DNB PKI
Class G
Certificate Policy

Version 1.4.0

Effective Date: 01.12.2013

Given, by authority:
PMA
DNB Bank ASA
Stranden 21
0021 Oslo
Norway
Email: pma@dnbnor.no

Document OID: <2.16.578.1.31.10.10.1>

List of Contents

DEFINITIONS AND ABBREVIATIONS

ARS: Action Request System. In the context of this document used for Certificate expiry reminders.

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

CA: Abbreviation for Certification Authority.

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

CDP: CRL Distribution Point. A link pointing to the Certificate Revocation List.

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 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 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].

Challenge Phrase: A word or collection of characters, which is used as End User's password in remote authentication to the CA, in order to access Certificate life-cycle services offered by the CA. A Challenge Phrase is not connected to the End User's Certificate.

CMS: Card Management System

CP: Abbreviation for Certificate Policy.

CPS: Abbreviation for Certification Practice Statement.

CRL: Abbreviation for Certificate Revocation List.

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

DN: Abbreviation for Distinguished Name.

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

ISACA: Information Systems Audit and Control Association.

OCSP: Online Certificate Status Protocol

Off-Site Secure Premises: A separate security zone with differentiated personnel authorization from the PKI specific functions.

OID: Abbreviation for Object Identifier.

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

PMA: Abbreviation for Policy Management Authority.

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

RA: Abbreviation for Registration Authority.

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.

RP: Abbreviation for Relying Party.

SEID: Norwegian "Samarbeidprosjekt om eID og eSignatur"

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

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] IETF RFC 2560 (1999): “Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP”, M. Myers VeriSign, R. Ankney CertCo, A. Malpani ValiCert, S. Galperin My CFO, C. Adams Entrust Technologies

[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

[12] WebTrust (www.webtrust.org) in “Trust Services Principles and Criteria”: http://www.webtrust.org/certauth_fin.htm

[13] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.1.6

VERSION HISTORY

Version	Date	Details
1.0	24.02.2011	Initial version
1.1	31.05.2011	Key Archival and VA OCSP services introduced. Both services are planned to be available Q4 2011
1.2	31.06.2011	Corrected after input from CA organization
1.3	08.11.2012	Updated with new profiles and CMS requirements
1.4	02.12.2013	Updateted with WebTrust requirements after 2013 audit

1 INTRODUCTION

This document is the principal statement of policies governing the DnB NOR PKI Class G Certificate Policy (CP). It states, at a general level, the business, legal and technical requirements for approving, issuing, revoking, managing and using DnB *NOR PKI Class G* Certificates. These requirements are provisioned to protect the security and integrity of the DnB NOR PKI and associated trust services.

This CP 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”

The DNB Class G CA’s control processes requirements, as stated in this Certificate Policy (CP), are designed and maintained to stay fully compliant with the requirements and regulations stated by WebTrust (www.webtrust.org) in [12] “Trust Services Principles and Criteria for Certification Authorities”.

In such cases where deviations are discovered, the requirements set down in this CP shall, without undue delay, be aligned to re-establish compliance and implemented accordingly in the CPS.

.

1.1 OVERVIEW

A Certificate Policy, as defined in X.509, is a named set of rules that determines the degree of trust that can be placed on the authenticity of the public keys signed by the Certificate Authority (CA) and the applicability of a certificate to a particular community with common security requirements. This CP is a single document that defines certificate policies for the DnB NOR PKI Class G subdomain of the Nets Eurida Primary Certificate Authority. It covers the requirements of the DnB NOR PKI Class G, and the deployment is covered by a separate Certification Practice Statement (CPS).

The DnB NOR PKI Certificate Service is a Chain Subordinate Authority (CA) of Nets Eurida Primary Certificate Authority, customized to meet the DnB NOR PKI requirements, which in turn is signed by OmniRoot (CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C= IE)

The DnB NOR PKI includes 3 classes of certificates:

DnB NOR PKI Class G: Generic manual- and autoenrolled certificates (covered by this CP).

DnB NOR PKI Class Q: Qualified certificates (**not** covered by this CP)

DnB NOR PKI Class E: Extended Validation certificates (**not** covered by this CP).

The following certificate profiles are handled under DnB NOR PKI Class G:

Manually enrolled:

- DnB NOR Enterprise certificates: Transaction signing and consistency by means of digital signature.
- DnB NOR Authentication Client certificates: Machine, application **client** authentication on the Windows platform: for (SSL, IEEE 802.1x etc)

- DnB NOR Authentication Server certificates: Machine, application **server** authentication on the Windows platform: for (SSL, IEEE 802.1x etc)
- DNB Authentication Server Client: Machine, application **client and server** authentication on the Windows platform: for (SSL, IEEE 802.1x etc)
- DNB NOR Code Signing: Digital signature of code and MS Office documents
- DNB NOR Document Signing: Digital signature of documents
- DNB NOR Email Signing: Digital signature of email (S/MIME)
- DNB Auth IPSec Manual: IP-Sec tunnelling and Outlook Anywhere
- DNB G1 TAM UID Authentication

Card Managment System (CMS):

- DNB G1 End User Smart Card: User authentication, IEEE 802.1x for DNB corporate wireless network.

Autoenrolled:

- DnB NOR Machine Client certificates: Machine, application client authentication on the Windows platform: for (SSL, IEEE 802.1x etc)
- DnB NOR Machine Server certificates: Machine, application server authentication on the Windows platform: for (SSL, IEEE 802.1x etc)
- DnBNORG1-IPSec
- DnB NOR Domain Controller Client certificates: Domain Controller client authentication on the Windows platform
- DnB NOR Domain Controller server certificates: Domain Controller server authentication on the Windows platform
- DnB NOR Encryption certificates: Mail encryption on the Windows platform

The CA and legal entities operating on CA's behalf shall be in compliance with Norwegian Law and in particular the Norwegian Act on electronic signatures [2].

The DnB NOR PKI Certificate Service supports issuance of publicly trusted certificates in line with the requirements of the [13] Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates, v.1.1.6 ("Baseline Requirements"), as published by the Certification Authority / Browser Forum ("CAB Forum Guidelines") at http://www.cabforum.org.

Certificates issued in line with Baseline Requirements, as stated above, shall contain the following policy identifier in the certificatePolicies extension:

OBJECT IDENTIFIER::= {joint-iso-itu-t(2) country (16) norway (578) organisasjon(1) dnbnor(31) policies(10) certifikatepolicy (10) DnB NOR PKI Class G (1) }.

1.2 DOCUMENT NAME AND IDENTIFICATION

This CP is identified by the following unique object identifier (OID):

Enterprise OBJECT IDENTIFIER::=

{joint-iso-itu-t(2) country (16) norway (578) organisasjon(1) dnbnor(31) policies(10) certifikatepolicy (10) DnB NOR PKI Class G (1) }.

1.3 PKI PARTICIPANTS

This CP has impact on the following PKI participants:

- Certification Authority
- Registration Authorities
- Subscribers
- End Users
- Relying Parties

1.3.1 CERTIFICATION AUTHORITY

DnB NOR ASA PKI Class G is the Certification Authority (CA) issuing DNB ASA Class G certificates. The DnB NOR CA is signed by Nets Eurida Primary Certificate Authority. DnB NOR is responsible for the Registration Authority.

1.3.2 REGISTRATION AUTHORITIES

DnB NOR employees and other approved associates may become Registration Authorities administrators under this Policy. Registration Authorities may perform parts of, or all RA functions depending on the rights granted.

1.3.3 SUBSCRIBERS

There must be an agreement between DnB NOR and the subscriber prior to accepting any certificate requests. Typical subscribers will be DnB NOR End Users (Card portal- (CMS-) and autoenrolled certificates for authentication, digital signature and encryption), System administrators requesting certificates for server authentication and PKI enabled applications.

1.3.4 END USERS

End Users under this CP are DNB employees, DNB partners and customers that are subjects to DnB NOR PKI Class G Certificates. SSL server certificates shall only be issued to DNB internal systems and services.

1.3.1 RELYING PARTIES

Relying Party is any party that accepts to rely on the security enforced by the DnB NOR PKI Class G.

1.3.2 OTHER PARTICIPANTS

No stipulations

1.4 CERTIFICATE USAGE

1.4.1 *Applicability*

This CP applies to DnB NOR PKI Class G. Certificates issued under this CP may only be used by participants listed under section 1.3, and provision some or all of the following security services:

- Confidentiality
- Authentication
- Integrity
- Non-repudiation

The Relying Party shall take into account the key usage purpose stated in the Certificates.

The issued keys and certificates are to be used on DNB client PC's and servers and on client PCs and servers of DNB customers to whom a valid agreement exist for the service requiring the certificate.

PCs and servers may be subject to malicious software being introduced, e.g. software that performs functions other than those intended. This CP does not deal with or protect against such malicious software.

1.4.2 *Appropriate Certificate uses*

All use of Certificates shall be in accordance with National law, this CP, ethical business standards and guidelines enforced by DNB ASA.

The Certificates are most commonly used for network and application authentication, electronic signatures, secure e-mail, file encryption, and authentication of clients and servers in secure communications.

1.4.3 *Prohibited Certificate uses*

The Certificates must not be used in defiance of applicable law, official rule, this CP or the corresponding CPS under which the certificates have been issued or in defiance of an agreement with the CA or guidelines given by the CA.

1.5 Policy administration

1.5.1 *Organization administering the document*

This CP and the corresponding CPS shall be administered and approved by the DNB Policy Management Authority (PMA).

1.5.2 *Contact person*

PMA

DNB

Stranden 21

0021 Oslo

Norway

Email: pma@dnbnor.no

1.5.3 *Person determining CPS suitability for the policy*

The suitability and applicability of the DnB NOR PKI Class G CPS shall be reviewed and approved by the DNB Policy Management Authority and legal department.

1.5.4 *CP APPROVAL PROCEDURES*

The DNB PKI Class G CP and any amendments made to it, shall be reviewed and approved by the DNB Policy Management Authority. Amendments to the CP may be made by reviewing and updating the entire CP or by publishing an addendum. The current version of the CP is always made available to the relying parties through the DNB repository as specified in section 2.2 Publication of Certificate information. All updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in Section: 5.4 Audit logging procedures of this CP.

1.6 DEFINITIONS AND ACRONYMS

See Definitions and Abbreviations.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

DNB ASA is responsible for publishing and managing repositories for the CA. The CA shall as a minimum have repositories for Certificates, CRLs, and documentation. These responsibilities may be a part of the agreement with- and delegated to an external CA Operator.

2.2 PUBLICATION OF CERTIFICATE INFORMATION

The CA Certificates shall be published at:

http://crl.dnbnor.no/DnB-NOR-ASA-PKI-Class-G.cer

Revocation information shall be published according to the CDP of the certificates at:

http://crl.dnbnor.no/class-g.crl

Revocation information shall be made available according to the Authority Information Access (AIA) at:

http://va.dnbnor.no/

Encryption certificates shall be published in the DNB Active Directory

The current versions of the following standard documents are published on the Internet at:

- Certificate Policy is made electronically at: http://pki-repository.dnbnor.no/

Agreements are kept in the DNB Archive according to section: 5.5 Records archival.

2.3 TIME OF FREQUENCY OF PUBLICATION

Updates to the CP are published in accordance with Section 9.12 Amendments. Updates to the Subscriber Agreement template, Relying Party Agreements, and other agreements posted on the repository are published as often as deemed necessary.

Section 4.9.7 CRL issuance frequency of this CP governs the frequency of certificate status information publication.

2.4 ACCESS CONTROLS ON REPOSITORIES

Access to the repository shall comply with the LDAP v.3 protocol for data stored in LDAP directories and with http or https for data stored at DNB websites.

Controls to prevent unauthorized access that may lead to adding, deleting, or modifying repository entries shall be implemented.

Queries against certificate repositories must be specific and qualified. It shall not be possible to browse or access certificates by non-explicit queries.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

Subject names appearing in Certificates are authenticated, unless the Certificate profile indicates otherwise. Certificates may contain alternative Subject names (SubjectAlternativeName) appearing in Certificate extensions.

Prior to Certificate issuance, the RA is obliged, on behalf of the CA, to make a unique identification of an End Entity. The ways of executing and documenting this identification shall be described in a binding Certification Practice Statement.

For autoenrolled certificates the internal DNB Directory shall govern the certificate issuance and provide verified End Entity information.

The CPS shall describe authentication/identification procedures for each of the following:

3.1.1 *TYPES OF NAMES*

CA uses X.509 v3 Distinguished Names in the Issuer and Subject fields.

Names are written using the UTF-8 character set. Country codes shall conform to ISO 3166-1 standard.

Names of Organization shall follow the Norwegian SEID standards of semantics for legal entities.

Subject names shall follow the SEID standards for natural persons. Non Norwegian names adhere to the same standards as far as possible.

Subject Distinguished Names used in Certificates shall permit the determination of the identity of the natural person who is Subject to the Certificate.

3.1.2 *NEED FOR NAMES TO BE MEANINGFUL*

Distinguished Names used in Certificates shall be meaningful, i.e. the DNs shall have a commonly understood semantics to determine the identity of the End Entity.

3.1.3 *ANONYMITY OR PSEUDONYMITY OF END USERS*

Use of anonymous or pseudonymous End Users shall not be supported.

3.1.4 *RULES FOR INTERPRETING VARIOUS NAME FORMS*

Distinguished Names shall be interpreted according to X.509 v3 standard.

3.1.5 *UNIQUENESS OF NAMES*

Distinguished Names shall be unique within each certificate service in the sense that one particular Distinguished Name always identifies the same subject; natural person, organisation or system.

3.1.6 *RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS*

Names used by natural persons and/or common names for Organizations must be in accordance with applicable law.

Names that conflict with protected names of natural persons or Organizations pursuant to law or Intellectual Property Rights shall not be used by Certificate applicants in their applications. The CA or any affiliated RA shall not be obliged to determine whether any name used in a Certificate application is a protected name.

Besides, neither the CA nor any RA shall resolve any type of name conflicts due to use of a name in a Certificate application. The CA and affiliated RAs 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*

Not applicable.

3.2.2 *Authentication of organization identity*

Organisations applying for Enterprise certificates shall present an organizational name according to the registered name and organization number (if available). This will constitute the Organization attribute of the Subject Distinguished Name according to the format description in section: 7 Certificate, CRL, and OCSP Profiles.

3.2.3 *Authentication of individual identity*

Authentication of a natural person as an individual identity for issuance of a Certificate shall satisfy the following rules:

The RA must ascertain that the information given by a natural person is provided voluntary and that the End User has got sufficient information and accepted the general terms and conditions in the standard End user Agreement.

3.2.4 *Non-verified Subscriber information*

Not applicable.

3.2.5 *Validation of authority*

Authorized signatories shall present a proof of written power of authority to represent the Organization and otherwise comply with the provisions stated in 3.2.3 Authentication of individual identity. All documentation shall be archived by the Registration Authority according to 5.5 Records archival.

3.2.6 *Criteria for interoperation*

Not applicable.

3.3 Identification and authentication for re-key requests

Not applicable.

3.3.1 *Identification and authentication for routine re-key*

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

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 an RA, or by the CA (see section 4.9.1).

Procedures for authenticating an End User requesting his/her Certificate revoked include:

- Receiving a message from an End User requesting revocation through communication providing reasonable assurance for the requestor identity, i.e. via telephone, facsimile, e-mail, postal mail, or courier service. Under some circumstances the End User may also be requested to answer the End User's Challenge Phrase.

Procedures for authenticating an Organization requesting a Certificate revoked include:

- Receiving a message from a member of the Organization requesting revocation through communication providing reasonable assurance for the requestor identity and membership, i.e. via telephone, facsimile, e-mail, postal mail, or courier service
- Receiving a proof of written power of authority to represent the Organization from the revocation requestor. The form of the proof to be submitted shall be specified in the Subscriber agreement.

Upon positive authentication a Revocation Officer shall revoke the Certificate without delay.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

Controls shall be in place granting that application records are legitimate and correct.

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 End Users as to when a particular Certificate is about to expire.

4.1.1 *WHO CAN SUBMIT A CERTIFICATE APPLICATION*

Certificate applications to the CA shall exclusively be submitted by Registration Authorities.

Natural persons may submit Certificate applications to an RA individually.

4.1.2 *MANUAL ENROLLMENT PROCESS AND RESPONSIBILITIES*

RA shall have the responsibility of establishing the enrolment processes to be used in dissemination services when receiving Certificates from CA.

4.1.3 *AUTO ENROLLMENT PROCESS AND RESPONSIBILITIES*

Authentication certificates for Users and machines shall be available for internal DNB employees, hired personnel authorized by DNB and internal Windows based services.

4.2 CERTIFICATE APPLICATION PROCESSING

All steps of the certification processes shall be logged for future audit. All certification operations shall be auditable in the context of RA-administrator and RA-session.

4.2.1 *PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS*

The RA 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 controls specified in section 4.2.1 are successfully passed, and all other requirements specified in the Subscriber agreement i.e. payment conditions, are satisfied. Otherwise, a Certificate application shall be rejected.

A Certificate application shall however be rejected if the Subscriber is insolvent, bankrupt, has presented false information to RA or CA or there has been proven material breach of previous agreements with RA or CA.

4.2.3 *TIME TO PROCESS CERTIFICATE APPLICATIONS*

The processing of the Certification Request shall be completed within reasonable time, typically within the following business day.

4.3 CERTIFICATE ISSUANCE

The RA is solely responsible for decisions as to whom Certificates are issued and record archival related to the subject authentication.

4.3.1 *CA ACTIONS DURING CERTIFICATE ISSUANCE*

All CA actions during issuance shall be logged. After signing of an End User Certificate the CA shall:

- Return the Certificate to the requesting RA

- Publish the Certificate according to 4.4.2.

4.3.2 *Notification by the RA to the Subject of issuance of Certificate*

The RA shall be responsible for notifying the End User of the issuance of the Certificate.

4.4 Certificate acceptance

4.4.1 *Conduct constituting Certificate acceptance*

End User may be asked to accept the Certificate at the moment of reception of the Certificate. Otherwise, when the End User starts using the Certificate, CA shall consider that the End User has accepted the Certificate and conditions related to the use of the Certificate.

4.4.2 *Publication of the Certificate by the CA*

CA shall publish the Certificate in the predetermined repository according to Certificate Profile specification.

4.4.3 *Notification of Certificate issuance by the CA to other entities*

No stipulations for End Entity certificates.

4.5 Key pair and Certificate usage

4.5.1 *End User's private key and Certificate usage*

- A Certificate shall be used lawfully in accordance with the terms of this CP and the relevant CPS.
- End Users must use Certificates consistently with the Key Usage field extensions included in the Certificates.
- End Users shall protect their private keys from unauthorized use and promptly start the revocation process if the private keys are compromised.
- End Users 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 responsibilities relating to the use of an End User's public key and certificate shall include:

- Checking for the most recent revocation status information regarding all Certificates in the Certificate chain
- Validating all signatures in the chain before accepting the signature
- Reading the CP and independently deciding for itself whether or not to rely on the Certificates
- Assessing the quality of the signature creation system, and deciding whether it produces signatures of sufficient quality.

4.6 Certificate renewal

Certificate renewal shall not be used.

4.7 Certificate re-key

Certificate re-key shall not be used.

4.8 CERTIFICATE MODIFICATION

Certificate modification shall not be used.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 *CIRCUMSTANCES FOR REVOCATION*

The RA has the right to immediately revoke a Certificate if the End User requests revocation or for good reason suspects an abuse. In addition, revocation may be performed for any objective reason, including 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 must be revoked if:

- There is a reason to believe that there has been a compromise of the End User private key, activation data or password that is used to access the private key.
- The End User has materially breached a material obligation, representation, or warranty under this CP and/or an applicable agreement.
- The Subscriber has materially breached an obligation, representation, or warranty under this CP and/or an applicable agreement. All Certificates associated with the Subscriber in question must be revoked.
- The Subscriber is insolvent or bankrupt
- The Subscriber agreement is terminated.
- 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, the Certificate was issued to a person other than the one named as the Subject of the Certificate, or the Certificate was issued without the authorization of the person named as the Subject of such Certificate.
- CA discovers or has reason to believe that a material fact in the Certificate application is false.
- CA determines that a material prerequisite to Certificate issuance was neither satisfied nor waived.
- The information within the Certificate, other than non-verified Subscriber information, is incorrect or has changed.
- The End User requests revocation of the Certificate
- The Certificate has been used in criminal activity or on websites forbidden by RA, CA or the Subscriber.

4.9.2 *WHO CAN REQUEST REVOCATION*

Revocation procedures shall ensure that a revocation has been requested either by an End User, a Subscriber, an RA or the 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 by the Revocation Officer
- Notifying the End User that a revocation has taken place. When sending the notification, contact information stored at the CA shall be used - contact information submitted by the requestor during the revocation request process must not be used. Electronically signed notifications may be used.

When requests are submitted to 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 a CA or RA Certificate must be submitted to the DNB Policy Management Authority (PMA). The reason for the request must be well documented.

4.9.4 *Revocation request grace period*

Revocation requests shall be submitted without undue delay when an End User and/or Subscriber become aware of circumstances indicating a reason for requesting revocation.

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

The processing of the Revocation Request operation by the CA shall be completed without undue delay.

4.9.6 *Revocation checking requirements for relaying 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.

4.9.7 *CRL issuance frequency*

The CRLs shall be published at a maximum time interval of 4 hours and have a validity of maximum 12 hours.

4.9.8 *Maximum latency for CRLs*

CRLs shall be posted to the repository without undue delay after generation.

4.9.9 *On-line revocation status checking availability*

Certificates revocation status information shall be available on-line by consulting the CRL that is 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 stipulation.

4.9.12 *Special requirements regarding key compromise*

PKI participants shall be notified of a compromise, or suspected compromise, of a CA or RA private key. This shall be done by publishing the information on the CA web page. In case of RA or CA key compromise, CA and RA shall inform the PMA without undue delay and initiate actions according to the Nets / DNB Collaboration procedures.

4.9.13 *Circumstances for suspension*

Not applicable

4.9.14 *Who can request suspension*

4.9.15 *Not applicable Procedure for suspension request*

4.9.16 *Not applicable Limits on suspension period*

4.10 Not applicable Certificate status service

4.10.1 *Operational characteristics*

The status of Certificates shall be available via CRL and OCSP through URLs specified in section 2.2.

4.10.2 *Service availability*

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

4.10.3 *Optional features*

No stipulation.

4.11 End of subscription

4.12 Key Archiving and recovery

4.12.1 *Key archiving and recovery policy and practices*

- RA shall be responsible for key recovery of private keys associated to User encryption Certificates.
- Notification of key recovery shall be sent to the email address found in the Subject Alternative Name included in the associated certificate.
- If the key recovery is initiated due to an ongoing public or internal investigation, the notification requirement may be set aside as long as the omission is in accordance with 9.4 Privacy of personal information.

4.12.2 *Session key encapsulation and recovery policy and practices*

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL SECURITY CONTROLS

The PKI shall adhere to internal security documentation which may contain sensitive security information that may only be available subsequently to agreements with the CA Operator. An overview of the physical security controls 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, which is part of the policy set mentioned above.

The requirements are derived from the need to prevent and detect unauthorized access to sensitive information and equipment.

The requirements shall be fulfilled by establishing high-security zones based on physical 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*

CAs and RAs shall back up critical system data. All data shall be protected from water, fire, or other environmental hazards.

5.1.7 *WASTE DISPOSAL*

CAs and RAs 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 PKI 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.

Personnel 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 from the view point of separation of duties and least privilege, determining position sensitivity based on duties and access levels, background screening and 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*

There shall be used personal physical and electronic credentials 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 shall conform to the specifications described in the relevant security documentation.

5.3 PERSONNEL CONTROLS

5.3.1 *QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS*

The CA shall use personnel that possess the expert knowledge, experience and qualifications necessary for providing the certification services and as appropriate to the job function.

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. Two Security Officers 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 security officers 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*

CAs and RAs 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*

Third party 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 need for third party 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 documented and supervised.

5.3.7 *DOCUMENTATION SUPPLIED TO PERSONNEL*

During initial training, retraining, or otherwise there will be 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, and Relying Parties who operate or use 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 events relating to the following shall be logged:

- CA signing key functions, including key generation, backup, recovery and destruction
- Certificate life cycle information, including successful and unsuccessful certificate applications, certificate issuances and certificate revocation requests, including the reason for the revocation.
- The life-cycle of keys managed by the CA, including any Subject keys generated by the CA
- Certificate Revocation List updates, generations and issuances.
- Custody of keys, devices and media holding keys.
- Compromise of a private key.
- Security Related Events.
- Cryptographic hardware security module events, such as usage, de-installation, service, or repair and retirement.
- System downtime, software crashes, and hardware failures.
- CA system actions performed by CA personnel, including software updates, hardware replacements, and upgrades.
- Successful and unsuccessful PKI service access attempts.
- Secure CA facility personnel and visitor entry and exit.
- Updates to the CP and CPS

.

5.4.2 *FREQUENCY OF PROCESSING LOG*

The electronic audit logs shall be stored at two separated locations..

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

Logs intended to give indication of system compromise shall send an alert to associated monitoring system and shall be subject to review if an alert is sent. Logs shall be processed as a minimum during periodic audits.

5.4.3 *RETENTION PERIOD FOR AUDIT LOGS*

All relevant information concerning issuance and use of any Certificates shall be retained for at least 10 years after the Certificates has been expired or posted on the revocation list.

5.4.4 *PROTECTION OF AUDIT LOGS*

Audit logs are classified as confidential and shall be treated as such. There shall be logic access controls for accessing the 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*

There shall be performed incremental backups of the audit logs on a daily basis. Full backup shall be performed at least on a weekly basis. These backups shall be stored in Off-Site Secure Premises..

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, 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 shall be 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 in Off-Site Secure Premises.

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)*

To the extent possible, the archive system shall be internal in-line, i.e. the archival shall be integrated with the production system and implemented as an automated system.

RA systems hosted externally may have archives externally at the RA.

5.5.7 *PROCEDURE TO OBTAIN AND VERIFY ARCHIVE INFORMATION*

No stipulation.

5.6 KEY CHANGEOVER

CA key changeover shall be carried out at latest 5 years before the 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 of CA facilities the CA shall develop, 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 and PMA. The disaster recovery task force 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 Secure Premises 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.

Incremental backups of the CA production data shall be performed at least on a daily basis. Full backup shall be performed at least on a weekly basis. Full system backup shall be performed prior to all configuration changes and upgrade of system components (software and hardware).These backups shall be stored in Off-Site Secure Premises and be retain for a minimum of two consecutive generations.

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 the CA or RA Certificate, the CA or RA Certificate shall be revoked. Requests for revocation of a CA or RA Certificate must be submitted to the Policy Management Authority. The reason for the request must be well documented.

Revocation of a CA Certificate shall be a decision by the Policy Management Authority.

Upon revocation of the Certificate containing the CA public key:

- The revocation shall be announced on the CA web site.
- Validation services shall be terminated for the revoked CA public key.
- The CA shall perform a key changeover in accordance with section 5.6, except following revocation of a CA Certificate in connection with the termination of a CA under section 5.8 of this CP.

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

A new CA key and Certificate shall be created in accordance with section 5.6 of this CP.

RA shall start re-authenticating Subscribers according to section 3.1. Both RA and CA shall prepare for such re-issue of Certificates. New Certificates shall be issued under new CA keys.

5.7.4 *BUSINESS CONTINUITY CAPABILITIES AFTER DISASTER*

Disaster recovery 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 5.1.1.

The CA organization shall have the capability of restoring or recovering operations within twenty-four (24) hours following a disaster with, at a minimum, support of Certificate issuance, Certificate revocation and publication of revocation information.

The disaster recovery plan shall make provisions for the full recovery within one week following disaster occurring at the Processing Center primary site.

The CA organization shall install and test equipment at its primary site to support CA and/or 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 CA or RA service. All business partners shall receive advance notification. CA or RA shall:

- Inform 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 three (3) months notice.
- Stop issuing revocation 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 10 years after CA or RA termination. Continued storage of these shall be according to provisions laid out in this CP.

6 TECHNICAL SECURITY CONTROLS

This chapter describes technical security controls that apply to the PKI participants regarding key generation, user authentication, Certificate registration, Certificate revocation, auditing and archiving.

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 *KEY PAIR GENERATION*

- All keys shall be produced in secure key generation systems. End User keys may be generated remotely from the CA. Local security measures shall be then put in place to ensure the desired level of security.
- CA keys shall be generated by the CA in a dedicated Hardware Secure Module (HSM).
- RA keys shall be generated by the RA in a dedicated Hardware Secure Module (HSM) or a safe hardware device that meets the requirements identified in FIPS 140-2 [6].
- Key generation shall be performed under the operation and supervision of two acknowledged Security Officers inhabiting the skill to perform the generation. CA keys generation procedure shall be described in details in appropriate documentation.
- End User key pairs shall be generated in highly secured premises. Routines shall be in place to prevent loss, modification, or unauthorized use of private keys.

6.1.2 *PRIVATE KEY DELIVERY TO END USER*

CAs and RAs shall ensure secure delivery of private keys to End Entities. Routines shall be in place to prevent loss, modification, or unauthorized use of private keys during the delivery.

6.1.3 *PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER*

In case the keys are not generated within the CA, the public key shall be delivered to the Certificate issuer in a request package complying with the PKCS#10 standard. Besides, 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 CA public key shall be made available to Relying Parties via a DNB website.

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. Minimum key sizes shall be set to 2048 bits RSA for End Entities. CA private keys shall be 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 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*

PKI participants shall take necessary precautions to prevent the loss, modification, or unauthorized use of the private keys.

6.2.1 *Cryptographic module standards and controls*

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 [6] level 3 or higher.

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*

No stipulation.

6.2.4 *Private key backup*

The CA 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*

Private encryption keys shall be archived by a key archival and recovery service. Keys shall be transported and stored in encrypted form. Access to the archived keys shall be granted only to appointed key archive administrators. All access to private encryption keys shall be traceable and subject to auditing.

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

Private keys shall be entered into a cryptographic module so as to prevent loss, theft, modification or unauthorized use of the private key. CA or RA private keys held on hardware cryptographic modules shall be stored in protected memory.

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*

The 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*

The CA Private Key

Only trusted personnel shall have access to any private keys belonging to the CA. 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 has been activated, the private key may be active for an indefinite period until it is deactivated when the CA goes offline.

Similarly, a threshold number of shareholders shall be required to supply their activation data in order to activate an offline CA private key. Once the private key is activated, it shall be active only for one session. The procedure around using an offline CA private key shall be described in details in an appropriate documentation.

The RA Private Keys

Only trusted personnel shall have access to private keys in an RA system. The trusted personnel shall be authenticated by use of a password or PIN before activation of the private keys.

The End User Private Keys

All End Users shall protect the activation data for their private keys against loss, unauthorized disclosure, or unauthorized use. The End User shall activate the private keys by supplying a password or PIN.

If the protected key media with appurtenant software supports PIN or password changes, the End User may change the corresponding PIN or password whenever the End User finds it appropriate. The PIN or password shall never be revealed or transmitted over any network in clear text.

6.2.9 *METHOD OF DEACTIVATING PRIVATE KEY*

Activated private keys in the CA and RA system shall not be able to be accessed unauthorized. When no longer in use, they must be deactivated using adequate logout and removal procedures. Deactivated private keys shall be protected and kept securely.

End Users should 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.

The RA private keys shall be destroyed by deletion and overwritten. This shall be witnessed and documented.

End Users have an obligation to protect their private keys from compromise. All private keys shall if possible be destroyed when they are no longer in use or needed.

6.2.11 *CRYPTOGRAPHIC MODULE RATING*

The cryptographic modules used by the CA shall be validated to FIPS 140-2 [6] level 3 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 stores. Public keys may be archived in the form of a certificate.

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 CA Certificate shall be set to a period not exceeding a maximum of fifteen (15) years.

The validity period for the RA User Certificates are set to a period not exceeding a maximum of three (3) years

The validity period for End Entity Certificates shall be set to a period not exceeding a maximum of five (5) years.

If the Certificate is used for encryption in the validity period, the private key may subsequently be used for decryption purposes after the Certificate has expired or has been revoked. Likewise, the public key may be used for signature verification of data that has been signed within the validity period of the Certificate.

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. Examples are a PIN or a password.

6.4.1 Activation data generation and installation

Passwords and PINs are used as activation data, see clause section 6.2.8. CA shall provide guidance to End Users on how to compose secure password. To the extent possible, CA shall impose automatic and non-circumventable restrictions on password composition.

6.4.2 Activation data protection

When entering activation codes, the End User shall take care to protect the code from compromise. This includes protection against other people observing the code/PIN during entry. Within reasonable doubt, End User shall make sure that the workstation, into which the activation code is entered, is free from malicious software that might compromise the activation code.

End User shall be duly informed on his/hers responsibility before accepting the Certificate.

6.4.3 Other aspects of activation data

To the extent activation data for private keys are transmitted in electronic form or otherwise, CA shall protect the transmission of such activation data using methods that protect against loss, theft, modification or unauthorized use of such private keys.

The activation data or the private key shall be transmitted through registered mail or shall be handed out to the End User present in person.

6.5 Computer security controls

All CA and RA functions shall take place on Trustworthy Systems.

Before invoking End User functions, End User shall take reasonable care to ascertain that the PC has not been compromised.

6.5.1 Specific computer security technical requirements

CA and RA shall ensure that software and data files are maintained on Trustworthy Systems.

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

6.6.1 *SYSTEM DEVELOPMENT CONTROLS*

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

Customer specific RA software may be approved by the CA.

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*

An officer from the CA Operator organization shall periodically verify the integrity of the CA software and supervise all configurations on the CA systems.

6.7 NETWORK SECURITY CONTROLS

The CA 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

All data related to Certificate life-cycles, as well as data stored for auditing and archiving purposes shall contain time information down to seconds, from use of a trusted time source. The system time of RA and CA shall be synchronised and differ by no more than 2 seconds.

7 CERTIFICATE, CRL, AND OCSP 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]. CA Certificate profile and End User Certificate profile are documented in the CA organisation PKI-Configuration documentation

7.2 CRL PROFILE

The CRL profile is based on RFC 5280 [8]. CRL profile is documented in the CA organisation PKI-Configuration documentation.

7.3 OCSP PROFILE

The OCSP profile is based on RFC 2560 [9]. OCSP profile is documented in the CA organisation PKI-Configuration documentation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

Compliance Audits shall be conducted at regular, at least once a year, intervals. This applies to CA signing operation, RA operation, and repository operation and may be conducted as external audits or self-asessments.

CA shall in agreements with RA or other CA subcontractors ensure that compliance audits may be coordinated with the regular compliance audit for the PKI services.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The auditor who perform compliance audit shall provide formal proof of qualification.

The auditor shall:

- Have a documented history of auditing security sensitive information systems.

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.

8.4 TOPICS COVERED BY ASSESSMENT

The following topics shall as a minimum to be covered:

- Documentation
- Exception handling
- Contingency
- Disaster recovery
- Tests
- Accountability
- Personnel training
- Ownership to processes
- Compliance statement
- Access control, both physical and logical
- System logging
- Auditlogs at RA and CA
- Change control.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Any findings making the RA and CA services unconformable with this document shall be reported to Policy Management Authority.

Policy Management Authority shall assess the risk associated with the deficiency, and proposes a time schedule for correcting the deficiency.

The CA Certificate shall be revoked, and all parties shall be informed if the PMA finds the deficiency to be fatal.

The CA Certificate shall be suspended and all parties shall be informed if the situation is deemed serious.

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 shall be communicated to relevant parties.

The CA shall be informed of the result of any relevant audits.

9 Other Business and Legal Matters

9.1 Fees

No stipulation.

9.2 Financial responsibility

9.2.1 *Insurance coverage*

No stipulation.

9.2.2 *Other assets*

No stipulation.

9.2.3 *Insurance or warranty coverage for End Users*

No stipulation.

9.3 Confidentiality of business information

All information pertaining to the CA and RA operation shall be handled on a need-to-know basis by all parties involved.

9.3.1 *Scope of confidential information*

The following types of information shall be kept confidential by the CA and RAs:

- Subscriber and End User information that does not appear in the certificates
- The CA and RA private keys
- Activation data, and Recovery Phrases
- Audit information
- Transactional information
- Information deemed to be handled as confidential according to applicable law, including but not limited to the Norwegian Personal Data Act
- Information deemed to be handled as confidential according to applicable agreement with CA.
- Operational and technical information that should be kept confidential due to security requirements in security practice standards applicable.

9.3.2 *Information not within the scope of confidential information*

Subscribers shall acknowledge that revocation data of all DnB NOR PKI Class G certificates is public information. Subscriber application data published within an issued digital certificate is inherently to be regarded as non-confidential information.

9.3.3 *Responsibility to protect confidential information*

All personnel in trusted positions shall handle all information in strict confidence. CA and RA shall not release any confidential information, unless otherwise required by law, without an authenticated, reasonably specific request by an authorized party.

Responsibilities to protect information shall be stated and regulated in terms and conditions with all PKI participants.

9.4 Privacy of personal information

9.4.1 *Privacy plan*

The Norwegian Personal Data Act and regulations given under the provisions of law and the EU data privacy directive in force [11] shall be respected by the DnB NOR PKI Class G service including the CA Operator. The received data from Subscribers and/or End Users shall be used solely for the purpose of issuance and use of Certificates and/or directly related certification services. The DnB NOR PKI service shall implement routines to ensure compliance to applicable regulations and directives.

9.4.2 *Information treated as private*

The following types of information shall be treated private by CA and RAs:

- Subscriber and End User data that does not appear in the Certificate
- Activation data and Recovery Phrases.

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, in accordance with Norwegian law, an End User is permitted to view private information that is stored within the CA or RA and that is solely associated with the End User.

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 the CA and/or RAs 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 in accordance with Norwegian law.

9.4.7 *Other information disclosure circumstances*

No stipulation.

9.5 Intellectual property rights

The structure of this document is based on:

- RFC 2527
- RFC 3647

9.6 Obligations

9.6.1 *CA obligations*

The conforming CA is responsible for all aspects of the issuance and management of a certificate referencing this CP, including:

- Certificate application/enrollment process.
- Certificate creation process.
- If applicable, posting of the certificate in a public repository.
- Suspension and revocation of the certificate.
- Ensuring that all aspects of the CA services and CA operations and CA infrastructure related to DnB NOR PKI Class G certificates shall be performed in accordance with the requirements, representations, and warranties of this CP.
- Adhere to the agreement made with the RA

By issuing a certificate under this CP, the CA certifies to the subscriber, and to all relying parties who reasonably and in good faith rely on the information contained in the certificate during its operational period, that:

- The CA has issued, and will manage, the certificate in accordance with this CP.
- There are no misrepresentations of fact in the certificate known to the CA.
- The certificate meets all material requirements of this CP.

9.6.2 *RA OBLIGATIONS*

The technical infrastructure of the RA services for DnB NOR PKI Class G is operated by the CA Operator while as the procedural aspect is the responsibility of DNB including:

- Authenticating the identity of the subject
- Depending on the service requirements, validating 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 CA.

9.6.3 *SUBSCRIBER OBLIGATIONS*

Subscribers shall:

- Accurately represent the information required of them in a certificate request.
- Properly protect their private key at all times, against loss, disclosure to any other party, modification and unauthorized use, in accordance with this CP. From the creation of their private and public key pair, subscribers are personally and solely responsible of the confidentiality and integrity of their private keys. Every usage of their private key is assumed to be the act of its owner.
- Upon suspicion that their private keys are compromised, notify the RA and request that the certificate is revoked.
- Upon any change of information in their certificates, notify the RA and request that the certificate is revoked.
- Use the keys and certificates only for the purposes authorized by the RA.
- Authorize the treatment and conservation of their personal data according to applicable service agreements.

9.6.4 *END USER OBLIGATIONS*

End Users shall ensure that:

- Certificates are used lawfully in accordance with the terms of this CP.
- Certificates are used consistently with the Key Usage field extensions included in the Certificates.
- Their private keys are protected from unauthorized use and promptly start the revocation process if the private keys are compromised.
- The use of the private key and certificate are discontinued following expiration or revocation of the Certificate.

9.6.5 *Relying Party obligations*

Relying parties shall:

- Independently make themselves familiar with this CP before drawing any conclusion on how much trust they can put in the use of the certificates.
- Only use the certificate for the prescribed applications and are under no circumstances allowed to use the certificates for forbidden applications.
- Check for the most recent revocation status information regarding all Certificates in the Certificate chain
- When receiving a digitally signed message, verify all digital signatures in the chain before accepting the signature.
- When validating a certificate, check it for its validity, revocation, or suspension.
- Assess the quality of the signature creation system, and deciding whether it produces signatures of sufficient quality.

9.6.6 *Obligations of other participants*

No stipulation.

9.7 Disclaimers of warranties

No stipulation.

9.8 Limitations of liability

No stipulation.

9.8.1 *CA limitations of liability*

No stipulation.

9.8.2 *End User limitations of liability*

No stipulation.

9.8.3 *RA limitations of liability*

No stipulation.

9.9 Indemnities

No stipulation.

9.9.1 *Indemnification by Subscribers*

9.9.2 *Indemnification by Relying Parties*

No stipulation.

9.10 Term and termination

This CP will at a minimum remain in force for the time period stated in 5.8 CA or RA termination, or as long as the PMA deems necessary. During this time period, portions of the document or its applicability to particular participants can be terminated by the PMA.

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 or the termination of the DnB NOR PKI Class G.

Before terminating CA activities, steps shall be taken as described in section 5.8 CA or RA termination.

9.10.3 *Effect of termination and survival*

The CP document shall be archived for at least 10 years after the last certificate issued under CP expires or is revoked.

9.11 Individual notices and communications with participants

Formal communication between CA and RA shall be conducted according to established collaboration procedures.

9.12 Amendments

9.12.1 *Procedure for amendment*

Amendments to this CP shall be administered by the PMA and must undergo the same procedures as for the initial approval. Rephrasing provisions to improve understandability and spelling corrections are not considered amendments.

9.12.2 *Notification mechanism and period*

Amendments to the CP document shall be published on the appropriate DNB repository at least one month before it becomes effective.

9.12.3 *Circumstances under which OID must be changed*

The PMA may decide to change the OID of this CP in case of substantial changes to the policy or CA service.

9.13 DISPUTE RESOLUTION PROVISIONS

Disputes arising from the content of this CP shall, as a first effort, be sought resolved by the PMA. If this turns out not to be possible, the PMA shall determine the appropriate next steps. Before resorting to any dispute resolution mechanism, parties shall agree to notify DNB PMA of the dispute with a view to seek dispute resolution.

9.14 GOVERNING LAW

This CP is constructed, and shall be interpreted, in accordance with Norwegian Law. All legal disputes arising from the content of this CP document, the managed CA service and RAs, the use of their services, the acceptance and use of any certificates or revocation information issued and made available by the DnB NOR PKI Class G shall be treated according to Norwegian Law.

9.15 COMPLIANCE WITH APPLICABLE LAW

This CP is constructed and shall be compliant with Norwegian Law. Activities covered by this CP, initiated from another country must also comply with Norwegian law and the governing law of that country.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 ENTIRE AGREEMENT

This CP supersedes any prior agreements, written or oral, between the parties covered by the present document.

This CP 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 CP, 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 CP shall be assignable by the parties, by operation of law or otherwise, provided such assignment is undertaken consistent with this CP articles on termination or cessation of operations.
.

9.16.3 SEVERABILITY

Should a clause of the present CP 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 shall also evaluate the implications for the remainder of the CP, which otherwise shall remain in force. Clauses deem unclear or unenforceable shall otherwise be interpreted in such manner as to affect the original intention of the parties.
Each and every provision of this CP 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 CP shall be enforced as a whole, whilst failure by any person to enforce any provision of this CP shall not be deemed a waiver of future enforcement of that or any other provision. Agreements between DNB and the parties detailed in this CP may contain additional provisions governing enforcement and shall be enforced according to the terms and conditions set forth within each respective agreement as long as it does not conflict with the general provisions of this CP.

9.16.5 *Force majeure*

Events that are outside the control of the CA, shall be dealt with immediately by the PMA.

9.17 Other provisions

No stipulation.