DNB PKI - CERTIFICATION PRACTICE STATEMENT (CPS) De Nederlandsche Bank

OID of this document: 2.16.528.1.1017.2.1.1.2

Date: November 16, 2018

OVERVIEW This document covers the Certification Practice Statement (CPS) that governs the functioning and operations of De Nederlandsche Bank Public Key Infrastructure (PKI).

This CPS is applicable to all participants related to De Nederlandsche Bank PKI hierarchy, including the Certification Authorities (CA), Registration Authorities, Certificate Applicants and Subscribers and Relying Parties, among others.

Control Sheet

Title	Certification Practice Statement
Author	André Lensink (department head ICT CIO Office)
Version	1.4
Date	16.11.2018

Change Log

Version	Date	Change Reason
0.1	01.09.2015	Initial Version
0.2	01.12.2015	Updates of OID information
0.3	15.04.2016	Adding text
0.4	08.06.2016	Adding text
0.5	04.03.2017	Revised after feedback stakeholders
1.0	13.04.2017	Modified text, added technical and contact information
1.1	15.06.2017	Added Certification Authority information
1.2	15.11.2017	Revised after feedback PKI-AB (ITC/SRMWG)
1.3	24.04.2018	Revised after feedback PKI-AB ((ITC/SRMWG)
1.4	16.11.2018	Revised after feedback PKI-AB (ITC/SRMWG)

Table of content

1. Content, rights and obligations established in Certification Practice Statement (CPS)

This section provides an overview of the content, rights and obligations established in the Certification Practice Statement (CPS) for De Nederlandsche Bank. Its content must be supplemented with the corresponding Certificate Policy (CP), applicable to the certificate requested or being used.
It is recommended that this CPS be read fully, as well as the applicable CPs, in order to understand the purposes, specifications, regulations, rights, obligations and responsibilities governing the provision of the certification service.

- This CPS and the related documentation regulate the entire life-cycle of electronic certificates, from their request to their end of subscription or revocation, as well as the relations that are established between the certificate applicant/subscriber, the Certification Authority and the relying parties.
- The Certification Authorities of De Nederlandsche Bank's PKI issue different types of certificates for which there are specific Certification Policies (CP). Consequently, when requesting any kind of certificate and in order to request and use them correctly, applicants must be aware of the content of this CPS and, as appropriate, the applicable CP. The stipulations contained in the Certificate Policies shall prevail over the regulations in this CPS.
- The CPS and the CPs set out the scope of liabilities for the different parties involved, as well as their limits as regards possible damages.
- Certificate subscribers shall make appropriate use of certificates and shall be solely responsible for any use other than that specified in the CPS and corresponding CP.
- Certificate subscribers shall notify the Certification Authority of any modification or variation in the data provided to obtain the certificate, regardless of whether or not said data is included on the certificate itself.
- Safekeeping of the private key by certificate subscribers is an essential requirement for the security of the system. Therefore, the Certification Authority will immediately be informed of the existence of any of the causes established in the CPS for revocation/suspension of certificate validity, thus enabling suspension/revocation of the compromised certificate to prevent its illegal use by unauthorized third parties.
- Persons who wish to rely on a certificate are responsible for verifying, using the information sources provided, that the certificate and the rest of the certificates in the chain of trust are valid and have not expired or been suspended or revoked.
- Furthermore, when drafting its content, European standards have been taken into consideration. Both the electronic certificates governed by Artikel 3:15a Burgerlijk Wetboek (Nederland) (B.W.) "de Wet Elektronische Handtekening", the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- Both the CPS and the rest of the related documentation are available to certificate applicants, subscribers and relying parties at https://www.dnb.nl/pki/ . See contact details below.

For more information contact the Certification Authority by e-mail at pki@dnb.nl.

2. Introduction

2.1 Overview

This document covers the Certification Practice Statement (CPS) that governs the functioning and operations of the Public Key Infrastructure (hereinafter referred to as PKI) of De Nederlandsche Bank (hereinafter referred to as DNB-PKI).
This CPS is applicable to all participants related to De Nederlandsche Bank PKI hierarchy, including the Certification Authorities (CA), Registration Authorities (RA), Certificate Applicants and Subscribers and Relying Parties, among others.

In order to give the document a uniform structure and facilitate its reading and analysis, all the sections established in RFC 3647 have been included. Where nothing has been established for any section the phrase "No stipulation" will appear.

This CPS assumes that the reader is conversant with the PKI, certificate and electronic signature concepts. If not, readers are recommended to obtain information on the aforementioned concepts before they continue reading this document.

2.2 Document name and Identification:

Name	Description
Title	CERTIFICATION PRACTICE STATEMENT (CPS) De Nederlandsche Bank
Classification	Public
Version	1.2
Date	November 2017
Document status	Final
Author	Information Security
O.I.D. (Object Identifier)	2.16.528.1.1017.2.1.1.2

2.3 Contact information:

Name	Description
Visit location	De Nederlandsche Bank Westeinde 1 1017 ZN Amsterdam The Netherlands
Telephone number	+31 20 524 9111
Email address	pki@dnb.nl
PGP key	http://www.dnb.nl/en/contact/index.jsp

2.4 General Architecture DNB PKI

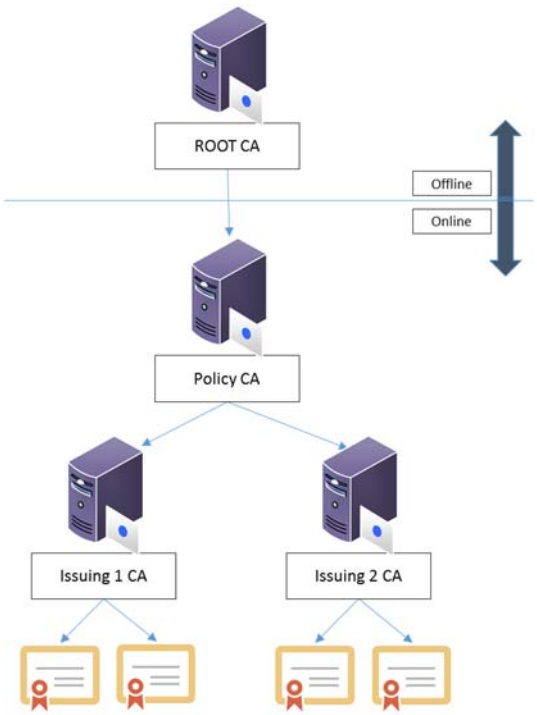

Figure 1 - Online and offline servers

The amount of Online servers can fluctuate. The figure only represents which server is Offline and which is Online.

Note: Some illustrations will be provided for better understanding. In the event of any difference or discrepancy between the text and the illustrations, the text will prevail in all cases, given the necessary synthetic nature of the illustrations.

3. Introduction

3.1 DNB-PKI Participants

This section will describe the participating entries and persons.

1. The Policies Approval Authority.
2. The Certification Authorities.
3. The Registration Authorities.
4. The Validation Authorities.
5. The Keys Archive.
6. The Applicants and Subscribers of the certificates issued by DNB-PKI.
7. The Relying Parties of the certificates issued by DNB-PKI.

3.1.1 The Policy Approval Authority

The Policies Approval Authority (PAA) is the organization established within the CIO office of the ICT Division of De Nederlandsche Bank and responsible for administering this CPS and DNB-PKI's Certificate Policies.
The PAA is also responsible, in the event of having to evaluate the possibility of an external CA interoperating with DNB-PKI, for establishing whether or not the CPS of said CA is suitable for the CP in question.
The PAA is responsible for analyzing the full or partial audit reports drawn up on DNB-PKI and, when necessary, for establishing the corrective actions to be taken.

3.1.2 Certification Authority

These are the individuals, policies, procedures and computer systems entrusted with issuing the electronic certificates and assigning them to their subscribers. Additionally, they carry out the renewal or revocation of the aforementioned certificates and generate the public and private keys, when so established under their practices and policies.
The De Nederlandsche Bank will act as CA for internal requests and for external ECB bank partners to create and assign certificates mentioned in the corresponding CPs.

The Certification Authority includes multiple technical components, the most significant data are:

1. Offline Root CA:

Distinguished Name	CN=DNBNL-ROOTCA, O=De Nederlandsche Bank N.V., C=NL
Serial Number	54 80 5e 6f 2a f5 e7 b6 40 29 c5 92 26 0e b8 5e
Distinguished Name of Issuer	CN=DNBNL-ROOTCA, O=De Nederlandsche Bank N.V., C=NL
Validity Period	From 10-05-2017 to 10-05-2057
Message Digest (SHA-1)	50 66 b1 18 22 0e 22 d2 73 e4 ff 55 2a 2d 86 cc e7 29 a0 c5

2. Online Policy CA:

Distinguished Name	CN=DNBNL-POLICYCA, O=De Nederlandsche Bank N.V., C=NL
Serial Number	7e 00 00 00 02 1c 79 bd 0d 89 4b d2 47 00 00 00 00 00 02
Distinguished Name of Issuer	CN=DNBNL-ROOTCA, O=De Nederlandsche Bank N.V., C=NL
Validity Period	From 11-05-2017 to 11-05-2037
Message Digest (SHA-1)	d7 8b c1 c7 9f cb d5 01 d7 89 e1 32 d1 0d ff c6 82 af 14 e1

3. Online Issuing CA:

Distinguished Name	CN=DNBNL-CA1, O=De Nederlandsche Bank N.V., C=NL
Serial Number	36 00 00 00 04 d5 30 0e 40 a5 d6 82 11 00 00 00 00 00 04
Distinguished Name of Issuer	CN=DNBNL-POLICYCA, O=De Nederlandsche Bank N.V., C=NL
Validity Period	From 15-05-2017 to 13-05-2027
Message Digest (SHA-1)	30 1c b1 7e d9 f5 c3 43 37 3a df a2 b7 c2 5f 2f 0b ac 52 70

4. Online Issuing CA:

Distinguished Name	CN=DNBNL-CA2, O=De Nederlandsche Bank N.V., C=NL
Serial Number	36 00 00 00 12 cc 02 d7 25 2b 5d 02 3e 00 00 00 00 00 12
Distinguished Name of Issuer	CN=DNBNL-POLICYCA, O=De Nederlandsche Bank N.V., C=NL
Validity Period	From 13-06-2017 to 11-06-2027
Message Digest (SHA-1)	56 9c 69 68 f4 bd a4 c8 ec 5b 7b 8e 5e 98 ca 9b ad fe cb 68

5. Online Issuing CA:

Distinguished Name	CN=DNBNL-CA-ONLINE, O=De Nederlandsche Bank N.V., C=NL
Serial Number	36 00 00 00 0c c9 18 7e 92 41 78 54 64 00 00 00 00 00 0c
Distinguished Name of Issuer	CN=DNBNL-POLICYCA, O=De Nederlandsche Bank N.V., C=NL
Validity Period	From 19-05-2017 to 17-05-2027
Message Digest (SHA-1)	ec db 96 39 46 53 c9 f8 6a 1f 2b f7 73 5d b2 36 5f 5a c2 3c

3.1.3 Registration Authority

This includes individuals, policies, procedures and computer systems entrusted with verifying the identity of those applying for electronic certificate and, when appropriate, of the attributes associated with them. RAs shall identify those applying for certificates pursuant to the rules established in this CPS and the corresponding CP, the relations between both parties will be governed by this CPS and the applicable CP.

The needed roles which shall be performed in accordance with this CPS and the relevant CPs, have been assigned internally. These roles are:

- Registration Officers (ROs) which are responsible for identifying certificate applicants, validating the documentation required during the identification process, gathering all the information necessary to issue the public key certificate and allowing the user to retrieve the certificate
- Key Recovery Officers (KROs) which participate during the recovery of encryption key pairs from the Key Archive (if applicable).
- Shared Mailbox Administrator: The Shared Mailbox Administrator (SMA) role is in charge of defining in the DNB-PKI system the attributes of those shared mailboxes that require an electronic certificate.

3.1.4 Validation Authority

The Validation Authority (VA) is the computer system, together with the corresponding policies and procedures, responsible for verifying the status of the certificates issued by DNB-PKI.
This is presented via Certificate Revocation Lists (CRL).

3.1.5 Key Archive

The Certificate Policies may establish the existence of a Keys Archive, which is a computer system that, together with the corresponding policies and procedures, enables the archiving and recovery of the private keys belonging to subscribers of the certificates regulated under said policies. The Keys Archive must guarantee the confidentiality of the private keys and their recovery must require the intervention of at least two people. The CP must regulate the request and processing procedures for key recovery.

3.1.6 Certificate Subscribers

A Certificate Subscriber is any individual or computer component for which a certificate is issued within the DNB-PKI environment. Certificate entitlement becomes effective once the certificate has been issued by the CA and accepted by the applicant.
The types of entities that can hold DNB-PKI certificates are defined and limited in each CP.

3.1.7 Relying Parties

Relying parties are individuals or entities other than subscribers that have decided to accept and rely on a certificate issued by DNB-PKI. The Certificate Policies corresponding to each type of certificate determine the relying parties for each certificate.

3.2 Certificate Usage

3.2.1 Appropriate certificate use

The appropriate use of each certificate is established in the Certificate Policies corresponding to each type of certificate.

3.2.2 Certificate usage constraints and restrictions

The certificates must be used in accordance with the functions and purposes defined in their corresponding CP and may not be used for activities or purposes not included therein.
Likewise, the certificates must be used solely in accordance with the applicable legislation.
Unless otherwise specified in the CP, the certificates may not be used to act as Registration Authority or Certification Authority, or for signing public key certificates of any kind or Certificate Revocation Lists (CRL).
The certification services provided by DNB-PKI have not been designed nor are they authorised for use in high risk activities or those that require fail-safe operations, such as those related to the running of hospital, nuclear or air or rail traffic control facilities, or any other where failure could lead to death, personal injury or serious environmental damage.
The Certificate Policies corresponding to each certificate may establish additional certificate usage constraints or restrictions.
It is not the purpose of this CPS to establish said additional constraints and restrictions.

3.3 Policy Administration

3.3.1 CPS

This CPS belongs to De Nederlandsche Bank.

3.3.2 Contact Person

This CPS is managed by the PAA of DNB-PKI. New versions of this CPS and CPs will be approved by these PAA and will become available.

3.3.3 Establishment of the suitability of a CPS from an External CA as regards the DNB-PKI Certificate Policies

In the event of having to evaluate the possibility of an external CA interoperating with DNB-PKI, the PAA is responsible for determining whether or not the CPS of the external CA is suitable for the CP in question.

3.3.4 Approval Procedure for this CPS

De Nederlandsche Bank, division ICT, is accountable for approving this Certificate Practice Statement (CPS), as well as the different Certificate Policies (CP); it has, nevertheless, authorized the CIO Office and in particular Information Security within the CIO office to elaborate and publish the needed updates to said documents, informing about them on a periodic basis.

4. Publication and Repository Responsibilities

4.1 External repositories

Repository	URL
Root CA CRLs distribution point	http://pki.dnb.nl/pki/dnbnl-rootca.crl
Policy CA CRLs distribution point	http://pki.dnb.nl/pki/dnbnl-policyca.crl
Issuing CA CRLs distribution point	http://pki.dnb.nl/pki/dnbnl-ca1.crl http://pki.dnb.nl/pki/dnbnl-ca1+.crl http://pki.dnb.nl/pki/dnbnl-ca2.crl http://pki.dnb.nl/pki/dnbnl-ca2+.crl http://pki.dnb.nl/pki/dnbnl-ca-online.crl http://pki.dnb.nl/pki/dnbnl-ca-online+.crl
Root CA certificate distribution point	http://pki.dnb.nl/pki/dnbnl-rootca.crt
Online CA certificate distribution point	http://pki.dnb.nl/pki/dnbnl-policyca.crt http://pki.dnb.nl/pki/dnbnl-ca1.crt http://pki.dnb.nl/pki/dnbnl-ca2.crt http://pki.dnb.nl/pki/dnbnl-ca-online.crt

4.2 Documentation on Practice Statements and Policies

Document	URL
Certification Practice Statement (CPS)	https://www.dnb.nl/pki/
Certificate Policy (CP)	https://www.dnb.nl/pki/

DNB-PKI repository does not contain any information of a confidential nature.

4.3 Publication of Certification Data, CPS and CP

Both the CPS and the rest of the related documentation are available to certificate applicants, subscribers and relying parties at https://www.dnb.nl/pki/

At https://www.dnb.nl/pki/ links to the DNB-PKI Certificate Revocation Lists (CRLs) are available in CRL v2 format. The CRL will be signed electronically by the DNB-PKI CA that issued them.
The information about certificate status can be obtained by accessing the CRL directly.

4.4 Publication Timescale or Frequency

The CPS and the CPs are published as they are created, as well as when any modification to them is approved.

4.5 Repository Access Controls

De Nederlandsche Bank, is authorized to modify, substitute or eliminate information from its repository or website. For this purpose, De Nederlandsche Bank has established controls that prevent unauthorized individuals from manipulating the information contained in the repositories.

5. Identification and Authentication (I&A)

5.1 Naming

5.1.1 Types of names
All certificate holders must have a distinguished name pursuant to the X.500 standard.
The procedure for distinguished name assignment is determined in the policy drawn up for this purpose, developed and described in the CP corresponding to the certificate in question.

5.1.2 The need for names to be meaningful
The procedure for making distinguished names meaningful is determined in the policy drawn up for this purpose, developed and described in the CP corresponding to the certificate in question.

5.1.3 Rules for interpreting various name formats
The rule applied by DNB-PKI for the interpretation of the distinguished names for subscribers of the certificates it issues is the ISO/IEC 9595 (X.500) Distinguished Name (DN) standard.

5.1.4 Uniqueness of names
Each Distinguished Name must be unique and unambiguous, the Certificate Policies will establish the procedures to guarantee this.

5.1.5 Name dispute resolution procedures
Any dispute concerning ownership of names will be resolved by Information Security / CIO Office.

5.1.6 Recognition, authentication, and the role of trademarks
No stipulation.

5.2 Initial Identity Validation

5.2.1 Means of proof of possession of the private key

In the event that the key pair is generated by the certificate applicant, the possession of the private key, shall be proven by sending the certificate signing request (CSR), which includes it's public key, to the CA. This procedure may be modified with another established in each case in the applicable CP.

5.2.2 Identity authentication for an entity

When applicable, each CP will establish the identity authentication procedure for entities.

5.2.3 Identity authentication for an individual

The CP applicable to each type of certificate will define the identification procedure, the minimum data to be provided by the applicant. Also the minimum aspects will be described like:

- Types of identity documents valid for identification.
- CA or RA procedures to identify the individual.
- Whether or not in-person identification is required.
- Means of proof of belonging to a specific organisation.

5.2.4 Non-verified applicant information

Each CP will establish which part of the information provided in the application for a certificate shall not necessarily be verified.

5.2.5 Validation of authority

For issuance of computer component certificates, verification of the authority of the person responsible for the application for said certificates will be established in the specific CP.

5.2.6 Criteria for operating with external CAs

Before establishing interoperation with external CAs, their suitability to meet certain requirements must be established. The minimum criteria to consider a CA suitable to interoperate with DBN-PKI, which may be extended in each case by the PAA, are:

- The external CA must provide a level of security in the handling of its certificates, and throughout their entire life cycle, equal, at least, to that of DNB-PKI. This requirement shall be included in the corresponding CPS and CP and in their fulfilment by the CA.
- It must provide an audit report from an independent Authority of recognised prestige regarding its operations, as a means of verifying the existing level of security. The PAA may waive this requirement for CAs belonging to Public Administrations or the European System of Central Banks.
- It must establish a collaboration agreement that sets out the commitments given as regards the security of the certificates included in the interoperation,

Even when the CA fulfils the aforementioned requirements, the PAA may refuse the application for interoperation without the need to give any justification.
Interoperation may be carried out by way of cross-certification, unilateral certification or by other means.

5.3 Identification and Authentication for Re-key Requests

5.3.1 Identification and authentication requirements for routine re-key

The identification and individual authentication processes are defined in the CP applicable to each type of certificate.

5.3.2 Identification and authentication requirements for re-key after certificate revocation

The identification and individual authentication processes are defined in the CP applicable to each type of certificate.

6. Certificate Life Cycle Operational Requirements

6.1 Certificate Application Process

6.1.1 Process for submitting a certificate application

The person who is allowed to submit a certificate is documented in the corresponding CP. To submit a certificate the terms and conditions application form must be completed and the identification documentation must be provided. All information will be approved by the Registration Authority. If needed the RA might refuse to issue a certificate to any applicant based exclusively on its own criteria and without leading to any liability whatsoever for any consequences may arise from that refusal.
After approval, the applicant will be informed about the delivery of the certificate and (when appropriate) the publication of certificates in the DNB-PKI internal repository.

6.1.2 Enrollment process

The enrollment process for a certificate is documented in the corresponding CP.

6.1.3 Time limit for processing the certificate applications

The Certification Authority shall not be held liable for any delays that may arise in the period between application for the certificate, publication in the DNB-PKI repository (when appropriate), and its delivery. In any case, the minimum deadlines for processing certificate applications will be established in the corresponding Certificate Policies.

6.2 Certificate Acceptance

6.2.1 Form of certificate acceptance

Certificate acceptance signifies commencement of the certificate applicants' obligations in relation to DNB-PKI.
Certificates that require identification in person shall carry certificate applicants' explicit acceptance and acknowledgement that they are in agreement with the terms and conditions contained in the terms and conditions acceptance form for the certification services provided by the DNB-PKI, which govern the rights and obligations assumed between DNB-PKI and certificate applicants. Likewise it shall also carry express declaration that the certificate applicants are aware of the existence of this CPS, which sets out the technology and operations of the electronic certificate services provided by DNB-PKI. The certificates applicants shall sign the terms and conditions application form.
For online renewals, terms and conditions acceptance may be carried out by way of electronic signature.
The corresponding CP may detail or extend the manner in which certificates are accepted.

6.2.2 Notification of certificate issuance by the CA to other Authorities

When a DNB-PKI CA issues a certificate pursuant to a certificate application processed through an RA, it shall send a copy of the same to the RA that forwarded the application.

6.3 Key Pair and Certificate Usage

6.3.1 Certificate subscribers' use of the private key and certificate

The responsibilities and constraints relating to the use of key pairs and certificates will be established in the corresponding CP.
Certificate subscribers may only use the private key and the certificate for the uses authorised in the CP and in accordance with the 'Key Usage' and 'Extended Key Usage' fields of the certificate. Likewise, certificate subscribers may only use the key pair and the certificate once they have accepted the terms and conditions of use established in the CPS and CP, and only for that which is stipulated therein.
Following certificate end-of-life or revocation, certificate subscribers must discontinue the use of the private key.

6.3.2 Relying parties' use of the public key and the certificate

Relying parties may only rely on the certificates as stipulated in the corresponding CP and in accordance with the 'Key Usage' field of the certificate.
Relying parties are obliged to check the status of a certificate using the mechanisms established in this CPS and the corresponding CP. Likewise, they accept the obligations regarding the conditions of use set forth in those documents.

6.4 Certificate Renewal

6.4.1 Circumstances for certificate renewal with no key changeover

All certificate renewals covered by this CPS shall be carried out with change of keys. Consequently, the remaining points in this section established in RFC 3647 are not included and, therefore, for the purposes of this Statement, their content is "no stipulation".

6.5 Certificate Re-key

6.5.1 Circumstances for certificate renewal with key changeover

The certificate renewal procedure shall depend on the CP applicable to each type of certificate.
A certificate may be renewed for the following reasons, among others:

- End of the validity period
- Modification of the data contained in the certificate.
- When the keys are compromised or are no longer fully reliable.
- Change of format.

All certificate renewals covered by this CPS shall be carried out with change of keys.

6.5.2 Who may request certificate renewal?

Renewal must be requested by certificate subscribers, although not all certificates include this option. Each CP will establish who may request a certificate renewal.

6.5.3 Procedures for processing certificate renewal requests with key changeover

During the renewal process, the RA will check that the information used to verify the identity and attributes of the certificate subscriber is still valid. If any of the certificate subscriber's data have changed, they must be verified and registered with the agreement of the certificate subscriber.
In any case, certificate renewal is subject to:

- The request being made in due time and manner, following the instructions and regulations established by DNB-PKI specifically for this purpose.
- The RA or CA not having certain knowledge of the existence of any cause for the revocation / suspension of the certificate.
- The request for the renewal of the provision of services being for the same type of certificate as the one initially issued.

6.5.4 Notification of the new certificate issuance to the certificate subscriber

Each CP shall establish the manner in which applicants will be informed that the corresponding certificate has been issued in their name.

6.5.5 Manner of acceptance of certificates with changed keys

Each CP shall establish the manner of acceptance.

6.5.6 Publication of certificates with the new keys by the CA

Each CP shall establish, when appropriate, the procedure for publishing the certificates in the DNB-PKI repository.

6.5.7 Notification of certificate issuance by the CA to other Authorities

When a DNB-PKI CA issues a certificate pursuant to a certificate application processed through an RA, it shall send a copy of the same to the RA that forwarded the application.

6.6 Certificate Modification

6.6.1 Circumstances for certificate modification

Certificate modification takes place when a new certificate is issued due to changes in the certificate information, not related to its public key or end-of-life of the certificate.
All certificate modifications carried out within the scope of this CPS will be treated as certificate renewals and, therefore, the previous points in this respect shall be applicable. Consequently, the remaining points in this section as established in RFC 3647 are not included, meaning that, for the purpose of this Statement, they are not covered.

6.7 Certificate Revocation and Suspension

6.7.1 Circumstances for revocation

Certificate revocation is the action that renders a certificate invalid prior to its expiry date. Certificate revocation produces the discontinuance of the certificate's validity, rendering it permanently inoperative as regards its inherent uses and, therefore, discontinuance of the provision of certification services. Revocation of a certificate prevents its legitimate use by the certificate subscriber.
The revocation request process is defined in the CP applicable to each type of certificate.
Revocation of a certificate entails its publication on the Certificate Revocation Lists (CRL). Once the period of validity of a revoked certificate has expired, it is removed from the CRL.

Causes for revocation:
Notwithstanding the applicable legislation, a certificate may be revoked in the following cases:

- Loss, disclosure, modification or any other circumstance that compromises the certificate subscriber's private key or when suspicion of such compromise exists.
- Deliberate misuse of keys and certificates, or failure to observe or infringement of the operational requirements contained on the Acceptance Form for the terms and conditions of the certification services provided by the DNB-PKI CA, in the associated CP or in this CPS.
- The certificate subscriber ceases to belong to the group, when that membership granted the certificate subscriber the right to hold the certificate.
- DNB-PKI ceases its activity.
- Defective issue of a certificate due to:
  1. Failure to comply with the material requirements for certificate issuance.
  2. Reasonable belief that basic information related to the certificate is or could be false.
  3. The existence of a data entry error or any other processing error.
- The key pair generated by the certificate subscriber has been found to be "weak".
- The information contained in a certificate or used for the application becomes inaccurate.
- By order of the certificate subscriber or an authorised third party.
- The certificate of a higher RA or CA in the certificate trust hierarchy is revoked.
- The existence of any other cause specified in this CPS or in the corresponding Certificate Policies established for each type of certificate.

The main effect of revocation as regards the certificate is the immediate and early termination of its term of validity, with which the certificate becomes invalid. Revocation shall not affect the underlying obligations created or notified by this CPS, nor shall its effects be retroactive.

6.7.2 Who can request revocation?

- The CA or any of the RAs may, at their own initiative, request the revocation of a certificate if they become aware or suspect that the certificate subscriber's private key has been compromised, or in the event of any other determining factor that recommends taking such action.
- Certificate subscribers or, in the case of component certificates, component managers may also request revocation of their certificates, which must be carried out in accordance with the conditions specified in *Procedures for requesting certificate revocation*. The identification policy for revocation requests is the same as that of the initial registration. The authentication policy shall accept revocation requests signed electronically by the certificate subscriber, as long as it is done using a valid certificate other than the one for which the revocation is requested. If this is not possible the person will be authenticated (shortly) or the manager will process the request.
- Via the standard ISO:20000 ITSM change process for a person who is leaving the company.

The different Certificate Policies may establish other identification procedures of a stricter nature.

6.7.3 Procedures for requesting certificate revocation

The revocation request procedure for each type of certificate shall be established in the corresponding CP.

6.7.4 Revocation request grace period

Revocation shall be carried out immediately following the processing of each request that is verified as valid. Therefore, the process will not include a grace period during which the revocation request may be cancelled.

6.7.5 Time limit for the CA to process the revocation request

Each CP shall establish the maximum time allowed for processing revocation requests. Notwithstanding the aforementioned, it is hereby established that, as a general rule, that time shall will be less than 24 hour.

6.7.6 Requirements for revocation verification by relying parties

Relying parties must check the validity of the certificate prior to each use and download the new CRL from the DNB-PKI repository when the one they hold expires. Certificate Revocation Lists stored in cache memory, even when not expired, do not guarantee availability of updated revocation data.
Optionally, unless the applicable CP establishes otherwise, the VA may be used for revocation verification. When the CP accepts other forms of revocation data publication, the requirements for checking data will be specified in the CP itself.

6.7.7 CRL issuance frequency

DNB-PKI shall publish a new CRL in its repository even when the CRL has not been modified.
Root CA at least every 6 months, Policy CA at least 3 days and Issuing CA each 24 hours.

6.7.8 Maximum latency between the generation of CRLs and their publication

Each CP will establish the maximum time allowed between generation of the CRLs and their publication in the repository.

6.7.9 Online certificate revocation status checking availability

DNB-PKI provides a repository on which it publishes the CRLs for verification of the status of the certificates it issues.

6.7.10 Online revocation checking requirements

Online parties must check the validity of the certificate prior to each use and download the new CRL from the DNB-PKI repository when the one they hold expires. Optionally, when using the VA, relying parties must have software capable of operating with an online highly available website to obtain the certificate information.

6.7.11 Special requirements for the revocation of compromised keys

There are no variations to the aforementioned clauses for revocation due to private key compromise.

6.7.12 Causes for suspension

Suspension is not an option, when needed a certificate is revoked.

6.7.13 Who can request the suspension?

Not applicable.

6.7.14 Procedure for requesting certificate suspension

Not applicable.

6.7.15 Suspension period limits

Not applicable.

6.8 Certificate Status Services

6.8.1 Operational characteristics
Publication of Certificate Revocation Lists (CRL) is provided.

6.8.2 Service availability
The CRL is available permanently, every day of the year.

6.8.3 Additional features
Not applicable.

6.9 End of Subscription
Certificate subscription may be ended due to the following causes:

- Certificate revocation due to any of the causes established in section *Who can request revocation*
- End of the certificate validity period.

If certificate renewal is not requested, the end of the subscription will terminate the relationship between the certificate subscriber and the CA.

6.10 Key Escrow and Recovery

6.10.1 Key escrow and recovery practices and policies
The policies and practices for key registration and recovery shall be identified in each CP that establishes private key escrow.
No private key for any certificate in which the non-repudiation electronic signature functionality has been authorised shall be escrowed (see whether or not the 'Key Usage' code is "1" in the 'nonRepudiation' field).

6.10.2 Session key protection and recovery policies and practices
When appropriate, the corresponding CP will identify the policies and practices for the protection and recovery of session keys.

7. Facility Management, and Operational Controls

7.1 Physical Security Controls

This point establishes the most significant measures taken to physical security controls.

7.1.1 Site location and construction

The buildings in which the DNB-PKI infrastructure is located are separated and capable of housing the PKI infrastructure. Multiple physical measures are taken to prevent theft or burglary.
All DNB-PKI's critical operations are carried out in physically secured facilities, with specific levels of security for the most critical elements.

7.1.2 Physical access

There is a complete system to control physical access by individuals at the entry and exit, comprising various levels of security. All sensitive operations are carried out within a physically secure facility with different levels of security required to access critical machinery and applications.
Loading and unloading areas are isolated and under permanent surveillance, by human and technical means.

7.1.3 Power and air-conditioning

The infrastructure is protected against power failures or any other electricity supply anomaly. Systems that so require have permanent power supply units as well as a generator.
The rooms in which DNB-PKI infrastructure equipment is located has air-conditioning.

7.1.4 Water exposure

Appropriate measures have been taken to prevent exposure of the equipment and cables to water.

7.1.5 Fire prevention and protection

The rooms have the suitable means (detectors and actors) to protect their content against fire.

7.1.6 Storage system

De Nederlandsche Bank has established all the necessary procedures to make backup copies of all its productive infrastructure data. De Nederlandsche Bank has organised backup copy plans, the same as those used in the rest of the banks central infrastructure, for all the sensitive data and those considered necessary for activity continuity.

7.1.7 Waste disposal

A waste management policy has been adopted that guarantees destruction of any material that could contain information, as well as a management policy for removable media.

7.1.8 Offsite backup

DNB-PKI has backup copies in two separate data centers, which have the necessary security measures in place and are suitably physically separated.

7.2 Procedural controls

For security reasons, the information related to procedural controls is considered confidential and only part of this is included herein.
DNB-PKI endeavours to ensure that all management, related to both operational and administrative procedures, is carried out in a secure manner, pursuant to the guidelines in this document, carrying out periodic audits.
Additionally, duties have been divided to prevent a single person from obtaining control of the entire infrastructure.

7.2.1 Roles responsible for PKI control and management

The following responsibilities are established for control and management of the PKI system

7.2.1.1 Roles to manage Hardware Security Modules (HSM)

HSM administrator role
HSM administrator is responsible for creating new partitions, delete or change existing partitions and to configure policies.

HSM operator role
HSM operator is the owner of the partition and is responsible for backup of the partition.

HSM audit role
HSM auditor is responsible for the operation of the HSM audit data.

Due to the HSM, a minimum of two people with sufficient professional capacity are required to perform the tasks of HSM Administration or Operation.

7.2.1.2 Roles to manage PKI infrastructure

Registration Officers
Responsible for issuing of the certificate, revocation when needed and for life cycle management of the issued certificate

Security Officer:
Responsible for establishing and verifying security policies and procedures.

PKI administrator:
Responsible for the operation of the systems that make up the PKI infrastructure, the hardware and the base software.

PKI Policy Manager:
Responsible for configuring, publishing and maintaining CA templates and policies.

PKI Issue Manager:
Authority responsible for approving submitted requests for creating and revoking PKI certificates

PKI Web manager:
Authority responsible for configuring, publishing and maintaining web content of the CA web enrolment servers.

PKI Audit Administrator:
Responsible for carrying out and reviewing internal audit data of the PKI infrastructure.

Backup Administrator:
Responsible for carrying out and reviewing the backup copies of the PKI infrastructure.

User Administrators:
Responsible for processing personal certificate requests, controlling their correct download by subscribers and subscribers' acceptance of the terms and conditions of use.

7.3 Personnel Controls

7.3.1 Requirements concerning professional qualification, knowledge and experience

All personnel working in the DNB-PKI environment must have sufficient knowledge, experience and training for optimum performance of their assigned duties.
Therefore, De Nederlandsche Bank carries out the personnel selection processes it considers necessary to ensure that the professional profiles of personnel are the most suitable to the features inherent to the tasks to be carried out.

7.3.2 Background checks and clearance procedures

In accordance with personnel selection procedures arenestablished by De Nederlandsche Bank.

7.3.3 Training requirements

In accordance with to procedures established by De Nederlandsche Bank.
Specifically, personnel related to PKI operations will receive the necessary training to ensure the correct performance of their duties.

7.3.4 Retraining requirements and frequency

In accordance with to procedures established by De Nederlandsche Bank.

7.3.5 Frequency and sequence for job rotation

No stipulation.

7.3.6 Sanctions for unauthorised actions

Unauthorised action shall be classified as a work offence, sanctioned pursuant to De Nederlandsche Bank Labour Regulations and in the Workers' Statute, without prejudice to the liabilities of any other kind that may be incurred.

7.3.7 Requirements for third party contracting

De Nederlandsche Bank general regulations shall be applied to contracting.

7.3.8 Documentation supplied to personnel

Access will be given to the mandatory security regulations together with this CPS and those contained in the applicable CP.

7.4 Audit Logging Procedures

7.4.1 Types of events recorded

All events produced within a high secure enterprise PKI environment will be recorded.

7.4.2 Frequency with which audit logs are processed

Logs are analysed manually when necessary, or using automatic tools, and there is no established frequency for this process.

7.4.3 Period for which audit logs are kept

The information generated in the audit logs is direct available until it is archived. Once archived, audit logs are kept for at least 3 years.

7.4.4 Audit log protection

Events logged by the PKI is protected and can only be accessed by the event viewing applications and with the appropriate access controls.

7.4.5 Audit log back up procedures

Backup copies of audit logs are made in accordance with the standard measures established by De Nederlandsche Bank.

7.4.6 Audit data collection system (internal vs. external)

The PKI's system for compiling audit data is a combination of automatic and manual processes carried out by the PKI applications and are stored in DNB-PKI internal systems and sent to central log facilities.

7.4.7 Notification to the subject who caused the event

No automatic notification of audit log file actions to the subject who caused the event has been established.

7.4.8 Vulnerability assessment

Vulnerability assessment is covered by De Nederlandsche Bank VPM proces. This process contains scanning on vulnerabilities, patching of systems within defined times and reporting.

7.5 Records Archival

7.5.1 Types of records archived

Each Certificate Authority within in DNB-PKI stores, for the established periods, all the information related to the operations carried out with certificates and keeps an events log.
Logged operations include those carried out by the administrators who use the DNB-PKI element administration applications, as well as all the data related to the registration process.

7.5.2 Archive retention period

All the information related to certificates is held for an appropriate period of time for a high secure enterprise PKI environment.

7.5.3 Archive protection

Events logged by the PKI is protected and can only be accessed by the event viewing applications and with the appropriate access controls.

7.5.4 Archive backup procedures

Backup copies of log archives are made in accordance with the standard measures established by De Nederlandsche Bank.

7.5.5 Requirements for time-stamping records

The information systems employed by DNB-PKI guarantee logging of the time at which the log entries were made. The moment in time in the systems comes from a secure source that establishes the date and time.

7.5.6 Audit data archive system (internal vs. external)

Data collection is internal to the Certification Authority and corresponds to the DNB-PKI.

7.5.7 Procedures to obtain and verify archived information

Events logged by the PKI are protected and can only be accessed by the event viewing and management applications.

7.6 Key Changeover

The procedures to provide subscribers and relying parties of the certificates of the former with a new CA public key, in the event of key changeover, are the same as those used to provide the current public key. Consequently, the new CA key will be published in the DNB-PKI repository.

7.7 Compromise and Disaster Recovery

7.7.1 Incident and compromise handling procedures

De Nederlandsche Bank has established a Contingency Plan that sets out the actions to be taken, resources to be used and personnel to be employed in the case of a deliberate or accidental event that renders useless or deteriorates the resources or certification services provided by DNB-PKI.

In the event of any compromise of the signature verification data of any Certification Authority, DNB-PKI shall inform all DNB-PKI certificate subscribers and relying parties known that all the certificates and revocation lists of certificates signed with said data are no longer valid. Service will be re-established as soon as possible.

7.7.2 Corruption of computing resources, software, and/or data

If computing resources, software, and/or data are corrupted or suspected to be corrupted, PKI operations will be halted until the environment's security has been re-established, with the incorporation of new components, the suitability of which can be accredited. At the same time, an audit will be carried out to identify the cause of the corruption and ensure it does not reoccur.
In the event that issued certificates are affected, the users of the same will be notified and new certificates will be issued.

7.7.3 Action procedures in the event of compromise of an Authority's private key

If a DNB CA's private key is compromised, it will be revoked immediately. The corresponding CRL will then be generated and published and the Authority's activity ceased, carrying out the generation, certification and start-up of a new Authority with a new key pair and with the same name as the eliminated one but updating the version identifier.
In the event that a DNB CA is affected, its revoked certificate shall remain accessible in the DNB-PKI repository in order to continue verifying the certificates issued whilst it was operational.
The Authorities that make up DNB-PKI that are dependent on the affected CA will be informed of the situation and urged to request new certification by the CA with its new key.
All the affected Authorities will be notified that the certificates and revocation data, supplied with CA's compromised key, cease to be valid from the moment of notification, so they must use the CA's new public key to verify data validity.
Certificates signed by the Authorities dependent on the affect CA during the period between key compromise and the corresponding certificate revocation will likewise be revoked, notifying their subscribers of this circumstance and issuing new certificates.

7.7.4 Installation following a natural disaster or another type of catastrophe

The DNB-PKI Certification Authority system can be reconstructed in the event of disaster. Hardware, software and procedures are available. Tests on rebuilding have been done.
With these elements it is possible to reconstruct the system as it was at the time the backup copy was made and, therefore, recover the CA, including its private keys.

7.8 CA or RA Termination

7.8.1 Certification Authority

In the event of termination of activities of a CA, DNB-PKI will ensure that the potential problems for its certificate subscribers and relying parties are kept to a minimum, as well as ensuring maintenance of the records required to provide certified proof of the certificates for legal purposes.
In the event of termination of the activities of one or all of the CA's, DNB-PKI will notify their certificate subscribers and relying parties, by any means that guarantee sending and receipt of said notifications

and with a minimum notice of two months prior to the termination of activities, that it intends to have the corresponding CA/CAs discontinue its/their activities as certification services provider/s.
In the event the DNB-PKI decides to transfer the activity to another Certification Services Provider, it shall notify its certificate subscribers regarding the transfer agreements. For this purpose, DNB-PKI shall send a document explaining the transfer terms and conditions and the characteristics of the Provider to which it proposes to transfer certificate management. This notification shall be carried out by any means that guarantee sending and receipt of the notification, at least two months prior to the effective termination of its activities.
Likewise, it shall report any other relevant circumstance that could prevent activity continuity.

7.8.2 Registration Authority

Once the Registration Authority ceases to carry out its duties, it shall transfer the records it holds to DNB-PKI, when the obligation subsists to maintain the information on file; otherwise, it will be destroyed.

8. Technical Security Controls

8.1 Key Pair Generation and Installation

8.1.1 Key pair generation

The key pairs for the Root CA, Policy CA and Issuing CA are generated in cryptographic hardware modules with at least FIPS 140-2 Level 3 certification. Key pairs for encrypting email are also stored in cryptographic hardware modules to provide recovery when needed.
Key pairs needed for internal systems might be generated and stored on the system self. The PKI CA is not responsible for these keys.

8.1.2 Delivery of private keys to certificate subscribers

The method used to deliver private keys to their certificate subscribers depends on each certificate and is established in the CP corresponding to each certificate.

8.1.3 Delivery of the public key to the certificate issuer

The method used to deliver the public key to their certificate subscribers depends on each certificate and is established in the CP corresponding to each certificate.

8.1.4 Delivery of the CA's public key to relying parties

The public key of the Root CA and the Online CA's are made available to relying parties in the DNB-PKI repository, notwithstanding the possibility of the CP establishing additional mechanisms for the delivery of these keys.

8.1.5 Key sizes

The Root CA key size is 4096 bits. The Online CA's key size is 4096 bits.
The size of the keys for each type of certificate issued by DNB-PKI is defined in the applicable CP.

8.1.6 Public key generation parameters and quality checks

RootCA and Online CA's keys are encoded pursuant to RFC 3280 and PKCS#1. The key generation algorithm is the RSA.
The key generation parameters for each type of certificate issued by DNB-PKI are determined in the applicable CP.
The procedures and means of checking the quality of the key generation parameters for each type of certificate issued by DNB-PKI are determined in the applicable CP.

8.1.7 Accepted key usage (KeyUsage field in X.509 v3)

The accepted key usage for each type of certificate issued by DNB-PKI is defined in the applicable CP.
All certificates issued by DNB-PKI contain the Key Usage extension defined under the X.509 v3 standard, which is classified as critical. Additional constraints may be established through the Extended Key Usage extension.
It should be noted that the efficiency of constraints based on certificate extensions can sometimes depend on the operational characteristics of computer applications that have not been designed by DNB-PKI.

8.2 Private Key Protection and Cryptographic device Engineering Controls

8.2.1 Cryptographic device standards

The cryptographic device used to store keys used by RootCA and OnlineCA's comply with at least FIPS 140-2 Level 3 certification. Keys stored in the cryptographic hardware module on the DNB company card is also at least FIPS 140-2 Level 3 certified.

8.2.2 Private key multi-person (k out of n) control

Both the Root CA and Online CA's private keys are under multi-person control. This is realized by means of booting the CA software requiring a minimum amount of operators from the CA. This is the only method available to activate said private key.
A certain number 'K' of HSM operators (where K≥2), out of a total of 'N', are necessary to activate and use the DNB-PKI Root CA and Online CA private keys.

8.2.3 Escrow of private keys

Escrow of the private keys for the certificates is carried out by their certificate subscribers. The DNB-PKI encipherment private keys are only escrowed by archiving them.

8.2.4 Private key backup copy

The private keys of the CA are archived under the protection of the HSMs belonging to each of them and to which only the administrators and operators of the CA have access. Backup is executed automatically, facilities and procedures are in place and tested.

8.2.5 Private key archive

Private keys for signature certificates of individuals are never archived in order to guarantee non-repudiation. Encipherment certificates private keys are archived and their recovery procedures are established in their CP.

8.2.6 Private key transfer into or from a cryptographic device

Private keys can only be transferred between cryptographic devices (HSM) and require the intervention of a certain number 'K' of HSM administrators (where K≥2), out of a total of 'N'.

8.2.7 Private key storage in a cryptographic device

Both the Root CA and Online CA's private keys are generated in cryptographic devices (HSM) and they are stored enciphered.

8.2.8 Private key activation method

As stipulated under section *Private key multi-person control* the private keys of both the Root CA and the Online CA are activated by booting the CA software using a certain number 'K' of HSM operators (where K≥2) of the corresponding CA, out of a total of 'N'. This is the only method to activate that private key.
Activation of the keys of the rest of the certificate subscribers is determined in the applicable Certificate Policies.

8.2.9 Private key deactivation method

Stored private keys are never deactivated, only destructed.

8.2.10 Private key destruction method

Revocation shall be carried out immediately following the processing of each request that is verified as valid. The corresponding stored private keys are destructed immediately.

8.2.11 Cryptographic device classification

The cryptographic devices used as HSM in the PKI infrastructure or on the DNB company card comply with the FIPS 140-2 Level 3 standard.

8.3 Computer Security Controls

The information under this section is confidential. Access to this information is limited to those who can prove a need to know, such as in the case of external or internal inspection audits.

8.3.1 Specific security technical requirements

The data related to this section are considered confidential information and are provided only to those who can certify a need to know.

8.3.2 Computer security evaluation

DNB-PKI permanently evaluates its level of security to identify any possible weaknesses and establish the corresponding corrective measures, through internal and external audits, as well as continuously carrying out security checks.

8.4 Life Cycle Security Controls

The information under this section is confidential. Access to this information is limited to those who can prove a need to know.

8.5 Network Security Controls

The information under this section is confidential. Access to this information is limited to those who can prove a need to know.

8.6 Timestamping

The information systems employed by DNB-PKI guarantee logging of the time at which the log entries were made. The moment in time in the systems comes from a secure source that establishes the date and time.

9. Certificate, CRL, and OCSP Profiles

9.1 Certificate Profile

9.1.1 Version number

DNB-PKI supports and uses X.509 Version 3 (X.509 v3) standards.

9.1.2 Certificate extensions

The certificate extensions used generically are:

Extension	Classification
KeyUsage	Classified as critical.
BasicConstraints	Classified as critical.
CertificatePolicies	Classified as non-critical.
SubjectAlternativeName	Classified as non-critical.
CRLDistributionPoint	Classified as non-critical.
Subject Key Identifier	Classified as non-critical.
Authority Key Identifier	Classified as non-critical.
ExtKeyUsage	Classified as non-critical.
Auth. Information Access	Classified as non-critical.

DNB-PKI Certificate Policies may establish variations in the set of extensions used for each type of certificate, if so it is are specified in the applicable CP.

DNB-PKI has documented the following proprietary extensions:

Concept	Description
Personal Name	
Personal Middle Name	
Personal Surname 1	Name and surnames of the individual who is the certificate subscriber
Personal Surname 2	
Employee Number	DNB employee or contracted personnel number
Common Name	User login name
User Principle Name	Employee Number@dnb.nl
User email address	DNB email address
National identifier Number	National ID document, Passport ID, etc.
DNB Application description	Display name of the DNB application or shared mailbox

9.1.3 Algorithm Object Identifiers (OID)
Cryptographic algorithm objects identifiers (OID): SHA256 RSA (2.16.528.1.1017)

9.1.4 Name formats
Certificates issued by DNB-PKI contain the X.500 distinguished name of the certificate issuer and that of the subject in the issuer name and subject name fields, respectively.

9.1.5 Name constraints
The names contained in the certificates are restricted to X.500 distinguished names, which are unique and unambiguous.

9.1.6 Certificate Policy Object Identifiers (OID)
DNB-PKI has established a policy for assignment of OIDs within its private enumeration scale under which the OID for all the DNB-PKI Policy Certificates begin with the prefix 2.16.528.1.1017:

Sub number	Description
.1	IT systems related to the PKI infrastructure
.2	Documentation related to the PKI infrastructure

Explanation sub number .1
This sub number is used to describe IT systems for the PKI.

Sub number	Description Subsidiary
Sub .1	Corp.

Sub number	Description Department
Sub .1.1	IT.

Sub number	Description Environment
Sub .1.1.1	Production.

Sub number	Description Technology
Sub .1.1.1.5	PKI of the Production Environment.

Sub number	Description General Policy
Sub .1.1.1.5.1	General Purpose Issuance Policy of the Production Environment.

Explanation sub number .2
This sub number is used to describe the documentation of the PKI infrastructure.

Sub number	Description Asset
Sub .2	Documentation.

Sub number	Description Environment
Sub .2.1	Production.

Sub number	Description Location
Sub .2.1.1	Internal.

Sub number	Description Sources
Sub .2.1.1.2	Certificate Practice Statement (CPS)
Sub .2.1.1.3	Certificate Policy Internal Users (CP)

9.1.7 Use of the "PolicyConstraints" extension
No stipulation.

9.1.8 Syntax and semantics of the “PolicyQualifier”
The Certificate Policies extension contains the following Policy Qualifiers:

- URL CPS: contains the URL to the CPS and the CP that govern the certificate.

9.1.9 Processing semantics for the critical “Certificate Policy” extension
The only critical extensions are the Basic Constraints and the Key Usage which are recommended.

9.2 CRL Profile

9.2.1 Version number
DNB-PKI supports and uses X.509 version 2 (v2) CRLs.

9.2.2 CRL and extensions
No stipulation.

9.3 OCSP Profile

9.3.1 Version number(s)
Not applicable.

9.3.2 OCSP Extensions
Not applicable.

10. Compliance Audit and Other Assessment

10.1 Frequency or Circumstances of Controls for each Authority

DNB-PKI will be audited at least once every 3 year, in accordance with the ESCB Certificate Acceptance Framework (CAF). This guarantees that it's functioning and operations are in accordance with the stipulations included in this CPS and the CPs.

10.2 Identity / Qualifications of the Auditor

Audits may be entrusted to external auditors or, as specified in the ESCB Audit Policy, to the ESCB Internal Auditors Committee (IAC) according to the annual audit program.
All teams or the person designated to carry out a security audit on DNB-PKI must fulfil the following requirements:

- Appropriate training and experience in PKI, security, cryptographic technology and audit procedures.
- Independence at the organizational level from the DNB-PKI Authority (RA, CA, KA or VA) being audited.

10.3 Relationship between the Assessor and the Entity being Assessed

Regardless of the purpose of the audit, the auditor and the audited party (DNB-PKI) shall not have any kind of relationship that could derive in a conflict of interests. In the case of internal auditors, these may not have any operational relationship with the area being audited.

10.4 Aspects Covered by Controls

The audit shall determine whether or not the DNB-PKI services are in accordance with this CPS and the applicable CPs. A Risk assessment will be done and scoping for audit will be determined after this.

10.5 Actions Taken as a Result of Deficiencies Found

Corrective measures shall be taken upon identification of deficiencies found as a result of the audit. The DNB-PKI Owner, in collaboration with the auditor, shall be responsible for establishing them.
In the event of observing serious deficiencies, the ITC may make, among others, the decision to revoke the CAF compliancy.

10.6 Notification of the Results

The audit team shall notify the results of the audit to the DNB-PKI Owner, as well as the DNB-PKI administrators and those of the Authority in which incidents were detected.

11. Other Business and Legal Matters

11.1 Fees

11.1.1 Certificate issuance or renewal fees
The fees for the issuance and renewal of each certificate are specified in the applicable CP.

11.1.2 Certificate access fees
The fees for certificate access are specified in the applicable CP.

11.1.3 Revocation or status information fees
The fees for access to the information on the status or revocation of each certificate are specified in the applicable CP.

11.1.4 Fees for other services, such as policy information
No fees shall be applied for supplying information on this CPS or the CPs managed by DNB-PKI or for any other additional service that may be known at the time of drawing up this document.
This provision may be modified by the CP applicable in each case.

11.1.5 Refund policy
Should any CP specify any fee applicable for certification or revocation services provided by DNB-PKI for the type of certificate it defines, the corresponding refund policy must be established.

11.2 Financial Responsibility

11.2.1 Insurance
De Nederlandsche Bank N.V., decided to realize the PKI infrastructure and procedures for internal use only.

11.2.2 Other assets
No stipulation.

11.2.3 Insurance or warranty coverage for end-entities
No stipulation.

11.3 Confidentiality of Business Information
Procedures and techniques are available to determine the classification of a document. These are used for all documents needed to create and maintain the DNB-PKI

11.3.1 Scope of confidential information
All information not considered by DNB-PKI as public shall be of a confidential nature and access may only be granted to those with an official need-to-know in order to perform their official duties related to the DNB-PKI.

11.3.2 Non-confidential information
The list of certificates suspended or revoked is considered public information and, therefore, available to third parties.

11.3.3 Duty to maintain professional secrecy
All personnel who takes part in any activities inherent to or derived from DNB-PKI are committed to maintaining professional secrecy and, therefore, are subject to the applicable legal provisions, in particular, Article 37 of the Statute of the European System of Central

Banks and of the European Central Bank and the corresponding national provisions applicable to the ESCB national central banks.
Likewise, contracted personnel that takes part in any DNB-PKI activities or operations are subject to the duty of professional secrecy within the framework of their contractual obligations with DNB-PKI CA and RA.

11.4 Privacy of Personal Information

11.4.1 Personal data protection policy
The procedures and operation of the DNB-PKI, this CPS and each CP are in line with the current valid national legislation applicable to the Eurosystem Central Banks.

11.4.2 Information considered private
All data corresponding to individuals is subject to the personal data protection laws.

11.4.3 Information not classified as private
Each CP shall establish the personal data to be included in the certificates and the certificate and CRL repositories. Acceptance by subscribers of the certificates issued in their name constitutes their consent to publication.

11.4.4 Responsibility to protect personal data
The ESCB Central Banks, including the Eurosystem Central Banks (as the owners of the ESCB-PKI) and De Nederlandsche Bank N.V. (as the Service Provider) are co-controllers for ESCB-PKI data protection purposes, and in accordance with the allocation of roles and responsibilities, comply with and apply the legal, technical and management measures required by the respective current valid national legislation transposing.

11.4.5 Notification of and consent to the use of personal data
Each CP shall establish the mechanisms to notify certificate applicants and, when appropriate, obtain their consent for the processing of their personal data.

11.4.6 Disclosure within legal proceedings
Personal data may only be disclosed to third parties, without the consent of the person affected, to the extent permitted under the applicable personal data protection law.

11.4.7 Other circumstances in which data may be made public
No stipulation.

11.5 Intellectual Property Rights
The DNB-PKI Service Provider has obtained all the necessary licenses regarding all intellectual property rights related to the electronic certificates issued by the DNB-PKI for individuals and technical components, the certificate revocation lists, the content of this CPS and the CPs as well as all intellectual property rights related to any other electronic or any other kind of document, protocol, computer program and hardware, file, directory, database and consultation service that may be required to carry out the DNB-PKI activities.
The object identifiers (OIDs) are property of De Nederlandsche Bank and have been registered with the Nederlands Normalisatie-instituut (NEN) under the Joint-iso-itu-t.Country.Nl.Nederlandse-organisatie the identified organizations section, having been assigned the number 2.16.528.1.1017.
Unless express agreement from DNB-PKI, no OID assigned to DNB-PKI may be partially or fully used, except for the specific uses included in the Certificate or Directory.

11.6 Representations and Warranties

11.6.1 Obligations of the CA

The CAs that operate within the DNB-PKI hierarchy must ensure that all the obligations established under this point are included, as applicable, in the Certificate Policies. Each CA shall be responsible for fulfilment of its obligations, as stipulated in this CPS, even when part of its activities is subcontracted. Likewise, each CA shall provide its services in a manner consistent with the CPS.
The CAs that operate within the DNB-PKI hierarchy have the following obligations:

CAO.1	To carry out their operations in accordance with this CPS.
CAO.2	To protect the private keys.
CAO.3	To issue certificates in accordance with the applicable CP.
CAO.4	Following receipt of a valid certificate application, to issue certificates in accordance with the X.509 v3 standard and the requirements of the application.
CAO.5	To issue certificates that are in accordance with the information known at the time of their issue, and free from data recording errors.
CAO.6	To publish the certificates, when necessary, to interoperate with other users or computer systems that so require.
CAO.7	To revoke the certificates in the terms of *Certificate Revocation and Suspension* and publish revoked certificates in the CRL and in the directory and web services referred to under section *CRL issuance frequency*
CAO.8	To notify changes to this CPS and the CPs as established under point *Notification Period and Mechanism*
CAO.9	To conserve the terms and conditions acceptance documents for the certification services of De Nederlandsche Bank certification authority that have been signed, on paper or electronically, by the certificate applicants in which they acknowledge that they have understood their obligations and rights, consent to the use of their personal data by the CA and confirm that the information provided is correct.
CAO.10	To guarantee the availability of the CRLs, pursuant to point *Online certificate revocation status checking availability* in this CPS.
CAO.11	In the event that the CA revokes a certificate, to notify this to the certificate users in accordance with the applicable CP.
CAO.12	To collaborate with the DNB-PKI authorities in validating re-keying.
CAO.13	To operate in accordance with the applicable current valid legislation.
CAO.14	To protect the keys in its custody, if any.
CAO.15	Not to store, under any circumstances, the signature creation data, the private key, of the subscribers of certificates issued for the purpose of using them for electronic signature *(key usage = nonrepudiation)*, whether acknowledged or not.

11.6.2 Obligations of the RA

The RAs operating in De Nederlandsche bank DNB-PKI shall fulfil the following obligations:

RAO.1	To identify Subscribers and/or Applicants and the organisations they represent correctly, in accordance with the procedures established in this CPS and Certificate Policies specific to each type of certificate, employing any legally approved means.
RAO.2	To formalise the issue of the Certificates to the Subscribers in the terms and conditions established in the Certificate Policies.
RAO.3	To store in a secure manner and for a reasonable period of time the documentation provided in the certificate issue process and in its suspension/revocation process.
RAO.4	To carry out any duties that may correspond, through the personnel necessary in each case, as established in this CPS.

11.6.3 Obligations of certificate subscribers

The subscribers of certificates issued under this CPS shall have the following obligations:

CSO.1	Provide accurate, full and truthful information regarding the data requested by those entrusted with their verification in order to carry out the registration process.
CSO.2	To inform DNB-PKI management of any modification to said data.
CSO.3	To understand and accept the terms and conditions of use of the certificates and, specifically, those contained in this CPS and the applicable CPs, as well as any modifications thereto.
CSO.4	To restrict and condition the use of the certificates to the scope of their labour relationship with the Nederlandsche Bank and pursuant to that permitted under the corresponding CP and this CPS.
CSO.5	To take the necessary care and measures to guarantee the safekeeping of their DNB company card, preventing its loss, disclosure, modification or unauthorised use.
CSO.6	The process to obtain the certificates requires the personal selection of a control PIN for the DNB company card and activation of the private key. The holder is responsible for keeping the PIN number secret.
CSO.7	To immediately request the revocation of a certificate upon detecting any inaccuracy in the information contained therein or upon becoming aware of or suspecting any compromise of the private key corresponding to the public key contained in the certificate due, among other causes, to: loss, theft, potential compromise, knowledge by third parties of the PIN.
CSO.8	Not monitor, manipulate or carry out any reverse engineering on the technical implementation (hardware and software) of the certification services.
CSO.9	Not to transfer or delegate to third parties their obligations pertaining to a certificate assigned to them.
CSO.10	Any other obligation derived under law, this CPS or the Certificate Policies.

11.6.4 Obligations of relying parties

Third parties who accept and rely on certificates issued by DNB-PKI shall have the following obligations:

RPO.1	To limit reliability on the certificates to the uses that they allow, pursuant to the certificate extensions and the corresponding CP.
RPO.2	To verify the validity of the certificates upon receipt of the documents signed electronically by checking that the certificate is valid and has not expired or been suspended or revoked.
RPO.3	To assume the responsibility for correct verification of the electronic signatures.
RPO.4	To assume responsibility for checking the validity as well as the revocation or suspension status of the certificates they accept and rely on.
RPO.5	To be aware of the guarantees and responsibilities derived from acceptance of the certificates on which they rely and accept that they are subject to them.
RPO.6	To notify any anomalous event or circumstance pertaining to the certificate, which could be considered cause for its revocation.

11.7 Disclaimers of Warranties

The DNB-PKI as certification service provider will be liable in case of damages to the signer or bona fide third parties in case of lack or delay while including certificates in the revocation information service.
De Nederlandsche Bank's PKI shall only accept liability for damages caused by undue use of a certificate when said certificate and its associated CP state, in a manner clearly recognisable by third parties, a limitation as to its possible use or as to the value of valid transactions that may be carried out using it.
De Nederlandsche Bank's PKI, as Provider of Certification Services, does not accept liability for the content of documents signed using its certificates.
De Nederlandsche Bank's PKI does not represent, in any way whatsoever, the users nor relying parties of the certificate it issues.

11.7.1 DNB-PKI liabilities

DNB-PKI assumes no liability in the event of losses or damages:

LIAB.1	Related to services it provides, in the event of war, natural disaster or any other kind of accidental or force majeure circumstances: public disorder, transport strike, loss of power and/or telephone service, computer viruses, deficiencies in telecommunication services or compromise in the asymmetric keys derived from an unforeseeable technological hazard.
LIAB.2	Incurred during the period between certificate application and delivery to the user.
LIAB.3	Caused by certificate usage that exceeds the limitations established in the same, the corresponding CP and this CPS.
LIAB.4	Caused by misuse of the information contained in the certificate.
LIAB.5	Caused by improper or fraudulent use of certificates or the CRLs issued by DNB-PKI
LIAB.6	De Nederlandsche Bank's PKI shall not hold itself liable in any way whatsoever for the use of certificates issued by its CAs and the private/public key pair linked to subscribers for any activity not specified in the CPS or in the corresponding Certificate Policies.
LIAB.7	De Nederlandsche Bank's PKI, as Provider of Certification Services, shall not be liable for the content of documents signed using its certificates, nor for any other use of its certificates.

11.7.2 Scope of liability coverage

Not applicable

11.8 Limitations of Liability

Except those stipulated in the provisions of this CPS or in the applicable CP and in the applicable legislation, De Nederlandsche Bank shall accept no other liability regarding certificate subscribers or relying parties in the event of losses or damages:

LIAB.1	Related to services it provides, in the event of war, natural disaster or any other kind of accidental or force majeure circumstances: public disorder, transport strike, loss of power and/or telephone service, computer viruses, deficiencies in telecommunication services or compromise in the asymmetric keys derived from an unforeseeable technological hazard.
LIAB.2	Incurred during the period between certificate application and delivery to the certificate subscriber.
LIAB.3	Caused by certificate usage that exceeds the limitations established in the same, the corresponding CP and this CPS.
LIAB.4	Caused by misuse of the information contained in the certificate.
LIAB.5	Caused by improper or fraudulent use of certificates or the CRLs issued by DNB-PKI CA.
LIAB.6	DNB-PKI CA and RAs shall not be held liable in any way whatsoever for the use of certificates issued by its CA and the private/public key pair linked to certificate
LIAB.7	DNB-PKI CA and RAs, shall not be held liable for the content of documents signed using its certificates, nor for any other use of its certificates.
LIAB.8	DNB-PKI CA and RAs shall not be held liable for any indirect, incidental, consequential or any other kind of damages, or for any loss of profits, loss of data, or other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance, or non-performance of Certificates, digital signatures, or other transactions or services contemplated by the present CPS.

11.9 Indemnities

DNB-PKI assumes no financial responsibility for improperly used certificates, CRLs, etc.

11.10 Term and Termination

11.10.1 Term

This CPS shall come into force from the moment it is published in the internal DNB-PKI repository. It shall remain valid until such time as it is expressly terminated due to the issue of a new version, or upon re-key of the Root CA keys, at which time a new version shall be drawn up.

11.10.2 CPS substitution and termination

This CPS shall be substituted for a new version, regardless of the importance of the changes carried out therein, meaning that it will always be applicable in its entirety.
When the CPS is terminated, it will be withdrawn from the DNB-PKI internal repository and will be held for an appropriate period of time for a high secure enterprise PKI environment.

11.10.3 Consequences of termination

The obligations and constraints established under this CPS, referring to audits, confidential information, DNB-PKI obligations and liabilities that came into being whilst it was in force shall continue to prevail following its substitution or termination with a new version in all terms which are not contrary to said new version.

11.11 Individual notices and communications with participants

All notifications, demands, applications or any other type of communication required in the practices described in this CPS shall be carried out by electronic message or in writing, by registered post, addressed to any of the addresses contained in the section *Policy Administration*. Electronic notifications shall be effective upon receipt by the recipients to which they are addressed.

11.12 Amendments

11.12.1 Amendment procedures

The Authority empowered to carry out and approve amendments to this CPS and corresponding Certificates Policies is the Policy Administration Authority (PAA).

11.12.2 Notification period and mechanism

Should the PAA deem that the amendments to the specifications could affect the acceptability of the certificates for specific purposes, it shall notify the users of certificates corresponding to the amended CP or CPS that an amendment has been carried out and that they should consult the new CPS in the internal repository.

11.12.3 Circumstances in which the OID must be changed

When, in the opinion of the PAA, the changes to specifications do not affect the acceptability of the certificates, the lower version number of the document will be increased as well as the last number of the Object Identifier (OID) that represents it, maintaining the highest version number of the document, as well as the rest of the associated OID. It is not considered necessary to notify this type of modification to users of the certificates corresponding to the CP or CPS modified.
Should the PAA deem that the amendments to the specifications could affect the acceptability of the certificates for specific purposes, the highest version number of the document shall be changed and its lowest number placed at zero. The last two numbers of the Object Identifier (OID) that represents it will also be modified. This type of modification will be notified to the users of the certificates corresponding to the CP or CPS modified.

11.13 Dispute Resolution Procedures

Resolution of any dispute between internal users and the DNB-PKI that may arise shall be submitted first to internal departments for further investigation. Procedures are available for users how to start this.

11.14 Governing Law

The CA, the RAs and the VA shall comply with the current valid applicable national laws and regulations.

11.15 Compliance with Applicable Law

The PAA is responsible for ensuring compliance with the applicable legislation stated under the previous point.

11.16 Miscellaneous Provisions

11.16.1 Entire agreement clause

All the relying parties accept the content of the latest version of this CPS and the applicable Certicate Policies in their entirety.

11.16.2 Independence

Should any of the provisions of this CPS be declared invalid, null or legally unenforceable, it shall be deemed as not included, unless said provisions were essential in such a way that excluding them from the CPS would render the latter without legal effect.

11.16.3 Resolution through the courts

No stipulation.

11.17 Other Provisions

No stipulation.

12. Definitions and Acronyms

12.1 Definitions

Within the scope of this CP the following terms are used:

Authentication	The process of verifying the identity of an applicant or subscriber of a DNB-PKI certificate
Electronic Certificate	A document signed electronically by a certification services provider, which links signature verification data (public key) to a signatory and confirms their identity. This is the definition contained in Law 59/2003, which this document extends to cases in which the signature verification data is linked to a computer component
Public Key and Private Key	The asymmetric cryptography on which the PKI is based employs a key pair in which what is enciphered with one of these can only be deciphered by the other, and vice versa. One of these keys is "public" and includes the electronic certificate, whilst the other is "private" and is only known by the certificate subscriber and, when appropriate, by the Keys Archive
Session Key	Key established to encipher communication between two entities. The key is established specifically for each communication, or session, and its utility expires upon termination of the session
Computer Component (or simply, "component")	Refers to any software or hardware device that may use electronic certificates, for its own use, for the purpose of its identification or for exchanging signed or enciphered data with relying parties
Directory	Data repository that is accessed through the LDAP protocol
Identification	The process of establishing the identity of an applicant or subscriber of a DNB-PKI certificate
User Identifier	A set of characters that are used to uniquely identify the user of a system
Public Key Infrastructure (PKI)	Set of individuals, policies, procedures, and computer systems necessary to provide authentication, encipherment, integrity and nonrepudiation services, by way of public and private key cryptography and electronic certificates
Trust Hierarchy	Set of certification authorities that maintain a relationship of trust by which a CA of a higher level guarantees the trustworthiness of one or several lower level CAs. In the case of DNB-PKI, the hierarchy has two levels, the Root CA at the top level guarantees the trustworthiness of its subordinate CAs
Provider of Certification Services	Individual or entity that issues electronic certificates or provides other services related to the electronic signature
Applicants	Individuals who apply for a certificate for themselves or for a computer component
Relying Parties	Individuals or entities other than subscribers that decide to accept and rely on a certificate issued by DNB-PKI
Subscribers	Individuals or computer components for which an electronic certificate is issued and accepted by said individuals or, in the case of component certificates, by the component manager

12.2 Acronyms

PAA	Policy Approval Authority
CA	Certification Authority
RA	Registration Authority
VA	Validation Authority
CRL	Certificate Revocation List
C	Country. Distinguished Name (DN) attribute of an object within the X.500 directory structure
CDP	CRL Distribution Point
CEN	Comité Européen de Normalisation
CN	Common Name. Distinguished Name (DN) attribute of an object within the X.500 directory structure
CSR	Certificate Signing Request: set of data that contains the public key and its electronic signature using the companion private key, sent to the Certification Authority for the issue of an electronic signature that contains said public key
CWA	CEN Workshop Agreement
DN	Distinguished Name. Unique identification of an entry within the X.500 directory structure
CPS	Certification Practice Statement
ETSI	European Telecommunications Standard Institute
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module. Cryptographic security module used to store keys and carry out secure cryptographic operations
IETF	Internet Engineering Task Force (internet standardisation organisation)
LDAP	Lightweight Directory Access Protocol
O	Organisation. Distinguished Name (DN) attribute of an object within the X.500 directory structure
OCSP	Online Certificate Status Protocol. Protocol that enables online verification of the validity of an electronic certificate
OID	Object Identifier
OU	Organisational Unit. Distinguished Name (DN) attribute of an object within the X.500 directory structure
CP	Certificate Policy
PIN	Personal Identification Number. Password that protects access to the DNB company card
PKCS	Public Key Infrastructure Standards. Internationally accepted PKI standards developed by RSA Laboratories
PKI	Public Key Infrastructure
DNB-PKI	De Nederlandsche Bank PKI
PKIX	Work group within the IETF (Internet Engineering Task Group) set up for the purpose of developing PKI and internet specifications
PCS	Provider of Certification Services
PUK	PIN UnlocK Code. Password used to unblock the DNB company card that has been blocked after repeatedly and consecutively entering the wrong PIN
RFC	Request For Comments (Standard issued by the IETF)