ING Corporate PKI G3 Public 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	This Certificate Policy (CP) for the ING Corporate PKI G3 Public 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 (PKI), in accordance with the applicable ING PKI Certificate Practice Statement (CPS). This document is publicly available outside ING Group.
Abstract	This Certificate Policy for the ING Corporate PKI G3 Public CA (CP) contains the rules governing the issuance and use of certificates among customers participating in the ING Public Key Infrastructure (PKI), in accordance with the ING Corporate PKI G3 Certification 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
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

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 Public CA.

Certificates issued by the ING Corporate PKI G3 Public CA under this CP provide standard trust and are only applicable for use in electronic communications between ING and its customers (e.g. natural persons, devices and/or applications) and provide a validated link between the identity of a customer (e.g. natural person, device or application) 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).

Private Keys associated with certificates issued by the ING Corporate PKI G3 Public CA can either be stored as a hardware or as a software token. In case a private key is stored in hardware, its certificate gives a high level of assurance to all Relying Parties. In case a private key is stored as a software token, its certificate gives a medium level of assurance to all Relying Parties. Under this policy, private keys stored as software tokens can never result in a high level of assurance.

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

- the identity of the end-entity named in the certificate
- the status of the end-entity as an employee of the customer
- the status of the end-entity as a device or application owned, controlled or managed by a customer of ING, and
- where applicable, the status of the domain name included in the certificate as being in the possession of a customer of ING Bank N.V.

1.2 Identification

Policy Name	ING Corporate PKI G3 Public 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	1.3.6.1.4.1.2787.200.1.6.12
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 Public 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	
Relying parties	
Certificate usage	CPS 1.4

2.1 End-users

Only customers of ING are eligible to have their employees apply for certificates issued by the ING Corporate PKI G3 Public CA. Under this policy, no certificates will be issued to natural persons who do not qualify as an employee of an ING customer nor to any other persons or entities.

For certification of devices the ING Corporate PKI G3 Public CA can only deliver such services with the participation of one or more natural persons representing the certified hardware. As a result, where this policy speaks of a device as an end-user, this not only refers to the hardware but also refers to its representative(s). Under this policy, customer devices can only be represented by employees of ING customers for certification purposes. Only customers of ING are eligible to have their employees apply for certificates issued by the ING Corporate PKI G3 Public CA.

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

2.2 Relying parties

Reliance on certificates issued under this policy is restricted to ING only. No other parties are allowed to rely on such certificates.

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 Public 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)

2.3 Certificate usage

The certificates issued under this policy are only and exclusively allowed for use in electronic communications between customers and ING, including devices and applications.

Depending on type, each certificate issued by the ING Corporate PKI G3 Public CA is a confirmation of the end-user's identity and status as an employee of a customer of ING, and allows the end-user to:

- Identify him/itself to, and be authenticated by, employees of ING, ING networks and ING applications;
- Send signed messages to selected ING employees, ING entities or entity departments;

- Receive encrypted messages from selected ING employees, ING entities or entity departments in order to decrypt these messages;
- Sign transactions and documents;
- Make use of Virtual Private Network (VPN) applications;
- Create Transport Layer Security (TLS) or Secure Socket Layer (SSL) connections for confidentiality purposes;
- Enable Virtual Private Network (VPN) applications as agreed upon by separate agreement with one of the ING entities.

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

Natural persons
The obligations of the ING Corporate PKI G3 Public CA regarding Natural Persons are exclusively dealt with by the Terms, as well as by the CPS. No additional stipulations are made by this CP.

Non-personal devices
The ING Corporate PKI G3 Public 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

Natural persons
The obligations of RAs that are subordinate to the ING PKI G3 Public CA are exclusively dealt with by the CPS. No additional stipulations are made by this CP.

Non-personal devices
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 policy 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 policy
- 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 Public CA are exclusively dealt with by the CPS.

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.

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 Public 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 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 PKI 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. Additional stipulations can - if applicable - be made by the Terms & Conditions.

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 Public CA. Insofar damages have been incurred by customers or by other parties as a result of the performance of an RA of the ING Corporate PKI G3 Public 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.

No additional stipulations are made by this CP.

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 Public 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 Public CA, the identity of the end-user is properly validated by the customer's RA. The validation of the application request will require evidence of the end-user's status as an employee of the customer, either through a review of credentials submitted by the end-user or by referencing an information system such as an up to date human resource database.

'Derived' registration is possible in that the end-user has either been pre-registered with the ING or customer, 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.

Requirements on the information (systems) supplying the evidence of the end-user's status as a customer of ING will be described in the appropriate procedures for certificate requests.

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.

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 Public 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 Public 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 Public 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.