ING Public Key Infrastructure G3 Certificate Practice Statement

Version 1.0 – December 2017

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 PKI Service Centre Location HBP F.01.084 PO Box 1800 1000 BV Amsterdam Netherlands e-Mail: pki@ing.com
Document version	Version 1.0 – December 2017
General	The format of this CPS 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 Practice Statement (CPS) contains the processes and procedures governing all certification services within the ING Corporate PKI G3, in accordance with the applicable Certificate Policies.
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 Corporate PKI Root G3 Certificate Policy • ING Corporate PKI Internal G3 Certificate Policy • ING Corporate PKI Public G3 Certificate Policy

List of abbreviations

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

Abbreviation	Term
CA	Certification Authority
CAO	Certification Authority Officer
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
ETSI	European Telecommunication Standards Institute
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
OID	Object Identifier
PAA	Policy Approval Authority
PKI	Public Key Infrastructure
PKCS	Public Key Cryptographic Standards.
PSC	PKI Service Centre
RA	Registration Authority

Index

1 Introduction

1.1 Overview

The Global ING Corporate Private Key Infrastructure (PKI) consists of two separate, independent certificate hierarchies: the ING Corporate PKI 2005 (with a SHA1-based root certificate) and the ING Corporate PKI G3

This Certification Practice Statement (CPS) contains the processes and procedures governing all certification services relating to the ING Corporate PKI G3. In addition, the services offered within the ING Corporate PKI G3 are governed by the following set of Certificate Policies (CP):

- ING Corporate PKI Root G3 CP
- ING Corporate PKI Internal G3 CP
- ING Corporate PKI Public G3 CP

The ING Corporate PKI G3 CPs and the ING Corporate PKI G3 CPS are publicly available and can be obtained via www.ing.com/pki or the ING Corporate PKI Service Centre (Information Sheet, page 2). The ING Corporate PKI G3 and the associated rules, regulations and procedures are based on ETSI TS 102.042.

For interpretation of this CPS, a basic knowledge of PKI and its related services is presumed. Readers without such basic knowledge are advised to get acquainted with PKI in general and the underlying services in particular before making use of or putting reliance on certificates issued within the ING Corporate PKI G3.

All ING Corporate PKI G3 services defined in this CPS are delivered and managed by ING Bank NV. For contacting ING Bank NV about the ING PKI services, please use the following details:

URL	www.ing.com/pki
Email	pki@ing.com
Postal address	ING Corporate PKI Service Centre Location Code HBP F.01.084 PO Box 1800 1000 BV Amsterdam the Netherlands
24/7 Suspension Service telephone number	+31.88.464.2224 (ACCI - Alarm & Communications Center ING)

1.2 Identification

The following table provides the details of the ING Corporate PKI G3 CPS:

Policy Name	ING Corporate PKI G3 Certification Practice Statement
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, contact www.ing.com/pki or the ING Corporate PKI service Centre (Information Sheet, page 2)
Policy Version	0.1
Policy Status	Draft
Policy OID	1.3.6.1.4.1.2787.200.1.6.10
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	2017-02-14

Date of expiry	NA

1.3 PKI participants

Certification Authorities (CA)

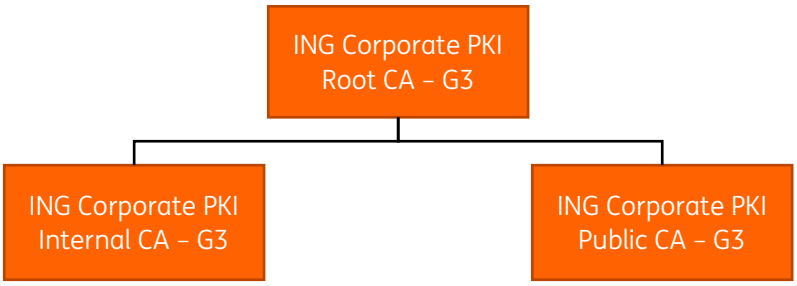
Within the ING Corporate PKI G3, the following Certification Authorities (CAs) exist:

- ING Corporate PKI G3 Root CA
- ING Corporate PKI G3 Internal CA
- ING Corporate PKI G3 Public CA

Each CA is authorised to create, sign, issue, manage and validate certificates within the terms made by its respective CP as well as this CPS. CAs are operated and managed by one or more CA operators (CAO).

The CAs responsible for the issuance of a certificate within the ING Corporate PKI G3 are (technically) identified by the following names:

- ING Corporate PKI G3 Root CA = "ING Corporate PKI Root CA - G3"
- ING Corporate PKI G3 Internal CA = "ING Corporate PKI Internal CA – G3"
- ING Corporate PKI G3 Public CA = "ING Corporate PKI Public CA – G3"



Registration Authorities (RA)

Within the ING Corporate PKI G3, a Registration Authority (RA) is responsible for authentication and registration of end-users. Only ING entities or parties specifically designated by ING are allowed to operate as an RA under this CPS - no other parties are allowed. RAs are represented, operated and managed by one or more trusted registrars. Only under strict conditions parties can be specifically designated by ING to operate as a RA under this CPS.

Repositories

All certificates that are issued within the ING Corporate PKI G3 are stored within the ING Corporate PKI G3 Repository. The ING Corporate PKI G3 Repository may be comprised of different systems operated and managed on different locations, and is wholly owned and supervised by ING Bank NV. CRLs are published at both the intranet and the internet, the specific CDPs are to be found in the certificates.

End-users

The following end-users are recognized within the ING Corporate PKI G3:

CA	End-User
ING Corporate PKI G3 Root CA	ING Corporate PKI CAs subordinate to this Root
ING Corporate PKI G3 Internal CA	Employees, Devices,Applications and Services of ING
ING Corporate PKI G3 Public CA	Customers of ING, including their devices and applications

This CPS is binding on each end-user and governs each end-user's performance with respect to the request for and usage of certificates.

Relying Parties

Reliance on certificates issued within the ING Corporate PKI G3 is restricted to the following parties:

Certificate	Relying Parties
Root certificate	All end-user entities
Internal certificate	All end-user entities
Public certificate	ING end-user entities only

This CPS is binding on each Relying Party, as well as the applicable CP. Unauthorized reliance on certificates issued within the ING Corporate PKI G3 is not accepted nor approved by ING Bank NV and does not make ING Bank NV responsible nor liable for such reliance in whatever manner.

1.4 Certificate usage

Depending on the type of certificate and the application, certificates issued within the ING Corporate PKI G3 will allow the end-user to perform any or all of the following actions:

- Identify himself to, and be authenticated by a person, network, device or application;
- Electronically sign data and let this signature be validated by a person, network, device or application;
- Encrypt data (ao messages, files, transactions);
- Decrypt encrypted data (ao messages, files, transactions);
- Establish secure communication channels through TLS (Transport Layer Security) connections for confidentiality purposes;
- Enable or make use of applications and/or services through VPN (Virtual Private Network).

Depending on the type of certificate and the application, ING Bank NV reserves the right to limit or restrict the usage of, and/or reliance on certain certificate functions. Any other usage of certificates issued by the ING Corporate PKI G3 is not allowed by ING Bank NV.

1.5 Policy administration

This CPS is managed by the ING Corporate PKI Policy Approval Authority (PAA). All questions regarding this CPS can be addressed to the ING Corporate PKI PAA via the ING Corporate PKI Service Centre (Information Sheet, page 2).

2 General Provisions

2.1 Obligations

This section contains the provisions applicable to the entities within the ING Corporate PKI G3.

CA Obligations

Each CA within the ING Corporate PKI G3, including its CA operators, shall be obliged to:

- Operate in full accordance with this CPS and the applicable CP, as well as with any applicable laws of the governing jurisdiction;
- Frequently verify that its RAs comply with the relevant provisions of the CPS and the applicable CP; and,
- Maintain an overview of all certificates in the ING PKI Repository and maintain certificate status information in a manner accessible to all Relying Parties.

The abovementioned obligations do not constitute the entire obligations for a CA within the ING Corporate PKI. Additional obligations may apply through this CPS or the applicable CP.

RA Obligations

Each entity acting as an RA within the ING Corporate PKI G3, including its trusted registrars shall be obliged to:

- Operate in full accordance with this CPS and the applicable CP, as well as with any applicable laws of the governing jurisdiction;
- 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 CPS and the applicable CP;
- Inform the CA as soon as possible about any formal change that has been made to any information included in the certificate; and,
- Immediately notify the CA in case a private key is compromised or lost, or when sufficient reason exists to presume that compromise or loss has taken place.

The abovementioned obligations do not constitute the entire obligations for an RA within the ING Corporate PKI G3. Additional obligations may apply through this CPS or the applicable CP.

End-User Obligations

An end-user who is issued a certificate within the ING Corporate PKI G3 shall be obliged to:

- Operate in accordance with the CPS and the applicable CP, as well as with any applicable laws of the governing jurisdiction;
- Inform the CA as soon as a change has been made to any information included in the certificate;
- Immediately notify the 24/7 Suspension Service (ACCI) in case the certificate is compromised or lost, or when reason exists to presume that the certificate or the related key material has been compromised or lost;
- Only use his certificates by himself and/or on his own behalf;
- Adequately ensure the confidentiality, safety and integrity of activation data and private keys;
- Immediately terminate any use of a key pair once its certificate has been revoked; and,
- Continue to safeguard the private key associated with a suspended or revoked certificate.

The abovementioned obligations do not constitute the entire obligations for an end-user within the ING Corporate PKI G3. Additional obligations may apply through this CPS or the applicable CP.

Relying Party obligations

All persons or entities authorized to act as a Relying Party under this CPS 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 only if the certificate has not expired, been suspended or been revoked, and only if a proper chain of trust can be established to the ING Corporate PKI Root CA – G3.

All persons or entities that are not authorized to act as a Relying Party under this CPS shall not put any trust whatsoever in a certificate issued within the ING Corporate PKI G3.

Repository Obligations

All CAs within the ING Corporate PKI G3 shall store the certificates issued under this CPS, as well as relevant certificate information such as CRLs, in the ING Corporate PKI Repository. In doing so, each CA shall use reasonably commercial efforts to maintain and keep the ING Corporate PKI Repository up-to-date.

2.2 Liability

Any liabilities regarding the CA's and RA's operating within the ING Corporate PKI G3 are exclusively dealt with by the applicable CP. No additional stipulations are made by this CPS.

2.3 Financial responsibility

Indemnification by relying parties and end-users

Any indemnifications to be made by relying parties or end-users are -if made- exclusively dealt with by the applicable CP. No additional stipulations are made by this CPS.

Fiduciary relationships

By appointing end-users within the ING Corporate PKI G3, an RA does not become an agent, fiduciary, trustee, or other representative of ING, insofar that RA is operated by a customer.

2.4 Interpretation and enforcement

Governing law

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

Force Majeure

Any stipulations regarding force majeure are exclusively dealt with by the applicable CP. No additional stipulations are made by this CPS.

Severability

Whenever possible, each provision of this CPS and the CPs shall be interpreted in such manner as to be effective and valid under governing law. If the application of any provision is held to be invalid or

unenforceable, such provision shall be enforced to the maximum extent possible and shall be amended to the extent necessary to make it valid and enforceable.

Survival

If the application of any provision of this CPS and the CPs shall be held to be invalid or unenforceable, then the validity and enforceability of all other provisions shall not in any way be affected or impaired thereby.

Merger

In case of merger all documents related to the ING Corporate PKI G3 will only be changed in accordance with the change procedure as stipulated in chapter 8 of this CPS.

Conflict of Provisions

In the event of a conflict between the provisions of the CP and the CPS, the following ranking will decide the prevailing document:

1. The applicable CP
2. ING Corporate PKI G3 CPS

Dispute resolution procedures

Dispute resolution procedures will be determined by the applicable CP. No additional stipulations are made by this CPS.

2.5 Fees

ING reserves the right to require payment of a fee for delivery of ING Corporate PKI G3 services. Fees may differ depending on certificate and service type and may be regularly increased or decreased at the exclusive discretion of ING Bank NV. The corresponding pricelist is exclusive internal information to ING Group.

2.6 Publication and repository

Each CA shall store its certificates and CRL in the ING Corporate PKI G3 repository. ING will ensure unrestricted access to certificate status information for all applicable relying parties.

This CPS and the associated CPs will be stored on a Web server and made available through the following address: www.ing.com/pki. Such documents can also be obtained through pki@ing.com.

All ING Corporate PKI G3 information not included in the ING Corporate PKI G3 Repository or on the abovementioned website is considered confidential by ING and is not publicly available.

2.7 Compliance audit

Frequency of entity compliance audit

ING Bank NV shall conduct a regular (internal) audit of the ING PKI. All audits shall be performed in compliance with this CPS.

Identity/qualifications of auditor
Internal auditors must be employed by ING.

Topics covered by audit
Topics are at the discretion of the assigned auditors.

Actions taken as a result of deficiency
In case one or more significant deficiencies are identified by an auditor, they have to be formally reported to responsible ING Bank NV management. Where a deficiency poses an immediate threat to the security or integrity of the ING Corporate PKI G3, a possible remedy shall be developed and implemented by ING Bank NV within the shortest term possible, but at least within thirty (30) days after notification has taken place. In case of a less threatening deficiency, appropriate steps must be initiated and executed within a reasonable timeframe.

After it has been implemented, each remedy shall be evaluated by the initial auditor for compliance.

Communication of results
ING Bank NV shall treat audit results as sensitive (commercial) information, and thus as confidential, meaning they will not be publicly available. Audit results will only be made available to the relevant ING departments.

2.8 Confidentiality
Insofar personal data is collected or processed within the ING Corporate PKI G3, it is kept confidential and handled in full compliance with applicable data protection legislation.

PKI certificate status information is by its nature not regarded as confidential and therefore publicly available via CRL and OCSP.

3 Identification and authentication

3.1 Initial registration

Types of names
CAs, RAs and end-users will be certified using a recognizable and, as far as possible and desirable, 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 will contain a combination of the following attributes:

- Common Name (CN);
- Organizational Unit Name (OU);
- Organization Name (O – *if used always equals 'ING'*) of Domain Component (DC – *restricted to windows domain based certificate requests only*)

The location for storing a relevant email address is as an rfc822 Name type in the SubjectAlternateName (SAN-email) field.

Need for names to be meaningful
This CPS does allow for the utilisation of pseudonymous names in certificates.

Uniqueness of Names
The Subject name appearing in each certificate will be need to uniquely bound to the end-user at the time of certificate issuance and unambiguous across the ING corporate PKI G3

Name Claim Dispute Resolution Procedure
ING reserves the exclusive right to decide any name claim dispute and take whatever steps necessary to resolve conflicting naming issues.

Recognition, authentication and roles of trademarks
ING may require an end-user to demonstrate its right to use a particular name.

Proof of possession of private key
Insofar applicable, all end-users must demonstrate possession of the private key associated with a requested public key during the certificate request procedure. This may be done through the use of any method consistent with RFC6712.

Authentication of Individual Identity, Organization Identity, Devices and Applications
Procedures for authentication will be decided by the applicable CP.

Where a domain name or email address is included in the certificate, ING authenticates the organization's right to use that domain name either as a fully qualified domain name or an e-mail domain.

3.2 Certificate renewal

Authentication of an end-user for certificate renewal shall be achieved by validating the end-user credentials, either by demonstrating possession of the private key corresponding to the private key of the current certificate or in the same matter as the initial registration as described in section 3.1.

3.3 Renewal after revocation

Revoked, suspended or expired certificates shall not be renewed. End-users with an expired certificate shall be re-authenticated in the same manner as the initial registration as described in section 3.1.

3.4 Authentication for certificate revocation

Authentication of an end-user requesting revocation of its certificate may be accomplished by demonstrating possession of the private key corresponding to the public key of the certificate that is to be revoked. Proof of possession shall be accomplished as described in section 3.1.

Whenever a certificate has to be revoked as a result of it being compromised in any way, the above procedure may no longer be followed. Subsequently, a request for revocation is then authenticated in the same manner as an initial registration as described in section 3.1.

If an authorized party other than the end-user, as defined in section 4.4.2, requests revocation of a certificate, authentication shall be done via a valid formal consent of a legal representative of that party, or one formally appointed by him for such purpose.

In case authentication of a revocation request is deemed impossible, the CA that issued the certificate will immediately suspend it. Subsequently, that CA or the RA shall seek independent confirmation of the request to determine whether the suspended certificate should be revoked or unsuspended in accordance with section 4.4.

4 Operational requirements

4.1 Certificate application, issuance, and acceptance

Procedural steps constituting certificate application, issuance and acceptance will be decided by the applicable CP.

4.2 Certificate suspension and revocation

The ING Corporate PKI G3 supports certificate Suspension and revocation.

Circumstances for revocation

A certificate may be revoked by the issuing CA if:

- The private key corresponding to the public key identified in the certificate is (considered) compromised, stolen or lost;
- The identifying information contained in the certificate is no longer valid;
- The certificate was not issued in accordance with this CPS or the applicable CP;
- The end-user is no longer eligible to use the certificate;
- It is determined that the end-user has failed to meet its obligations under the CPS, the applicable CP, or any other document applicable to the certificate;
- The end-user no longer wants or requires a certificate; or,
- Material changes to the certificate profile need to be made.

In the event that a CA ceases operations, all certificates issued by that CA shall be revoked prior to the date that the CA ceased operations.

Who can request revocation

A CA may revoke a certificate issued by it:

- On its own initiative;
- At the request of the trusted registrar, the end-user or its manager;
    - End-users can only request the revocation of their own certificates;
    - Trusted registrars and managers can also request the revocation of certificates within their managed group.

Procedure for revocation request

In case of an emergency (e.g. a compromise of the private key) a certificate can be suspended via the 24/7 Suspension Service, using the contact details in 1.1. After this emergency suspension, a normal revocation request has to be submitted to the RA who registered the end-User (see below).

The authentication of an Emergency Suspension request will be performed in accordance with section 3.4.

A normal revocation requests may be done in writing, by phone or on-line to the RA who registered the end-user. If a request is made through the RA, it will notify the CA promptly or as soon as authentication of the requestor has taken place.

Each revocation request must indicate the reason for the revocation (e.g., key compromise, change in affiliation, end-user request) and clearly identify the certificate to be revoked.

The authentication of a revocation request will be performed in accordance with section 3.4.

Once processing of a revocation request is initiated, the CA will revoke the certificate as soon as possible.

Once a certificate has been revoked, a new CRL will be published containing the serial number of the revoked certificate.

Revocation request grace period

For automated processed a certificate will first be suspended and seven (7) days after suspension the status will be changed to revoke. For manual processes there is no revocation grace period.

Circumstances for Suspension

A certificate will be suspended by the issuing CA if:

- The private key corresponding to the public key identified in the certificate is suspected to be compromised, stolen or lost;
- The identifying information contained in the certificate is no longer valid;
- The certificate was not issued in accordance with this CPS or the applicable CP;
- The end-user is no longer eligible to use the certificate;
- The end-user no longer wants or requires a certificate;
- Material changes to the certificate profile need to be made;
- A revocation request is being made, so as to properly authenticate the requestor whilst minimizing any risks;

Who Can Request Suspension

A CA may suspend a certificate issued by it:

- On its own initiative;
- At the request of the trusted registrar, the end-user or its manager;
    - End-users can only request the suspension of their own certificates;
    - Trusted registrars and managers can also request the suspension of certificates within their managed group.

Procedure for suspension request

In case of an emergency (e.g. a compromise of the private key) a certificate can be suspended via the 24/7 Suspension Service, using the contact details in 1.1. After this emergency suspension, a normal suspension request has to be submitted to the RA who registered the end-User (see below).
In normal cases, Suspension requests may be made in writing, by phone or on-line to the RA who registered the end-user. If a request is made through the RA, it will notify the CA promptly or as soon as authentication of the requestor has taken place. An unsuspension request can be submitted through the same procedure as the suspension request.

Each Suspension request must identify the certificate to be suspended.

The authentication of a Suspension request will be performed in accordance with section 3.4. Once processing of a Suspension request is initiated, the CA will suspend the certificate as soon as possible.

Once a certificate has been suspended, a new CRL will be published containing the serial number of the suspended certificate (with a status of 'on hold'). When a certificate has been unsuspended, the serial number of the previously suspended certificate will be removed from the CRL.

Limits on Suspension Period

Apart from the initial validity term of the certificate, no limit to the Suspension period exists.

CRL issuance frequency

All sub-ordinate CAs within the ING Corporate PKI G3 will issue a new CRL at least every twenty-four (24) hours and publish it to the ING PKI Repository. In case of Suspension or revocation of a certificate, a CA will issue and publish an updated CRL as soon as possible.

The ING Corporate PKI Root CA G3 will issue a new CRL at least every two (2) years

CRL or other forms of revocation advertisement checking requirements

A relying party shall only rely on a certificate's contents after checking with the applicable CRL or OCSP for the latest certificate status information, either manually or by automated means.

4.3 Security audit procedures

ING shall maintain adequate records and archives of information pertaining to the operation of the ING Corporate PKI G3. For this purpose, the software used by ING automatically preserves an audit trail for the three primary states in the certificate lifecycle, i.e. generation, operational use and expiry.

Type of events recorded

The minimum records to be kept by ING to enable auditing of the CA systems shall include:

- Key life cycle management events of ING Corporate PKI G3 entities

- Certificate life cycle management events
- Security related events

The selected recorded events are at the discretion of ING and can be changed without further notice.

Frequency and procedures for audit log processing
Audit logs for the ING PKI will be processed on at least a monthly basis.

CA Audit personnel will review CA audit logs every month, including verification of its integrity. Any actions taken following these reviews will be documented.

Retention period for audit logs
ING shall retain all audit logs related to the ING PKI until seven years after disposal of the CA.

Protection of audit log
Access to audit logs shall be restricted to qualified personnel only and protected by a combination of physical and logical security controls.

Audit log back-up procedures
Audit log files shall regularly be archived and stored in a secure storage facility.

Notification to event causing Subject
Where an event is logged by the audit collection system, no notice will be given to the individual, organization, device, or Application, which caused the event.

Vulnerability assessments
Each CA within the ING Corporate PKI G3 will frequently perform a vulnerability assessment of its CA system, with a minimum of once per year. Following an examination of monitored events, appropriate action will be taken when required.

4.4 Records archival
All record archival requirements described in this paragraph apply to ING only and not to its customers or to any other third parties, except where specifically noted.

Types of records archived
The selection of records to be archived, in relation to all actions and information that is relevant to each certificate application and to the generation, issuance, distribution, usage, suspension, revocation, renewal and expiration of all certificates issued by ING Corporate PKI G3 is at the discretion of ING Group NV and can be changed without further notice. All archived records will be considered confidential and treated as such.

Retention period for archive
Archived materials shall be retained for a period of at least seven years after expiration or revocation of the related CA, unless applicable local regulations require a shorter or longer term. In such cases, the maximum term defined in those regulations will prevail.

Disposal of archive records shall be conducted in accordance with adequate professional standards. After disposal, archived records must be permanently unreadable and impossible to reconstruct.

Protection of archive

All archives created for the ING Corporate PKI G3 shall be logically secured and shall be stored in adequately safeguarded locations owned or managed by ING.

Archive backup procedures

All electronic records, including digital copies of physical documents, shall be backed up regularly and stored in a way that enables examination during their retention period. Records that consist only in a physical form will not be backed up by ING.

Archive collection system

Archived records shall be transferred to separate physical media external to the CA host system and Applications.

Procedures to obtain and verify archive information

The integrity of archives created for the ING PKI shall be capable of verification. Integrity verification can be done:

- At the time the archive is prepared;
- Periodically at the time of a programmed security audit; and,
- At any other time when a full security audit is required.

4.5 Key update

The ING Corporate PKI G3 supports a process to update the key pair associated with the certificate prior to the end of the certificate's validity period, so as to avoid a disruption in security services as a result of an expired certificate.

Requests for a key update are authenticated in accordance with section 3.1.

A key update may not be processed if the corresponding certificate is expired, revoked, or suspended. In these cases a key update is to be regarded as an initial request in accordance with section 3.1.

(Sub-)CA key renewal is not applicable. Prior to the end of the (sub-)CAs validity period, a new (sub-) CA will be created, with respects to the usage periods as described in section 6.3.

4.6 Compromise and disaster recovery

Within the ING Corporate PKI G3, procedures have been established to enable system or service recovery in case of a compromise or disaster disruption. Such procedures are considered highly confidential by ING and are not publicly available. ING will take all appropriate measures to minimize disruptions of the ING Corporate PKI G3 services.

4.7 CA termination

If ING decides to terminate the services of a CA within the ING Corporate PKI G3, it will:

- Publish information of its termination at least three months prior to termination;
- Revoke all certificates issued by that CA which have not yet expired;

- Refuse issuance of any new certificates; and,
- Perform any tasks required to maintain and provide continuous access to record archives in accordance with section 4.6.

5 Physical, procedural and personnel security controls

5.1 Physical controls

Physical security controls shall be implemented to control access to the ING Corporate PKI G3 environment in an appropriate manner.

Physical security controls for the CAs and RAs

Physical security controls will be implemented to secure the CA and RA system. More specifically, the ING Corporate PKI G3 will:

- Use sufficient power and air conditioning facilities;
- Use protection from water exposure;
- Use a fire suppression system;
- Protect all storage media from environmental threats such as temperature, water exposure and magnetism;
- Ensure that media used for storage of information is sanitised or destroyed before released for disposal; and
- Ensure that facilities used for off-site backup have the same level of security as the primary site.

Each CA and RA system will be located in a secured area with physical access and intrusion detection controls, including:

- Manual or electronic monitoring of authorised and unauthorised intrusion;
- Listed access of personnel and third-parties under supervision of at least one CA/RA operator;
- Maintenance of a site access log;
- Storage of all removable media and paper containing sensitive information in secured containers or vaults; and
- A perimeter security check of the secured area at least once every twenty-four (24) hours.

Physical security controls for the trusted registrars

Trusted registrars should treat all activation data that allows entry to a private key as confidential and protect it as such. Activation data should be memorised as much as possible, with all paper versions being destroyed, and may not be transferred to people in other roles or made public in any other way. Trusted registrars shall not leave their computers unattended when the private key is in an activated state (i.e. when the password has been entered) but must close all active sessions before doing so.

Physical security controls for end-users

End-users should treat all activation data that allows entry to a private key as confidential and protect it as such. Activation data should be memorised as much as possible, with all paper versions being destroyed, and may not be transferred to other persons or made public in any other way. End-users shall not leave their computers unattended when the private key is in an activated state (i.e. when the password has been entered) but must close all active sessions before doing so.

5.2 Procedural controls

Trusted roles

All ING personnel that have access to or control over cryptographic operations that may materially influence the operation of the ING Corporate PKI G3 with respect to certificate issuance, use, suspension, or revocation, including access to restricted operations of the ING Corporate PKI G3, shall, for purposes of this CPS, be considered as serving in a trusted role. Such personnel includes, but is not limited to, CA operators, trusted registrars, system administration personnel, engineering personnel, security management and managers who are designated to oversee the operations of the ING Corporate PKI G3.

Trusted roles for CAs

Within the ING Corporate PKI G3, duties with regard to critical functions of CA systems are separated to prevent one person from maliciously using a CA system without detection. System access for each trusted role is limited to those actions that are required to perform certain responsibilities. At least three distinct trusted roles will be distinguished for each CA:

1. Day-to-day operation of a CA system, and
2. Management and audit of CA operations, and
3. Management of changes to system requirements including its policies, procedures, or personnel.

Trusted roles for RAs

All trusted registrars within the ING Corporate PKI G3 are considered to be acting in a trusted role. Each trusted registrar must perform its function in a secure and trustworthy manner and must be qualified to do so, in compliance with 5.3.

In case a customer operates an RA, it is the customer's responsibility and liability to ensure that all Registrars perform their functions in a secure and trustworthy manner and are qualified to do so, in compliance with 5.3.

Identification and authentication for each role

All trusted roles for CAs have their identity and authorisation verified before they are:

- Included in the access list for the CA site;
- Included in the access list for physical access to the CA system;
- (if required) Given a certificate for the performance of their CA role; and
- (if required) Given an account and/or access on the PKI system.

Each of these certificates and accounts (with the exception of CA signing certificates) is restricted (through the use of PKI software, operating system and procedural controls), to actions authorised for that role.

CA and RA operations are secured, using mechanisms such as smart card-based strong authentication and encryption, when accessed across a shared network.

5.3 Personnel controls

Individuals assuming trusted roles shall be of unquestionable loyalty, trustworthiness and integrity. Individuals assigned to a trusted role for a CA shall:

- Be appointed in writing by ING;
- Not be assigned other duties that may conflict with the duties defined for the trusted role;

- Be a permanent employee or other authorised individual, and not subject to frequent re-assignment or extended periods of absence;
- Not have been previously relieved of a past assignment for reasons of negligence or non-performance of duties, and
- Have sufficient expertise and knowledge required for the performance of their duties.

6 Technical security controls

Note: all technical security controls are solely applicable to the key pairs and corresponding certificates generated by the ING Corporate PKI G3.

6.1 Key pair generation, delivery and installation

Key pair generation
Key pairs will be generated by the Requester/Component Owner in either a HSM, a smart card or a software keystore depending on the envisioned level of trust is should support; the public key will be signed off by the appropriate ING Corporate PKI G3 CA.

Private key delivery to entity
Only in exceptional cases, at the discretion of the asset owner of the ING Corporate PKI G3, smart cards containing private keys may be delivered to the end-user in person or may be securely delivered via standard or signed mail so long as they are distributed separately from any activation data required to access the private keys.

CA public key delivery to users
The CA certificate containing the public key corresponding to the CAs signing key is delivered to each end-user using a secure and authenticated certificate management protocol such as RFC2510. The key is always downloadable from www.ing.com/pki.

Key sizes
All end-user Key pairs shall have a minimum size of 2048 bit RSA and a maximum size not exceeding the size of the issuing CA.
All key pairs for CAs will have a minimum size of 4096 bit RSA.

The key size limits will be periodically reviewed, with a minimum of once a year, to judge their appropriateness for securing communications.

Hardware/Software key generation
All key pairs for PKI Core components are generated in a hardware cryptographic module.

Key usage purposes (as per X.509 v3 key usage field)
Key usage purposes are specified using the X.509 Certificate key usage extension, which is marked critical and used in accordance with RFC2459. Usage for specific types of certificates that may be issued under this CPS is in accordance with section 7.

Key pairs issued to formal ING Corporate PKI subCAs may only be used to sign certificates and CRLs.

6.2 Private key protections

Access to private keys is restricted and requires activation data only available to the associated end-user. Security measures regarding private keys should be in line with the ING Security Standards on key material.

Standards for cryptographic module

All cryptographic operations of CAs are performed in a hardware security module (HSM) rated to at least FIPS 140-1 Level 3 or otherwise verified to an equivalent level of functionality and assurance.

All end-user smart cards are rated to at least FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance.

Private key (n out of m) multi-person control

Three person-control is required for access to the ING Corporate PKI G3 Root CA. Two person-control is required for access to all ING Corporate PKI G3 SubCA signing keys.

Private key escrow

Each CA supports escrow of private keys used for encryption where required by law. Signing keys will never be escrowed.

Private key backup

All keys related to PKI components will be backed-up. Backed-up keys are stored in encrypted form and protected at a level similar to or higher than the level stipulated for the primary version of the key.

Private key archival

All End-Entity key pairs, excluding singing keys, used for encryption will be archived to support optional key recovery services. Each CA provides for the recovery of an archived private decryption key upon request by the end-user, the associated customer or legal officers following authentication in accordance with section 3.

Private key entry into cryptographic module

Private keys in cryptographic modules shall be stored in such way that they can be used inside the module but never be retrieved from the cryptographic module.

If the private key is generated inside the cryptographic module, it shall remain there without ever leaving that module. If the private key is generated outside the cryptographic module, it has to be entered into the module without ever leaving the key generation environment.

The key generation environment must have controls in place to ensure that no person can access a generated private key without detection.

Method of activating private key

The private key shall be protected from exposure and unauthorised usage by end-user specific activation data.

Method of deactivating private key
The cryptographic module automatically deactivates all active private keys once the module itself is deactivated. In addition, the cryptographic module contains means of deactivating a private key after each use.

Method of destroying private key
Upon termination of the usage of a CAs key pair, all copies of the private key shall be securely destroyed.

6.3 Other aspects of key pair management
Cryptographic token initialisation, key loading, and personalisation shall be performed in a secure way.

Usage periods for the public and private keys
- Key pairs used to perform CA functions have a maximum validity of twenty (20) years;
- All end-entity key pairs will have a maximum validity depending on the purpose and approval method. In case of automated request and approval the maximum validity is 15 months (1 year + 3 months grace period). In case of manual request and approval the maximum validity is 39 months (3 years + 3 months grace period)

Key pairs are not to be used beyond their validity period.

In case it is decided by ING that updating CA key pairs would be good practice or required to ensure the trustworthiness of the ING Corporate PKI G3, they may be revoked and reissued at any time before their expiry.

6.4 Activation data
Security measures regarding activation data should be in line with the ING Security Standards on key material.

Activation data generation and installation
All activation data is unique and unpredictable and offers a security level appropriate to that of the protected key pair.

Activation data protection
Data used for key pair activation must be protected from unauthorised use by a combination of cryptographic and physical access control mechanisms. The level of protection must be adequate to deter a motivated attacker with substantial resources. If a reusable password scheme is used, the mechanism shall include a facility to temporarily lock the account after a predetermined number of login attempts.

6.5 Computer security controls

Specific computer security technical requirements
In general, each CA system provides computer security controls sufficient to support the requirements for the definition of trusted roles and separation of duties in accordance with section 5 and the use of

key pairs in accordance with section 6. The controls also support the audit log and archive requirements in accordance with section 4.

Specifically, each CA utilises a CA system that provides the following minimum functionalities:

- Access control to CA services and trusted roles;
- Enforced separation of duties for trusted roles;
- Identification and authentication of trusted roles and associated identities;
- Use of cryptography for session communication;
- Archival of CA history and audit data;
- Audit of security-related events;
- Self-test of security-related CA services;
- Trusted path for identification of trusted roles and associated identities; and
- Recovery mechanisms for keys and the CA system.

This functionality may be provided by the operating system, or through a combination of the operating system, the CA system software, and physical safeguards.

6.6 Life cycle technical controls

System development controls

The development of the CA system is performed in a controlled environment that provides protection against the insertion of malicious logic. The software vendor has a quality system that has been certified as compliant with international standards or must make its quality system available for inspection upon request.

Security management controls

A formal configuration management methodology is used for installation and ongoing maintenance of a CA system.

The CA system software, when first loaded, provides a method for the CA to verify that the software on the system:

- Originated from the software developer;
- Has not been modified prior to installation; and
- Is the version intended for use.

Life cycle security ratings

Each CA utilises a mechanism to periodically verify the integrity of the software and has mechanisms and policies in place to control and monitor the configuration of the CA system.

During installation and at periodic intervals, the integrity of the CA system software and configuration is validated by ING.

6.7 Network security controls

The CA system is protected from attacks through any open or general purpose network with which it is connected.

6.8 Cryptographic module engineering controls

See sections 6.2 and 6.6.

7 Certificate and CRL profiles

7.1 Certificate profile

Certificates issued under this CPS are constructed according to X.509 standards
The certificate profile per type of certificate is determined by the applicable CP.

Version number(s)

The version field shall be set to 2, indicating that the version is X.509v3.

Certificate extensions

Certificate extensions are processed in accordance with the appropriate standards.

All certificates issued under this CPS contain the X.509 Certificate Policy extension. This extension is not marked critical.

All certificates issued under this CPS contain the X.509 key usage extension. This extension is marked critical.

Algorithm object identifiers

For signatures, the RSA algorithm with SHA256 hashing (OID 1.2.840.113549.1.1.11) is being used.
For encryption, the RSA algorithm (OID 1.2.840.113549.1.1.1) is being used.

Name forms and constraints

The use of name fields is in accordance with section 3.1.

Certificate policy Object Identifier

See section 1.2.

Policy qualifiers syntax and semantics

Each CA populates the policy qualifiers extension with a general disclaimer and reference to the URL through which the CP, this CPS and other related documents can be obtained.

Processing semantics for the critical certificate policy extension

See section 1.5.

7.2 CRL profile

Version number(s)

Each ING PKI Issuing CA shall support X.509 version 3.

CRL and CRL entry extensions
All software within the ING PKI correctly processes CRL extensions conform standards.

8 Specification administration

8.1 Specification change procedures

Items that can change without notification

Typographical corrections may be made to this CPS and the CPs without prior notification of end-users and without creating a new version.

Changes may be made to this CPS and the CPs without notification of end-users and with creating a new version, insofar as the changes don't materially affect the conditions relevant to certificate(s) in use by the end-users at the moment the new version becomes effective.

Items which change requires a new policy

All changes that are not covered by 8.1.1 are considered to materially affect the contents of the CPS and the CPs and will require a new version as well as notification to end-users prior to replacing the original version.

8.2 Publication and notification policies

All changes as referred to in 8.1.1. may be made without the implicit or explicit approval of the PAA.

All changes as referred to in 8.1.2 shall only be made with the explicit approval of the PAA. Such changes shall undergo a maximum review and comment period of thirty (30) days, after which the proposed modifications will be inserted and a new version published, insofar the changes are not amended or rejected by the PAA.

When required, according to section 8.1 of this policy, all end-users will be notified of the changes either electronically or in writing. Notice of change will include the date of issuance of the new version, which will be at least one week after the notification date.

8.3 Applicability and acceptance of changes

All changes to this CPS shall become effective one month after publication. Use of, or reliance on a certificate after notification and after the changes have become effective shall be deemed acceptance of the modified terms.

9 References

[PKCS1] RSA Laboratories. ***PKCS #1 – RSA Cryptography Standard***, version 2.0, October 1998. Available at http://www.rsasecurity.com/rsalabs/pkcs/index.html.

[X509] ITU-T Recommendation X.509 (1997 E): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, June 1997.