Nets Electronic ID Services

Eurida Primary CA
Certification Practice Statement

Version 1.0

Effective Date: August 16, 2012

Document OID: 2.16.578.1.15.1.3.3.2.1.0

Copyright

Disclaimer

NETS NORWAY AS has provided the information in this document for use by Nets Eurida Primary CA.

NETS NORWAY AS MAKES NO REPRESENTATION OR WARRANTY AS TO THE ENFORCEABILITY OR LEGAL EFFECT OF THIS DOCUMENT AND OTHER MATERIALS PRODUCED THROUGH THE USE OF THIS DOCUMENT, INCLUDING APPENDIXES AND REFERENCES TO OTHER DOCUMENTS MADE FOR PROJECT PURPOSES, UNLESS EXPLICILTLY STATED IN THE APPLICABLE DOCUMENT.

NETS NORWAY AS SHALL NOT BE LIABLE FOR ANY DAMAGES ARISING FROM OR IN CONNECTION WITH THE ENFORCEABILITY OR LEGAL EFFECT OF DOCUMENTS OR OTHER MATERIALS PRODUCED THROUGH THIS DOCUMENT INCLUDING APPENDIXES AND REFERENCES TO OTHER DOCUMENTS, UNLESS EXPLICILTLY STATED IN THE APPLICABLE DOCUMENT.

NETS NORWAY AS

N – 0045 Oslo

NORWAY

List of Contents

DEFINITIONS AND ABBREVIATIONS

Best Practices: That which is widely accepted as best security practices at a particular point in time.

CA Certificate: A Certificate which is used by the CA exclusively to sign issued Certificates and CRLs.

Certificate: A certificate is formatted data that cryptographically binds an identified Subject to a public key. It allows the Subject taking part in an electronic transaction to prove its identity to other participants.

Certificate Revocation List (CRL): A periodically generated list of revoked Certificates issued by a specific CA. A CRL is normally signed by the CA Certificate.

Certificate Policy (CP): Named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements [3].

Certification Authority (CA): Authority trusted by one or more users to create and assign Certificates [3].

Certification Hierarchy: A set of End User certificates and a number of CA Certificates that traverse up to a common root CA.

Certification Practice Statement (CPS): Statement of the practices that a Certification Authority employs in issuing Certificates [1].

CRL Distribution Point (CDP): A Certificate extension that identifies how CRL information is obtained.

Distinguished Name (DN): A name structured according to X.500 standard that is used to unambiguously identify the Subject of a Certificate.

End User: An entity that is the Subject of a Certificate issued by the CA. End User can not be the CA itself.

Hardware Secure Module (HSM): Hardware-based security device that generate, stores and protects cryptographic keys as well as provides cryptographic functions. In the context of this document an HSM SHALL meet the requirements identified in FIPS 140-2 level 3 [6] or higher.

ISACA: Information Systems Audit and Control Association.

Nets CA Management: An authority body within Nets Norway AS responsible for the management and accountability for ensuring compliance to CPs for Nets owned CAs.

Nets Policy Management Authority (PMA): An authority body within Nets Norway AS appointed by Nets CA Management with mandate to establish, conduct quality control, maintain, administer and authorize CPs.

Object Identifier (OID): A specially-formatted sequence of numbers that is registered in accordance with internationally-recognized procedures for object identifier registration.

Online Certificate Status Protocol (OCSP): As defined in RFC 2560.

Organization: A legal entity named in the Certificate Subject Distinguished Name and/or issuer distinguished name.

Processing Center: IT-facilities and associated processes, personnel and procedures that support the CA and RA.

Public Key Infrastructure (PKI): Is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

Registration Authority (RA): An entity respecting the CA's CP and CPS, which is assigned by the CA to assist preparing Certificate applications, validating application information, and receiving revocation requests. A CA may contract a third party RA with a business contract referring to the CP and CPS, or it can act as a Registration Authority itself.

Relying Party (RP): A legal entity or a natural person that acts in reliance on a Certificate.

Repository: A data store into which Certificates, revocation information and legal documents are posted.

Revocation Officer: A person assigned by the CA or RA to approve Certificate revocation requests, and who is responsible for revoking Certificates.

Subject: An entity identified in a Certificate as the holder of the private key associated with the public key given in the Certificate.

Subordinate CA (SubCA): In a hierarchical PKI, a CA whose Certificate is signed by the Eurida Primary CA, and whose activities are constrained by the Eurida Primary CP.

Subscriber: An entity subscribing with a Certification Authority on behalf of one or more Subjects. A Subject may be a Subscriber acting on its own behalf.

Trustworthy System: System satisfying Best Practices with regard to physical and cryptographic trustworthiness.

REFERENCES

[1] IETF RFC 3647 (2003): “Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework”, S. Chokhani, W. Ford, R. Sabett, C. Merrill, S.Wu

[2] Act on electronic signatures: LOV 2001-06-15 nr 81. http://www.lovdata.no/all/hl-20010615-081.html

[3] ETSI TS 101 456 v1.4.3 (2007 May): “Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates”

[4] Directive 1999/93/EC of 13. December 1999 on a Community Framework for Electronic Signatures

[5] ITU-T X.509 (2005 August): “Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks”

[6] FIPS PUB 140-2 (2001 May 25): “Security Requirements for Cryptographic Modules”

[7] ETSI TS 102 176-1 v2.0.0 (2007 November): “Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms”

[8] IETF RFC 5280 (2008): “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, D.Cooper NIST, S. Santesson Microsoft, S. Farrell Trinity College Dublin, S.Boeyen Entrust, R. Housley Vigil Security, W. Polk NIST

[9] ETSI TS 101 862 v1.3.2 (2004 June): “Qualified Certificate profile”

[10] ISO/IEC 17021:2006 (2006 September 15): ”Conformity assessment – Requirements for bodies providing audit and certification of management systems”

[11] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

1 INTRODUCTION

This document is the Certification Practice Statement (CPS) for Eurida Primary CA, and as such serves as a statement of practices that Nets Norway AS employs during issuance and management of X.509 Certificates in accordance with the Certificate Policy (CP) established for the Eurida Primary CA. This practice applies for the following Nets Norway AS products:

- Eurida Primary CA CP with document OID 2.16.578.1.15.1.3.3.1.1.0

Eurida Primary CA CPS defines the underlying certification processes for the Eurida Primary CA, RA and Subscribers. It notifies all parties involved of their roles and responsibilities. This CPS also explains the repository operations, Certificate life-cycle operations, facility, management and operational controls and technical security controls that apply to the Eurida Primary CA.

This CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 [1] for Certificate Policy and Certification Practice Statement construction.

Not all sections of RFC 3647 [1] are used. Sections that are not used or are not applicable, have a default value of “No stipulation” or “Not applicable”.

1.1 Overview

The Eurida Primary CA, which is signed by OmniRoot (CN = Baltimore CyberTrust Root, OU = CyberTrust, O = Baltimore, C = IE), issues high quality and highly trusted digital CA Certificates to entities including private and public companies.

Only the CA Certificate type is issued under this CPS.

The Eurida Primary CA operates in compliance with Norwegian Law and in particular the Norwegian Act on electronic signatures [2].

1.2 Document name and identification

This document is the Eurida Primary CA Certification Practice Statement. Insignificant revisions may be made without changing the version number of this CPS. Revisions not denoted “significant” are those deemed by Nets Policy Management Authority to have minimal or no impact on Subscribers and Relying Parties using Certificates and CRLs.

This Eurida Primary CA CPS is identified by the following OID:

OBJECT IDENTIFIER::= {joint-iso-itu-t(2) country(16) norway(578) organization(1) nets-norway(15) esecurity(1) eurida-primary-ca(3) practice-statement(2) cps-version-1(1)}.

This document has the following OID:

OBJECT IDENTIFIER::= {joint-iso-itu-t(2) country(16) norway(578) organization(1) nets-group(15) esecurity(1) eurida-primary-ca(3) document(3) cps(2) major-version(1) minor-version(0)}.

1.3 PKI participants

This CPS has impact on the following Certification Authorities:

- Eurida Primary CA
- SubCAs of Eurida Primary CA.

In addition, this CPS has impact on the following PKI participants:

- Registration Authorities
- Subscribers.

1.4 Certificate usage

The Eurida Primary CA is used for signing the CA Certificates of SubCAs.

CA Certificates will not be used for any functions except CA functions.

Key Usage for the Eurida Primary CA Certificate is restricted to:

- keyCertSign
- cRLSign.

The Eurida Primary CA Certificate MUST NOT be used in any way that is not consistent with the applicable law, or the agreements, the CP and the CPS under which the Certificate have been issued.

The Relying Party is obliged to take into account the key usage purpose stated in the Certificates.

1.5 Policy administration

The organization responsible for the Eurida Primary CA CPS is the Nets Policy Management Authority.

The postal address for the Nets Policy Management Authority is:

Nets Policy Management Authority
Nets Norway AS
N-0045 Oslo
Norway

Visiting address:

Haavard Martinsens vei 54, Rommen, Oslo, Norway

+ 47 22 89 89 89 (phone)

E-mail: esec-eid-no@nets.eu

The Nets Policy Management Authority (PMA) determines the suitability and applicability of this CPS.

Approval of this CPS and any subsequent amendments are done by Nets CA Management.

Subsequent amendments to this CPS shall be in the form of a document containing the amended form of the CPS. Updates supersede any designated or conflicting provisions of the referenced version of the CPS. The PMA shall determine whether changes to the CPS require a change in the CPS Object Identifier.

1.6 Definitions and acronyms

See Definitions and Abbreviations.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

Nets Norway AS is responsible for publishing and managing repositories for the PKI service. All updates and amendments are logged.

Nets Norway AS maintains the repository services and adheres to:

- Responsibility to apply to the provisions in this CPS and the applicable CP
- Service level
- Protection of repository services against intrusion, unauthorized changes, and denial of service attacks.

2.1 Repositories

Eurida Primary CA only publishes its own CA Certificate and CRL. No other Certificates are published by Eurida Primary CA. The repository is a web server available over HTTP. Eurida Primary CA has no LDAP repository.

2.2 Publication of certification information

The Eurida Primary CA Certificate is published at:

- http://ca.eurida.com/ca/euridaprimary.cer

The Eurida Primary CA CRL is published at:

- http://crl.eurida.com/crl/euridaprimary.crl

The current version of the Eurida Primary CA Certificate Policy is published at:

- http://ca.eurida.com/repository/

2.3 Time or frequency of publication

The amendments to the above cited documents will be published as soon as possible after Nets Policy Management Authority resolutions.

CRLs are issued at least as often as stated in the Eurida Primary CP, and with guaranteed validity duration.

2.4 Access controls on repositories

Nets Norway AS has implemented controls to prevent unauthorized persons from adding, deleting, or modifying repository entries on the PKI platform.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

Names are implemented according to the Eurida Primary CA CP.

Subject names appearing in CA Certificates are authenticated.

Eurida Primary CA Certificates will not contain alternative Subject names in Certificate extensions. Prior to Certificate issuance, the Eurida Primary CA does make a unique identification of the SubCA in question.

Meaningful in the context of need for names to be meaningful, means that the name form has commonly understood semantics. For the present CPS the following adhere:

- Common name is meaningful.
- Organization name is meaningful.
- Organization unit is meaningful.

There will not be support for anonymous or pseudonymous Subjects.

Subject Name included in a Certificate will be unique, in order to permit the determination of the identity of the Subject.

Distinguished Names are interpreted according to the X.509 v3 standard and are used in accordance with applicable law.

It is the responsibility of the Subscriber not to use names that conflict with protected names of natural persons or Organizations pursuant to law or Intellectual Property Rights in any jurisdiction. Nets Norway AS has no obligation to determine whether any name used in a Certificate application is a protected name or infringe any rights of any third party.

Nets Norway AS is not obliged to arbitrate, mediate or resolve any type of name conflicts or disputes related to intellectual property or use of a name in a Certificate application. Eurida Primary CA is entitled to reject or suspend a Certificate application or issued Certificate in case of such conflict, without being liable to any Certificate applicant.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

Key pair generation for the SubCAs that are to be signed by Eurida Primary CA are generated on a safe hardware device which conforms to FIPS 140-2 level 3 standards [6].

SubCAs keys that are to be signed by Eurida Primary CA are generated on a safe hardware device which conforms to FIPS 140-2 level 3 standards [6]. Possession of the private key is verified by verifying the digital signature on the certification requests provided by SubCAs to Eurida Primary CA.

3.2.2 Authentication of organization identity

Organizations subscribing with Eurida Primary CA are authenticated by verifying organization name and number in European Business Register. Organizations not registered by the European Business Register are required to provide corresponding and sufficient documentations from a public Register of Business Enterprises in the applicable country.

3.2.3 Authentication of individual identity

All Subscriber information included in Certificates is verified.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

No stipulation.

3.2.6 Criteria for interoperation

No stipulation.

3.3 Identification and authentication for re-key requests

Certificate re-key is not used.

3.3.1 Identification and authentication for routine re-key

No stipulation.

3.3.2 Identification and authentication for re-key after revocation

No stipulation.

3.4 Identification and authentication for revocation request

Revocation procedures ensure that revocation has been requested by a Subscriber. Under some circumstances a revocation may be requested by the Eurida Primary CA itself (see section 4.9).

Procedures for authenticating a Subscriber which is an organizational entity as a revocation requestor include:

- Receiving a message from a member of the organization requesting revocation through communication providing reasonable assurance for the requestor identity and membership.
- Compliance to agreement between the parties.

Upon positive authentication the Eurida Primary CA revokes the Certificate without delay.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

Controls are in place in order to ensure that application records are legitimate and correct.

Eurida Primary CA collects application information for administrative and maintenance purposes, or control purposes in national registers, e.g. information to produce invoices, or to inform SubCAs as to when a particular Certificate is about to expire.

4.1.1 Who can submit a Certificate application

Eurida Primary CA is only accepting applications from other Certification Authorities.

4.1.2 Enrolment process and responsibilities

The enrolment procedures are described in key ceremony document for relevant SubCAs.

4.2 Certificate application processing

All relevant steps of the Certificate request processing are logged for audit purposes. All certification operations are also auditable.

4.2.1 Performing identification and authentication functions

As only organizations can subscribe with Eurida Primary CA, identification and authentication of subscribing SubCAs is verified by checking a national register of organizations.

4.2.2 Approval or rejection of Certificate applications

A Certificate application is approved if the stipulated controls are successfully passed, and all other requirements specified in relevant agreements are satisfied. Otherwise, a Certificate application will be rejected.

4.2.3 Time to process Certificate applications

Processing of the Certificate application starts without deliberate delays.

4.3 Certificate issuance

SubCAs' certificates are generated in a security zone with use of Eurida Primary CA keys stored on an HSM.

4.3.1 CA actions during Certificate issuance

All CA actions during issuance are logged.

4.3.2 Notification to subscriber by the CA

After signing of a SubCA Certificate by Eurida Primary CA, said Certificate is returned to the requestor.

4.4 Certificate acceptance

4.4.1 Conduct constituting Certificate acceptance

SubCA is asked to accept its Certificate at the moment of reception of the Certificate.

4.4.2 Publication of the Certificate by the CA

SubCA publishes its CA Certificates in a predetermined repository according to its PKI documentation.

4.4.3 Notification of Certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and Certificate usage

SubCA Certificates must be used in accordance with the terms of this CPS and the Eurida Primary CP.

4.5.1 SubCA private key and Certificate usage

SubCAs must ensure that their Certificate is used consistently with the Key Usage extension field included in the Certificate.

Under Eurida Primary CA regulations, SubCAs shall not issue new Certificates after expiration or revocation of the SubCA Certificate.

SubCAs must protect their private key from unauthorized use and promptly start the revocation process if the private key is compromised.

4.5.2 Relying Party public key and Certificate usage

Attention is drawn to stipulations in section 9.6.4.

4.6 Certificate renewal

Certificate renewal is not supported as a separate service by Eurida Primary CA. Every renewal request is treated as a new Certificate application. This does not hinder a SubCA from sending a renewal request by providing the original certification request for a new certification.

4.6.1 Circumstance for Certificate renewal

Not applicable.

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing Certificate renewal requests

Not applicable.

4.6.4 Notification of new Certificate issuance to Subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal Certificate

Not applicable.

4.6.6 Publication of the renewed Certificate by Eurida Primary CA

Not applicable.

4.6.7 Notification of Certificate Issuance by Eurida Primary CA to other Entities

Not applicable.

4.7 Certificate re-key

Certificate re-key is not used by Eurida Primary CA.

4.7.1 Circumstance for Certificate re-key

Not applicable.

4.7.2 Who may request certification of a new public key

Not applicable.

4.7.3 Processing Certificate re-keying requests

Not applicable.

4.7.4 Notification of new Certificate issuance to Subscriber

Not applicable.

4.7.5 Conduct constituting acceptance of a re-keyed Certificate

Not applicable.

4.7.6 Publication of the re-keyed Certificate by the CA

Not applicable.

4.7.7 Notification of Certificate Issuance by the CA to other Entities

Not applicable.

4.8 Certificate modification

Certificate modification is not supported. Every modification request is treated as a new Certificate application.

A Subscriber who wishes to modify a Certificate may revoke the Certificate which contains obsolete information and apply for a new Certificate.

4.8.1 Circumstance for Certificate Modification

Not applicable.

4.8.2 Who may request Modification

Not applicable.

4.8.3 Processing Certificate Modification requests

Not applicable.

4.8.4 Notification of new Certificate issuance to Subscriber

Not applicable.

4.8.5 Conduct constituting acceptance of modified Certificate

Not applicable.

4.8.6 Publication of the modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to other Entities

Not applicable.

4.9 test

4.10 Certificate revocation and suspension

Upon revocation of a Certificate, the operational period of that Certificate is immediately considered terminated. Revoked Certificates are then listed in applicable CRL.

4.10.1 Circumstances for revocation

Eurida Primary CA has the right to immediately revoke a Certificate if the Subscriber requests revocation or for good reason suspects an abuse. In addition, revocation may be performed for any objective reason, included but not limited to circumstances that may reasonably be expected to affect the reliability, security or integrity of the Certificate or key pair associated with it.

Certificates will be revoked if:

- There is a reason to believe that there has been a compromise of the private key.
- The Subscriber has materially breached a material obligation, representation, or warranty under this CPS and/or an applicable agreement.
- The Subscriber agreement is terminated.
- Eurida Primary CA discovers or has reason to believe that the Certificate was issued in a manner not in accordance with the procedures required by this CPS.
- Eurida Primary CA discovers or has reason to believe that a material fact in the Certificate application is false.
- Eurida Primary CA determines that a material prerequisite to Certificate issuance was neither satisfied nor waived.
- The SubCA requests revocation of the Certificate.

4.10.2 Who can request revocation

Revocation procedures ensure that a revocation has been requested either by a Subscriber or Eurida Primary CA.

4.10.3 Procedure for revocation request

Acceptable procedure for revocation requests includes:

- Authenticating the revocation requestor according to stipulations described in section 3.4
- Accepting the revocation request upon positive authentication
- Revocation of the Certificate without delay
- Notifying the Subscriber that revocation has taken place. A notification is sent to the Subscriber using contact information specified in the Subscriber's agreement.

When requests are submitted to Eurida Primary CA the following information is logged:

- Originator of the request
- Time/date of the arrival of the request
- Reason for revocation
- Whether or not the originator has any reason to believe that the Certificate has been or could be used by unauthorized persons
- Officer receiving the request
- The procedure used to verify the authenticity of the request.

Requests for revocation of a Eurida Primary CA Certificate must be submitted to the Nets Policy Management Authority. The reason for the request must be well documented.

Revocation shall be a decision of the Nets CA Management.

4.10.4 Revocation request grace period

No stipulation.

4.10.5 Time within which CA must process the revocation request

Eurida Primary CA processes all revocation requests without delay. The amount of time required depends on the nature of the revocation request, the party requesting the revocation, and other factors surrounding the revocation request.

4.10.6 Revocation checking requirements for relaying parties

Relying Parties are obliged to check online for the most recent revocation status information regarding all Certificates in the Certificate chain before accepting any Certificate.

4.10.7 CRL issuance frequency

CRLs that are signed by Eurida Primary CA are issued and published at least every 9th month and have a validity of 12 months.

4.10.8 Maximum latency for CRLs

CRLs are posted to the repository without undue delay after generation.

4.10.9 Online revocation status checking availability

Certificate revocation status information is available online by consulting the CRL available as described in section 2.2.

4.10.10 Online revocation checking requirements

See section 4.10.6.

4.10.11 Other forms of revocation advertisements available

No stipulation.

4.10.12 Special requirements regarding key compromise

All SubCAs will be notified of a compromise, or suspected compromise, of Eurida Primary CA private key. This will be done by publishing the information on the Eurida Primary CA web page as specified in section 2.2.

4.10.13 Circumstances for suspension

Certificate suspension is not supported.

4.10.14 Who can request suspension

No applicable.

4.10.15 Procedure for suspension request

No applicable.

4.10.16 Limits on suspension period

No applicable.

4.11 Certificate status service

The status of Certificates is available via CRLs at URLs specified in section 2.2.

4.11.1 Operational characteristics

Certificate status services are available 24x7 with exception of scheduled maintenance.

4.11.2 Service availability

See section 4.11.1.

4.11.3 Optional features

No stipulation.

4.11.4 End of subscription

SubCA's subscription ends with expiration of its Certificate, or when its Certificate gets revoked.

4.12 Key escrow and recovery

Eurida Primary CA does not escrow nor recover SubCA private keys.

4.12.1 Key escrow and recovery policy and practices

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical security controls

Eurida Primary CA adheres to internal security documentation which contains sensitive security information that may only be available subsequently to agreements with Nets Norway AS. An overview of the physical security controls is described below.

5.1.1 Site location and construction

CA servers, HSMs, repositories and RA servers are located in physically secured premises, according to [3]. Specifics are described in the relevant security documentation, which is part of the documentations mentioned above.

The requirements are fulfilled with high-security zones based on physical and logical barriers.

5.1.2 Physical access

Access to each barrier of physical security is controlled so that each barrier can only be accessed by personnel authorized for that specific barrier. All access is auditable.

5.1.3 Power and air conditioning

The secure premises have double power supplies from two separate power sources. In addition the buildings are supplied with a UPS-battery banks which are dimensioned to maintain the proper voltage until the on-site power plant is online and delivering power.

An air-cooling system is available in the secure premises, and temperature and humidity are controlled automatically and continuously.

5.1.4 Water exposures

All security rooms are shielded against water exposures.

5.1.5 Fire prevention and protection

Fire prevention and protection systems are online at all times. These meet or exceed all local safety regulations.

5.1.6 Media storage

Eurida Primary CA and RA are backing up critical system data. All data are protected from water, fire, or other environmental hazards.

5.1.7 Waste disposal

Eurida Primary CA and RA have implement procedures for the disposal of paper, magnetic and optical media, or any other waste to prevent the unauthorized use of, access to, or disclosure of waste containing confidential or private information.

5.1.8 Off-site backup

The Eurida Primary CA and RA are backed up to offline media after every CA or CRL signing. This backup is stored in a separate location from the Eurida Primary CA premises.

5.2 Procedural controls

This section describes the controls imposed upon personnel performing in trusted roles.

5.2.1 Trusted roles

Security roles and responsibilities are documented in job descriptions. Trusted roles, on which the security of the PKI operation is dependent, are clearly identified.

Personnel security procedures for personnel in trusted roles are in line with the recommendations given in the referenced documents [1], [4] and [5].

Each role has a role description which defines responsibility, routines and which part of the system the personnel performing the role have access to.

5.2.2 Number of persons required per task

Personnel involved in PKI operations have job descriptions based on separation of duties and least privilege, determining position sensitivity based on duties and access levels, background screening and employee training and awareness.

The relevant security documentation describes tasks that require more than one person.

5.2.3 Identification and authentication for each role

Personal physical and electronic credentials are used for all jobs on the IT-systems, thus ensuring traceability and feasible auditing conditions.

5.2.4 Roles requiring separation of duties

All roles requiring separation of duties conform to the specifications described in the relevant security documentation.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Personnel that possess the expert knowledge, experience and qualifications necessary for providing the certification services and as appropriate to the job function are maintaining and operating Eurida Primary CA.

Eurida Primary CA personnel are certified as trusted employees. In addition they have at least 6 months PKI-experience and have a proven PKI system competence. The skills of all personnel are checked before qualifying them to the PKI system.

5.3.2 Background check procedures

Background checks of trusted employees are performed. The background checks are in accordance with applicable national law.

5.3.3 Training requirements

The training before obtaining authorization to work on the PKI production systems is carried out with hands-on working experience on the IT-systems.

The candidate must prove his/her skills to the security officers who perform the authorization.

All persons that are granted access to the PKI facilities keep continuity in working with the systems, ensuring that they have necessary skills for maintaining the systems.

5.3.4 Job rotation frequency and sequence

No stipulation.

5.3.5 Sanctions for unauthorized actions

Eurida Primary CA has established, maintains, and enforces employment policies for the disciplinary actions of personnel resulting from unauthorized actions. Such disciplinary actions are in accordance with national Employment Protection Acts and agreements between employee and employer. The agreements are not a hindrance of employers' right to move employees from trusted roles or revoke access to systems if necessary. Disciplinary actions may include measures up to and including termination of employment.

5.3.6 Independent contractor requirements

Third party contractors as well as unauthorized CA employees are not left alone in the secured premises, and do not work alone on the CA system.

When necessary for third party contractors and unauthorized CA personnel to work in the secured premises, or directly on the CA system in any way, they are accompanied by two authorized system administrators. The tasks are documented and supervised.

5.3.7 Documentation supplied to personnel

During initial training, retraining, or otherwise there is need of extended system documentation. During the training period, the personnel gain thorough knowledge of the existing documentation, and part of the appointment to trusted roles consist of giving access to all the required documentation.

5.4 Audit logging procedures

Eurida Primary CA and RA keep records of events sufficient to prove that they comply with the provisions of Eurida Primary CP.

All recorded events carry a date and time statement and the identity of the entity that has caused the event.

5.4.1 Types of events recorded

The events relating to the following are logged:

- Events relating to registration of Certificate applications
- Events relating to the life-cycle of CA keys
- Events relating to the life-cycle of Certificates issued by the Eurida Primary CA
- Events relating to the life-cycle of keys managed by the CA, including any Subject keys generated by the CA
- Events relating to Certificate revocation, including revocation requests, revocation reports and the resulting actions.

5.4.2 Frequency of processing log

Systems are in place which control that events are recorded continuously and as intended.

Logs are processed during periodic audits and on a need basis.

5.4.3 Retention period for audit logs

All relevant information concerning issuance of any Eurida Primary CA Certificates are retained for at least 5 years after the Certificates has been expired or posted on the revocation list.

5.4.4 Protection of audit logs

Logs are classified as confidential and are treated as such. There are logic access controls for accessing the logs.

Audit logs are only viewed by trusted personnel as specified in the relevant security documentation.

Measures are taken by CA to ensure the functionality for verification of audit logs and to protect the audit logs from unauthorized viewing, modification, deletion, or other tampering.

5.4.5 Audit log backup procedures

Full backup is performed after an event such as signing a CA Certificate or signing a CRL.

5.4.6 Audit collection system (internal vs. external)

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

Vulnerability assessments based on the audit logs are as a minimum carried out whenever a material deficiency is discovered.

5.5 Records archival

Records archival conform to the stipulations described in section 5.4.

5.5.1 Types of records archived

The records archived include the following:

- Records relating to registration information
- Records relating to the CA environmental events
- Records relating to the key management events
- Records relating to the Certificate management events.

5.5.2 Retention period for archive

Stipulations are equivalent to section 5.4.3.

5.5.3 Protection of archive

Archives are subject to logical and physical protection according to Best Practices.

5.5.4 Archive backup procedures

All full archive backups are stored in a secure safe offsite from the CA itself.

5.5.5 Requirements for time-stamping of records

Certificates, CRLs, other revocation database records as well as audit logs contain time and date information.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedure to obtain and verify archive information

No stipulation.

5.6 Key changeover

CA key changeover for Eurida Primary CA will be carried out at latest 5 years before the CA Certificate expiry date. The process facilitates that the new CA Certificate with its public key is made available to Subscribers and Relying Parties. The procedure for this will be the same as the procedure used for the publishing the original CA key.

5.7 Compromise and disaster recovery

For the secure operating CA facilities the CA has developed, implemented and maintains a business continuity plan.

Contracts with the operating environment and other suppliers contain clauses stipulating that CA organization receive immediate attention and service outside of normal working hours, to the extent necessary, in effort to combat the compromise and/or disaster.

5.7.1 Incident and compromise handling procedures

The business continuity plan describes:

- How to restore information systems services and key business functions back to their normal condition.
- In details what, if and how the CA organization intends to run its operation between the disaster that has occurred and the moment when business is restored to its normal condition.
- In details how the CA organization intends to fulfil its obligations with respect to this CPS.

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

Corruption of computing resources, software, and/or data by any operating environment will promptly be reported to CA. ”Kriseteamet” as defined in the Nets Norway AS Quality System convenes, assesses the situation and its consequences and decides on a response to the event according to the agreed procedures.

On incidents of pure corruption of software – i.e. without there being any key compromise or other security compromise involved, an immediate rollback to the latest version known to work will be initiated.

Backups of the following CA information are kept in off-site storage and made available in the event of a compromise or disaster:

- Application logs
- Certificate application data
- Audit data, according to section 5.4
- Database records for all Certificates issued.

Backups of CA private keys are generated and maintained in accordance with section 6.2.4.

5.7.3 Entity private key compromise procedures

In the event of a compromise of the private key of a SubCA the Certificate will be revoked. Requests for revocation must be submitted according to section 4.9.

Upon revocation of the Certificate containing the SubCA public key:

- The revocation will be announced on the CA web site
- Validation services are terminated for the revoked CA public key
- The SubCA will perform a key changeover in accordance with the SubCA CP, following revocation of a CA Certificate in connection with the termination of a CA under section 5.8 of this CPS.

Revocation will effectively stop all verification of Certificates issued under the compromised key. The SubCA shall cease all further use of such private keys.

5.7.4 Business continuity capabilities after disaster

Disaster recovery site has the physical security protections specified in:

- Section 5.1 Physical Security Controls
- Section 5.2 Procedural Controls
- Section 5.3 Personnel Security Controls.

This includes the enforcement of physical security barriers in accordance with section 5.1.1.

The business continuity plan makes provisions for a recovery within the timeframe specified in customer agreements.

The CA organization installs and tests equipment at its primary site to support CA/RA/repository functions following all but a major disaster that would render the entire facility inoperable. Such equipment ensures redundancy and fault tolerance.

5.8 CA or RA termination

Termination is a controlled cessation of CA or RA services. All business partners will receive advance notification. Before termination, the CA or RA will:

- Inform Eurida Primary CA Subscribers about its intention to end operation, with no less than six (6) months' notice
- Make publicly available information about its intention to end operations, with no less than 3 months' notice
- Stop issuing CRL information (by CRL and OCSP), and thereby inherently deem all issued Certificates as revoked. Alternatively revoke the Certificates prior to issuing the last CRL
- Ensure the secure preservation and maintenance of all relevant databases, archives, records and documents, for these to be made available on request for a commercial reasonable period of time, not less than 5 years after CA or RA termination.

Continued storage of these will be according to provisions laid out in this CPS.

The requirements of this section may be varied by contract, to the extent that such modifications affect only the contracting parties.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

The Eurida Primary CA keys have been generated by Eurida Primary CA in a dedicated Hardware Secure Module (HSM) that meets the requirements identified in FIPS 140-2 level 3 [6].

CA Key Generation was performed under the operation and supervision of two acknowledged Security Officers inhabiting the skill to perform the generation. CA keys generation procedure is described in details in Key Generation Ceremony documentation.

SubCA key pairs will be generated in highly secured premises in a HSM. Routines are in place to prevent loss, modification, or unauthorized use of private keys.

6.1.2 Private key delivery to End User

Not applicable.

6.1.3 Public key delivery to Certificate issuer

During generation of the private/public key pair for the Eurida Primary CA the public key was made available as a Certificate request complying with the PKCS#10 standard.

SubCA after generation of its private/public key pair will also generate a PKCS#10 certification request which will be delivered to Eurida Primary CA. Eurida Primary CA will then verify that:

- The public key has not been altered during transit
- The Certificate applicant possesses the private key corresponding to the transferred public key.

6.1.4 CA public key delivery to Relying Parties

The Eurida Primary CA Certificate is made available to Relying Parties via http://ca.eurida.com/ca/euridaprimary.cer.

6.1.5 Key sizes

Key pairs have sufficient length to prevent others from determining the key pair's private key using exhaustive search during usage period for such key pairs. Eurida Primary CA private keys as well as SubCAs private keys are set to a minimum of 2048 bits RSA keys.

6.1.6 Public key parameters generation and quality checking

To ensure high quality the key parameters are generated and tested according to techniques similar to those described in ETSI TS 102 176-1 [7].

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

Key Usage extension of Certificates is populated in accordance with RFC 5280 [8].

6.2 Private key protection and cryptographic module engineering controls

The Eurida Primary CA keys are stored in HSM's inside security zones to prevent the loss, modification, or unauthorized use of the private keys.

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

The CA ensures that CA keys are generated in accordance with industry standards, see [4], annex II (g) and annex II (f).

In particular:

- Certification Authority key generation is undertaken in a physically secured environment by personnel in trusted roles under at least dual control. The personnel authorized to carry out this function are limited to those required to do so under the CA practices
- CA key generation is carried out within a device which meets the requirements identified in FIPS 140-2 level 3 [6] or higher.

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

Multi-person control is enforced to protect the activation data needed to activate CA private keys, and it is described in an appropriate documentation.

6.2.3 Private key escrow

Eurida Primary CA does not escrow any private keys.

6.2.4 Private key backup

Eurida Primary CA private keys and the SubCAs private keys are backed up.

Private keys that are backed up are protected from unauthorized modification or disclosure.

When outside the signature-creation device, the CA private key is encrypted.

The CA private key is backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment. The personnel authorized to carry out this function are limited to those required to do so.

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

6.2.5 Private key archival

There is no private key archival.

6.2.6 Private key transfer into or from a cryptographic module

In the event that a private key is to be transported from one cryptographic module to another, the private key is encrypted during transport.

6.2.7 Private key storage on cryptographic module

Eurida Primary CA private keys have been generated in and by a hardware cryptographic module. Private keys never exist in plain text form outside the cryptographic module boundary.

6.2.8 Method of activating private key

Only trusted personnel have access to any private keys belonging to Eurida Primary CA. Private keys are activated by two Key Custodians, by supplying their activation data which is stored on secure media.

Once the private key has been activated it will be deactivated according to procedure when the session is finished. The procedure is described in key ceremony documents.

6.2.9 Method of Deactivating private key

When no longer in use, the private keys are deactivated.

Deactivated private keys are protected and kept securely.

6.2.10 Method of destroying private key

The CA private keys stored on CA cryptographic hardware are destroyed upon device retirement. All handling of the CA private keys is witnessed and documented.

6.2.11 Cryptographic module rating

The cryptographic modules used by the CA are validated to FIPS 140-2 level 3 [6] standards.

6.3 Other aspects of key pair management

6.3.1 Public key archival

All issued Certificates including public keys are stored in the CA Certificate database.

6.3.2 Certificate operational periods and key pairs usage periods

The Certificates have a defined, limited usage period.

The validity period for the Eurida Primary CA Certificate is set to a period not exceeding a maximum of twenty (20) years. The validity period for SubCA under Eurida Primary CA is set to a period not exceeding a maximum of fifteen (15) years.

6.4 Activation data

Activation data are referred to as data values other than whole private keys that is required to operate private keys or cryptographic modules containing private keys.

6.4.1 Activation data generation and installation

See clause section 6.2.

6.4.2 Activation data protection

See clause section 6.2.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

All CA and RA functions take place on Trustworthy Systems.

6.5.1 Specific computer security technical requirements

Access to Nets Norway AS production facilities are limited and supervised. The facilities are protected by multiple security zones. Access to each zone as well as logical access to machines, software and databases is protected as described in the relevant security documentation.

Production networks are logically protected and supervised.

6.5.2 Computer security rating

Computer security rating follows ETSI TS 101 456 standard [3] requirements for Trustworthy Systems deployment and maintenance or equivalent.

6.6 Life cycle technical controls

This section addresses system development- and security management controls.

6.6.1 System development controls

CA and RA use a design and development process that enforces quality assurance and process correctness – see Nets Norway AS Quality System.

6.6.2 Security management controls

The CA organization has policies in place to control and monitor the configuration of their systems.

6.6.3 Life cycle security controls

The integrity of the CA software is periodically verified. All configurations on the CA systems are supervised.

6.7 Network security controls

Eurida Primary CA and SubCAs perform CA and RA functions using networks secured according to Best Practices. The controls aim to prevent and detect unauthorized access and tempering attempts.

All communications of sensitive information between the CA and RAs are protected by use of point-to-point encryption for confidentiality, and electronic signatures for non-repudiation and authentication.

6.8 Time-stamping

For Eurida Primary CA

Before Eurida Primary CA is used for CA or CRL signing, the clock are checked and corrected as needed. A trusted time source is used for this purpose.

For SubCAs

All data related to Certificate life-cycles, as well as data stored for auditing and archiving purposes are given date and time with the use of a trusted time source.

7 CERTIFICATE AND CRL PROFILES

This chapter specifies the Certificate and CRL format. This includes information on profiles, versions, and extensions used.

7.1 Certificate profiles

The Certificate profiles are based on RFC 5280 [8]. The Certificate profile used for issuance of SubCA Certificates is included in section 7.1 of the Eurida Primary CA CP.

For each SubCA, the SubCA Certificate profiles are documented in the corresponding PKI-configuration documentation maintained by Nets Norway AS. PKI configuration documents are classified as confidential.

7.1.1 Version numbers

No stipulation.

7.1.2 Certificate extensions

No stipulation.

7.1.3 Algorithm object identifiers

No stipulation.

7.1.4 Name forms

No stipulation.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object I

No stipulation.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extensions

No stipulation.

7.2 CRL Profile

The CRL profile is based on RFC 5280 [8] and described in detail in section 7.2 of the Eurida Primary CA CP. The CRL profile is also documented in the Eurida Primary PKI configuration documentation maintained by Nets Norway AS.

7.2.1 Version number(s)

No stipulation.

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP Profile

Not applicable.

7.3.1 Version number(s)

Not applicable.

7.3.2 OCSP extensions

Not applicable.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices specified in this CPS have been designed to meet or exceed the requirements of generally accepted industry standards related to the operation of CAs.

8.1 Frequency or circumstances of assessment

Compliance Audits are conducted at regular intervals. This applies to CA signing operation, RA operation, and is conducted as external audits or self-assessments.

8.2 Identity/qualifications of assessor

The auditor who performs the compliance audit is required to provide formal proof of qualification including:

- Has a documented history of auditing security sensitive information systems
- Abides by and conforms with the applicable standards and best practices as set forth by the relevant standards committees
- Is knowledgeable about the operations of the CA and has an expertise in public key security technology, data centres, personnel controls, and other relevant fields of interest
- Be certified by ISACA as Certified Information Systems Auditor.

Unless there exist any contradictory indications, an auditor complying with ISO 17021 standards [10] for accreditation bodies will be deemed qualified.

8.3 Assessor's relationship to assessed entity

The auditor or closely related persons to the auditor shall have no financial or other interest in the entity being audited including but not limited to ownership, shares and options that could create a significant bias in the auditor's evaluation.

8.4 Topics covered by assessment

Following topics are as a minimum covered:

- Documentation
- Contingency
- Accountability
- Personnel training
- Ownership to processes
- Compliance statement
- Access control, both physical and logical
- Logging
- Change control

- Exception handling.

8.5 Actions taken as a result of deficiency

Any findings making the RA and CA services unconformable with this document are reported.

Nets Policy Management Authority (PMA) assesses any risk associated with the deficiency, and proposes a time schedule for correcting deficiencies.

The Eurida Primary CA Certificate and any SubCA Certificates will be revoked, and all parties will be informed if the Eurida Primary CA finds the deficiency to be fatal.

The CA may, at its own discretion, revoke all RA Certificates if the audit discloses material defects in the operations of the RA.

8.6 Communication of results

The results of each audit are reported directly to the Policy Management Authority and any other appropriate entities that may be entitled to a copy of the results by law, regulation, or agreement.

In cases where CA subcontracts services that are within the CA responsibility, the CA shall be informed of the result of any relevant audits.

9 Other Business and Legal Matters

9.1 Fees

Nets Norway AS may charge fees for the provision and usage of the Certificates and appurtenant services regulated by this document.

9.1.1 Certificate issuance or renewal fees

Certificate issuance or renewal fees will be regulated in agreements between each CA and its Subscribers.

9.1.2 Certificate access fees

Nets Norway AS is entitled to charge for revocation access.

9.1.3 Revocation or status information access fees

No stipulation.

9.1.4 Fees for other Services

For SubCA's managed or hosted by Nets Norway AS, there will be Subscriber arrangements not regulated by this CPS.

9.1.5 Refund Policy

No stipulation.

9.2 Financial responsibility

Eurida Primary CA has sufficient financial resources to maintain its operations as set out in the CP.

9.2.1 Insurance Coverage

Nets Norway AS maintains third party insurance coverage for its liabilities (errors and omissions) to other participants, including SubCA, Subscribers, and Relying Parties.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of confidential information

The types of information listed below are kept confidential by the Eurida Primary CA. SubCAs and RAs are also obliged to keep the same information confidential.

- Subscriber and End User information that does not appear in the Certificates
- The CA and RA private keys
- Audit information
- Transactional information
- Information deemed to be handled as confidential according to applicable law
- Operational and technical information that should be kept confidential due to security requirements in applicable security practice standards.

9.3.2 Information not within the scope of confidential information

All information that is not within the scope of confidential information specified in section 9.3.1, or within the scope of private information specified in section 9.4.2 is not considered as confidential.

9.3.3 Responsibility to Protect Confidential Information

Confidential information is only disclosed in compliance with applicable non-disclosure clauses.

Upon a valid request, a Subscriber may view confidential information that is stored within the CA or RA solely associated with the Subscriber.

9.4 Privacy of personal information

9.4.1 Privacy plan

The received data from Subscribers is solely used for the purpose of issuance and use of Certificates and/or directly related certification services and is handled in accordance with the Norwegian Personal Data Act and regulations given under the provisions of law and the EU data privacy directive in force [11].

9.4.2 Information treated as private

The following types of information are to be treated private by CAs and RAs:

- Subscriber data that does not appear in the SubCA Certificate.

9.4.3 Information not deemed private

All information that is not within the scope of private information specified in section 9.4.2, or that is not deemed private according to the Norwegian data privacy law and regulations and EU directives in force, is not considered private.

9.4.4 Responsibility to protect private information

Upon a valid request, a SubCA is permitted to view private information that is stored within the CA or RA and that is solely associated with the SubCA.

For Eurida Primary CA, the following will apply:

- The received data from Subscribers will be used solely for the provision of SubCA Certificates and/or CRL services.

9.4.5 Notice and consent to use private information

Unless otherwise specified in applicable local privacy laws, no private information is used by Nets Norway AS without consent of the legal entity and/or natural person to whom the information applies.

9.4.6 Disclosure pursuant to judicial or administrative process

Disclosure of information to third party, including but not limited to public authorities, police and court of justice will be performed in accordance with Norwegian law.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

All title, copyrights, trademarks, service marks, patents, patent applications, knowhow and all other intellectual proprietary rights now known or hereafter recognized in any jurisdiction (the IP Rights) in and to Nets Norway AS technology, web sites, documentation, products and services (the Proprietary Materials), whether registered or not, are owned and will continue to be exclusively owned by Nets Norway AS and/or its licensors.

A SubCA has the right to the Certificates issued to the SubCA and related documentation, including the right to require suspension or revocation of the Certificate.

Rights to names, title, trademark and/or company names protected by law remains with the rightful owner or licensee. SubCA is responsible for obtaining authorization, if necessary, to use such names etc in the Certificate.

9.6 Representations and warranties

9.6.1 CA Representations and warranties

Eurida Primary CA ensures that:

- Information included in SubCA Certificates conforms with information provided by the Subscribers in the SubCA Certificate application
- At the time of issuance, the Subject of the Certificate is in possession of the private key that corresponds to the public key included in the Certificate
- Issued Certificates conform with stipulations in this CPS
- Its operations and services comply to stipulations described in this CPS

The SubCA obligations are:

- Keep its private key private, which means that no entity other than the SubCA shall be given access to the private key.
- Submit accurate, true and correct information during the Certificate application process.
- Use the Certificate for purposes consistent with this CPS.

9.6.2 RA Representations and warranties

The technical infrastructure of the RA services is operated by Nets Norway AS.

RA obligations are:

- Authenticate the identity of the subject
- Depending on the service requirements, validate the connection between a public key and the requester identity including a suitable proof of possession method of the corresponding private key
- Adhere to the agreement made with the corresponding CAs.

9.6.3 Subscriber Representations and warranties

No stipulation.

9.6.4 Relying Party Representations and warranties

Relying Party obligations are:

- Check for the most recent revocation status information regarding all Certificates in the Certificate chain.
- Validate all signatures in the chain.
- Read the CPS, Certificate information and applicable instructions imposed by RA and CA, and independently decide whether or not to rely on a Certificate.
- Assess the quality of the signature creation system, and decide whether it produces signatures of sufficient quality for the intended purpose.

Relying Parties bear any legal consequences of their failure to perform the Relying Party obligations specified in this CPS.

9.6.5 Representations and warranties of other Participants

No stipulation.

9.7 Disclaimers of warranties

The SubCA Certificate does not tell whether, to what extent or in which context the SubCA is authorized to represent the Subscriber.

Nets Norway AS does not warrant: The accuracy of any unverifiable piece of information contained in Certificates except as it may be stated in the CP.

9.8 Limitations of liability

Unless specified otherwise in business agreements, Nets Norway AS is not liable to any End User for damages arising from use of an End User Certificate.

Nets Norway AS is under no circumstances responsible for loss of data, loss of earnings or any other derived and indirect losses unless this is due to culpable negligence or willful misconduct.

Nets Norway AS is under no circumstances liable to RA unless otherwise agreed in a separate agreement.

9.9 Indemnities

Nets Norway AS assumes no financial responsibility for improper use of Certificates, Certificate status information or other information regulated by this CP.

To the extent permitted by applicable law, Nets Norway AS and RAs shall be indemnified by Subscribers for any loss or claim arising out of the Subscriber's failure to conform to the stipulations in this document.

9.10 Term and termination

Present CPS remains in force until notice of the opposite is communicated by Nets Norway AS, on the website: http://ca.eurida.com/repository.

Notified changes shall be appropriately marked by an indicated version.

9.10.1 Term

This document becomes effective according to the date indicated on the front page. No term is set for its expiration.

9.10.2 Termination

This CPS remains effective until it is superseded by a newer version.

9.10.3 Effect of termination and survival

The CPS document is archived for at least 5 years after the last Certificate issued under this CPS expires or is revoked.

9.11 Individual notices and communications with participants

All notices and other communications which may or are required to be given pursuant to the present CP SHALL be in writing and addressed to:

Postal Address:

Nets Policy Management Authority,
Nets Norway AS
0045 Oslo
Norway
+ 47 22 89 89 89 (phone)

E-mail: esec-eid-no@nets.eu

Website: www.nets.eu

9.12 Amendments

The Nets Policy Management Authority (PMA) is authorized to make amendments and updates to this CPS. Any amendments shall be approved by the Nets CA Management.

9.12.1 Procedure for amendment

The only changes that may be made to these CPS specifications without notification are minor changes that do not affect the assurance level of this CPS.

Errors, updates, or suggested changes to this document will be communicated to the PMA as identified in the present document. The request must include a description of the change, consequence analyze, and contact information of the person requesting the change. The PMA shall accept, modify or reject the proposed change after completion of a review phase.

It is at PMAs discretion to dictate that changes to the CPs be posted on the CA web page, without delay, with immediate effect, if it considers this to be necessary to prevent a security breach or stop a security violation. The CA shall contact Relying Parties and communicate the change as soon as possible.

When receiving suggestions for changes, CA has to take due consideration to the fact that any change may effect a wide population of Certificate Holders and Relying Parties.

9.12.2 Notification mechanism and period

Proposed material changes will be posted on the CA web page. PMA will encourage users to comment upon them, stipulating a time frame within which comments will be taken into consideration.

Based on the comments and the PMA view, CA may decide to withdraw the proposed changes, amend them and republish them for further comments, or to publish them as changes to the CPS.

All changes to the present CPS, other than editorial or typographical corrections or contact detail changes will be subject to an incremented version of the document Object Identifier for the present CP.

9.12.3 Circumstances under which OID must be changed

Major changes that may materially change the acceptability of Certificates for specific purposes require corresponding changes to the CPS OID. Minor changes to this CPS do not require a change in the CPS OID that may be communicated by the CA.

9.13 Dispute resolution provisions

Parties will attempt to resolve any dispute that may arise from or in connection with this CPS amicably. Any dispute arising from or in connection with this CPS which cannot be resolved through negotiations, may finally be resolved by Norwegian courts. The legal venue shall be Oslo, Norway.

9.14 Governing law

This CPS is constructed and shall be interpreted in accordance with Norwegian Law.

9.15 Compliance with applicable law

The present CPS and provision of Nets Electronic ID Services are compliant to relevant and applicable Norwegian laws.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

This CPS supersedes any prior agreements, written or oral, between the parties covered by the present document unless specifically stated otherwise in the prior agreements.

This CPS shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances and intended usage of a product or service. In interpreting this CPS, parties shall also take into account the international scope and application of the services involved.

9.16.2 Assignment

The rights and obligations detailed in this CPS are assignable by the parties, by operation of law or otherwise, provided such assignment is undertaken consistent with this CPS articles on termination or cessation of operations.

9.16.3 Severability

Should a clause of the present CPS be deemed as being invalid, in conflict with Norwegian law, or the governing law of any PKI Participant because it has been declared invalid or unenforceable by court or other law-enforcing entity, the clause should be removed or replaced by a valid clause by the PMA. The PMA also evaluate the implications for the remainder of the CPS, which otherwise remain in force. Clauses deemed unclear or unenforceable are otherwise interpreted in such manner as to affect the original intention of the parties.

Each and every provision of this CPS that provides for a limitation of liability, disclaimer of or limitation upon any warranties or other obligations, or exclusion of damages is intended to be severable and independent of any other provision and is to be enforced as such.

9.16.4 Enforcement

This CPS is enforced as a whole, whilst failure by any person to enforce any provision of this CPS is not deemed a waiver of future enforcement of that or any other provision.

9.16.5 Force majeure

Events that are outside the control of Nets Norway AS, will be dealt with immediately by the PMA.

Nets Norway AS is not liable for any breach of its obligations, representations, warranties, or for its failure to perform where such failure or breach is as a result of a Force Majeure Event, including, but not limited to, labour dispute, strike, lockout or interruption or failure of electricity, phone or computer network service or any other system operated by any other party over which Nets Norway AS has no control, or other similar causes beyond reasonable control where Nets Norway AS is without fault or negligence.

9.17 Other provisions

No stipulation.