ING Public Key Infrastructure Customer Certificate Policy

Version 5.4 - November 2015

ING

Colophon

Commissioned by	ING PKI Policy Approval Authority (PAA)
Additional copies	Additional copies of this document can be obtained via the ING internet site www.ing.com/pki or by mail: pki@ing.com.
Document version	Version 5.4 - November 2015
General	This document is publicly available outside ING Group.
Abstract	This Certificate Policy (CP) for the ING PKI Customer CA 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 PKI Certification Practice Statement (CPS).
Audience	The information contained in this document is intended for all users of the ING Corporate PKI.
References	• ING PKI Certificate Practice Statement • ING PKI Certificate Policy Root CA • ING PKI Employee Certificate Policy • ING PKI Technical Certificate Policy • ANSI X9.79 7.1 • ETSI 102.042

Contents

1. Overview

See ING PKI Certificate Practice Statement, § 1.1.

Under this Policy, ING Bank N.V. will act as the ING PKI Customer CA.

The ING PKI and the associated rules, regulations and procedures are based on ETSI 102.042.

The Certificates that are issued by the ING PKI Customer CA 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.

Customer Certificates can be issued to natural persons, organisational identities and to non-personal devices (e.g technical certificates for ING Customers).

Private Keys associated with Certificates issued by the ING PKI Customer CA can either be stored on a Smart Card or as a Software Token. In case a Private Key is stored on a Smart Card, 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 PKI Customer CA gives a confirmation of:

- the identity of the End-User named in the Certificate
- the status of the End-User as an Employee of the Customer
- the status of the End-User 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.

When the ING Customer CA 2005 restricts its certification services to non-personal devices (e.g. technical certificates for ING Customers), it can only deliver such services with the participation of one or more natural persons representing the certified hardware. As a result, in such cases where this Policy speaks of 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 PKI Customer 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.

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

Cross-certification with CA's operated by other parties then ING is not permitted under this Policy.

1.1. Definition of Terms

See ING PKI Certificate Practice Statement, § 1.2.

The definitions of terms used in this Policy are determined by the ING PKI Glossary.

1.2. Identification

See ING PKI Certificate Practice Statement, § 1.3.

Policy Name	ING PKI Customer Certificate Policy
Policy Qualifier	ING Bank N.V. is the issuer of this certificate. Restrictions may apply to its use; please check the applicable CP and CPS for details. For information, contact www.ing.com/pki or pki@ing.com
Policy Version	5.4
Policy Status	Final
Policy Ref/OID Medium Level of Assurance	1.3.6.1.4.1.2787.200.1.6.3.50
Policy Ref/OID High Level of Assurance	1.3.6.1.4.1.2787.200.1.6.3.70
Policy Ref/OID High Level (non-Repudiation) of Assurance	1.3.6.1.4.1.2787.200.1.6.3.71
Date of Issue	November 9th 2015
Date of Expiry	na
Related CPS	ING PKI Certificate Practice Statement

1.3. Administration & Contact Information

See ING PKI Certificate Practice Statement, § 1.6.

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

2. Applicability

See ING PKI Certificate Practice Statement, § 1.4, 1.5.

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 PKI Customer CA is a high or medium level 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
- make use of Virtual Private Network (VPN) applications,
- create Secure Socket Layer (SSL) connections for confidentiality purposes, and
- enable Virtual Private Network (VPN) applications as agreed upon by separate agreement with one of the ING entities.

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 PKI Technical 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).

This Policy is binding on each End-User that applies for and/or obtains Certificates issued by the ING PKI Customer CA, by virtue of the Terms and Conditions ING PKI Customer CA (hereafter to be referred to as 'the Terms').

3. Obligations

See ING PKI Certificate Practice Statement, § 2.1.

3.1. CA Obligations

See ING PKI Certificate Practice Statement, § 2.1.1.

3.1.1 Natural Persons
The obligations of the ING PKI Customer CA regarding Natural Persons are exclusively dealt with by the Terms, as well as by the ING PKI Certification Practice Statement. No additional stipulations are made by this CP.

3.1.2 Non-Personal Devices
The ING PKI Customer CA, including its Operators, shall be obliged to:

- operate in accordance with this Policy and the ING PKI 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 ING PKI CPS
- only generate a Certificate upon a receipt of a valid Certificate issuance approval from an RA
- securely distribute Activation Data and Private Keys to its End-Users, and
- publish Certificates in the ING PKI Repository and maintain Certificate information therein, including CRL's.

3.2. RA Obligations

See ING PKI Certificate Practice Statement, § 2.1.2.

3.2.1 Natural Persons
The obligations of RAs that are subordinate to the ING PKI Customer CA are exclusively dealt with by the Terms, as well as by the ING PKI Certification Practice Statement. No additional stipulations are made by this CP.

3.2.2 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 ING PKI 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 ING PKI 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

ING PKI Certificate Practice Statement § 2.1.3.

The obligations of End-Users of the ING PKI Customer CA are exclusively dealt with by the Terms, as well as by the ING PKI Certificate Practice Statement. No additional stipulations are made by this CP.

3.4. Relying Party Obligations

See ING PKI Certificate Practice Statement, § 2.1.4.

All persons or entities acting as Relying Parties under this Policy 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 PKI Technical CA only if the Certificate has not been expired, suspended or revoked, and only if a proper chain of trust can be established to the ING PKI Root CA.

3.5. Repository Obligations

See ING PKI Certificate Practice Statement, § 2.1.5.

All obligations regarding the ING PKI Repository are exclusively dealt with by the ING PKI Certification Practice Statement. No additional stipulations are made by this CP.

4. Liability

See ING PKI Certificate Practice Statement, § 2.2.

4.1. CA Liability

See ING PKI Certificate Practice Statement, § 2.2.1.

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. In no event shall the aggregate and cumulative liability of ING Bank N.V. exceed the amount of EUR 1,000,000 (one million euros) per incident.

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 ING PKI 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

See ING PKI Certificate Practice Statement, § 2.2.2.

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

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

4.3. Governing Law

See ING PKI Certificate Practice Statement, § 2.4.1.

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

Disputes are exclusively dealt with by the Terms. No additional stipulations are made by this CP.

5. Confidentiality

See ING PKI Certificate Practice Statement, § 2.8.

All Customer information obtained during the registration phase is kept confidential and handled in full compliance with applicable data protection legislation. The ING PKI Privacy Statement applies to all ING PKI activities, including those of the ING PKI Customer CA.

6. Identification & Authentication

See ING PKI Certificate Practice Statement, § 3.1.

Before a Certificate is being issued by the ING PKI Customer 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.

7. Certificate Application Procedure

See ING PKI Certificate Practice Statement, § 4.1.

Each request for a Certificate to be issued by the ING PKI Customer CA must at least contain the following procedural steps:

- submitting proof of the identity and Employee status of the End-User in accordance with section 6 of this Policy
- submitting proof of Private Key possession by the End-User, in case of key pair generation by the applicant, and
- storing evidence by the RA with regard to all performed identification and authentication procedures.

8. Certificate Issuance & Delivery

See ING PKI Certificate Practice Statement, § 4.2.

Only after successful identification and authentication of an End-User, in accordance with sections 6 and 7 of this Policy, the ING PKI Customer CA will:

- generate a Certificate using the contents of the Certificate Application
- generate a corresponding Public and Private Key in case of Key Pair generation by the ING PKI Customer CA, or verify the possession of a Private Key in case of Key Pair generation by the End-User
- securely distribute the Certificate and, in case of Key Pair generation by the ING PKI Customer CA, the associated Private Key to the End-User, and
- provide Activation Data and instructions for the collection and/or acceptance of a Certificate.

Certificates and/or Private Keys will be delivered directly to the End-User separate from any required Activation Data. In case of Key Pair generation by the ING PKI Customer CA, the Private Key will be securely distributed to the End-User in a manner separated from the distribution of Activation Data.

When a Certificate is stored on a Smart Card, the Smart Card will be delivered to the End-User in initial suspended mode. Acceptance of the Certificate will result in un-suspension of the Smart Card.

Once the ING PKI Customer CA has issued a Certificate, it is immediately offered for publication in the ING PKI Repository.

9. Certificate Acceptance

See ING PKI Certificate Practice Statement, § 4.3.

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, and
- all information contained in the Certificate is correct and up to date.

Acceptance of the Certificate will result in un-suspension of the Smart Card.
Usage of a Certificate by the End-User implies his Acceptance of the Certificate contents.

10. Administrative Procedures

See ING PKI Certificate Practice Statement, § 8.

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 is not a part of the actual operation of the RA.

Administrative procedures as described in the ING PKI CPS apply to this Policy as well

More information

For more information
please visit
www.ing.com/pki
or mail to pki@ing.com

ING