DeNederlandscheBank
EUROSYSTEEM

DNB PKI - Certificate Policy (CP) for Internal User certificates

OID of this document: 2.16.528.1.1017.2.1.1.3

Date: November 16, 2018

OVERVIEW This document covers the Certification Policy for internal user certificates (CP) that governs the functioning and operations certificates of De Nederlandsche Bank Public Key Infrastructure (PKI).

This CP 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 Policy (CP) for user certificates
Author	André Lensink (department head ICT CIO Office)
Version	1.3
Date	16.11.2018

Change Log

Version	Date	Change Reason
0.1	20.04.2016	Initial Version
0.2	08.06.2019	Text added
0.3	12.10.2016	Text review
0.9	21.04.2017	Adding information
1.0	26.06.2017	Final Version
1.1	15.11.2017	Revised after feedback PKI-AB (ITC/SRMWG)
1.2	24.04.2018	Revised after feedback PKI-AB (ITC/SRMWG)
1.3	16.11.2018	Revised after feedback PKI-AB (ITC/SRMWG)

Table of content

1. Content, rights and obligations established in this Certificate Policy (CP) for internal users

This document covers the Certificate Policy (CP) for internal users certificates issued by the Corporate Certification Authority of the De Nederlandsche Bank Public Key Infrastructure (hereinafter, DNB-PKI).

This CP details and completes the "Certification Practice Statement" (CPS) of the De Nederlandsche Bank PKI, containing the rules to which the use of the certificates defined in this policy are subject, as well as the scope of application and the technical characteristics of this type of certificate.

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 CP includes all the activities for managing internal users certificates throughout life cycle, and serves as a guide for the relations between DNB-PKI Corporate CA and its users. Consequently, all the parties involved must be aware of the content of this CP and activities to the stipulations therein.
This CP 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.

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

2. Introduction

2.1 Overview

This document provides both users and De Nederlandsche Bank – as the Public Key Infrastructure (PKI) operator – with a summary of the binding certification guidelines of De Nederlandsche Bank for the issuance of internal user certificates in the form of a Certificate Policy (CP).

2.2 Document name and Identification:

Name	Description
Title	Certificate Policy (CP) for Internal Users Certificates
Classification	Public
Version	1.1
Date	November 2017
Document status	Final
Author	Information Security
O.I.D. (Object Identifier)	2.16.528.1.1017.2.1.1.3

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

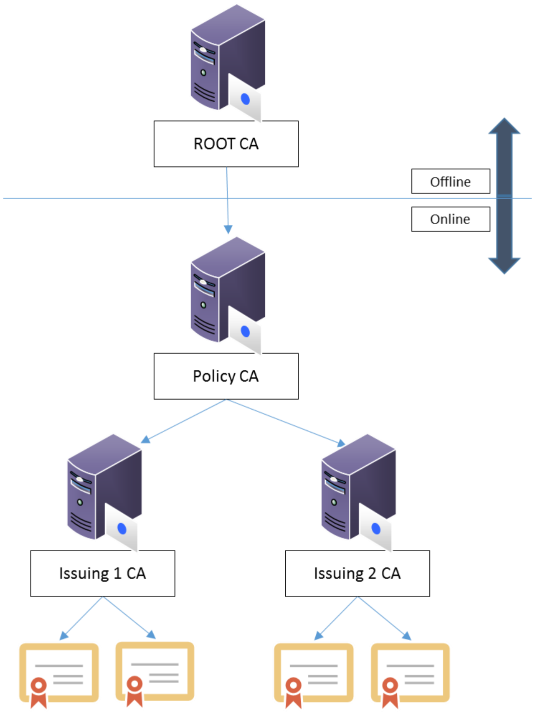

Figure 1 – Online and offline servers

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 PKI Participants

The participating entities and persons beside the owner of de DNB-PKI are:

1. The Policy Approval Authority.
2. The Certification Authority.
3. The Registration Authority.
4. The Validation Authority.
5. The Keys Archive.
6. The Subscribers.
7. The Relying Parties.

3.1.1 Policy Approval Authority

The Policy Approval Authority is defined in accordance with the DNB-PKI Certification Practice Statement.

3.1.2 Certification Authority

The Certification Authority is defined in accordance with the DNB-PKI Certification Practice Statement.

3.1.3 Registration Authority

The Registration Authorities are defined in accordance with the DNB-PKI Certification Practice Statement.

3.1.4 Validation Authority

The Validation Authority is defined in accordance with the DNB-PKI Certification Practice Statement.

3.1.5 Key Archive

The Key Archive enables escrow and recovery of the private keys of encryption certificates. When needed keys are generated and stored in cryptographic devices. To recover a key multiple PKI employees are required to fulfill this action and to process it to the applicant.

3.1.6 Certificate Subscribers

A subscriber is defined as: De Nederlandsche Bank employees or contracted personnel with access to De Nederlandsche Bank information systems.
A standard user certificate can be used for authentication of the user on devices and applications, which accepts this mechanism and for electronic signature. For encrypting email a separate certificate is created and connected to the applicant.

3.1.7 Relying Parties

Relying parties can use this CP to decide whether a user certificate, and the binding therein, are sufficiently trustworthy to authenticate and verify the subscriber and to decrypt emails from the subscriber.

3.2 Certificate Usage

3.2.1 Appropriate certificate use

Certificates for internal users issued by De Nederlandsche Bank may only be used by its employees or contracted personnel, both in the internal and external relations necessary for the internal, inherent or operational running of the institution.

3.2.2 Certificate Usage Constraints and Restrictions

Any other use not included in the previous point shall be excluded.

3.3 Policy Administration

3.3.1 Certificate Policy

This CP belongs to De Nederlandsche Bank.

3.3.2 Contact Person

As specified in DNB-PKI's Certification Practice Statement.

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

As specified in DNB-PKI's Certification Practice Statement.

3.3.4 Approval Procedures for this CP

As specified in DNB-PKI's Certification Practice Statement.

4. Repositories and Publication of Information

4.1 External repositories

As specified in DNB-PKI's Certification Practice Statement.

4.2 Documentation on Practice Statements and Policies

As specified in DNB-PKI's Certification Practice Statement.

4.3 Publication of Certification Data

As specified in DNB-PKI's Certification Practice Statement.

4.4 Publication Timescale or Frequency

As specified in DNB-PKI's Certification Practice Statement.

4.5 Repository Access Controls

As specified in DNB-PKI's Certification Practice Statement.

5. Identification and Authentication

5.1 Naming

5.1.1 Types of names

The name of the certificate issued (Distinguished Name = DN) must comply with the X.509 standard.

Name	Description
Common Name (CN)	Unique DNB user identifier
Organizational Unit (OU)	Users, Divisions
Organization (O)	De Nederlandsche Bank N.V.
Country (C)	NL
Subject Alternative Names (SAN)	CN@dnb.nl

5.1.2 The need for names to be meaningful

In all cases the Distinguished Name of the certificates must be meaningful and are subject to the rules established in the previous point in this respect.

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

Certificate DNs may not be repeated. The use of the users unique DNB account code guarantees the uniqueness of the Distinguished Name (DN).

5.1.5 Name dispute resolution procedures

As specified in DNB-PKI's Certification Practice Statement.

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

The key pair for the personal certificate is only stored in the cryptographic device of the DNB company card. The owner of the card can give access to this cryptographic device via a PIN.
The key pair for some administrator certificates are stored in the cryptographic device of the DNB company card. The owner of the card can give access to this cryptographic device via a PIN.

5.2.2 Identity authentication for an entity

Issue of certificates for entities is not considered.

5.2.3 Identity authentication for an individual

Authentication of identity of an individual requires their physical presence and will be identified by way of an identification document valid at law.

5.2.4 Non-verified applicant information

All the information stated in the previous section must be verified.

5.2.5 Validation of authority

No stipulation, given that the issue of certificates for entities is not considered.

5.2.6 Criteria for operating with external CAs

As specified in DNB-PKI's Certification Practice Statement

5.3 Identification and Authentication for Re-key Requests

5.3.1 Identification and authentication requirements for routine re-key

The individual identification process shall be the same as in the initial validation.

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

The individual identification process shall be the same as in the initial validation.

6. Certificate Life Cycle Operational Requirements

6.1 Certificate Application Proces

6.1.1 Who can submit a certificate application?

De Nederlandsche Bank employees or contracted personnel with access to De Nederlandsche Bank information systems can submit a user certificate.
Application for a certificate does not mean it will be obtained, the RA might refuse to issue the user 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.

6.1.2 Enrollment process and applicants' responsibilities

To obtain a user certificate the standard ISO:20000 ITSM change management process is used and consist of the following steps:

1. New employees or contracted personnel data is added to internal systems after approval of multiple conditions.
2. A change is created and send to an internal department to create a windows account & user certificate request.
3. The employee or contracted personnel is authenticated in person.
4. The DNB company card for access to the building is transferred to the authenticated person
5. The employee or contracted personnel goes to the Service desk with his/her DNB company card for authentication
6. The employee or contracted personnel receives the PKI Terms and Conditions document and signs it.
7. The Service desk initializes the DNB company card, in presence of the card holder, with a certificate lifecycle management tool. Via this tool the user certificate is transferred to the DNB Company card and a random PIN is generated.
8. The DNB company card with the user certificate is transferred to the employee or contracted personnel.
9. PIN and instruction about how to change the initial PIN will be transferred to the applicant. The applicant is urged to change the PIN immediately.

To provide confidentiality, separations of duty is in place.

6.1.3 Time limit for processing the certificate applications

As specified in DNB-PKI's Certification Practice Statement.

6.2 Certificate Acceptance

6.2.1 Form of certificate acceptance

As specified in DNB-PKI's Certification Practice Statement.

6.2.2 Notification of certificate issuance by the CA to other Authorities

Not applicable.

6.3 Key Pair and Certificate Usage

6.3.1 Subscribers' use of the private key and certificate

As specified in DNB-PKI's Certification Practice Statement.

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

As specified in DNB-PKI's Certification Practice Statement.

6.4 Certificate Renewal

6.4.1 Circumstances for certificate renewal with no key changeover

As specified in DNB-PKI's Certification Practice Statement.

6.5 Certificate Re-key

6.5.1 Circumstances for certificate renewal with key changeover

As specified in DNB-PKI's Certification Practice Statement.

6.5.2 Who may request certificate renewal?

See section *Who can submit a certificate application*

6.5.3 Procedures for processing certificate renewal requests with key changeover

See section *Enrollment process and applicants' responsibilities*

6.5.4 Notification of the new certificate issuance to the certificate subscriber

See section *Enrollment process and applicants' responsibilities*

6.5.5 Manner of acceptance of certificates with changed keys

Each user will only be entitled to use one set of activated keys. As a result there will be no added value for resigning a new T&C form as the previous certificates have been revoked prior to distributing new ones.

6.5.6 Publication of certificates with the new keys by the CA

Not applicable.

6.5.7 Notification of certificate issuance by the CA to other Authorities

Not applicable.

6.6 Certificate Modification

6.6.1 Circumstances for certificate modification

As specified in DNB-PKI's Certification Practice Statement.

6.7 Certificate Revocation and Suspension

6.7.1 Circumstances for revocation

As specified in DNB-PKI's Certification Practice Statement.

6.7.2 Who can request revocation?

As specified in DNB-PKI's Certification Practice Statement.

6.7.3 Procedures for requesting certificate revocation

The standard ISO:20000 ITSM change management process is used.

6.7.4 Revocation request grace period

As specified in DNB-PKI's Certification Practice Statement.

6.7.5 Time limit for the CA to process the revocation request

Requests for revocation of user certificates are processed immediately.

6.7.6 Requirements for revocation verification by relying parties

Verification of revocations is mandatory for each use made of a user certificate, a CRL is available to check the status of the certificate.

6.7.7 CRL issuance frequency

As specified in DNB-PKI's Certification Practice Statement.

6.7.8 Maximum latency between the generation of CRLs and their publication

The maximum time allowed between generation of the CRLs and their publication in the repository is 6 hours.

6.7.9 Online certificate revocation status checking availability

As specified in DNB-PKI's Certification Practice Statement.

6.7.10 Online revocation checking requirements

As specified in DNB-PKI's Certification Practice Statement.

6.7.11 Special requirements for the renewal of compromised keys

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

6.7.12 Causes for suspension

An internal user certificate will not be suspended. Might there be a reason for suspension the certificate will be revoked.

6.7.13 Who can request the suspension?

No stipulation.

6.7.14 Procedure for requesting certificate suspension

No stipulation.

6.7.15 Suspension period limits

No stipulation.

6.8 Certificate status services

6.8.1 Operational characteristics

As specified in DNB-PKI's Certification Practice Statement.

6.8.2 Service availability

As specified in DNB-PKI's Certification Practice Statement.

6.8.3 Additional features

As specified in DNB-PKI's Certification Practice Statement.

6.9 End of Subscription

As specified in DNB-PKI's Certification Practice Statement.

6.10 Key Escrow and Recovery

6.10.1 Key escrow and recovery practices and policies

The only private keys that are archived in the Key Archive are the keys corresponding to encryption certificates, which are part of the personal certificate package.

De Nederlandsche Bank employees or contracted personnel with access to De Nederlandsche Bank information systems are authorized to request recovery of their own keys using the ISO:20000 ITSM change management process.

Once the request has been approved, members of Department Information Security Management in the role of Key Archive Administrators act as follows:

1. Once verified the signed request, one of the Key Archive Administrators, in presence of the second, accesses the Registration Authority application to recover from the Key Archive a PKCS#12 file with the encryption private key.
2. The second Key Archive Administrator enters the PIN required to protect the PKCS#12 file.
3. The second Key Archive Administrator facilitates the PIN to the requestor.
4. The first Key Archive Administrator facilitates the recovered PKCS#12 file to the requestor.

6.10.2 Session key protection and recovery policies and practices

No stipulation.

7. Management, Operational, and Physical Controls

7.1 Physical Security Controls

7.1.1 Site location and construction
As specified in DNB-PKI's Certification Practice Statement.

7.1.2 Physical access
As specified in DNB-PKI's Certification Practice Statement.

7.1.3 Power and air-conditioning
As specified in DNB-PKI's Certification Practice Statement.

7.1.4 Water exposure
As specified in DNB-PKI's Certification Practice Statement.

7.1.5 Fire prevention and protection
As specified in DNB-PKI's Certification Practice Statement.

7.1.6 Storage system
As specified in DNB-PKI's Certification Practice Statement.

7.1.7 Waste disposal
As specified in DNB-PKI's Certification Practice Statement.

7.1.8 Offsite backup
As specified in DNB-PKI's Certification Practice Statement.

7.2 Procedural controls

7.2.1 Roles responsible for PKI control and management
As specified in DNB-PKI's Certification Practice Statement.

7.3 Personnel Security Control

7.3.1 Requirements concerning professional qualification, knowledge and experience
As specified in DNB-PKI's Certification Practice Statement.

7.3.2 Background checks and clearance procedures
As specified in DNB-PKI's Certification Practice Statement.

7.3.3 Training requirements
As specified in DNB-PKI's Certification Practice Statement.

7.3.4 Retraining requirements and frequency
As specified in DNB-PKI's Certification Practice Statement.

7.3.5 Frequency and sequence for job rotation
As specified in DNB-PKI's Certification Practice Statement.

7.3.6 Sanctions for unauthorised actions
As specified in DNB-PKI's Certification Practice Statement.

7.3.7 Requirements for third party contracting
As specified in DNB-PKI's Certification Practice Statement.

7.3.8 Documentation supplied to personnel
As specified in DNB-PKI's Certification Practice Statement.

7.4 Audit Logging Procedures

7.4.1 Types of events recorded
As specified in DNB-PKI's Certification Practice Statement.

7.4.2 Frequency with which audit logs are processed
As specified in DNB-PKI's Certification Practice Statement.

7.4.3 Period for which audit logs are kept
As specified in DNB-PKI's Certification Practice Statement.

7.4.4 Audit log protection
As specified in DNB-PKI's Certification Practice Statement.

7.4.5 Audit log back up procedures
As specified in DNB-PKI's Certification Practice Statement.

7.4.6 Audit data collection system (internal vs. external)
As specified in DNB-PKI's Certification Practice Statement.

7.4.7 Notification to the subject who caused the event
As specified in DNB-PKI's Certification Practice Statement.

7.4.8 Vulnerability assessment
As specified in DNB-PKI's Certification Practice Statement.

7.5 Records Archive

7.5.1 Types of records archived
As specified in DNB-PKI's Certification Practice Statement.

7.5.2 Archive retention period
As specified in DNB-PKI's Certification Practice Statement.

7.5.3 Archive protection
As specified in DNB-PKI's Certification Practice Statement.

7.5.4 Archive backup procedures
As specified in DNB-PKI's Certification Practice Statement.

7.5.5 Requirements for time-stamping records
As specified in DNB-PKI's Certification Practice Statement.

7.5.6 Audit data archive system (internal vs. external)
As specified in DNB-PKI's Certification Practice Statement.

7.5.7 Procedures to obtain and verify archived information
As specified in DNB-PKI's Certification Practice Statement.

7.6 CA Key Changeover

As specified in DNB-PKI's Certification Practice Statement.

7.7 Compromised Key and Disaster Recovery

7.7.1 Incident and compromise handling procedures

As specified in DNB-PKI's Certification Practice Statement.

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

As specified in DNB-PKI's Certification Practice Statement.

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

As specified in DNB-PKI's Certification Practice Statement.

7.7.4 Installation following a natural disaster or another type of catastrophe

As specified in DNB-PKI's Certification Practice Statement.

7.8 CA or RA Termination

7.8.1 Certification Authority

As specified in DNB-PKI's Certification Practice Statement.

7.8.2 Registration Authority

No stipulation

8. Technical Security Controls

This paragraph describes the technical security controls for issuing certificates under this CP. For other information see DNB-PKI's Certification Practice Statement.

8.1 Key pair Generation and Installation

8.1.1 Key pair generation

As specified in DNB-PKI's Certification Practice Statement.

8.1.2 Delivery of private keys to subscribers

See section *Who can submit a certificate application*

8.1.3 Delivery of the public key to the certificate issuer

The public key is generated by the DNB-PKI Corporate CA and therefore delivery is not applicable.

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

As specified in DNB-PKI's Certification Practice Statement.

8.1.5 Key sizes

The key size for internal user certificates is minimal 2048 bits

8.1.6 Public key generation parameters and quality checks

Component public keys are encoded pursuant to RFC 5280 and PKCS#1. The key generation algorithm is the RSA.

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

As specified in DNB-PKI's Certification Practice Statement.

8.2 Private Key Protection and Cryptographic device Engineering Controls

8.2.1 Cryptographic device standards

As specified in DNB-PKI's Certification Practice Statement.

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

As specified in DNB-PKI's Certification Practice Statement.

8.2.3 Escrow of private keys

As specified in DNB-PKI's Certification Practice Statement.

8.2.4 Private key backup copy

As specified in DNB-PKI's Certification Practice Statement.

8.2.5 Private key archive

The DNB-PKI Corporate CA, once the internal user certificates issuance process has finalized, does not keep a copy of its private key and, therefore, the private key can only be found on the corresponding cryptographic card held by the subscriber.

8.2.6 Private key transfer into or from a cryptographic device

No stipulation.

8.2.7 Private key storage in a cryptographic device

Internal user certificates are stored on the cryptographic device of the DNB company card from the subscriber. This device has at least FIPS 140-2 Level 3 certification.

8.2.8 Private key activation method

For internal user certificates procedures and software is in place to create a key pair. Due to separation of duty one department will create the keys, another department will transfer is to the corresponding DNB company card. When needed for email encryption a separate procedure is available to transfer the keys to the corresponding hardware.

8.2.9 Private key deactivation method

For deactivating the keys of a user the System Administrator, with authorization from two HSM Administrators, shall fulfill this request via existing procedures.

8.2.10 Private key destruction method

As specified in DNB-PKI's Certification Practice Statement.

8.2.11 Cryptographic device classification

As specified in DNB-PKI's Certification Practice Statement.

8.3 Computer Security Controls

8.3.1 Specific security technical requirements

As specified in DNB-PKI's Certification Practice Statement.

8.3.2 Computer security evaluation

As specified in DNB-PKI's Certification Practice Statement.

8.4 Life cycle security controls

As specified in DNB-PKI's Certification Practice Statement.

8.5 Network Security Controls

As specified in DNB-PKI's Certification Practice Statement.

8.6 Time-stamping

As specified in DNB-PKI's Certification Practice Statement.

9. Certificate and CRL Profiles

9.1 Certificate Profile

9.1.1 Version number

Internal user certificates use the X.509 version 3 (X.509 v3) standard.

9.1.2 Certificate extensions

The certificate extensions used generically are as specified in DNB-PKI's Certification Practice Statement. Below are the fields for internal user certificates:

Table authentication certificate profile:

	FIELD	CONTENT	CRITICAL extensions
1	Version	V3	
2	Serial Number	Random	
3	Signature Algorithm	sha256 RSA	

4	Issuer Distinguished Name	CN=DNBNL-CA1
		O=De Nederlandsche Bank N.V.
		C=NL	

5	Lifetime	5 years	

6	Subject	E=<email address>
		CN=<Account number>
		OU=Users
		OU=Divisions
		O=DNB
		C=NL	

7	Subject Public Key Info	Algorithm: RSA Encryption Minimum key length: 2048 (big string)	
8	Key Usage	Digital Signature, Key Encipherment	YES
9	Enhanced Key Usage	Smart Card Logon Client Authentication	

Table secure e-mail certificate profile:

	FIELD	CONTENT	CRITICAL extensions
1	Version	V3	
2	Serial Number	Random	
3	Signature Algorithm	sha256 RSA	

4	Issuer Distinguished Name	CN=DNBNL-CA1
		O=De Nederlandsche Bank N.V.
		C=NL	

5	Lifetime	3 years	

6	Subject	CN=<Account number>
		E=<email address>	

7	Subject Public Key Info	Algorithm: RSA Encryption Minimum key length: 2048 (big string)	
8	Basic Constraints	End Entity	YES
9	Key Usage	Digital Signature, Key Encipherment, Data Encipherment	YES
10	Enhanced Key Usage	Secure Email Client Authentication	

9.1.3 Algorithm Object Identifiers (OID)

As specified in DNB-PKI's Certification Practice Statement.

9.1.4 Name formats

As specified in DNB-PKI's Certification Practice Statement.

9.1.5 Name constraints

As specified in DNB-PKI's Certification Practice Statement.

9.1.6 Certificate Policy Object Identifiers (OID)

As specified in DNB-PKI's Certification Practice Statement.

9.1.7 Use of the "PolicyConstraints" extension

No stipulation.

9.1.8 Syntax and semantics of the “PolicyQualifier

As specified in DNB-PKI's Certification Practice Statement.

9.1.9 Processing semantics for the critical “CertificatePolicy” extension

No stipulation.

9.2 CRL Profile

9.2.1 Version number

As specified in DNB-PKI's Certification Practice Statement.

9.2.2 CRL and extensions

No stipulation.

9.3 OCSP Profile

9.3.1 Version number(s)

As specified in DNB-PKI's Certification Practice Statement.

9.3.2 OCSP Extensions

As specified in DNB-PKI's Certification Practice Statement.

10. Compliance Audits and Other Controls

10.1 Frequency or Circumstances of Controls for each Authority

As specified in DNB-PKI's Certification Practice Statement.

10.2 Identity/Qualifications of the Auditor

As specified in DNB-PKI's Certification Practice Statement.

10.3 Relationship between the Assessor and the Entity being Assessed

As specified in DNB-PKI's Certification Practice Statement.

10.4 Aspects Covered by Controls

As specified in DNB-PKI's Certification Practice Statement.

10.5 Actions Taken as a Result of Deficiencies Found

As specified in DNB-PKI's Certification Practice Statement.

10.6 Notification of the Results

As specified in DNB-PKI's Certification Practice Statement.

11. Other Legal and Business Matters

11.1 Fees

11.1.1 Certificate issuance or renewal fees

No fees are applied for the issue or revocation of certificates under this Certificate Policy.

11.1.2 Certificate access fees

Access to certificates issued under this Policy is free of charge and, therefore, no fee is applicable to them.

11.1.3 Revocation or status information fees

Access to information on the status or revocation of the certificates is open and free of charge and, therefore, no fees are applicable.

11.1.4 Fees for other services, such as policy information

No fee shall be applied for information services on this policy, nor on any additional service that is known at the time of drawing up this document.

11.1.5 Refund policy

Given that there are no fees for this Certificate Policy, no refund policy is required.

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

11.3.1 Scope of confidential information

As specified in DNB-PKI's Certification Practice Statement.

11.3.2 Non-confidential information

As specified in DNB-PKI's Certification Practice Statement.

11.3.3 Duty to maintain professional secrecy

As specified in DNB-PKI's Certification Practice Statement.

11.4 Privacy of Personal Information

11.4.1 Personal data protection policy

As specified in DNB-PKI's Certification Practice Statement.

11.4.2 Information considered private

As specified in DNB-PKI's Certification Practice Statement.

11.4.3 Information not classified as private

As specified in DNB-PKI's Certification Practice Statement.

11.4.4 Responsibility to protect personal data

As specified in DNB-PKI's Certification Practice Statement.

11.4.5 Notification of and consent to the use of personal data

As specified in DNB-PKI's Certification Practice Statement.

11.4.6 Disclosure within legal proceedings

As specified in DNB-PKI's Certification Practice Statement.

11.4.7 Other circumstances in which data may be made public

As specified in DNB-PKI's Certification Practice Statement.

11.5 Intellectual Property Rights

As specified in DNB-PKI's Certification Practice Statement.

11.6 Representations and Warranties

11.6.1 Obligations of the CA

As specified in DNB-PKI's Certification Practice Statement.

11.6.2 Obligations of the RA

As specified in DNB-PKI's Certification Practice Statement.

11.6.3 Obligations of certificate subscribers

As specified in DNB-PKI's Certification Practice Statement.

11.6.4 Obligations of relying parties

As specified in DNB-PKI's Certification Practice Statement.

11.7 Disclaimers of Warranties

11.7.1 DNB-PKI's liabilities

As specified in DNB-PKI's Certification Practice Statement.

11.7.2 Scope of liability coverage

As specified in DNB-PKI's Certification Practice Statement.

11.8 Limitations of Liability

As specified in DNB-PKI's Certification Practice Statement.

11.9 Indemnities

As specified in DNB-PKI's Certification Practice Statement.

11.10 Term and Termination

11.10.1 Term

This CP shall enter into force from the moment it is approved by the Policy Approval Authority and published in the DNB-PKI repository.
This CP 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 DNB-PKI Corporate CA keys, at which time it is mandatory to issue a new version.

11.10.2 CP substitution and termination

This CP shall always be substituted by 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 version of the CP is outdated, the outdated version will be withdrawn from the DNB-PKI public repository, although it will be held for a period of 1 year maximum.

11.10.3 Consequences of termination

The obligations and constraints established under this CP, 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

As specified in DNB-PKI CPS.

11.12 Specification Amendment Procedures

11.12.1 Amendment procedures

As specified in DNB-PKI's Certification Practice Statement.

11.12.2 Notification period and mechanism

As specified in DNB-PKI's Certification Practice Statement.

11.12.3 Circumstances in which the OID must be changed

As specified in DNB-PKI's Certification Practice Statement.

11.13 Disputes and Jurisdiction

As specified in DNB-PKI's Certification Practice Statement.

11.14 Governing Law

As specified in DNB-PKI's Certification Practice Statement.

11.15 Compliance with Applicable Law

As specified in DNB-PKI's Certification Practice Statement.

11.16 Miscellaneous Provisions

11.16.1 Entire agreement clause

As specified in DNB-PKI's Certification Practice Statement.

11.16.2 Independence

Should any of the provisions of this CP 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 CP 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 a 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 a DNB company card that has been blocked after repeatedly and consecutively entering the wrong PIN
RFC	Request For Comments (Standard issued by the IETF)