EUROPEAN COMMISSION
DIRECTORATE-GENERAL
HUMAN RESOURCES AND SECURITY
Directorate HR.DS - Security
Information Security

CommisSign-2 PKI

Certificate Policy and Practice Statement

Version 1.0, 09/02/2018

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111

Commission européenne, 2920 Luxembourg, LUXEMBOURG - Tel. +352 43011

Contents

1. INTRODUCTION

This document is based on RFC 7382 which contains a template for a certificate practice statement. It is intended for use by the European Commission and others who need to assess the trustworthiness of the CommisSign-2 CA and determine the suitability of its certificates in meeting their requirements for electronic information security.

The following conventions mean:

- Normal font: implemented and operational,
- *Italic font*: not yet implemented, for future developments,

The European Commission has implemented 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 Authorities (CAs) – named European Commission Root CA – 2 (Subject Key Identifier: 2f a4 95 b9 10 96 e5 ba db 85 2f 17 d3 54 8c 5c db ac d3 57) and CommisSign – 2 (Subject Key Identifier: 9a fb 8f 76 66 98 dc ac 2c d7 77 36 71 6d ba e3 67 47 91 f6) – 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-2 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-2 CA Certificate Practice Statement (CPS).

1.1. Overview

This CPS describes:

- Participants
- Publication of the certificates and Certificate Revocation Lists (CRLs)
- How certificates are issued, managed, re-keyed, renewed, and revoked
- Facility management (physical security, personnel, audit, etc.)
- Key management
- Business and legal issues

This PKI encompasses several types of certificates (see [RFC6480] for more details):

- CA certificates for each organization distributing INRs and for each subscriber INR holder.

- End-entity (EE) certificates for organizations to use to validate digital signatures on PKI-signed objects (see definition in Section 1.6).

The practices in this document support the level **NCP**, unless specified otherwise.

The CommisSign-2 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 sensitive 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-2 CA domain.

Issuance of a public key certificate under any of this CPS:

- is not to be used as the sole and sufficient credential to grant access to or protect EU Classified Information (EUCI), certificates may however be used as part of the implementation of a system for the protection of EUCI, together with other measures, and upon accreditation by HR.DS.

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

Concerning the enforceability, construction, interpretation and validity of this Certificate Practice Statement and the associated Certificate Policy, the CommisSign-2 CA will be governed by European Commission regulations.

The European Commission Policy Authority (PA) 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-2 CAs operate in accordance with policies and practices defined in relevant Certification and Certificate documents. The PA is endorsed by the Information Security Steering Board.

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 a Central Registration Authority (RA) and Local Registration Authorities (LRAs) to collect information, verify identity and authorise, and request certificate management actions on behalf of their user population. The certificate delivery may be automated, provided that the

requester identity is unambiguously and securely verified against a trusted identity provider.

1.2. Document Name and 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. PKI Participants

Note that in a PKI the term "subscriber" refers to an individual or organization that is a subject of a certificate issued by a CA. Also note that, for brevity, this document always refers to PKI participants as organizations or entities, even though some of them are individuals.

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

The CommisSign-2 CA is a Certification Authority within the European Commission PKI.

1.3.1. Certification Authorities

The CommisSign-2 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-2 CA will be publicly available on an https webpage, and organisations intending to have secure exchanges with the Commission are encouraged to trust the CommisSign-2 CA.

The CommisSign-2 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. Any derogation to this practice needs to be approved by the PA.

The CommisSign-2 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 CommisSign-2 CA is responsible for:

- creation 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 CRLs;

- Running an OCSP service;
- operating the CA in accordance with this CPS;
- approving and assigning individuals to fulfil PKI related positions, an maintaining a list of the positions and roles;
- 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 or RA certificates.

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.

The CommisSign-2 CA will comply with the provisions of the applicable Commission Information and IT Security rules, all provisions in this CPS, and relevant European and national regulations.

The **CommisSign-2 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). Manual operations requiring the validation of an LRA or a RA will only be provided during Commission business hours in Brussels;
- issue certificates to the European Commission Staff, 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 CRLs on a regular schedule as per this CPS and the X.509 Certificate Policy for the European Commission PKI;
- Run an OCSP service;

- notify others (e.g. relying parties) of certificate issuance/revocation by provision of access to certificates, CRLs, in the CommisSign-2 CA repository;

- ensure awareness of and adherence to this CPS within the CommisSign-2 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-2 CA domain;

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

- report the 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-2 CA certifies it has issued a certificate to the named subscriber, that the information stated in the certificate was verified in accordance with this CPS, and the subscriber has accepted the certificate.

The CommisSign-2 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-2 CA protects its private keys in accordance with the provision of Sections 5 and 6 of this CPS.

The CommisSign-2 CA protects the private keys it holds or stores in accordance with Sections 5 and 6 of this CPS.

The CommisSign-2 CA's signing key is used for signing certificates and CRLs.

1.3.2. Registration Authorities

A Registration Authority (RA) is an entity that is responsible for the End Entity administration on behalf of the Commission CA. There is one Central Registration Authority (RA), and there are several Local Registration Authorities (LRAs) – usually at least one for each Commission department plus a backup.

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 where required;

- monitoring the system status, 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 the 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

The European Commission RA and LRAs within the CommisSign-2 CA domain are obliged 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 LRAs. 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 logs on 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 Section 3 of this CPS.

The **LRAs** are obliged to:

- verify the accuracy and authenticity of the information provided by subscribers for a certificate(the LRAs provide this verification on behalf of the CommisSign-2 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. RA and LRA private keys are delivered on smartcards and protected by a PIN code.

1.3.3. Subscribers

Subscribers use private keys issued by the CommisSign-2 CA for approved applications. Subscribers are members of Commission Staff.

A certificate may also 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 his rights to a second person as a backup.

In addition, subscribers may use certificates issued by the CommisSign-2 CA to encrypt information for, and verify the digital signatures of, other subscribers (within the CommisSign-2 CA domain as well as cross-certified domains). As such, subscribers may also be 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-2 CA.

Subscribers are obliged to:

- make true representation at all times to both the CommisSign-2 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 other electronic media depending on their local implementation;

- remove the private key support from the computer when not in use if private keys are stored on a USB key, a smart card or other removable electronic media;

- keep the private key support on their person or to store it in a secure, locked container if private keys are stored on a mobile phone, USB key, a smart card or other removable electronic media. The private key may not be accessed before authentication, either via PIN code, fingerprint authentication or password;

- protect their subscriber password, PIN code or fingerprint, according to ICT security rules;

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

- inform their local RA or helpdesk 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-2 CA and RA that any information submitted to the CA or RA is complete and accurate.

Subscribers' use of their private keys is 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.

1.3.4. Relying Parties

A Relying Party may be either a certificate subject of the CommisSign-2 CA or a subscriber of an external CA that has trusted the CommisSign-2 CA. The rights and obligations of a relying party who is a certificate subject of the CommisSign-2 CA are covered in this CPS.

In the CommisSign-2 CA domain, end entities may be both subscribers and relying parties. As relying parties, they are obliged to:

- restrict reliance on certificates issued by the CommisSign-2 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 *CRLs and/or OCSP validation*, [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-2 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 subscriber's 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-2 CA.

1.3.5. Other Participants

Not applicable.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

Some of the certificates that may be issued under this PKI could be used to support operation of this infrastructure, e.g., access control for the repository system as described in Section 2.4. Such uses also are permitted under the PKI certificate policy.

Server certificates are only for internal use within the Commission and/or the institutions (e.g. EEAS and others).

User certificates may be used inside and outside the Commission, particularly for SECEM or other email protection

Certificates and keys issued by the Commissign-2 PKI cannot be used as the only measure to protect information up to the level of **RESTREINT UE / EU RESTRICTED**

Certificate and keys issues by the Commissign-2 PKI are appropriate for the protection of sensitive non classified information (see security notices). It is recommended to apply a marking on information signed and/or encrypted with the Commissign-2 PKI.

1.4.2. Prohibited Certificate Uses

Any uses other than those described in Section 1.4.1 are prohibited.

1.5. Policy Administration

1.5.1. Organization Administering the Document

This CPS is administered by the European Commission.

Unit HR.DS.3 Information Security and EUCI
Berlaymont Building
Rue de la Loi 200
1000 Brussels
Belgium

1.5.2. HR-SECURITY-PKI-SUPPORT@ec.europa.euContact Person

The Security Directorate of the European Commission (HR.DS) administers this certification practice statement.

The contact person is Maresa MEISSL, Head of Unit HR.DS.3.

1.5.3. Person Determining CPS Suitability for the Policy

Not applicable.

1.5.4. CPS Approval Procedures

The European Commission PA makes the determination that the CommisSign-2 CA's CPS complies with Certificate Policy for European Commission PKI.

1.6. Definitions and Acronyms

1.6.1. Definitions

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

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-2 CA and for performing backups of the CommisSign-2 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-2 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.

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

Certificate Policy (CP): a CP is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements. The CP for the PKI is [RFC6484] and the ETSI NCP (normalized certificate policy) **Certification Practice Statement** (CPS): a CPS is a document that specifies the practices that a Certification Authority employs in issuing certificates.

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.

Commission staff: persons employed by the European Commission as defined in the Commission staff regulations.

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: the directory system used at the Commission.

Distribution of INRs: a process of distribution of the INRs along the respective number hierarchy. IANA distributes blocks of IP addresses and Autonomous System Numbers (ASNs) to the five Regional Internet Registries (RIRs). RIRs distribute smaller address blocks and Autonomous System Numbers to organizations within their service regions, who in turn distribute IP addresses to their customers.

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 or 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.

Internet Assigned Numbers Authority (IANA): IANA is responsible for global coordination of the Internet Protocol addressing systems and ASNs used for routing Internet traffic. IANA distributes INRs to RIRs.

Internet Number Resources (INRs): INRs are number values for three protocol parameter sets, namely:

- IP version 4 addresses,
- IP version 6 addresses, and
- Identifiers used in Internet inter-domain routing, currently Border Gateway Protocol-4 ASNs.

Internet Service Provider (ISP): an ISP is an organization managing and selling Internet services to other organizations.

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

National Internet Registry (NIR): an NIR is an organization that manages the distribution of INRs for a portion of the geopolitical area covered by a Regional Internet Registry. NIRs form an optional second tier in the tree scheme used to manage INR distribution.

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

Online Certificate Status Protocol (OCSP): The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.

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

Operational Authority: personnel who are responsible for the overall operation of an EC 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, including inter alia CA officers.

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 (PA): a European Commission body responsible for setting, implementing, and administering policy decisions regarding CPs and CPSs 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. an 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.

Regional Internet Registry (RIR): an RIR is an organization that manages the distribution of INRs for a geopolitical area.

PKI-signed object: a PKI-signed object is a digitally signed data object (other than a certificate or CRL) declared to be such an object by a Standards Track RFC. A PKI-signed object can be validated using certificates issued under this PKI. The content and format of these data constructs depend on the context in which validation of claims of current holdings of INRs takes place. Examples of these objects are repository manifests [RFC6486] and Route Origin Authorizations (ROAs) [RFC6482].

Sponsor: a Sponsor in the European Commission PKI is the EC 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.

1.6.2. Acronyms

CA	Certification Authority
CUG	Closed User Group
DG	Directorate General
EC	European Commission

HR.DS	DG HR Security Directorate
HSM	Hardware Security Module
IDA	Interchange of Data between Administrations
LRA	Local Registration Authority
MS	Member State
PA	Policy Authority
PKI	Public Key Infrastructure
RA	Registration Authority
TCP/IP	Transmission Control Protocol/Internet Protocol
URL	Unified Resource Locator

1.7. Object Identifiers

The following Object Identifiers (OIDs) have been registered for the EC PKI system.

Object description	OID
NCP policy compliance	0.4.0.2042.1.1
European Commission	1.3.130
ARES	1.3.130.0
CommisSigndocumentation	1.3.130.0.0.
CP	**1.3.130.0.0.1**
CP V1	**1.3.130.0.0.1.1**
CPS	**1.3.130.0.0.2**
CPS V1	**1.3.130.0.0.2.1**
Information systems	1.3.130.1
PKIs	**1.3.130.2**
CommisSign-2	**1.3.130.2.1**
Test	**1.3.130.2.1.9**
User certificates policy	**1.3.130.2.1.9.1**

	TLS Server authentication	**1.3.130.2.1.9.2**
	Code signing	**1.3.130.2.1.9.3**
	Function/role	**1.3.130.2.1.9.4**
Production		**1.3.130.2.1.1**
	User certificates policy	**1.3.130.2.1.1.1**
	TLS Server authentication	**1.3.130.2.1.1.2**
	Code signing	**1.3.130.2.1.1.3**
	Function/role	**1.3.130.2.1.1.4**

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

The repository for this CPS and the Certificate Policy for the European Commission is a web site that is accessible from https://commissign.pki.ec.europa.eu/info/cp/.

The repository for published certificates is the Commission LDAP and Active Directory.

The repository for the CRL is:

http://commissign.pki.ec.europa.eu/info/crl/RootCA.arl

The repository for OCSP is:

http://commissign.pki.ec.europa.eu/info/ocsp

2.2. Publication of Certification Information

The CommisSign-2 CA publishes the following:

- the CommisSign-2 root certificates on a web site;
- copies of this Certificate Policy and Practice Statement on a web site https://commissign.pki.ec.europa.eu/info/cp/;
- all public key certificates issued by the CommisSign-2 CA in the European Commission ActiveDirectory,

- the most recent CRL of user public key certificates that have been revoked by the CommisSign-2 CA on a web site: http://commissign.pki.ec.europa.eu/info/crl/RootCA.arl

2.3. Time or Frequency of Publication

The European Commission CA will publish its CRL prior to the 'NextUpdate' value in the scheduled CRL previously issued by the CA.

Certificates issued by the CommisSign-2 CA are posted to the European Commission Directory immediately upon issue. When certificates are revoked they are written in CRLs which are published in accordance with section 4.9.7. 'CRL Issuance Frequency' of this CPS.

2.4. Access Controls on Repositories

The trusted information repository is the Commission's Directory service, which is managed by DIGIT, including the access controls. The PKI system relies upon the integrity and authenticity of data from the information repository.

Certificates are available via the European Commission Directory and are read-only. Only the CommisSign-2 CA has write and delete privileges.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types of Names

The subject of each certificate issued by this organization is identified by an X.500 Distinguished Name (DN). The distinguished name will consist of a single Common Name (CN) attribute with a value generated by the European Commission.

The SubjectAlternateName (SAN) may also be specified for one or more additional fully qualified domain name(s), a contact e-mail address, or another unique identifier.

3.1.1.1.User Certificates

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:

1. the subscriber's CUID and the subscriber's Commission E-mail SMTP address are unique for the subscriber among the Commission staff;

2. 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.

3.1.1.2.Server Certificates

The Common Name (CN) is the fully qualified domain name of the server, which will be included in the certificate request.

3.1.1.3.Code-signing Certificates

The Common Name (CN) for code-signing certificates is defined by the subscriber. There are no requirements for the format or contents of the Common Name.

3.1.1.4.Functional Mailbox Certificates

The Common Name (CN) for functional mailbox certificates is provided by the subscriber, and is normally the Display Name of the functional mailbox. It follows the European Commission's naming standard for functional mailboxes.

3.1.1.5.Device Certificates

No stipulation.

3.1.2. Need for Names to Be Meaningful

The Subject name in each certificate need not be meaningful in the conventional, human-readable sense.

3.1.3. Anonymity or Pseudonymity of Subscribers

Although Subject names in certificates issued by this organization do not need to be meaningful and may appear random, anonymity is not a function of this PKI; thus, no explicit support for this feature is provided.

3.1.4. Rules for Interpreting Various Name Forms

No stipulation.

3.1.5. Uniqueness of Names

The certificate SubjectName is unique for all end entities within the CommisSign-2 CA domain. The uniqueness of the subscriber's CUID and Commission E-mail SMTP address are assured through the use of ActiveDirectory for SECEM certificates or manual checks by the RA for other certificates.

3.1.6. Recognition, Authentication, and Role of Trademarks

No stipulation.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

Proof of possession of a private key is handled automatically by the digital signature of the signing request.

3.2.2. Authentication of Organization Identity

Public key certificates are issued to individuals whenever possible. For the case of functional mailboxes where there are several individuals acting in one capacity, an encryption certificate is issued that contains the name of a functional mailbox. A signature certificate may also be issued for a functional mailbox if requested by the mailbox owner.

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 are 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).

3.2.3. 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 the latter 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.

3.2.4. Non-verified Subscriber Information

No non-verified subscriber data is included in certificates issued under this certificate policy.

3.2.5. Validation of Authority

LRAs are designated by Local Security officers in their Directorate General. Their identity is verified by the RA, and the RA maintains a list of the approved LRAs.

3.2.6. Criteria for Interoperation

The PKI is neither intended nor designed to interoperate with any other PKI.

3.3. Identification and Authentication for Re-key Requests

3.3.1. Identification and Authentication for Routine Re-key

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 Re-key is applied each time the user's certificate is no longer valid. This procedure is identical to the procedure of Initial Registration.

3.3.2. Identification and Authentication for Re-key after Revocation

For subscribers whose certificates have been revoked, they must apply the same procedure as a Routine Re-key.

3.4. Identification and Authentication for Revocation Request

Revocation is described in Section 4.9 'Certificate Revocation and Suspension' of this CPS.

4. CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

Certificate applications may be submitted by all Commission staff and by personnel of other organisations that have a specific agreement with the European Commission.

4.1.2. Enrolment Process and Responsibilities

See § 4.3.

4.2. Certificate Application Processing

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 (external or internal, as defined in the email address),
- proof of subscriber's affiliation,
- subscriber's Commission e-mail SMTP address,
- subscriber's Common User Identifier,
- information about the terms specified in this CPS.

Depending on the type of certificate requested, the request is processed after an automatic verification of the identity of the subscriber or validated manually by a RA.

4.2.1. Performing Identification and Authentication Functions

Using the information provided by the certificate requester, the RA and LRA perform identity verification according to the requirements noted in section 3.2 'Authentication of Organisation Identity' and 'Authentication of Individual Identity'.

4.2.2. Approval or Rejection of Certificate Applications

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.

4.2.3. Time to Process Certificate Applications

The RA team replies to all requests introduced by the LRA of the application within one business day.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

These procedures are described in documentation released only to Commission staff, for security reasons.

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

See 4.3.1.

4.3.3. Notification of Certificate Issuance by the CA to Other Entities

None.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

Acceptance by the subscriber of his/her responsibilities regarding certificate use is secured in the certificate request process as described in Section 4.2 of this CPS. The subscriber is informed 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 4.3 of this CPS. The operation of the secure communications protocol between the subscriber and the CommisSign-2 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.

4.4.2. Publication of the Certificate by the CA

Encryption certificates will be immediately published in the Commission directory once issued, following the procedure described in Section 4.4.1.

All other certificates are not published. They are presented by the certificate owner to Relying Parties when required.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

None.

4.5. Key Pair and Certificate Usage

A summary of the use model for the PKI is provided below.

4.5.1. Subscriber Private Key and Certificate Usage

The following use cases are supported by the system:

- Root CA
    - Signs the certificates for Issuing CAs
    - Signs the Authority Revocation List (ARL)
    - Issues certificates for Root CA administrators
- Issuing CA
    - Signs the certificates for End Entities
    - Signs the Certificate Revocation List (CRL)
    - Issues certificates for PKI trusted roles
- End Entities
    - Use of certificates for digital signature
    - Use of certificates for decryption
    - Use of certificates for authentication

4.5.2. Relying Party Public Key and Certificate Usage

The relying parties use PKI EE certificates to:

- Verify signed objects
- Encrypt messages
- Authenticate subscribers

4.6. Certificate Renewal

Certificates will not be renewed. Instead, a new certificate will be issued in accordance with the procedure described in § 4.3.

4.7. Certificate Re-key

Certificate re-key operations will be performed in accordance with the procedure described in § 4.3.

4.8. Certificate Modification

Certificates will not be modified. Instead, a new certificate will be issued in accordance with the procedure described in § 4.3.

4.9. Certificate Revocation and Suspension

4.9.1. 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 can include, but are not limited to:

- erroneous information on a certificate,
- non-acceptance by the subscriber,
- dismissal or suspension for cause,
- compromise or suspected compromise of private keys and/or user passwords and profile,
- termination of employment,
- end of service for servers, devices or functional mailboxes
- failure of the subscriber to meet their obligations under this document and relevant certificate policies.

4.9.2. 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-2 CA,
- personnel of a RA associated with the CommisSign-2 CA,
- The Director of the Security Directorate,
- L'"Autorité investi du pouvoir de nomination" (AIPN),
- the European Commission PA,
- Certificates should be revoked when persons leave the Commission. Certificate should be preferably renewed when persons change posts in the Commission.

4.9.3. Procedure for Revocation Request

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 LRA. When the RA logs on to the CA server to process the revocation, the CommisSign-2 CA will update OCSP responder and the CRL. The local RA will inform the revocation requester as soon as practicable.

Revoked certificates are published in the CRL and removed from the European Commission Directory, in accordance with Section 4.9.7 '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.

4.9.4. Revocation Request Grace Period

No stipulation.

4.9.5. Time within Which CA Must Process the Revocation Request

Revocation requests will be processed within one working day.

4.9.6. Revocation Checking Requirement for Relying Parties

A relying party is responsible for checking the certificate status with the issuer of the certificate whenever the relying party validates a certificate, either by reading the CRL or via a request to the OCSP.

4.9.7. CRL Issuance Frequency

Each CRL contains a 'nextUpdate' value, and a new CRL will be published at or before that time. The European Commission will set the 'nextUpdate' value when it issues a CRL, to signal when the next scheduled CRL will be issued.

The CommisSign-2 CA issues CRLs to the European Commission Directory every 12 hours. CRLs will also be issued between these intervals whenever a certificate is revoked.

The CRL lifetime will be set to 72 hours.

4.9.8. Maximum Latency for CRLs

A CRL will be published to the repository system within 15 minutes after generation.

4.10. Certificate Status Services

The European Commission supports the Online Certificate Status Protocol (OCSP) and issues CRLs. The URLs for the OCSP and the CRL are included in the certificates.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. Physical Controls

5.1.1. Site Location and Construction

The CommisSign-2 CA is contained in an area (the PKI room) to which access is controlled through an entry point and limited to authorised personnel.

The PKI room is has no external walls and no windows. The walls are permanent, solid walls and do not include any temporary or partition walls. The floor and ceiling are also solid.

The room has two secure doors made out of metal. One door allows entry and exit, with dual factor authentication for access. The second door is an emergency exit only.

5.1.2. Physical Access

The CommisSign-2 CA facility is locked and only authorised and appropriately screened personnel are allowed access. The PKI room is locked and electronically monitored 24 hours a day and 7 days a week. Electronic logs are maintained of physical access to the PKI room.

Only the following personnel have access to the PKI room:

- HSM Administrator
- HSM Operator
- PKI Administrator
- System Administrator (for the PKI systems)
- System Operator (for the PKI systems)

The RA systems are in the same room. The room is not shared with any other systems, and no other personnel have access to it.

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 risk of water exposure is mitigated through the installation of a false floor which raises the technical equipment above the solid floor. There are no water pipes passing over the technical room.

5.1.5. Fire Prevention and Protection

The CommisSign-2 CA facility is supplied with a fire extinguishing system in accordance with European Commission internal standards.

5.1.6. Media Storage

Storage media used by the CommisSign-2 CA are protected from environmental threats of temperature, humidity and magnetism. They are stored in the PKI room and so they are protected by the same measures as the systems.

5.1.7. Waste Disposal

Media used for the storage of information of the CommisSign-2 CA files are sanitised or destroyed in accordance with the European Commission's *Standard on Sanitisation of Media* before they are released for disposal.

Normal office waste is removed or destroyed in accordance with local European Commission rules.

5.1.8. Off-Site Backup

There is no off-site backup facility installed in 2017. A facility will be installed in 2018

5.2. Procedural Controls

5.2.1. Trusted Roles

Personnel filling these roles shall successfully complete the personal security clearance procedure for critical-sensitive positions.

5.2.1.1.CA Trusted Roles:

The Security Directorate (HR.DS) operates the CommisSign-2 CA. It plays the role of CA Operation Authority, CA officers and CA System Administrators describe below.

To ensure that one person acting alone cannot circumvent safeguards, multiple roles and individuals share responsibilities of the CommisSign-2 CA. Each account on the CommisSign-2 CA system has limited capabilities commensurate with the individual's role. The roles within the CommisSign-2 CA are:

- PKI Administrator

  PKI administrators are technical people having knowledge of PKI concepts and procedures. For business continuity there shall be (at least) two PKI administrators. Assignments of this role are made in a written form signed by the Head of Unit responsible for the PKI. System administrator role (see below) and PKI administrator roles shall be assigned to the same persons as they have similar capabilities on PKI services configuration.

  Responsibilities:

  - PKI software (OpenTrust PKI, OpenTrust CMS) installation, configuration and maintenance.
  - Certification profiles configuration
  - Roles configuration
  - Roles assignment in PKI software configuration (PMA remains administratively responsible for assignment of trusted roles. PKI admin only registers the assignment in OpenTrust configurations.)
  - Connects PKI systems to their HSMs

- System Administrators

  System administrators are technical people having knowledge of PKI concepts and procedures and of system management tasks. For business continuity there shall be (at least) two System administrators. Assignments of this role are made in a written form signed by PKI Management Authority members. System administrator role and PKI administrator roles shall be assigned to the same persons as they have similar capabilities on PKI services configuration.

Responsibilities:

System administrators are responsible for PKI systems configuration at both system and PKI software levels.

- System operator

  System operators are technical people having knowledge of system, OpenTrust operational procedures and tasks. For business continuity there shall be (at least) two System operators. Assignments of this role are made in a written form signed by PKI Management Authority members. System operator role can be assigned to the same persons as System administrator as they require similar competencies.

  Responsibilities:

  System operators are responsible for day to day operations on PKI systems: operational monitoring, backups, export/purge of audit logs etc.

5.2.1.2. RA Trusted Roles:

At least two individuals are designated as RAs, who have the authority to:

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

5.2.1.3. LRA Trusted Roles:

At least two individuals at each Commission department or autonomous entity are designated as LRAs. LRAs have the authority to:

- accept and process certificate requests,
- transmit subscriber information to the CA,
- receive subscriber authorisation information from the RA,
- verify the subscriber'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

Four Key Custodians are appointed who hold the smart cards that are required to use the RA HSM. All four are required to initialise the Root CA

(the key ceremony) or to replace a key custodian smartcard, and two are required for issuing the Authority Revocation List, revoking the issuing CA or authorising a new issuing CA.

The following tasks are defined as sensitive and require at least two individuals to perform the tasks. This is implemented as the PKI Administrator role, which requires two individuals to authenticate and therefore implements dual control.

The PKI Administrator role is required to:

- add and delete other CA Officers and RAs
- define certificate profiles

In addition, key recovery is performed by the Key Recovery Officer together with a Registration Officer.

All other tasks may be performed by a single person holding the appropriate role. A procedure may include multiple tasks that must be performed by different roles.

5.2.3. Identification and 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-2 CA system. In addition, they are entered in the CommisSign-2 CA database with their role and authorities specified. In the execution of sensitive operations, RA and LRA personnel authenticate themselves using smart card.

5.2.4. Roles Requiring Separation of Duties

The principles for the segregation of PKI roles are to:

1. Isolate from one another responsibilities for
   - configuration (e.g. roles definition and assignment),
   - service delivery, and
   - controlling or auditing.
2. Enforce (or at least facilitate) dual or multiple control during the execution of sensitive tasks (e.g. role assignment or certificate profile definition)

PKI services governance is the responsibility of the PMA. Overall PKI services configuration is the responsibility of PKI and System administrators.

The definition and assignment of roles are under the responsibility of the PKI administrators.

Service delivery is the responsibility of System Operator, Sponsor (LRA), registration officer and Key recovery Officer.

Controlling is the responsibility of PKI auditor.

Within service delivery the collaboration of sponsor and registration officer can be used to enable dual control on end entity enrolment. It is expected that multiple control on entity enrolment relies on an out-of-band procedure involving subscriber and local registration authority.

The roles and details of the segregation between them are defined in an Access Control Policy.

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

Personnel filling these roles shall successfully complete a personal security clearance procedure for sensitive positions. The following roles are deemed to be critical sensitive positions with a high risk classification:

- HSM Administrator
- HSM Operator
- Registration Officer for Authorities
- PKI Administrator
- System Administrator
- System Operator
- Registration Authority

LRAs are deemed to be critical sensitive positions with a moderate risk classification.

5.3.2. Background Check Procedures

All background checks are performed by the Security Directorate in accordance with the European Commission's 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-2 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-2 CA system. Refresher training is conducted in accordance with these changes.

5.3.5. Job Rotation Frequency and Sequence

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-2 CA or RAs, disciplinary action may be taken in accordance with the European Commission's internal rules and procedures.

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. Independent Contractor Requirements

Contractor personnel employed to operate any part of the CommisSign-2 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-2 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-2 CA provides technical help desk support for all domain users.

5.4. Audit Logging Procedures

5.4.1. Types of Events Recorded

All significant security events on the CommisSign-2 CA software are automatically time stamped and recorded in audit log files. Audit records will include the date, time, responsible user or process, and summary content data relating to the event. These include events such as:

- Access to CA computing equipment (e.g. logon, logout)

- Messages received requesting CA actions (e.g. certificate requests, certificate revocation requests, compromise notifications)

- 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 for CA Officers, RAs, and subscribers,

- Interactions with the ActiveDirectory 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, 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,

- Software and/or configuration updates to the CA

- Any attempts to change or delete audit data

- System start-up and shutdown.

- Clock adjustments

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 physical access to the CommisSign-2 CA facility.

5.4.2. Frequency of Processing Log

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

5.4.3. Retention Period for Audit Log

The audit trails are electronically retained under the CommisSign-2 CA configurations. Audit trails relating to digital certificates must be kept for at least seven years after the expiry of the certificate, in line with the

requirements for the NCP trust level. Other logs for which there is no regulatory requirement will be kept for at least 18 months.

Section 5.4.5 ‘Audit Log Backup Procedures’ describes the archive procedures for these logs.

5.4.4. Protection of Audit Log

The CommisSign-2 platform produces different audit logs:

- PKI service event logs
- Operating system logs

The PKI service logs register all certificate life cycle events (request, request approval, certificate issuance and/or revocation). They also register all PKI services configuration changes (roles and certificate profiles definitions, role assignments) and all logins to PKI services.

Operating system logs register system events like system start-up or shutdown, login attempts, execution of privileged commands.

Additionally system configuration changes are tracked by a dedicated software application and recorded in system logs.

PKI service logs are stored in the PKI services database(s). They can be viewed through PKI service web interfaces. Access to the log view facilities is granted to trusted roles, namely the PKI administrator and the PKI auditor. Registration officers or LRA may also be granted log viewing capability.

PKI service logs are signed and chained so that no entry can be altered, removed or added without the change being noticed.

Operating system logs are standard operating system logs. Access to log files is controlled through the file system. Write access is limited to privileged accounts.

Both PKI and system logs are forwarded to a central log server that keeps a reference copy of all logs. Access to that log server is granted only to system administrators.

5.4.5. Audit Log Backup Procedures

The central log server is backed up in full once a week, and an incremental backup is taken every weekday. Backups are kept for at least one month, and are held offline.

5.4.6. Audit Collection System (Internal vs. External)

The audit trail accumulation system is internal to the CommisSign-2 CA software system.

5.4.7. 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.

5.4.8. Vulnerability Assessments

A vulnerability assessment was performed during the implementation of the system. Further assessments are performed on a regular basis, at least yearly.

5.5. Records Archival

No stipulation.

5.6. Key Recovery

A key may be retrieved in three cases:

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

Examples of reasons for subscriber requested key recovery include:

- a subscriber forgets a password,
- a subscriber loses or damages a private key file,
- a subscriber requires access to information that was encrypted with a previous key.

The procedure for key recovery will be updated in a future version of this document.

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 procedure for key recovery will be updated in a future version of this document.

5.7. Key Changeover

The CA key rollover is organized in a way that is similar to the RFC 6489 procedure:

1. A new CA is created next to the current one.

2. The new CA is created with keys and a name that are different from the current CA's keys and name.

3. A transition period is organized during which the subordinates of current CA progressively migrate to the new CA (i.e. have a certificate issued by the new CA).

4. When all subordinates of the current CA have migrated to the new CA, the current CA becomes the old CA and the new CA becomes the current one.

5. The old CA keeps issuing CRLs until its expiry date (or revocation).

5.8. Compromise and Disaster Recovery

5.8.1. System Compromise

This section addresses breaches of the confidentiality or integrity of one or more components of the PKI system.

The actions to be taken depend on the component(s) of the system that is (are) compromised:

- If the OCSP or CRL are compromised, the appliance(s) or hosting server(s) will be replaced with a clean installation and a new copy of the CRL information from the issuing CA.

- If the issuing CA is compromised, it will be revoked by the Root CA and a new issuing CA will be created using the same procedure as in § 5.7, except that the compromised CA and all certificates issued will be immediately revoked.

- If the Root CA is compromised, then the entire system will be replaced. This procedure is out of scope of this CPS since a new system will be covered by a new CPS.

Any compromise will be formally investigated by the Security Directorate.

5.8.2. Disaster Recovery

This section addresses breaches of the availability of one or more components of the PKI system.

The Root CA and the Issuing CA are both backed up on a regular basis. The backups will be used to recover the systems in the event of a disaster.

If the systems hosting the OCSP or the CRL need to be recovered, they will be reinstalled and populated with data from the issuing CA.

More detailed procedures for disaster recovery will be updated in a future version of this document.

5.9. CA or RA Termination

In the event of CommisSign-2 CA termination, the European Commission PA provides oversight of the termination process. The RA and LRAs shall work with the CA to notify all subscribers of the CommisSign-2 CA cessation of operation.

All certificates issued by the CommisSign-2 CA shall be revoked.

The European Commission shall retain an archive of the CommisSign-2 CA database in accordance with the internal Security Policy and European Commission and relevant Member States regulations.

6. TECHNICAL SECURITY CONTROLS

This section describes the technical security controls used by the European Commission.

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

The CommisSign-2 CA signing key pair is created during a key ceremony. The CA signing keys are protected by an HSM. In addition, root CA keys are protected by a secret split among four persons (key custodians).

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

6.1.2. Private Key Delivery to Subscriber

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-2 CA system using a secure communications protocol.

6.1.4. CA Public Key Delivery to Relying Parties

For subscribers and relying parties within the European Commission, the CA public key is installed in the standard workstation configuration.

For external relying parties, the CommisSign-2 CA verification public key is delivered in a CA certificate using a secure procedure.

6.1.5. Key Sizes

User signing key pairs are at least 2048 bit RSA.

The CommisSign-2 CA signing key pair is at least 4096 bit RSA.

The key sizes may be increased in the future depending on the evolution of cryptographic technologies.

6.1.6. Public Key Parameter Generation and Quality Checking

No stipulation.

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

Server or device authentication key pairs are used to provide authentication and to protect symmetric keys used to protect communication sessions.

The CommisSign-2 CA signing key is used to sign certificates and CRLs issued by that CA.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

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. Cryptographic Module Standards and Controls

The cryptographic module used by the software used in the CommisSign-2 CA domain complies with FIPS 140-2 at level 3.

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

Subscribers may recover their own encryption keys with the approval of the LRA.

Multi-person control is required for the recovery of private keys by third parties (see section 5.6).

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 private keys in the root CA and the issuing CA are backed up in encrypted form on two USB drives which are held in separate secure locations.

6.2.5. Private Key Archival

No stipulation.

6.2.6. Private Key Transfer into or from a Cryptographic Module

Private keys are generated by the cryptographic modules (HSMs). On the root CA, the control over the keys can be transferred to a new HSM with the intervention of an HSM administrator and two HSM operators. On the issuing CA, this operation is performed by an HSM administrator and a PKI administrator.

6.2.7. Private Key Storage on Cryptographic Module

The private key for the European Commission production CA will be stored in the secure environment on the production CA, which is encrypted by a key held on the cryptographic module (HSM). It will be protected from unauthorised use by the physical and technical security controls described elsewhere in this document.

6.2.8. 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.

6.2.9. 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.

6.2.10. Method of Destroying Private Key

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

6.2.11. Cryptographic Module Rating

No stipulation.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

No stipulation.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

The CommisSign-2 CA public key and certificate – 10 years

The CommisSign-2 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

No stipulation.

6.4.2. Activation Data Protection

No stipulation.

6.4.3. Other Aspects of Activation Data

No stipulation.

6.5. Computer Security Controls

The workstations used for connecting to the PKI system must be on the Commission's internal network and running a European Commission reference configuration.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

No stipulation.

6.6.2. Security Management Controls

The security management controls for the CommisSign-2 CA include:

- a software utility and policies in place to control and monitor the CA system configuration;
- the CommisSign-2 CA equipment is dedicated to administering a key management infrastructure;
- the CommisSign-2 CA equipment does not have installed applications or component software, which are not part of the CA configuration; and
- the CommisSign-2 CA equipment updates are installed by trusted and trained personnel in a defined manner.

6.6.3. Life Cycle Security Controls

Equipment procurement procedures are in line with the Commission's internal procurement rules.

The CommisSign-2 CA equipment is installed, maintained and updated by or under the supervision of the PKI administrators. All changes are subject to a formal change control process.

6.7. Network Security Controls

The network zone on which the CommisSign-2 system resides is segregated from the Commission's internal network by a network firewall, and has no other connections. System administration is only performed from workstations on that network.

Remote access from outside this network zone to the CommisSign-2 CA system is limited to the RA interface and the Credential Management System, and is secured using a secure communications protocol. No other remote access is permitted and all other network ports are blocked.

6.8. Time-Stamping

The PKI does not make use of time-stamping.

7. CERTIFICATE AND CRL PROFILES

See [RFC6487].

7.1. Certificate Profile

7.1.1. Version Number

The CommisSign-2 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-2 CA security domain is generated by the CommisSign-2 CA system
signature Algorithm:	identifier for the algorithm used by the CommisSign-2 CA to sign the certificate
issuer:	certificate issuer the CommisSign-2 CA Distinguished Name
validity:	certificate validity period - notBefore start date and notAfter end date are specified
subject:	certificate subject Distinguished Name

Fields	Description
public key information:	algorithm identifier Public key
Thumbprint Algorithm:	Algorithm identifier
Thumbprint	

7.1.2. Certificate Extensions

There are no supported extensions.

7.1.3. Algorithm Object IDs

The CommisSign-2 CA supports the following algorithms:

Algorithm	Object Identifier	Issuing Authority
SHA2WithRSAEncryption	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-2 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-2 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-2 CA, is the cRLDistributionPoints extension. The CRL shall be retrieved from the CRL distribution point directory entry indicated in the certificate, unless a current copy of that CRL is cached at the subscriber's client software.]

7.2. CRL Profile

7.2.1. Version Number

CRLs issued by the CommisSign-2 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-2 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-2 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-2 CA. and the X.509 version 2 CRL and CRL entry extensions that are not supported in CRL's issued by the CommisSign-2 CA.

7.2.2.1. Supported Extensions

The following table the CRL and CRL entry extensions supported by the CommisSign-2 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
CRLNumberparticular	Non critical	Not optional	Incremented each time a CRL is changed

EXTENSION	CRITICAL /NON CRITICAL	OPTIONAL	NOTES
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 CRLs Element [1] and [2] are never present together in the same revocation list Elements [3] and [4] are not used

7.2.2.2.Unsupported Extensions

The CommisSign-2 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. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. Frequency of Compliance Audit

An audit on the CommisSign-2 CA operation is performed at least every three years, either internally or through a third party.

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

The CommisSign-2 CA reserves the right to require periodic inspections and audits of any RA facility within the CommisSign-2 CA's domain to validate that the RA is operating in accordance with the security practices and procedures laid out in this CPS.

8.2. 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.

8.3. Auditor's Relationship to Audited CA

The auditor approved by the PA and the CommisSign-2 CA are separate entities within the European Commission organisational structure

8.4. Topics Covered by Audit

The subjects of the compliance audit are the CommisSign-2 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.

8.5. 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 60 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-2 CA, including end entity 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-2 CA shall resume service and new certificates are issued to end entities.

8.6. Communication of Results

Results of the annual audit are provided to the European Commission PA, the CommisSign-2 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.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

Fees are charged to other Commission bodies and European Union institutions in accordance with the European Commission's financial procedures.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

No stipulation.

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3. Confidentiality of Business Information

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

9.3.1. Scope of Confidential Information

Each subscriber’s private signing key is treated as restricted to that subscriber. The CommisSign-2 CA and central RA have no access to these keys.

Each subscriber's confidentiality private key is treated 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 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-2 CA or RA shall be handled as sensitive non-classified information, 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 or CRL is considered as sensitive non-classified information and shall not be released unless required by law or regulation.

Audit logs will not be publicly available.

Any keys held by the CommisSign-2 CA are considered as sensitive non-classified information and shall be released only to an 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. The root CA is classified RESTREINT UE / EU RESTRICTED.

9.3.2. Information Not within the Scope of Confidential Information

Information included in public certificates and CRLs issued by the CommisSign-2 CA is considered public.

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

9.3.3. Responsibility to Protect Confidential Information

The protection of the confidential information as defined in this section is under the responsibility of the CommisSign-2 PA.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

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

9.4.2. Information Treated as Private

Each subscriber's private signing key is classified as restricted to that subscriber. The CommisSign-2 CA and central RA have no access to these keys.

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

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-2 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 or CRL is considered Restricted and shall not be released unless required by law or regulation.

9.4.3. Information Not Deemed Private

Information included in public certificates and CRLs issued by the CommisSign-2 CA are considered Public.

When a certificate is revoked by the CommisSign-2 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.

9.4.4. Responsibility to Protect Private Information

The protection of the confidential information as defined in this section is under the responsibility of the CommisSign-2 PA.

9.4.5. Notice and Consent to Use Private Information

No stipulation. No additional private information is obtained from subscribers.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

The CommisSign-2 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-2 CA.

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5. Intellectual Property Rights (if Applicable)

Certificates, CRLs and ARLs issued by the CommisSign-2 CA, the Certificate Policy for the European Commission PKI and this CPS are all property of the European Commission.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

The CommisSign-2 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.

9.6.2. Subscriber Representations and Warranties

No stipulation.

9.6.3. Relying Party Representations and Warranties

No stipulation.

9.7. Disclaimers of Warranties

The European Commission, the CommisSign-2 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-2 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 CRLs issued by the CommisSign-2 CA;

- due to disclosure of personal information contained within certificates and revocation lists.

The CommisSign-2 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.

9.8. Limitations of Liability

The European Commission, the CommisSign-2 CA, the RA and LRAs, disclaim 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-2 CA and RAs are not intermediaries to transactions between subscribers and relying parties. Claims against the CommisSign-2 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.

9.9. Indemnities

No stipulation.

9.10. Term and Termination

9.10.1. Term

The issuing CA will have a lifetime of 20 years.

9.10.2. Termination

The active issuing CA will be replaced after 10 years, and the old CA will remain valid until the end of its lifetime. An issuing CA that has been compromised will be terminated immediately, and the CA and all certificates issued by it will be immediately revoked.

9.10.3. Effect of Termination and Survival

No stipulation.

9.11. Individual Notices and Communications with Participants

No stipulation.

9.12. Amendments

9.12.1. Procedure for Amendment

This CPS shall be reviewed in its entirety whenever a relevant change is made to the system or the procedures, or after three years. Errors, updates, or suggested changes to this document shall be communicated to the contact in section 1.5.

9.12.2. 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 using certificates and CRLs issued under this CPS, may be made with no change to the document version number and no notification to the users.

9.12.3. 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 using certificates and CRLs 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.

9.12.4. Notification Mechanism and Period

Notifications shall be sent to the LRAs and publicised on the European Commission's website.

9.13. Dispute Resolution Provisions

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-2 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-2 CA OA for resolution.

9.14. Governing Law

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

9.15. Compliance with Applicable Law

The CommisSign-2 system is subject to European Commission legislation including the following:

- Commission Decision of 16 August 2006 C(2006) 3602 concerning the security of information systems used by the European Commission
- Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission
- Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

No stipulation.

9.16.2. Assignment

No stipulation.

9.16.3. Severability

No stipulation.

9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5. Force Majeure

No stipulation.