ING Public Key Infrastructure Certificate Policy For Class 1 Certificates

Version 2.0 – June 2024

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 – 14 June 2024
General	The format of this CP 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 Policy (CP) identifies the certificate types and use cases issued by the Class 1 Issuing Certificate Authorities (CAs) within the ING Corporate PKI, as supported by the applicable Certification Practise Statement (CPS).
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

Index

1 Introduction

The ING Corporate PKI issues digital certificates. The various relevant Class 1 types of certificates are listed on pki.ing.com.

1.1 Overview

This CP covers all Class 1 CAs and RAs operating under these CAs as identified in the CPS. All relevant and related 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 claims in the related CPS are valid for all certificates and services issued under this CP. Where the CPS covers the relevant topics in this CP the remark will be 'No additional stipulations made'.

1.2 Document Name and Identification

Document Name	ING Corporate PKI G4 CP Class 1
Date of issue	2024-06-114
Date of expiry	NA

1.3 PKI participants

No additional stipulations made.

1.4 Certificate usage

The Class 1 CAs will issue the types of certificates as indicated at https://www.pki.ing.com/

1.5 Policy administration

No additional stipulations made.

Specification change procedures

Items that can change without notification

Changes may be made to this CP 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 CP 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 CP shall be reviewed at least every two years, by or on behalf of the PAA. Suggested changes to this CP 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. For Class 1 CA's this notification might also be the publication of the change on pki.ing.com. 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 CP 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 CP and various other related information are published in the Repository.

2.1 Repositories

For Class 1 certificates no registration in certificate transparency (CT) logs will be performed.
No additional stipulations made.

2.2 Publication and repository responsibilities

The storage of certificates and CRL is managed within the PKI-application.
Publication of CRLs and, where applicable certificates, is done via the generic website, https://pki.ing.net.

2.3 Publication and repository responsibilities

No additional stipulations made.

2.4 Access controls on repositories

No additional stipulations made.

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

No additional stipulations made.

3.2 Initial identity validation

No additional stipulations made.

3.3 Identification and Authentication for Re-key requests

No additional stipulations made.

3.4 Identification and Authentication for Re-key after Revocation

No additional stipulations made.

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 3.2, requests revocation of a certificate, authentication shall be done in a similar manner as the authentication of the request.

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 in a similar manner as the authentication of the request.

4 Certificate Life-Cycle Operational Requirements

The CPS describes generic stipulations insofar applicable to all certificates. Specific stipulations are made in this CP.

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

Who can submit a certificate application
A certificate request can be done by the legal person seeking to obtain a personal certificate or the asset owner, or his delegate, when requiring a certificate for one of its assets.

Approval or rejection of certificate applications
A CA/RA will reject the request if the information cannot be verified against a PAA identified and approved source or if the information is identified to be incomplete/inaccurate/wrong.

Time to process certificate applications
An automated request will be handled as soon as possible, targeting to keep it below 2 minutes. Manual request will be targeted to be processed within 5 working days.

Subscriber private key and certificate usage
Key and certificate usage should be in accordance with the ITSS on Data encryption and Cryptography.

4.2 Certificate Renewal

The ING Corporate PKI Class 1 CAs do not support certificate renewal.

4.3 Certificate Re-key

Not applicable.

4.4 Certificate Modification

Certificate modification can only be achieved by revoking the existing certificate and requesting a new certificate.

4.5 Certificate revocation and suspension

No additional stipulations made.

4.6 Certificate status services

CRL issuance frequency
No additional stipulations made.

Certificate status information availability
No additional stipulations made.

4.7 End of subscription

No additional stipulations made.

4.8 Key Escrow and Recovery

Private key escrow and archival
No additional stipulations made.

5 Facility, Management, and Operational Controls

5.1 Physical security controls

Class 1 Root and Intermediate CAs will be located within the High Secure Environment (HSE). Class 1 Issuing CAs can be located both within and outside of the HSE. For CAs hosted outside the HSE, the standard Data Centre security measures are deemed to be sufficient.

No additional stipulations made.

5.2 Procedural controls

No additional stipulations made.

5.3 Personnel controls

No additional stipulations made.

5.4 Audit logging procedures

Type of events recorded
No additional stipulations made.

Retention period for audit logs
In deviation of the CPS Class 1 audit logs are only retained for at least 3 months, after either the destruction of the CA key or the revocation or expiration of the CA certificate, whichever comes last.

Protection of audit log
Security audit logs for Class 1 Root CAs are protected by the PKI-application. For Class 1 Issuing CAs no separate protection has been implemented.

Audit log back-up procedures
Class 1 Audit logs are not backed up.

Audit collection system
Audit logs for Class 1 Issuing CAs are sent to the central monitoring solutions.
No additional stipulations made.

Notification to event causing Subject
No stipulation

Vulnerability assessments
No additional stipulations made.

5.5 Records archival

Types of records archived
No additional stipulations made.

Retention period for archive
In deviation of the CPS the CA will retain archived materials, for at least 3 months after either the destruction of the CA key or the revocation or expiration of the CA certificate, whichever comes last.

Protection of archive
No additional stipulations made.

Archive backup procedures
No additional stipulations made.

Archive collection system
No additional stipulations made.

Procedures to obtain and verify archive information
No stipulation

5.6 Compromise and disaster recovery
No additional stipulations made.

5.7 CA or RA termination
For Class 1 CA/RA there are no additional tasks defined.

6 Technical security Controls

6.1 Key pair generation, delivery, and installation

No additional stipulations made.

6.2 Private key protection and Cryptographic Module Engineering Controls

Standards for cryptographic module

No additional stipulations made.

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

Only for CA, no additional stipulations made.

Private key backup

All Class 1 RA, interface and operational account private keys will be backed up conform the ITSS on Data Encryption and Cryptography.

Private key entry into cryptographic module

No additional stipulations made.

Method of activating private key (CA)

No additional stipulations made.

Method of deactivating private key (CA)

No additional stipulations made.

Method of destroying private key (CA)

No additional stipulations made.

6.3 Other aspects of key pair management

No additional stipulations made.

6.4 Activation data

No additional stipulations made.

6.5 Computer security controls

For Class 1 Cas, next to the central ING NTP also standard provider supported NTP solutions are allowed.

No additional stipulations made.

6.6 Life cycle technical controls

No additional stipulations made.

6.7 Network security controls

No additional stipulations made.

7 Certificate, CRL and OCSP profiles

7.1 Certificate profile

Can be obtained via the ING Corporate PKI Internet site: https://www.pki.ing.com/

7.2 CRL profile

No additional stipulations made.

7.3 OCSP profile

No additional stipulations made.

8 Compliance audit and other assessments

No additional stipulations made.

9 Other Business and Legal Matters

9.1 Fees

No additional stipulations made.

9.2 Financial responsibility

No additional stipulations made.

9.3 Confidentiality of business information

No additional stipulations made.

9.4 Privacy of personal information

No additional stipulations made.

9.5 Intellectual property rights

No additional stipulations made.

9.6 Representations and Warranties

No additional stipulations made.

9.7 Disclaimers of Warranties

No additional stipulations made.

9.8 Limitations of Liability

No additional stipulations made.

9.9 Indemnities

No additional stipulations made.

9.10 Term of Termination

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

This CP will remain in effect until replaced by a newer version or until 3 months after termination of the last Class 1 CA.

9.11 Individual notices and communications with participants

No additional stipulations made.

9.12 Amendments

No additional stipulations made.

9.13 Dispute resolution procedures

For Class 1 CAs disputes will be resolved by the Product Owner of the ING Corporate PKI, the PAA will be informed of the resolution.

Conflict of Provisions

No additional stipulations made.

9.14 Governing law

Class 1 CAs are governed by the laws of the Netherlands, unless otherwise set out in specific subscriber agreements or specific relying party agreements.

9.15 Interpretation and enforcement

No additional stipulations made.

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*** latest version. 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

Document change log

Version	Remarks
V1.1	Initial version for G4, based on RFC3647.
V2.0	Processed review comments, finalized version