ComSign Europe Limited

(A Comda Group Company)

Certification Practice Statement (CPS)

For Electronic Certificates

Version 1.0

Dated: 23/07/2014

Table of Contents

Contents

1. INTRODUCTION

ComSign Europe Ltd. is a Certification Authority issuing qualified certificates for electronic signatures. These procedures represent the practices that ComSign Europe employs in issuing and managing certificates and the way it applies to its different Certificate Policies (CP).

These procedures can be accessed at the company's internet site www.comsigneurope.com/cps.pdf.

Any service agreement between ComSign Europe and an applicant is dependent, from a contractual perspective, on the execution by both parties of a subscriber agreement.

1.1 Overview

The electronic certificate issuing services of ComSign Europe are intended to support secure e-commerce and other electronic services, in order to provide a solution for the technical, business and personal needs of electronic signature technology-users. ComSign Europe serves as a trustworthy third party that issues, manages and revokes electronic certificates according to these procedures.

ComSign Europe acts as a certification service provider that verifies the relationship between a particular electronic signature and the signer.

The PKI that is at the basis of ComSign Europe activity as a certificate service provider outsources a separate Certificate Factory unit and an in-house infrastructure for all other services described in the CPS that are not provided by the Certificate Factory.

ComSign Europe and the parties to whom ComSign Europe may outsource services are obliged to maintain the ComSign Europe PKI Infrastructure in accordance with this CPS.

ComSign Europe is a Certification Authority in multiple hierarchies and with Registration Authorities in different modes. Notwithstanding, for the subscriber, ComSign Europe is the sole Certificate Service Provider (CSP).

The certificate issuance services include application, proper identification of the applicant, issuing and revoking certificates, and documenting the actions taken by ComSign Europe, the RAs and other sub-contractors.

The certificates issued within the ComSign Europe PKI hierarchy provide multiple levels of assurance. Except for the "Qualified" hierarchy that has the purpose to facilitate Qualified Electronic Signatures in accordance with the Directive 1999/93/EC, the assurance level is determined by the CP.

1.2 Document name and identification

Certification Practice Statement (CPS) v1.0

The version number appears left to the decimal point. The sub-version number appears right to the decimal point and represents the number of the updated version. Amendments that represent a fundamental change in the service and/or processes associated with it will require a change of version instead of an update.

Current and past CPS can be found in ComSign Europe's repository.

1.3 PKI Participants

1.3.1 **Certification Authorities**

ComSign Europe is the only Certification Authority (CA) within the scope of these procedures. ComSign Europe reserves the right to establish additional CA's.

1.3.2 **Registration Authorities**

The certificate issuance services of ComSign Europe are managed in a manner that allows the services related to applications for the issuance of electronic certificates, identification and registration of applicants to be handled by a Registration Authority. Resellers and Registration Authorities (RAs) cannot issue certificates on behalf of any public CA under this CPS. The Registration Authority is obligated to this CPS and instructions issued by the CA. The Registration Authority is hierarchically subordinated to the CA. This ensures that the uniformity of the certificate issuance services provided by the CA and its representatives is maintained. The RA is further obliged: (a) to represent accurately the information it prepares for a CA; (b) to (depending on the CP) keep, for up to 30 years after the expiry of the last certificate, supporting evidence for any certificate request made to a CA (e.g., certificate request forms). In particular, archived copies of all information used to verify the identity of the certificate holder and any references to his professional status, including any reference numbers on the documentation submitted for verification, and any limitations of its validity together with a copy of the subscriber agreement signed by the subscriber, including all obligations incumbent on him, and (c) in the case of an external RA, to maintain all undertakings as per the contractual agreement entered between ComSign Europe and the external RA.

The RA is responsible to receive certificate applicants, complete the form containing details of certificate applicants, confirm and verify the identity of the certificate applicants, implement the process of issuing the certificate and, after issuance, verify that it functions properly. Subsequently, receive payment and issue the invoice and receipt. If the certificate is to be revoked, confirm the identity of the person requesting the revocation, and revoke the certificate. See section 9.6.2.

1.3.3 **Subscribers**

Subscribers can be a physical person, acting in its private capacity, an authorized representative of another individual and an authorized representative of a corporation

or organization or legal entity. Both the subscriber and the body it represents must be identified in accordance with the applicable CP.

A subscriber may also be any corporation, organization, legal entity, a device, an address or a service, which can be identified in accordance with the relevant CP.

1.3.4 **Relying Parties**

Any party relying on the data certified in the certificates is considered a relying party. The responsibility of the CSP towards the relying parties is limited in accordance with these procedures, the provisions in the CP and/or the terms stated in the certificate. The CSP does not grant any representation on the ability of the applications to apply the certificates and the services to any particular use. Neither does the CSP guarantee that these applications will make correct use of the certificates. The responsibility to ensure the correct use and ability to use the certificates rests entirely with those entities responsible for the applications.

1.3.5 **Other Participants**

Other participants within the PKI infrastructure may include:

A. The Certificate Service Provider (CSP). ComSign Europe acts as the Certificate Service Provider (CSP) with authority to outsource different services and tasks to other parties.

B. The Subject. The Subject is the entity which is certified by the certificates. As such the subject may be a participant. The subject may be the subscriber or somebody or some entity associated with the subscriber.

C. The Subject Device Provision Service. A participant, with a distinct responsibility, that can be an outsourced partner of the CSP is the subject device provision service. This participant is responsible to handle and manage the devices that store private keys of certificates (generally called "private key holding devices"). In particular, secure tokens, smart cards, SCDs, Secure User Devices (SUDs), or SSCDs can be subject to the management of this participant. The main role of this participant is to handle the life cycle of these tokens according to the provisions of this CPS.

D. The Policy Approval Council. The Policy Approval Council of ComSign Europe is a high-level management body named CEPAC (ComSign Europe Policy Approval Council) with the authority and responsibility for specifying and approving the ComSign Europe trusted service provider (TSP) services, policies and practices; approving the Certification Practice Statement(s), Certificate Policies, Signing Policies, Time-stamping Policies and other TSP related documents or decisions which have an impact on the responsibility and/or liability of ComSign Europe as a trusted service provider; defining the review process including responsibilities for maintaining the policies; defining the review process that ensures that the certificate practices are properly implemented by the Certification Authorities (CAs), PKI participants, signing

authority, time-stamping authorities (TSA) etc.; defining the review and audit process that ensures that the trusted roles and authorities are compliant with and act in accordance with the policies; publishing the policies and their revisions to the subscribers and relying parties; and specifying cross-certification procedures and handling cross-certification requests.

1.4 Certificate Usage

1.4.1 **Appropriate certificate uses**

Appropriate certificate usages are listed either in the certificate or in the relevant CP or CPs referred to in these certificates.

1.4.2 **Prohibited certificate usages**

Prohibited certificate usages are all those that are not explicitly listed in the authorized certificate usages list.

1.5 Policy administration

1.5.1 **Organization administering the document**

The CEPAC is the organization administering this document.

1.5.2 **Contact person**

All questions and comments concerning this CPS must be addressed to:
ComSign Europe Policy Approval Council c/o Chief Technical Officer
(CTO) Longcroft House 2/8 Victoria Avenue
Bishopgate, London EC2M 4NS England
www.comsigneurope.
info@comsigneurope.

1.5.3 **Person determining the CPS suitability for the policy**

The CEPAC is responsible for determining: (a) a risk assessment policy and initiating audits that shall be carried out to evaluate business requirements and determine the security requirements with respect to this CPS; (b) the ComSign Europe's CPS suitability to any ComSign Europe CP and (c) issuing the CPs, determining their suitability to the CPS and authorize RAs to register certificate requests and CAs to issue certificates under a particular ComSign Europe CP and this CPS.

1.5.4 **CPS approval procedures**

For the CPS:

Only editorial, typographical corrections or changes to the contact details can be made without notification. All other changes, including errors, updates or other

suggested changes must first be approved by CEPAC and inserted in an updated version of this document carrying a new OID. The date of publication and the effective date shall be indicated on the title page of the CPS/CP. See section 9.12.3.

For Definitions and Acronyms:

No additions or modifications are allowed that create ambiguity with regard to existing definitions and acronyms. Additions and modifications are accepted, modified or rejected by CEPAC. The latest and most up-to-date version is published.

1.6 Definitions and acronyms

In these Procedures, the terms listed below will have the meanings stated beside them:

The Procedures or **these Procedures**	The procedures described below that regulate the activities of ComSign Europe as a Certification Authority. These procedures apply only to the electronic certificates (as defined below).
Application	The process by which the applicant (as defined below) requests the issuance of an electronic certificate.
Applicant or **Subscriber**	A person or a corporation or a public institution that submits a request for issuing an electronic certificate.
Certificate owner	An applicant to whom an electronic certificate was issued.
Comsign Europe Repository	The ComSign Europe database that contains publicly accessible information including, but not limited to, this CPS and the list of revoked electronic certificates, as published on the ComSign Internet site. The ComSign Europe Repository also includes additional information that is not accessible to the public, for example, the list of valid certificates.
Electronic Identification	the process of using person identification data in electronic form that unambiguously represents a natural or legal person
Electronic Identification Means	a material or immaterial unit containing data, and which is used to access services online
Electronic Identification Scheme	a system for electronic identification under which electronic identification means are issued to persons

Authentication	an electronic process that allows the validation of the electronic identification of a natural or legal person; or authentication of the origin and integrity of an electronic data a natural person who creates an electronic signature
Signatory	
Electronic Signature	data in electronic form which are attached to or logically associated with other electronic data and which are used by the signatory to sign
Advanced Electronic Signature	an electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using electronic signature creation data that the signatory can, with high level of confidence, use under his sole control; and (d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable
Qualified Electronic Signature	an advanced electronic signature which is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures
Electronic Signature Creation Data	unique data which are used by the signatory to create an electronic signature
Certificate	an electronic attestation which links electronic signature or seal validation data of a natural or a legal person respectively to the certificate and confirms those data of that person
Qualified Certificate for Electronic Signature	an attestation which is used to support electronic signatures, is issued by a qualified trust service provider and meets the requirements laid down in Directive 1999/93/CE as well as any future relevant legislation replacing it.
Trust Service	any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals
Trust Service Provider	means a natural or a legal person who provides one or more trust services
Qualified Trust Service Provider	a trust service provider who meets the requirements laid down in Directive 1999/93/CE as well as in any future relevant legislation replacing it

Product	hardware or software, or relevant components thereof, which are intended to be used for the provision of trust services
Electronic Signature Creation Device	electronic signature creation device means configured software or hardware used to create an electronic signature
Qualified Electronic Signature Creation Device	an electronic signature creation device which meets the requirements laid down in Directive 1999/93/CE as well as in any future relevant legislation replacing it
Creator of a Seal	a legal person who creates an electronic seal
Electronic Seal	data in electronic form which are attached to or logically associated with other electronic data to ensure the origin and the integrity of the associated data
Advanced Electronic Seal	an electronic seal which meets the following requirements: (a) it is uniquely linked to the creator of the seal; (b) it is capable of identifying the creator of the seal; (c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and (d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable
Qualified Electronic Seal	an advanced electronic seal which is created by a qualified electronic seal creation device, and which is based on a qualified certificate for electronic seal
Electronic Seal Creation Data	unique data which are used by the creator of the electronic seal to create an electronic seal
Qualified Certificate for Electronic Seal	an attestation which is used to support an electronic seal, is issued by a qualified trust service provider and meets the requirements laid down in Directive 1999/93/CE as well as in any future relevant legislation replacing it
Electronic Time Stamp	electronic time stamp means data in electronic form which binds other electronic data to a particular time thus establishing evidence that these data existed at that time
Qualified Electronic Time Stamp	an electronic time stamp which meets the requirements laid down in Directive 1999/93/CE as well as in any future relevant legislation replacing it
Electronic Document	a document in any electronic format
Qualified Certificate for Website Authentication	an attestation issued by a qualified trust service provider which makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued, and meets the requirements laid down in Directive 1999/93/CE as well as in any future relevant legislation replacing it

Validation Data	data which are used to validate an electronic signature or an electronic seal
Relying Party	A third party who receives a message signed with an electronic signature and who takes or refrains from action on the basis of the electronic signature and/or on information found in ComSign Europe's Repository
Registration Authority	An internal or external party that was appointed by ComSign Europe as a Registration Authority for the purpose of registering and identifying applicants and handling applications for the issuance and/or revocation of electronic certificates
Revoked certificate	A certificate listed in the certificates revocation list (CRL) in the ComSign Europe Repository.
Valid certificate	A certificate listed in the list of valid certificates in the ComSign Europe Repository.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

The following describes the ways in which ComSign Europe publishes relevant information to the public, to relying parties, certificate owners and applicants, the publishing frequency and methods of access. Publication is provided either directly by ComSign Europe or outsourced.

2.1 Repositories

ComSign Europe manages a collection of databases designed for storage and retrieval of certificate and other relevant information. Together they are known as the "Repository." ComSign Europe's Repository includes, *inter alia*, the following: a database of valid electronic certificates (including ComSign Europe's root certificates), a database of revoked certificates, additional information regarding the revocation of certificates and lists of revoked certificates, and other information as decided by CEPAC from time to time.
Only part of the information published in ComSign Europe's Repository is accessible for the public view. The list of revoked certificates containing their serial number and date of revocation is accessible for controlled viewing.

2.2 Publication of certification information

CAs within the ComSign Europe PKI shall make publicly available, in their repositories: The CPS; The list of Definitions and Acronyms; The publically applicable CPs under which certificates are issued according to this CPS; Certification Revocation Lists (CRL); Authority Revocation Lists (ARL); All CA certificates issued by the CA, self-signed CA certificates and cross certificates for cross certified CAs (if exist); subscriber agreements;

Certificates issued by the CA in conformance with this CPS but only if so stipulated in the CP referred to in the certificates. In case such end-entity certificates are published, publication of these certificates is subject to permission by the certificate holder or subscriber. The CP can state that the acceptance of a certificate implicitly acknowledges and confirms the correctness of the data certified in the certificate.

ComSign Europe shall provide relevant information about issued certificates when necessary to aid in dispute resolution concerning, for example, electronic signatures.

CRL's shall contain revocation status information about all revoked and suspended certificates, during the lifetime of the appropriate CA certificate.

2.3 Time or frequency of publication

CPS publication shall be in accordance with the CPS change procedures.
CRL publication shall be no later than every 12 hours or immediately after a certificate is revoked, whichever is earlier. The published list of revoked certificates is valid for 24 hours.
In order to remove any doubt, the updated and valid list of revoked certificates is the one that appears in the ComSign Europe repository. A relying party must conduct a new, online check of the database of revoked certificates every time that it wishes to rely on a certificate in order to ensure that he/she is checking the certificate against the most recently updated list of revoked certificates.

2.4 Access controls on repositories

There is free access to the ComSign Europe repository of revoked certificates, CPSs and certain CPs on the Internet at the address appearing on the certificate and using other methods of communication, as determined by the CA from time to time. Access controls access to certificates are optional at the discretion of the CA and may be part of a specific rule of a particular CP.

The documents stored at the repository and accessible to the public are protected against unauthorized modifications.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

The name of the owner is specified on the certificate in accordance with the X.509 standard. It is possible to issue several certificates for **different** authorized signatories of the same applicant corporation and/or organization, as long as they are issued in accordance with this CPS and the applicable CP. It is possible to issue several electronic certificates to the same applicant.

3.1.2 Need for names to be meaningful

In case of the use of pseudonyms, organization and corporation names and the like, the name listed in the certificate must be meaningful in the sense that they can be associated with a name of a natural or legal person thus avoiding and/or limiting possible errors.

3.1.3 Anonymity or pseudonymity of subscribers

The use of a pseudonym is allowed by ComSign Europe CSP, but only in addition to other attributes and in conformance with the CP, allowing adequate identification and authentication and limiting future misunderstandings and errors concerning the identity of the subscriber.

3.1.4 Rules for interpreting various name forms

This is determined in the CP.

3.1.5 Uniqueness of names

The rules for the uniqueness of names are determined in the CP.

3.1.6 Recognition, authentication, and role of trademarks

ComSign Europe cannot guarantee that the names issued in the certificates will include the trademark requested by the subscriber. No RA or CA within the ComSign Europe infrastructure is obliged to perform any trademark infringement investigation at the time the Naming information is provided by an entity. ComSign Europe is not liable for any trademark infringement by a Subscriber or a third party.

The applicants and certificate owners warrant to ComSign Europe that their use of the details that appear on the application do not impair or violate the rights of any third party, in any jurisdiction, in respect of their trademarks, service marks, trade names or any other intellectual property. That they are not attempting to use any of

the details appearing on the certificate application for any illegal purpose including, but not limited to, causing a breach of contract, or other illegal intervention in contractual relationships, unfair competition, damage to the reputation of another and misleading any person, corporation or legal entity.

ComSign Europe shall not be held responsible for the legality, adequacy and correctness of the information that a certificate owner provided to ComSign Europe or to its repository.

It is the sole responsibility and liability of the subscriber and/or certificate owner that the information provided does not violate any rule of law in any jurisdiction where the content of the certificate or the repository may be used or viewed. Therefore, applicants and certificate owners must be aware of the existence of various laws regarding data transfer, and especially encrypted data or data that includes encryption algorithms, and that these laws may be significantly different in different countries and states. Furthermore, in most cases it is not possible to limit the distribution of content via the Internet or certain other networks based on the location of the user/viewer, which may require applicants and certificate owners to obey the laws of any jurisdiction where the content may be viewed or used.

In case of any name claim dispute, the claimant will contact ComSign Europe Certificate Services (see contact information in section 1.5.2). ComSign Europe will investigate the grounds on which the name claim dispute is based. Any entity acting within the ComSign Europe PKI Infrastructure is obliged to give appropriate and sufficient co-operation to an investigation mentioned in this section. In case the name claim dispute is due to an error of ComSign Europe, ComSign Europe will undertake immediate action, free of charge, to solve the problem. In case the name claim dispute is due to negligence or malicious actions of a Subscriber or a Relying Party, ComSign Europe reserves the right to terminate the contractual relationship immediately, to revoke the certificate and to refuse to continue any collaboration with that person. ComSign Europe further reserves the right to undertake legal actions and collect costs and expenses.

3.2 Initial identity validation

3.2.1 **Method to prove possession of private key**

Whether this is required is determined in the CP. In general the following situations may occur: (a) The private key is generated in a secure token or in a SSCD provided by ComSign Europe or which is already in the possession and under the sole control of the subject; (b) The private key is generated on a server at the subscribers premises; (c) The private key is generated, with the physical presence of a ComSign Europe representative, on a secure HSM at the subscriber's premises; (d) The private key is generated centrally by ComSign Europe in a secure environment and transferred securely to the subject; (e) The private key is generated centrally by ComSign Europe in a secure environment and transferred securely to the subject where it is injected securely in a secure token which is under the sole control of the subject; (f) The private key is generated in a token which is not yet in the possession of the subject.

Where applicable, all certificate requests must be signed by the subscriber using the Private Key that corresponds to the Public Key in the request (e.g. using PKCS#10 standards). This will enable the RA to verify the user's Private Key possession.

Other requirements may be that the origin of the request itself (namely a particular secure token or SSCD) is authenticated as well by the RA prior to generating the Private Key.

The methods employed to achieve the above objectives are described in internal documents, which can be made available to auditors or other parties after the approval of CEPAC and under the conditions defined by CEPAC (such as the signing of a Non-Disclosure Agreement).

3.2.2 **Authentication of organization identity**

The RAs within the ComSign Europe PKI Infrastructure are obliged to undertake the procedures set forth in the relevant CP and in the appropriate internal documents in order to authenticate the organization identity.

The authentication of an organization identity will require the appropriate documents as specified in the applicable CP (see relevant CP for details).

3.2.3 **Authentication of individual identity**

The RA within the ComSign Europe PKI Infrastructure is obliged to undertake the procedures as set forth in the relevant CP and in the appropriate internal documents in order to authenticate the identity of the applicant.

The authentication of an individual entity will require the appropriate documents as specified in the applicable CP (see relevant CP for details).

3.2.4 **Non-verified subscriber information**

The RA within the ComSign Europe PKI Infrastructure is obliged to undertake the procedures as set forth in the relevant CP. As a rule, non-verified information shall not be certified.

3.2.5 **Validation of authority**

The RA within the ComSign Europe PKI Infrastructure is obliged to undertake the procedures as set forth in the relevant CP.

If applicable, the application should include the authorization from a legal representative (or an authorized person) of the organization that the applicant can obtain and use the requested professional identity.

3.2.6 **Criteria for interoperation**

Not applicable.

3.3 Identification and authentication for re-key requests

3.3.1 **Identification and authentication for routine re-key**

This must be on the same level of trust as the initial identity validation. The re-key request that contains the new key may be signed using the current valid key and make use of the data based on the original verification.

3.3.2 **Identification and authentication for re-key after revocation**

This requires a process that gives the same level of assurance as the one used for the initial registration.

3.4 Identification and authentication for revocation request

The initiator of a revocation request should be sufficiently authenticated and authorized to demand the revocation in order to reduce the risk of wrongful revocation.

The methods employed to achieve the above objectives are described in internal documents, which can be made available to auditors or other parties after the approval of CEPAC and under the conditions defined by CEPAC's internal documents (such as the signing of a Non-Disclosure Agreement).

3.5 Identification and authentication of the Applicant's e-mail address

The RA within the ComSign Europe PKI Infrastructure is obliged to undertake the procedures as set forth in the relevant CP and in the appropriate internal documents in order to verify and authenticate the applicant's e-mail address.

The verification and authentication of the e-mail address will require an appropriate procedure as specified in the relevant CP.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 **Who can submit a certificate application**

The CP determines who can submit a certificate application. There are different permitted methods of enrollment depending on the identity of the applicant. Typically, the following may apply for a certificate application: (a) The future certificate holder or subject; (b) An RA or LRA; (c) An authorized personal

representative of the subscriber organization; (d) Authorized systems of the subscriber organization

4.1.2 **Enrollment process and responsibilities**

The enrollment process can be initiated in several ways: (a) Before submitting the actual application, ComSign Europe, either directly or by one of its appointed representatives as well as in its web site, can provide instructions regarding the process and the required documentations. (b) The applicant is authorized by the appropriate persons or services to apply for certain certificates. This requires the existence of a contractual agreement between ComSign Europe and the subscriber organization (to which the authorized persons or services belong) that stipulates the rights and constraints of the subscriber organization to appoint/authorize subjects. (c) An individual submits a request in his/her own name. This requires the existence of a contractual agreement between ComSign Europe and the individual requestor before the enrollment process can proceed.

Following the initiation of the enrollment process, the actual certificate application must be submitted. The CP can limit by whom and in what way this takes place. If the RA or LRA does not submit the certificate application, either after reception from another participant or by their own initiative, the RA or LRA needs to establish a process and/or procedure for the applicant to submit their application. The procedures are described in the applicable contractual agreement (e.g. purchase order, subscriber agreement, and CP).

The RA or LRA is responsible to take all measures to ensure that the application is accurate. Subscribers are obliged to give accurate and complete information to the certification service provider (CA, RA) in accordance with the related CP, particularly concerning registration. A valid approach of how this can be achieved is described in internal documents, which can be made available to auditors or other parties after the approval of CEPAC and under the conditions defined by CEPAC (such as the signing of a Non-Disclosure Agreement).

Based on the application and depending on the applicable CP the key pair will be generated by the applicant or the CSP: (a) In case the applicant generates the key pair, an electronic certificate request will be provided during application. (b) In case the CSP (e.g. at RA premises) generates the key pair, measures will be taken to protect the private key during its transfer to the certificate holder.

The applicant will accept the applicable contractual agreement (purchase order, subscriber agreement, and CP) assuring that the information provided earlier is correct. Herewith the applicant will also authorize the creation and the publication of the issued certificate in the ComSign Europe certificate public registry if this is in accordance with the CP.

4.2 Certificate application processing

4.2.1 **Performing identification and authentication functions**

The application must be strongly authenticated. This can happen either explicitly or implicitly. A valid approach of how application processing can be achieved is described in internal documents, which can be made available to auditors or other

parties after the approval of CEPAC and under the conditions defined by CEPAC (such as the signing of a Non-Disclosure Agreement).

4.2.2 **Approval or rejection of certificate applications**

Applications can be based on accurate information sources. However, these must be verified by the applicant and then accepted or rejected. When certificate applications are made in accordance with this CPS and the applicable CP, the approval is by default and without further delays.

4.2.3 **Time to process certificate application**

Whenever possible, certificate applications shall be processed on a continuous basis with the aim to complete the process as quickly as reasonably possible. However, in the event of delay or need to complete data, documents, authorizations and the like, as well as in the event technical issues may prolong the processing, a time limit is set in the appropriate CP and the passing of that limit will require the initialization of the application process in ensure the correctness of the data.

4.3 Certificate issuance

4.3.1 **CA actions during certificate issuance**

Unless otherwise provided in the applicable CP, the issuing CA performs certificate issuance and for this ensures that new certificates are issued securely.

The process of issuing the certificates is securely linked to the associated registration, the certificate rekey, renewal or recertification. In particular, as part of certificate issuance by the issuing CA, the following procedures have to be followed: (a) The RA must compare the electronic information provided by the applicant to the information presented in the signed contractual agreement in case a separate contractual agreement is signed. The information provided in the signed contractual agreement prevails over the electronic information. (b) The RA sends the request securely to the CA. (c) The certificate holder or the authorized person (if this is allowed by the CP) verifies and approves the information to be certified. (d) If the applicant performs the key generation, the RA checks the self-signed request (e.g., PKCS#10 request). If the issuing CA (CSP) generates the subscriber's private key, then it is securely transferred to the applicant in accordance with the CP. (e) The CA will generate the certificate and publish it in the ComSign Europe Certificate Public Registry if this is in accordance with the CP. Certificates are generated and issued in accordance with the applicable laws and regulations. (f) The certificate is sent directly to the applicant. (g) An audit trail is created of all the requests and the resulting generations of certificates. (h) The RA archives all the information in accordance with the CP.

4.3.2 **Notification to subscriber by the CA of issuance of certificate**

The subscriber can be notified by the CA that the certificate was issued.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The certificate is deemed to have been accepted by default if the certificate was created as a result of an issuance process triggered by the applicant. During that issuance process, the subscriber is asked to verify the accuracy and correctness of the content of his/her certificate. In case of reported inconsistencies, the issuance process will be halted or the data will be corrected. This will be the subscriber's sole remedy for any acceptance refusal.

In case the subject or the subscriber wants to revoke this acceptance, certificate revocation may still be used but the provisions of certificate revocation will apply.

4.4.2 Publication of the certificate by the CA

Whether or not the certificate is published and where it is published is determined in the CP.

4.4.3 Notification of certificate issuance by the CA to other entities

Whether or not notification of certificate issuance to other entities takes place and which entities are involved is determined in the CP.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The subscriber private key and certificate usage appropriate use of the private key and certificate is determined by the CP.

4.5.2 Relying party public key and certificate usage

Appropriate use of the private key and certificate is determined by the CP.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

A precondition for renewal is that the CP must allow this. Certificate renewal is considered as a new certificate application with the exception that a previously certified public key and the corresponding private key is reused and all the certified data, including the CP, is still valid. No certificate renewal may take place after certificate revocation due to the risk of key compromise. It also has to be ensured that there are no changes in the certified data (except for the validity period), the trust chain or the CP. If evolutions in technology or other conditions with the same effect require the CSP to change the cryptographic key lengths and algorithms, the CP must be modified and therefore certificate renewal is not allowed. Furthermore, the subscriber must still have a contractual agreement with ComSign Europe that is valid in the new validity period of the certificate or must agree to a new one that covers the extended period. The new validity period must be in accordance with the CP, which

can impose limitations of maximum validity. If these conditions are met, renewal can take place prior to the expiration period of the current certificate. A condition to the use of the new certificate is the revocation of the old certificate.

4.6.2 **Who may request renewal**

The CP determines who may request renewal (if this is allowed).

4.6.3 **Processing certificate renewal requests**

In addition to a voluntary renewal request by the subscriber, renewal may be initiated based on a rule preconfigured by the CSP and agreed on in an agreement with ComSign Europe. All renewals are subject to the existence of an agreement between ComSign Europe and the subscriber that future purchases may be made by the subscriber to renew the certificate.

The RA is responsible to ensure that the conditions for renewal are met.

A valid approach of how this can be achieved is described in internal documents, which can be made available to auditors or other parties after the approval of CEPAC and under the conditions defined by CEPAC (such as the signing of a NonDisclosure Agreement).

4.6.4 **Notification of new certificate issuance to subscriber**

The subscriber can be notified of renewed certificate issuance.

4.6.5 **Conduct constituting acceptance of a re-keyed certificate**

Since the renewal of the certificate is requested and in some cases also initiated by the subscriber, acceptance is deemed to be by default, after the certificate holder or the authorized person (if this is allowed by the CP) verifies and approves the information to be certified.

4.6.6 **Publication of the re-keyed certificate by the CA**

Whether or not the certificate is published and where it is published is determined in the CP.

4.6.7 **Notification of certificate issuance by the CA to other entities**

Whether or not notification of certificate issuance to other entities takes place and which entities are involved is determined in the CP.

4.7 Certificate re-key

4.7.1 **Circumstance for certificate re-key**

A precondition for re-key is that the CP must allow this. Any change in the certified data (including the CP) and the CA hierarchy, any action or event (such as certificate

expiration or revocation), any evolution which necessitates a new key length and/or algorithm change can be a circumstance for certificate re-key. Furthermore, the subscriber must still have a contractual agreement with ComSign Europe that is valid in the new validity period of the certificate or must agree to a new one that covers the new period. The new validity period must be in accordance with the CP, which can impose limitations on maximum validity. If these conditions are met, re-key can take place whenever a new certificate is needed due to the invalidity of the previous certificate. If this is allowed by the CP and the conditions for such an action are met, certificate renewal or certificate modification with re-certification can be alternatives for a re-key.

4.7.2 **Who may request certification of a new public key**

The CP determines who may request certification of a new public key.

4.7.3 **Processing certificate re-keying requests**

Certificate re-keying may be initiated based on a rule preconfigured by the CSP and agreed on in an agreement with ComSign Europe. All re-keyes are subject to the existence of an agreement between ComSign Europe and the subscriber that future purchases may be made by the subscriber to re-key the certificate.

The RA is responsible to ensure that the conditions for re-keying are met.

A valid approach of how this can be achieved is described in internal documents, which can be made available to auditors or other parties after the approval of CEPAC and under the conditions defined by CEPAC (such as the signing of a NonDisclosure Agreement).

4.7.4 **Notification of new certificate issuance to subscriber**

The subscriber can be notified of the new certificate issuance by means of reporting.

4.7.5 **Conduct constituting acceptance of a re-keyed certificate**

Since the re-key of the certificate is requested and in some cases also initiated by the subscriber, acceptance is deemed to be by default, after the certificate holder or the authorized person (if this is allowed by the CP) verifies and approves the information to be certified.

4.7.6 **Publication of the re-keyed certificate by the CA**

Whether or not the certificate is published and where it is published is determined in the CP.

4.7.7 **Notification of certificate issuance by the CA to other entities**

Whether or not notification of certificate issuance to other entities takes place and which entities are involved is determined in the CP.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

A precondition for certificate modification is that the CP must allow this. Certificate modification always entails re-certification, employing a process similar to the "Initial identity validation" for the modified information. Certificate modification is considered a new certificate application with the exception that a previous key pair can be reused. Certificate modification cannot take place after certificate revocation.

Any change in the certified data (including the CP) and the CA hierarchy, other than a change that requires certificate revocation, may require certificate modification. Furthermore, the subscriber must be under a valid contractual agreement with ComSign Europe for the entire validity period of the certificate or must agree to a new one that covers the new period. The new validity period must be in accordance with the CP, which can impose limitations of maximum validity. If these conditions are met, modification can take place whenever a new certificate is needed due to the invalidity of the previous certificate. It must be assured that the previous certificates must be revoked.

4.8.2 Who may request certificate modification

The CP determines who may request a permitted certificate modification.

4.8.3 Processing certificate modification requests

Certificate modification may be initiated based on a rule preconfigured by the CSP and agreed on in an agreement with ComSign Europe. All modifications are subject to the existence of an agreement between ComSign Europe and the subscriber that future purchases may be made by the subscriber to modify the certificate. The RA is responsible to ensure that the conditions for modifications are met. A valid approach of how this can be achieved is described in internal documents, which can be made available to auditors or other parties after the approval of CEPAC and under the conditions defined by CEPAC (such as the signing of a Non-Disclosure Agreement).

4.8.4 Notification of new certificate issuance to subscriber

The subscriber can be notified of the new certificate issuance.

4.8.5 Conduct constituting acceptance of modified certificate

Since the modification of the certificate is requested and in some cases also initiated by the subscriber, acceptance is deemed to be by default, after the certificate holder or the authorized person (if this is allowed by the CP) verifies and approves the (new) information to be certified.

4.8.6 **Publication of the modified certificate by the CA**

Whether or not the certificate is published and where it is published is determined in the CP.

4.8.7 **Notification of certificate issuance by the CA to other entities**

Whether or not notification of certificate issuance to other entities takes place and which entities are involved is determined in the CP.

4.9 Certificate revocation and suspension

4.9.1 **Circumstances for revocation**

A valid (unexpired) certificate must be revoked if: (a) The certified information is not valid any more or the content has changed (including the demise or dissolution of the subject); (b) There is a significant risk of private key compromise or the private key has already been compromised [Note: previous certificates of the same key that have not expired and have not yet been revoked must also be revoked in this case]; (c) The security of algorithms and key lengths employed in the certificate are, or will shortly become, below the standard of acceptability; (d) The certificate has been issued based on wrong or falsified information; (e) The subscriber has violated or otherwise ended the contractual provisions and agreement; (f) The certified entity does not exist anymore as an entity associated with the subscriber; (g) The CA stops its activities without another CA taking over its activities; (h) The issuing CA certificate's private key has been compromised.

4.9.2 **Who can request revocation**

The main responsibility lies with either the certificate holder (subject) or the authorized person of the subscriber's organization. These persons can also be considered certificate holders, for example in the case of a non-personal certificate or a certificate that does not identify a physical person in the certificate's subject.

If the subject is a physical person certified as belonging to an organization and this organization is the subscriber, then an authorized person of the subscriber's organization has the responsibility to request revocation in case the certified person is leaving the organization.

Depending on the circumstances leading to the revocation, the revocation request can also be made by an RA or LRA having taken part in the registration of the concerned certificate, the CSP (represented by the ComSign Europe Policy Approval Council (CEPAC)), an authorized person representing the CA, an authorized legal authority.

4.9.3 **Procedure for a revocation request**

Revocation requests are submitted after adequate authentication and authorization of the requestor.

A valid approach of how this can be achieved is described in internal documents, which can be made available to auditors or other parties after the approval of CEPAC and under the conditions defined by CEPAC (such as the signing of a NonDisclosure Agreement).

The revocation procedures are set forth in this CPS and the applicable CP. The certificate holder and, if applicable, the legal representative of the organization (or his authorized delegate) will be notified of the revocation.

In case the certificate has been revoked due to CA compromise or operator errors, CA will provide, free of charge, a new equivalent certificate to the subscriber.

The request for revocation shall be recorded and archived. All relevant information about the certificate will stay archived for a period as specified in the CP. A revoked certificate (i.e., not suspended), may not be reinstated.

4.9.4 **Revocation request grace period**

The revocation request must be made as soon as possible if the reason for revocation include the invalidity of the certified data or the possible (future) compromise of the private key, and not later than after 12 hours if the requestor is not subject to Force Majeure.

The CSP shall not be held responsible for unauthorized use of a certificate's private key during the revocation request grace period or afterwards.

4.9.5 **Time within which CA must process the revocation request**

This is determined by the CP.

Revocation management services are available 24 hours per day, 7 days per week. Upon system failure, service failure or other factors that are not under the control of the CA, the CA shall make best endeavors to ensure that this service is not unavailable for an unreasonable period of time.

4.9.6 **Revocation checking requirement for relying parties**

Revocation status information is available 24 hours per day, 7 days per week. Upon system failure, service or other factors that are not under the control of the CA, the CA shall make best endeavors to ensure that this information service is not unavailable for an unreasonable period of time. The integrity and authenticity of the status information in the CRL is ensured by the fact that this CRL is electronically signed by the issuing CA. Revocation status information is also publicly and internationally available on http://crl.comsigneurope.com/ComSignEurope.crt. The relying party must take into account a grace period for the revocation period which includes a grace period for the propagation delay (between the reporting of the revocation request and the actual availability of up-to-date revocation information for relying parties) which normally corresponds to the CRL issuance frequency and a grace period for the delay in between the occurrence (e.g. the device holding the

private key has been stolen) and the actual reporting. It should be noted that it will not always be possible for the certificate holder or authorized person to make an immediate report to the revocation service.

It is up to the relying party to choose to accept the risk of not applying a grace period. The CSP is not responsible if the relying party suffers damages due to outdated validity data in case it chose not to take into account a grace period for either initial checking or for a later (re-)validation.

4.9.7 **CRL issuance frequency (if applicable)**

The CRL issuance frequency is determined by the CP. It shall be at least every twenty-four (24) hours.

4.9.8 **Maximum latency for CRLs (if applicable)**

The CRL maximum latency is determined by the CP.

4.9.9 **On-line revocation/status checking availability**

On-line revocation/status checking is not available. OCSP (Online Certificate Status Protocol) services may be additionally provided, see applicable CP and certificate content for details

4.9.10 **On-line revocation checking requirements**

Not applicable.

4.9.11 **Other forms of revocation advertisements available**

If allowed by the CP, suspension/revocation status information is also publicly and internationally available onhttp://fedir.comsigneurope.com/crl.

4.9.12 **Special requirements re-key compromise**

If the reason for requesting revocation is key compromise, the requestor should make the request with a minimum of delay. It must be noted though that the CSP does not record the reason for the revocation request and neither does the CRL include this type of information.

4.9.13 **Circumstances for suspension**

Any circumstance that may lead to the need for revocation and any circumstance in which a requester chooses to temporarily suspend the certificate in order to prevent

the use of the certificate during a certain time, can be considered as a valid reason for suspension.

Example reasons for suspension: the device holding the private key has been misplaced but will probably be found again, The device holding the private key is broken, the certificate holder has a lengthy leave during which he or she will not make use of the certificate, a payment as agreed in the contract between ComSign Europe and the subscriber is overdue.

4.9.14 **Who can request suspension**

The certificate holder (subject), an authorized person of the subscriber's organization, an RA or LRA having taken part in the registration of the concerned certificate, the CSP (represented by the ComSign Europe Policy Approval Council (CEPAC)), an authorized administrator of the CSP or acting for the CSP, an authorized person representing the CA and an authorized legal authority.

4.9.15 **Procedure for suspension request**

Suspension requests are submitted after adequate authentication and authorization of the requestor. A valid approach of how this can be achieved is described in internal documents, which can be made available to auditors or other parties after the approval of CEPAC and under the conditions defined by CEPAC (such as the signing of a Non-Disclosure Agreement).

The suspension/un-suspension procedures are set forth in this CPS and the applicable CP. The certificate holder and, if applicable, the legal representative of the organization (or his authorized delegate) will be notified of the suspension. The request for suspension shall be recorded and archived. All relevant information about the certificate will stay archived for a period as specified in the CP.

A suspended certificate can be un-suspended by the same parties that can request the suspension in accordance with the CP. Un-suspension requests are submitted after adequate authentication and authorization of the requestor. A valid approach of how this can be achieved is described in internal documents, which can be made available to auditors or other parties after the approval of CEPAC and under the conditions defined by CEPAC (such as the signing of a Non-Disclosure Agreement). The request for un-suspension shall be recorded and archived. All relevant information about the certificate will stay archived for a period as specified in the CP.

4.9.16 **Limits on the suspension period**

The limits on the suspension period are determined by the CP.

4.10 Certificate status services

4.10.1 **Operational characteristics**

The CRL status checking shall take place by downloading the relevant CRL from the web site specified in the CP.

4.10.2 **Service availability**

Revocation status information is available 24 hours per day, 7 days per week. Upon system failure, service or other factors that are not under the control of the CA, the CA shall make best endeavors to ensure that this information service is not unavailable for an unreasonable period of time.

4.10.3 **Optional features**

Not applicable.

4.11 End of subscription

Subscription may terminate either at the end of the agreed contractual subscription period or due to an occurrence that demands termination (such as failure to pay the due subscription fee).

Termination of subscription entails certificate revocation.

4.12 Key escrow and recovery

4.12.1 **Key escrow and recovery policy and practices**

Unless specifically permitted by the CP, key escrow and recovery services are not available under this CPS. When permitted, the archiving of a private key takes place automatically and securely as soon as the key is generated. The private key is stored in a secure key archive encrypted by a master key, which can only be exported and revealed in a restrictive procedure under special circumstances such as dual control.

If supported by this CPS, there are three types of key recovery: (a) Recovery of an archived key by the certificate holder (e.g. subject) in case of a personal certificate; (b) Recovery of an archived key of a personal certificate by an authorized person of ComSign Europe and (c) Recovery of an archived key by an authorized person belonging to an organization in the case of group-managed non-personal certificates.

A valid approach of how this can be achieved is described in internal documents, which can be made available to auditors or other parties after the approval of CEPAC and under the conditions defined by CEPAC (such as the signing of a NonDisclosure Agreement).

4.12.2 **Session key encapsulation and recovery policy and practices**

For all types of key recovery actions, the parties involved must be authenticated and authorized securely and all events need to be traced in secure audit trails.

Recovery of an archived key of a personal certificate by an authorized person of ComSign Europe must take place under "dual control" where both an authorized requestor and authorized approver exist. Before the requestor can recover the private key, the approver needs to approve this. In this case, segregation of duties is strict. Usually, the circumstance for such a recovery is a request by a recognized authority,

which can demonstrate the legal right to make such a request, and for the purpose of a legal investigation.

The ComSign Europe Policy Approval Council (CEPAC) determines which persons are authorized to fulfill the roles above and which conditions and procedures need to be adhered.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

Note:

Different functions that support the CSP may be outsourced to specialized partners. As a result, the controls in this section may vary and are described in more detail in the documentation of the outsourced service providers. However, ComSign Europe is the sole CSP and therefore, the minimal required controls may be exceeded but must be met.

The methods employed to achieve the controls below are described in internal documents, which can be made available to auditors or other parties after the approval of CEPAC and under the conditions defined by CEPAC internal documents (such as the signing of a Non-Disclosure Agreement).

5.1 Physical controls

The Certificate Authorities within the scope of this CPS have the following minimal physical controls.

5.1.1 Site location and construction

The CSP implements physical controls on its owned, leased or rented premises. The infrastructure is logically separated from any other certificate management infrastructure, used for other purposes.

5.1.2 Physical access

Physical access is restricted by physical barriers and implementing mechanisms to control physical movement from one area of the facility to another or control access into high-security zones.

5.1.3 Power and air conditioning

Power and air conditioning have built-in redundancy to avoid a failure of the infrastructure due to the loss of power or extreme temperatures.

5.1.4 Water exposures

Physical sites are protected from water exposure.

5.1.5 Fire prevention and protection

The CSP implements prevention and protection measures as well as measures against fire exposures.

5.1.6 Media storage

Media are stored securely. Backup media are also stored in a separate location that is physically secure and protected from fire and water damages.

5.1.7 Waste disposal

Waste disposal is controlled and any material that contains confidential or private data is destroyed sufficiently to prevent data exposure.

5.1.8 **Off-site backup**

The CPS implements an off-site backup and a DRP program.

5.2 Procedural controls

5.2.1 **Trusted roles**

The internal security policies define trusted roles for security sensitive tasks.

5.2.2 **Number of persons required per task**

The internal security policies define the number of persons required per task.

5.2.3 **Identification and authentication for each role**

Each trusted role is duly identified and authenticated.

5.2.4 **Roles requiring separation of duties**

The internal security policies define the roles requiring separation of duties. Where dual control is required, at least two trusted members of the staff need to bring their respective and split knowledge in order to be able to proceed with an ongoing operation.

5.3 Personnel controls

5.3.1 **Qualifications, experience, and clearance requirements**

The CSP implements personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties. Each staff member must execute a signed undertaking for maintaining confidentiality and protecting personal data.

5.3.2 **Background check procedures**

An investigation of all members of staff who are candidates to serve in trusted roles is conducted by the CSP in a reasonable attempt to determine their trustworthiness.

5.3.3 **Training requirements**

The CSP organizes trainings that provide reasonable assurance of the trustworthiness and competence of the members of the staff.

5.3.4 **Retraining frequency and requirements**

The CSP organizes retraining that provides reasonable assurance of the trustworthiness and competence of the members of the staff.

5.3.5 **Job rotation frequency and sequence**

The internal security policies define job rotation frequencies if needed.

5.3.6 **Sanctions for unauthorized actions**

The CSP ensures that all actions with respect to the ComSign Europe CAs and the other CSP services can be attributed to the system and the person that has performed the action. The CSP appropriately sanctions any unauthorized action.

5.3.7 **Independent contractor requirements**

Independent contractors performing tasks of trusted roles or tasks that may endanger the security of the CSP are subject to the same personnel control requirements as internal staff.

5.3.8 **Documentation supplied to personnel**

Personnel are supplied with sufficient documentation so that they can perform their duties in a satisfactory way.

5.4 Audit logging procedures

5.4.1 **Types of events recorded**

The types of events that are recorded in audit logs include, without limitation, tasks performed by users in any role (this includes operators and administrators), tasks performed by automated services and applications, the creation and status changes of the ComSign Europe certificates, other transaction requests together with record of the requesting identity, type of request, indication of whether the transaction was completed or not and eventual reason why the transaction was not completed and the creation of public registry entries

5.4.2 **Frequency of processing log**

All the information that is mentioned in section 5.4.1 of this CPS is processed online.

5.4.3 **Retention period for audit log**

Audit logs will be retained for a period of up to 30 years depending on the CP.

5.4.4 **Protection of audit log**

Logs created by the CA/RA components of the ComSign Europe infrastructure are adequately protected. Only dedicated internal ComSign Europe qualified staff members and duly (sub-) contracted and authorized personnel are allowed to process these files. Access control is restricted to the database access and physical location access to which only authorized people have access.

5.4.5 **Audit log backup procedures**

The back-up of the application audit log files is done with an adequate frequency. The back-up location is protected with similar security level measures as the principal location.

5.4.6 **Audit collection system (internal vs. external)**

Both are used.

5.4.7 **Notification to event-causing subject**

Not applicable.

5.4.8 **Vulnerability assessments**

Security Information and Event Management tools are deployed when needed.

5.5 Records archival

5.5.1 **Types of records archived**

All audit data, mentioned in the previous section, is archived. In addition, all certificate application information, and documentation supporting certificate applications must also be archived. This may include, if applicable, the signed registration forms (contractual agreements) and the subscribers' applications for certificates. In addition, the following information pertaining to the Certificate Authorities are archived: (a) electronic certificate requests; (b) the contents of issued certificates; (c) records on CA re-keying including key identifiers and cross certificates; (d) records on cross certification including the inquiry for cross certification and the performed actions; (e) CRL's; (f) results of an audit or assessment and (g) current and former CPs and CPS's.

5.5.2 **Retention period for archive**

The retention period for archives depends on the CP.

5.5.3 **Protection of archive**

The archive is protected in a reasonable level against data loss, loss of integrity and loss of confidentiality.

5.5.4 **Archive backup procedures**

These procedures are described in internal documentation.

5.5.5 **Requirements for time-stamping of records**

The archive employs the most suitable techniques for integrity protection.

5.5.6 **Archive collection system (internal or external)**

Archive collection applies to both internal and external sources.

5.5.7 **Procedures to obtain and verify archive information**

The CSP specifies the procedures to obtain and specify archive information in internal documents.

5.6 Key changeover

Whenever a new CA root key generation is required, the same procedure described in section 6.1 is initiated. It is possible that the new key will be certified using the certificate issued to the old key. Once generated, new certificates will be signed using the new key regardless the fact that the certificate for the old key may still be valid.

5.7 Compromise and disaster recovery

5.7.1 **Incident and compromise handling procedures**

This issue is dealt with in internal documents available to ComSign Europe authorized personnel and auditors.

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

These sources are backed up and/or foreseen to enable the resumption of the CA in due time.

5.7.3 **Entity private key compromise procedures**

This matter is dealt with in internal documents available to ComSign Europe personnel and auditors. Such an incident will be communicated without delay and necessary steps will be taken.

5.7.4 **Business continuity capabilities after a disaster**

A Business Continuity Plan is foreseen to enable the resumption of the CA in due time.

5.8 CA or RA termination

ComSign Europe will terminate or interrupt its operations due to the issue of a preemptory liquidation order for the liquidation of ComSign Europe and/or if the Board of Directors of ComSign Europe adopts a resolution terminating ComSign Europe's activity as a CA and/or as a result of a legal decree or court order.

If ComSign Europe's operations are terminated, ComSign Europe will take the following steps: (a) Inform all Subscribers, cross-certifying CA's and Relying Parties under agreement with the CA or under similar forms of established relations; (b) Inform the appropriate legal regulation administration of the termination and its possible consequences; (c) transfer its activities to another CA of the same quality and security level; if this is not possible, revoke the certificates two (2) months after having informed the Subscribers and archive all relevant certificate information for the next 30 years, (d) when possible, make a public announcement of its scheduled termination at least three (3) months ahead of time; (e) Terminate the revocation verification service in order to alert relying parties; and, (f) Terminate all authorizations of subcontractors acting on behalf of the CA in the process of issuing certificates (g) cancel the appointment of all Registration Authorities authorized to act on its behalf.

ComSign Europe shall allocate sufficient funds to secure such future actions.

In the event of termination of RA services, the RA obligations and undertakings are transferred to the CA. When both services (RA and CA) are terminated, the above shall apply.

Note: A reorganization entailing the transfer of services from one organization to another, or the transfer of the CA service from an old CA key to a new CA key are not considered as CA Termination.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

CA certificate key pair generation is described in internal documents, which can be made available to auditors or other parties after the approval of CEPAC and under the conditions defined by CEPAC (such as the signing of a Non-Disclosure Agreement).

Generating the ComSign Europe's CAs' keys shall take place in a physically secure environment by personnel in trusted roles under, at least, dual control. The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CAs practices. The keys encrypting the CA backup keys are split in several parts that cannot be used alone to decrypt the CA back-up keys. Once generated, access rights granted to the previously authorized persons are retracted and can only be reinstated again after approval of the ComSign Europe Policy Approval Council (CEPAC).

When key generation is performed by the subscriber, reliable technical means ensuring an adequate security level must be employed in order to, among others, prevent or detect any integrity flaw to a piece of data that has been encrypted or decrypted with the keys and to prevent or detect any unauthorized usage of a Private Key. In particular, the subscriber is obliged to generate its keys using a key generation algorithm, a key length, and a signature algorithm recognized as being fit for the

purposes of certificate usage. If the CP requires use of an SSCD and the subscriber generates its keys, then the key shall be created within an SSCD. The allowed methods of key pair generation and the minimal requirements for endentity certificates are determined by the CP.

6.1.2 **Private key delivery to subscriber**

When applicable, delivery should be secure, protecting the integrity, authenticity and confidentiality of the private key.

For Qualified certificates, the private key must be generated on the SSCD of the certificate holder and must not be delivered in any other way.

If allowed by the CP, the private key may be generated during a key ceremony on the secure HSM of the subscriber or on a secure HSM that sufficiently guarantees that the private key never leaves the secure HSM and can be used only by the subscriber.

If the Private/Public Key pair is generated by the CSP (e.g., at LRA premises), the Private Key can be provided by: (a) SSCD delivery provided measures were taken to ensure that the SSCD can be used only by the SSCD holder (subject) with the private key; (b) Secure connection (applicable for assurance levels Normalized and lower); (c) CD-ROM or memory stick (applicable for assurance levels Normalized and lower and provided the private key is protected with a password (in conformance with the password policy known only by the subscriber); and, (d) By e-mail (applicable for assurance levels Lightweight and lower, provided the private key is protected with a password (in conformance with the password policy) known only by the subscriber.

A valid approach of how private key delivery can be achieved is described in internal documents, which can be made available to auditors or other parties after the approval of CEPAC and under the conditions defined by CEPAC (such as the signing of a Non-Disclosure Agreement).

6.1.3 **Public key delivery to certificate issuer**

There are different ways to deliver a certificate signing requests depending on the CP. All are based on PKCS#10 requests in DER or PEM format: (a) A PKCS#10 submitted from a Private Key Holding Device, a SCD or SSCD via a secure channel that protects the authenticity of origin of the request, the integrity and the confidentiality. In case of an SSCD used by a qualified certificate, the SSCD itself must be authenticated; (b) A PKCS#10 submitted via a secured online web form by a subscriber which identity is authenticated; (c) A PKCS#10 on a memory stick or similar storage device delivered in person by the Subscriber to the LRA; (d) A PKCS#10, included in an e-mail, signed by the subscriber private key that was previously certified, provided the related certificate is still valid; (e) A PKCS#10, signed by the subscriber private key that was previously certified, provided the related certificate is still valid. This is only possible when using an electronic rekey possibility and when authorized in the applicable CP.

6.1.4 **CA public key delivery to relying parties**

The CA Public Keys are published on the ComSign Europe public registry and ComSign Europe e-certificates web site.

6.1.5 **Key sizes**

It is advised for certificates to have a key size (RSA) of minimum 2048 bits. However, for specific applications, other key lengths could be specified in the CP.

6.1.6 **Public key parameters generation and quality checking**

Public Key RSA exponents are chosen with security considerations. The Public Key module generation is done with state of the art parameter generation technology. CA components of the ComSign Europe PKI use Hardware Security Modules (HSM) that includes internal key pair generation. In this case the key is inside the HSM and cannot be retrieved. HSM devices used by ComSign Europe are FIPS 140-2 level 3.

6.1.7 **Key usage purposes (as per X.509 v3 key usage field)**

Each CA key pair key pair has the key usage "Signing Certificates and CRL's" enabled in the corresponding certificate and is only used for the purpose of generating certificates and CRL's, as defined in section 7.3.3 of ETSI TS 101 456, within physically secure premises.

The x.509v3 certificates issued by the CA contain the key usage certificate extension, restricting the purpose to which the certificate can be applied, in compliance with the CP under which the certificate is issued. See applicable CP for details.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 **Cryptographic module standards and controls**

CA key generation shall be performed using an algorithm recognized as being fit for the purposes of qualified certificates. The selected key length and algorithm shall suit the issue of qualified certificates by the CA.

CA key generation shall be carried out within a device which either meets the requirements identified in FIPS 140-2, level 3 or higher; or, meets the requirements identified in CEN Workshop Agreement 14167-2, CWA 14167-3 or CWA 141674; or, is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408, or equivalent security criteria.

A suitable time before expiration of its CA signing key, the CA shall generate a new certificate-signing key pair and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA key. The new CA key shall also be generated and distributed in accordance with this policy. This will be performed in a timely manner in order to allow all relevant parties (subjects, subscribers, relying parties, higher level CAs, etc.) to be notified of this key

changeover and to implement the required operations. This does not apply to a CA ceasing its operations before its own certificate-signing certificate has expired.

The HSM's that are used by the CA components of the ComSign Europe PKI segment are FIPS 140-2 Level 3. These HSM's are also EAL4+ Common Criteria certified.
Subscribers must protect their Private Key at all times, against loss, disclosure, modification and unauthorized use, in accordance with this CPS and the related CP. From the creation of their key pair, subscribers are personally and solely responsible of the confidentiality and integrity of their Private Keys. Every usage of their Private Key is assumed that of its owner. The PIN or password, used to protect against unauthorized use of the Private Key shall never be stored in the same location as the Private Key itself or next to its storage media or unprotected. Access to the Private Key must be limited to the subscriber or its authorized representative.

6.2.2 **Private key (n out of m) multi-person control**

The Private Keys of the ComSign Europe CA's are encrypted by a Storage Master Key (SMK), a strong encryption key that is split-up over smart cards or tokens that are protected with multiple password (shares). A certain number of shares ('N' out of 'M') out of the total shares held by different operators (or managers depending on security level) need to be available to restart an engine.

6.2.3 **Private key escrow**

Not applicable.

6.2.4 **Private key backup**

When outside the secure cryptographic device the CA private signing keys shall be protected in a way that ensures the same level of protection as provided by the secure cryptographic device.

The CA private signing key shall be backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secure environment. The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices.

Backup copies of the CA private signing keys shall be subject to the same or greater level of security controls as keys currently in use.

Where the keys are stored in a dedicated key processing hardware module, access controls shall be in place to ensure that the keys are not accessible outside the hardware module.

6.2.5 **Private key archival**

Upon expiration of a ComSign Europe CA Certificate, the key pair associated with the certificate will be securely retained for a period of at least 1 year using the hardware cryptographic modules that meet the security requirements of this CPS.

These CA key pairs shall not be used for any signing events after their expiration date, unless the CA Certificate has been renewed by the terms of this CPS.

If required and allowed (see applicable CP) the certificate holders' private encryption keys will be securely archived within the ComSign Europe CA infrastructure in accordance with this CPS.

The private keys used for electronic signatures should never be archived. In case of qualified certificates, key archival is strictly prohibited.

Access to the certificate holder's private key (key recovery) by an entitled authority requires dual control.

For the recovery of a private key the strongly authenticated request of an authorized person, acting on behalf of the authority that is entitled to demand the key recovery, must be approved by strongly authenticated and authorized security officer. The recovery must happen in a secure way in order that only the entitled authority can get access to the private key.
For the recovery of a private key by the certificate holder(s), a strongly authenticated and authorized request is required. The recovery must happen in a secure way in order that only the certificate holder(s) can get access to the private key.

A valid approach of how private key delivery can be achieved is described in internal documents, which can be made available to auditors or other parties after the approval of CEPAC and under the conditions defined by CEPAC (such as the signing of a Non-Disclosure Agreement).

6.2.6 **Private key transfer into or from a cryptographic module**

This depends on the CP. Private key transfer must happen in a sufficiently secure way to meet the requirements of the CP. The procedure is described in internal documents.

6.2.7 **Private key storage on cryptographic module**

This depends on the CP. Private key storage on a cryptographic module must happen in a sufficiently secure way to meet the requirements of the CP. The procedure is described in internal documents.

6.2.8 **Method of activating private key**

There are two types of methods of activating a supported private key:

Private Key activation by a person. For personal certificates, this is the mandated method. The private key is activated each time the PIN code is correctly entered or a similarly strong level or stronger level of authentication is attained by the certificate and key holder.

Private Key activation by a service. For non-personal certificates. The private key is activated automatically each time a strongly authenticated request accesses the service.

6.2.9 Method of deactivating private key

Private Keys are always deactivated after each activation and subsequent use.

6.2.10 Method of destroying private key

Private Key destruction requires that the private key data cease to exist. This can happen by fully erasing the memory where the key is stored or by physically destroying the device that holds the Private Key provided the destruction be such that the private key can never be extracted or used anymore.

A logical destruction of the private key is discussed in internal documents, which can be made available to auditors or other parties after the approval of CEPAC and under the conditions defined by CEPAC (such as the signing of a Non-Disclosure Agreement).

6.2.11 Cryptographic Module Rating

The CSP defines the following levels of Cryptographic Module Rating: SSCD: The requirements are defined by the relevant CEN/ETSI Technical Specifications and EN standards.
SCD: The requirements are defined by the relevant CEN/ETSI Technical Specifications and EN standards.
SUD: The requirements are defined by the relevant CEN/ETSI Technical Specifications and EN standards.
Private Key Holding Device: The requirements, though they are not strict, are defined by the relevant CEN/ETSI Technical Specifications and EN standards.

6.3 Other aspects of key pair management

6.3.1 Public key archival

When applicable, must meet the requirements of section 5.5.

6.3.2 Certificate operational periods and key pair usage periods

The maximum periods are defined in the CP. Shorter periods may be selected at the discretion of the requestor, wherever the CP allows this.

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data generation and installation meets the requirements of protecting the security of the activation data. The details are discussed in internal documents.

6.4.2 Activation data protection

Activation data protection meets the requirements of protecting the security of the activation data. The details are discussed in internal documents.

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

These are described in internal documents.

6.5.2 Computer security rating

Computer security rating is such that the security meets the required level defined by the relevant CP.

6.6 Life cycle technical controls

6.6.1 System development controls

The controls are such that the security meets the required level defined by the relevant CP.

6.6.2 Security management controls

The controls are such that the security meets the required level defined by the relevant CP.

6.6.3 Life cycle security controls

The controls are such that the security meets the required level defined by the relevant CP. In particular, for certificate generation, the CSP shall ensure that:

Certificate and revocation status information signing cryptographic hardware is not tampered with during shipment; AND
Certificate and revocation status information signing cryptographic hardware is not tampered with while stored; AND
The installation, activation, backup and recovery of the CAs signing keys in cryptographic hardware shall require dual control of at least two trusted roles; AND
Certificate and revocation status information signing cryptographic hardware is functioning correctly; AND

CA private signing keys stored on CA cryptographic hardware are destroyed upon device retirement. In particular, if the CA issues a SSCD; AND
The SSCD preparation shall be securely controlled by the service provider; AND
The SSCD shall be securely stored and distributed whenever the storage or distribution could possibly lead to key compromise or misuse of the SSCD; AND
SSCD deactivation and reactivation shall be securely controlled; AND
Where the SSCD has associated user activation data (e.g. PIN code), the activation data shall be securely prepared and distributed separately from the secure signaturecreation device. This may be achieved by ensuring distribution of activation data and delivery of SSCD via a different route and medium.

6.7 Network security controls

The CSP shall ensure that network components are kept in a physically secure environment and their configurations periodically audited for compliance with the requirements specified by the CSP. Furthermore, continuous monitoring and alarm facilities shall be provided to enable the CSP to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources. This may use, for example, an intrusion detection system, access control monitoring and alarm facilities.

6.8 Time-stamping

A date and time stamp is intended to improve the reliability of ComSign Europe's certificate issuing services. A date and time stamp attests to the correct date and time when an action was performed and the identity of the person or device that created the stamp. The date and time stamp reflects Greenwich Mean Time (GMT) and uses the Universal Time Convention (UTC). A ComSign Europe date and time stamp relies on a trustworthy, third-party time source that supplies official Universal Time readings at any given moment.

ComSign Europe will imprint a date and time stamp on the following data, whether directly on the data itself or on a parallel, reliable audit channel: (a) Certificates' (b) Lists of revoked certificates and other records of databases of revoked certificates and (c) Additional data, according to the relevant CP.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate profile

Certificates issued under this CPS shall be constructed according to ISO 9594-8 (x.509). Inclusion of data elements in certificates shall be consistent with the applicable CP. Content of the certificates are provided in the applicable CPs.

7.1.1 Version number(s)

Certificates issued under this CPS are x.509 version 3 Certificates.

7.1.2 Certificate extensions

The certificate extensions used correspond the definitions in RFC 5280.

7.1.3 Algorithm object identifiers

Applicable algorithm OIDs are specified in each CP.

7.1.4 Name forms

These are specified in each CP.

7.1.5 Name constraints

These are specified in each CP.

7.1.6 Certificate policy object identifier

This is specified in each CP.

7.1.7 Usage of Policy Constraints extension

These are specified in each CP.

7.1.8 Policy qualifiers syntax and semantics

These are specified in each CP.

7.1.9 **Processing semantics for the critical Certificate Policies extension**

These are specified in each CP.

7.2 CRL profile

7.2.1 **Version number(s)**

CRL version 2 is supported.

7.2.2 **CRL and CRL entry extensions**

As per x.509 version 2.

7.3 OCSP profile

Not applicable.

8. Compliance audit and other assessments

8.1 Frequency or circumstances of assessment

The ComSign Europe Policy Approval Council (CEPAC), shall reserve the right to require periodic and non-periodic inspections and audits of any CA facility within its domain to validate that the CA is operating in accordance with the security practices and procedures laid down in the present CPS, in the appropriate CP's and in internal documents.

CA's operating under this CPS shall be audited regularly for conformance with the present CPS and the appropriate CP's.

The ComSign Europe Policy Approval Council (CEPAC) shall reserve the right to require periodic and non-periodic inspections and audits of any RA facilities to validate that the RA is operating in accordance with the security practices and procedures laid out in the present CPS, in the appropriate CP's and in internal documents.

8.2 Identity/qualifications of assessor

The auditor shall have qualifications in accordance with best commercial practice and as mandated by law. The auditor must perform CA or Information System Security Audits as its main task, and must be thoroughly familiar with the CA's CPS.

8.3 Assessor's relationship to assessed entity

The auditor and CA shall have a contractual relationship for the performance of the audit, and be sufficiently organizationally separated from the audited CA to provide an unbiased, independent evaluation. The auditor shall be a certified public auditor if required by the appropriate CP or by the law.

8.4 Topics covered by assessment

a) The audit only compares the practices laid down in this CPS and the appropriate CP's with the onsite CA's implementation. All aspects of the CA's operation as specified in this CPS shall be subject to an audit compliance inspection. b) The audit shall also consider the operations of CA's subcontractors. c) It is the Relying Party's and cross-certifying CA's own responsibility to judge whether the CPS meets the requirements in this CPS, or to trust the statement of compliance by the CA.

8.5 Actions taken as a result of deficiency

Any discrepancies between a CA's operation and a stipulation of its CP's /CPS must be noted and immediately notified to the ComSign Europe Policy Approval Council (CEPAC). The CEPAC will determine a remedy, including a time for completion.

Any remedy may include permanent or temporary CA cessation, but several factors must be considered in this decision, including the severity of the discrepancy and the risks it imposes and the disruption to the certificate using community. Any remedy

may include that other certifying CA's may: immediately revoke cross certification certificates of the CA, allow the CA to continue operations for thirty days pending correction of any problems prior to revocation, or indicate the irregularities, but allow the CA to continue operations until the next audit without revocation. The decision regarding what actions to take will be based on previous response to problems, the severity of the irregularities, and the recommendations from the auditor. If a cross certificate of another CA is revoked, the CA shall immediately update the Authority Revocation List. Depending on the situation, contractual agreements, applicable laws and regulations, the CA may have to notify all its subscribers and indicate how it will proceed.

8.6 Communication of results

a) Conclusive results of the audits shall be distributed to the audited RA, the audited CA, and to the ComSign Europe Policy Approval Council (CEPAC). Conclusive result is hereby defined to be the information of all irregularities, which may affect a relying party's trust in a certificate, including an adequate judgment of its level of seriousness but excluding detailed information that can be used to attack the system.

b) Any CA or RA found not to be in compliance with this CPS shall be notified immediately at the completion of the audit. Required remedies shall be defined and communicated to such CA or RA as soon as possible to limit the risks. The implementation of remedies shall be communicated to the ComSign Europe Policy Approval Council (CEPAC). A special audit may be required to confirm the implementation of the effectiveness of the remedy.

9. Other business and legal matters

9.1 Fees

9.1.1 **Certificate issuance or renewal fees**

Fees are subject to change and are published on the ComSign Europe web site. (www.comsigneurope.com) or in subscriber agreements. Changes shall not take effect retroactively.

9.1.2 **Certificate access fees**

There are no certificate access fees.

9.1.3 **Revocation or status information access fees**

There are no revocation access fees.

9.1.4 Fees for other services

Fees are provided by ComSign Europe on a regularly updated pricing list with no retroactive effect.

9.1.5 Refund policy

No refund is applicable to early termination, revocation and the like. Issue of a new certificate following revocation is subject to full payment.

9.2 Financial responsibility

9.2.1 Insurance coverage

The CSP is duly insured to cover general financial responsibility.

9.2.2 Other assets

No general provisions are made. Specific provisions can be made for particular contractual agreements.

9.2.3 Insurance or warranty coverage for end-entities

No general provisions are made. Specific provisions can be made for particular contractual agreements.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

a) It is recommended that a certificate does not contain information that is not necessary for its effective use, such that no sensitive information is contained therein.
b) ComSign Europe certification services may request not-to-be-certified information to be used in managing the certificates, or for billing purposes, or for archiving purposes, or for any other reason, such as imposed by law. This information may contain sensitive information or personal data. The protection of the storage of these data shall be assured so that this remains confidential at all times in accordance to the data privacy law, and other applicable laws. The personal data which is supplied to ComSign Europe or to the local registration authority (whenever applicable) (paper or electronic information) by the certificate holder in the certificate request and delivery are duly incorporated, archived and protected according to the UK privacy law, in the files of ComSign Europe. The data will be used for the providing of the ComSign Europe PKI services. The Subscriber has the right to access and correct this data, and to refuse, on demand and without fees, any usage of this information for direct marketing purposes.

c) All information in the CA or RA records (not repository) shall be handled as sensitive, and access shall be restricted to those with official needs. Any personal or corporate information held by CA's or RA'S which is not appearing on issued certificates is considered confidential and shall not be released without the prior consent of the subscriber, unless required otherwise by law. Records that contain sensitive information shall have access control protection in place commensurate with the information to be protected.
d) No one, at all times, shall have access to a private signing key other than the owner of the corresponding certificate; it is recommended that the owner is prevented from viewing its Private Keys in unencrypted form.
e) All Private Keys used and handled within the CA operation under this CPS are to be kept confidential.
f) Audit logs and records shall not be made available as a whole, except as required by law. Only records of individual transactions may be released according to this CPS.

9.3.2 **Information not within the scope of confidential information**

a) Certificates, CRL's, revocation/suspension information and any information available on http://crl.comsigneurope.com/ComSignEurope.crt are not considered confidential. b) Identification information or other personal or corporate information appearing on certificates is not considered confidential.

9.3.3 **Responsibility to protect confidential information**

All participants that receive confidential information are under the obligation to protect it from compromise, and refrain from using it or disclosing it to third parties.

9.4 Privacy of personal information

9.4.1 **Privacy plan**

The applicable privacy plan that applies to a CSP or a subcontractor's activities will be recorded and reviewed to be in conformance with the CPS if this is needed and if required by applicable law or policy.

9.4.2 **Information treated as private**

Information that does not appear in the certificate or is not used for certificate management and token management services is considered as private.

9.4.3 **Information not deemed private**

See previous section.

9.4.4 **Responsibility to protect private information**

All information that is considered as private is subject to the applicable privacy plan. Participants that receive private information are obliged by contract to secure it, and refrain from using it and from disclosing it to third parties.

Information objects in certificates issued under this CPS and applicable CPs are regarded as personal data of the subscriber. In order to carry out its tasks in an efficient manner, ComSign Europe uses databases with these personal data. In this regard, ComSign Europe respects the privacy of the persons concerned. The subscriber authorizes ComSign Europe to publish such personal data in its repositories.

9.4.5 **Notice and consent to use private information**

Any use of private information requires consent from individuals to whom this information refers. General consent can be given by accepting the Subscriber Agreement. This consent is preserved either explicitly by means of signed contracts or implicitly by making use of the ComSign Europe Token Manager, in which the acceptance of the Subscriber Agreement terms is logged in audit trails.

9.4.6 **Disclosure pursuant to judicial or administrative process**

Any circumstances under which a participant is required to disclose private information pursuant to judicial, administrative process in a private or governmental proceeding, or in any legal proceeding must be demonstrated and the authorization will be archived by the CSP.

9.4.7 **Other information disclosure circumstances**

Other information disclosure circumstances must be approved by the individuals concerned or by the ComSign Europe Policy Approval Council (CEPAC) in accordance with legal restrictions.

9.5 Intellectual property rights

The present CPS and the applicable CPs are the property of ComSign Europe and are protected by intellectual property rights, unless otherwise agreed. Any use not allowed by the CPS and the applicable CPs may entail civil and criminal proceedings.

9.6 Representations and warranties

9.6.1 **CA Representations and warranties**

Comsign warrants that during its operation as a CA it will ensure that:

- The certificate does not contain any factual misrepresentations of which ComSign Europe is aware;
- There are no copying mistakes in the data, as received by ComSign Europe from the certificate applicant, that result from ComSign Europe not taking reasonable precautions when creating the certificate;
- The certificate complies with all material requirements of these procedures;

- After the certificate is issued, ComSign Europe will not have an ongoing obligation to investigate and check the degree of accuracy and correctness of the information included in the application for issuing a certificate, unless ComSign Europe receives explicit notification that one of the details appearing on the certificate is incorrect. In this case, the certificate will be revoked and it will be possible, at the request of the certificate owner, to issue a new certificate that contains the correct information subject to payment of the appropriate fee.
- ComSign's signature device was not impaired.

ComSign Europe will not be held responsible for damage caused by relying on an electronic certificate that it issued, if it can prove that it took all reasonable precautions to fulfill its obligations according to this CPS. The responsibility of ComSign Europe is, as noted, subject to the limitations listed below in this CPS. Without detracting from the above, ComSign Europe is committed to:

- Provide the infrastructure and the certificate issuing services, including the establishment, publication and operation of ComSign Europe's Repository, in a trustworthy and accessible manner as detailed in these procedures;
- Provide the controls and foundation for ComSign Europe's public key infrastructure (PKI), including protection of ComSign Europe's keys;
- Implement the procedures for verifying certificate applications, as listed in the relevant CP;
- Publish a list of revoked certificates in ComSign Europe's Repository, in a manner that is accessible, on-line and immediate for whomever wishes to rely on a particular electronic certificate;
- Revoke certificates as required by these procedures; - Handle certificates renewals as stated in these procedures.

9.6.2 **RA Representations and warranties**

Some of the certificate issuing services provided by ComSign Europe may also be provided by representatives on its behalf (RAs). The representatives of ComSign Europe must be appointed as such and serve under a contractual agreement regulating their activities and authorities. The RAs represent ComSign Europe at its discretion and their representation may be revoked as per the terms of their appointment. The RAs will participate in the services provided by ComSign for all matters relating to receiving and handling applications for electronic certificates, identifying applicants, and registering them. RAs are obligated to act in accordance with these procedures, the relevant CPs and comply with all applicable warranties and undertakings of ComSign Europe.

9.6.3 **Subscriber representations and warranties**

The Subscriber represents and warrants that:

Throughout the entire validity period of the certificate, to take all reasonable measures for the safe keeping of his/her signature device and to prevent its unauthorized use;

Throughout the entire validity period of the certificate, to inform ComSign Europe immediately upon learning that his/her control of the signature device has been impaired;

To the best of his/her knowledge, all representations made by the Subscriber to ComSign Europe regarding the information contained in the certificate are correct;

To the best of his/her knowledge, all information about himself contained in the certificate is complete and correct;

Every certificate applicant and certificate owner is required to confirm and declare in the subscriber agreement that after the certificate is issued, he/she, him/her/herself, and not ComSign Europe (or its representative), is solely responsible for safeguarding the signature device from damage, loss, exposure, modification or unauthorized use.

Furthermore, the subscriber agreement obligates certificate owners not to copy, reproduce, or reverse-engineer the technology that ComSign Europe uses to issue the certificates.

See also section 3.1.6.

9.6.4 **Relying party representations and warranties**

The Relying Party represents and warrants that when relying on a certificate, it will carry out all of the following prior to taking any action based on the certificate:

- Check the validity of the electronic signature on the electronic message.
- Verify that the certificate has not been revoked.
- Check and acknowledge the permitted usages and limitations listed in the certificate.
- When relying on the electronic signature of a corporate body or organization, conduct a due diligence to ensure that the person representing the corporate body or organization is dully authorized to commit the corporate body or organization by the specific undertaking executed with the electronic signature.

A relying party who does not verify the validity of a certificate as described above risks relying on an invalid electronic certificate and may be held legally responsible for any damage that might be caused as a result of not checking the validity of the electronic certificate. ComSign Europe will not bear any responsibility for any damage caused by relying on a revoked certificate.

A relying party, who chooses to rely on a revoked electronic certificate for a legal action taken after revocation of the certificate or on an electronic certificate that cannot be verified according to these procedures, may be held responsible for all damages that might be caused by relying on an electronic certificate whose validity was not verified. An attempt to verify the validity of a revoked certificate whose revocation was published on the CRL and/or a verification check done when ComSign Europe's database of revoked certificates and/or the computer of the relying party are not on-line will produce a reply indicating that the certificate is invalid and/or that its validity cannot be verified. In this case, the relying party should not rely on the certificate and if it does so, it is at its sole responsibility.

9.6.5 **Representations and warranties of other participants**

As per specific and individual terms and conditions applicable and present in the relevant documents and agreements regulating the activities of other participants.

9.7 Disclaimers of warranties

ComSign Europe and/or its representatives –

- Do not guarantee that a certificate owner will not deny any certificate or message.
- Do not guarantee any software other than the technology and software that ComSign Europe uses to issue the certificates and the device on which the signature device is stored, if supplied by ComSign Europe.
- Are not responsible for any damages caused by relying on a revoked certificate whose details were published in the CRL prior to being relied upon.
- Will not be liable for any indirect damages resulting from and/or related to any use, for any purpose, of certificates and/or electronic signatures. ComSign Europe and/or its representatives may be held liable only for direct damages caused naturally and in the ordinary course of events from the non-execution of its obligations.
- Will not be liable for the use of the electronic certificates in control equipment, in dangerous circumstances and/or uses that require fail-proof performance, such as operating nuclear facilities, aircraft navigation, communication systems, air traffic control systems and/or any situation in which failure might be a direct cause of death or bodily harm or environmental damage.

9.8 Limitations of liability

ComSign Europe may limit its liability as well as limit the types of certificate usage or transaction amounts for which the certificate may be used.
If the aforementioned limitations are listed on the electronic certificate, ComSign Europe and its representatives will not be responsible for damage caused as a result of violating these limitations. Furthermore, ComSign Europe may limit its liability toward a certificate owner in the subscription agreement.

Limitations on certificate usages will be executed only according the certificate owner's specific request. The form of the request will be formulated in the appropriate CP.

In any event, the total liability of ComSign Europe and/or its representatives toward any party (including, *inter alia*, a subscriber, applicant or relying party) will not exceed TBD for a single electronic signature produced and a single transactions related to that single signature and not exceed TBD for all of the electronic signatures produced and all of the transactions related to a particular certificate. The above limitation on damages and payment for damages applies to any type of loss and damage including direct damages, compensation, indirect damages, special and consequential damages, exemplary compensations or secondary damages caused to any person including the subscriber, applicant, recipient or a relying party and which are caused due to relying on or using a certificate that ComSign Europe issues,

manages, uses, suspends or revokes, or for relying upon or using an expired certificate. This limitation on damages or payment for damages also applies to contractual liability, tort liability and any liability claim. Subject to the aforementioned conditions, the liability limit for each certificate will be allocated first to the earlier claims in order to reach a final settlement of the conflict, unless an authorized court instructs otherwise. In no event shall ComSign Europe be obliged to pay an amount exceeding the total maximum liability sum for each certificate, regardless of the method used to distribute maximum liability among several claimants.

9.9 Indemnities

This section refers to a section in the subscriber agreement and can be supplemented by additional contractual agreements.

9.10 Term and termination

9.10.1 **Term**

This CPS, and all changes and amendments thereto, will become valid and invalidate the previous version immediately upon its publication.

9.10.2 **Termination**

ComSign's procedures, as published from time to time, will remain in force until replaced by a new version of the procedures.

9.10.3 **Effect of termination and survival**

See above.

9.11 Individual notices and communications with participants

This section applies to specific arrangements, if any, represented in the subscriber agreement.

9.12 Amendments

9.12.1 **Procedure for amendment**

This CPS may be amended by issuing a partial update. The partial update, as well as any correction to these procedures, will be published with the date that CEPAC has approved it, in a manner that will make it possible to monitor the date on which a document became valid and when the previous document or chapter became invalid. Amendments will be applicable from the date of publication after having been approved by CEPAC, however this does not add obligations towards anyone to whom a certificate was issued previously, on the basis of a previous CPS as long as the certificate remains valid. After an updated CPS is published, certificate owners are given a 60-day extension for filing objections, amendments or reservations so that

ComSign Europe may consider them and submit them to CEPAC, if necessary. ComSign Europe will send a written response to all comments received. There will be no response to comments received more than 60 days after the updated CPS is published.

9.12.2 **Notification mechanism and period**

Unless provided otherwise in these procedures, if any party to these procedures wishes or is required to send a notification, request, or application regarding these procedures, the said message shall be sent using an electronically signed message in a manner that conforms to the requirements of these procedures, or in writing. Electronic messages will be valid when the sender receives a valid return receipt, which must be received within five (5) days. Otherwise, a written notification must be sent using a courier service that provides a written delivery receipt, or by registered mail to the last reported address of the notified party.

9.12.3 **Circumstances under which OID must be changed**

Amendments that represent a fundamental change in the service and/or processes associated with it will require a change of version instead of an update all other amendments may be executed through an update to a published version. OID's will change whenever an update or new a version is published. See sections 1.2 and 1.5.4 above.

9.13 Dispute resolution provisions

Prior to using any kind of mechanism for conflict resolution (including legal proceedings or arbitration) to deal with a dispute related to any aspect of these procedures or to a certificate issued by ComSign Europe, the injured party must notify ComSign Europe, the RA and any other party relevant to the dispute, so they can attempt to settle the dispute among themselves.

9.14 Governing law

These procedures have been formulated in accordance with EU directives and other legislations without reference to other laws and/or rules regarding the choice of law, and without any requirement to establish a commercial connection to any particular state.
The choice of law was made to ensure uniform procedures and interpretation for all users, without reference to their place of residence or where their certificates are used.

9.15 Compliance with applicable law

These procedures comply with any applicable law and whenever a contradiction exists, the applicable law shall prevail.

9.16 Miscellaneous provisions

9.16.1 **Entire agreement**

This text of the CPS represents the entire document and replaces all other, previous texts and any other text, whether written or oral, has no validity, either explicit or implied, unless otherwise stated in these procedures as amended from time to time.

9.16.2 **Assignment**

ComSign Europe may assign its rights and/or obligations as described in these procedures to any other party, subject to specific agreements and undertakings with subscribers and other participants.

9.16.3 **Severability**

Unless determined otherwise, these procedures will be interpreted in a manner consistent with applicable law and reasonable commercial behavior in the given circumstances. When interpreting these procedures, it is necessary to consider their international extent and application, the benefits inherent in encouraging uniformity of their implementation and maintaining good faith.

In the event of any contradiction between these procedures and the applicable law as well as other binding rules, such binding rules will prevail and the contradicting terms of these procedures will be overlooked. In the event of any contradiction between the provisions of the subscriber agreement and the provisions of this CPS, the provisions of this CPS will prevail. In the event of any contradiction between the provisions of the updated CPS, and a previous version of the CPS, the updated version will prevail.

9.16.4 **Enforcement (attorneys' fees and waiver of rights)**

No waiver, discount, delay, extension or avoidance of on-time action by ComSign Europe and/or a subscriber shall be interpreted as a waiver on their part of any rights as described in this CPS, and shall not be used as an argument or injunction against a claim on their part.

9.16.5 **Force Majeure**

ComSign Europe and its representatives shall not be responsible for any breach, delay, or avoidance of performance in accordance with this CPS caused by events beyond its control such as force majeure, wars, periods of market emergency, epidemics, power outages beyond the control of ComSign Europe, fires, earthquakes and other disasters for which ComSign Europe was unable to reasonably prepare.

9.17 Other provisions

This section refers to a section in the subscriber agreement and can be supplemented by additional contractual agreements.