DNB PKI
Class G
CPS
Certification Practice Statement

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: <2.16.578.1.31.10.10.2>

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 linkt 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] DnB NOR PKI – Collaboration: Document describing the interaction procedures betw, CA-Operator and DNB PKI organization.

[13] DnB NOR PKI – Business Continuity Plan: Document describing CA Operator Business Continuity Plans

[14] DnB NOR PKI – Key Creation Cerwemony: Document describing DnB NOR PKI Class G CA bootstrap procedure.

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

[16] 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 and WebTrust conformance requirements
1.4	01.11.2013	Updated with new profiles and WebTrust conformance requirements

1 INTRODUCTION

This document is the Certification Practice Statement (CPS) for *DnB NOR PKI* Class G certificates, and as such serves as a statement for the practices that DNB employs approving, issuing, managing, using and revoking Digital X.509 Certificates in accordance with the DnB *NOR PKI Certificate Policy for class G Certificates.* It defines the underlying certification processes for Subscribers and describes DNB's repository operations. The CPS is also a means of notification of roles and responsibilities for parties involved in Certificate based practices within the DnB NOR PKI.

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

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

The *DnB NOR PKI* Class G CA's control processes, as stated in this Certification Practice Statement (CPS), are designed and maintained to stay fully compliant with the requirements and regulations stated by WebTrust (www.webtrust.org) in [15] "Trust Services Principles and Criteria for Certification Authorities".

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

The current active Seal for *DnB NOR PKI* Class G may be found at:
https://cert.webtrust.org/ViewSeal?id=1366

1.1 OVERVIEW

The DnB NOR PKI Class G Certificate Service is a Subordinate Certificate Authority (CA) of Nets Eurida Primary Certificate Authority, operated by Nets eSecuriy and customized to meet the DnB NOR PKI requirements. The Eurida Primary Certificate Authority, which in turn is signed by OmniRoot (CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE), issues high quality and highly trusted digital certificates to entities including private and public companies. The CA Operator performs managed PKI Services associated with public key operations including receiving requests, issuing and revoking digital certificates and the issuing and publishing Certificate Revocation Lists (CRLs). The DnB NOR PKI Class G Certificate Service is operated for the community of its employees, partners and customers. All Registration Authorities governed by this CPS are operated by DNB ASA.

The DnB NOR PKI includes 3 classes of certificates:

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

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

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

A digital certificate is formatted data that cryptographically binds an identified subscriber with a public key. As detailed in this CPS, a range of distinct certificate types are offered. The different certificate types have differing intended usages. As the suggested usage for a digital

certificate differs on a per application basis, Subscribers are expected to appropriately study the requirements for their specific application before applying for a specific certificate.

The following certificate profiles are under provision of 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.

Card Managment System (CMS):

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

Autoenrolled:

- DnB NOR Encryption certificates: Mail encryption on the Windows platform
- 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

The CA and legal entities operating on CA's behalf are 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 [16] 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 is the Certification Practice Statement (CPS) for DnB NOR PKI Class G certificates. Insignificant revisions may be made without changing the version number of this CPS. Revisions not denoted “significant” are those deemed by the CA’s Policy Management Authority to have minimal or no impact on Subscribers and Relying Parties using certificates and the CRLs issued by the service.

This CPS 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) certifikatepracticestatement (11) DnB NOR PKI Class G (1) Major version(1)Minor version(1) }.

1.3 PKI PARTICIPANTS

This CPS 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 . DnB NOR CA is signed by Nets Eurida Primary Certificate Authority. DnB NOR is responsible for the RA function.

DNB employees and other approved associates may become RA Operators under this Policy. Registration Operators may perform parts of or all RA functions depending on the rights granted.

1.3.2 *SUBSCRIBERS*

For manually enrolled certificates, an agreement between the subscriber and DNB is established prior to accepting any certificate requests. Typical subscribers will be DNB Customers requesting Enterprise certificates, System Administrators requesting certificates for authentication of servers and PKI enabled applications.

WebRA users are subscribers of manually enrolled authentication certificates on Smart Card.

For autoenrolled certificates, a Group Policy definition must be established for the User or System in the DNB Active Directory. Group Policy definitions are maintained by System Administrators of the AD.

Smartcard based User certificates are provisioned by self-service via the ActiveId Card management System (CMS).

Regardless of the Subject listed in the Certificate, the Subscriber always has the responsibility of ensuring that the Certificate is used appropriately as denoted in the agreement for each service.

1.3.3 *End Users*

End Users under this CPS are DNB employees, partners and customers that are subjects to DnB NOR PKI Class G Certificates. SSL server certificates are only issued to DNB infrastructure components.

1.3.1 *Relying Parties*

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

1.3.2 *Other participants*

No stipulations

1.4 Certificate usage

1.4.1 *Applicability*

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

- Confidentiality
- Authentication
- Integrity
- Non-repudiation

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

The issued keys and certificates are to be used on client PCs and servers of DNB and selected 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 intended. This CPS does not deal with specific protection against such malicious software.

1.4.2 *Appropriate Certificate uses*

All participants are responsible ensure that the use of the Certificates are in accordance with National law, this CPS, ethical business standards and guidelines from the CA.

Each party using or relying on a certificate are bound by and obliged to comply with the terms and conditions set forth in the applicable agreement between the party and DNB.

The Certificates are most commonly used for electronic signatures to secure economic transactions and WEB service, machine and user authentication.

1.4.3 *Prohibited Certificate uses*

The Certificates must not be used in defiance of applicable law, official rule, this CPS 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 CPS and the corresponding CP are 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 is reviewed and approved by DNB Policy Management Authority and legal department.

1.5.4 *CPS approval procedures*

The DnB NOR PKI Class G CPS and any amendments made to it are reviewed and approved by DNB Policy Management Authority. Amendments to the CPS may be made by reviewing and updating the entire CPS or by publishing an addendum. The current version of the CPS is always made available to the relying parties through DNB's repository. All updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in Section 5.4 Audit logging procedures of this CPS.

1.5.5 . *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 PKI Service including CP, CPS and Subscriber Agreement templates. Repositories for Certificates, CRL and audit information are managed by the CA-Operator. The DNB Policy Management Authority has the responsibility for documentation pertaining to the PKI Service. All updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in referenced in Section 5.4 in this CPS. A complete version history of this CPS is published. DNB makes all reasonable efforts to ensure that parties accessing its Repositories receive accurate, updated, and correct information.

2.2 PUBLICATION OF CERTIFICATE INFORMATION

The CA Certificates are published at:

http://crl.dnbnor.no/dnb-nor-asa-pki-class-G.cer

Revocation information is published according to the CDP of the certificates at:

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

Revocation information is made available on internet and DNB Extranet according to the Authority Information Access (AIA) at:

http://va.dnbnor.no/

Encryption certificates are published in the DNB internal directory

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

- Certificate Policy (CP) and Certification Practice Statement (CPS) are made electronically available 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 CPS 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 necessary.

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

2.4 ACCESS CONTROLS ON REPOSITORIES

CP, CPS published by the CA Operator and agreement templates published in the internal DNB document repository may be accessed on a read-only basis by anyone visiting the site,

provided they agree to the site's terms and conditions. The repository entries are protected from unauthorized additions, modification, or deletions.

The AD is only accessible from the internal DNB network and is protected from unauthorized access that may lead to adding, deleting, or modifying repository entries.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

Subject names appearing in Certificates are authenticated, unless the Certificate profile indicates otherwise. Certificates may also 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 is described in this CPS.

3.1.1 *TYPES OF NAMES*

The DnB NOR Class G certificates uses X.509 v3 non-null Distinguished Name (DN) in the Issuer and Subject fields. Names are encoded as UTF8String.

Country (C) is a two letter ISO 3166-1 string representing the country of the End Entity.

Organization (O) and Organization Unit (OU) follows the Norwegian SEID standards of semantics for legal entities.

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

Subject Distinguished Name used in Certificates permits the determination of the identity of the natural person who is Subject to the Certificate.

Issuer Distinguished Name is:

C=no; O=DnB NOR ASA 981276957; CN=DnB NOR ASA PKI Class G

The Subject Distinguished Name varies depending on the certificate profile and service.

3.1.2 *NEED FOR NAMES TO BE MEANINGFUL*

The DnB NOR PKI Class G uses non-ambiguous designations and commonly used semantics to identify the End Entity. The CN attribute of an End Entity certificate Subject contains a reasonable representation of the name of the End Entity.

For further details for each certificate type see 7.1 Certificate profiles.

3.1.3 *ANONYMITY OR PSEUDONYMITY OF END USERS*

The DnB NOR PKI Class G does not have support for anonymous or pseudonymous End Users.

3.1.4 *RULES FOR INTERPRETING VARIOUS NAME FORMS*

Distinguished Names are interpreted according to X.509 v3 standard.

3.1.5 *UNIQUENESS OF NAMES*

Each certificate issued by the DnB NOR PKI Class G is unique within each certificate service in the sense that one particular Distinguished Name always identifies the same subject; natural person, organisation or system within that service. The uniqueness is guaranteed for at least as long as the certificate issued to the Requester is valid.

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.

Subscribers are solely responsible for ensuring the legality of any information presented for use in a DnB NOR PKI Class G Certificate. It is the responsibility of the Subscriber not to use names that conflict with protected names of natural persons or Organizations pursuant to law or Intellectual Property Rights in any jurisdiction. DNB has no obligation to determine whether any name used in a certificate application is a protected name or infringe any rights of any third party.

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

3.2 Initial identity validation

Based on the submitted certificate information, the DnB NOR PKI Class G RA confirms the following information:

- The Requester is authorized to request a certificate for the particular End Entity or is the same person as the person identified in the certificate application.
- The Requester holds the private key corresponding to the public key to be included in the certificate.
- The information to be published in the certificate is accurate except for any non-verified Subscriber information pertaining to the service in question.

For manually enrolled certificates, the authorization and certificate information is validated and approved by the RA Administrator.

For self provisioned certificates via ActiveID Smart Card Portal, the authorization and certificate information is validated and approved by the CMS Administrator.

For autoenrolled certificates, the authorization and certificate information is validated and approved by the AD System Administrator.

The Subscriber has a continuous obligation to observe the accuracy of the submitted information and notify the RA of any changes that would affect the validity of the certificate. Failure to comply with the terms and conditions in this CPS may result in the revocation of the subscriber's Digital Certificate.

3.2.1 *Method to prove possession of private key*

For details regarding requirements and procedures for proof of possession, see service specific descriptions.

3.2.2 *Authentication of organization identity*

Organisations applying for Enterprise certificates are obliged to present an organizational name according to its registered name and organization number (if available). This will constitute the Organization attribute of the Subject Distinguished Name according to the format description in 7.1 Certificate profiles.

3.2.3 *Authentication of individual identity*

Authentication of a natural person as an individual identity for issuance of a Certificate is performed according to the following rules:

The RA ascertains 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.

For natural persons acting on behalf of an organizational Subscriber, the following rules apply:

- The individual claiming procura shall present a proof of written power of authority to represent the Organization.

3.2.4 *NON-VERIFIED SUBSCRIBER INFORMATION*

DnB NOR PKI Class G CA does not validate information not listed as being validated under each service in 4.2 Certificate application processing.

3.2.5 *VALIDATION OF AUTHORITY*

Power of authority for enterprise certificates is documented according to 3.2.3 Authentication of individual identity, and all documentation archived by the Registration Authority according to Section 5.5 Records archival.

3.2.6 *CRITERIA FOR INTEROPERATION*

The DnB NOR PKI Class G is a Subordinate Authority (CA) of Nets Eurida Primary Certificate Authority.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 *IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY*

The DnB NOR PKI Class G PKI does not support certificate re-keying. Every certificate request is treated as an initial request, and requires the verification procedure to be followed.

3.3.2 *IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION*

See previous paragraph.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Prior to revoking a certificate, the DnB NOR PKI Class G RA verifies that the revocation was requested by an authorized entity 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.

- A revocation request may be initiated by DNB as a normal or forced termination of an employee agreement.

- A Certificate revocation may be an automated step of terminating a DNB Employee smartcard.

Procedures for authenticating a Certificate revocation request include:

- Receiving a message from a DNB employee 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 is specified in the Subscriber agreement.
- A revocation initiated by DNB may be performed by WebRA operators, Helpdesk operators or CMS Operator (as an integrated part of a smart card termination.)

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

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

Prior to the issuance of a certificate, controls are made to ensure that application records are legitimate, correct and in accordance with this CPS. For all applicable services, the RA issues a certificate expiry request to the DNB ARS.

The CA is entitled to collect application information for administrative and maintenance purposes.

4.1.1 *WHO CAN SUBMIT A CERTIFICATE APPLICATION*

Manually enrolled certificates:

Prior to the issuance of a certificate, the DNB RA Administrators will validate the application in accordance with this CPS which involves verifying the identity and authorization of the applicant.

Natural persons may submit Certificate applications to an RA individually or on behalf of an organization to which the person holds a procura or other authorization stated in the customer agreement.

Autoenrolled certificates:

Autoenrolled certificates are requested based on policies and information maintained in the DNB Active Directory. The required AD information is established and maintained based on DNB HR information and system administration requirements.

Certificate requests to the CA are submitted exclusively by DNB Registration Authorities and End Entities of the DNB network domains.

4.1.2 *MANUAL ENROLLMENT PROCESS AND RESPONSIBILITIES*

DNB RA has the responsibility of establishing the dissemination processes when receiving certificates from CA.

WebRA Administrators perform manual certificate enrollment according to the procedures established for each certificate profile/service.

4.1.3 *AUTO ENROLLMENT PROCESS AND RESPONSIBILITIES*

Authentication certificates for users and machines are made available through autoenrollment services for internal DNB employees, hired personnel authorized by DNB and internal Windows based services.

4.2 CERTIFICATE APPLICATION PROCESSING

Manually enrolled certificates:

All application records, as defined by the specific customer service agreements are archived in the DNB Archive. The archive references are maintained in the DNB Web RA.

All relevant steps of the certificate request process are logged for future audit. All certification operations are auditable by RA Administrator and RA-session. Complete Audit logs and functions to access the audit information are made available by the CA Operator.

Autoenrolled certificates:

All autoenroll certification operations are auditable by autoenroll agent authentication and session information. Complete Audit logs and functions to access the audit information are made available by the CA Operator.

4.2.1 *Performing identification and authentication functions*

The RA performs 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 is approved if the controls specified in section 3.2 are successfully passed, and all other requirements specified in the Subscriber agreement are satisfied. Otherwise, the Certificate application will be rejected.

4.2.3 *Time to process Certificate applications*

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

4.3 Certificate issuance

For manually enrolled certificates, the RA is solely responsible for decisions as to whom Certificates are issued and record archival related to the subject authentication.

For autoenrolled certificates, authorized personnel within DNB will configure the autoenrollment service to accommodate with information maintained in the DNB Active Directory to issue certificates to the proper End Entities. User entities in DNB Active Directory is provisioned by the enterprise HR system.

4.3.1 *CA actions during Certificate issuance*

All CA actions during issuance are logged. After signing an End User Certificate the CA:

- Returns the Certificate to the requesting End User, RA or Autoenrollment agent
- Publishes the Certificate according to 4.4.2.

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

For manual enrollment, the RA is responsible for notifying the End User of the issuance of the Certificate.

For autoenrolled certificates the End User is informed by standard Windows prompts and notifications when applicable.

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, the End User is deemed to have accepted the Certificate and conditions related to the use of the Certificate.

4.4.2 *Publication of the Certificate by the CA*

CA publishes 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*

According to stipulations in Section 9.6.4 End User obligations.

4.5.2 *Relying Party public key and Certificate usage*

According to stipulations in Section 9.6.5 Relying Party obligations.

4.6 Certificate renewal

The DnB NOR PKI Class G PKI service does not support certificate renewal. Every certificate application is treated as a new certificate application.

4.7 Certificate re-key

The DnB NOR PKI Class G PKI service does not support certificate re-keying. Every certificate application is treated as a new certificate application.

4.8 Certificate modification

The DnB NOR PKI Class G PKI service does not support certificate modification. Every certificate application is treated as a new certificate application.

4.9 Certificate revocation and suspension

Upon revocation of a certificate, the operational period of that certificate is immediately considered terminated and the serial number of the revoked certificate will be placed in the CRL. The time delay before the certificate suspension/revocation is effective, is 12 upto hours.

4.9.1 *Circumstances for revocation*

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, included but not limited to: circumstances that may reasonably be expected to affect the reliability, security or integrity of the certificate or key pair associated with it.

Certificates must be revoked if:

- The End User requests revocation of the Certificate
- 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 breached a material obligation, representation, or warranty under this CPS and/or an applicable agreement
- The End User is terminating the employee or labour agreement with DNB, either by intension or by enforcement
- The Subscriber has materially breached a material obligation, representation, or warranty under this CPS and/or an applicable agreement. All Certificates associated with the Subscriber in question must be revoked
- The Subscriber agreement is terminated
- RA 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 organization named as the Subject of such Certificate

- RA discovers or has reason to believe that a material fact in the Certificate application is false
- RA 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 Certificate has been used in criminal activity or on websites forbidden by RA, CA or the Subscriber
- The smartcard, on which the private key corresponding to the certificate, has been terminated or.

4.9.2 *WHO CAN REQUEST REVOCATION*

Revocation procedures ensure that a revocation has been requested either by an End User, a Subscriber, DNB RA or the DnB NOR PKI Class G CA.

4.9.3 *PROCEDURE FOR REVOCATION REQUEST*

The revocation procedure 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 RA Revocation Officer
- Notifying Partner responsible or Customer Account Manager for certificates issued to DNB partners or customer
- Depending on the service requirement, notifying the End User that a revocation has taken place. When sending the notification, contact information stored in the RA is used - contact information submitted by the requestor during the revocation request process is not used.

When requests are submitted to RA the following information is logged:

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

Requests for revocation of a 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*

End User and/or Subscriber are obliged to submit revocation requests without undue delay when they become aware of circumstances indicating a reason for requesting revocation.

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

The DNB RA processes all revocation requests without delay. The amount of time required depends on the nature of the revocation request, the party requesting the revocation, and other factors surrounding the revocation request. Ordinary certificate revocation requests are processed automatically upon receipt within one business day.

The CA processes the Revocation Request automatically and has an expected processing time of max 2 seconds.

4.9.6 *Revocation checking requirements for relaying parties*

Relying Parties are obliged to 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 will be published at a time interval of 4 hours. The validity for the CRL will be 12 hours from time of issuance, giving a grace period of 8 hours.

4.9.8 *Maximum latency for CRLs*

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

4.9.9 *On-line revocation status checking availability*

Certificates revocation status information is available on-line by consulting the CRL or accessing the OCSP service that are made available according to stipulations in section 2.2.

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 will be notified of a compromise, or suspected compromise, of a CA or RA private key. This is done by publishing the information on the DnB NOR PKI Class G Repository web page. In case of RA or CA key compromise, CA and RA will inform the PMA without undue delay and initiate actions according to the CA Operator/ DNB Collaboration procedures.

4.9.13 *Circumstances for suspension*

4.9.14 *Not applicableWho can request suspension*

4.9.15 *Not applicableProcedure for suspension request*

Not applicable

4.9.16 *Limits on suspension period*

4.10 Not applicableCertificate status service

4.10.1 *Operational characteristics*

The status of Certificates is made available on-line via CRL and OCSP as specified in section 2.2.

4.10.2 *Service availability*

Certificate status services has a planned availability of 99.9%, 24x7 with exception of scheduled maintenance.

4.10.3 *Optional features*

Not applicable.

4.11 End of subscription

If a customer terminates the customer agreement, based on which a DnB NOR PKI Class G certificates have been issued, all valid certificates pertaining to that agreement will be revoked on the termination date of the agreement.

4.12 Key Archiving and recovery

4.12.1 *Key archiving and recovery policy and practices*

- The DNB RA shall be responsible for key recovery of private keys associated to User encryption Certificates. As an interim solution, the Key Archival and Recovery Service (KAS) will be handled by the CA-organisation as a centralized service. The Key Archival Officer (KAO) and Key Recovery Operator (KRO) roles, appointed in the Key Archival Key Ceremony, will be held by DNB personnel.
- 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*

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL SECURITY CONTROLS

The PKI adheres 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 are 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 are fulfilled by establishing high-security zones based on physical barriers.

5.1.2 PHYSICAL ACCESS

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

5.1.3 POWER AND AIR CONDITIONING

The secure premises have double power supplies from two separate power sources. In addition the building is 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 is available in secure premises, and temperature and humidity is controlled automatically and continuously.

5.1.4 WATER EXPOSURES

All security rooms are shielded against water exposures.

5.1.5 FIRE PREVENTION AND PROTECTION

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

5.1.6 MEDIA STORAGE

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

5.1.7 WASTE DISPOSAL

CAs and RAs have implemented procedures for the disposal of paper, magnetic and optical media, and 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

Production database transaction data is synchronously transferred from primary location to secondary location. Slave databases at secondary location are updated continuously, with 12 hours playback available. All full database- and system back-ups are transferred to secondary Off-Site Secure Premises and additionally to off-line media in a third location. The locations are described in details in the relevant security documentation.

The following back-up schedule is implemented:

- Daily: database back-up (6 days retention)

- Weekly: database back-up (3 weeks retention)
- Monthly: database back-up (11 months retention)
- Yearly: Full system back-up including databases (10 years retention)
- Back-ups preceding system upgrades and configuration changes

5.2 Procedural controls

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

5.2.1 *Trusted roles*

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

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

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

5.2.2 *Number of persons required per task*

Personnel involved in PKI operations 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 is done between general functions and PKI specific functions. These differentiations 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 are used for all jobs on the IT-systems, thus ensuring traceability and feasible auditing conditions.

5.2.4 *Roles requiring separation of duties*

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

5.3 Personnel controls

5.3.1 *Qualifications, experience, and clearance requirements*

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

CA personnel are certified as trusted employees. In addition they 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. The skills of all personnel are checked before qualifying them to the PKI system.

5.3.2 *Background check procedures*

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

5.3.3 *Training requirements*

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

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

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

5.3.4 *JOB ROTATION FREQUENCY AND SEQUENCE*

No stipulation.

5.3.5 *SANCTIONS FOR UNAUTHORIZED ACTIONS*

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

5.3.6 *INDEPENDENT CONTRACTOR REQUIREMENTS*

Third party contractors as well as unauthorized CA employees are not left alone in the secured premises, and never, in any way, work alone on the CA system.

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

5.3.7 *DOCUMENTATION SUPPLIED TO PERSONNEL*

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

5.4 AUDIT LOGGING PROCEDURES

Processing Centers, RAs, and Relying Parties who operate or use services covered by this document, keep records of events sufficient to prove, within reasonable doubt that they comply with the provisions of this CPS.

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

5.4.1 *TYPES OF EVENTS RECORDED*

The events relating to the following are logged:

.

- 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 are stored at two separated locations.

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

Logs intended to give indication of system compromise automatically send an alert to the associated monitoring system and are subject to review if an alert is sent. Logs are 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 are 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*

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

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

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

5.4.5 *Audit log backup procedures*

Incremental backups of the audit logs are performed on a daily basis. Full backup is performed on a five days a week basis. Weekly and monthly full back-ups are preserved at a secondary site and 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 are as a minimum carried out whenever a material deficiency is discovered.

5.5 Records archival

Records archival conform to the stipulations described in section 5.4.

5.5.1 *Types of records archived*

The records archived are in accordance with section 5.4, and include the following:

- Records relating to registration information

- Records relating to the CA environmental events
- Records relating to the key management events
- Records relating to the Certificate management events

5.5.2 *Retention period for archive*

Stipulations are equivalent to section 5.4.3.

5.5.3 *Protection of archive*

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

5.5.4 *Archive backup procedures*

All full archive backups are stored in Off-Site Secure Premises. All electronic records are archived on both primary and secondary sites.

5.5.5 *Requirements for time-stamping of records*

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

5.5.6 *Archive collection system (internal or external)*

For certificates issued by the WebRA, documentation, as described in Section 3.2 Initial identity validation, is scanned and stored in the DNB Archive. Archive references are generated by the DNB archive system and linked to the Certificate Request in the WebRA database.

For autoenrolled certificates, the Cerificate Requests are generated based on policy information in the DNB Active Directory. Autoenrollmen policies for user certificates are established based on employment agreements maintained in the DNB HR system.

.

5.5.7 *Procedure to obtain and verify archive information*

No stipulation.

5.6 Key changeover

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

5.7 Compromise and disaster recovery

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

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

5.7.1 *Incident and compromise handling procedures*

The business continuity plan describes:

- How to restore information systems services and key business functions back to their normal condition

- In details what, if and how the CA organization intends to run its operation between the disaster that has occurred and the moment when business is restored to its normal condition
- In details how the CA organization intends to fulfil its obligations with respect to this CPS

5.7.2 *COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED*

Corruption of computing resources, software, and/or data of any operating environment is promptly communicated between CA Operator and DNB PMA according to agreed and documented collaboration procedures. The disaster recovery task force convenes, assesses the situation and its consequences and decides on a response to the event.

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

Backups of the following CA information are stored 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

Back-ups of CA private keys are generated and maintained in accordance with section 6.2.4.

5.7.3 *ENTITY PRIVATE KEY COMPROMISE PROCEDURES*

In the event of a compromise of the private key of the CA or RA Certificate, the PMA determines if the CA or RA Certificate will be revoked. Requests for revocation of a CA or RA Certificate must be submitted to the PMA. The reason for the request must be well documented.

Upon revocation of the Certificate containing the CA public key:

- The revocation will be announced on the CA web site
- Validation services are terminated for the revoked CA public key
- The CA will 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 CPS

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

A new CA key and Certificate is created in accordance with section 5.6 of this CPS.

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

5.7.4 *BUSINESS CONTINUITY CAPABILITIES AFTER DISASTER*

Secondary site has 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 includes the enforcement of physical security barriers in accordance with section 5.1.1.

The business continuity plan makes provisions for a recovery within the timeframe specified in the agreement following a disaster occurring at the Processing Centre sites..

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

5.8 CA OR RA TERMINATION

Termination is a controlled cessation of CA or RA service. All business partners will receive advance notification. Before terminating its own CA activities, DNB will take the following steps, where possible:

- 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 CRL information (by CRL and OCSP), and thereby inherently deem all issued certificates as revoked. Alternatively revoke the certificates prior to issuing the last CRL.
- Ensure the secure preservation and maintenance of all relevant databases, archives, records and documents, for these to be made available on request for a commercial reasonable period of time, not less than 10 years after CA or RA termination.

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

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

6 TECHNICAL SECURITY CONTROLS

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 are produced in secure key generation systems. End User keys will in most cases be generated remotely from the CA. Local security measures are in such cases put in place to ensure the desired level of security.

CA keys are generated by the CA in a dedicated Hardware Secure Module (HSM) that meets the requirements identified in FIPS 140-2 [6].

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

End User key pairs are generated in highly secured premises. Routines are in place to prevent loss, modification, or unauthorized use of private keys.

6.1.2 *PRIVATE KEY DELIVERY TO END USER*

The CA performs no generation of private keys to End Users.

6.1.3 *PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER*

For End User certificates, the public key is delivered to the Certificate issuer in a request package complying with the PKCS#10 standard. Besides, the entity that generates the keys ensures 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 certificate is made available to Relying Parties via a DNB website.

6.1.5 *KEY SIZES*

Key pairs have sufficient length to prevent others from determining the key pair's private key using exhaustive search during usage period for such key pairs. Key sizes will be set to minimum 2048 bits RSA for End Users. CA private keys are set to a minimum of 2048 bits RSA keys.

6.1.6 *PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING*

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

6.1.7 *KEY USAGE PURPOSES (AS PER X.509 V3 KEY USAGE FIELD)*

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

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

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

In particular:

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

6.2.2 *PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL*

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

6.2.3 *PRIVATE KEY ESCROW*

No stipulation.

6.2.4 *PRIVATE KEY BACKUP*

The CA backs up its private keys.

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

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

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

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

6.2.5 *PRIVATE KEY ARCHIVAL*

Private encryption keys are archived by a key archival and recovery service (KAS). Keys are transported and stored in encrypted form. The keys are encrypted with a Long Term Storage Key (LTSK). Access to the archived keys are granted only to appointed DNB roles: Key Archival Operator(KAO) and Key Recovery Operator(KRO). 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 are 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 are stored in protected memory.

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

6.2.7 *PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE*

The CA private keys are generated in and by a hardware cryptographic module. Private keys never exist in plain text form outside the cryptographic module boundary.

6.2.8 *METHOD OF ACTIVATING PRIVATE KEY*

The CA Private Key:

Only trusted personnel have access to any private keys belonging to the CA. Private key is activated by two Key Custodians, by supplying their activation data which is 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, two Key Custodians are required to supply their activation data in order to activate an offline CA private key. Once the private key is activated, it is active only for one session. The procedure around using an offline CA private key is documented in detail.

The RA Private Keys

Only trusted personnel have access to private keys in the RA system. The trusted personnel are authenticated by use of a of private keys on smartcards protected by PIN.

The End User Private Keys

All End Users are obliged to protect the activation data for their private keys against loss, unauthorized disclosure, or unauthorized use. End Users are required to 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 are never 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 cannot be accessed unauthorized. When no longer in use, they are deactivated using adequate logout and removal procedures. Deactivated private keys are protected and kept securely.

End Users are requested to 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 are destroyed upon device retirement. All handling of the CA private keys is witnessed and documented.

The RA private keys are destroyed by deletion and overwritten. This is witnessed and documented.

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

6.2.11 *CRYPTOGRAPHIC MODULE RATING*

The cryptographic modules used by the CA are 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 issued certificates are stored in the CA certificate database. Encryption certificates are published to CA public directory and DNB internal Active Directory.

6.3.2 *CERTIFICATE OPERATIONAL PERIODS AND KEY PAIRS USAGE PERIODS*

The Certificates have a defined, limited usage period.

The validity period for the CA Certificate is 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 of three (3) years.

The validity period for End Entity Certificates are set to a period not exceeding three (3) 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 are 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. End Users are provided general guidance on how to compose secure passwords. To the extent possible, PKI enabled applications will impose automatic and non-circumventable restrictions on password composition.

6.4.2 *Activation data protection*

When entering activation codes, the End User is obliged to protect the code from compromise. This includes protection against other people observing the code/PIN during entry. Within reasonable doubt, it is the End Users responsibility to 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 is 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, RA will 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 are transmitted through registered mail or handed out to the End User present in person.

6.5 Computer security controls

All CA and RA functions 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*

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

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

Production networks are logically protected and supervised.

6.5.2 *Computer security rating*

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

6.6 Life cycle technical controls

6.6.1 *System development controls*

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

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

6.6.3 *LIFE CYCLE SECURITY CONTROLS*

The CA Operator Security Officer periodically verifies the integrity of the CA software and supervise all configurations on the CA systems.

6.7 NETWORK SECURITY CONTROLS

CA and RA functions are performed using networks secured according to Best Practices. The controls prevent and detect unauthorized access and tempering attempts.

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

6.8 TIME-STAMPING

All data related to Certificate life-cycles, as well as data stored for auditing and archiving purposes contain time information down to seconds, from use of a trusted time source. The system time of RA and CA is synchronised and differs 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 PKI-Configuration documentation maintained by the CA operator.

7.2 CRL PROFILE

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

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

The practices specified in this CPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards including the AICPA/CICA WebTrust Program for Certification Authorities, ANS X9.79:2001 PKI Practices and Policy Framework, and other industry standards related to the operation of CAs.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

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

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

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

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

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

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

8.4 TOPICS COVERED BY ASSESSMENT

The following topics are as a minimum covered:

- Service integrity
- User data integrity
- Documentation
- Exception handling
- Contingency
- Disaster recovery
- Tests
- Accountability
- Personnel training
- Ownership to processes
- Compliance statement
- Access control, both physical and logical
- System logging
- Auditlog 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 are reported to Policy Management Authority.

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

The CA Certificate is revoked, and all parties are informed if the Policy Management Authority finds the deficiency to be fatal.

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

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

8.6 Communication of results

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

Any insurance or warranty coverage for End Users is regulated through service specific agreements and are outside the scope of this CPS as long as it does not violate the provisions of this CPS.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

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

9.3.1 *SCOPE OF CONFIDENTIAL INFORMATION*

The following types of information are 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
- External or internal audit trail records and reports
- 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 Operator.
- Operational and technical information that should be kept confidential due to security requirements in applicable security practice standards.
- Internal tracks and records on the operations of the infrastructure, certificate management and enrollment services and data.

9.3.2 *INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION*

Subscribers 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 regarded as non-confidential information.

9.3.3 *Responsibility to protect confidential information*

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

Responsibilities to protect information is 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] is enforced by the DnB NOR PKI service including the CA Operator. The received data from Subscribers and/or End Users is solely for the purpose of issuance and use of Certificates and/or directly related certification services. The DnB NOR PKI service maintains routines to ensure compliance to applicable regulations and directives.

9.4.2 *Information treated as private*

The following types of information are to 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, is not considered 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 is used by the CA Operator or DNB 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 will be performed in accordance with Norwegian law.

9.4.7 *Other information disclosure circumstances*

No stipulation.

9.5 Intellectual property rights

DNB owns all intellectual property rights associated with DnB NOR PKI Class G service repositories, web sites, digital certificates, templates and publications including this CPS.

The structure of this document is based on:

- RFC 2527
- RFC 3647

9.6 OBLIGATIONS

9.6.1 CA OBLIGATIONS

CA-Operator obligations are handled in separate agreements with DnB NOR PKI Class G. General obligations are listed below: A Certificate authority service conforming to this CPS is operated by the CA Operator. The conforming CA is responsible for all aspects of the issuance and management of a certificate referencing this CPS, including:

- Certificate application/enrollment process
- Certificate creation process
- If applicable, posting of the certificate in a public repository
- Signing and publishing of suspension and revocation information
- Ensuring that all aspects of the CA services, operations and infrastructure related to DnB NOR PKI Class G certificates are performed in accordance with the requirements, representations, and warranties of this CPS

By issuing a certificate under this CPS, 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 CPS
- There are no misrepresentations of fact in the certificate known to the CA
- The certificate meets all material requirements of this CPS

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 are obliged to:

- 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 CPS. 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 are obliged to ensure that:

- DnB NOR PKI Class G certificates are used lawfully in accordance with the terms of this CPS
- 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 are obliged to:

- Independently make themselves familiar with this CPS before drawing any conclusion on how much trust they can put in the use of a DnB NOR PKI Class G certificates
- Only use the certificate for the proscribed 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

DNB uses applications, services and procedures that, to the best of our knowledge, perform as required by this CPS, but declines any warranty as to their full correctness. Also DNB cannot be held responsible for any misuse or unchecked acceptance of certificates issued under the DnB NOR PKI by a subscriber or any other party. Any relying party that accepts a certificate, for any usage for which it was not issued, does so on its own risk and responsibility.

9.8 Limitations of liability

Limitations and liabilities are evaluated and regulated in all Subscriber and Relying party agreements. DNB ASA declines any liability for damages incurred by the non-issuance of a

requested certificate, or damages incurred as consequence of revoked certificates being unduly accepted by a relying party.

9.8.1 *CA LIMITATIONS OF LIABILITY*

No stipulation.

9.8.2 *END USER LIMITATIONS OF LIABILITY*

Parties relying on a digital certificate must verify a digital signature at all times by checking the validity of a digital certificate through the CRL provided by DnB NOR PKI. Relying on an unverified digital signature may result in risks that the Relying Party, and not DNB, assumes in whole.

9.8.3 *RA LIMITATIONS OF LIABILITY*

DNB reserves its right to refuse to issue a certificate to any party as it sees fit, without incurring any liability or responsibility for any loss or expenses arising out of such refusal. DNB reserves the right not to disclose reasons for such a refusal.

9.9 INDEMNITIES

End entities shall indemnify and hold harmless DNB ASA and contractors against all claims and settlements resulting from fraudulent information provided with the certificate application, and the use and acceptance of a certificate which violates the provisions of this CPS.

9.9.1 *INDEMNIFICATION BY SUBSCRIBERS*

By entering a Subscriber relation with DnB NOR PKI Class G, the Subscriber agrees to indemnify and hold DNB and contractors harmless in case of damage or loss caused by the use or publication of a certificate that arises from:

- Any false or misrepresented data supplied by the Subscriber or Requester.
- Any negligent or intended failure of the Subscriber and Requester to disclose a material fact.
- Any failure by the Requester to protect their confidential data, including the private key.
- Any failure to take reasonable precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's confidential data.
- Breaking any laws applicable in his/her country or territory including those related to intellectual property protection, computer viruses and malware, accessing computer systems etc.

9.9.2 *INDEMNIFICATION BY RELYING PARTIES*

Subscribers are liable for any misrepresentations they make in certificates to third parties that rely on the certificates issued by DnB NOR PKI Class G service.

9.10 TERM AND TERMINATION

This CPS 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 CPS remains effective until it is superseded by a newer version or the termination of the DnB NOR PKI Class G.

9.10.3 *Effect of termination and survival*

The CPS document is archived for at least 10 years after the last certificate issued under this CPS expires or is revoked.

Before terminating its own CA activities, DNB will take steps as described in section 5.8 CA or RA termination.

9.11 Individual notices and communications with participants

Formal communication between CA and RA is conducted according to established and documented collaboration procedures. Communication with Subscribers and End Entities will be conducted according to this CPS and any Customer agreements for the services relying on DnB NOR PKI Class G.

9.12 Amendments

9.12.1 *Procedure for amendment*

Amendments to this CPS are administered by the DNB PMA and undergo the same procedures as for the initial approval. Rephrasing provisions to improve understandability and spelling corrections are not considered amendments and will be made without notice and without changing the version number of this CPS.
Controls are in place to reasonably ensure that the CPS is not amended and published without the prior authorization of the DNB PMA.

9.12.2 *Notification mechanism and period*

Amendments to the CPS document are published on the appropriate DNB web site at minimum 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 CPS in case of substantial changes to the policy or CA service.

9.13 Dispute resolution provisions

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

9.14 Governing law

This CPS is constructed, and shall be interpreted, in accordance with Norwegian Law. All legal disputes arising from the content of this CPS 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 CPS is constructed and is compliant with Norwegian Law. Activities covered by this CPS, 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 CPS supersedes any prior agreements, written or oral, between the parties covered by the present document unless specifically stated otherwise in the prior agreements.

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

9.16.2 ASSIGNMENT

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

9.16.3 SEVERABILITY

Should a clause of the present CPS be deemed as being invalid, in conflict with Norwegian law, or the governing law of any PKI Participant because it has been declared invalid or unenforceable by court or other law-enforcing entity, the clause should be removed or replaced by a valid clause by the PMA. The PMA also evaluate the implications for the remainder of the CPS, which otherwise remain in force. Clauses deemed unclear or unenforceable are otherwise interpreted in such manner as to affect the original intention of the parties.
Each and every provision of this CPS that provides for a limitation of liability, disclaimer of or limitation upon any warranties or other obligations, or exclusion of damages is intended to be severable and independent of any other provision and is to be enforced as such.

9.16.4 ENFORCEMENT

This CPS is enforced as a whole, whilst failure by any person to enforce any provision of this CPS is not deemed a waiver of future enforcement of that or any other provision.
Agreements between DNB and the parties detailed in this CPS may contain additional provisions governing enforcement and are 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 CPS.

9.16.5 FORCE MAJEURE

Events that are outside the control of the DnB NOR PKI, will be dealt with immediately by the PMA.

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

9.17 OTHER PROVISIONS

No stipulation.