OU | NO | Postal Code | Zip code |
| L | NO | -- | City or Locality |
| C | YES | -- | Country |
| O | YES | -- | Full name of the organization where holds / plays the position or function defined in the "OU = Entitlement" |
| OU | NO | Organization ID | The organization identifier, such as NIPC |
| OU | NO | Organization Address1 | Organization Postal Address |
| OU | NO | Organization PostalCode | Organization Zip Code |
| OU | NO | Organzation City | City or locality of the Organization |
| OU | NO | Organization Limitation1 | Any limitations for use of signature (line 1) |
| OU | NO | Organization Limitation2 | Any limitations for use of signature (line 2) |
| OU | NO | Organization Limitation3 | Any limitations for use of signature (line 3) |
| OU | NO | Obs1 | Any comments |
| OU | YES | -- | Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa |
| OU | YES | -- | Certificate Profile - Qualified Certificate - Member |

Certificates issued from 01/07/2016:

| *Type* | *required* | *Identifier* | *Description* |
|---|---|---|---|
| CN | YES | -- | Holder Full Name |
| OU | NO | RemoteQSCDManagement | Only present on certificates issued for remote signature |
| G | YES | -- | Holder first name(s) |
| SN | YES | -- | Holder last name(s) |
| SERIALNUMBER | NO | -- | Holder ID, according to ETSI EN 319 412 |
| E | YES | -- | Holder's email address, or to which he has access |
| T | NO | -- | Academic degree or another that the holder can use |
| OU | YES | Entitlement | Position or function that takes / plays in the organization (see field "O") |
| C | YES | -- | Country |
| O | YES | -- | Full name of the organization where holds / plays the position or function defined in the "OU = Entitlement" |
| ORGANIZATION IDENTIFIER | YES | -- | Organization ID, according to ETSI EN 319 412 |
| OU | NO | Limitation1 | Any limitations for use of signature (line 1) |
| OU | NO | Limitation2 | Any limitations for use of signature (line 2) |
| OU | NO | Limitation3 | Any limitations for use of signature (line 3) |
| OU | NO | Obs1 | Any comments (line 1) |
| OU | NO | Obs2 | Any comments (line 2) |
| OU | NO | Obs3 | Any comments (line 3) |
| OU | YES | -- | Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa |
| OU | YES | -- | Certificate Profile - Qualified Certificate - Member |

#### 7.1.4.4. ORGANIZATION PROFILE

This certificate profile aims to identify a legal person.

It is an electronic seal certificate that is intended solely to be used by a legal person.

It is not a suitable to bind contractually the legal person, just as in the physical world a stamp / seal of an organization is not enough to bind that organization.

| *Type* | *required* | *Identifier* | *Description* |
|---|---|---|---|
| CN | YES | -- | Holder Full Name (organization) |
| OU | NO | RemoteQSCDManagement | Only present on certificates issued for remote signature |
| E | YES | -- | Holder's email address, or to which he has access |
| C | YES | -- | Coutry |
| O | YES | -- | Full name of the organization |
| ORGANIZATION IDENTIFIER | YES | -- | Organization ID, according to ETSI EN 319 412 |
| OU | NO | Limitation1 | Any limitations for seal usage (line 1) |
| OU | NO | Limitation2 | Any limitations for seal usage (line 2) |
| OU | NO | Limitation3 | Any limitations for seal usage (line 3) |
| OU | NO | Obs1 | Any comments (line 1) |
| OU | NO | Obs2 | Any comments (line 2) |
| OU | NO | Obs3 | Any comments (line 3) |
| OU | YES | -- | Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa |
| OU | YES | -- | Certificate Profile - Qualified Certificate - Organization |

#### 7.1.4.5. REPRESENTATIVE PROFILE

This certificate profile aims to identify an individual person, as legal representative or attorney of an organization, entitled to, solely, bind a legal person, with any limitations identified in the respective fields of the certificate.

Certificates issued before 01/07/2016:

| *Type* | *required* | *Identifier* | *Description* |
|---|---|---|---|
| CN | YES | -- | Organization full Name |
| E | YES | -- | Email address of the representative, or the representative has access |
| OU | YES | Entitlement | Powers of representation that the representative / attorney hold |
| C | YES | -- | Coutry |
| OU | NO | ID | Organization Identifier (if applicable), such as NIPC |
| OU | NO | Address1 | Organization Postal Address (if applicable) (line 1) |
| OU | NO | Address2 | Organization Postal Address (if applicable) (line 2) |
| OU | NO | PostalCode | Organization Zip code (if applicable) |
| OU | NO | City | Organization City or locality (if applicable) |
| OU | YES | Representative Name | Full name of representative/attorney |
| OU | NO | Representative ID | Identification number of the representative / attorney, such as ID or Tax ID |
| OU | NO | Representative Limitations1 | Any limitations for use of the signature by the representative / attorney (line 1) |
| OU | NO | Representative Limitations2 | Any limitations for use of the signature by the representative / attorney (line 2) |
| OU | NO | Representative Limitations3 | Any limitations for use of the signature by the representative / attorney (line 3) |

| | | | |
|---|---|---|---|
| OU | NO | Obs1 | Any comments (line 1) |
| OU | NO | Obs2 | Any comments (line 2) |
| OU | NO | Obs3 | Any comments (line 3) |
| OU | YES | -- | Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa |
| OU | YES | -- | Certificate Profile - Qualified Certificate - Representative |

Certificates issued from 01/07/2016:

| *Type* | *required* | *Identifier* | *Description* |
|---|---|---|---|
| CN | YES | -- | Holder Full Name |
| OU | NO | RemoteQSCDManagement | Only present on certificates issued for remote signature |
| G | YES | -- | Holder first name(s) |
| SN | YES | -- | Holder last name(s) |
| SERIALNUMBER | NO | -- | Holder ID, according to ETSI EN 319 412 |
| E | YES | -- | Holder's email address, or to which he has access |
| T | NO | -- | Academic degree or another that the holder can use |
| OU | YES | Entitlement | Powers of representation that the representative / attorney hold |
| C | YES | -- | Country |
| O | YES | -- | Full name of the organization |
| ORGANIZATION IDENTIFIER | YES | -- | Organization ID, according to ETSI EN 319 412 |
| OU | NO | Limitations1 | Any limitations for use of the signature by the representative / attorney (line 1) |
| OU | NO | Limitations2 | Any limitations for use of the signature by the representative / attorney (line 2) |
| OU | NO | Limitations3 | Any limitations for use of the signature by the representative / attorney (line 3) |
| OU | NO | Obs1 | Any comments (line 1) |
| OU | NO | Obs2 | Any comments (line 2) |
| OU | NO | Obs3 | Any comments (line 3) |
| OU | YES | -- | Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa |
| OU | YES | -- | Certificate Profile - Qualified Certificate - Member |

### 7.1.5. NAME CONSTRAINTS

Non spitulated.

### 7.1.6. CERTIFICATE POLICY OBJECT IDENTIFIER

Where this extension is used, certificates contain the respective identifier as defined in the STN CP, section 1.2.

### 7.1.7. USAGE OF POLICY CONSTRAINTS EXTENSION

Non stipulated.

### 7.1.8. POLICY QUALIFIERS SYNTAX AND SEMANTICS

Certificates contain a "Policy Qualifier" in the extension "Certificate Policies", as described in section 7.1.2.2.

#### 7.1.9. PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICY EXTENSION
Non stipulated.

## 7.2. CRL PROFILE
The issued CRLs contain the basic fields and specific contents in the following table:

| *Field* | *Value* |
|---|---|
| Version | See section 7.2.1 |
| Signature Algorithm | Identification of the algorithm used to sign the CRL. The algorithm used is sha1WithRSAEncryption (OID 1.2.840.113549.1.1.5) |
| Issuer | Issuer of the CRL |
| Efective Date | Issue date of the CRL. The CRL are effective upon issuance |
| Next Update | Date on which the next CRL will be issued. The emission frequency of the CRL is defined in section 4.4.7 |
| Revoked Certificates | List of revoked certificates, including the serial number and date of revocation |

#### 7.2.1. VERSION NUMBER(S)
It is used the version 2 (two) format for X.509 CRLs as RFC 3280.

#### 7.2.2. CRL AND CRL ENTRY EXTENSIONS
Non stipulated

## 7.3. OCSP PROFILE
The OCSP protocol (Online Certificate Status Protocol) is a form of DigitalSign giving information about the revocation status of a particular certificate.

The OCSP Responders are as set forth in RFC 2560.

#### 7.3.1. VERSION NUMBER(S)
It is used the version one (1) from OCSP specification according RFC 2560.

#### 7.3.2. OCSP EXTENSIONS
DigitalSign does not use the "nonce" on OCSP responses.

# 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS
It is performed an annual audit by an accredited entity for the DigitalSign / BT Data Center operations and Key Management operations, which support service management of EC DIGITALSIGN.

Beyond compliance assessments and audits, DigitalSign is responsible for performing other reviews and investigations to ensure the reliability of the subdomain that operates in STN, which includes but is not limited to the following:

- DigitalSign or its authorized representative, is responsible, within its sole discretion, to play at any time, an audit or investigation to a RA client, provided there is reason to believe that the audited entity has failed to compliance with the standards of the STN, has suffered an incident, acted or failed to act for the entity did not fail, which could potentially threaten the security or integrity of the STN.
- DigitalSign or its authorized representative is responsible for evaluating the Risk Management to RA clients in the fulfillment of their usual ordinary course of business.

DigitalSign, or their legal representatives, may delegate the performance of these audits, reviews or investigations to a third party auditor duly accredited by the authority. Entities that are subject to audits, reviews or investigations should establish cooperation with DigitalSign and the personnel carrying out the audit, evaluation or investigation.

## 8.1. FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT

Audits are conducted at least on an annual basis.

## 8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

Audits to the DigitalSign should be performed by appropriately accredited auditor, in accordance with applicable local laws.

## 8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

Audit operations to DigitalSign are performed by an independent auditor.

## 8.4. TOPICS COVERED BY ASSESSMENT

The scope of audits and other assessment includes compliance with applicable law, with this CPS, and other rules, procedures and processes (especially those related to key management operations, resources, management and operation controls and life cycle certificate management).

## 8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Regarding the results of conformity assessments or audits, exceptions or significant deficiencies identified will result in the determination of actions to be taken.

This determination is made by DigitalSign Administration, together with the leaders of the concerned areas. DigitalSign Administration is responsible for developing and implementing the corrective action plan. If DigitalSign determines that such exceptions or deficiencies may pose an immediate threat to the security or integrity of the STN, this plan must be developed within 30 days and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, DigitalSign management will assess the implications of such occurrences and will determine the appropriate course of action.

## 8.6. COMMUNICATIONS OF RESULTS

The results of audits and evaluations of compliance must be delivered to DigitalSign within the contractually stipulated deadlines.

The information about the corrective actions performed and / or to be performed shall be sent to the competent authority in the shortest time possible (when applicable).

# 9. OTHER BUSINESS & LEGAL MATTERS

## 9.1. FEES

### 9.1.1. CERTIFICATE ISSUANCE OR RENEWAL FEES

Fees may be charged for issuing procedures, and / or renewal of certificates.

### 9.1.2. CERTIFICATE ACCESS FEES

It will not be charged any fees for the certificates available in the repository.

### 9.1.3. REVOCATION OR STATUS INFORMATION ACCESS FEES

It will not be charged any fees for the availability of the CRL in the repository, in accordance with the stipulations of this CPS.

Customized CRL issuance, OCSP services, or other value added service for status information or revocation of certificates will be subject to the charge of contracted fees.

### 9.1.4. FEES FOR OTHER SERVICES SUCH AS POLICY INFORMATION

Consultation of this CPS and other documents relating to policies, practices and procedures is not subject to any charging fees.

Ownership rights of this information must be guaranteed.

### 9.1.5. REFUND POLICY

No refunds are provided for any actions of certificate revocation.

## 9.2. FINANCIAL RESPONSIBILITY

### 9.2.1. INSURANCE COVERAGE

DigitalSign maintains insurance coverage for errors and omissions performed within the scope of its activity, through liability insurance with a capital fixed in law of 125,000 €.

### 9.2.2. OTHER ASSETS

Registration Authority customers must have sufficient financial resources to maintain their operations and perform their duties should bear the liability risks to its subscribers and relying parties.

## 9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

### 9.3.1. SCOPE OF CONFIDENTIAL INFORMATION

The following records must be kept confidential and private, according to Section 9.3.2:

- Registration of requests for issuing certificates
- EC DIGITALSIGN private keys, and other related security features
- Transactional records (both full records and traces)
- Any information concerning security parameters
- Audit reports performed by DigitalSign or its auditors (whether internal or external)
- Contingency planning and disaster recovery
- Security measures for monitoring the operations of hardware and software from DigitalSign and certification service management.

### 9.3.2. INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

Certificates, certificate revocation and other status information, DigitalSign's repository and information contained therein are not considered Confidential / Private Information.

Information that is not expressly considered Confidential / Private Information, under section 9.3.1, shall not be considered confidential or private. This section is subject to applicable privacy laws.

### 9.3.3. RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

DigitalSign ensures security of confidential information, avoiding that can be discovered or compromised by third parties.

## 9.4. PRIVACY OF PERSONAL INFORMATION

### 9.4.1. PRIVACY PLAN

DigitalSign repository keeps its Privacy Policy.

### 9.4.2. INFORMATION TREATED AS PRIVATE

Any information about Subscribers that is not publicly available through the contents of issued certificates, directory of certificates and CRL is treated as private.

### 9.4.3. INFORMATION NOT DEEMED PRIVATE

Subject to any applicable legislation, all information made public in a certificate is not considered private.

#### 9.4.4. RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

All STN participants receiving private information must prevent it from being compromised or unveiled to third parties, and shall comply with all applicable privacy laws.

#### 9.4.5. NOTICE AND CONSENT TO USE PRIVATE INFORMATION

Unless otherwise stated in this CPS, in the Privacy Policy or applicable contract, the private information will not be used without the consent of the party to whom the information applies. This section is subjected to the application of privacy laws.

#### 9.4.6. DISCLOSURE TO LAW ENFORCEMENT OFFICIALS

All DigitalSign subdomain participants should recognize that DigitalSign is forced to reveal Confidential / Private information if, in good faith, DigitalSign considers it release necessary in response to subpoenas and court orders.

#### 9.4.7. OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

Non stipulated.

### 9.5. INTELLECTUAL PROPERTY RIGHTS

The assignment of intellectual property rights among participants of the STN subdomain, exept end users and relying parties, is determined by the contracts applicable to these participants.

All intellectual property rights, including certificates, CRL, OIDs, CPS and key pair belong to their rightful owners / authors / senders.

Holders certificate key pairs are owned by the holder, as well as the names and other information in the DN.

### 9.6. REPRESENTATIONS AND WARRANTIES

#### 9.6.1. CA REPRESENTATION AND WARRANTIES

DigitalSign warrant:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate.
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate.
- That issued certificates meet all the requirements of this CPS
- The revocation services and use of a repository conform to this CPS in all material aspects.

### 9.6.2. RA REPRESENTATION AND WARRANTIES

Digitalsign contracts with RAs warrant:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate.
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate.
- That issued certificates meet all the requirements of this CPS.
- The revocation services and use of a repository conform to this CPS in all material aspects.

### 9.6.3. SUBSCRIBER REPRESENTATION AND WARRANTIES

DigitalSign contracts with subscribers ensure that:

- Accept and are obliged to fulfill the contract of issued digital certificate.
- Are obliged to respect the rules of use of the digital certificate (and respective private key) and ensure that they will not modify in any way, its technical configuration
- Ensure the confidentiality of the process of obtaining and using the respective digital certificate and private key
- Declare that they know what are the legal effects attributed to the use of digital certificate and digital signature
- Declare that they are liable for any use that is given to the digital certificate (and corresponding private key) and the resulting consequences
- Declare that they are obliged to revoke or inform DigitalSign immediately on suspicion or loss of control of the private key or incorrectness or alteration of information on the certificate, while valid
- Declare that from the certificate revocation or the expiry of its validity, it is prohibited to use the respective signature creation data to generate an electronic signature.

### 9.6.4. RELYING PARTY REPRESENTATIONS AND WARRANTIES

Relying Third Party Charters require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in this CPS.

## 9.7. DISCLAIMERS OF WARRANTIES

DigitalSign refuse all warranties that are not linked to obligations established in this CPS.

## 9.8. CERTIFICATION AUTHORITY LIMITATIONS OF LIABILITY

DigitalSign guarantees damages or losses caused to end users and relying parties resulting from their activity, according to applicable legislation.

DigitalSign is not liable for any loss or damage resulting from abusive use or outside the scope of the contract with users and / relying parties.

DigitalSign assumes no liability in the event of service failure related causes of Force Majeure such as natural disasters, war or other similar.

## 9.9. INDEMNITIES

DigitalSign assumes its responsibility with respect to any compensation from accordance with applicable law.

## 9.10. TERM AND TERMINATION

### 9.10.1. TERM

All documents related to the CA activity, including this CPS and any subsequent amendments become effective after publication in the repository.

### 9.10.2. TERMINATION

All documents related to the CA activity, including this CPS and any subsequent amendments shall remain in effect until publication of a new version or change.

## 9.11. INDIVIDUAL NOTICES AND COMMUNICATION

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

## 9.12. AMENDMENTS

### 9.12.1. PROCEDURE FOR AMENDMENT

To ensure the update of this CPS, DigitalSign's administration meets with intervals not exceeding one (1) year, with the Operations Director and Technical Services Director for evaluation of possible needs for improvement and change.

Changes to this CPS shall be approved by the administration. Changes must be made through documents, containing the amended form of the CPS or an update.

Changes, corrections and / or updates shall be published in the form of new versions of the CPS (and / or their respective CPs), replacing any previous version.

### 9.12.2. NOTIFICATION MECHANISM AND PERIOD

DigitalSign reserves the right to correct these CPS without notice to corrections which are not materially relevant according to the criteria of DigitalSign, including but not limited to errors writing URLS changes, contact changes, etc

In cases where the alterations or amendments may affect the acceptability of certificates for the purposes that they have been issued, it will be tried the notification to interested parties that a change or correction was made.

#### 9.12.3. CIRCUMSTANCE UNDER WHICH OID MUST BE CHANGED

If DigitalSign determines that the amendment to the identifier (OID) of the certificate policy is required, the amendment shall contain the new identifiers. Otherwise, the amendments should not require a change in the policy certificate identifier.

## 9.13. DISPUTE RESOLUTION PROVISIONS

#### 9.13.1. DISPUTES AMONG DIGITALSIGN AND RA CUSTOMERS

These conflicts must be resolved by the provisions of the contract between the parties.

#### 9.13.2. DISPUTES WITH END-USER SUBSCRIBERS OR RELYING PARTIES

Upon what is allowed by law, all contracts must contain a clause for conflict resolution.

## 9.14. GOVERNING LAW

Subject to any limitations imposed by law, the Portuguese law should exercise authority, construction, interpretation and validity of this CPS, regardless of the choice of contract or other legal provision. This choice of law is made to ensure uniform procedures and interpretations to all participants of the subdomain that the DigitalSign operates in STN, no matter their location.

## 9.15. COMPLIANCE WITH APPLICABLE LAW

This CPS is subject to the laws, rules, regulations, ordinances, edicts, or other, whether national, state, local or foreign, including but not limited to, restrictions in the import or export of software, hardware or technical information.

## 9.16. MISCELLANEOUS PROVISIONS

#### 9.16.1. ENTIRE AGREEMENT

Non applicable

#### 9.16.2. ASSIGNMENT

Non applicable

#### 9.16.3. SEVERABILITY
Non applicable

#### 9.16.4. ENFORCEMENT
Non applicable

#### 9.16.5. FORCE MAJEURE
Non applicable

## 9.17. OTHER PROVISIONS

#### 9.17.1. MANAGEMENT GROUP (GRUPO DE GESTÃO)
The management group is constituted by:

- Administrator
- CEO
- Quality Director
- Systems' Administrator
- Systems' Operator
- Security Administrator
- Systems' Auditor
- External Consultant (by invitation)

The duties, responsibilities and objectives of this management group are defined in the CA internal documents.

# 10. APPENDIX A – ACRONYMS AND DEFINITIONS

| | |
|---|---|
| **CA** | Certifying Authority |
| **EC DIGITALSIGN** | DigitalSign – Certificadora Digital, SA Certification Authority |
| **CPS** | Certification Practices Statement |
| **CP** | Symantec Trust Network Certificate Policies |
| **STN** | Symantec Trust Network |
| **PKI** | Public Key Infrastructure |
| **OID** | Unique number of "object identifier" |
| **BT** | British Telecomunications, plc |
| **Symantec** | Symantec, Inc |
| **RA** | Registry Authority |
| **CRL** | Certificate Revocation List |
| **OCSP** | Online Status Certificate Protocol |
| **CP** | Certificate Policy |
| **SCU** | Signing Cryptographic Units |
| **LSVA** | Logical Security Vulnerability Assessment. |
| **FIPS** | United State Federal Information Processing Standards |
| **HSM** | Hardware Security Module |
| **PKCS** | Public-Key Cryptography Standard |
| **RFC** | Request for comment |
| **S/MIME** | Secure multipurpose Internet mail extensions |
| **SSL** | Secure Sockets Layer |