EUROPEAN COMMISSION
DIRECTORATE-GENERAL
PERSONNEL AND ADMINISTRATION
Directorate SPS - Protocol and Security Service
Informatics Security

European Commission

CERTIFICATE PRACTICE STATEMENT

(Version 1.0 dated 25/02/2002)

Bâtiment Jean Monnet, Rue Alcide de Gasperi, L-2920 Luxembourg. Telephone: (352)43011.

Rue de la Loi 200, B-1049 Bruxelles / Wetstraat 200, B-1049 Brussel - Belgium. Telephone: (32-2)299 11 11.

Table of Content

(Version 1.0 dated 25/02/2002) 1
1. INTRODUCTION 8
1.1. Overview 8
1.2. Identification 9
1.3. Community and Applicability 9
1.3.1. Certification Authority (CA) 10
1.3.2. Registration Authorities (RAs) 11
1.3.3. Repositories 11
1.3.4. Subscribers 11
1.3.5. Relying Parties 12
1.3.6. Applicability 12
1.4. Contact Details 13
2. GENERAL PROVISIONS 13
2.1. Obligations 13
2.1.1. CA Obligations 13
2.1.2. RA and LRA Obligations 14
2.1.3. Subscriber Obligations 15
2.1.4. Relying Party Obligations 16
2.1.5. Repository Obligations 17
2.2. Liability [To be reviewed by Legal Service] 17
2.2.1. Warranties And Limitations On Warranties 17
2.2.2. Disclaimers And Limitations Of Liability 18
2.2.3. Other Terms And Conditions 18
2.3. Financial Responsibility 19
2.3.1. Indemnification By Relying Parties 19
2.3.2. Fiduciary Relationships 19
2.4. Interpretation and Enforcement 19
2.4.1. Governing Law 19
2.4.2. Severability, Survival, Merger, Notice 19
2.4.3. Dispute Resolution Procedures 19
2.5. Fees 19
2.6. Publication and Repository 19
2.6.1. Publication of CA Information 19
2.6.2. Frequency Of Publication 20

2.6.3. Access Controls 20
2.6.4. Repositories 20
2.7. Compliance audit [To be implemented] [to be reviewed when implemented] 21
2.7.1. Frequency Of Compliance Audit 21
2.7.2. Identity/qualifications Of CA Auditor 21
2.7.3. Auditor's Relationship To Audited CA 21
2.7.4. Topics Covered By Audit 22
2.7.5. Actions Taken As A Result Of Audit 22
2.7.6. Communication Of Results 22
2.8. Confidentiality Policy 23
2.8.1. Types Of Information Not To Be Disclosed 23
2.8.2. Types Of Information Which Are Considered Public 24
2.8.3. Disclosure Of Certificate Revocation Information 24
2.8.4. Release To Law Enforcement Officials 24
2.8.5. Other Information Release Circumstances 24
2.9. Intellectual Property Rights 24
3. IDENTIFICATION AND AUTHENTICATION 25
3.1. Initial Registration 25
3.1.1. Types Of Names 25
3.1.2. Need For Names To Be Meaningful 25
3.1.3. Rules For Interpreting Various Name Forms 25
3.1.4. Uniqueness Of Names 25
3.1.5. Name Claim Dispute Resolution Procedure 25
3.1.6. Recognition, Authentication And Roles Of Trademarks 26
3.1.7. Method To Prove Possession Of Private Key 26
3.1.8. Authentication Of Organisation Identity 26
3.1.9. Authentication Of Individual Identity 26
3.1.10. Authentication of Subscriber's Affiliation: 27
3.1.11. Authentication of Subscriber's Identity: 27
3.1.12. Authentication Of Devices Or Applications 27
3.2. Routine Rekey 27
3.3. Rekey After Revocation 27
3.4. Revocation Request 27
4. OPERATIONAL REQUIREMENTS 28
4.1. Certificate Application 28

4.2. Certificate Issuance 28
4.3. Certificate Acceptance 30
4.4. Certificate Suspension and Revocation 31
4.4.1. Circumstances For Revocation 31
4.4.2. Who Can Request Revocation 31
4.4.3. Procedure For Revocation Request [To be implemented] [To be reviewed when implemented] 31
4.4.4. Revocation Request Grace Period 32
4.4.5. Circumstances For Suspension 32
4.4.6. Who Can Request Suspension 32
4.4.7. Procedure For Suspension Request 32
4.4.8. Limits On Suspension Period 32
4.4.9. CRL Issuance Frequency 33
4.4.10. CRL Checking Requirements 33
4.4.11. On-line Revocation/status Checking Availability 33
4.4.12. On-line Revocation Checking Requirements 33
4.4.13. Other Forms Of Revocation Advertisements Available 33
4.4.14. Checking Requirements For Other Forms Of Revocation Advertisements 33
4.4.15. Special Requirements Key Compromise 33
4.5. Security Audit Procedures [To be implemented] [To be reviewed when implemented] 34
4.5.1. Types Of Event Recorded 34
4.5.2. Frequency Of Audit Log Processing 34
4.5.3. Retention Period For Audit Log 35
4.5.4. Protection Of Audit Log 35
4.5.5. Audit Log Backup Procedures 35
4.5.6. Audit Collection System 35
4.5.7. Notification To Event Causing Subject 35
4.5.8. Vulnerability Assessments 35
4.6. Records Archival [To be implemented] [To be reviewed when implemented] 35
4.6.1. Types Of Data Archived 35
4.6.2. Retention Period For Archive 36
4.6.3. Protection Of Archive 36
4.6.4. Archive Backup Procedures 37
4.6.5. Archive Collection System 37

4.6.6. Procedures To Obtain And Verify Archive Information 37
4.7. Key Changeover 37
4.8. Compromise and Disaster Recovery [To be implemented] [To be review when implemented] 37
4.8.1. Computing Resources, Software, And/or Data Are Corrupted 37
4.8.2. Entity Key Recovery 38
4.8.3. Disaster Recovery 40
4.9. CA Termination 40
5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS 40
5.1. Physical Security Controls 40
5.1.1. Site Location And Construction 40
5.1.2. Physical Access 41
5.1.3. Power And Air Conditioning 41
5.1.4. Water Exposures 41
5.1.5. Fire Prevention And Protection 41
5.1.6. Media Storage 41
5.1.7. Waste Disposal 41
5.1.8. Off-site Backup [Not applicable] 41
5.2. Procedural Controls 42
5.2.1. Trusted Roles 42
5.2.2. Number Of Persons Required Per Task 43
5.2.3. Identification & Authentication For Each Role 44
5.3. Personnel Security Controls 44
5.3.1. Background, Qualifications, Experience, and Clearance Requirements 44
5.3.2. Background Check Procedures 44
5.3.3. Training Requirements 44
5.3.4. Retraining Frequency And Requirements 44
5.3.5. Job Rotation 44
5.3.6. Sanctions For Unauthorised Actions 44
5.3.7. Contracting Personnel 45
5.3.8. Documentation Supplied To Personnel 45
6. TECHNICAL SECURITY CONTROLS 45
6.1. Key Pair Generation and Installation 45
6.1.1. Key Pair Generation 45
6.1.2. Private Key Delivery To Entity 45

6.1.3. Public Key Delivery To Certificate Issuer 45
6.1.4. CA Public Key Delivery To Users 45
6.1.5. Asymmetric Key Sizes 46
6.1.6. Public Key Parameters Generation 46
6.1.7. Parameter Quality Checking 46
6.1.8. Hardware/software Key Generation 46
6.1.9. Key Usage Purposes (as per X.509v3 field) 46
6.2. Private Key Protection 46
6.2.1. Standards For Crypto-module 46
6.2.2. Private Key Multi-person Control 46
6.2.3. Private Key Escrow 47
6.2.4. Private Key Backup 47
6.2.5. Private Key Archival 47
6.2.6. Private Key Entry Into Cryptographic Module 47
6.2.7. Method Of Activating Private Key 47
6.2.8. Method Of Deactivating Private Key 47
6.2.9. Method Of Destroying Private Key 47
6.3. Other Aspects of Key Pair Management 47
6.3.1. Public Key Archival 47
6.3.2. Usage Periods For The Public And Private Keys 47
6.4. Activation Data 48
6.4.1. Activation Data Generation And Installation 48
6.4.2. Activation Data Protection 48
6.4.3. Other Aspects Of Activation Data 48
6.5. Computer Security Controls 48
6.5.1. Specific Computer Security Technical Requirements 48
6.5.2. Computer Security Rating 49
6.6. Life Cycle Security Controls 49
6.6.1. System Development Controls 49
6.6.2. Security Management Controls 49
6.7. Network Security Controls 49
6.8. Cryptographic Module Engineering Controls 49
7. CERTIFICATE AND CRL PROFILE 50
7.1. Certificate Profile 50
7.1.1. Version Number 50
7.1.2. Certificate Extensions 50

7.1.3. Algorithm Object IDs 50
7.1.4. Name Forms 51
7.1.5. Name Constraints 51
7.1.6. Certificate Policy Object Identifier 51
7.1.7. Usage Of Policy Constraints Extension 51
7.1.8. Policy Qualifiers Syntax And Semantics 51
7.1.9. Processing Semantics For The Critical Certificate Policy 51
7.2. CRL Profile [To be reviewed when implemented] 51
7.2.1. Version Number 51
7.2.2. CRL and CRL Entry Extensions 52
8. SPECIFICATION ADMINISTRATION 53
8.1. Specification change procedures 53
8.1.1. Items That Can Change Without Notification 53
8.1.2. Changes With Notification 53
8.2. Publication and notification policies 54
8.3. CPS approval procedures 54
9. ANNEXES 55
9.1. Acronyms 55
9.2. Definitions 55
9.3. Reference Documents 58

1. INTRODUCTION

The general outline of this document is based on RFC 2527 that contains a comprehensive analysis of the subject.

The framework issued from the document RFC 2527 provides a comprehensive list of topics that need to be covered in a certification practice statement.

The following conventions meaning:

- Normal font: implemented and operational,
- Italic font: not yet implemented, for future developments,
- Text between square brackets: to be discussed

The European Commission is implementing a Public Key Infrastructure (PKI) to provide security for its electronic information. This PKI consists of systems, products and services, which provide and manage X.509 certificates for public-key cryptography.

It is the purpose of this document to describe the certification practices that have been implemented by the European Commission Certification Authority (CA) – named CommisSign -to ensure the CA's trustworthiness in issuing public key certificates to subscribers. This document has been drafted to comply with the requirements of the Certificate Policy (CP) for the European Public Key Infrastructure (PKI). The relationship between the European Commission PKI CP and this document is the CP states the policies of the CommisSign CA and this document provides the implementation details of the CP.

Users of this document should consult the Certificate Policy (CP) for the European Commission Public Key Infrastructure (PKI) to obtain information concerning the underlying policies for the CommisSign CA Certificate Practice Statement (CPS).

1.1. Overview

This practice statement specification follows and complies with the Internet Engineering Task Force Public Key Infrastructure X.509 (IETF PKIX) Part 4 Certificate Policy and Certification Practice Statement Framework.

This document is intended for use by the European Commission and others who need to assess the trustworthiness of the CommisSign CA and determine the suitability of its certificates in meeting their requirements for electronic information security.

The practices in this document support medium assurance, unless specified otherwise. As European Commission adds other assurance levels, this document will be modified to describe the practices for these levels.

The CommisSign CA Certificate Practice Statement (CPS) describes the creation, management and use of Version 3 X.509 public-key certificates in applications requiring communication between networked computer-based systems and applications requiring electronic information integrity and

confidentiality. Such applications include, but are not limited to, electronic mail; transmission of up to and including EU restricted information; digital signature of electronic forms. Please note, the term, "X.509 certificates", as used within this document implies X.509 version 3 certificates. Also note, the term, "PKI client software" or "PKI software" refers to the software that provides PKI functionality within the CommisSign CA domain.

Issuance of a public key certificate under any of this CPS

- is not to be used for protection of EU Confidential, EU Secret and EU Top Secret information,

- does not imply that the subscriber has any authority to conduct business transactions on behalf of the European Commission.

The European Commission PKI Policy Authority evaluates this CPS. The Policy Authority (PA) approves all CPS's of CA's within the European Commission PKI.

Concerning the enforceability, construction, interpretation and validity of this Certificate Practice Statement and the associated Certificate Policy, the CommisSign CA will be governed by European Commission regulations

The European Commission Policy Authority is responsible for the overall management of the European Commission PKI. The PA is responsible for defining the policies under which the European Commission PKI operates. The PA duties include ensuring that CommisSign CA's operate in accordance with policies and practices defined in relevant Certification and Certificate documents, and approving and administering cross certifications. The PA is vested in the European Commission College.

The European Commission Certificate Authority (CA) is responsible for the creation and management of Version 3 X.509 public-key certificates for use by European Commission and in accordance with the European Commission CP and this CPS.

The European Commission uses Central Registration Authority (RA) and Local Registration Authority (LRA) to collect information, verify identity and authorise, and request certificate management actions on behalf of their user population.

1.2. Identification

This document is the European Commission Certification Authority Certification Practice Statement (CPS). The practices stated herein conform to the Security Policy for the European Commission Public Key Infrastructure (PKI).

1.3. Community and Applicability

This CPS has been designed to satisfy general public key certificate requirements of the European Commission

The CommisSign CA is a Certification Authority within the European Commission PKI.

1.3.1. Certification Authority (CA)

The CommisSign CA is intended for use within the European Commission and potentially with organisations or individuals that are outside of the European Commission but exchange emails with the European Commission.

The CommisSign CA issues, signs and manages public key certificates. The CA issues user certificates to all Commission Staff excluding any other persons on an as-needed basis.

The CommisSign CA includes people who are responsible for the overall operation of the CA and people who operate and maintain the CA server and the CA software. The CA Operation Authority (OA) is responsible for the establishment and administration of the CA Practice Statement and management of Master key. The OA is responsible for reviewing the operations of the RAs within its CA domain. The OA reports to the PA regarding issues of CA operation.

The CA Officers are responsible for the operation and administration of the CA server and CA software.

The CommisSign CA is responsible for:

- creating and signing of X.509 certificates binding subscribers belonging to Commission Staff with their public keys;
- disseminating X.509 certificates through Directories;
- promulgating certificate status through CRL's; [not operational]
- operating the CA in accordance with this CPS;
- approving and assigning individuals to fulfil PKI Officer positions;
- reviewing and auditing RA and LRA operations within its domain;
- resolving disputes between end users and the CA , RA or LRA;
- requesting revocation of PKI Officer’s or RAs' certificate.

When necessary, this CPS distinguishes the different users and roles accessing the CA functions. When this distinction is not required, the term CA is used to refer to the total CA entity, including the software and its operations.

(* Please note: a cross certification shall be in accordance with this CPS and any additional requirements determined by the European Commission Policy Authority (PA). All cross certification between the Commission Users and other CAs will be done pursuant to instructions from the Commission PA.

Any acknowledgement made with other CAs shall be documented and applicable disclaimers made available to Commission Users.)

1.3.2. Registration Authorities (RAs)

A Registration Authority (RA) is an entity that is responsible of the End Entity administration on behalf of the Commission CA. There are one Central Registration Authority (RA) and several Local Registration Authorities (LRA).

The terms RA/LRA are used to refer to an individual within the European Commission with RA/LRA privileges who performs the RA/LRA functions.

The **RA** is responsible for:

- identifying and authenticating the administrative identity of certificate applicants;
- creating and changing user's SubjectName on the certificate
- viewing audit logs and reporting suspicious events to the CA Operation Authority; and
- creating various reports of user status.

The **LRA** is responsible for:

- identifying and authenticating the physical identity of certificate applicants;
- verifying the authenticity of the request for a certificate;
- verifying user's SubjectName;
- receiving and distributing subscriber authorisation information;
- performing certificate and management functions for their end entity population (i.e. enabling users, disabling/suspending user certificates),
- updating certificates, [*revoking certificates* and] managing key recovery for end-entities

1.3.3. Repositories

The CommisSign CA uses the European Commission Directory to publish and distribute certificates, Certificate Revocation Lists (CRLs) [and Authority Revocation Lists (ARL's)]. The Informatic Directorate manages the European Commission Directory. The Directory is available 24 hours a day with operational support available 12 hours a day, 5 days a week.

1.3.4. Subscribers

Subscribers use private keys [issued and/or] certified by the CommisSign CA for approved applications. Subscribers belong to the Commission Staff.

A certificate may be issued to a functional mail box. In this case, the person who is responsible for this non-human end entity needs to apply and maintain a certificate for this entity. This person can delegate its rights to a second person (as a backup person).

In addition, subscribers may use certificates issued by the CommisSign CA to encrypt information for, and verify the digital signatures of, other subscribers (within the CommisSign CA domain as well as cross-certified domains). As such, subscribers are also relying parties.

In this CPS, the term end entity is used to represent users in general including their roles as subscribers and relying parties. Where separation of these roles is required in this CPS, the term Subscriber is used to refer to an end entity as a certificate subject, while Relying Party is used to refer to an end entity verifying certificates issued by the CommisSign CA.

1.3.5. Relying Parties

A Relying Party may be either a certificate subject of the CommisSign CA or a subscriber of an external CA that has [signed a cross certification agreement with] trusted the CommisSign CA. The rights and obligations of a relying party who is a certificate subject of the CommisSign CA are covered in this CPS. [The rights and obligations of a relying party belonging to an external CA are covered by the cross certification agreement between the two owners of the CA's].

1.3.6. Applicability

The practices described in this CPS apply to the CommisSign CA and its administrators, the European Commission RAs and their administrators, the repository used by the CommisSign CA, to end entities certified by the CommisSign CA, and to relying parties.

The practices in this CPS are suitable for certificate uses such as electronic authentication, authorisation and data integrity for the European Commission information up to and including Critical information systems (see ICT Security Policy).

The practices in this CPS are suitable for certificate uses such as confidentiality for the European Commission information up to and including EU Restricted (see ICT Security Policy).

Prohibited applications shall be those identified by the European Commission PA. In general term applications for which issued certificates are prohibited, are:

- applications that use or contain EU Confidential, EU Secret and EU Top Secret information,

- applications that have no relevance to the work of the Commission.

1.4. Contact Details

The Protocol and Security Service of the European Commission administer this certification practice statement.

The contact person is:

Mr Gérard BREMAUD

CommisSign CA Operations Authority

Protocol and Security Service

Jean-Monnet Building B2/072

L-2920 LUXEMBOURG

2. GENERAL PROVISIONS

2.1. Obligations

2.1.1. CA Obligations

The CommisSign CA will comply with the provisions in the ICT Security Policy, all provisions in this CPS, and relevant European and national regulations.

The **CommisSign CA** is obliged to:

- establish, maintain and publish a Certificate Practice Statement;
- provide CA services in accordance with the practices described in this CPS;
- provide CA server services 7 days a week, 24 hours per day with the stipulation that this is not a warranty of 100% availability (availability may be affected by system maintenance, system repair, or by factors outside the control of the CA);
- issue certificates to the European Commission Staff [and to other CA's], in accordance with the practices referenced in this CPS and the X.509 Certificate Policy for the European Commission PKI;
- revoke certificates upon receipt of a valid request to do so, in accordance with the practices this CPS and the X.509 Certificate Policy for the European Commission PKI;
- provide encryption key recovery services, in accordance with the practices this CPS and the X.509 Certificate Policy for the European Commission PKI;
- issue and publish CRL's[and ARL's] on a regular schedule as per this CPS and the X.509 Certificate Policy for the European Commission PKI;

- notify others (e.g. relying parties) of certificate issuance/revocation by provision of access to certificates, CRL's, [and ARL's] in the CommisSign CA repository;

- ensure awareness of and adherence to this CPS within the CommisSign CA's subscriber and RA communities through publication of the CPS and X.509 Certificate Policy for the European Commission PKI and audit of RA's within the CommisSign CA domain;

- ensure ,in concert with the European Commission PA, corrective actions to CA or RA deficiencies identified by an audit;

- report status of corrective actions to the PA.

Upon creation, a subscriber's certificate is published in the European Commission Directory. When a subscriber's certificate is revoked it is published in written to the Certificate Revocation List and published in the European Commission Directory.

By publishing a certificate in the European Commission Directory, the CommisSign CA certifies it has issued a certificate to the named subscriber; and that the information stated in the certificate was verified in accordance with this CPS; and the subscriber has accepted the certificate.

The CommisSign CA provides notification of a subscriber's and relying party's rights and obligations under this CPS through the publication of this CPS and the X.509 Certificate Policy for the European Commission PKI.

The CommisSign CA protects its private keys in accordance with the provision of Section 6 of this CPS.

[The CommisSign CA protects the private keys it holds or stores in accordance with Sections 4 and 6 of this CPS] .

The CommisSign CA's signing key is used for signing certificates, and CRLs.

[The CommisSign CA may issue and sign cross certificates with other CA's only as expressly authorised by the European Commission PA].

2.1.2. RA and LRA Obligations

The European Commission RA and LRA's within the CommisSign CA domain are obligated to conform to the stipulations of this CPS and the X.509 Certificate Policy for the European Commission PKI.

The **RA** is obliged to:

- provide RA services to their respective LRA's. Hours of operation for the RA are the normal working hours of the Commission;

- ensure the RA services are in accordance with the stipulation of the relevant practices of this document and the X.509 Certificate Policy for the European Commission PKI;

- be accountable for transactions performed on behalf of the CA;

- bring to the attention of their subscribers all relevant information pertaining to the rights and obligations of the CA, RA and Subscriber contained in this CPS, the Subscriber Agreement, and any other relevant document outlining the terms and conditions of use.

When the RA logons to the CA server to process a certificate request, the RA is certifying that it has authenticated the identity of that subscriber in accordance with the practices described in Sections 3 and 4 of this CPS.

The **LRA's** are obliged to:

- verify the accuracy and authenticity of the information provided by subscribers for a certificate(the LRA's provide this verification on behalf of the CommisSign CA),

- request revocation of a subscriber’s certificates in accordance with the stipulations in this document],

- ensure the LRA services are in accordance with the stipulation of the relevant practices of this document and the X.509 Certificate Policy for the European Commission PKI,

- be accountable for transactions performed on behalf of the CA,

- be responsible for processing requests for certificate issuance [*and revocation]*,

- notify the subscriber when the request has been approved and if any subsequent action is required by the subscriber.

Each RA and LRA must ensure that his or her private keys are protected in accordance with the controls described in Section 6 of this CPS.

RA and LRA use of their private keys are restricted to the work of the European Commission and only for purposes authorised by the X.509 Certificate Policy for the European Commission PKI and in conformance with this CPS.

2.1.3. Subscriber Obligations

In the CommisSign CA domain, end entities are both subscribers and relying parties. As subscribers, they are obliged to:

- make true representation at all times to both the CommisSign CA and RA regarding information in their certificates and other identification and authentication information,

- use certificates exclusively for legal and authorised work of the European Commission, consistent with the applicable certificate policy and this CPS,

- protect private keys by storing them either on a hard disk, [on a smart card] or on a diskette depending on DG implementation,

- remove the private key support from the computer when not in use If private keys are stored on a diskette[or on a smart card],

- keep the private key support on their person or to store it in a secure, locked container If private keys are stored on a diskette[or on a smart card],

- protect their subscriber password, according to ICT security rules;

- inform their local RA within 48 hours of a change to any information included in their certificate or certificate application request;

- inform their local RA within 8 hours of a suspected compromise of one/both of their private keys,

- take reasonable precautions to prevent loss, disclosure, modification, or unauthorised use of their private keys.

By adhering to the practices described in this CPS, subscribers fulfil the obligations imposed upon them by the policies under which their certificates are issued.

[By signing a certificate request (i.e. issuance, revocation, recovery), a subscriber certifies to the CommisSign CA and RA that any information submitted to the CA or RA is complete and accurate.]

Subscribers use of their private keys are restricted to the work of the European Commission and only for purposes authorised by the Security Policy for the European Commission PKI and in conformance with this CPS.

2.1.4. Relying Party Obligations

In the CommisSign CA domain, end entities are both subscribers and relying parties. As relying parties, they are obliged to:

- restrict reliance on certificates issued by the CommisSign CA to appropriate uses for those certificates, in accordance with the X.509 Certificate Policy for the European Commission PKI and in accordance with this CPS;

- verify certificates, including use of *CRL's[and ARL's]*, [taking into account any critical extensions]. [(Verification of certificates is in accordance with the certification path validation procedure specified in ITU-T Recommendation X.509 Information Technology – Open Systems Interconnection – The Directory: Authentication Framework ISO/IEC 9594-8 (1997)).]

- trust and make use of certificates only if a valid certificate chain is established between the relying party and the certificate subject.

Prior to using a subscriber's certificate, a relying party must ensure that it is appropriate for the intended use by familiarising themselves with the policy and CPS under which the certificate was issued.

Relying parties are responsible for validating the CommisSign CA signature, and expiry date on a certificate prior to using the associated public key. In addition the relying party is responsible for verifying the subscribers digital signature prior to accepting digitally signed data. Where verification is performed automatically by a cryptographic process and supporting hardware/software installed on the relying parties' workstation, relying parties should ensure that they are using compatible software.

Prior to using a certificate, relying parties are required to check the certificate status against a current CRL. The relying parting must verify the digital signature of the CRL to ensure that it was signed by the CommisSign CA.

2.1.5. Repository Obligations

[CommisSign Root Certificates, CPS, CRL's [and Subscribers Certificates] are available to Relying Parties in accordance with practices described in Section 4.4. 'CRL Issuance Frequency' of this CPS.]

2.2. Liability [To be reviewed by Legal Service]

[As the CommisSign CA and RA functions are provided by the European Commission, the liabilities related to both functions are combined in this CPS.

The CommisSign CA, RA and LRA and the European Commission assume no liability whatsoever in relation to the use of the European Commission PKI certificates or associated public/private key pairs for any use other than the uses described in the Certificate Policy for the European Commission PKI and this CPS.

2.2.1. Warranties And Limitations On Warranties

The CommisSign CA and RA warrant and promise to:

- provide certification services consistent with the certificate policy identified in the X.509 Certificate Policy for the European Commission PKI and this CPS;

- perform the identification and authentication procedures as set forth in Section 3 of this CPS;

- provide key management services including certificate issuance, publication, revocation, key recovery and update in accordance with the certificate policy identified in the X.509 Certificate Policy for the European Commission PKI and this CPS.

The European Commission, its staff make no representations, warranties or conditions, express or implied, other than as expressly stated in identified in the Certificate Policy for the European Commission PKI and this CPS.

2.2.2. Disclaimers And Limitations Of Liability

The European Commission, the CommisSign CA and RAs are not liable for any loss:

- of CA or RA service due to war, natural disasters or other uncontrollable forces;
- incurred between the time a certificate is revoked and the next scheduled issuance of a CRL;
- due to unauthorised use of certificates issued by the CommisSign CA, and use of certificates beyond the prescribed use defined by the X.509 Certificate Policy for the European Commission PKI and this CPS;
- caused by fraudulent or negligent use of certificates and/or CRL's [and/or ARL's] issued by the CommisSign CA;
- due to disclosure of personal information contained within certificates and revocation lists.

The CommisSign CA and RAs disclaim all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided (except that it came from an authorised source), and further disclaim any and all liability for negligence and lack of reasonable care on the parts of subscribers and relying parties.

The European Commission, the CommisSign CA, the RA and LRA's, disclaims any liability of any kind whatsoever for any award, damages or other claim or obligation of any kind arising from tort, contract or any other reason with respect to any service associated with the issuance, use of, or reliance upon, the European Commission PKI certificate or its associated public/private key pair used by a subscriber or relying party.

Requesters and relying parties are not eligible for compensation claims for losses resulting from inappropriate or fraudulent use of this PKI.

In addition, the CommisSign CA and RAs are not an intermediary to transactions between subscribers and relying parties. Claims against the CommisSign CA and/or RA are limited to showing that a CA or RA operated in a manner inconsistent with X.509 Certificate Policy for the European Commission PKI and this CPS.]

2.2.3. Other Terms And Conditions

No stipulation.]

2.3. Financial Responsibility

2.3.1. Indemnification By Relying Parties

No stipulation.

2.3.2. Fiduciary Relationships

Issuance of certificates by the CommisSign CA and assistance in that issuance by the European Commission RA does not make the European Commission or its CA or RA an agent, fiduciary, trustee, or other representative of requesters or relying parties, or others using the European Commission PKI responsible.

2.4. Interpretation and Enforcement

2.4.1. Governing Law

European and national regulations shall govern the enforceability, construction, interpretation, and validity of this CPS.

2.4.2. Severability, Survival, Merger, Notice

Severance or merger may result in changes to the scope, management and/or operation of the CommisSign CA. In such an event, the X.509 Certificate Policy for the European Commission PKI and this CPS may require modification as well. Changes to the operations will occur consistent with the administrative requirements stipulated in Section 8 of this CPS.

2.4.3. Dispute Resolution Procedures

Any dispute related to key and certificate management between the European Commission and an organisation or individual outside of the European Commission shall be resolved using an appropriate dispute settlement mechanism. The dispute shall be resolved by negotiation if possible. A dispute not settled by negotiation should be resolved through arbitration by the European Commission PA.

Within the CommisSign CA domain, disputes between the European Commission users, one of which acts in the role of a subscriber and the other which acts in the role of a relying party, or between the European Commission users and the CA or RA, shall initially be reported to the CommisSign CA OA for resolution.

2.5. Fees

No stipulation.

2.6. Publication and Repository

2.6.1. Publication of CA Information

The CommisSign CA publishes the following:

- *the CommiSign root certificates on a web site;*

- *copies of [the ICT Security Policy for the European Commission and] this CPS on a web site;*

- *all public key certificates issued by the CommisSign CA in the European Commission Directory,*

- *the most recent CRL of user public key certificates that have been revoked by the CommisSign CA in the European Commission Directory and on a WEB site,*

- *[the most recent ARL of the external Certification Authority that have been revoked by the Commission Policy Authority are published in the European Commission Directory],*

2.6.2. Frequency Of Publication

Once activated, certificates issued by the CommisSign CA are posted once a day to the European Commission Directory. When certificates are revoked they are written in CRL's which are published in accordance with section 4.4. 'CRL Issuance Frequency' of this CPS. [When cross certificates are revoked they are written in ARL's that are published in accordance with section 4.4. 'CRL Issuance Frequency' of this CPS.]

2.6.3. Access Controls

The CommisSign CA CPS and the Certificate Policy for the European Commission have read-only access and are available via the web site. Only CommisSign CA personnel have write or modify access on these documents.

[Certificates and CRL's are available via the European Commission Directory and are read-only. Only the CommisSign CA had read/write and delete privileges.]

2.6.4. Repositories

The repository for certificates, CRLs [and ARL's] issued by the CommisSign CA is provided by the European Commission Directory system. [The protocol used to access the directory is the Lightweight Directory Access Protocol (LDAP) version 2, as specified in Request for Comment (RFC) 1777 Lightweight Directory Access Protocol (1995). LDAP version 2 is used over TCP transport, as defined in Section 3.1 of RFC 1777.]

[When conveyed in LDAP requests and results, attributes defined in X.500 are encoded using string representations defined in RFC 1778 the String Representation of Standard Attribute Syntaxes (1995). These string encoding were based on the attribute definitions from X.500 (1988). Thus, the string representations of the following are for version 1 certificates and version 1 revocation lists:

- userCertificate (RFC 1778 Section 2.25)

- CACertificate (RFC 1778 Section 2.26)
- authorityRevocationList, (RFC 1778 Section 2.27)
- certificateRevocationList, (RFC 1778 Section 2.28)
- crossCertificatePair, (RFC 1778 Section 2.29)

Since this CPS uses version 3 certificates and version 2 revocation lists, as defined in X.509, the RFC 1778 string encoding of these attributes is inappropriate. For this reason, these attributes are encoded using a syntax similar to the syntax Undefined from Section 2.1 of RFC 1778: values of these attributes are encoded as if they were values of type OCTET STRING, with the string value of the encoding being the DER-encoding of the value itself.]

The repository for this CPS and the Certificate Policy for the European Commission is a web site that is accessible from [TBD – URL to be assigned]

2.7. Compliance audit [To be implemented] [to be reviewed when implemented]

2.7.1. Frequency Of Compliance Audit

A full and formal audit on the CommisSign CA operation is performed annually.

The PA may order a compliance audit by an auditor at any time at its discretion.

The CommisSign CA reserves the right to require periodic and a periodic inspections and audits of any RA facility within the CommisSign CA's domain to validate that the RA is operating in accordance with the security practices and procedures laid out in this CPS.

2.7.2. Identity/qualifications Of CA Auditor

The PA must approve any person or entity seeking to perform a compliance audit. The auditor must perform CA or Information System Security Audits as its primary responsibility, demonstrate significant experience with PKI and cryptographic technologies as well as the operation of relevant PKI software and familiarity with the European Commission policies and regulations.

2.7.3. Auditor's Relationship To Audited CA

The auditor approved by the PA and the CommisSign CA are separate entities within the European Commission organisational structure

2.7.4. Topics Covered By Audit

The subjects of the compliance audit are the CommisSign CA and RA implementation of those technical, procedural and personnel practices described in this CPS. Some areas of focus for the audit are:

- identification and authentication,
- operational functions/services,
- physical, procedural and personnel security controls,
- technical security controls.

2.7.5. Actions Taken As A Result Of Audit

There are three possible actions to be taken, should a deficiency be identified:

(1) continue to operate as usual,

(2) continue to operate but at a lower assurance level,

(3) suspend operation.

If a deficiency is identified, the auditor, with input from the European Commission PA, determines which of these actions to take. The decision regarding which of these actions to take will be based on the severity of the irregularities, the risks imposed, and the disruption to the certificate using community.

If Action 1 or 2 is taken, the European Commission PA and the OA are responsible for ensuring that corrective actions are taken within 30 days. At that time, or earlier if approved by the PA and auditor, the audit team shall reassess. If, upon reassessment, corrective actions have not been taken, the auditor determines if more severe action (e.g. Action 3) is required.

If Action 3 is taken, all certificates issued by the CommisSign CA, including end entity certificates and CA cross certificates, are revoked prior to the suspension of the service.

The European Commission PA and the European Commission CA OA are responsible for reporting the status of any corrective action to the auditor on a weekly basis. The PA and auditor together determine when the reassessment is to occur. If the deficiencies are deemed to be corrected upon reassessment, the CommisSign CA shall resume service and new certificates are issued to end entities and other external CAs, depending on conditions specified in individual cross certification agreements.]

2.7.6. Communication Of Results

Results of the annual audit are provided to the European Commission PA, the CommisSign CA and each European Commission LRA IT Security Manager. In the case of Action 2, the European Commission PA, with

assistance from the auditor, determines if subscribers need to be informed of the action. In the case of Action 3, the European Commission PA ensures that all users are informed of the action. Communication with the purpose of informing subscribers of any deficiency and action is performed via e-mail when possible. If a subscriber does not have e-mail access, then a memo is delivered through the European Commission mail service.

The method and detail of notification of audit results to CAs cross certified with the CommisSign CA shall be defined within the cross certification agreement between the two parties. Unless specified in a particular cross certification agreement, no communication of the audit results shall occur outside the European Commission.

2.8. Confidentiality Policy

All information that is not considered by the European Commission PA to be public domain information is kept confidential.

2.8.1. Types Of Information Not To Be Disclosed

Each subscriber's private signing key is classified as restricted to that subscriber. The CommisSign CA and central RA have no access to these keys.

Each subscriber's confidentiality private key is classified as restricted to that subscriber.

On a temporary basis, only one set of public/private key is available and is related to the 'Confidentiality Private Key'. Anything that concerns a signing key is not applicable. However, confidentiality private keys are backed-up by the local LRA and are protected in accordance with Section 6 of this CPS.

Information held in audit trails is considered restricted to the European Commission and shall not be released outside the institution, unless required by law or regulations.

Collection of personal information may be subject to collection, maintenance, retention and protection requirements of the Regulation N° 45/2001 of the European Parliament and of the Council of 18 December 2000. Personal information stored locally by the CommisSign CA or RA shall be handled as restricted, and access shall be granted only to those with an official need-to-know in order to perform their official duties.

Personal and corporate information held by the European Commission PA, CA and RA, other than that which is explicitly published as part of a certificate, CRL [, or ARL,] is considered Restricted and shall not be released unless required by law or regulation.

Generally, the results of annual audits are kept Restricted, with exceptions as outlined in Section 2.7 'Communication Of Results' of this CPS.

In general, audit logs will not be publicly available.

Any keys held by the CommisSign CA are considered Restricted and shall be released only to a authorised European Commission organisational authority, in accordance with this CPS, and the Security Policy for the European Commission PKI, or a law enforcement official, in accordance with European Commission regulations, European and State Members Law and this CPS.

2.8.2. Types Of Information Which Are Considered Public

Information included in public certificates, CRL's [and ARL] issued by the CommisSign CA are considered Public.

Information in the Certificate Policy for the European Commission PKI and this CPS is considered public.

2.8.3. Disclosure Of Certificate Revocation Information

When a certificate is revoked by the CommisSign CA, a reason code is included in the CRL entry for the action. This reason code is considered public and may be shared with all other subscribers and relying parties. However, no other details concerning the revocation are disclosed.

2.8.4. Release To Law Enforcement Officials

The CommisSign CA and RAs will not disclose certificate or certificate-related information to any third party, except when:

- authorised by the Security Policy for European Commission PKI and this CPS;
- required to be disclosed by law, European Commission, European and member State regulations, or court order;
- authorised by the subscriber when necessary to effect an appropriate use of the certificate.

Any requests for the disclosure of information must be signed and delivered to the local European Commission RA or CommisSign CA.

2.8.5. Other Information Release Circumstances

No stipulation.

2.9. Intellectual Property Rights

Certificates, *CRL's*[, and ARL's] issued by the CommisSign CA, the Certificate Policy for the European Commission PKI and this CPS are all property of the European Commission.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Initial Registration

3.1.1. Types Of Names

The RA extracts the following information from the Commission directory system:

- subscriber's last name (LASTNAME)
- subscriber's first name (FIRSTNAME)
- subscriber's CUID (unique and harmonised internal user identifier)
- subscriber's Commission E-mail SMTP address (SMTP)

The RA assumes that:

- the subscriber's CUID and the subscriber's Commission E-mail SMTP address are unique for the subscriber among the Commission staff;
- there is a one to one relationship between the subscriber's CUID and the subscriber's Commission E-mail SMTP address.
- The RA constructs the certificate SubjectName according to the following format:/CN=LASTNAME FIRSTNAME (CUID) /E=SMTP.

The RA registers the subscriber's SubjectName into the CA database.

3.1.2. Need For Names To Be Meaningful

If the subscriber is an individual, the name assigned to the Common Name attribute is the subscriber’s name.

If the subscriber is an organisation entity, the name assigned to the Common Name is the name of functional mailbox.

3.1.3. Rules For Interpreting Various Name Forms

No stipulation.

3.1.4. Uniqueness Of Names

Certificate SubjectName are unique for all end entities within the CommisSign CA domain. The User Management of the Commission has the responsibility to assure the uniqueness of the subscriber's CUID and Commission E-mail SMTP address.

3.1.5. Name Claim Dispute Resolution Procedure

Any dispute is resolved at the discretion of the User Management of the Commission.

3.1.6. Recognition, Authentication And Roles Of Trademarks

No stipulation.

3.1.7. Method To Prove Possession Of Private Key

Proof of possession of a private key is handled automatically by the operations of a secure communications protocol.

3.1.8. Authentication Of Organisation Identity

Public-key certificates are issued to individuals whenever possible. For those cases where there are several individuals acting in one capacity, only an encryption certificate is issued that contains the name of a functional mailbox. A signature certificate is not issued for a functional mailbox.

Individuals acting on behalf of the functional mailbox use their own individual signature certificate.

A functional mailbox for an organisation must be made by an individual authorised to act on behalf of the prospective subscriber. This authorised individual must be the person in the organisation who will be responsible for ensuring control of the certificates and the associated private keys, including accounting for which user has control of the keys at what time.

Identification and authentication of the prospective subscriber is as follows:

- the RA verifies the identity and authority of the individual acting on behalf of the prospective subscriber and their authority to receive the keys on behalf of that organisation.;

- the RA or CA keeps a record of the type and details of identification used; and the RA or CA shall retain the name of the person responsible for the mailbox to which the organisational certificate is issued.

The procedures that constitute the issuance of an organisational certificate do not conflict with other stipulations of this CPS (e.g., key generation, private key protection, and user obligations).

[In the case of issuing cross-certificates to other CAs, the CommisSign CA issues cross certificates to other CAs with the approval of the European Commission PA. The European Commission PA reviews the policies and procedures of the other CA before approving a cross certification. Conversely, the CommisSign CA's CPS and X.509 Certificate Policy for European Commission PKI are made available to the other CA for review.]

3.1.9. Authentication Of Individual Identity

An application for an individual to be a subscriber must be made by the individual or by his hierarchy on behalf of him. In this former case, the subscriber must be informed. In addition to the identification and authentication described below, the prospective subscriber must personally

present him or herself to their LRA for authentication prior to certificate issuance.

It is the responsibility of the RA to obtain confirmation of affiliation. It is the responsibility of the LRA to obtain confirmation of the identity of the subscriber applying for a certificate. The authentication procedure includes the processes described in the following sections.

3.1.10. Authentication of Subscriber's Affiliation:

Confirmation of the subscriber's affiliation with the European Commission must be provided to the RA before a certificate may be issued to the subscriber. The subscriber's proof of affiliation is provided through the European Commission Directory. The presence of the subscriber in the European Commission Directory is controlled by administrative procedure.

3.1.11. Authentication of Subscriber's Identity:

The LRA performs identity verification either at the time of the certificate request or prior to the request – using the RA files and archives authentication documentation.

Confirmation of the subscriber's identity must be verified by the LRA through the service card.

3.1.12. Authentication Of Devices Or Applications

No stipulation.

3.2. Routine Rekey

Re-keying a certificate means that that a new certificate is created with:

- the same SubjectName,
- a new serial number,
- a new public key,
- and possibly a different validity period.

The procedure of Routine Rekey is applied each time the user's certificate is not valid anymore. This procedure is identical to the procedure of Initial Registration.

3.3. Rekey After Revocation

For subscribers whose certificates have been revoked, they must apply the same procedure than the procedure for Routine Rekey.

3.4. Revocation Request

Revocation is described in Section 4.4 'Certificate Suspension & Revocation' of this CPS.

4. OPERATIONAL REQUIREMENTS

4.1. Certificate Application

Prior to certificate issuance, a subscriber must submit a request. The request includes the following information:

- subscriber's full name,
- subscriber's type of European Commission affiliation,
- proof of subscriber's affiliation,
- subscriber's Commission e-mail SMTP address,
- subscriber's Common User Identifier,
- acknowledgment of the terms specified in this CPS.

Depending on the RA's authentication process, the RA may choose to include additional information on the certificate request to assist in the identity confirmation.

The certificate request is signed by the subscriber (if this is an individual request) and by the LRA (via a signed e-mail). The LRA sends this request to the RA.

Using the information provided by the certificate requester, the RA and LRA perform identity verification according to the requirements noted in section 3.1 'Authentication of Organisation Identity' and 'Authentication Of Individual Identity'. Based on the verification, the RA either accepts or refuses the certificate request. The RA notifies the subscriber of acceptance or refusal. The RA notes the action taken on the certificate request, the verification action taken and then signs and dates the request. The RA retains the certificate request.

4.2. Certificate Issuance

The procedure described below is the **standard procedure**:

(1) The subscriber sends a request for a certificate to the LRA of his DG (explicit request) or the LRA gets the list of the candidate subscriber(s) from his hierarchy (implicit request);

(2) The LRA transmits the request to the RA by a signed-mail;

(3) The LRA informs the candidate subscriber(s) and warns them that they will receive an identification code from the RA and another identification code from himself;

(4) The RA performs an administrative check of the subscriber and inserts the subscriber's SubjectName into the CA database;

(5) The CA sends a registration file by secured way containing the subscriber's SubjectName and an identification code C1 to the RA;

(6) The RA sends by a secured e-mail to the demanding LRA the registration file;

(7) The RA sends by confidential mail to the subscriber a paper document indicating his identification code C1;

(8) The LRA checks if the subscriber physically exists after receipt of the registration file from the RA;

(9) The LRA contacts the CA to confirm the existence of the subscriber;

(10) The CA updates the registration file and sends a second identification code C2 to the LRA;

(11) The LRA sends to the subscriber the registration file (by floppy, e-mail) and a paper containing the identification code C2;

(12) The LRA helps the registered subscriber(s), that possess his registration file and the two codes, C1 and C2, to generate their keys and to get a certificate from the CA. During the key generation process, the registered subscriber must be present to enter the RA and LRA identification codes and an initial password for the private key;

(13) The registered subscriber stores his private key on hard disk, floppy[or smart card] according to the DG storage policy;

Certificate publication: on a daily rhythm,

(1) The CA officers generate a file containing all the certificates and deliver it to the Commission directory administrator at 21:15;

(2) The Commission directory administrator updates the Commission directory with the certificates at 22:00.

The procedure described below is an **amended and temporary** procedure to offer a "Key recovery" procedure at the DG level. This procedure will be abandoned and the normal one used, when two sets of keys for, respectively, signature and encryption, and a central key recovery service for the latter are available. The temporary procedure for a certificate request is the following (the (*) mark indicates that the usual procedure has not been modified):

(1) The subscriber sends a request for a certificate to the LRA of his DG (explicit request) or the LRA gets the list of the candidate subscriber(s) from his hierarchy implicit request; (*)

(2) The LRA transmits the request to the RA by a signed-mail (*);

(3) The LRA informs the candidate subscriber(s) and warns them that they will receive an identification code from the RA and an other identification code from himself (*);

(4) The RA performs an administrative check of the subscriber and inserts the subscriber's SubjectName into the CA database (*);

(5) The CA sends a registration file containing the subscriber's SubjectName and an identification code C1 to the RA (*);

(6) The RA sends by a secured e-mail to the demanding LRA the registration file and the identification code C1;

(7) The RA sends to the subscriber (by e-mail) a message indicating the certificate request;

(8) The LRA checks if the subscriber physically exists after receipt of the registration file from the RA (*);

(9) The LRA contacts the CA to confirm the existence of the subscriber (*);

(10) The CA updates the registration file and sends a second identification code C2 to the LRA (*);

(11) The LRA that possesses the registration file and the two identification codes of the subscriber, creates a key pair;

(12) The LRA contacts the CA and requests a certificate (the LRA identifies himself to the CA with his two identification codes of the subscriber);

(13) The LRA makes a copy of the key file containing the private key and the public key certificate of the subscriber, and of the initial password;

(14) The LRA puts the key file and the initial password in a safe under the control of the Security Officer;

(15) The LRA hands out the key file and the initial password to the subscriber;

(16) The LRA helps the registered subscriber(s) to store the key file on hard disk or on floppy depending on the DG storage policy.

4.3. Certificate Acceptance

Acceptance by the subscriber of his/her responsibilities regarding certificate use is secured in the certificate request process as described in Section 4.1 of this CPS. *The subscriber signs an acknowledgement of the terms of this CPS and terms noted in the Subscriber's Agreement*.

Acceptance of the certificate occurs in the certificate issuance process described in Section 4.2 of this CPS. The operation of the secure communications protocol between the subscriber and the CommisSign CA involves the mutual authentication of the two parties and request and response operations that constitute acceptance by the subscriber of the resulting public key certificates.

4.4. Certificate Suspension and Revocation

4.4.1. Circumstances For Revocation

Encryption and/or signature verification certificates are revoked when the certificates are no longer trusted, for any reason. This includes certificates for subscribers, RAs, and CA Officers. Reasons for loss of trust in certificates include, but are not limited to:

- dismissal or suspension for cause,
- compromise or suspected compromise of private keys and/or user passwords and profile,
- termination of employment,
- failure of the requester to meet their obligations under this document and relevant certificate policies.

4.4.2. Who Can Request Revocation

The revocation of a certificate may only be requested by:

- the subscriber in whose name the certificate has been issued,
- *the individual who made the application for the certificate on behalf of a functional mail box,*
- *the subscriber's management, if the subscriber belongs to European Commission staff,*
- *personnel of the CommisSign CA,*
- *personnel of a RA associated with the CommisSign CA,*
- *The Director of the Protocol and Security Service,*
- *L'"Autorité investi du pouvoir de nomination" (AIPN),*
- *the European Commission PA,*

4.4.3. Procedure For Revocation Request [To be implemented] [To be reviewed when implemented]

Any requester wishing to revoke a certificate, must notify their local RA, complete and sign a written approval for revocation, and present themselves in person with their badge.

The LRA is responsible for processing certificate revocations and renewals. Certificate revocation must be requested in writing to the local RA. When the RA logons to the CA server to process the revocation, the CommisSign CA will update the CRL immediately. The local RA will inform the revocation requester as soon as practicable.

Revoked certificates are published in CRL's and posted to the European Commission Directory, in accordance with Section 4.4 'CRL Issuance Frequency' of this CPS. RAs can immediately post a CRL if deemed necessary.

Written approval must be obtained for auditing purposes and must contain the following information:

- date of revocation request,
- name of the owner of the certificate (i.e. subscriber),
- detailed reason for requesting revocation,
- name and title of person requesting revocation,
- contact information of person requesting revocation,
- signature of person requesting revocation,

Written approvals are sent to the RA. In cases requiring immediate revocation of a subscriber's certificate, an e-mail request or call must be sent to the RA and must be confirmed by written approval.

Upon receipt and confirmation of the written approval, the RA revokes the subscriber's certificate by logging in to the CA server and performing the certificate revocation. The RA records the event in the RA Administration Logbook. The RA notes the action taken on the written approval and then signs and dates the approval. The RA retains the revocation written approval.

4.4.4. Revocation Request Grace Period

No stipulation.

4.4.5. Circumstances For Suspension

No stipulation.

4.4.6. Who Can Request Suspension

No stipulation.

4.4.7. Procedure For Suspension Request

No stipulation.

4.4.8. Limits On Suspension Period

No stipulation.

4.4.9. CRL Issuance Frequency

The CommisSign CA issues CRL's [and ARL's] to the European Commission Directory every 24 hours. The CRL's [and ARL's] are issued 7 days per week. Upon exception, CRL's [and ARL's] may also be issued between these intervals (e.g.: upon detection of a serious compromise situation).

4.4.10. CRL Checking Requirements

[Each certificate issued by the CommisSign CA shall include the full DN of the CRL Distribution Point to be checked during the verification of the certificate.]

Before using a certificate, relying parties must check its status against a current copy of the CRL. If it is temporarily unfeasible to obtain revocation information, then the relying party must either reject the use of the certificate, or make an informed decision to accept the risk, responsibility and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this CPS.

4.4.11. On-line Revocation/status Checking Availability

The European Commission PKI does not currently support on-line revocation/status checking.

4.4.12. On-line Revocation Checking Requirements

No stipulation.

4.4.13. Other Forms Of Revocation Advertisements Available

No stipulation.

4.4.14. Checking Requirements For Other Forms Of Revocation Advertisements

No stipulation.

4.4.15. Special Requirements Key Compromise

Key Compromise is a security incident that must be processed.

In any key compromise situation involving an end entity key, a report is filed with the local RA indicating the circumstances under which the compromise occurred. If accidental, on the part of the requester, no further action is required. Otherwise, the local RA reports the compromise to the Protocol and Security Service for a possible follow-up investigation and potential action in accordance with the procedures described in the ICT Security Policy.

In the event of the compromise, or suspected compromise, of the CommisSign CA signing key, the CommisSign CA shall immediately notify the PA. With co-operation of the European Commission PA, the

CommisSign CA shall notify all CA's to whom it has issued cross certificates.

4.5. Security Audit Procedures [To be implemented] [To be reviewed when implemented]

4.5.1. Types Of Event Recorded

[All significant security events on the CommisSign CA software are automatically time stamped and recorded in audit log files. These include events such as:

- successful and failed attempts to initialise subscribers, remove, enable, disable, update, and recover subscribers, their keys, and certificates,
- successful and failed attempts to create, remove, login as, set, reset, and change passwords of, revoke privileges of, create, update, and recover keys and certificates CA Officers, RAs, and subscribers,
- failed interactions with the directory including successful and failed connection attempts, read and write operations by the CA system,
- all events related to certificate revocation, security policy modification and validation, CA software start-up and stop, database backup, cross certification, certificate and certificate chain validation, attribute certificate management, user upgrade, DN change, database and audit trail,
- management, certificate life-cycle management and other miscellaneous events,
- system start-up and shutdown.

The CA system administrator maintains information concerning:

- system configuration changes and maintenance,
- administrator privileges,
- discrepancy and compromise reports,
- unauthorised attempts at network access to the CA system.

The CA facility has an electronic monitoring system that provides information concerning access to the CommisSign CA facility.]

4.5.2. Frequency Of Audit Log Processing

[The European commission CA Officers process audit logs weekly, investigating any alerts or irregularities in the logs.]

4.5.3. Retention Period For Audit Log

[The audit trails are electronically retained indefinitely under the CommisSign CA configurations. Section 4.5 'Audit Log Backup Procedures' describes the archive procedures for these logs.]

4.5.4. Protection Of Audit Log

[The audit trail is stored in regular operating system flat files. Each audit trail file consists of an audit header that contains information about the audits in the file and a list of events. A Message Authentication Code (MAC) is created for each of the audit events and the audit header. Each audit trail file has a different audit key used to generate the MAC. The European Commission CA Master User for the CommisSign CA protects the audit key that is stored in the audit header.

The audit trail can be spread across many files. A new audit trail file is created whenever the current audit trail file reaches a pre-set size of 100 Kbytes or the CA master key is updated.]

4.5.5. Audit Log Backup Procedures

[Audit trails are backed up nightly as part of a regular CA system backup. Audit trail files are archived by the CA system administrator on a weekly basis. All files, including the latest audit trail file, are moved to magnetic tapes and stored in a secure archive facility.]

4.5.6. Audit Collection System

[The audit trail accumulation system is internal to the CommisSign CA software system.]

4.5.7. Notification To Event Causing Subject

[Where an event is logged by the audit collection system, notification is not sent to the individual causing the audit event. The subject may be notified that their action was successful or unsuccessful but not that their action was audited.]

4.5.8. Vulnerability Assessments

[The CommisSign CA system administrator and CA officers use the processes identified in the System Security Audit Procedures section of this CPS to monitor, assess and address as required system vulnerabilities.]

4.6. Records Archival [To be implemented] [To be reviewed when implemented]

4.6.1. Types Of Data Archived

[In the execution of the RA and LRA function, various documents are provided to the RA and LRAs. These documents include:

- identification information,

- certificate requests,
- certificate revocation approvals,
- key recovery approvals;

Some information provided is personal information and falls under the Regulation (EC) N° 45/2001 of the European Parliament and of the Council of 18 December 2000. This information shall be stored securely in accordance with these Regulation requirements. Access to this information shall be limited to RA personnel.

The types of events recorded in the CA system database include:

- creation of the CA signing key pair,
- addition and removal of end users from the system,
- changes to the encryption key pair history and verification public key history for all users, including certificate issuance and revocation events,
- changes to the DN of end users,
- addition/removal of RA and CA Officer privileges,
- changes to the privileges of RAs and CA Officers,
- changes to some aspects of policy such as certificate validity period,
- creation and revocation of cross-certificates.

In addition the CommisSign CA system provides audit log data as described in Section 4.5 of this CPS.]

4.6.2. Retention Period For Archive

[Audit information (per Section 4.5 of this CPS), subscriber key and certificate requests/approvals, and identification and authentication information are archived for five years.]

[Digital signature certificates, confidentiality private keys stored by a CA [, ARL's] and CRL's generated by a CA, are archived in accordance with European Commission and relevant Member States regulations.]

4.6.3. Protection Of Archive

[The CommisSign CA system database is [encrypted and] protected by the CA system. Protection of the audit trail is as described in Section 4.5 ‘Protection of Audit Log’ of this CPS.

The archive media is protected by physical security in that it is retained in a restricted access facility to which only the CommisSign CA system administrators and CA Master Users have access.]

4.6.4. Archive Backup Procedures

[Archive files are backed up as they are created. Originals are stored on-site and housed with the CommisSign CA system. Backup files are stored at a secure and separate geographic location.]

4.6.5. Archive Collection System

[The archive collection system (backup facility) for the CommisSign CA system database is internal to the CommisSign CA system.

The archive collection system (backup facility) for the audit trail files is described in Section 4.5 'Audit Log Backup Procedures' and 'Audit Collection System' of this CPS.

The archiving of both data stores onto separate media and the secure storage of that media is external from the CommisSign CA system.]

4.6.6. Procedures To Obtain And Verify Archive Information

[Twice per year, the archive tapes are retrieved by the CommisSign CA Officer and verified to ensure no damage or loss of data has occurred. If any has occurred, the backup archive is retrieved, becomes the new master archive, and a new backup is produced.

Once every five years, a new backup of each archive is produced, even if there is no evidence of damage or loss of data on the master or backup archive. For each tape, the new backup becomes the master archive, the previous master archive becomes the backup archive and the previous backup archive tape is securely recycled.]

4.7. Key Changeover

Refer to Sections 3.2 and 3.3 of this CPS.

4.8. Compromise and Disaster Recovery [To be implemented] [To be review when implemented]

4.8.1. Computing Resources, Software, And/or Data Are Corrupted

In the event of a disaster or serious compromise, the following applies to the CommisSign CA and the RAs. The steps for recovering a secure environment are as follows:

(1) all CommisSign CA system passwords shall be changed for CA Master Users, CA Officers, and RAs (in case of a CA compromise);

(2) depending on the nature of the disaster, some or all user certificates shall be revoked;

(3) if the directory becomes unstable or if the directory is suspected to be corrupt, the directory data, encryption certificates, and CRLs must be recovered. Once the Directory Administrator has restored the directory from backup, the CA Master User will update the PKI

information in the directory. PKI information includes CRLs and certificates that have changed since the last directory backup:

(4) should a CA Officer or RA's profiles need recovery, the profiles may be recovered by another CA Officer or RA.

Refer to Section 4.4 'Special Requirements Key Compromise' concerning CA key compromise.

4.8.2. Entity Key Recovery

The standard procedure has been amended to offer a Key recovery procedure at the DG level. Private key copy and associated initial password are kept by the Security Officer of the DG in a safe and access controlled area. Only the security officer or duly authorised official representative may access the keys and passwords. Only LRAs perform key recoveries. The LRA and the Security Officer are present to authorise and perform key recovery operations. If the LRA and the Security Officer are unavailable, CA Officers act as substitute administrators in emergency cases. The key may be retrieved in three cases:

- at the user request;
- at Disciplinary or equivalent internal entity request;
- at the Director General request in case of permanent or important unavailability of the user harming seriously to the interest of the service.

[The timeframe for completion of non-emergency key recovery requests is within 48 hours. In emergency cases, the local RA is contacted.]

4.8.2.1.Key recovery at User request

Examples of reasons for subscriber requested key recovery include:

- a subscriber forgets a password,
- a subscriber loses or damages a private key file.

For the subscriber's protection from unauthorised requests, the subscriber must

- make arrangements to appear in person and
- submit written approval to the LRA stating the reason for the recovery.

Upon receipt of written approval, the LRAs visually verify the identity of the subscriber using the employee service card, and performs the key recovery process. LRA log the recovery event for auditing purposes. The LRA note the action taken on the written approval, and then sign and date the approval. The LRA retains the recovery written approval.

LRA then present the subscriber with instructions for obtaining new authorisation information.

4.8.2.2.Key recovery at third party request

Examples of reasons for key recovery without subscriber consent include:

- a subscriber has left the organisation and the subscriber's supervisor or department management needs to decrypt files for business continuity
- a subscriber's actions are in question by the European Commission and the subscriber's files need to be reviewed
- a subscriber's actions are in question by an external law enforcement body and the subscriber's files need to be reviewed.

The key recovery requester needs to contact their Security Officer. Written approval from both the subscriber's general Director and from the body requesting key recovery action is submitted to the LRA's before the action is performed. The request must contain the following:

- date of recovery request,
- name of the owner of the keys (i.e. subscriber),
- requester's name and European Commission organisation,
- detailed reason for requesting access to subscriber's files,
- specific name(s) of person(s) allowed to see subscriber's files and to be responsible for subsequent viewing by any unnamed persons,
- description (and/or filename(s)) of subscriber's files to be viewed, or statement of approval to access all files,
- description of LRA role beyond key recovery action, including what information to provide if the subscriber should inquire about the change in their CommisSign CA accessibility.

Upon receipt of written approval, the LRAs contact the appropriate parties to schedule key recovery actions.

[Note: In certain situations, LRA may be given a court order requesting key recovery. In this case, the court order will be the equivalent of a written approval.]

If applicable, requesters should bring a diskette containing subscriber's files to be viewed at the scheduled recovery process. LRAs (under the control of the Security Officer) may load files on a local machine for decrypting/viewing and then delete decrypted files at the completion of the process, avoiding potential unauthorised viewing.

Requesters should first confirm that the LRAs have machines with the required software to view the files. If not, the LRAs may travel to the requester's location within the European Commission site.

Upon receipt of written approval, the LRAs visually verify the identity of authorised person(s) using the employee badge, perform the key recovery process, and log the recovery event. The LRAs note the action taken on the written approval, and then sign and date the approval. The LRAs retain the written approval for auditing purposes.

If the subscriber will be retaining accessibility privileges to the CommisSign CA after the requested key recovery is completed, the RAs perform another key recovery process so the subscriber may be ensured that no one has access to their key data any longer.

When applicable, the LRA may disable the recovered subscriber's CommisSign CA account after the scheduled process if a short, remote viewing time limit has been requested. Re-enabling the account shall be based on instructions provided by the requester.

External entities refer to any law enforcement body. Requests by an external entity must be processed through the Protocol and Security Service.

The steps followed in the case of key recovery without subscriber consent are followed for external entity requests.

4.8.3. Disaster Recovery

[The CommisSign CA has a disaster recovery plan that describes procedures to recover from a disaster or serious compromise. A standby CA is configured at a disaster recovery site at an alternate European Commission Centre.]

4.9. CA Termination

In the event of CommisSign CA termination, the European Commission PA provides oversight of the termination process. The RA and LRA's shall work with the CA to notify all subscribers of the CommisSign CA cessation of operation.

All certificates issued by the CommisSign CA shall be revoked.

The European Commission shall retain an archive of the CommisSign CA database in accordance with IS Security Policy and European Commission and relevant Member States regulations.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1. Physical Security Controls

5.1.1. Site Location And Construction

The CommisSign CA is contained in an area to which access is controlled through an entry point and limited to authorise personnel. The facility that houses is locked, and electronically monitored 24 hours a day and 7 days a week. [Electronic logs are maintained of physical access to the Protocol and Security Service.]

5.1.2. Physical Access

The CommisSign CA facility is locked and only authorised and appropriately screened personnel are allowed access. The only personnel allowed access to the CommisSign CA are the CommisSign CA Master Users, CA Officers and CA system administrator.

[The RA systems are placed in locations where access is restricted.] The Central RAs are logically protected by smart card.

Subscribers must comply with this CPS and the Certificate Policy for the European Commission regarding protection and use of their keys. Subscribers are advised of these requirements but are not audited or monitored on a regular basis.

5.1.3. Power And Air Conditioning

The European Commission CA facility is supplied with power and air conditioning sufficient to create a reliable operating environment. Personnel areas within the facility are supplied with sufficient utilities to satisfy operational, health, and safety needs.

5.1.4. Water Exposures

The CommisSign CA workstation it is not in danger of exposure to water.

5.1.5. Fire Prevention And Protection

[The CommisSign CA facility is supplied with a fire extinguishing system in accordance with European Commission HST Service policy and code.]

5.1.6. Media Storage

[Storage media used by the CommisSign CA is protected from environmental threats of temperature, humidity and magnetism.]

5.1.7. Waste Disposal

Media used for the storage of information of the CommisSign CA files is sanitised or destroyed before released for disposal.

Normal office waste shall be removed or destroyed in accordance with local the European Commission rules.

5.1.8. Off-site Backup [Not applicable]

[The backup CA facility has equivalent security and controls as the primary CommisSign CA.]

5.2. Procedural Controls

5.2.1. Trusted Roles

[Personnel filling these roles shall successfully complete background investigations for critical-sensitive positions. Background investigation criteria and other personnel security controls are noted in the following sections.]

5.2.1.1.CA Trusted Roles:

Protocol and Security Service operates the CommiSign CA. It plays the role of CA Operation Authority, CA officers and CA System Administrators describe below.

To ensure the one person acting alone cannot circumvent safeguards, multiple roles and individuals share responsibilities of the CommisSign CA. Each account on the CommisSign CA system has limited capabilities commensurate with the individual's role. The roles within the CommisSign CA are:

- CA Master Users

[Three individuals shall be assigned as CA Master Users.]The CA Operation Authority appoints the Master Users. Master Users have the authority to:

– generate and maintain the Master key of the CommisSign CA,

– change the CA Server passwords,

– recover CA Officers in the event they have forgotten their passwords.

- CA Officers

[Three individuals are assigned as CA Officers.]The CA Operation Authority appoints the CA Officers. The CA Officers have the authority to:

– set and modify the security policy for the CommisSign CA, in accordance with this CPS and the Certificate Policy for European Commission;

– set the number of required authorisations for sensitive operations;

– add and delete RA and LRAs;

– [issue, update, and revoke cross certification agreements at the direction of the European Commission PA;]

– change RA and LRA smart card Pin Code;

– set default certificate profiles (lifetimes, etc.);

– process audit logs and ensure PKI system database is backed up.

- CA System Administrators

[Two individuals are assigned CA system administrator responsibilities, with one acting as a backup.]The CA Operation Authority appoints the CA system administrators. The CA system administrators are responsible for

– Maintaining the correct operation and configuration of the underlying hardware and software for the CommisSign CA;

– Performing backups of the CommisSign CA system.

5.2.1.2.RA Trusted Roles:

At least two individuals are designated as RAs. RA's have the authority to:

- accept and process certificate request[, certificate revocation/suspension][and key recovery requests],
- verify of an applicant's identity,
- transmit applicant information to the CA,
- receive and distribute subscriber authorisation information,

5.2.1.3.LRA Trusted Roles:

At least two individuals at each General Directorate or autonomous entity (Delegations, ...) are designated as LRAs. LRA's have the authority to:

- accept and process certificate request,
- transmit applicant information to the CA,
- receive subscriber authorisation information from the RA,
- verify the applicant's identity and physical presence,
- distribute authorisation information to the subscriber,
- Assist the subscriber during the key and certification creation process.

5.2.2. Number Of Persons Required Per Task

The following tasks are defined as sensitive and require at least two individuals to perform the tasks.

Two CA Officers are required to:

- add and delete other CA Officers and RAs
- set default certificate profiles

LRA and SO are required to:

- perform key recovery

5.2.3. Identification & Authentication For Each Role

Identification and authorisation for RA and LRA personnel follow requirements identified in Section 5.3.

Once these personnel are authorised, they are issued a certificate and smart card, which identifies and authenticates them to the CommisSign CA system. In addition, the are entered in the CommisSign CA database with their role and authorities specified. In the execution of sensitive operations, RA and LRA personnel authenticate themselves using smart card.

5.3. Personnel Security Controls

5.3.1. Background, Qualifications, Experience, and Clearance Requirements

[Personnel filling these roles shall successfully complete background investigations for critical-sensitive positions. CA Master Users, CA Officers and RA are deemed to be critical sensitive positions with a high risk classification. LRA's are deemed critical sensitive positions with a moderate risk classification.]

5.3.2. Background Check Procedures

All background checks are performed in accordance with the European Commission and European government Personnel Security Policies.

5.3.3. Training Requirements

Personnel performing duties with respect to the operation of a CA, RA or LRA receive:

- training in the operation of the software and/or hardware used in the CommisSign CA system
- training in the duties they are expected to perform
- briefing on stipulations of this CPS and the Certificate Policy for the European Commission PKI

5.3.4. Retraining Frequency And Requirements

The requirements of the previous section are kept current to accommodate changes in the CommisSign CA system. Refresher training is conducted in accordance with these changes.

5.3.5. Job Rotation

No stipulation.

5.3.6. Sanctions For Unauthorised Actions

In the event of actual or suspected unauthorised action by a person performing duties with respect to the operation of the CommisSign CA or

RAs, disciplinary action could be taken (in accordance with the European Commission status).

Contravention of this CPS or the Certificate Policy for the European Commission whether through negligence or with malicious intent, is subject to privilege revocation and/or administrative discipline.

5.3.7. Contracting Personnel

Contractor personnel employed to operate any part of the CommisSign CA or RAs are subject to the same criteria as a European Commission statutory employee, and cleared to the level of the role performed as identified in Section 5.3.

5.3.8. Documentation Supplied To Personnel

This CPS is made available to the CommisSign CA and RA personnel and to subscribers. Operation manuals are made available to CA and RA personnel so they can operate and maintain the hardware and PKI software.

In addition to the CPS, the subscribers are provided information on the use and protection of the software used within the European Commission domain and the CommisSign CA provides technical help desk support for all domain users.

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

The CommisSign CA signing key pair is created during the initial start up of the CA master control application and is protected by the CA master key.

For users, the PKI client software generates the digital signature key pair. Keys generated by software may be stored in a file on a disk or on a removable diskette.

6.1.2. Private Key Delivery To Entity

For the digital signature key pair, as the key pair is generated by the subscriber's user software, no delivery of the private key is required.

6.1.3. Public Key Delivery To Certificate Issuer

The signature verification public key is delivered securely to the CommisSign CA system using a secure communications protocol.

6.1.4. CA Public Key Delivery To Users

The CommisSign CA verification public key is delivered to subscribers in a CA certificate using a secure communications protocol. The CommisSign CA verifies that public key is delivered to external relying party in a CA

certificate held on a European Commission Web server using a secure protocol.

6.1.5. Asymmetric Key Sizes

User signing key pairs are 1024 bit RSA.

The CommisSign CA signing key pair is 1024 bit RSA. The session keys of secure communications protocol are Triple DES.

6.1.6. Public Key Parameters Generation

No stipulation

6.1.7. Parameter Quality Checking

No stipulation

6.1.8. Hardware/software Key Generation

The CommisSign CA Master key is stored in hardware. All other entity keys are generated in the PKI client software.

6.1.9. Key Usage Purposes (as per X.509v3 field)

The digital signature key pair is used to provide authentication, integrity, and support for non-repudiation services.

The encryption key pair is used to protect a symmetric key used to encrypt data and as such provides confidentiality services.

The CommisSign CA signing key is used to sign certificates, CRL's, [and ARL's] issued by that CA. The session keys of the secure communications protocol are used to provide secure communications for key management operations.

For a temporary period, there is only one key pair.

6.2. Private Key Protection

The following sections describe the technical and procedural techniques for private key protection. The protections noted below do not negate the subscriber’s responsibility to protect their private keys from disclosure.

6.2.1. Standards For Crypto-module

The cryptographic module used by the software used in the CommisSign CA domain complies with [.....]

6.2.2. Private Key Multi-person Control

Multiple person control is required for private key recovery, refer to Section 5.2. ‘Number of Persons Required Per Task’.

6.2.3. Private Key Escrow

Escrow of private keys by an external third party is not provided.

6.2.4. Private Key Backup

The CommisSign CA private keys in the CommisSign CA system database. The subscriber's private signing key is never backed up in the CommisSign CA system, in order to provide support for non-repudiation services. [The CommisSign CA system database is encrypted.] [The CommisSign CA system database is backed up nightly.]

6.2.5. Private Key Archival

Refer to Section 4.6 of this CPS for information on key archival.

6.2.6. Private Key Entry Into Cryptographic Module

The CommisSign CA signing private key and the subscriber signing private key are generated in software, within the cryptographic module, and not entered by other entities into that module.

Private keys are stored encrypted in the cryptographic module and are decrypted only at the time at which they are actually being used.

6.2.7. Method Of Activating Private Key

Private keys are activated at the time the subscriber logins to the cryptographic client software. The login is in the form of a password that is protected from disclosure while it is being entered.

6.2.8. Method Of Deactivating Private Key

The private keys remain active for the period of login. The login period is ended either by the subscriber logging out or by the subscriber key deactivation.

6.2.9. Method Of Destroying Private Key

Permanent destruction of private keys is achieved with secure delete operations.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

Refer to section 6.2 for key backup and archival.

6.3.2. Usage Periods For The Public And Private Keys

The CommisSign CA public key and certificate – [10 years]

The CommisSign CA private signing key –[10 years.]

Subscriber public verification key and certificate - two years

6.4. Activation Data

6.4.1. Activation Data Generation And Installation

Passwords or smart cards are required by all entities logging on to the PKI software. The software applies a stringent set of rules to each password to ensure it is secure. Passwords are mandatory for CA. RA and LRA's are protected by smart card.

Rules on password selection include:

- it must have at least twelve characters;
- it must have at least one upper-case letter, special characters and digit;
- it must have at least one lower-case letter;
- it must not contain many occurrences of the same character;
- it must not be the same as the entity's profile name; and
- it must not contain a long sub-string of the entity's profile name.

Data used for subscriber initialisation is described in Section 4.2 of this CPS.

6.4.2. Activation Data Protection

For the CommisSign CA Server System Administration, CA Officers, and RAs, user names and password check values are stored in the CommisSign CA system database.

6.4.3. Other Aspects Of Activation Data

No stipulation.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

[The CommisSign CA system provides the following functionality through the operating system and a combination of the operating system, the CommisSign CA software and physical controls:

- access control to CA services and PKI roles;
- enforced separation of duties for PKI roles;
- identification and authentication of PKI roles and associated identities,
- use of cryptography for session communication and database security;
- archival of CA and end entity history and audit data;
- audit of security related events; and

- recovery mechanisms for keys and the CA system.

Information on this functionality is provided in the respective sections of this CPS.

6.5.2. Computer Security Rating

No stipulation.

6.6. Life Cycle Security Controls

6.6.1. System Development Controls

No stipulation.

6.6.2. Security Management Controls

The security management controls for the CommisSign CA include:

- a mechanism and/or policies in place to control and monitor the CA system configuration;
- the CommisSign CA equipment is dedicated to administering a key management infrastructure;
- the CommisSign CA equipment does not have installed applications or component software, which are not part of the CA configuration, with the exception of virus protection software; and
- the CommisSign CA equipment updates are installed by trusted and trained personnel in a defined manner.

6.7. Network Security Controls

[Remote access to the CommisSign CA system is secured using a secure communications protocol. No other remote access is permitted and features including inbound FTP are disabled. All TCP/IP ports are be blocked except those required by the PKI enabled event auditing and the audit of all failed operations and low-frequency successes.]

6.8. Cryptographic Module Engineering Controls

The cryptographic module of the PKI software is designed to comply with [.....] The CommisSign CA master key is stored in a hardware device that complies with [.....]

The cryptographic module to generate keys used by the PKI software is designed to comply with [.....]

7. CERTIFICATE AND CRL PROFILE

7.1. Certificate Profile

7.1.1. Version Number

The CommisSign CA issues X.509 Version 3 certificates in accordance with the PKIX Certificate and CRL profile. The following X.509 fields are supported:

Fields	**Description**
version:	version field is set to v3
serial number:	when a new user certificate is created, a unique serial number within the CommisSign CA security domain is generated by the CommisSign CA system
signature Algorithm:	identifier for the algorithm used by the CommisSign CA to sign the certificate
issuer:	certificate issuer the CommisSign CA Distinguished Name
validity:	certificate validity period - notBefore start date and notAfter end date are specified
subject:	certificate subject Distinguished Name
public key information:	algorithm identifier Public key
Thumbprint Algorithm:	Algoritm identifier
Thumbprint	

7.1.2. Certificate Extensions

There are no supported extensions.

7.1.3. Algorithm Object IDs

The CommisSign CA supports the following algorithms:

Algorithm	**Object Identifier**	**Issuing Authority**
SHA1WithRSAEncryption	1 2 840 113549 1 1 5	UTIMACO
DES-EDE3-CBC	1 2 840 113549 3 7	UTIMACO

7.1.4. Name Forms

In a certificate, the issuer DN and subject DN fields contain the full X.500 Distinguished Name of the certificate issuer or certificate subject.

7.1.5. Name Constraints

Name constraints are not used by the CommisSign CA.

7.1.6. Certificate Policy Object Identifier

No stipulation.

7.1.7. Usage Of Policy Constraints Extension

Policy constraints are not used by the CommisSign CA.

7.1.8. Policy Qualifiers Syntax And Semantics

No stipulation.

7.1.9. Processing Semantics For The Critical Certificate Policy

[The only certificate extension, which may be identified as critical in certificates issued by the CommisSign CA, is the cRLDistributionPoints extension. The CRL or ARL shall be retrieved from the CRL distribution point directory entry indicated in the certificate, unless a current copy of that CRL or ARL is cached at the subscriber's client software.]

7.2. CRL Profile [To be reviewed when implemented]

7.2.1. Version Number

CRLs issued by the CommisSign CA are X.509 version 2 CRLs in accordance with PKIX Certificate and CRL profile.

The following is a list of the fields in the X.509 version 2 CRL format that are used by the CommisSign CA:

Fields	**Descriptions**
Version	set to v2
Signature	identifier of the algorithm used to sign the CRL
Issuer	the full Distinguished Name of the CommisSign CA
this update	time of CRL issue
next update	time of next expected CRL update
revoked certificates	list of revoked certificate information

7.2.2. CRL and CRL Entry Extensions

The following Section describes the X.509 version 2 CRL and CRL entry extensions that are supported by the CommisSign CA. and the X.509 version 2 CRL and CRL entry extensions that are not supported in CRL's issued by the CommisSign CA.

7.2.2.1.Supported Extensions

The following table the CRL and CRL entry extensions supported by the CommisSign CA.

EXTENSION	**CRITICAL / NON CRITICAL**	**OPTIONAL**	**NOTES**
AuthorityKeyIdentifier	Non critical	Not optional	Only element [0] (authorityKeyIdentifier) is filled in Contains a 20 byte hash of the subjectPublicKeyInfo in the CA certificate
CRLNumber particular	Non critical	Not optional	Incremented each time a CRL/ARL is changed
ReasonCode	Non critical	Not optional	CRL entry extension – only reason codes (0), (1), (3), (4) and (5) are currently supported
IssuingDistributionPoint	Critical	Not optional	Element [0] (distributionPoint) includes the full DN of the distribution point Element [1] (onlyContainsUserCerts) is included for CRL’s Element [2] (onlyContainsCACerts) is included for ARL’s Element [1] and [2] are never present together in the same revocation list Elements [3] and [4] are

EXTENSION	CRITICAL / NON CRITICAL	OPTIONAL	NOTES
			not used

7.2.2.2.Unsupported Extensions

The CommisSign CA does not support the following X.509 version 2 CRL extensions:

- issuer alternative name,
- hold instruction code,
- invalidity date,
- certificate issuer,
- delta CRL indicator,

8. SPECIFICATION ADMINISTRATION

8.1. Specification change procedures

This CPS shall be reviewed in its entirety every year. Errors, updates, or suggested changes to this document shall be communicated to the contact in section 1.4.

8.1.1. Items That Can Change Without Notification

Changes to items within this CPS which, in the judgement of the PA, have no or minimal impact on the users and cross certified CA domains using certificates and CRL's issued under this CPS, may be made with no change to the document version number and no notification to the users.

8.1.2. Changes With Notification

Changes to the certificate policy supported by this CPS as well as changes to items within this CPS which, in the judgement of the PA may have significant impact on the users and cross certified CA domains using certificates and CRL's issued under this CPS, may be made with 30 days notice to the user community and the version number of this document shall be increased accordingly.

8.1.2.1.List of Items

Any items in this CPS may be subject to the notification requirement as identified in Sections 8.1 ‘Items That Can Change Without Notification’ and ‘Changes With Notification’.

8.1.2.2.Notification Mechanism

Thirty days prior to major changes to this CPS, notification of the upcoming changes will be posted on the CommisSign CA web site and conveyed to cross-certified CA organisations via secure e-mail. The notification shall contain a statement of proposed changes; the final date for receipt of comments; and the proposed effective date of change. The PA may request CA's to notify their subscribers of the proposed changes.

8.1.2.3.Comment Period

The comment period will be 30 days unless otherwise specified. The comment period will be defined in the notification.

8.1.2.4.Mechanism To Handle Comments

Comments on proposed changes must be directed to CA Operations Authority (OA). Such communication must include a description of the change, a change justification, contact information for the person requesting the change, and signature of the person requesting the change.

The OA shall accept, accept with modifications, or reject the proposed change after completion of the comment period. OA disposition of proposed changes are reviewed with the European Commission PA. Decisions with respect to the proposed changes are at the discretion of the OA and PA.

8.1.2.5.Period For Final Change Notice

The OA determines the period for final change notice.

8.1.2.6.Items Whose Change Requires A New Policy

If a policy change is determined by the PA to warrant the issuance of a new policy, the PA may assign a new Object Identifier (OID) for the modified policy.

8.2. Publication and notification policies

The OA will publish this CPS and the Certificate Policy for the European Commission PKI on the CommisSign CA web site. It will also disseminate information via e-mail to anyone that request.

8.3. CPS approval procedures

The European Commission PA makes the determination that the CommisSign CA’s CPS complies with Certificate Policy for European Commission PKI.

9. ANNEXES

9.1. Acronyms

ARL	Authority Revocation List
CA	Certification Authority
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CUG	Closed User Group
DG	Directorate General
EC	European Commission
IDA	Interchange of Data between Administrations
LRA	Local Registration Authority
MS	Member State
PA	Policy Authority
PKI	Public Key Infrastructure
PASS	Protocol and Security Service
RA	Registration Authority
TCP/IP	Transmission Control Protocol/Internet Protocol
URL	Unified Resource Locator

9.2. Definitions

Activation Data Private data, other than keys, that are required to access cryptographic modules.

Authority Revocation List (ARL) A list of revoked CA certificates. An ARL is a CRL for CA cross certificates.

CA Administrators The CA system administrators are individuals who are responsible for maintaining the correct operation and configuration of the hardware and software for the CommisSign CA and for performing backups of the CommisSign CA system.

CA Master users The CA Master users are individuals who have the authority to generate and maintain the master key of the CommisSign CA, to change the CA server passwords and to recover CA Officers in the event they have forgotten their passwords.

CA Officers The CA Officers are individuals who are responsible for the operation and administration of the CA server and CA software.

CA Operation authority The CA Operation Authority is responsible for the establishment and administration of the CA Practice Statement and management of Master key.

Certificate The public key of a user, together with some other information, rendered unforgeable by digitally signing it with the private key of the certification authority that issued it. The certificate format is in accordance with ITU-T Recommendation X.509.

Certificate Revocation List (CRL) A list of revoked certificates that is created and signed by the same CA that issued the certificates. A certificate is added to the list if it is revoked (e.g., because of suspected key compromise). In some circumstances the CA may choose to split a CRL into a series of smaller CRLs.

Certification Authority An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.

Commission staff Commission staff are persons employed by the European Commission. They are individuals in regular salaried appointments to positions carrying duties and responsibilities within the European Commission.

Digital Signature The result of a transformation of a message by means of a cryptographic system using keys such that a person who has the initial message can determine:

(1) whether the transformation was created using the key that corresponds to the signer's key; and

(2) whether the message has been altered since the transformation was made.

Directory A directory system that conforms to the ITU-T X.500 series of Recommendations.

Employee An employee is any person employed by the European Commission.

End Entity An Entity that uses the keys and certificates created within the PKI for purposes other than the management of the aforementioned keys and certificates. An End Entity may be a Subscriber, a Relying Party.

Entity Any autonomous element within the Public Key Infrastructure. This may be a CA, a RA or an End Entity.

High-security Zone An area to which access is controlled through an entry point and limited to authorised, appropriately screened personnel and properly escorted visitors. High-Security Zones should be separated by a

perimeter. High-Security Zones are monitored 24 hours a day and 7 days a week by security staff, other personnel or electronic means.

Issuing CA In the context of a particular certificate, the issuing CA is the CA that signed and issued the certificate.

MD5 One of the message digest algorithms developed by RSA Data Security Inc.

Object Identifier (OID) The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class.

Organisation A department, agency, corporation, partnership, trust, joint venture or other association.

Operational Authority Personnel who are responsible for the overall operation of a EUROPEAN COMMISSION PKI CA. Their responsibility covers areas such as staffing, finances, and dispute resolution. The Operational Authority role does not require an account on the CA workstation.

PKI Officers Any person authorised to perform the duties defined to operate a PKI.

Public Key Infrastructure A structure of hardware, software, people, processes and policies that uses Digital Signature technology to provide Relying Parties with a verifiable association between the public component of an asymmetric key pair with a specific subscriber.

Policy Authority A European Commission body responsible for setting, implementing, and administering policy decisions regarding CP's and CPS's throughout the European Commission PKI.

Registration Authority (RA) An Entity that is responsible for the identification and authentication of certificate subscribers before certificate issuance, but does not actually sign or issue the certificates (i.e., a RA is delegated certain tasks on behalf of a CA).

Relying Party A person who uses a certificate signed by a European Commission PKI CA to authenticate a digital signature or to encrypt communications to the certificate subject, and is a subscriber of a European Commission PKI CA or a PKI which is cross certified with the European Commission PKI.

Sponsor A Sponsor in the European Commission PKI is the European Commission department or civil servant that has nominated that a specific individual or organisation be issued a certificate. (E.g., for an employee this may be the employee’s manager). The Sponsor is responsible for informing the CA or RA if the relationship with the subscriber is terminated or has changed such that the certificate should be revoked or updated.

Subscriber An individual or organisation whose public key is certified in a public key certificate. In the European Commission PKI this could be a civil servant, or a European Commission contractor. Subscribers may have one or more certificates from a specific CA associated with them; most will have at least two active certificates - one containing their Digital Signature verification key; the other containing their Confidentiality encryption key.

9.3. Reference Documents

[RD1] ICT Security Policy

[RD2] Document RFC 2527

[RD3] Regulation n°45/2001 of the European parliament and of the Council of 18 December 2000