ING Public Key Infrastructure

Terms & Conditions ING Customer Group Mailbox Encryption Certificate

Version 5.4 - November 2015

1. General

These Terms & Conditions are applicable to the ING Customer Group Mailbox Encryption Certificates issued by the ING Corporate PKI.

In addition to the above, the ING PKI Customer Certificate Policy (CCP) and the ING PKI Certificate Practice Statement (CPS) shall apply. Users of an ING Customer Group Mailbox Encryption Certificate are expected to have knowledge of the contents of these documents. ING will supply these documents when an application is made for an ING Customer Group Mailbox Encryption Certificate. The documents can also be found at www.ing.com/pki and/or applied for at the ING PKI Service Centre (see the information sheet on the second page of these Terms & Conditions).

ING Bank NV acts as the supplier of the ING Customer Group Mailbox Encryption Certificate.

To clarify the position of the ING Corporate PKI, this text uses the term "ING Corporate PKI" where, from a legal point of view, ING Bank NV is meant in its capacity as supplier of the ING Corporate PKI.

2. Target audience and use

ING Customer Group Mailbox Encryption Certificates are exclusively intended to be used for the purpose of securing electronic communication with ING.

3. Restrictions

The use of the ING Customer Group Mailbox Encryption Certificate is restricted to the purpose for which the certificate was requested. Acquisition of a certificate in no way implies the direct or indirect acquisition of any power of attorney from ING.

Any use of an ING Customer Group Mailbox Encryption Certificate other than as described above is prohibited. Any such use shall not result in any commitment or liability of ING Corporate PKI.

4. Related documents

The ING PKI Glossary, the ING PKI Customer Certificate Policy (CCP), the ING PKI Certificate Practice Statement (CPS) and the ING PKI Privacy Statement make an integrated whole with these Terms & Conditions.

The ING PKI Service Centre reserves the right to change these documents according to the procedure laid down in the ING PKI CPS.

4.1. Document hierarchy

In the event of inconsistency between the documents, the following ranking shall apply:

1. ING PKI Terms & Conditions ING I-Dentity Card
2. ING PKI Glossary
3. ING PKI Customer Certificate Policy
4. ING PKI Certificate Practice Statement
5. ING PKI Privacy Statement

5. Obligations

5.1. ING Corporate PKI

The ING Corporate PKI shall:

1. manage the personal data of the applicant/user of an ING Customer Group Mailbox Encryption Certificate in confidence in accordance with the applicable legislation and shall store the data in compliance with the terms as determined in the applicable legislation
2. manage the event logs in accordance with the applicable legislation and shall store the event logs in compliance with the terms as determined in the applicable legislation.

5.2. Applicant/user

Every applicant/user of an ING Customer Group Mailbox Encryption Certificate shall:

1. provide the ING Corporate PKI with accurate and complete information only, in all actions relating to the ING Customer Group Mailbox Encryption Certificate
2. act in accordance with the obligations, procedures and rules as laid down in the ING PKI Customer Certificate Policy and the ING PKI Certificate Practice Statement
3. only use the ING Customer Group Mailbox Encryption Certificate when valid and has not – insofar as he/she reasonably can be expected to know – been revoked
4. immediately inform the issuer in the event of (any suspicion of) abuse or the ING Customer Group Mailbox Encryption Certificate and/or the accompanying password, so the validity of the certificate can be revoked
5. immediately inform the issuer of any changes to the data (that were) relevant to the application for the ING Customer Group Mailbox Encryption Certificate
6. use, manage and store the ING Customer Group Mailbox Encryption Certificate and the password supplied in a careful, responsible and reliable manner, which includes the obligation to keep the password secret, so that unauthorised use of the ING Customer Group Mailbox Encryption Certificate can in all reasonableness be ruled out
7. perform no actions which endangers the confidentiality or continuity of the ING Corporate PKI, the ING Business Units or the ING Group.

5.3. Trusting Third Party

Any party wishing to put trust in an ING Customer Group Mailbox Encryption Certificate shall:

1. check the ING Customer Group Mailbox Encryption Certificate in order to validate if the ING Customer Group Mailbox Encryption Certificate has actual been issued by ING Corporate PKI
2. check the ING Customer Group Mailbox Encryption Certificate in order to verify the validity with regard to date of issue and expiry date
3. check the ING Customer Group Mailbox Encryption Certificate in order to verify the validity with regard to suspension and/or revocation (see §6).

6. Validation

Validation of the ING Customer Group Mailbox Encryption Certificate is done via CRL (Certificate Revocation List) checking. The physical location of the CRL belonging to the ING Customer Group Mailbox Encryption Certificates is published in the certificate.

7. Liability

The ING Corporate PKI shall not be liable for any direct or indirect (financial) damage as a result of the use of the ING Customer Group Mailbox Encryption Certificates. This includes property damage ("vermogensschade") and/or any purely financial damage ("zuivere vermogensschade"), including and without limitation consequential damage, damage caused by late delivery, loss of profits or income, lost savings, loss of or damage to (corporate) data and/or damage resulting from business stagnation by ING companies and/or ING customers. In no event shall the aggregate and cumulative liability of the ING Corporate PKI exceed the sum of € 100,000 (one hundred thousand euro's) per occurrence whereby related occurrences will be treated as one single occurrence.

The ING Corporate PKI shall not be liable for the content of any communication and/or transaction initiated by ING companies, ING customers and/or any other party, nor for any damages as a result of the use of ING Customer Group Mailbox Encryption Certificates not covered by these Terms & Conditions, the related Policy and/or Certificate Practice Statement.

The ING Corporate PKI shall not be liable for the loss of data, including certificates, or for the unavailability of the ING Corporate PKI as a result of a malfunction or calamity in the functioning of telecommunication companies and/or data communication facilities, regardless of the way in which the transmission is established.

8. Applicable law

Dutch law is applicable to the ING Corporate PKI and related documents.

9. Disputes

Disputes relating to the ING Corporate PKI will be referred to the competent court in Amsterdam, without reservation of the parties' right to lodge an appeal and/or appeal to the court of cassation.

10. Quality Level Standard

The ING Corporate PKI is build conform the ETSI 102.042 standard. More information on ETSI can be found at www.etsi.org.

Contact

ING PKI Service Centre6
PO Box 1800
1000 BV Amsterdam
Netherlands
e-Mail: pki@ing.com