ING Corporate PKI G3 Internal Certificate Policy

Version 1.0 – March 2018

ING Corporate PKI Service Centre

Document information

Commissioned by

ING Corporate PKI Policy Approval Authority

Additional copies of this document

Can be obtained via the ING Corporate PKI Internet site: https://www.pki.ing.com/

Or requested at:

ING Corporate Crypto team
PO Box 1800
1000 BV Amsterdam
Netherlands
Email: ING.Corporate.Crypto@ing.nl

Document version

Version 1.0 – March 2018

General

The format of this Certificate Policy is based on the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Statement Framework (RFC3647). Unneeded or irrelevant clauses have been removed for optimal readability

This document is publicly available outside ING Group.

Abstract

This Certificate Policy (CP) for the ING Corporate PKI G3 Internal CA contains the rules governing the issuance and use of Certificates for Employees, Devices, Applications and Services of ING as part of the ING Public Key Infrastructure G3 (PKI), in accordance with the applicable ING PKI Certificate Practice Statement (CPS).

Audience

The information contained in this document is intended for all active users of the ING Corporate PKI from the moment of publication.

References

- ETSI TS 102.042 'Policy requirements for certification authorities issuing public key certificates'
- IETF RFC 3647 'Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework'
- ING Public Key Infrastructure G3 Certificate Practice Statement

List of abbreviations

The abbreviations listed in the below table will be used throughout this CP.

Abbreviation	Term
CA	Certification Authority
CN	Common Name
CP	(This) Certificate Policy
CPS	(The associated) Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
ETSI	European Telecommunication Standards Institute
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
OID	Object Identifier
PAA	Policy Approval Authority
PKI	Public Key Infrastructure
RA	Registration Authority
VPN	Virtual Private Network

Index

1 Policy

CPS References	
Overview	CPS 1.1
Identification	CPS 1.2
Administration & contact information	CPS 1.5

1.1 Overview

Under this Certificate Policy (CP), ING Bank N.V. will act as the ING Corporate PKI G3 Internal CA.

Certificates issued by the ING Corporate PKI G3 Internal CA under this CP provide either a medium level of confirmation (via standard certificates with the private key stored as software token) or a high level of confirmation (via enhanced trust certificates with the private key stored in hardware and appropriate issuing procedures) of ING employees as well as ING devices and applications.

The certificates provide a validated link between the identity of an ING device/application or an ING employee and a public key. As a result, where this policy speaks of a device/application as an end-user, this not only refers to the hardware/software but also refers to its representative(s).

Each certificate issued by the ING Corporate PKI G3 Internal CA gives a confirmation of:

- Identity of the end-user named in the certificate
- Status of the end-user as ING employee, ING device or ING application
- (where applicable) Status of the domain name included in the certificate as being in the possession of ING Bank N.V. and/or ING Group.

Level of confirmation (to all relying parties):	Confirmation is provided by:
Medium level confirmation (trustworthy, but no optimal security)	Standard certificates (private key stored as software token; high level of confirmation is never possible)
High level of confirmation (trustworthy, optimal security)	Enhanced trust certificates (private key stored in hardware, appropriate issuing procedures)

1.2 Identification

Policy Name	ING Corporate PKI G3 Internal Certificate Policy
Policy Qualifier	ING Bank NV is the issuer of this certificate. Restrictions may apply to the use - please check the applicable CP and CPS for details. For information, visit www.ing.com/pki or contact the ING Corporate PKI service Centre.
Policy Version	1.0
Policy Status	Final
Policy OID	1.3.6.1.4.1.2787.200.1.6.11
Policy is registered with	Base policy 1.3.6.1.4.1.2787 is registered for ING Group with Joint ISO-ITU standards organization
Date of issue	2018-03-05
Date of expiry	NA

Related CPS	ING Corporate PKI G3 Certification Practice Statement

1.3 Administration & Contact Information

The ING Corporate PKI G3 Internal Certificate Policy is managed by the ING Corporate PKI Policy Approval Authority (PAA). All questions regarding this policy can be addressed to the PAA via email: pki@ing.com.

2 Applicability

CPS References	
PKI Participants	CPS 1.3
End-users	
Registration authorities	
Relying parties	
Certificate usage	CPS 1.4

2.1 End users

Only natural persons who can be considered employees of ING or persons/devices/applications owned, managed or controlled by ING are eligible to apply for certificates issued by the ING Corporate PKI G3 Internal CA.

For certification of devices/applications the ING Corporate PKI G3 Internal CA can only deliver such services with the participation of one or more natural persons representing the certified hardware/software. As a result, where this policy speaks of a device/application as an end-user, this not only refers to the hardware/software but also refers to its representative(s). Under this policy, ING devices/applications can only be represented by employees of ING for certification purposes.

This CP is binding on each end-user that applies for and/or obtains certificates issued by the ING Corporate PKI G3 Internal CA.

2.2 Registration authorities

Only ING entities are eligible as an RA subordinate to the ING Corporate PKI G3 Internal CA. No other entities will be allowed as RA by ING under this policy, unless specifically designated by ING.

2.3 Relying parties

Reliance on certificates issued under this policy is restricted to ING, including its employees, and ING customers. No other parties are allowed to rely on such certificates, unless specifically designated by ING.

It is the relying party's sole responsibility to decide for which communications, including but not limited to transactions, it relies on a certificate issued by the ING Corporate PKI G3 Internal CA, based on its own perception of the trustworthiness of the procedures followed prior to certificate issuance (as described in section 6 of this policy)

2.4 Certificate usage

The certificates issued by the ING Corporate PKI G3 Internal CA are only applicable for use in (secure) electronic communications between:

- ING devices (e.g. servers, routers, VPN hosts, et cetera) and devices of customers of ING,
- ING and third parties (applications, devices and natural persons),
- ING devices among each other,
- ING networks or applications and its employees,
- ING employees and selected ING relations
- ING employees among each other.

Depending on type, each certificate issued by the ING Corporate PKI G3 Internal CA is a high level or medium level confirmation of the end-user's identity and status as an ING employee, ING device or ING application.

Certificates issued by the ING Corporate PKI G3 Internal CA allow the end-user to:

- Identify himself to, and be authenticated by, employees and customers of ING, selected ING networks and applications;
- Send signed messages to ING entities, employees of ING and designated ING relations;
- Receive encrypted messages from ING entities,
- Employees of ING and designated ING relations in order to decrypt these messages;
- Sign transactions and documents;
- Create Transport Layer Security (TLS) or Secure Socket Layer (SSL) connections for confidentiality purposes;
- Enable Virtual Private Network (VPN) applications
- Sign software and code to make it trustworthy for ING internal usage

Cross-certification with CAs operated by other parties than ING is not permitted under this policy.

3 Obligations

CPS References	
Obligations	CPS 2.1
CA obligations	
RA obligations	
End-user obligations	
Relying party obligations	
Repository obligations	CPS fully applies

Obligations as described in the CPS can be altered through applicable contracts.

3.1 CA obligations

The ING Corporate PKI G3 Internal CA, including its operators, shall be obliged to:

- Operate in accordance with this policy and the CPS, as well as with any applicable laws of the governing jurisdiction
- Frequently verify that all its subordinate RAs comply with the relevant provisions of this policy and of the CPS
- Only generate a certificate upon a receipt of a valid certificate issuance approval from an RA

- Publish certificates in the ING PKI repository and maintain certificate information therein, including CRLs.

3.2 RA obligations

Each RA, including its operators, shall be obliged to:

- Validate the identity of end-users in a manner complying with the procedures defined in this CP and in the CPS
- Take all reasonable measures to ensure that end-users are aware of their respective rights and obligations with respect to the use of certificates issued under this CP
- Operate in accordance with this policy and the CPS, as well as with any applicable laws of the governing jurisdiction, and
- Store proof of all checks performed before certificate issuance approval.

3.3 End-user obligations

The obligations of end-users of the ING Corporate PKI G3 Internal CA are exclusively dealt with by this policy.

Each end-user associated with a certificate issued by the ING Corporate PKI G3 Internal CA shall:

- Comply with applicable obligations, procedures and controls in the CP and CPS;
- Use the certificate only insofar it is valid and not revoked to his/her knowledge;
- Immediately report to the end-user's CA in case of any compromise or loss of a private key, or when there is any reason to suspect compromise or loss thereof;
- Immediately report to the end-user's CA in case of any change to the information included in the certificate request or in the certificate;
- Use the certificates, the activation data, the key pairs, and the Software or Hardware Tokens in a normal, responsible and trustworthy manner, taking into account the interest of ING and,
- Withhold of any activities which may endanger or undermine the trustworthiness or continuity of the ING PKI environment, the ING Group and/or the ING entity he/she is employed with.

Each end-user shall be exclusively responsible for monitoring, investigating or confirming the accuracy of the information submitted to the ING Corporate PKI G3 Internal CA as well as the certificate contents. The certificate, the activation data, and the private key, or any software related thereto, are restricted only to be used by the end-user. He/she shall not lease, copy, sell, assign (sub)license, grant any limited rights on, nor make available to any third party the certificate, the activation data, or the private key. As a consequence of the PKI mechanism, the Public Part of the certificate will be made public automatically and can freely be shared.

Intellectual property

As far as ING Bank NV provides the end-user with software and/or database licenses from third parties, the license conditions and guarantees of that third party will apply and the end-user shall act accordingly. The end-user shall follow all reasonable instructions given by ING Bank NV with regard to the use of the intellectual property rights applicable to the certificate, the activation data, and the private key, or any related software.

Enforcement of these obligations

Breach of this code will result in measures by management of the end-user. Such measures will be based on the employment contract or similar contractual relationship between the end-user and ING and could ultimately result in termination of the employment agreement or similar contractual relationship, notwithstanding any other legal measures ING could take under applicable law.

Applicability of other codes

End-users are legally bound to the rules and regulations as stated in the ING Orange Code and any other local ING General Code of Conduct if available

3.4 Relying Party obligations

Under this policy, all relying parties shall be obliged to:

- Verify certificates in accordance with the certification path validation procedure specified in ITU-T Rec. X.509:1997 | ISO/IEC 9594-8 (1997), taking into consideration any critical extensions; and,
- Trust a certificate issued by the ING Corporate PKI G3 Internal CA only if the certificate has not expired or been revoked, and only if a proper chain of trust can be established to the ING Corporate PKI G3 Root CA.

4 Liability

CPS References	
Liability	CPS 2.2
CA liability	
RA liability	
Financial responsibility	CPS 2.3
Interpretation and enforcement (Governing law, Force majeure)	CPS 2.4

4.1 CA liability

ING Bank N.V. shall not be liable for any (financial) damages as a result of the property damages (‘vermogensschade’) and/or any purely financial damages (‘zuivere vermogensschade’), which shall include, without limitation, damages due to late delivery, loss of or damage to data, loss of profits or income, incurred by customers or by other parties.

ING Bank N.V. shall not be liable for the content of communication and/or transactions initiated by customers, employees or by other parties, nor for any damages resulting from use of the certificate not permitted under this policy or in the CPS. ING accepts no liability for loss of data, including certificates, or for the inability to use the ING Corporate PKI G3 due to a defect in or failure to function of telecommunications or data communications facilities, regardless of the manner in which the transmission takes place.

4.2 RA liability

ING Bank N.V. does not accept any liability for ING entities functioning as an RA subordinate to the ING Corporate PKI G3 Internal CA. Insofar damages have been incurred by any party as a result of the performance of an RA of the ING Corporate PKI G3 Internal CA, such incidents will be covered as part of the CA liability as defined and restricted in 4.1.

4.3 Financial responsibility

In no event shall the aggregate and cumulative liability of ING Bank N.V. exceed the amount of € 1.000.000,- (one million euros) per incident.

4.4 Interpretation and enforcement

Governing law
The construction, validity, interpretation, enforceability and performance of this policy are governed by the laws of The Netherlands.

In case of a dispute regarding the ING Corporate PKI G3 Internal CA or certificates issued by it, ING Bank NV shall use its best efforts to negotiate such a dispute in good faith and to settle it amicably. If such negotiations fail to resolve the dispute within two weeks, either party shall be entitled to submit the dispute to arbitrage in accordance with the rules of The Netherlands Arbitration Institute. The language of the proceedings shall be English. Neither party shall be restricted in its right to seek immediate injunctive relief ('voorlopige voorzieningen') in summary proceedings ('kort geding') if it deems such necessary.

Force majeure
Not applicable

5 Confidentiality

CPS References	
Confidentiality	CPS 2.8

Insofar personal data is collected during the registration phase, it is kept confidential and handled in full compliance with applicable data protection legislation. The Privacy Statement of ING Bank N.V. applies to all ING Corporate PKI activities, including those of the ING Corporate PKI G3 Internal CA.

6 Identification & authentication

CPS References	
Identification & authentication	CPS 3.1
Types of names	

6.1 Identity validation

Before a certificate is being issued by the ING Corporate PKI G3 Internal CA, the identity of the end-user is validated by a subordinate RA. This validation will require:

- Evidence of either:
  - The end-user's status as an employee of ING, either through a review of credentials submitted by the end-user or by referencing an ING information system such as an up to date human resource database.
    Requirements on the information (systems) supplying the evidence of the end-user's

    status as an employee of ING will be described in the appropriate procedures for certificate requests.
    - the status of the device to be certified as being owned, managed or controlled by ING, either through a review of credentials submitted by the end-user, or by referencing an internal or external information system such as an up to date database
- Evidence of the authority of the representative to request a certificate on behalf of the end-user

‘Derived’ registration is possible in that the end-user has either been pre-registered with the ING, or has already registered with a third party information system – trusted for the purpose of identity validation – but only insofar the preceding registration procedure complies with the requirements of this policy.

Credentials to be supplied by the end-user and identification and authentication requirements will be described in the appropriate procedures for certificate requests.

Names to be registered for certificates need to be meaningful, in so far that names are to be tracked back to the subscriber.

6.2 Types of names

CAs, RAs and end-users will be certified using a recognizable and unique X.500 Distinguished Name (DN) in the certificate ’Subject name’ field, in accordance with RFC6818. The DN will be in the form of a ’printableString, utf8String’ and is never to be left blank.

Each DN is constructed conform the Corporate Directory Service structure or the appropriate Active Directory Domain structure.

If an end-user’s email address should be stored, then the location should be an rfc822 Name type in the SubjectAlternateName field.

For a VPN/TLS/SSL certificate at least one SubjectAlternateName-DNS field must be filled during the request process and should preferably match the CN.

7 Certificate application, issuance, and acceptance

CPS References	
Certificate application, issuance and acceptance	CPS 4.1
Certificate application procedure	
Certificate issuance & delivery	
Certificate acceptance	

7.1 Certificate application procedure

Each request for a certificate to be issued by the ING Corporate PKI G3 Internal CA must at least contain the following procedural steps:

- Submitting proof of the identity and status of the end-user in accordance with section 6 of this policy;
- Submitting proof of private key possession by the end-user;
- Storing evidence with regard to all validation procedures performed by the RA.

7.2 Certificate issuance & delivery

Only after successful identification and authentication of an end-user, in accordance with sections 6 and 7 of this policy, the ING Corporate PKI G3 Internal CA will:

- Generate a certificate using the contents of the certificate application;
- Verify the possession of a private key by the end-user;
- Distribute the certificate;
- Provide activation data and instructions for the collection and/or acceptance of a certificate;
- Archive encryption keys, if Escrow is required.

Certificates will be delivered directly to the end-user separate from any required activation data.

Once the ING Corporate PKI G3 Internal CA has issued a certificate, it is immediately offered for publication in the ING PKI repository.

7.3 Certificate acceptance

The end-user shall explicitly accept the certificate requested by him. By accepting a certificate, the end-user certifies that to his or her knowledge:

- No unauthorised person has ever had access to the private key corresponding to the public key contained in the certificate;
- No unauthorised person has ever had access to activation data;
- All information contained in the certificate is correct and up to date;
- The certificate is functioning properly with the certified device or application (if applicable).

8 Certificate & CRL profiles

CPS References	
Certificate & CRL profile	CPS 7.1
Name forms and constraints	

Certificates issued under this CP will have the following set of properties, in addition to the stipulations in the CPS:

- Certificate policy object identifier: see Policy OID in ‘Identification’ (section 1)
- Key usage: limited to the described certificate usage in section 2.4.

Name forms and constraints

The use of name fields is in accordance with section 6.

9 Administration procedures

CPS References	
Administration procedures	CPS 8 fully applies to this policy as well.

The end-user shall be notified by the RA about:

- Issuance of the certificate
- Suspension of the certificate
- Revocation of the certificate
- Expiring of the certificate

insofar the notification has not already originated from the actual operation of the RA.

Administrative procedures as described in the CPS apply to this policy as well.