ING Public Key Infrastructure Certification Practice Statement

Version 2.0 – December, 7th 2023

Crypto Service Centre Board (CSCB)

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: Crypto Service Centre Board Location HBP E4.071 PO Box 1800 1000 BV Amsterdam Netherlands e-Mail: pki@ing.com
Document version	Version 2.0 – 7 December 2023
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 rated **C1 (Public)**.
Abstract	This Certificate Practice Statement (CPS) contains the processes and procedures governing all certification services within the ING Corporate PKI, 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, starting from G4 onwards, from the moment of publication.
References	Most recent versions of the following references are used, unless stated otherwise: • 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' • ETSI EN 319 401 'General Policy Requirements for Trust Service Providers' • ETSI EN 319 411-1 'Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements' • IT Security Standards on Data Encryption and Cryptography • CA/Browser (CAB) Forum Baseline Requirements

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
CDP	Certificate Distribution Point
CPS	Certification Practice Statement
CSCB	Crypto Service Centre Board, delegate of the PAA
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
RA	Registration Authority

Roles and Responsibilities

The governing bodies, and their responsibilities, listed below will be used throughout this CPS.

Approval Authority (PAA)

The PAA is the governance body of the ING Corporate PKI and performs the following activities:

- Define and formulate requirements of the CPs, in accordance to ING standards;
- Validate the suitability of implementation of the CPS as stipulated by the CPs;
- Governance of the ING Corporate PKI, including handling conflicts between participants, manage deviation towards standards, changes to policies and requirements and communication to stakeholders.

The abovementioned activities do not constitute the entire obligations or responsibilities for the PAA within the ING Corporate PKI. Additional obligations may apply through this CPS.

The roles and responsibilities of the PAA may be performed by the CSCB, as a delegate.

Certificate Authority (CA)

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

- Operate in full accordance with this CPS and the applicable CPs, 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 CPs;
- Cooperate with (internal) audits performed as provided in Chapter 8; and,
- Maintain certificate status information in a manner accessible to all Relying Parties.

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

Registration Authority (RA)

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

- Operate in full accordance with this CPS and the applicable CPs, as well as with any applicable laws of the governing jurisdiction;
- Cooperate with (internal) audits performed as provided in Chapter 8;
- Take all reasonable measures to ensure that subscribers are aware of their respective rights and obligations with respect to the use of certificates issued under this CPS and the applicable CPs;
- 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 activities do not constitute the entire obligations for an RA within the ING Corporate PKI. Additional obligations may apply through this CPS or the applicable CPs.

Index

1 Introduction

The ING Corporate PKI issues digital certificates. The various types of certificates are listed on pki.ing.com.

1.1 Overview

This CPS describes the practices and procedures of (i) the CAs and (ii) RAs operating under the CAs. All legal documents about the ING Corporate PKI are publicly available and can be obtained via pki.ing.com or the Crypto Service Centre Board (Information Sheet, page 2). The ING Corporate PKI and the associated rules, regulations and procedures are based on the most recent versions of ETSI EN 319 401 and ETSI EN 319 411-1 at the date of publication of this CPS.

The ING Corporate PKI sets out two levels of assurance provided by certificates within the PKI, 'Class 1' and 'Class 2'. These levels represent varying degrees of rigor and depth, as described in the table below.

Assurance level	Description
Class 1	Enterprise grade CA implementation that reflects the minimum trust levels conform the requirements from the Policy Approval Authority.
Class 2	ETSI based CA implementation that reflects a higher trust level conform the applicable requirements determined by the Policy Approval Authority.

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

URL	pki.ing.com
Email	pki@ing.com
Postal address	Refer to pki.ing.com
24/7 Suspension Service telephone number	+31 88 464 22 24 (ACCI – Alarm & Communications Center ING)

1.2 Document Name and Identification

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

Policy Name	ING Corporate PKI Certification Practice Statement
Policy Qualifier	For information, consult pki.ing.com or the Crypto service Centre Board (Information Sheet, page 2)
Policy Version	2.0
Policy Status	FINAL
Policy OID	1.3.6.1.4.1.2787.200.4
Policy is registered with	Base policy 1.3.6.1.4.1.2787 is registered for ING with Joint ISO-ITU standards organization
Date of issue	2023-12-07
Date of expiry	NA

1.3 PKI participants

Certification Authorities (CA)

In the ING Corporate PKI, each CA may authorise Certificate Signing Requests (CSRs) and Public Keys from subscribers whose identity has been verified, according to applicable trust level, as provided herein by a RA. CAs may create, sign, issue, revoke and handle certificates and CRLs within the terms made by its respective CP as well as this CPS. CAs are operated and managed by CA operators (CAO).

This CPS covers all activities performed by CAs published on pki.ing.com.

Registration Authorities (RA)

Within the ING Corporate PKI, a Registration Authority (RA) is responsible for authentication and registration of subscribers. Only ING entities or parties explicitly 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. Parties can be specifically designated by ING to operate as a RA under this CPS, under conditions set by a relevant Subscriber agreement and established by the Policy Approval Authority.

Subscribers

Subscribers may use CA services within its acceptable use. A subscriber, as used herein, may refer to both the subject of the certificate and the entity that contracted with the CA for the certificate's issuance.

The following subscribers are recognized within the ING Corporate PKI:

- ING Employees;
- ING Customers;
- ING Contractors; and
- Assets used, managed or contracted by ING.

Relying Parties

A relying party is a person, entity, or organization that relies on a valid certificate. Relying parties must be part of ING or are external parties that have explicitly agreed through contractual agreement on trusting the ING Corporate PKI. Unauthorized reliance on certificates issued within the ING Corporate PKI is not accepted nor approved by ING Groep N.V. and does not make ING Groep N.V. responsible nor liable for such reliance in whatever manner.

Other Parties

Within the ING Corporate PKI, no other parties provide PKI-related services.

1.4 Certificate usage

Certificate usage is limited to usages as specified in the various types of issued certificates and as prescribed by the relevant CP. ING Groep N.V. 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 is prohibited by ING Groep N.V.

The use of all certificates issued by the CA shall be for lawful purposes and consistent with applicable laws, including without limitation, applicable export or import laws.

1.5 Policy administration

This CPS shall be administered, managed, and approved 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 Crypto Service Centre Board (Information Sheet, page 2).

Specification change procedures

Items that can change without notification

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

Items which change requires a new policy

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

Publication and notification policies

All changes as referred to in the above paragraph 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.

This CPS shall be reviewed at least every two years, by or on behalf of the PAA. Suggested changes to this CPS from this periodic review shall follow the same process as for other changes as described above.

When required, according to section in the above paragraph of this policy, all subscribers 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 fifteen (15) days after the notification date.

Applicability and acceptance of changes

All changes to this CPS shall become effective fifteen (15) days 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.

2 Publication and Repository Responsibilities

The ING Corporate PKI maintains the Repository to store various information related to the certificates and the operation of CAs and RAs. The CPS and various other related information are published in the Repository.

2.1 Repositories

Where applicable, the CAs maintain the repositories to allow access to certificate-related and certificate revocation information. The repositories are the only approved source for CRL and other information about certificates.

The CA will adhere to the latest version of the CPS published in the repository.

This CPS and the associated CPs will be stored on a Web server and made available through the following address: pki.ing.com. Such documents can also be obtained through pki@ing.com. All ING Corporate PKI information not published on the abovementioned website is considered confidential by ING and is not publicly available.

2.2 Publication and repository responsibilities

The requirement for storage of certificates and CRL is specified under each CP.

This CPS is structured in the RFC3647 format.

2.3 Publication and repository responsibilities

The CPS will be re-issued and published when a newer version is approved. The newer CPS will be updated with an incremented number.

CRLs and OCSP responses will be updated as per paragraph 4.6.

2.4 Access controls on repositories

Information published in the repository is public information. Read only access is unrestricted. The CAs have implemented logical and physical controls to prevent unauthorized write access to its repositories.

3 Identification and authentication

The Policy Approval Authority mandates the verification practices for verifying identification and authentication, and may, in its discretion, update such practices.

3.1 Naming

Before issuing a certificate, the CAs ensure that all subject organization information in the certificate conforms to the requirements of, and has been verified in accordance with the procedures prescribed in the applicable CP and matches the information confirmed and documented by the RA pursuant to its verification processes.

Types of names

The subject names in a certificate comply with the X.501 Distinguished Name (DN) form. The CAs shall use a single naming convention as specified in each applicable CP(s).

Need for names to be meaningful

The certificates issued pursuant to this CPS are meaningful only if the names that appear in the certificates can be validated against a central system of reference which is acknowledged by the CA. Names used in the certificates must identify the person or object to which they are assigned in a meaningful way.

Anonymity or Pseudonymity of subscribers

No stipulations are made by this CPS.

Uniqueness of Names

Names shall be defined unambiguously for each Subject in a Repository. The Distinguished Name attribute will usually be unique to the Subject to which it is issued. Each Certificate shall be issued a unique serial number within the name space of its Issuing-CA.

Name Claim Dispute Resolution Procedure

No stipulations are made by this CPS.

Recognition, authentication and roles of trademarks

No stipulations are made by this CPS.

3.2 Initial identity validation

Proof of possession of private key
Insofar applicable, all subscribers must demonstrate possession of the private key associated with a 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 are decided by the RA and approved by the PAA.

3.3 Identification and Authentication for Re-key requests

Each certificate shall contain a certificate expiration date. The subscriber is responsible to monitor the certificate expiration date and timely request for certificate re-keying.

Authentication of a subscriber for certificate re-key shall be achieved by validating the subscriber credentials, either by demonstrating possession of the private key corresponding to the public key of the current certificate or in the same matter as the initial registration as described in section 3.2.

3.4 Identification and Authentication for Re-key after Revocation

Revoked, suspended or expired certificates shall not be rekeyed. Upon revocation of a certificate, the subscriber shall immediately cease using such certificate and shall remove such certificate from any devices and/or software in which it has been installed.

3.5 Identification and Authentication for Revocation Requests

A subscriber may request revocation of a certificate at any time provided that the CA can validate the subscriber is the person, organization, or entity to whom the certificate was issued.
Authentication of a subscriber 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;
- authenticated in the same manner as an initial registration as described in section 3.2;
- providing a revocation secret, as set during the request.

If an authorized party other than the subscriber, as defined in section 4.5. requests revocation of a certificate, authentication shall be done via a valid formal consent, as described by the applicable CP, of a representative of that party, or one formally appointed for such purpose.

In case authentication of a revocation request is not possible within an acceptable timeframe, the CA that issued the certificate may immediately suspend it, if investigation yields reasonable cause. 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 the applicable CP.

4 Certificate Life-Cycle Operational Requirements

This CPS describes generic stipulations insofar applicable to all certificates. Specific stipulations are made in the applicable CPs.

4.1 Certificate application, application processing, issuance, acceptance, key pair generation and certificate usage

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

The CA will follow the documented actions defined by the applicable CP for verifying all data requested for inclusion in the certificate. In cases where the certificate request does not contain all the necessary information about the subscriber, the CA will obtain the remaining information from a reliable data source.

Assurance level	Description
Class 1	Enterprise grade CA implementation that reflects the minimum trust levels conform the requirements from the Policy Approval Authority. Details about applicable requirements can be found on pki.ing.com
Class 2	ETSI based CA implementation that reflects a higher trust level conform the applicable requirements determined by the Policy Approval Authority. Details about applicable requirements can be found on pki.ing.com

Who can submit a certificate application

Either the subscriber or an individual authorized to request certificates on behalf of the subscriber may submit certificate requests. Subscribers are responsible for any data that the subscriber or an agent of the subscriber supplies to the RA.

Approval or rejection of certificate applications

The CA or RA rejects any certificate application that cannot be verified or is unauthorized.

Time to process certificate applications

No stipulations are made by this CPS.

Subscriber private key and certificate usage

Key Pair generation, and other technical specifications, shall adhere to the ING IT Security Standards for Data Encryption and Cryptography. No further stipulations are made by this CPS.

4.2 Certificate Renewal

Revoked, suspended or expired certificates shall not be renewed. The subscriber must apply for a new certificate and replace the certificate that has been revoked.

4.3 Certificate Re-key

No stipulations are made by this CPS.

4.4 Certificate Modification

No stipulations are made by this CPS.

4.5 Certificate revocation and suspension

Each CA supports revocation and suspension when stipulated by the applicable CP.

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 subscriber is no longer eligible to use the certificate;
- It is determined that the subscriber has failed to meet its obligations under the CPS, the applicable CP, or any other document applicable to the certificate;
- The subscriber no longer wants or requires a certificate (end of subscription to CA services); 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 ceasing the CA.

Who can request revocation

A CA may revoke a certificate issued by it:

- On its own initiative;
- At the request of a RA, for certificates within their scope;
- At the request of subscribers, for their own certificates;
- At the request of managers, for certificates within their managed group.

Procedure for revocation request

The procedures for revocation request are stipulated in the applicable CP(s).

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

Revocation request grace period
Revocation request grace period(s) are stipulated in the applicable CP(s).

Circumstances for Suspension
A certificate will be suspended by the issuing CA if:

- The revocation request is entered via an automated means, to allow unsuspension in case of irregularities or availability risks;
- Private key materials need to be transported to minimize the impact of a potential compromise;
- 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 a RA, for certificates within their scope.

Procedure for suspension request
Subscribers are not able to request suspension. Therefore, no stipulations are made in this CPS.

Limits on Suspension Period
Limits for suspension periods are stipulated in the applicable CP(s).

4.6 Certificate status services

CRL issuance frequency
All Root- and Intermediate-CAs will issue a new CRL at least every one (1) year and publish it.

All Issuing-CAs will issue a new CRL at least every seven (7) days and publish it, unless the applicable CP stipulates otherwise.

Certificate status information availability
Certificate status information, when required, is available through CRL and/or OCSP, 24 hours per day, 7 days per week.

4.7 End of subscription
A subscription ends at the moment a certificate expires or is revoked.

4.8 Key Escrow and Recovery

Private key escrow and archival
A CA shall support escrow of private encryption keys where required by law or when stipulated by the applicable CP. Signing and mixed purpose keys will not be escrowed.

All private keys in escrow will be archived. A CA provides for the recovery of such private key upon request by the subscriber, the private key owner, its ING representative or a designated Corporate Security & Investigations (CSI) member following authentication in accordance with section 3.2.

5 Facility, Management, and Operational Controls

5.1 Physical security controls

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

Physical security controls for the Root- and Intermediate-CAs

Physical security controls will be implemented to secure the CA system. More specifically, the ING Corporate PKI 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 and water exposure;
- Listed access of personnel and third-parties under supervision of at least one CA operator;
- Ensure that media used for storage of information is sanitised or destroyed before released for disposal; and
- Ensure that facilities used for CA sites (e.g. backup) have a similar level of security as the primary site.

Each Root- and Intermediate-CA system will be located in a High Secure Environment (HSE) conform ING standards.

Physical security controls for Issuing-CAs

No stipulations are made by this CPS.

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 with respect to certificate issuance, use, suspension, or revocation, including access to restricted operations of the ING Corporate PKI, 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 (RAs), DevOps personnel, auditors, key custodians, security management and managers who are designated to oversee the operations of the ING Corporate PKI.

Within the ING Corporate PKI, 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. Additionally, for compliance reasons, there are roles that may not be combined (toxic combinations).

Trusted role	Description	Toxic combinations	Multi-person control requirement	Knowledge requirement(s)
CA Operators	Management and implementation of changes to CA requirements and configurations including its policies, procedures or roles	CA Auditor	4-eye principle (with same role)	Proven and validated knowledge of the application and potential impact of activities
Trusted registrars (RAs) and delegates	Perform request validation and approve certificate (revocation) request according to standards	RA Auditor Manager (in case of self-approval)	No requirements	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

DevOps personnel	Day-to-day operation of a CA underlying infrastructure, including monitoring, alerting, implementing security measures, etc. Management of RA components including key material.	CA Auditor	4-eye principle (with same role) [high secure environment] Dual control (approval flow, with same role) [non-high secure environment]	Engineer requirements, while understanding security requirements and impact.
CA Auditor	Audit CA operations, controls	CA Operator DevOps pers. Key cust. A Key cust. B Key cust. C	No requirement	Auditor requirements in compliance with chapter 8
RA Auditor	Audit RA operations, procedures, controls and systems	Trusted Registrar (RA) of the subject of audit	No requirement	Auditor requirements in compliance with chapter 8
Key custodian A	Management of the 'A' part of the PKI CA component key materials	CA Auditor Key cust. B Key cust. C	Combined with B and C for Root-CA keys – 6-eye principle Combined with B for non-Root-CA keys – 4-eye principle	No requirements

Key custodian B	Management of the 'B' part of the PKI CA component key materials	CA Auditor Key cust. A Key cust. C	Combined with A and C for Root-CA keys – 6-eye principle Combined with A for non-Root-CA keys – 4-eye principle	No requirements
Key custodian C	Management of the 'C' part of the PKI CA component key materials (Root-CA only)	CA Auditor Key cust. A Key cust. B	Combined with A and B for Root-CA keys – 6-eye principle	No requirements
Independent Observer	Observe CA key generation and usage	All other trusted roles except Security Manager and Manager	For Root-CA keys, class 1&2, non-ING (external observer)	Relevant experience
Security Manager	Responsible for all security (from physical to logical) related decisions within the service	CA Operator Key cust. A Key cust. B Key cust. C	No requirement	Relevant security experience
Manager (Area Lead)	Leads the team, sets the standards and takes responsibility for developing, innovating and safeguarding knowledge	CA Operator DevOps pers. Key cust. A Key cust. B Key cust. C	No requirement	No requirement

Identification and authentication for each role
All trusted roles for CAs have their identity and authorisation verified before they are accepted in their respective roles.

5.3 Personnel controls
Individuals assigned to a trusted role for a CA, excluding the Independent Observer, shall:

- Be authorized and registered for that role in ING's applicable systems;
- Not be assigned other duties that may conflict with the duties defined for the trusted role;
- Prior to the engagement of any person in a trusted role, the CA or RA shall verify the identity and trustworthiness of such person;
- For roles directly interacting with the CA / CA system, an additional screening by ING internal screening department, according to the applicable standards for sensitive roles is mandatory;
- Be sufficiently trained and have the required knowledge for the performance of their duties.

After validation by the PAA (or its delegates), individuals assigned as an Independent Observer:

- May be authorized and registered for that role;
- Are confirmed to be sufficiently trained and have the required knowledge for the performance of their duties.

5.4 Audit logging procedures
ING shall time-stamp and record significant security events in the CAs as audit logs in audit trail files. The audit trail files are processed on a regular basis.

Type of events recorded
The minimum records to be kept by ING to enable auditing of the CA systems shall include, at least:

- Key life cycle management events of ING Corporate PKI entities;
- Certificate life cycle management events;
- Security related events.

Retention period for audit logs
Unless otherwise stated in the applicable CP, the CA will retain the events recorded as specified above, for at least two years, after either the destruction of the CA key or the revocation or expiration of the CA certificate, whichever comes last.

Protection of audit log
Stipulations are made by the applicable CP(s).

Audit log back-up procedures
Stipulations are made by the applicable CP(s).

Audit collection system
No stipulations are made by this CPS.

Notification to event causing Subject
Stipulations are made by the applicable CP(s).

Vulnerability assessments
The ING Corporate PKI will periodically be subject to a vulnerability assessment, conform ING standards. Follow-up actions to remediate deviations shall follow ING standards.

5.5 Records archival
All record archival requirements described in this paragraph apply to ING Corporate PKI only and not to its customers or to any other third parties, except where specifically approved/required by the PAA. The records archival, where applicable, is securely stored on ING internal premises.

Assurance level	Description
Class 1	Records shall not be archived, unless specified in applicable CP(s).
Class 2	Records shall regularly be archived and stored in a secure storage facility.

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 is at the discretion of ING Groep N.V. and can be changed without further notice. All archived records will be considered confidential and treated as such.

Retention period for archive
Unless otherwise stated in the applicable CP, the CA will retain archived materials, for at least two years after either the destruction of the CA key or the revocation or expiration of the CA certificate, whichever comes last.

Disposal of archive records shall be conducted in accordance with adequate professional standards. The chosen method for disposal and destruction must assure that archived records shall be permanently unreadable.

Protection of archive
All archives created for the ING Corporate PKI shall be logically secured and shall be stored in adequately safeguarded locations owned or managed by ING. Mitigating measures are taken to ensure confidentiality, integrity and availability of the archive. The operational effectiveness of these measures are audited according to Chapter 8.

Archive backup procedures
No stipulations are made by this CPS.

Archive collection system
No stipulations are made by this CPS.

Procedures to obtain and verify archive information
Stipulations are made by the applicable CP(s).

5.6 Compromise and disaster recovery
Within the ING Corporate PKI, 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 services.

5.7 CA or RA termination
If ING decides to terminate the services of a CA or RA within the ING Corporate PKI, ING will develop a termination plan aimed at minimizing disruption to subscribers and relying parties. This plan may include, as deemed necessary by the PAA:

- Publishing a notice of termination at least three months prior to termination;
- Provisions necessary for the transfer of CA or RA services to a successor CA or RA;
- Refuse issuance of any new certificates;
- Termination of authorization for all entities that are authorized to act on behalf of the ING Corporate PKI in carrying out functions related to the process of issuing certificates;
- Revoke remaining valid certificates within termination scope on the termination date;
- Provisions necessary to provide certificate validation information for at least the lifetime of all active certificates;
- Perform any tasks required to maintain and provide continuous access to record archives in accordance with the applicable CP.

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.

6.1 Key pair generation, delivery and installation

Key pair generation

The public key parameters are conform the ING ITSS on Data Encryption and Cryptography.

Key pairs will be generated by the subscriber/component owner in either approved hardware or software depending on the envisioned level of trust and scope it should support; the public key will be signed off by the appropriate ING Corporate PKI CA.

Private key delivery to entity

Only in exceptional cases, at the discretion of the PAA (or its delegates), keystores containing private keys may be delivered to the subscriber 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 public key is always downloadable from pki.ing.com.

Key sizes

Key size implemented for subscribers and CAs are conform the ING ITSS on Data Encryption and Cryptography.

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. Further stipulations are made by the applicable CPs.

6.2 Private key protection and Cryptographic Module Engineering Controls

Access to private keys is restricted and requires activation data only available to the associated subscriber. Security measures regarding private keys should be in line with the ING ITSS on Data Encryption and Cryptography.

Standards for cryptographic module

The standards for cryptographic modules and operations of CAs implemented are specified and reviewed conform the ITSS on Data Encryption and Cryptography.

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

Entity	Class 1	Class 2
Root-CA	4-eyes / 2 roles	6-eyes / 3 roles
Intermediate-CA	4-eyes / 2 roles	4-eyes / 2 roles
Issuing-CA	4-eyes / 1 role	4-eyes / 2 roles

Private key backup
All CA private keys will be backed-up. Other keys are backed-up based on risk assessment as stipulated by the applicable CP.

Backed-up keys are stored in encrypted form and protected, conform the standards stipulated by the IT Security Standard for Data Encryption and Cryptography.

Private key entry into cryptographic module
The implemented standards for private keys in cryptographic modules and operations are specified and reviewed conform the IT Security Standards on Data Encryption and Cryptography.

Method of activating private key (CA)
The method of activating private key is conform standard operating procedures.

Method of deactivating private key (CA)
The method of deactivating private key is conform standard operating procedures.

Method of destroying private key (CA)
The method of destroying private key is conform standard operating procedures.

6.3 Other aspects of key pair management
Cryptographic token initialisation, key loading, and personalisation shall be performed in a secure way. All aspects of key pair management are conform the IT Security Standards for Data Encryption and Cryptography.

6.4 Activation data
Security measures regarding activation data should be in line with the ING IT Security Standards on Data Encryption and Cryptography.

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;
- Central ING NTP functionality;
- 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 CA makes use of Commercial Off The Shelf (COTS) products for the hardware, software, and network components. The software vendor has a quality system that has been certified as compliant with applicable standards.

Components developed or maintained by ING or its delegates must adhere to the ING Minimum Standards.

Security management controls

General security management controls are implemented conform ING Minimum Standards.

Specific, security management controls for CA related activities follow ETSI standards for Trust Service Providers.

6.7 Network security controls

The CA has implemented security controls to comply with the CA/Browser Forum's Network and Certificate System Security Requirements and ING Minimum Standards for network segmentation.

7 Certificate, CRL and OCSP 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[1], indicating that the version is X.509v3.

Certificate extensions

Certificate extensions are processed in accordance with the CA/B forum baseline requirements.

Where relevant, 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

Algorithm object identifiers are stipulated by the applicable CP(s).

Name forms and constraints

The use of name fields is in accordance with section 3.1. Further stipulations are made by the applicable CP(s).

Certificate policy Object Identifier

CP Object Identifiers are specified by the applicable CP(s).

Policy qualifiers syntax and semantics

Each Issuing CA populates the policy qualifiers extension with a 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

Certificate policies extension is marked Not Critical.

[1] The versioning is zero-based. Version 1 is 0x00, version 2 is 0x01, version 3 is 0x02, etc.

7.2 CRL profile

Version number(s)
Each ING PKI Issuing-CA shall support X.509 version 2.

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

7.3 OCSP profile

The profile for the Online Certificate Status Protocol (OCSP) messages issued by a CA conform to the specifications contained in the IETF RFC 6960 Internet X.509 PKI Online Certificate Status Protocol (OCSP)Profile.

8 Compliance audit and other assessments

Frequency of entity compliance audit

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

Assurance level	Description
Class 1	Self-assessment or validation is performed at least once per year.
Class 2	Audit is performed by an independent (internal) party against the latest ETSI standards, at least each 5 years.

Circumstances that will trigger an assessment

The following circumstances may trigger an assessment:

- An audit plan;
- Pre-operational assessment as a condition of allowing an entity to be operational; or
- An investigation following a possible or actual compromise of security.

Minimum qualifications of auditor

The minimum required qualifications of auditors is dependent on the assessment scope and assurance level.

Assurance level	Description
Class 1	Minimum qualifications for experience and domain knowledge is determined and approved by the PAA or its delegates.
Class 2	Minimum qualifications for experience and knowledge is determined through external certification (CISA or equivalent) and approved by the PAA. Auditors are required to be independent.

Topics covered by audit

Topics are at the discretion of the assigned auditors and aligned with the PAA or its delegates.

Actions taken as a result of deficiency

In case one or more significant deficiencies are identified by an (internal) auditor, they have to be formally reported to responsible ING Groep N.V. management. Where a deficiency poses an immediate threat to the security or integrity of the ING Corporate PKI, a possible remedy shall be developed, implemented and resolved by ING Groep N.V., conform the standard ING processes.

Communication of results

ING Groep N.V. shall treat audit results as sensitive (commercial) information, and thus as confidential, meaning they will not be publicly available. Decisions around communication of audit results will be at the discretion of the PAA.

9 Other Business and Legal Matters

9.1 Fees

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

9.2 Financial responsibility

Indemnification by relying parties and subscribers

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

Fiduciary relationships

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

9.3 Confidentiality of business information

PKI certificate status information is by its nature regarded as non-confidential and therefore publicly available.

9.4 Privacy of personal information

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

9.5 Intellectual property rights

No stipulations are made by this CPS.

9.6 Representations and Warranties

No stipulations are made by this CPS.

9.7 Disclaimers of Warranties

No stipulations are made by this CPS.

9.8 Limitations of Liability

Any liabilities regarding the CAs and RAs operating within the ING Corporate PKI are exclusively dealt with by the applicable CP. No additional stipulations are made by this CPS.

9.9 Indemnities

No stipulations are made by this CPS.

9.10 Term of Termination

This CPS will be effective fifteen (15) days after this CPS is published in the Repository and will continue until a newer version of the CPS is published.

This CPS will remain in effect until replaced by a newer version.

9.11 Individual notices and communications with participants

Unless otherwise set out in a Subscriber Agreement or Relying Party Agreement, any notice to be given to the ING Corporate PKI under this CPS, a Subscriber Agreement, or a Relying Party Agreement shall be given in writing to the (e-mail) address specified in Crypto Service Centre Board (Information Sheet, page 2).

Any notice to be given by the ING Corporate PKI under the CPS or any Subscriber Agreement shall be given by e-mail to the last e-mail address for the Subscriber known with the PKI Corporate PKI. In the event of notice by e-mail, the notice shall become effective fifteen (15) days after publishing.

9.12 Amendments

No stipulations are made by this CPS.

9.13 Dispute resolution procedures

Dispute resolution procedures will be determined by the applicable CP. No additional stipulations are made by 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. ING Corporate PKI CPS
2. The applicable CP

9.14 Governing law

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

9.15 Interpretation and enforcement

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

Force Majeure

Force majeure is covered by the Dutch law (art. 6:75 Dutch Civil Code).

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 will only be changed in accordance with the change procedure as stipulated in chapter 8 of this CPS.

10 References

[PKCS1] RSA Laboratories. ***PKCS #1 – RSA Cryptography Specifications*** Version 2.2. Available at https://tools.ietf.org/html/rfc8017

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

[ITSS1] ING Global CISO. ***IT Security Standard on Data Encryption and Cryptography*** version 5.1.0. Available at CISO Bookshelf.

[RFC3647] IETF. ***Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC3647).*** Available at https://datatracker.ietf.org/doc/rfc3647/

[RFC2459] IETF. ***Internet X.509 Public Key Infrastructure Certificate and CRL Profile.*** Available at https://datatracker.ietf.org/doc/rfc2459/

[CAB1.7] CA/Browser Forum. ***Network and Certificate System Security Requirements*** Version 1.7. https://cabforum.org/wp-content/uploads/CA-Browser-Forum-Network-Security-Guidelines-v1.7.pdf

11 Document change log

Version	Remarks
V2.0	Initial version for G4, based on RFC3647.