

Portuguese CVCA Certificate Policy

Policy

MULTICERT_PJ.PEP.EAC_24.1.2_0001_pt.doc

Project Identification: PEP EAC

CA Identification: CVCA

Rating: Restrict

Version: 1.1

Date: 30/04/10

Legal Advice Copyright © 2002-2009 MULTICERT — Serviços de Certificação Electrónica, S.A. (MULTICERT)

All rights reserved: MULTICERT holds all intellectual property rights over this document or has been duly authorised to use them. Trademarks included in this document are used only to identify products and services and are subject to the respective legal rules. This document and all parts thereof, may not be copied, reproduced, stored, translated or transmitted to third parties by any means without the prior written consent of MULTICERT. The Client must also warrant that it will not use the know-how and the working methodologies of MULTICERT outside the scope of this project or to third parties

Confidentiality

Information data posted in all pages of this document, including organizational concepts, constitute financial or commercial secret information or are confidential and privileged and are owned by MULTICERT. They are given in trust to the Client with the condition of not being used or disclosed other than the scope of Client and within the terms to be established, without the authorisation of MULTICERT. The Client may allow some collaborating parties, consultants and agents who require knowledge of this document to access to its content, but it shall undertake by all means to assure that the aforementioned persons and entities shall be obliged to the same terms of confidentiality as the Client.

The aforementioned restrictions shall not limit the right to use or disclose the information of this document by identifying the client in the Project where they were obtained by another source and are not subject to any secrecy rule or if they were already disclosed by third parties.

Document Identification: MULTICERT_PJ.PEP.EAC_24.1.2_0001_pt.doc

Keywords: keyword

Document Type: Policy

Title: Portuguese CVCA Certificate Policy

Original Language: Original Language

Language of Publication: English

Rating: Restrict

Date: 30/04/10

Current Version: 1.1

Project Identification: PEP EAC

CA Identification: CVCA

Client: SEF

Version History

Version Number	Date	Details	Author(s)
<u>1.0</u>	<u>08/06/09</u>	<u>Initial Draft</u>	<u>Sara Loja</u>
1.1	30/04/10	<u>Incorporated comments by SEF</u>	Sara Loja

Related Documents

Document Identification	Details	Author(s)
Property	Property	Property
Property	Property	Property

Executive Abstract

A Country Verifying Certification Authority (CVCA) is a non-public certification authority included in a national EAC-PKI.

The needed of this CA is to define the access rights to sensitive data stored on a domestic MRTD chip for all DV's (Document Verifiers).

For the CVCA implementation a set of policy and rules are defined in order to assure a business continuity plan and a level of security when operating a CA.

This document defines the trust between the CVCA and the DV's concerning all policies and rules defined essentially by the Common Certificate Policy for the Extended Access Control Infrastructure for Passports and Travel Documents Issued by EU Member States.

Table of Contents

Portuguese CVCA Certificate Policy	1
Executive Abstract	3
Table of Contents.....	4
Introduction.....	9
Goals.....	9
Intended Readers	9
Document Structure	9
1 Introduction.....	10
1.1 Overview.....	10
1.2 Documentation Name and Identification	10
1.3 PKI Participants	10
1.3.1 Certification Authorities.....	11
1.3.2 Registration Authorities.....	11
1.3.3 Subscribers.....	11
1.3.4 Relying Party.....	11
1.3.5 Other participants	12
1.4 Certificate Usage	12
1.4.1 Appropriate certificate uses.....	12
1.4.2 Prohibited certificate uses	12
1.5 Policy Administration.....	12
1.5.1 Organization	12
1.6 Person determining CPS suitability for the policy	13
1.7 CPS approval procedures	13
1.8 Definitions and Acronyms	13
2 Publication and Repository Responsibilities.....	17
2.1 Repositories.....	17
2.2 Publication of certification information.....	17
2.3 Time and frequency of publication.....	17
2.4 Access control on repositories	17
3 Identification and Authentication	18
3.1 Naming.....	18
3.2 Initial Identity Validation.....	18
3.2.1 National CVCA.....	18
3.2.2 CVCA to CVCA	18
3.2.3 DV to CVCA	18
3.2.4 IS to DV	19
3.3 Identification and Authentication for Re-Key Requests	19
3.3.1 DV to CVCA	19

3.3.2	IS to DVCA.....	19
4	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....	20
4.1	Certificate Application.....	20
4.1.1	Who can submit a certificate application?.....	20
4.1.2	Enrollment process and responsibilities	20
4.2	Certificate application processing	20
4.2.1	Performing identification and authentication functions	20
4.2.2	Approval or rejection of certificate applications	20
4.2.3	Time to process certificate applications.....	21
4.3	Certificate issuance	21
4.3.1	CA actions during certificate issuance.....	21
4.3.2	Notification to subscriber by the CA of issuance of certificate	21
4.4	Certificate acceptance	21
4.4.1	Conduct constituting certificate acceptance.....	21
4.4.2	Publication of the certificate by the CA	21
4.4.3	Notification of certificate issuance by the CA to other entities	22
4.5	Key pair and Certificate Security Rules	22
4.6	Certificate renewal.....	22
4.6.1	Circumstance for certificate renewal.....	22
4.6.2	Who may request renewal.....	22
4.6.3	Processing certificate renewal requests.....	23
4.6.4	Notification of new certificate issuance to subscriber	23
4.6.5	Conduct constituting acceptance of a renewal certificate.....	23
4.6.6	Publication of the renewal certificate by the CA.....	23
4.6.7	Notification of certificate issuance by the CA to other entities	23
4.7	Certificate re-key.....	23
4.7.1	Circumstance for certificate re-key.....	23
4.7.2	Who may request certification of a new public key	23
4.7.3	Processing certificate re-keying requests	23
4.7.4	Notification of new certificate issuance to subscriber	23
4.7.5	Conduct constituting acceptance of a re-keyed certificate	23
4.7.6	Publication of the re-keyed certificate by the CA.....	24
4.7.7	Notification of certificate issuance by the CA to other entities	24
4.8	Certificate modification.....	24
4.9	Certificate revocation and suspension	24
4.10	Certificate status services.....	24
4.11	End of subscription.....	24
4.12	Key escrow and recovery.....	24
5	Management, Operational and Physical Controls.....	25
5.1	Physical Controls.....	25
5.1.1	Site location and construction	25
5.1.2	Physical access.....	25
5.1.3	Power and air conditioning.....	26
5.1.4	Water exposures.....	26

5.1.5	Fire prevention and protection	26
5.1.6	Media storage	26
5.1.7	Waste disposal	26
5.1.8	Off-site backup	27
5.2	Procedural controls	27
5.2.1	Working Groups	27
5.2.2	Number of persons required per task.....	30
5.2.3	Roles requiring separation of duties.....	30
5.3	Personnel controls	31
5.3.1	Qualifications, experience, and clearance requirements.....	31
5.3.2	Background check procedures	31
5.3.3	Training requirements	31
5.3.4	Retraining frequency and requirements.....	31
5.3.5	Job rotation frequency and sequence.....	31
5.3.6	Sanctions for unauthorized actions.....	31
5.3.7	Independent contractor requirements	31
5.3.8	Documentation supplied to personnel	31
5.4	Audit Logging Procedures.....	31
5.4.1	Types of Events Recorded.....	31
5.4.2	Frequency of Processing Log.....	32
5.4.3	Retention Period for Audit Log.....	32
5.4.4	Protection of Audit Log	32
5.4.5	Audit Log Backup Procedures	32
5.4.6	Audit Collection System (Internal vs. External).....	32
5.4.7	Notification to Event-Causing Subject	32
5.4.8	Vulnerability Assessments.....	32
5.5	Records archival.....	33
5.5.1	Types of records archived	33
5.5.2	Retention period for archive.....	33
5.5.3	Protection of archive	33
5.5.4	Archive backup procedures	33
5.5.5	Requirements for time-stamping of records.....	33
5.5.6	Archive collection system (internal or external).....	33
5.5.7	Procedures to obtain and verify archive information	33
5.6	Key changeover.....	33
5.7	Compromise and disaster recovery	34
5.7.1	Incident and compromise handling procedures	34
5.7.2	Computing resources, software, and/or data are corrupted.....	34
5.7.3	Entity private key compromise procedures.....	34
5.7.4	Business continuity capabilities after a disaster.....	34
5.8	CA or RA termination.....	34
6	TECHNICAL SECURITY CONTROLS.....	35
6.1	Key pair generation and installation	35
6.1.1	Key pair generation.....	35

6.1.2	Private key delivery to subscriber.....	35
6.1.3	Public key delivery to certificate issuer	35
6.1.4	CA public key delivery to relying parties	35
6.1.5	Key sizes.....	35
6.1.6	Public key parameters generation and quality checking	35
6.1.7	Key usage	35
6.2	Private Key Protection and Cryptographic Module Engineering Controls	36
6.2.1	Cryptographic Module Standards and Controls	36
6.2.2	Private Key (n out of m) Multi-Person Control	37
6.2.3	Key Archival.....	37
6.2.4	Private Key Transfer into or from a Cryptographic Module	37
6.2.5	Private Key Storage on Cryptographic Module	37
6.2.6	Method of Activating Private Key	37
6.2.7	Method of Deactivating Private Key.....	37
6.2.8	Method of Destroying the Private Key.....	38
6.2.9	Cryptographic Module Rating.....	38
6.3	Other Aspects of Key Pair Management.....	38
6.3.1	Public Key Archival.....	38
6.3.2	Certificate Operational Periods	38
6.4	Activation data	38
6.4.1	Activation data generation and installation	38
6.4.2	Activation data protection.....	38
6.4.3	Other aspects of activation data	39
6.5	Computer security controls.....	39
6.5.1	Specific computer security technical requirements.....	39
6.5.2	Computer security rating	39
6.6	Life cycle security controls.....	39
6.6.1	System development controls	39
6.6.2	Security management controls	39
6.6.3	Life cycle security controls.....	39
6.7	Network security controls.....	39
7	Certificate Profiles.....	40
8	Compliance Audit and other Assessments	42
8.1	Frequency or Circumstances of Assessment.....	42
8.2	Identity/Qualifications of Assessor	42
8.3	Assessor's Relationship to Assessed Entity.....	42
8.4	Topics Covered by Assessment	42
8.5	Actions Taken as a Result of Deficiency.....	42
8.6	Communication of Results	43
9	OTHER BUSINESS AND LEGAL MATTERS	44
9.1	Fees.....	44
9.2	Financial responsibility	44
9.3	Confidentiality of Business Information	44
9.4	Privacy of personal information.....	44

9.5	Intellectual property rights	44
9.6	Representations and warranties	44
9.6.1	CA representations and warranties	44
9.6.2	RA representations and warranties.....	45
9.6.3	Subscriber representations and warranties	45
9.6.4	Relying party representations and warranties	45
9.6.5	Representations and warranties of other participants	45
9.7	Disclaimers of warranties	45
9.8	Limitations of liability	45
9.9	Indemnities	45
9.10	Term and termination	46
9.10.1	Term.....	46
9.10.2	Termination	46
9.10.3	Effect of Termination and Survival	46
9.11	Individual notices and communications with participants	46
9.12	Amendments.....	46
9.12.1	Procedure for Amendment	46
9.12.2	Circumstances under which OID must be changed.....	46
9.13	Dispute resolution provisions.....	47
9.14	Governing law	47
9.15	Compliance with applicable law.....	47
9.16	Miscellaneous provisions.....	47
9.16.1	Entire agreement	47
9.16.2	Assignment.....	47
9.16.3	Severability	47
9.16.4	Enforcement (attorneys' fees and waiver of rights)	47
9.16.5	Force Majeure	47
9.17	Other provisions	47
	Bibliography	48

Introduction

Goals

This document is a Certification Practice Statement, or CPS, whose purpose is to publicly present statement of the practices for issuing and validating Certificates and for supporting reliance on Certificates. It is intended to inform rather than to prescribe legal rules and obligations, and it strives to be simple, straightforward, and readable by a large audience, including people without extensive technical or legal expertise.

This document describes the general practices that SEF (*Serviço de Estrangeiros e Fronteiras*) follows in issuing and managing Certificates for Machine Readable Travel Documents [1], and explains what a Certificate provides and means, what an Authorized Relying Party and other interested persons need to do to rely reasonably on SEF-issued Certificates. This document is subject to change from time to time.

Certificates issued by SEF contain a reference to a CPS in order to enable Authorized Relying Parties and other interested persons to locate further information about the Certificate and the entity that issued it.

Intended Readers

This document should be read by:

- SEF
- All members of CVCA operation Groups
- All EU State Members

Document Structure

The first seven chapters are dedicated to describe the most important certificate procedures and practices. The eighth chapter is dedicated to describe compliance audits and other assessment. The ninth chapter is dedicated to describe legal matters.

I Introduction

I.1 Overview

A Certificate Policy has the meaning of resume all policies and rules applicable to a CA. In the present case, considering the Common Certificate Policy for the Extended Access Control Infrastructure for Passports and Travel Documents Issued by EU Member States, this Certificate Policy describes the CA functionality and operation including all Human Resources and environments needed.

I.2 Documentation Name and Identification

This Certificate Policy is identified by the following attributes:

Document Information	
Document Name	CVCA Portuguese Certificate Policy
Document Version	1.1
OID	
Document State	Draft
Issuing Date	2010/04/30
Validity	Not Applicable
Localization	INCM

I.3 PKI Participants

This chapter gives an overview of the PKI Participants. The next table shows all the participants.

	Certification Authority	Registration Authority	Subscriber	Relying Party
CVCA ⁱ	x	x		

DVⁱⁱ	x	x	x	x
ISⁱⁱⁱ			x	x
MRTD^{iv}				x

1.3.1 Certification Authorities

The Root Certification Authority of a national EAC-PKI is called Country Verifying Certification Authority.

The Portuguese CVCA does not have a superior CA, such as a root. Rather, the Portuguese CVCA acts as its own root and has issued itself a self-signed root Certificate. It also issues DVCA certificates. Thus, the EAC-PKI hierarchy consists only of the Portuguese non-public CVCA issuing certificates to its subscribers which are the Document Verifiers responsible for the Inspection Systems.

The Portuguese CVCA determines the access level of all the DV's to the sensitive data stored on the MRTD chips by issuing DV certificates entitling access control attributes.

1.3.2 Registration Authorities

The Country Verifier Registration Authorities have the responsibility of the certificate requests deliverance. The identification and authentication on this request should result on a trustworthy Document Verifier Certificate Request to the CVCA. The CVCA is responsible for the DVCA certificate issuance.

Each DVCA has in the same way a DVRA, Document Verifier Registration Authority, who is responsible for the identification and authentication of the Inspection Systems Certificate Requests. After the IS certificate issuance the DVCA is responsible for its renovation or revocation.

All rules and policies of CVCA are also applicable to the DVCA and both Registration Authorities.

1.3.3 Subscribers

The subscribers identified by this policy are the DVCA, CVCA certificate holder, and the IS, DVCA certificate holder.

The only subscriber under the CVCA is the European Commission, to whom all DVCA certificates are issued.

In this CP, "subscriber" (the entity which contracts the issuance of the certificate) and "subject" (the entity to whom the credential is bound) can be used interchangeably.

1.3.4 Relying Party

A Relying Party is an individual, an entity or system that acts in reliance of a certificate and/or a digital signature issued under the CVCA.

The Relying Parties identified on this policy are:

- Document Verifiers (DV's);
- Inspection Systems (IS's);

- Machine Readable Travel Documents (MRTD's).

I.3.5 Other participants

No stipulation.

I.4 Certificate Usage

I.4.1 Appropriate certificate uses

CVCA key pair and certificate were issued for the following purposes:

- CVCA private Key is used only to sign national and external DVCA certificates;
- CVCA certificate is used to verify signatures realized by nacional and external DV;

DVCA key pair and certificate were issued for the following purposes:

- DVCA private key is only used to sign national IS certificates;
- DVCA certificate is used to verify signatures of national and external IS certificates.

For the following certificates the trusted certification path is:

- CVCA certificate: Self-signed Certificate;
- DCVA certificate: signed by, at least, the national CVCA;
- IS certificate: signed by DVCA

Relying Parties should verify the following trusted path certification:

- DV: National CVCA certificate is an authorized Member State CVCA Certificate;
- IS: National DVCA certificate is signed by a CVCA certificate of an authorized Member State CVCA Certificate;
- MRTD: IS Certificate issued by a DVCA which certificate is signed by a CVCA certificate of an authorized Member State CVCA Certificate.

Trusted certification paths are used to read fingerprint biometrics store on the MRTD's to verify the identity of his holder.

I.4.2 Prohibited certificate uses

Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

CVCA Certificates may not be used for any functions except CVCA functions.

I.5 Policy Administration

I.5.1 Organization

Name	CVCA Policy Working Group Contacts
Responsible:	Pedro Sousa / Susana Fonseca
Address:	Serviço de Estrangeiros e Fronteiras Av. Do Casal de Cabanas. Urb. Cabanas Golfe, N°1 Tagus Park 2734-505 Barcarena - Oeiras Portugal
e-mail:	cps.manager@pep.pt
Web site:	www.sef.pt
Phone number:	+351214236200

1.6 Person determining CPS suitability for the policy

The Policy Working Group determines the suitability and applicability of this CPS.

1.7 CPS approval procedures

Approval of this CPS and subsequent amendments (or updates) shall be made by the Policy Working Group. Amendments (or updates) shall be published in the form of new releases of the CPS. Amendments and updates supersede any designated or conflicting provisions of the referenced version of the CPS.

The Policy Working Group shall determine whether changes to the CPS require a change in the Certificate policy object identifiers of the Certificate policies.

1.8 Definitions and Acronyms

The next table shows all the terms used during this document:

Term	Meanings
------	----------

Authentication	<i>The process of establishing that individuals, organizations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual or organization. This corresponds to the second process involved with identification, as shown in the definition of "identification" below. Authentication can also refer to a security service that provides assurances that individuals, organizations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organization, or device. Thus, it is said that a digital signature of a message authenticates the message's sender.</i>
Certificate Policy (CP)	<i>A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.</i>
Certification Authority (CA)	<i>An authority trusted and authorised to issue and manage X.509 Public Key Certificates and CRLs. Certification Authority</i>
Certification path	<i>An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.</i>
Certification Practice Statement (CPS)	<i>A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates, and providing access to them, in accordance with specific requirements (e.g., requirements specified in the Certificate Policy, or requirements specified in a contract for services).</i>
CVCA	<i>Country Verifying Certification Authority</i>
DN	<i>Distinguished Name</i>
DNS	<i>Dynamic Network Services</i>
DS	<i>Document Signer</i>
DVCA	<i>Document Verifying Certification Authority</i>
EC	<i>European Commission</i>
HSM	<i>Hardware Security Module</i>
ICAO	<i>International Civil Aviation Organization</i>
Identification	<i>The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization. In the context of a PKI, identification refers to two processes: (1) establishing that a given name of an individual or organization corresponds to a real-world identity of an individual or organization, and (2) establishing that an individual or organization applying for or seeking access to something under that name is, in fact, the named individual or organization. A person seeking identification may be a certificate applicant, an applicant for employment in a trusted position within a PKI participant, or a person seeking access to a network or software application, such as a CA administrator seeking access to CA systems.</i>

Intellectual Property Rights (IPR)	<i>Includes copyright works, databases, data, designs, discoveries, inventions, improvements, know-how, confidential information, all title, rights and interests to and in all of these or arising out of them (whether such rights exist, or are of a kind which exist, at the time of this agreement or whether they or that kind only come into existence afterwards), applications for and registrations of them and the rights in them, and the right to apply for any form of protection for any of these things and rights (whether such rights exist, or are of a kind which exist, at the time of this agreement or whether they or that kind only come into existence afterwards) In each case it includes the aforesaid title, rights and interests in every part of the world for their full term, including any renewals and extensions, the right to receive any income from them, and the right to sue in respect of any past, continuing or future infringement of any of them, and to claim and receive damages (or an account of profits) and interest in respect of any such infringement.</i>
Issuing CA	<i>In the context of a particular certificate, the issuing CA is the CA that issued the certificate.</i>
MRTD	<i>Machine Readable Travel Documents</i>
OID	<i>Object Identifier</i>
PEM	<i>Privacy Enhanced Mail (according to [13], [14], [15], [16])</i>
PEP	<i>Passaporte Electrónico Português</i>
Policy qualifier	<i>Policy-dependent information that may accompany a CP identifier in an X.509 certificate. Such information can include a pointer to the URL of the applicable CPS or relying party agreement. It may also include text (or number causing the appearance of text) that contains terms of the use of the certificate or other legal information.</i>
Registration Authority (RA)	<i>An entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by subscribers to renew or re-key their certificates. RAs, however, do not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).</i>
Relying Party	<i>An individual or an organisation, who acts in reliance on a certificate and digital signatures, verified using that certificate.</i>
Root Authority	<i>The Certification Authority (CA) at the top of a CA hierarchy.</i>
SEF	<i>Serviço de Estrangeiros e Fronteiras</i>
Subject	<i>The holder of a private key corresponding to a public key. The term “Subject” can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject’s Certificate.</i>

Subscriber	<i>In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organizational Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.</i>
UPS	<i>Uninterruptible Power Supply</i>
URI	<i>Uniform Resource Identifiers</i>

2 Publication and Repository Responsibilities

The European Commission is the responsible entity who maintains the list of contact details for CVCA's and DV's .

This information is available on the web site of the Directorate General for Justice, Freedom and Security (DG-JLS) of European Commission.

2.1 Repositories

EC is responsible for the repository functions of the Portuguese CVCA. Upon revocation of the Portuguese CVCA, EC publishes notice of such revocation in the repository.

2.2 Publication of certification information

A web-based repository that permits Relying Parties to make online inquiries regarding the CVCA is under development.

2.3 Time and frequency of publication

No stipulation

2.4 Access control on repositories

No stipulation

3 Identification and Authentication

3.1 Naming

The Certification Authority Reference, defined by TR-EAC A.6.1, is used for identification of the public key used to verify the signature of the certification authority.

The Certificate Authority Reference must be equal to the Certificate Holder Reference. This last one must correspond to the Certification Authority Certificate.

The Certificate Holder Reference identifies the certificate public key and should be unique in all certificates issued by the CA.

In accordance with TR-03110 chapter A6.1, the Certificate Holder Reference should be composed by the following:

- Country Code: The ISO 3166-1 ALPHA-2 country code of the certificate holder's country;
- Holder Mnemonic: A mnemonic that represents the certificate holder;
- Sequence Number: Numeric or alphanumeric sequence number.

3.2 Initial Identity Validation

3.2.1 National CVCA

SEF is the entity responsible for the authentication and identification of CVCA.

3.2.2 CVCA to CVCA

In order to recognize the CVCA the following requirements should be fulfilled:

- CVCA Portuguese Certificate Policy;
- A copy of the CVCA Public Key.

These requirements should be available to the European Commission in order to be distributed to the other CVCA's participants.

This document, CVCA Portuguese Certificate Policy should be verified every year and, in case of changes, the latest version should be submitted to the European Commission for distribution.

3.2.3 DV to CVCA

When a DVCA submits a request do the Portuguese CVCA this communication should be done by a trusted channel.

In the request, the DVCA must include:

- The public part of the DV Certificate Pratic Statement;
- The latest Certificate of Conformity with the National Certificate Policy for the DV;
- A list of the organizations using Inspection Systems (IS) subscribing the DV;

- A Certificate Request as specified in TR-EAC, paragraph A.4.2. This certificate request must include the Outer Signature, as defined in TR.EAC paragraph A4.3.4, signed by the DVs supervising CVCA.

3.2.4 IS to DV

An IS requests is made do DV's by hand and delivered in DV Operators Hands. A Certificate Request Form accompanied by the IS Certificate Request is also delivery to the operators in order to identify and authenticate the request.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 DV to CVCA

When a DVCA submits a request do the Portuguese CVCA this communication should be done by a trusted channel.

The CVCA should confirm the followings requirements before submit the request:

- The request is formatted in accordance with TR-EAC paragraph A.4.2
- The last DVCA certificate is still valid;
- The DV's Certificate Conformity is valid;
- That the outer signature of the request is created with a key which is valid with respect to a certificate if that DV, issued by the CVCA.

3.3.2 IS to DVCA

DVCA should only re-key a IS certificate if:

- IS stills registered as operational;
- IS is not registered as stolen/missing.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

Any individual who is a formally authorized Certificate Applicant may submit certificate requests.

4.1.2 Enrollment process and responsibilities

4.1.2.1 CVCA Certificates

SEF is the authorized entity responsible for the CVCA certificate issuance.

4.1.2.2 DVCA Certificates

An authorized Certificate Applicant shall submit the DVCA certificate issuance request form, and undergo an enrollment process consisting of:

- generating the key pair (private and public key);
- generating the corresponding certificate request;
- generating the hash of the certificate request, in PEM format;
- saving the certificate request and the hash in a CD/DVD;
- delivering, in hand, the CD and the DVCA certificate issuance form to SEF CA operators. The SEF CA operators will verify the identity of the Certificate Applicants and return a dated and signed copy of the DVCA certificate issuance form.
- receiving, handed by the SEF CA operators, the DVCA certificate issued form and the CD with the DVCA certificate (corresponding to the certificate request) in PEM format;
- installing the DVCA certificate and returning a dated and signed copy of the DVCA certificate issued form.

Notice that CVCA and DVCA are operated by the same Working Groups.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

SEF performs identification and authentication of all required information in terms of section 3.2.

4.2.2 Approval or rejection of certificate applications

4.2.2.1 CVCA Certificates

The Portuguese CVCA certificate must be issued only by authorized and valid members. The CVCA certificate should be issued only during a generation key ceremony.

4.2.2.2 DVCA Certificates

SEF will approve an application for a DVCA certificate if the following criteria are met:

- successful identification and authentication of all required information in terms of section 3.2;
- DVCA certificate issuance request form correctly filled;
- valid certificate request;

CVCA must issue the DVCA certificate in 72 hours.

In any other case, SEF will reject the ECD certificate application.

4.2.2.3 IS Certificates

SEF will approve an IS certificate issuance if the following criteria are met:

- successful identification and authentication of all required information in terms of section 3.2;
- IS certificate issuance request form correctly filled;
- valid certificate request;

In any other case, SEF will reject the DVCA certificate application.

4.2.3 Time to process certificate applications

All certificates shall be issued in no more than three (3) working days, after the approval of the certificate application.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

As in section 4.1.2

The segregation of functions in place, doesn't allow that less than four (4) Working Group members issue any certificate.

4.3.2 Notification to subscriber by the CA of issuance of certificate

As in section 4.1.2

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The following conduct constitutes certificate acceptance:

- installing the certificate and returning a dated and signed copy of the certificate issued form.

4.4.2 Publication of the certificate by the CA

As in Section 2.

4.4.3 Notification of certificate issuance by the CA to other entities

SEF must give 90 days' notification that their CVCA certificate is about to change, and then distribute the new CVCA certificate by strictly secure diplomatic means (out-of-band distribution) to EU.

4.5 Key pair and Certificate Security Rules

CVCA's, DV's and IS's must be compliant with the following requirements:

- Ensure that accurate and complete information is submitted to the CVCA/DVCA;
- The key pair is only used in accordance with the limitations imposed by this CP;
- Ensure that there is no unauthorized use of the private key;
- Keys are generated in accordance with TR-EAC;
- Only use private keys for signing or decrypting within a secure cryptographic device as described in section 6.2.
- Notify a CVCA/DV without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:
 - A private key has been lost, stolen or potentially compromised;
 - Control Over the private key has been lost due to compromise of activation data;
 - Inaccuracy or changes to the certificate content, as notified to the subscriber or subject,
- Following compromise, the use of a private key is immediately and permanently discontinued;
- In the case of being informed that CVCA or DV's private key has been compromised and certificates signed by these Private Key's should not be relied upon and should act appropriately.

Key pair and certificate usage should be indicating by CVCA/DVCA in the Certificate issuance form.

DVCA and IS should only use the private key for the purposes indicated by the certificate issuer as described in section 1.4

4.6 Certificate renewal

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

Certificate renewal is not allowed for CVCA or DVCA.

4.6.1 Circumstance for certificate renewal

No stipulation.

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing certificate renewal requests

No stipulation.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate re-key

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

4.7.1 Circumstance for certificate re-key

The CVCA certificate will be re-keyed 10 days before the end of validity of the certificate, which is 3 (three) years. The period of re-key was defined concerning the following:

- the length of time the CVCA key will be used to issue DVCA certificates
- the longest validity period of any DVCA certificate issued under that key, and
- the period of time necessary to propagate the DVCA certificate.

4.7.2 Who may request certification of a new public key

As in section 4.1.1.

4.7.3 Processing certificate re-keying requests

As in section 4.1.2 and 4.2.

4.7.4 Notification of new certificate issuance to subscriber

As in section 4.3.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

As in section 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

As in section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

As in section 4.4.3.

4.8 Certificate modification

Certificate modification is not allowed by Portuguese CVCA.

4.9 Certificate revocation and suspension

Certificate revocation and suspension are not allowed by Portuguese CVCA. See section 5.7.

4.10 Certificate status services

Portuguese CVCA does not support certificate status services.

4.11 End of subscription

Not applicable.

4.12 Key escrow and recovery

Portuguese CVCA does not allow key escrow.

5 Management, Operational and Physical Controls

SEF has implemented several policies and rules regarding physical, procedural and personnel controls, which support the security requirements of this CPS. This section describes an overview of the non-technical security requirements used to securely perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, auditing and archiving. These non-technical security controls are critical to trusting the certificates since lack of security may compromise CA operations.

5.1 Physical Controls

5.1.1 Site location and construction

The Portuguese CVCA operations are conducted inside a small high-security room in a high security zone, within a physically protected building that deters, prevents, and detects unauthorized access, based on multiple tiers of physical security.

The following operation conditions are assured in the protected building:

- Clearly defined security perimeters;
- Solid walls, real floor and real ceiling preventing unauthorized entry;
- Hinges and locks of the high-security room access doors are protected against break-in. If necessary, the doors can be armoured;
- The perimeter of the building is physically sound (i.e., there are no gaps in the perimeter where a break-in could easily occur);

A manned reception area and other means to control physical access are in place to restrict access to authorized personnel only.

5.1.2 Physical access

Portuguese CVCA systems are protected by a minimum of four tiers of physical security (protected building, high-security zone, high-security area, high-security room), with access to the lower tier required before gaining access to the higher tier.

Progressively restrictive physical access privileges control access to each tier. Sensitive CA operational activity, creation and storage of cryptographic material, any activity related to the lifecycle of the certification process such as authentication, verification, and issuance, occur within the high-security room. Access to each tier requires the use of a badge (yellow badge to access the protected building and red badge to access the other tiers). Physical access is automatically logged and video recorded for audit purposes.

Access to red badge tiers enforces individual access control through the use of two factor authentication. Unescorted personnel, including untrusted employees or visitors, are not allowed into such secured areas. Unless all personnel inside these areas are known to each other, they are required to wear visible identification and are obliged to challenge anyone not complying with this rule.

Access to the high-security room requires dual control, each through the use of two factor authentication, including biometrics. Cryptographic hardware and keying material are further protected

through the use of locked safes, cabinets and lockers. Access to the high-security room, cryptographic hardware and keying material is restricted in accordance with Working Groups segregation of duties requirements.

5.1.3 Power and air conditioning

SEF's secure facilities are equipped with primary and backup equipment that ensures the 24 hours a day / 7 days a week functioning of:

- power systems to ensure continuous, uninterrupted access to electric power (backup systems consist of UPS batteries and diesel electricity generators), and
- heating/ventilation/air conditioning systems to control temperature, relative humidity and moisture level, providing adequate conditions for correct functioning of all the electronic and mechanical equipments present inside the environment. A GSM alert system is in place, which will automatically phone the high-security room maintenance team with a pre-registered message, if temperature conditions fall out of the adequate range.

5.1.4 Water exposures

SEF has taken reasonable precautions to minimize the impact of water exposure to Portuguese CVCA systems. A flooding detection and alarm system is in place in the high-security room and surrounding area (high-security area).

5.1.5 Fire prevention and protection

SEF has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. Complying with local fire safety regulations:

- fire detection and alarm system are in place in all the physical security tiers,
- portable and fixed fire extinguishing equipment are readily available, placed conspicuously and within easy reach so they can be accessed quickly while a fire is still small,
- fire emergency procedure are well defined.

5.1.6 Media storage

All media containing production software and data, audit, archive, or backup information is stored in locked safes and cabinets within SEF's high-security room and, in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized Working Group members and protect such media from accidental damage (e.g., water and fire).

When, for backup purposes, sensitive information must be moved from the high-security room to the secure off-site storage facility, the process must be performed under the supervision of, at least, 2 (two) Working Group members that must ensure the safe transportation of the information to its final destination. The information (or the information container) must be in the member(s)'s sight at all times.

If a situation arises that implies the physical move of certain hardware containing storage media (i.e., fixed hard disks) from the high-security room for purposes other than backup, every item of that hardware is checked to determine whether they contain any sensitive data. In that case, the information must be neutralized using whatever means necessary (like storage media formatting, cryptographic hardware reset or even physical destruction of the storage media/equipment).

5.1.7 Waste disposal

Sensitive documents and materials are shredded before disposal.

Media used to collect or transmit sensitive information are rendered unreadable (securely erased or physically destroyed) before disposal. Cryptographic devices and keying material are physically destroyed

or zeroized in accordance to the manufacturers' guidance, prior to disposal. Other storage hardware (hard disks or other storage equipment) must be zeroized before disposal, using whatever means necessary (secure formatting or physical destruction of the storage media/equipment).

5.1.8 Off-site backup

Off-site backup media is stored in locked safes and cabinets in SEF's secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water and fire).

5.2 Procedural controls

In this section, requirements for recognizing trusted roles are described, together with the responsibilities for each role. This section also includes the separation of duties in terms of the roles that cannot be performed by the same individuals.

5.2.1 Working Groups

Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations.

SEF has established that Trusted roles are grouped in seven different categories (named as working groups), to ensure that multiple Trusted Persons are required to perform sensitive tasks.

5.2.1.1 Policy Working Group

This group's purpose is to define all the CA's policies and guarantee their update and availability. This group must have a minimum of two members.

This group's duties are:

- Managing the "Information Environment",
- Defining all the CA's policies,
- Guaranteeing that policies are available to whoever is necessary,
- Playing the "Security Administrator" role, as defined in [19], article 29th,
- Ensuring the CA's CP are supported by the CA's CPS.

5.2.1.2 Audit Working Group

This group will audit the execution of CA processes and ceremonies, registering sensible operations and validating the security of all resources used. This group must have a minimum of two members.

This group's duties are:

- Sanctioning the exactness of processes,
- Investigating suspicions of procedural fraud,
- Checking functionality of safety controls (alarm devices, fire detectors, etc), when present in an environment,
- Registering all security auditable procedures,
- Registering all security auditable checks,
- Check all logs relating to the Portuguese CVCA;

- Playing the “System auditor” role, as defined in [19], article 29th,
- According to [19], article 30th:
 - The auditor must be independent from the certification authority, needs to have recognized competency, experience and qualifications proven in the information security area in the performance of security auditory and usage of the ISO/IEC 17799 standard, and needs to have been credentiated by the “*Gabinete Nacional de Segurança*”;
 - The certification authority needs to make proof, with the annual audit and security report (produced by the accredited security auditor), that risk evaluation has been assured, identifying and implementing all the measures necessary to information security;
 - The security auditor must guarantee that its team members do not perform partially or discriminatorily and that none of the auditors has worked for the certification authority in the previous 3 years nor have they any other kind of agreement or legal contract with the certification authority.

5.2.1.3 Operation Working Group

This group is responsible for the major tasks of the CA’s everyday operation, including backup operations and monitoring hardware and software malfunctions. The members of this group must be composed of (at least) 4 (four) members .

This group’s duties are:

- Managing the “Operation Environment” and “Operational Environment”,
- Perform the CA’s routine operations,
- Perform the CA’s systems backup ceremonies,
- Perform the CA’s systems monitoring ceremonies,
- To monitor, report and quantify hardware and software incidents and malfunctions, calculating its consequent cost to the company,
- Playing the “System Administrator” role, as defined in [19], article 29th,
- Playing the “System Operator” role, as defined in [19], article 29th,
- Playing the “Registration Administrator” role, as defined in [19], article 29th.

5.2.1.4 Authentication Working Group

This group is responsible for providing, managing and keeping, all non personal passwords and authentication tokens. This group must also take adequate measures in case of a security token or password compromise. The members of this group must be composed of (at least) 6 (six) members.

No member of this group is allowed to enter “Operation Environment” without presence of member of the Operation Working Group and/or Auditing Working Group.

These group duties are:

- Managing the “Authentication Environment”,
- Managing all non personal passwords,
- Maintaining an inventory of all existing authentication tokens used in the "Operation

Environment" and, when these tokens are entrusted to someone, to register the identification of the member(s) in its possession storing these registers in the "Authentication Environment",

- Maintaining an inventory of all the passwords used in the "Operation Environment" and, when these passwords are entrusted to someone, to register the identification of the member(s) in its possession storing these registers in the "Authentication Environment",
- To entrust each of other groups members with no more than per need authentication tokens, used in the "Operation Environment", to perform his/her duties,
- To entrust each of other groups members with no more than per need authentication passwords, used in the "Operation Environment", to perform his/her duties,
- To register the return of the authentication tokens, used by users in the "Operation Environment",
- To register the change of authentication passwords used inside the "Operation Environment",
- To register the loss of an authentication token, used by users in the "Operation Environment",
- To register the compromise of an authenticating password, used by users in the "Operation Environment",
- To evaluate business risks concerning the loss of an authentication token or the compromise of an authentication password used inside each "Operation Environment",
- To take active measures to prevent the compromise of each "Operation Environment" in case of an authentication token loss or the compromise of an authentication password used in the "Operation Environment",
- To evaluate requests for documentation replication.

5.2.1.5 Setup Working Group

This group is responsible for the initial setup of the CA (hardware, software, passwords), until its initialization. This group must have a minimum of one member.

This group's duties are:

- To install and configure the CA's base software,
- To setup, install and configure the CA's hardware,
- To setup any passwords, for the first time, that will have to be changed afterwards by the appropriated group.

5.2.1.6 Management Working Group

This group is responsible for appointing the working group's members, as well as approving documents. This group must have a minimum of two members.

These group duties are:

- Managing for the "Management Environment",
- Revising and approving documentation,
- Appointing all members of all working groups,
- Publishing identification of all individuals that are part of working groups, in one or more locations, that can be easily accessed by authorized parties.

5.2.1.7 Custody Working Group

This group is responsible for safekeeping some sensitive items (authentication tokens, etc) in their facilities. This group must use the secure environments made available to them in order to keep items in their procession.

This group's duties are:

- To guard sensitive items, such as authentication tokens, etc, using whichever means they find adequate to accomplish the security requirements,
- To safely delivery those items to authorized group members that are explicitly allowed to access them, after following the proper entrust procedures.

5.2.2 Number of persons required per task

SEF enforces rigorous control procedures to ensure the segregation of duties based on working group membership and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

The internal control procedures are designed to ensure that at a minimum, two trusted persons are required to have either physical or logical access to security devices. 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 separate parts of the activation key and vice versa.

5.2.3 Roles requiring separation of duties

The following matrix defines the working group memberships that are not allowed in conjunction for any member. The X represents a denied combination.

	Setup	Policy	Operation	Authentication	Audit	Custody	Management
Setup					x	x	x
Policy					x	x	x
Operation				x	x	x	x
Authentication			x		x	x	x
Audit	x	x	x	x		x	x
Custody	x	x	x	x	x		x
Management	x	x	x	x	x	x	

5.3 Personnel controls

SEF requires that personnel seeking to become members of the Working Groups:

- are approved by SEF HR after performing SEF's usual personnel security recruitment control,
- present proof of background, qualifications, and experience needed to perform the Working Group duties.

5.3.1 Qualifications, experience, and clearance requirements

SEF requires that personnel seeking to become members of the Working Groups present proof of background, qualifications, and experience needed to perform the Working Group duties, as well as government clearances if needed.

5.3.2 Background check procedures

SEF conducts background checks which include:

- confirmation of the identification, using documentation from reliable sources, and
- search of criminal records.

5.3.3 Training requirements

SEF provides members of the Working Groups with the adequate information and training to perform its duties competently and satisfactorily.

5.3.4 Retraining frequency and requirements

SEF provides updates training to members of the Working Groups to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

Appropriate sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of entity systems are taking, according to SEF rules and national security laws.

5.3.7 Independent contractor requirements

Independent contractors or consultants are permitted access to SEF's high-security room, only to the extent they are escorted and directly supervised by SEF's Working Group members, at all times.

5.3.8 Documentation supplied to personnel

SEF provides members of the Working Groups with the adequate information to perform its duties competently and satisfactorily.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Significant events generate auditable logs. These include, at least, the following:

- certificate application, request, issuance, renewal, rekey and revocation;
- CRL publishing;
- security-related events, including:
 - access attempts (successful and unsuccessful) to sensitive CA system resources;
 - operations performed by Working Group members,
 - physical security tiers entry/exit.

Log entries include the following information:

- serial number of the event;
- date and time of the event;
- identity of the subject that caused the event;
- category of the event;
- description of the event.

5.4.2 Frequency of Processing Log

Erro! Nome desconhecido de propriedade de documento examines and reviews the audit logs on a regular basis and, additionally, if there is any suspicious or unusual activity or threats of any kind. Actions taken based on audit log reviews are also documented.

5.4.3 Retention Period for Audit Log

Audit logs are kept available onsite for at least 2 (two) months after processing, and then are archived on the terms described in Section 5.5.

5.4.4 Protection of Audit Log

Audit logs are only examined and reviewed by authorized Working Group members.

Besides, audit logs are protected against modification, deletion and other tampering schemes by electronic audit mechanisms, allowing the detection of such an occurrence, if any.

5.4.5 Audit Log Backup Procedures

Backups of audit logs are created in a regular basis on long term storage media.

5.4.6 Audit Collection System (Internal vs. External)

Audit logs are collected simultaneously internally and externally to the CA system.

5.4.7 Notification to Event-Causing Subject

Audit events are logged to the audit collection system and kept secure, but no notice is given to the subject who caused an audit event to occur.

5.4.8 Vulnerability Assessments

Erro! Nome desconhecido de propriedade de documento regularly inspects the audit logs in order to assess potential attempts to breach the security of the system.

5.5 Records archival

5.5.1 Types of records archived

SEF archives all audit data, certificate application information and documentation, and documentation supporting lifecycle operations.

5.5.2 Retention period for archive

Records shall be retained for the time periods set by the national laws.

5.5.3 Protection of archive

SEF protect the archive so that:

- only authorized Working Group members can view and have access to the archive,
- the archive is protected against modification and deletion,
- the archive is protected against the deterioration of the media on which it is stored, through periodically migration to fresh media, and
- the archive is protected against obsolescence of hardware, operating systems, and other software, by retaining as part of the archive, the hardware, operating systems, and/or other software in order to permit access to and use of archived records over time,
- the archives are kept at SEF's secure off-site storage facility.

5.5.4 Archive backup procedures

Backups of archives are incrementally or fully backed up on WORM (Write Once Read Many) devices.

5.5.5 Requirements for time-stamping of records

Some archive entries shall contain time and date information. Such time and date information must not be cryptographic-based.

5.5.6 Archive collection system (internal or external)

Archive collection systems are internal.

5.5.7 Procedures to obtain and verify archive information

Only authorized Working Group members have access to the archives. The integrity of the archive can be verified by its restoration.

5.6 Key changeover

No stipulation

5.7 Compromise and disaster recovery

This section describes requirements relating to notification and recovery procedures in the event of compromise or disaster.

5.7.1 Incident and compromise handling procedures

Backups of CA private keys (generated and maintained in accordance with section **Error! Reference source not found.**) and archived records (section 5.5.1) are kept in SEF's secure off-site facility and made available in case of compromise or disaster.

5.7.2 Computing resources, software, and/or data are corrupted

In the event, computing resources, software, and/or data are corrupted or suspected to be corrupted, the backup of the CA private key and archived records can be obtained and the integrity of the original data can be verified.

If the computing resources, software, and/or data are corrupted, appropriate incident response should be taken. The incident response can include the re-establishment of the corrupted equipment/data, using similar equipment and/or restoring backup/archived data.

5.7.3 Entity private key compromise procedures

In the event the Portuguese CVCA private key is compromised or suspected to be compromised, appropriate incident response should be taken. The incident response can include:

- revocation of the Portuguese CVCA certificate and communication to relying parties, in accordance to section 4.9,
- generation of a new key pair in accordance with section 4.7..

5.7.4 Business continuity capabilities after a disaster

SEF has the needed computing resources, software, backup data, archived records and backup CA private key at its secure off-site facility, to re-establish or recover essential operations (certificate issuance and revocation, with the publication of revocation information) after a natural or other disaster.

5.8 CA or RA termination

In case of Portuguese CVCA termination, SEF should:

- Notify all CVCA's with which it is registered of the termination;
- Notify all CVCA's with which it is registered, of the CVCA, if any if any, which will be taking over responsibility for national DV's,
- Notify all DV's which it supplies with certificates of termination
- Notify all DV's with which it supplies with certificates, of the CVCA, if any, which will be taking over responsibility for national DV's,
- Any replacement CVCA must continue to provide certificates for MRTD's issued under the original Portuguese CVCA,
- The CVCA shall destroy, or withdraw from use, its private keys.

6 TECHNICAL SECURITY CONTROLS

This section defines the security measures taken by the Portuguese CVCA to protect its cryptographic keys and activation data. Secure key management is critical to ensure that all secret and private keys and activation data are protected and used only by authorized personnel.

6.1 Key pair generation and installation

6.1.1 Key pair generation

The Portuguese CVCA key pair generation is performed by Working Group authorized members, in a planned and audited Key Generation Process, in accordance with written procedures. The activities performed in each key generation process are recorded, dated and signed by all Working Group members involved. These records are kept for audit purposes.

For the Portuguese CVCA key, the cryptographic hardware used for key generation meet the requirements of FIPS 140-1 level 3 and performs all key management, key storage, and key operations exclusively within hardware. Comprehensive security policies, split user roles, and two-factor, trusted path authentication prevent unauthorized access to critical root keys. Direct hardware-to-hardware backup permits auditable backups of key material for backup and disaster recovery.

6.1.2 Private key delivery to subscriber

For DVCA key pairs, private key delivery to subscriber is not applicable, since the key pairs are generated by the end-use subscriber (Certificate Applicant).

6.1.3 Public key delivery to certificate issuer

DVCA Certificate Applicant delivers, in hand, a CD/DVD with the Certificate Signing Request (CSR) and the DVCA certificate issuance form to SEF CA operators

6.1.4 CA public key delivery to relying parties

As in section 2.2.

6.1.5 Key sizes

Key pairs shall be of sufficient length to prevent others from determining the key pair private key using cryptanalysis during the period of expect utilization of such key pair. The expected key size strength is:

- CVCA key pairs– 4096 bits ECDSA,
- DVCA key pairs – 2048 bits ECDSA.

6.1.6 Public key parameters generation and quality checking

As in section 6.1.1.

6.1.7 Key usage

The Portuguese CVCA keys must only be used for the following purposes:

- Signing Certificate issued to DVCA's,
- Validating signatures of certificates issued by DVCA's;

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Requirements for private key protection and cryptographic modules need to be considered for the Portuguese CVCA and DVCA – SEF has implemented a combination of physical, logical, and procedural controls to ensure the security of Portuguese CVCA and DVCA private keys.

6.2.1 Cryptographic Module Standards and Controls

For Portuguese CVCA and DVCA key pair generation and private key storage, SEF uses hardware cryptographic modules that are certified or meet the requirements of the following standards:

Physical Security

- Common Criteria EAL 4+
- FIPS 140-2, Level 3

Regulatory Standards Certification

- U/L 1950 (EN60950) & CSA C22.2 compliant
- FCC Part 15 - Class B
- ISO - 9002 Certification
- RoHS compliant
- BAC and EAC ePassport Certification

Roles

- Two-Factor Authentication

API Support

- PKCS#11
- Microsoft CAPI, and CNG
- JCA/JCE
- OpenSSL

Random Number Generation

- ANSI X9.17 (Annex C)

Asymmetric Key Encryption and Key Exchange

- Diffie-Hellman (1024-4096 bit)
- RSA (512-4096 bit)
- PKCS#1 v1.5
- OAEP PKCS#1 v2.0

Digital Signing

- RSA (1024-4096-bit)
- DSA (512-1024-bit)

- PKCS#1 v1.5
 - Message Authentication Codes (MAC)
 - HMAC-MD5
 - HMAC-SHA-1
 - SSL3-MD5-MAC
 - SSL3-SHA-1-MAC
- Elliptical Curve Cryptography (ECC)
- Korean Algorithms
- ECC Brainpool Curves (named and user-defined)
- Suite B Algorithm Support and ARIA support

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

SEF has implemented technical and procedural mechanisms that require the participation of multiple Working Group members to perform sensitive CA cryptographic operations.

The activation data needed to make use of the Portuguese CVCA private key is spitted into separate parts (stored in role-splitting PED Keys – small, key-shaped digital identification tokens –), which are held by different Working Group members. A threshold number of separate parts (n) out of the total number of separated parts (m) is required to activate the Portuguese CVCA private key stored on the hardware cryptographic module. The threshold number of separate parts needed to activate the Portuguese CVCA private key is 2.

6.2.3 Key Archival

CVCA and DVCA private keys are erased in an auditable and accountable manner after reaching the end of their validity period (or if revoked before the ending of that period).

6.2.4 Private Key Transfer into or from a Cryptographic Module

CVCA private key never leave a FIPS 140-1 Level 3 cryptographic token.

Even when these key pairs are backed up to another cryptographic token, direct hardware-to-hardware backup is performed and such key pairs are transported between modules in encrypted form.

6.2.5 Private Key Storage on Cryptographic Module

CVCA and DVCA private keys are stored in encrypted form on the hardware cryptographic modules.

6.2.6 Method of Activating Private Key

In order to activate the Portuguese CVCA's private key(s) it is required the intervention of, at least, four members of the Working Groups. Once the key is activated, it will remain active until a deactivation process is executed.

6.2.7 Method of Deactivating Private Key

In order to deactivate the CVCA's private key(s) it is required the intervention of, at least, four members of the Working Groups. Once the key is deactivated, it will remain inactive until an activation process is executed.

6.2.8 Method of Destroying the Private Key

As referred in section 6.2.3, CVCA and DVCA private key must be securely destroyed in an auditable and accountable manner.

SEF destroys private keys in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the private key. SEF uses the zeroization function of its hardware cryptographic modules and other appropriate means to ensure the complete destruction of CA private keys.

6.2.9 Cryptographic Module Rating

See section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Portuguese CVCA is archived as a consequence of the backup operations performed by the Working Group members, assuring that those public keys may be used over time in case of primary's system malfunction.

6.3.2 Certificate Operational Periods

The operational period of a certificate ends when it expires or is revoked.

	Minimum Validity Period	Maximum Validity Period
CVCA Certificate	6(six) months	3 years
DVCA Certificate	2(two) weeks	3 month

6.4 Activation data

Protection of activation data prevents unauthorized use of the private key. Activation data refers to data values other than whole private keys that are required to operate private keys or cryptographic modules containing private keys, such as a PIN, passphrase, or portions of a private key used in a key-splitting scheme.

6.4.1 Activation data generation and installation

The activation data needed to make use of the Portuguese CVCA private key is split into separate parts (stored in role-splitting PED Keys – small, key-shaped digital identification tokens –), which are held by different Working Group members (as referred in section 6.2.2). The separate parts are generated in accordance with the planned and audited Key Generation Process and meet the requirements set by the FIPS 140-1 level 3 cryptographic hardware.

The password required to protect the ECD private key is generated by the FIPS 140-1 level 3 cryptographic hardware and displayed once on the PED (Pin Entry Device). Each time that the ECD private key needs to be activated, the password has to be manually entered on the PED.

6.4.2 Activation data protection

The activation data (separate parts and/or password) will be memorized and stored in tamper-evident tokens or envelopes which are then kept in secure safes.

The Portuguese CVCA private key is kept in encrypted form, stored in hardware cryptographic tokens.

6.4.3 Other aspects of activation data

If activation data for private keys needs to be transmitted, the transmission shall be protected against loss, theft, modification and unauthorized disclosure.

Activation data will be destroyed (by overwriting and/or physical destruction) when the associated private key is erased.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

SEF limits access to Portuguese CVCA production servers to those Working Group members with a valid reason to such access. SEF ensures that the Portuguese CVCA server run off-line, is shut down after each DVCA certificate issuance or other technical intervention and meet the general best practices requirements for identification, authentication, access control, administration, audit, object reuse, accountability, reliability of service and data exchange.

6.5.2 Computer security rating

The Portuguese CVCA hardware cryptographic module satisfies the EAL 4+ assurance requirements of Common Criteria for Information Technology Security Evaluation.

6.6 Life cycle security controls

6.6.1 System development controls

Applications are developed and implemented by third-parties in accordance with their systems development and change management standards. An auditable method is provided to verify that the software on the Portuguese CVCA servers, prior to the first time that it is used, has not been modified. All the configuration and software changes during maintenance are performed by Working Group member using auditable methods.

6.6.2 Security management controls

SEF has mechanisms and/or Working Groups in place to control and monitor the configuration of the CA systems. The SEF CA system, when first started, will be verified to ensure that the software is originated from the software developer and has not been modified prior to installation.

6.6.3 Life cycle security controls

No stipulation

6.7 Network security controls

Portuguese CVCA is not connected to any network.

7 Certificate Profiles

The next table shows the CV Certificate profile

Data Object
CV Certificate
Certificate Body
Certificate Profile Identifier
Certification Authority Reference
Public Key
Certificate Holder Reference
Certificate Holder Authorization Template
Certificate Effective Date
Certificate Expiration Date
Certificate Extensions
Signature

Each of these fields is explained in more detail on TR-03110-v2.01 specification on section C.1.

The next table shows the CV Certificate Request Profile:

Data Object
Authentication
CV Certificate
Certificate Body
Certificate Profile Identifier
Certification Authority Reference

Public Key
Certificate Holder Reference
Certificate Extensions
Signature
Certificate Authority Reference
Signature

Each of these fields is explained in more detail on TR-03110-v2.01 specification on section C.2.

8 Compliance Audit and other Assessments

A regular examination of compliance to this CPS and other rules, procedures and processes will be performed by SEFs Working Group audit members.

In addition to compliance audits, SEF will perform other reviews and investigations to ensure the compliance of the Portuguese CVCA PKI with national laws ([19], [20], [21]). The performance of these audits, reviews and investigations can be delegated to a third party audit firm.

8.1 Frequency or Circumstances of Assessment

Portuguese CVCA audits are performed at least once every three years. These audit are performed by an accredited security auditor.

8.2 Identity/Qualifications of Assessor

Compliance audits or other assessments are performed by personnel with:

- required qualifications as demanded by law [19] (The auditor must be independent from the certification authority, needs to have recognized competency, experience and qualifications proven in the information security area in the performance of security auditory and usage of the ISO/IEC 17799 standard, and needs to have been credentiated by the “*Gabinete Nacional de Segurança*”),
- know-how in public key infrastructure technology, information security tools and techniques,
- security auditing certification by a known certification body.

8.3 Assessor's Relationship to Assessed Entity

Regular examination of compliance will be performed by SEFs Working Group audit members.

When the compliance audits or other assessments are performed by third party auditors, those auditors must be independent of SEF, as demanded by law [19] (The security auditor must guarantee that its team members do not perform partially or discriminatorily and that none of the auditors has worked for the certification authority in the previous 3 years nor have they any other kind of agreement or legal contract with the certification authority.).

8.4 Topics Covered by Assessment

The scope of audits and other assessments include the compliance with national laws ([19], [20], [21]) and with this CPS and other rules, procedures and processes (especially those related to key management operations, facility, management and operational controls, and certificate life cycle management).

8.5 Actions Taken as a Result of Deficiency

Actions taken as a result of deficiencies found during the assessment will be decided by SEF management, with input from the auditor and the Working Group members. SEF management is responsible for:

- approving a corrective action plan developed within 30 days and implemented within a reasonable period of time, in case of significant deficiencies identified,
- determining the course of action, in case of less serious deficiencies.

Audit Working Group has the responsibility of regular audits.

8.6 Communication of Results

Only a Certificate of Conformity issued by the Security Auditor can confirm the compliance with this CP.

If a DV is not compliant with this CP, this DV should notify all CVCA's from which it receive certificates and the CVCA's must not issue certificates for this DVCA.

9 OTHER BUSINESS AND LEGAL MATTERS

This section covers general business and legal matters.

9.1 Fees

No stipulation.

9.2 Financial responsibility

No stipulation.

9.3 Confidentiality of Business Information

No stipulation.

9.4 Privacy of personal information

Fingerprint Biometrics obtained from MRTD's must be deleted after finishing the comparison process with the fingerprint collected by the IS from the bearer.

9.5 Intellectual property rights

All Intellectual Property Rights shall remain vested in the party creating or owning the same and nothing in this CP shall confer or be deemed to confer on any party any rights or licenses of the Intellectual Property Rights of the other party.

CVCA PKI's root public keys and the root Certificates containing them, including all public keys and self-signed Certificates, are the property of SEF. Key pairs corresponding to CVCA Certificates and DVCA Certificates are the property of SEF.

9.6 Representations and warranties

9.6.1 CA representations and warranties

SEF warrants that:

- ✓ There are no material misrepresentation 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 failure to exercise reasonable care in managing the Certificate Application or creating the Certificate;
- ✓ The Certificates meet all material requirements of the CP;
- ✓ Revocation services and use of repository conform to the applicable CPS in all material aspects.

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

SEF warrant that regarding DVCA and IS certificates:

- ✓ Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the CVCA/IS certificate and the Certificate has been accepted and is operational at the time the digital signature is created,
- ✓ The private key is protected and no unauthorized person has ever had access to the DVCA/IS private key,
- ✓ All information contained in the Certificate is true,
- ✓ The Certificate is being used exclusively for authorized and legal purposes, consistent with this CP, and
- ✓ The IS certificate is an end-user certificate and not a CA certificate, and therefore is not using the private key corresponding to any public key listed in the IS Certificate for purposes of digitally signing any Certificate (or any other format of certified public key), as a CA or otherwise.

9.6.4 Relying party representations and warranties

Receiving states agree that:

- ✓ Portuguese CVCA certificates are distributed by strictly secure diplomatic means (out-of-band distribution),
- ✓ They shall access to the EC ask for Certificate information;
- ✓ Only the parties that are provided with the appropriate public key certificates will be able to verify the authenticity and integrity of data signed by the CVCA private key.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

No stipulation.

9.8 Limitations of liability

No stipulation.

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

The CA-related documents (including this CP) become effective as soon as they are approved by the Management Working Group and are only terminated or changed by their ruling.

9.10.2 Termination

The Management Working Group may rule in favor of the termination or amendment of a CA-related document (including this CP) when:

- its contents are considered as incomplete, inaccurate or erroneous,
- its contents have been compromised.

In that case, the terminated document will be replaced by a new version.

9.10.3 Effect of Termination and Survival

After the Management Working Group rules in favor of the termination of a CA-related document, the Policy Working Group has 30 business days to submit a substitute document(s) to the Management Working Group for approval.

9.11 Individual notices and communications with participants

All participants shall use reasonable methods to communicate with each other. Those methods may include digital signed e-mail, fax, signed forms or other, depending of the criticality and subject of the communication.

9.12 Amendments

9.12.1 Procedure for Amendment

In order to amend this document or any of the certificate policies, it's necessary to submit a formal request to the Policy Working Group, stating (at least):

- the requester's identification,
- the request reason,
- the requested amendments.

The Policy Working Group will review the request and, if its pertinence is verified, will proceed to the necessary document updates, resulting in a new draft version of the document. The new draft document is then made available to all Working Group members and to affected parties (if any) to enable its scrutiny. Counting from the availability date, the different parties have 15 business days to submit their comments. When that period ends, the Policy Working Group has another 15 business days to analyze all the received comments and, if relevant, incorporate them on the document, after which the document is approved submitted to the Management Working Group for publishing, by which amendments become final and effective.

9.12.2 Circumstances under which OID must be changed

The Policy Working Group shall determine whether changes to the CPS require a change in the Certificate policy OID or the CPS pointer URL of the Certificate policies.

9.13 Dispute resolution provisions

All disputes will be resolved by SEF management.

9.14 Governing law

This CP shall be governed by the laws of Portugal.

9.15 Compliance with applicable law

This CP is subject to applicable national, European laws, rules, regulations, ordinances, decrees and orders including, but not limited to, restrictions on exporting or importing software, hardware or technical information

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

No stipulation.

Bibliography

- [1] Technical Report – PKI for Machine Readable Travel Document offering ICC read-only access, release 1.1, 01 October 2004, ICAO
- [2] Common Certificate Policy for the Extended Access Control Infrastructure for Passports and Travel Documents issued by EU Members States (V 1.0)
- [3] TR-03110 specification (v 2.001) – Advanced Security Mechanisms for Machine Readable Travel Documents
- [4] RFC 3280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- [5] ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework, June 1997.
- [6] RFC 3279 – Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- [7] ISO/IEC 3166 – Codes for the representation of names and countries and their subdivisions, 1997
- [8] RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework
- [9] RFC 3280 - Internet X.509 PKI - Certificate and CRL Profile
- [10] ECN PEP Policies – Certificate Policies
- [11] FIPS 140-1: Security Requirements for Cryptographic Modules, January 4, 1994.
- [12] Portuguese law, “Decreto Regulamentar n.º 25/2004, de 15 de Julho”
- [13] Portuguese law, “Decreto-Lei n.º 290-D/99, de 2 de Agosto”
- [14] Portuguese law, “Decreto-Lei n.º 62/2003, de 3 de Abril”

ⁱ Country Verifying Certification Authority
ⁱⁱ Document Verifying
ⁱⁱⁱ Inspection System
^{iv} Machine Readable Travel Document