Nets Electronic ID Services

Eurida Primary CA Certificate Policy

Version 1.1

Effective Date: February 12, 2014

Given, by authority:

Nets CA Management
Haavard Martinsens vei 54
N- 0045 Oslo
Norway

Document OID: 2.16.578.1.15.1.3.3.1.1.0

Copyright

Disclaimer

Nets Norway AS has provided the information in this document for use by 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: Public key and other Subject related information signed by a CA. A Certificate binds an unambiguous name assigned to the Subject of the Certificate to its public key.

Certificate Revocation List (CRL): A periodically generated list of revoked Certificates belonging to a specific CA. A CRL is normally signed by said 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]

Collaboration Document: A document which describes the ways of communicating between Nets and the owner of a SubCA.

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

Eurida Primary CA: The organization which is the Certification Authority for the Eurida Primary CA Certification Hierarchy.

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

ISACA: Information Systems Audit and Control Association.

Key Custodians: A trusted role with responsibility to protect the private keys used in key ceremonies.

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.

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.

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

Registration Authority (RA): An entity operating in accordance with 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 act as a Registration Authority itself.

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

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

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): A CA whose Certificate is certified by the Eurida Primary CA, and whose activities are constrained by the Eurida Primary CA CP

Subscriber: An entity subscribing with Eurida Primary CA on behalf of one or more Subjects. Subscribers of Eurida Primary CA SHALL be legal entities.

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] ISO/IEC 17021:2011 (2011 April 01): ”Conformity assessment – Requirements for bodies providing audit and certification of management systems”

[10] 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

[11] http://www.webtrust.org/homepage-documents/item54279.pdf

1 INTRODUCTION

The purpose of Eurida Primary CA is to be a trusted Certification Authority for signing SubCA Certificates. All SubCA's SHALL be delivered on the Nets Electronic ID Services.

The Eurida Primary CA shall itself be signed by an Omniroot root CA which is trusted in browsers, OS's etc.

Eurida Primary CA shall be WebTrust certified [11].

Eurida Primary CA is provided by Nets Norway AS.

This document is the principal statement of policies governing the Eurida Primary CA PKI. It states legal and technical requirements for approving, issuing, managing, using, revoking, and renewing Certificates issued by Eurida Primary CA and provides associated trust for all SubCA's. This CP is not a legal agreement between Nets Norway AS and Eurida Primary CA participants. Contractual obligations between Nets Norway AS and Eurida Primary CA participants are established by means of agreements with such participants.

This CP conforms to the Internet Engineering Task Force (IETF) RFC 3647 [1] for Certificate Policy and Certification Practice Statement construction. In addition this CP also adopts the current version of the CA/Browser Forum requirements as set forth in "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" published at www.cabforum.org.

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".

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document (in uppercase, as shown) are to be interpreted as described in [RFC2119].

1.1 Overview

The Eurida Primary CA and organizations operating on Eurida Primary CA's behalf SHALL be in compliance with Norwegian Law and in particular the Norwegian Act on electronic signatures [2].

The Eurida Primary CA MAY be used for signing of different SubCA's issuing non-qualified Certificates or qualified Certificates in accordance with the requirements for issuers of qualified Certificates, cf. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, as implemented in the Norwegian Electronic Signature Act of 15.th June 2001 nr 81 [2].

All Certificates issued by Eurida Primary CA MAY include a unique CP Object Identifier.

A number of SubCA's MAY exist under the Eurida Primary CA, depending on the commercial arrangements in place between Nets Norway AS and the separate legal entities involved. Each SubCA SHALL operate using its own CP which SHALL pay due regard to the requirements placed on it by the content of this CP.

The authors of this CP are appointed by the Nets Policy Management Authority (PMA). The PMA is responsible for proposing changes to the CP, updating the CP, and soliciting comments to CP.

1.2 Document name and identification

This document is the Eurida Primary CA Certificate Policy (CP). Nets Norway AS, as the policy defining authority, have assigned an Object Identifier for the Certificate Policy specified in this document.

This Eurida Primary CA CP SHALL be 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) certificate-policy(1) cp-version-one(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) cp(1) major-version(1) minor-version(0)}.

1.3 PKI participants

This CP has impact on the following PKI participants:

- Eurida Primary CA
- SubCA's
- PKI Participants of SubCA's
- Registration Authorities
- Subscribers

All the above are collectively called Eurida Primary CA Community Members.

Nets Norway AS is the Eurida Primary CA. Eurida Primary CA SHALL be responsible for adequate RA functions and the dissemination of Certificates.

Nets Norway AS acts as the Registration Authority (RA) under this CP.

In the context of Eurida Primary CA, the community of Subscribers consists of SubCA's who subscribe with the Eurida Primary CA for certification of their Certificate signature keys. The community of Relying Parties is made up of all parties who choose to rely on the Eurida Primary CA Certificate.

1.4 Certificate usage

The Eurida Primary CA is used for signing the CA Certificate of SubCA's.

CA Certificates MAY NOT be used for any functions except CA functions.

Certificates issued under this CP MAY only be used in the community stated in section 1.3.

Key Usage for the Eurida Primary CA Certificate SHALL be 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.

1.5 Policy administration

The Organization responsible for the Eurida Primary CA CP and CPS is the Nets Policy Management Authority.

The postal address for the Nets Policy Management Authority is:

Nets Policy Management Authority
Nets Norway AS
0045 Oslo
Norway

Visiting address:

Haavard Martinsens vei 54, Rommen, Oslo

+ 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 CP.

Approval of this CP and any subsequent amendments SHALL be done by Nets CA Management.

Subsequent amendments to this CP SHALL be in the form of a document containing the amended form of the CP. Updates supersede any designated or conflicting provisions of the referenced version of the CP. The PMA SHALL determine whether changes to the CP require a change in the Certificate Policy 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 Eurida Primary CA. Eurida Primary CA repositories consist of Certificate repositories, CRLs and documentation repositories.

Nets Norway AS SHALL enter into an agreement with any entity participating in providing repository services stipulating:

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

2.1 Repositories

Eurida Primary CA SHALL NOT publish Certificates other than its own CA Certificate as well as the CRL. The repository SHALL be a web server available over HTTP. Eurida Primary CA has no LDAP repository.

2.2 Publication of Certificate information

Eurida Primary CA Certificate SHALL be published at:

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

The Eurida Primary CA CRL SHALL be 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 Nets PMA amendments to the above cited documents SHALL be published as soon as possible after PMA resolutions.

CRLs SHALL be issued at a minimum every 9 months with a validity of 12 months.
Section 4.9.7 of this CP governs the frequency of Certificate status information publication.

2.4 Access controls on repositories

CA SHALL implement controls to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

Subject names appearing in Eurida Primary CA Certificates are authenticated. Eurida Primary CA Certificates will not contain alternative Subject names in Certificate extensions.

Prior to Certificate issuance, Eurida Primary CA is obliged to make a unique identification of the SubCA in question. The ways of executing and documenting this identification SHALL be described in a Certification Practice Statement regulating the certification process.

The certification process SHALL be objected to strict identification and formal name affiliation prior to Certificate issuance.

Eurida Primary CA uses X.509 Names in the Issuer and Subject fields.

Subject names and Issuer names used in the Certificates SHALL follow the RFC5280 standard.

According to requirements of this CP, names included in Certificates have to be as registered. That means that neither pseudonyms nor anonymous names SHALL be used.

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

- Common name SHALL be meaningful.
- Organization name SHALL be meaningful.
- Organization unit SHALL be meaningful.

There SHALL NOT be support for anonymous or pseudonymous Subjects.

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

Names used by enterprises MUST be in accordance with applicable law.

Names that conflict with protected names of persons or enterprises pursuant to law or Intellectual Property Rights SHALL NOT be used by Certificate applicants in their applications. Eurida Primary CA or any SubCA SHALL NOT be obliged to determine whether any name used in a Certificate application is a protected name.

Besides, neither Eurida Primary CA nor any SubCA SHALL resolve any type of conflicts over the possession of a name used in a Certificate application. Eurida Primary CA SHALL be entitled to reject or suspend a Certificate application 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

All key pair generation and Certificate requests SHALL be generated on a safe hardware device which meets the requirements identified in FIPS 140-2 level 3 [6] or higher.

3.2.2 Authentication of organization Identity

Organizations that subscribe with the Eurida Primary CA SHALL sign up their responsibilities by ordinary business procedures.

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 issued by the Eurida Primary CA SHALL be verified.

3.2.4 Non-verified subscriber information

No stipulations.

3.2.5 Validation of Authority

No stipulations.

3.2.6 Criteria for interoperation

No stipulations.

3.3 Identification and authentication for re-key requests

Certificate re-key SHALL NOT be used.

3.3.1 Identification and authentication for routine re-key

No stipulations.

3.3.2 Identification and authentication for re-key after revocation

No stipulations.

3.4 Identification and authentication for revocation request

Revocation procedures SHALL 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 SHALL 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 SHALL revoke the Certificate without delay.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

Controls SHALL be in place that grants that application records are legitimate and correct.

Eurida Primary CA SHALL be entitled to collect application information for administrative and maintenance purposes, or control purposes in national registers, e.g. information to produce invoices, or to inform the SubCA as to when a particular Certificate is about to expire.

4.1.1 Who can submit a certificate application

Certificate applications to Eurida Primary CA SHALL exclusively be submitted by other Certification Authorities.

4.1.2 Enrolment process and responsibilities

The SubCA SHALL have the responsibility of establishing processes to be used for generating and submitting Certificate requests to Eurida Primary CA, and for receiving Certificates from Eurida Primary CA. Said SubCA processes SHALL be in line with the statements of prevailing CP.

4.2 Certificate application processing

All steps of the certification processes SHALL be logged.

4.2.1 Performing identification and authentication functions

Eurida Primary CA SHALL perform identification and authentication of all required information from the applicant as described in section 3.2.

4.2.2 Approval or rejection of certificate applications

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

4.2.3 Time to process certificate applications

The processing of the Certificate application SHALL begin within a reasonable time. There is no stipulation of the time to complete the processing.

4.3 Certificate issuance

All keys SHALL be produced in secure key generation systems. Local security measures SHALL be put in place to ensure the desired level of security.

4.3.1 CA actions during certificate issuance

All CA actions during issuance SHALL be logged.

4.3.2 Notification to subscriber by Eurida Primary CA

After signing a SubCA Certificate the Eurida Primary CA SHALL return the Certificate to the requestor.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

SubCA SHALL be asked to accept the Certificate at the moment of reception of the Certificate.

4.4.2 Notification of certificate issuance by Eurida Primary CA to other entities

No stipulations.

4.5 Key pair and Certificate usage

A Certificate SHALL be used lawfully in accordance with the terms of this CP and the Eurida Primary CA CPS.

Certificates issued by Eurida Primary CA SHALL be used consistently with the Key Usage extension field included in the Certificates.

4.5.1 SubCA private key and Certificate usage

SubCA's SHALL protect their private key from unauthorized use and promptly start the revocation process if the private key is compromised.

SubCA's SHALL discontinue use of the private key following expiration or revocation of the Certificate.

4.5.2 Relying Party public key and Certificate usage

Relying Party SHALL:

- Check for the most recent revocation status information regarding all Certificates in the Certificate chain
- Validate all signatures in the chain
- Read the CP and independently decide for itself whether or not to rely on the Certificates

4.6 Certificate renewal

SubCA's MAY be renewed.

4.6.1 Circumstance for Certificate renewal

The SubCA Certificate MAY be renewed if the current SubCA Certificate is about to expire or expired.

4.6.2 Who MAY request renewal

The SubCA MAY request renewal.

4.6.3 Processing Certificate renewal requests

All steps of the certificate renewal processes SHALL be logged.

4.6.4 Notification of new Certificate issuance to subscriber

After signing a SubCA Certificate the Eurida Primary CA SHALL return the Certificate to the requestor.

4.6.5 Conduct constituting acceptance of a renewal Certificate

SubCA SHALL be asked to accept the Certificate at the moment of reception of the Certificate.

4.6.6 Publication of the renewed Certificate by Eurida Primary CA

No stipulations.

4.6.7 Notification of certificate issuance by Eurida Primary CA to other entities

No stipulations.

4.7 Certificate re-key

Certificate re-key SHALL NOT be used.

If a Sub CA wishes to maintain continuity of Certificate usage, the Sub CA SHALL apply for a new Certificate before validity expires, according to stipulations described in section 4.1.

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 Eurida Primary CA

Not applicable.

4.7.7 Notification of Certificate issuance by Eurida Primary CA to other entities

Not applicable.

4.8 Certificate modification

Certificate modification SHALL NOT be used.

A Subscriber who wishes to modify a Certificate SHALL revoke the Certificate which contains obsolete information, and the Subscriber SHALL apply for a new Certificate according to stipulations described in section 4.1.

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 Eurida Primary CA

Not applicable.

4.8.7 Notification of Certificate issuance by Eurida Primary CA to other entities

Not applicable.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Certificates issued by Eurida Primary CA MUST be revoked if:

- There is a reason to believe that there has been a compromise of the SubCA private key.
- The SubCA has materially breached a material obligation, representation, or warranty under this CP 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 policy or the applicable 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.

4.9.2 Who can request revocation

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

4.9.3 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 a revocation has taken place. When sending the notification, contact information as specified in agreements SHALL be used

When requests are submitted to Eurida Primary CA the following information SHALL be 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 Eurida Primary CA Certificate MUST be submitted to the Policy Management Authority. The reason for the request MUST be well documented.

Revocation SHALL be a decision by the Nets CA Management.

Revocation requests SHALL be submitted as soon as a Subscriber becomes aware that circumstances indicate a reason for requesting revocation.

4.9.4 Revocation request grace period

No stipulations.

4.9.5 Time within which Eurida Primary CA MUST process the revocation request

Processing of revocation requests SHALL take place without delay.

4.9.6 Revocation checking requirements for Relying Parties

Relying Party SHALL check on-line for the most recent revocation status information regarding all Certificates in the Certificate chain before accepting any Certificate or transactions done by the use of Eurida Primary CA.

4.9.7 CRL issuance frequency

CRLs for SubCA Certificates SHALL be issued at least every 9th month with a validity of 12 months.

4.9.8 Maximum latency for CRLs

CRLs SHALL be posted to the repository within a reasonable time after generation.

4.9.9 On-line revocation status checking availability

Certificates revocation status information SHALL be available on-line by consulting the CRL, available according to stipulations described in section 2.2, or by using an OCSP responder if available.

4.9.10 On-line revocation checking requirements

See section 4.9.6

4.9.11 Other forms of revocation advertisements available

No stipulations.

4.9.12 Special requirements regarding key compromise

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

In addition there SHALL exist a Eurida Primary CA private key compromise chapter in each Collaboration Document. This chapter SHALL address the situation in terms of who is to be notified (parties and people) and which actions should be taken.

4.9.13 Circumstances for suspension

Certificate suspension is not supported.

4.9.14 Who can request suspension

No stipulation, see section 4.9.13.

4.9.15 Procedure for suspension request

No stipulation, see section 4.9.13.

4.9.16 Limits on suspension period

No stipulation, see section 4.9.13.

4.10 Certificate status service

The status of Certificates issued by Eurida Primary CA SHALL be available via CRL, at URLs specified in section 2.2.

4.10.1 Operational characteristics

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

4.10.2 Service availability

See section 4.10.1.

4.10.3 Optional features

No stipulations.

4.11 End of subscription

A SubCA MAY end the subscription for a Eurida Primary CA Certificate by not renewing the expired Certificate, or by revoking a valid Certificate.

4.12 Key escrow and recovery

SubCA keys will not be escrowed.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical security controls

The Eurida Primary CA SHALL adhere to the Nets Norway AS Quality System which MAY contain sensitive security information that MAY only be available subsequently to agreements with Nets Norway AS. An overview of the physical security control requirements is described below.

5.1.1 Site location and construction

CA servers, HSMs, repositories and RA servers SHALL be located in physically secured premises, according to [3]. Specifics are described in the relevant security documentation.

There SHALL be high-security zones based on physical and logical barriers.

5.1.2 Physical access

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

5.1.3 Power and air conditioning

The secure premises SHALL have double power supplies from two separate power sources. In addition the building SHALL be supplied with a UPS-battery bank which is dimensioned to maintain the proper voltage until the on-site power plant is on-line and delivering power.

An air-cooling system SHALL be available in secure premises, and temperature and humidity SHALL be controlled automatically and continuously.

5.1.4 Water exposures

All security rooms SHALL be shielded against water exposures.

5.1.5 Fire prevention and protection

Fire prevention and protection systems SHALL be on-line at all times. These SHALL meet or exceed all local safety regulations.

5.1.6 Media storage

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

5.1.7 Waste disposal

CA and RA SHALL 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

Backup SHALL be stored in off-site secure premises. The off-site secure premises SHALL be described in details in the relevant security documentation.

5.2 Procedural controls

This section describes requirements imposed by this CP upon personnel performing trusted roles.

5.2.1 Trusted roles

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

Security procedures for personnel in trusted roles SHALL be in line with the recommendations given in the referenced documents [1], [4] and [5].

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

5.2.2 Number of persons required per task

Personnel involved in PKI operations SHALL have job descriptions defined. The job descriptions SHALL include:

- Separation of duties and least privilege
- Position sensitivity based on duties and access levels
- Background screening
- Employee training and awareness.

Where appropriate, differentiation SHALL be done between general functions and PKI specific functions. These differentiations SHALL include skills and experience requirements.

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 for all jobs on the IT-systems SHALL be used, thus ensuring traceability and feasible auditing conditions.

5.2.4 Roles requiring separation of duties

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

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Eurida Primary CA SHALL employ personnel that possess the expert knowledge, experience and qualifications necessary for providing the certification services and the job function.

Eurida Primary CA personnel SHALL be certified as trusted employees. In addition they SHALL have at least 6 months PKI-experience and MUST have a proven PKI system competence to obtain permission to access to the PKI production system. Immediate supervisor and one security officer SHALL check the skills of all personnel before qualifying them to the PKI system.

5.3.2 Background check procedures

Background check of trusted employees SHALL be performed. The background check SHALL be in accordance with applicable national law.

5.3.3 Training requirements

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

The candidate SHALL prove his/her skills to the supervisor and security officer who perform the authorization.

All persons that are granted access to the PKI facilities SHALL 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 SHALL establish, maintain, and enforce employment policies for the disciplinary actions of personnel resulting from unauthorized actions. Such disciplinary actions SHALL be in accordance with applicable Employment Protection Acts and agreements between employee and employer. As a minimum such agreements MUST NOT be 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

Independent contractors as well as unauthorized CA employees SHALL NOT be left alone in the secured premises, or in any way be left to work alone on the CA system.

In the requisite for independent contractors or unauthorized CA personnel to work in the secured premises, or directly on the CA system in any way, they SHALL be accompanied by two authorized system administrators. The tasks SHALL be well documented and supervised.

5.3.7 Documentation supplied to personnel

During initial training, retraining, or otherwise there will be a need of extended system documentation. During the training period, the personnel SHALL have gained thorough

knowledge of the existing documentation, and part of the appointment to trusted roles SHALL consist of giving access to all the required documentation.

5.4 Audit logging procedures

Processing Centers/RAs/Relying Parties operating or using services covered by this document, MUST keep records of events sufficient to prove, within reasonable doubt that they comply with the provisions of this CP.

All recorded events SHALL 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 following events SHALL be 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.

The CA SHALL ensure that the privacy of Subject information is maintained.

5.4.2 Frequency of processing log

System SHALL be in place that control that events are recorded continuously and as intended.

Logs SHALL be 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 Certificate SHALL be 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

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

Measures SHALL be 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 back-up SHALL be 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 SHALL as a minimum be carried out whenever a material deficiency is discovered.

5.5 Records archival

Records archival SHALL conform to the stipulations described in section 5.4.

5.5.1 Types of records archived

The records archived SHALL be in accordance with section 5.4.1, and they SHALL 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 SHALL be subject to logical and physical protection according to Best Practices.

5.5.4 Archive backup procedures

Archive backup SHALL be stored off-site.

5.5.5 Requirements for time-stamping of records

Certificates, CRLs, other revocation database records as well as audit logs SHALL contain time and date information. Such time information need not be cryptographic-based.

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 SHALL be carried out at latest 5 years before the Eurida Primary CA Certificate expiry date. The process SHALL facilitate that the new CA Certificate with its public key is made available to Subscribers and Relying Parties. The procedure for this SHALL 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 SHALL develop, test, maintain, and implement a business continuity plan.

Contracts with the operating environment and other suppliers SHALL contain clauses stipulating that CA organization SHALL receive immediate attention and SHALL receive 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 SHALL describe:

- 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 CP.

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

Corruption of computing resources, software, and/or data by any operating environment SHALL be promptly reported to CA. ”Kriseteamet” as defined in the Nets Norway AS Quality System SHALL convene, assess the situation and its consequences and decide 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, there SHALL be executed an immediate rollback to the latest version known to work.

Backups of the following CA information SHALL be 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.

Back-ups of CA private keys SHALL be 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 SHALL 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 SHALL be announced on the Eurida Primary CA web site as defined in 2.2.
- Validation services SHALL be terminated for the revoked SubCA public key.
- The SubCA SHALL perform a key changeover in accordance with the SubCA CP, except following revocation of a SubCA Certificate in connection with the termination of a SubCA under section 5.8 of this CP.

Revocation SHALL 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

Business continuity sites SHALL have the physical security protections specified in the requirements described in:

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

This SHALL include the enforcement of physical security barriers in accordance with section 5.1.

The CA organization SHALL have the capability of restoring or recovering operations.

The CA organization SHALL install and test 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 SHALL ensure redundancy and fault tolerance.

5.8 CA or RA termination

Termination is a controlled cessation of a CA or RA service. All business partners SHALL receive advance notification. CA or RA SHALL:

- Inform Eurida Primary CA Subscribers about its intention to end operation, with not less than 6 months' notice
- Make publicly available information about its intention to end operations, with no less than 3 months' notice
- 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 SHALL be according to provisions laid out in this CP.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

The Eurida Primary CA keys SHALL be generated by Eurida Primary CA in a dedicated HSM.

The key generation SHALL be performed under the operation and supervision of two acknowledged security officers inhabiting the skill to perform the generation. The procedure for generating CA keys SHALL be described in details in appropriate documentation.

SubCA key pairs SHALL be generated in highly secured premises in an HSM. Routines SHALL be 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 SHALL be made available as a certificate request complying with the PKCS#10 standard.

Generation of the private/public key pair for a SubCA SHALL also cause a PKCS#10 certificate request to be generated. This PKCS#10 file SHALL be delivered to Eurida Primary CA. In addition, the entity that generates the keys SHALL ensure 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 SHALL be of 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 SHALL be set to a minimum of 2048 bits RSA keys. The same applies to SubCA private keys.

6.1.6 Public key parameters generation and quality checking

To ensure high quality the key parameters SHALL be 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 SHALL be 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 SHALL ensure 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 SHALL be undertaken in physically secured environment by personnel in trusted roles under at least dual control. The personnel authorized to carry out this function SHALL be limited to those required to do so under the CA practices.
- CA key generation SHALL be carried out within a device which meets the requirements identified in FIPS 140-2 level 3 [6] or higher.
- Certification Authority key generation SHALL be performed using an algorithm recognized as being fit for the purpose.

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

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

6.2.3 Private key escrow

Eurida Primary CA SHALL NOT escrow any private keys.

6.2.4 Private key backup

Eurida Primary CA and the SubCA's SHALL back up its private keys.

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

When outside the signature-creation device, the CA private signing key SHALL be encrypted.

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 secured environment. The personnel authorized to carry out this function SHALL be limited to those required to do so.

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.

6.2.5 Private key archival

There SHALL be 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 MUST be encrypted during transport.

6.2.7 Private key storage on cryptographic module

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

6.2.8 Method of activating private key

Only trusted personnel SHALL have access to any Eurida Primary CA private key. Such a private key SHALL be activated by a threshold number of Key Custodians, by supplying their activation data which SHALL be stored on secure media.

Once the private key is activated, it SHALL be active only for one session. The procedure around using a Eurida Primary CA private key SHALL be described in detail in an appropriate documentation.

Unauthorized access to activated private keys in the CA and RA system SHALL NOT be allowed.

6.2.9 Method of deactivating private key

When no longer in use, private keys MUST be deactivated using adequate logout and removal procedures. Deactivated private keys SHALL be protected and kept securely.

SubCA's SHALL deactivate their private keys when they are no longer in use. The process of deactivating private keys MAY include a logout and removal procedure.

6.2.10 Method of destroying private key

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

6.2.11 Cryptographic module rating

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

6.3 Other aspects of key pair management

6.3.1 Public key archival

All public keys SHALL be archived in one or more data store.

6.3.2 Certificate operational periods and key pairs usage periods

The Certificates SHALL have a defined, limited usage period.

The validity period for the Eurida Primary CA Certificate SHALL be set to a period not exceeding a maximum of twenty (20) years.

The validity period for SubCA Certificates SHALL be set to a period not exceeding a maximum of fifteen (15) years.

6.4 Activation data

Activation data SHALL be 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 SHALL take place on trustworthy systems.

6.5.1 Specific computer security technical requirements

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

Production networks SHALL be logically protected and supervised.

6.5.2 Computer security rating

Computer security rating SHALL follow ETSI TS 101 456 standard [3] requirements for trustworthy systems deployment and maintenance.

6.6 Life cycle technical controls

This section addresses system development- and security management controls.

6.6.1 System development controls

CA and RA SHALL use a design and development process that enforces quality assurance and process correctness.

6.6.2 Security management controls

The CA organization SHALL have mechanisms and/or policies in place to control and monitor the configuration of their systems.

Upon installation, and with a given frequency, CA SHALL validate the integrity of the CA system.

6.6.3 Life cycle security controls

Eurida Primary CA SHALL periodically verify the integrity of the CA software and all configurations on the CA systems SHALL be supervised.

6.7 Network security controls

Eurida Primary CA and SubCA's SHALL perform CA and RA functions using networks secured according to Best Practices. The controls SHALL prevent and detect unauthorized access and tempering attempts.

All communications of sensitive information between the CA and RAs SHALL be 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 SHALL be checked and corrected as needed. A trusted time source SHALL be used for this purpose.

For SubCA's

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

7 CERTIFICATE AND CRL PROFILES

7.1 Certificate profiles

The Certificate profiles are based on RFC 5280 [8].

Version X.509 v3 Certificates SHALL be used.

The table below lists contents of Certificates going to be externally visible.

Section	Key	Value		Mand	Edit	Crit
Distinguished Name (DN)	Distinguished Name (DN)	cn=<>, o=<>, c=<>				
	- Country (C)	NO		True	False	
	- Organization (O)	Nets Norway AS – 990224978		True	False	
	- Common Name (CN)	Eurida Primary CA		True	False	
Validity	Start	Time of issuance		True	True	
	End			True	False	
	Maximum Span	20 years		N/A	N/A	
Key properties	Key size	2048		True	False	
	Key Algorithm	RSA		True	False	
	Key Usage	Certificate Signing, CRL Signing		True	False	True
	Key Storage	Hardware		True	False	
	Generation Site	Certificate Authority		True	False	
Extensions	Basic Constraints	IsCA	True	False	False	True
		PathLength	1	True	False	
	Subject Key Identifier	SubjectKeyID	160-bit SHA-1 hash of public key	True	False	
	Authority Key Identifier	AuthorityKeyID	160-bit SHA-1 hash of CA public key No name or serial number	True	N/A	

Section	Key	Value	Mand	Edit	Crit
		included			
Other	Signature algorithm	sha1WithRSAEncryption	True	False	
	DirectoryString character encoding	UTF8	N/A	N/A	

Keystore: HSM

7.2 CRL Profile

The CRL profile SHALL be in conformance with RFC 5280 [8] and as described in details in the table below.

Field	*Format*	Value
Version number	INTEGER	X.509 version 2 CRL
Signature algorithm	AlgorithmIdentifier	Sha256WithRSAEncryption
Issuer DN	Distinguish Name	Subject DN of the CA that issued the CRL
Last update	UTCTime	Specifies when the CRL was generated
Next update	UTCTime	Specifies when the CRL expires
RevokedCertificates:		OPTIONAL if no Certificates are present, otherwise each Revoked Certificate entry consists of three following fields:
.certSerial Numb	INTEGER	The Certificate Serial Number of the revoked Certificate
.revocationDate	UTCTime	The date of the revocation
.crlEntryExtension	Extension	OPTIONAL - ReasonCode MAY be used - InvalidityData is not used
CrlExtension	Extension	- CRLNumber - AuthorityKeyIdentifier (with KeyID only)

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Eurida Primary CA and all SubCA's as well as RA's for Eurida Primary CA and SubCA's SHALL be WebTrust certified [11].

8.1 Frequency or circumstances of assessment

Compliance Audits SHALL be conducted at regular intervals. This applies to CA signing operation and RA operations.

8.2 Identity/qualifications of assessor

The auditor SHALL provide formal proof of qualification. Unless there exist any contradictory indications, the auditor complying with the ISO 17021 standard [9] for accreditation bodies SHALL be deemed qualified. Besides, the auditor SHALL:

- Be certified by ISACA as Certified Information Systems Auditor
- Have a documented history of auditing security sensitive information systems.

8.3 Assessor's relationship to assessed entity

The auditor SHALL have no financial or other interest in the entity being audited, including but not limited to ownership, shares and options.

8.4 Topics covered by assessment

At least the following topics SHALL be covered:

- Documentation
- Exception handling
- 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 CA services unconformable with this document SHALL be corrected.

Nets Policy Management Authority SHALL assess the risk associated with the deficiency, and approve a time schedule for correcting the deficiency.

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

CA MAY, at its own discretion, revoke all Certificates for which a certain organization has acted as RA, if the audit discloses material defects in the operations of the RA.

8.6 Communication of results

The results SHALL be communicated to relevant parties.

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 CP.

9.1.1 Certificate issuance or renewal fees

Certificate issuance or renewal fees SHALL be regulated in agreements between Nets Norway AS and the Subscribers.

9.1.2 Certificate access fees

Nets Norway AS SHALL be entitled to charge for revocation access.

9.1.3 Revocation or status information access fees

No stipulations.

9.1.4 Fees for other services

Fees for other services MAY be regulated in agreements between Nets Norway AS and the Subscribers.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

Nets Norway AS SHALL have sufficient financial resources to maintain its operations set out in this CP.

9.2.1 Insurance coverage

Nets Norway AS SHALL maintain 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 following types of information SHALL be kept confidential by Eurida Primary CA and the SubCA's and RAs:

- Subscriber 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.

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 SHALL NOT be considered as confidential.

9.3.3 Responsibility to protect confidential information

Revealing of information SHALL comply with applicable non-disclosure clauses that as a minimum are in accordance with Norwegian law.

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

Norwegian data privacy law and regulations and the EU directive in force [10] SHALL be respected by the CA. The received data from Subscribers SHALL be used solely for the provision of SubCA Certificates and/or CRL services.

9.4.2 Information treated as private

The following types of information are to be treated private by CA 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, SHALL NOT be considered as 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.

9.4.5 Notice and consent to use private information

Unless otherwise specified in applicable local privacy laws, no private information SHALL be 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 SHALL 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 Obligations

9.6.1 CA representations and warranties

Eurida Primary CA has the obligation to ensure that:

- Information included in a SubCA Certificate conforms with information provided by the Subscriber 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 CP
- Its operations and services comply to stipulations described in this CP.

As a minimum, Subscribers that are organizational entities are obliged to:

- Instruct its members on permitted use of the Certificates.

SubCA obligations are:

- Keep its private key private, which means that no person or application 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 CP.

9.6.2 RA representations and warranties

The technical infrastructure of the RA services SHALL be 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 CP, 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 Party is solely responsible for deciding whether or not to trust a Certificate. Relying Party MUST decide whether information other than information given by CA is necessary in order to decide on fitness for a particular purpose. Relying Party is solely responsible for requesting and/or obtaining such information.

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

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 this CP.

9.8 Limitations of liability

Unless specified otherwise in business agreements, Nets Norway AS SHALL NOT be 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 CP 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 CP remains effective until it is superseded by a newer version.

9.10.3 Effect of termination and survival

The CP document SHALL be archived for at least 5 years after the last certificate issued under this CP 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 CP. 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 CP specifications without notification are minor changes that do not affect the assurance level of this CP.

Errors, updates, or suggested changes to this document SHALL be communicated to the PMA as identified in the present CP. The request MUST include a description of the change, consequence analysis, 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 CP 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 Subscribers and communicate the change as soon as possible.

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

9.12.2 Notification mechanism and period

Proposed material changes SHALL be posted on the CA web page. PMA SHALL 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 review, CA MAY decide to withdraw the proposed changes, amend them and republish them for further comments, or to publish them as changes to the CP.

All changes to the present CP, other than editorial or typographical corrections or contact detail changes SHALL 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 CP OID. Minor changes to this CP do not require a change in the CP OID that may be communicated by the CA.

9.13 Dispute resolution provisions

Parties SHALL attempt to resolve any dispute that may arise from or in connection with this CP amicably. Any dispute arising from or in connection with this CP 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 CP is constructed and SHALL be interpreted in accordance with Norwegian Law.

9.15 Compliance with applicable law

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

9.16 Miscellaneous provisions

There SHALL exist a unique Collaboration Document between Nets and each organization owning a SubCA which has been signed by Eurida Primary CA.

9.17 Other provisions

No stipulation.