ING Public Key Infrastructure Certificate Practice Statement

Version 5.4 - November 2015

ING

Colophon

Commissioned by	ING Corporate PKI Policy Approval Authority
Additional copies	Additional copies of this document can be obtained via the ING internet site www.ing.com/pki or by mail: pki@ing.com.
Document version	Version 5.4 - November 2015
General	The format of this CPS is based on the Internet Engineering Task Force Public Key Infrastructure (IETF PKIX) Part 4 Certificate Policy and Certification Practice Statement Framework (RFC2527) 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, in accordance with the applicable Certificate Policies.
Audience	The information contained in this document is intended for all users of the ING Corporate PKI.
References	• ING PKI Certificate Policy Root CA • ING PKI Customer Certificate Policy • ING PKI Employee Certificate Policy • ING PKI Technical Certificate Policy • ING PKI Code of Conduct for Technical Certificates • ING PKI Code of Conduct for Employee Certificates • Terms and Conditions ING PKI Customer CA • Terms and Conditions ING PKI Technical CA • ING PKI Glossary • ANSI X9.79 7.1 • ETSI 102.042 • The Internet Engineering Task Force Public Key Infrastructure (IETF PKIX) Part 4 Certificate Policy and Certification Practice Statement Framework (RFC2527).
Statement Extended Validation	The ING Technical CA 2005 conforms to the current version of the CA/Browser Forum
SSL Certificates	Guidelines for Issuance and Management of Extended Validation Certificates ('Guidelines') published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

List of abbreviations

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

Abbreviation	Term
BU	Business Unit
CA	Certification Authority
CA	Certification Authority Officer
CDS	Corporate Directory Service
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
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardisation Sector
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol
OID	Object Identifier
PAA	Policy Approval Authority
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKCS	Public Key Cryptographic Standards.
PSC	PKI Service Centre
PSE	Personal Security Environment
RA	Registration Authority
RSA	Rivest Shamir Adleman (encryption algorithm)
SLA	Service Level Agreement

Contents

1. Introduction

1.1. Overview

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

- ING PKI Certificate Policy Root CA
- ING PKI Customer CP
- ING PKI Employee CP
- ING PKI Technical CP.

Except for the ING PKI Certificate Policy Root CA, the CP's and the ING PKI CPS are publicly available and can be obtained via www.ing.com/pki or the ING PKI Service Centre (Information Sheet, page 2).

The format of this CPS is based on the Internet Engineering Task Force Public Key Infrastructure (IETF PKIX) Part 4 Certificate Policy and Certification Practice Statement Framework (RFC2527).

The ING PKI and the associated rules, regulations and procedures are based on ETSI 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 below services in particular before making use of or putting reliance on Certificates issued within the ING PKI.

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

URL	www.ing.com/pki
E-mail	pki@ing.com
Postal address	ING PKI Service Centre PO Box 1800 1000 BV Amsterdam the Netherlands
24/7 Suspension Service	+31 88 464 2224

1.2. Definitions and Acronyms

The capitalised terms used in this Certification Practice Statement refer to and have the meaning of the definitions described in the ING PKI Glossary, which is publicly available at www.ing.com/pki or via the ING PKI Service Centre (Information Sheet, page 2).

1.3. Identification

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

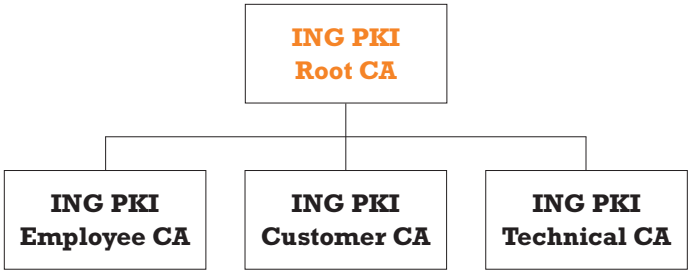
Policy Name	ING PKI Certificate Practice Statement
Policy Qualifier	ING Bank N.V. is the issuer of this certificate. Restrictions may apply to its use; please check the applicable CP and CPS for details. For information, contact www.ing.com/pki or pki@ing.com
Policy Version	5.4
Policy Status	Final
Policy OID	1.3.6.1.4.1.2787.200.1.6
Policy is registered with	Joint ISO-ITU standards organisation
Date of Issue	November 9th 2015
Date of Expiry	na

1.4. PKI Participants

1.4.1 Certification Authorities (CA)

Within the ING PKI, the following Certification Authorities exist:

- ING PKI Root CA
- ING PKI Employee CA
- ING PKI Customer CA
- ING PKI Technical CA



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

Each CA responsible for the issuance of a Certificate within the ING PKI is (technically) identified by the following names:

- ING PKI Root CA = 'ING Root CA 2005'
- ING PKI Employee CA = 'ING Employee CA 2005'
- ING PKI Customer CA = 'ING Customer CA 2005'
- ING PKI Technical CA = 'ING Technical CA 2005'.

1.4.2 Registration Authorities (RA)

Within the ING PKI, a Registration Authority (RA) is responsible for authentication and registration of End-Users. Only ING entities, Customers of ING or parties specifically designated by ING are allowed to operate as an RA under this CPS – no other parties are allowed. RA's 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 an RA under this CPS.

Conditions are described in the Outsourcings Policies of ING Group.

1.4.3 Repositories

All Certificates that are issued within the ING PKI are stored in the ING PKI Repository, being the whole of directories which include status information pertaining to all Certificates. The ING PKI Repository may be comprised of different systems operated and managed on different locations, and is wholly owned and supervised by ING Bank N.V.. CRL's are published at the internet, the specific URL's are to be found in the certificates.

1.4.4 End-Users

The following End-Users are recognised within the ING PKI:

CA	End-User
ING PKI Root CA ING PKI	CA's subordinate to the Root
ING PKI Technical CA	Devices or Applications of ING or – under strict conditions – Customers of ING
ING PKI Employee CA	Employees of ING
ING PKI Customer CA	Customers of ING, including Customer devices and applications

This CPS is binding on each End-User by virtue of a Code of Conduct (ING) or Terms & Conditions (non-ING), and governs each End-User's performance with respect to the request for and usage of Certificates.

1.4.5 Relying Parties

Reliance on Certificates issued within the ING PKI is restricted to the following parties:

Certificate	Relying Parties
Root Certificate	All end-user entities
Technical Certificate used by ING	All end-user entities
Technical Certificate used by Customers	ING end-user entities only
Employee Certificate	All end-user entities
Customer Certificate	ING end-user entities only
Technical Certificate submitted under Customer CA	ING end-user entities only

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

1.5. Certificate Usage

1.5.1 Appropriate Certificate Use

Depending on the type of Certificate and the Application, Certificates issued within the ING PKI will allow the End-User to either:

- 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 with ING through SSL (Secure Socket Layer) connections for confidentiality purposes
- Enable or make use of ING Applications through VPN (Virtual Private Network).

Any other usage of Certificates issued within the ING PKI is not allowed by ING Bank N.V..

1.5.2 Prohibited Certificate Use

Whenever reliance restrictions apply (see the table in 1.4.5) it is not allowed to use Certificates for securing communications with anyone other than the parties authorised by ING Bank N.V..
Depending on the type of Certificate and the Application, ING Bank N.V. reserves the right to limit or restrict the usage of and/or reliance on certain Certificate functions as described in 1.5.1.

1.6. Policy Administration

1.6.1 Organisation administering the document

This CPS is managed by the ING PKI Policy Approval Authority (PAA).

1.6.2 Contact address

All questions regarding this CPS can be addressed to the ING PKI PAA via the ING 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 PKI.

2.1.1 CA Obligations

Each CA within the ING PKI, 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 RA's comply with the relevant provisions of the CPS and the applicable CP
- Publish Certificates in the ING PKI Repository and maintain Certificate status information therein in a manner accessible to all Relying Parties.

The abovementioned obligations do not constitute the entire obligations for a CA within the ING PKI. Additional obligations may apply through this CPS, a CP or Terms and Conditions.

2.1.2 RA Obligations

Each entity acting as an RA within the ING PKI, 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 PKI. Additional obligations may apply through this CPS, a CP or Terms and Conditions.

2.1.3 End-User Obligations

An End-User who is issued a Certificate within the ING PKI shall be obliged to:

- Operate in accordance with the CPS and the applicable CP
- Operate in accordance with any applicable Code of Conduct or Terms and Conditions, 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 in case the certificate is compromised or lost, or when sufficient reason exists to presume that the certificate has been compromised or lost
- Only use his Certificates by himself and 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 or has expired
- Continue to safeguard the Private Key associated with a suspended Certificate, and
- Securely destroy a Smart Card containing the Private Key associated with a revoked Certificate.

The abovementioned obligations do not constitute the entire obligations for an End-User within the ING PKI. Additional obligations may apply through this CPS, a CP, a Code of Conduct or Terms and Conditions.

2.1.4 Relying Party obligations

All persons or entities authorised 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 PKI Root CA.

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

2.1.5 Repository Obligations

All CA's within the ING PKI shall publish their Certificates issued under this CPS, as well as relevant Certificate information such as CRL's, in the ING PKI Repository. In doing so, each CA shall use reasonably commercial efforts to maintain and keep the ING PKI Repository up-to-date.

2.2. Liability

2.2.1 CA Liability

Any liabilities regarding the CA's operating within the ING PKI are exclusively dealt with by the applicable CP and/or Terms and Conditions. No additional stipulations are made by this CPS.

2.2.2 RA Liability
Any liabilities regarding the RA's operating within the ING PKI are exclusively dealt with by the applicable CP and/or Terms and Conditions. No additional stipulations are made by this CPS.

2.3. Financial Responsibility

2.3.1 Indemnification by Relying Parties
Any indemnifications to be made by Relying Parties are – if made – exclusively dealt with by the applicable CP. No additional stipulations are made by this CPS.

2.3.2 Indemnification by End-Users
Any indemnifications to be made by End-Users are – if made – exclusively dealt with by the applicable CP and/or Terms and Conditions. No additional stipulations are made by this CPS.

2.3.3 Fiduciary relationships
By appointing End-Users within the ING PKI, an RA does not become an agent, fiduciary, trustee, or other representative of ING, insofar that RA is operated by a Customer.

2.3.4 Administrative process
Not stipulated.

2.4. Interpretation and enforcement

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

2.4.2 Force Majeure
Any stipulations regarding force majeure are exclusively dealt with by the applicable CP and/or Terms and Conditions. No additional stipulations are made by this CPS.

2.4.3 Assignment
Not stipulated.

2.4.4 Severability, Survival, Merger, Conflict of Provisions, Waiver, Notice

2.4.4.1 Severability
Whenever possible, each provision of this CPS, the CPs and the ING PKI Glossary 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.

2.4.4.4 Survival
If the Application of any provision of this CPS, the CP's and the ING PKI Glossary 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.

2.4.4.5 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.

2.4.4.6 Conflict of Provisions
In the event of a conflict between the provisions of the CP, the CPS and any applicable Code of Conduct or Terms and Conditions, the following ranking will decide the prevailing document:
1. Code of Conduct/Terms and Conditions
2. ING PKI Glossary
3. The applicable CP
4. ING PKI CPS
5. ING PKI Privacy Statement.

2.4.4.7 Waiver
Not stipulated.

2.4.4.8 Notice
Not stipulated.

2.4.5 Dispute resolution procedures
Dispute resolution procedures will be determined by the applicable CP and/or by the Terms and Conditions. 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 PKI services. Fees may differ depending on Certificate type and may be regularly increased or decreased at the exclusive discretion of ING. The corresponding pricelist is exclusive internal information to ING Group.

2.6. Publication and Repository

2.6.1 Publication of ING PKI Information
Each CA shall store its Certificates and CRL in the ING PKI Repository. ING will ensure unrestricted access to Certificate status information for all applicable Relying Parties. Certificates are internal and external to ING Group available via LDAP directories.

This CPS, the associated CP's, the ING PKI Glossary and the ING PKI Privacy Statement 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 PKI information not included in the ING PKI Repository or on the abovementioned website is considered confidential by ING and is not publicly available.

2.6.2 Access controls
Not stipulated.

2.7. Compliance Audit

2.7.1 Frequency of Entity compliance audit
Frequently, with a minimum of once per year, ING Bank N.V. shall conduct an internal audit of the ING PKI. All audits shall be performed in compliance with this CPS.

2.7.2 Identity/qualifications of auditor
Internal auditors must have a minimum of two years of previous IT auditing experience and must be employed by ING.

2.7.3 Topics covered by audit
Each audit will include, but is not limited to, compliance with:
- ING PKI CP's, and
- ING PKI CPS.

Topics covered by each audit will include but are not limited to:
1. CA and RA environmental controls
2. CA and RA physical security controls
3. Key management controls
4. Certificate life cycle management controls
5. CA and RA infrastructure/administrative controls.

2.7.4 Actions taken as a result of deficiency
In case one or more significant deficiencies are identified by an internal or external auditor, they have to be formally reported to responsible ING Bank N.V. management. Where a deficiency poses an immediate threat to the security or integrity of the ING PKI, a possible remedy shall be developed and implemented by ING Bank N.V. within the shortest term possible, but at least within thirty 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.

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

2.8. Confidentiality
Insofar personal data is collected or processed within the ING PKI, it is kept confidential and handled in full compliance with applicable data protection legislation. The ING PKI Privacy Statement applies to all ING PKI activities.
Certificate status information is not regarded as confidential and therefore public available via CRL.

3. Identification and Authentication

3.1. Initial Registration

3.1.1 Types of names
CA's, RA's and End-Users will be certified using a recognisable and unique X.500 Distinguished Name (DN) in the Certificate 'Subject name' field, in accordance with RFC2459. The DN will be in the form of a 'printableString' or 'utf8String' and is never to be left blank.

Each DN will contain an Organisation Name attribute set to 'O = ING' and a combination of the following attributes:
- Organisational Unit Name (OU)
- Common Name (CN).

This CPS does allow for the utilisation of pseudonymous names in Certificates.

The location for storing an End-User's email address is as an rfc822Name type in the SubjectAlternateName field.

3.1.2 Need for names to be meaningful
All End-User names assigned in Certificates shall be derived from Directories owned or managed by ING. This includes the need for names for Technical Certificates or Customer Technical Certificates to be meaningful (in the assigned Directories).

3.1.3 Rules for Interpreting Various Name Forms
The rules for interpreting various name forms for Employee Certificates will be defined by the scheme of the CDS directory. There is no stipulation regarding rules for interpreting various name forms for Technical Certificates or Customer Certificates.

3.1.4 Uniqueness of Names
The Subject name appearing in each Certificate will be unique at the time of Certificate issuance and unambiguous across the ING PKI. If necessary, additional unique identifiers may be appended to the distinguished name to ensure the name's uniqueness within the ING PKI.

3.1.5 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.

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

3.1.7 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 a shared secret or some other method consistent with the key transfer protocol described in the PKIX Certificate Management Protocol (RFC2510).

Whenever Key Pairs are generated by ING, the above proof-of-possession procedure does not apply.

3.1.8 Authentication of Individual Identity
Procedures for authentication of individual entities will be decided by the applicable CP's, i.e. the Certificate Policy for ING PKI Employee CA and the Certificate Policy for ING PKI Customer CA.

3.1.9 Authentication of Devices and Applications
Procedures for authentication of Devices and Applications will be decided by the applicable CP, i.e. the Certificate Policy for ING PKI Technical CA and the Certificate Policy for the ING PKI Customer CA.

3.1.10 Authentication of Organisation Identity
Whenever a certificate contains an organization's name, the identity of the organization and other enrollment information provided by Certificate Applicants is confirmed in accordance with the procedures set forth in ING's documented Validation Procedures.
At a minimum ING shall:

• Determine that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government agency or competent authority that confirms the existence of the organization

• Confirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organization, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Certificate Applicant is Authorized to do so.

When a certificate includes the name of an individual as an authorized representative of the Organization, the employment of that individual and his/her authority to act on behalf of the Organization shall also be confirmed.

Where a domain name or e-mail 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 demonstrating possession of the Private Key corresponding to the Public Key of the Certificate to be updated, in accordance with section 4.7. Automatic updates will not require authentication of the End-User's identity.

Once a Certificate has expired, the above procedure shall no longer be an option. As a result, a request for renewal is then authenticated in the same manner as an 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 in the same manner as described in section

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 renewal is then authenticated in the same manner as an initial registration as described in section 3.1.

If an authorised 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 reactivated in accordance with section 4.4.

4. Operational Requirements

4.1. Certificate application

Procedural steps constituting the Certificate request process will be decided by the applicable Certificate Policy.

4.2. Certificate issuance

Procedural steps constituting Certificate issuance will be decided by the applicable Certificate Policy.

4.3. Certificate Acceptance

Procedural steps constituting Certificate Acceptance will be decided by the applicable Certificate Policy.

4.4. Certificate Suspension and Revocation

The ING PKI supports Certificate Suspension and Revocation.

4.4.1 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 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 does not make use of at least one application provided by ING that is necessarily supported by the ING PKI
- It is determined that the End-User has failed to meet its obligations under the CPS, the applicable CP, or any other document, like the Terms and Conditions, 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.

4.4.2 Who can request Revocation

A CA may revoke a Certificate issued by it:

- On it's own initiative
- At the request of the Customer, 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.

4.4.3 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 fax, 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.

The end-user of the revoked Certificate will automatically, immediately be informed via e-Mail.

The RA is electronically informed in case of revocation and emergency suspension via normal reporting procedures.

4.4.4 Revocation request grace period

There is no Revocation grace period.

4.4.5 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
- It is determined that the End-User has failed to meet its material obligations under this CPS, or any other agreement, terms, conditions, regulation, or law applicable to the Certificate that may be in force
- 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
- The end-user will not need the certificate for a longer period (holidays etc).

If required, Certificates may be generated and distributed in a suspended state for security reasons, to be lifted once Acceptance has taken place. (e.g. Roaming Certificates).

4.4.6 Who Can Request Suspension

A CA may suspend a Certificate issued by it:

- On it's own initiative
- At the request of the Customer, 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.

4.4.7 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 fax, 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 Suspension request must indicate the reason for the Suspension and 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, and the CA or RA will inform the End-User about the new status of its Certificate.

Prior to the end of the Suspension period, the CA or RA will investigate the circumstances of the Suspension and either revoke or reactivate the Certificate. Reactivation shall only be allowed if it has been sufficiently demonstrated that the reason for Suspension is no longer valid.

The end-user of the suspended Certificate will beinformed.

4.4.8 Limits on Suspension Period

Apart from the initial Validity term of the Certificate, no limit to the Suspension period exists.

4.4.9 CRL issuance frequency

All CA's within the ING PKI, the ING PKI Root excluded, 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.

4.4.10 CRL checking requirements

Insofar authorised to do so, a party shall only rely on a Certificate's contents after checking with the applicable CRL for the latest Certificate status information, either manually or by automated means.

4.4.11 Checking requirements for other forms of Revocation advertisements

Not stipulated.

4.5. Security audit procedures

ING shall maintain adequate records and archives of information pertaining to the operation of the ING PKI. 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.

4.5.1 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, including
  - Cryptographic device life cycle management events
  - Key generation processes (successful and unsuccessful)
  - Key renewal and key recovery
  - Key backup, storage and archival
  - Records of the destruction of media containing key material, activation data or personal information of End-users
- Certificate life cycle management events, including
  - Certificate application, suspension and revocation requests (successful and unsuccessful)
  - Registration records, including records relating to rejected application requests (regarding a/o identification/authentication methods and storage of identification documents)
  - Registration records regarding Trusted Registrars/ Delegated RAO's
  - Certificate issuance and distribution records, including updates to online status systems
  - Generation, suspension, revocation and renewal of certificates
  - Generation and issuance of CRL's

- Security related events, including
  - PKI (security) system actions performed by ING PKI staff
  - Attempts to create, remove, set passwords or change the system privileges of ING PKI system administrators or security administrators
  - Security related incidents like PKI system access attempts (successful and unsuccessful)
  - System crashes, hardware failures and other anomalies like failed read-and-write on the ING PKI Repository
  - ING PKI CA facility visitor entry/exit.

The minimum records to be kept by ING to enable auditing of all non-CA Systems used within the ING PKI shall include:

- Physical access logs
- Operating system start-up and shutdown
- Application start-up and shutdown
- Data back-up and recovery events
- Login and logoff attempts
- Unauthorised attempts to access system files or network components
- System configuration changes and maintenance
- Personnel changes
- Discrepancy and compromise reports, and
- Inspection and compliance reports.

All logs, whether electronic or manual, contain the date and time of the event, and the identity of the Entity which caused the event.

4.5.2 Frequency and procedures for audit log processing

Audit logs for the ING PKI will be processed on at least a weekly basis.

CA personnel will review audit logs every week, including verification of its integrity and inspection of all entries. Any actions taken following these reviews will be documented. Backups will be made on daily bases. Year backups will be held for at least seven (7) years.

4.5.3 Retention period for audit logs

ING shall retain all audit logs related to the ING PKI for a maximum period of seven (7) years.

4.5.4 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.

4.5.5 Audit log back-up procedures

Audit log files shall be backed-up and stored in a secure off-site storage facility.

4.5.6 Audit collection system

Not stipulated.

4.5.7 Notification to event causing Subject

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

4.5.8 Vulnerability assessments

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

4.6. 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.

4.6.1 Types of records archived

The minimum 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 PKI shall include:

- Authentication records
- Registration records, including records relating to rejected requests
- Key generation requests, including whether or not key generation was successful
- Certificate generation requests, including whether or not Certificate generation was successful
- Certificate issuance and Revocation records
- Audit records, including security related events
- Contract materials
- Signing keys for Certification Authorities, Registration Authorities, CRL's and OCSP responders
- Confidentiality keys, and
- Certificates.

All archived records will be considered confidential and treated as such.

4.6.2 Retention period for archive

Archived materials shall be retained for a period of seven (7) years after expiration or revocation, 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.

4.6.3 Protection of archive

All archives created for the ING PKI shall be logically secured and shall be stored in adequately safeguarded locations owned or managed by ING. Archives shall be located in an environment which is protected from environmental factors such as temperature, humidity, and magnetism.

Each archive shall employ:

- Storage of records in secure fire-proof containers
- Detailed registers containing signed recordings for all lodgements and withdrawals of Archives, and
- Clear labelling of all storage media.

4.6.4 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.

4.6.5 Archive collection system

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

4.6.6 Procedures to obtain and verify archive information

The integrity of all electronic archives created for the ING PKI shall be capable of verification, so as to ensure that the archived data:

1. Exists
2. Is not corrupted
3. Has not been changed
4. Is complete, and
5. Is in its original form.

Integrity verification shall 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.

4.7. Key Update

The ING PKI 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-)CA's validity period, a new (sub-)CA will be created, with respects to the usage periods as described in section 6.3.2.

4.8. Compromise and disaster recovery

Within the ING 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 minimise disruptions of the ING PKI services.

4.8.1 Computing resources, software, and/or data are corrupted

Not stipulated.

4.8.2 CA/RA Public Key is revoked

Not stipulated.

4.8.3 CA/RA key is compromised

Not stipulated.

4.9. CA Termination

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

- Publish information of its termination at least three (3) 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 all hardware and software within the ING PKI. This includes the CA host computers and any external cryptographic hardware module or hardware profile storage device.

5.1.1 Physical Security Controls for the CA's and RA's

Physical security controls will be implemented to secure the CA and RA System. More specifically, the ING 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, 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, and
- A perimeter security check of the secured area at least once every twenty-four (24) hours.

5.1.2 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 other persons 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.

5.1.3 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

5.2.1 Trusted Roles

All ING personnel that have access to or control over cryptographic operations that may materially influence the operation of the ING PKI with respect to Certificate issuance, Use, Suspension, or Revocation, including access to restricted operations of the ING 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, system administration personnel, engineering personnel, security management and managers who are designated to oversee the operations of the ING PKI.

5.2.1.1 Trusted Roles for CA's

Within the ING 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. At least three (3) 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.

5.2.1.2 Trusted Roles for RA's

All Trusted Registrars within the ING PKI 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.

All Trusted Registrars within the ING PKI acting as registrar for EV SSL Certificates will be screened at ING C3 level.

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.

5.2.1.3 Identification and authentication for each role

All Trusted Roles for CA's 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
- Given a Certificate for the performance of their CA role, and

- Given an account on the PKI system.

Each of these Certificates and accounts (with the exception of CA signing Certificates) is:
- Directly attributable to an individual
- Not shared, and
- Is restricted (through the use of CA software, operating system and procedural controls), to actions authorised for that role.

CA 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.

6.1. Key Pair generation and installation

6.1.1 Key Pair generation

All Employee and Customer Key Pairs will be securely generated on a HSM or on Smart Cards by ING. For security purposes, End-Users are not allowed to generate any Key Pairs.

All Technical Key Pairs will be generated by the Requester/ Component Owner; the public key will be signed off by the appropriate ING PKI CA.

6.1.2 Private Key delivery to entity

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.

6.1.3 Public Key delivery to Certificate issuer

Not stipulated.

6.1.4 CA Public Key delivery to users

The CA Certificate containing the Public Key corresponding to the CA's signing key is delivered to each End-User using a secure and authenticated Certificate management protocol such as RFC2510. The key is either available on the Smart Card issued to the end-user or downloadable from www.ing.com/pki.

6.1.5 Key sizes

All End-User Key Pairs shall have a minimum size of 1024 bit RSA.

All EV SSL Certificates will have a minimum size of 2048 bit RSA.
All Key Pairs for CA's will have a minimum size of 2048 bit RSA.
The minimum key sizes will be periodically reviewed, with a minimum of once a year, to judge their appropriateness for securing communications.

6.1.6 Hardware/Software key generation

All Key Pairs are generated in a hardware cryptographic module.

6.1.7 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 CA's may only be used to sign Certificates and CRL's.

Private Keys issued to personnel serving in Trusted Roles, as defined in section 5, may be used only for such purposes. If required, personnel shall be issued sets of End-User keys and Certificates to be used for purposes other than in the performance of the duties defined for the Trusted Role.

6.2. Private Key Protections

Private Keys must be stored on a Smart Card or, in case of a Soft Certificate, a protected network location owned and managed by ING. Access to Private Keys is restricted and requires Activation Data only submitted to the associated End-User.

6.2.1 Standards for cryptographic module

All cryptographic operations of CA's 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. All End-User software tokens are rated to at least FIPS 140-1 Level 1 or otherwise verified to an equivalent level of functionality and assurance.

6.2.2 Private Key (n out of m) multi-person control

Three (3) person-control is required for access to the ING PKI Root. Two (2) person-control is required for access to all CA signing keys. One (1) person control is permitted for all other keys.

6.2.3 Private Key escrow

Each CA supports escrow of private decryption keys where required by law. Signing keys for Non-repudiation will not be escrowed.

6.2.4 Private Key backup

All Key Pairs will be backed-up, excluding signing keys. 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.

From the Root CA en sub-CA's all keys will be backed-up.

6.2.5 Private Key archival
All Key Pairs used for encryption may be archived to support optional key recovery services, excluding signing keys. Each CA provides for the recovery of an archived private decryption key upon request by the End-User or the associated Customer following authentication in accordance with section 3.

6.2.6 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, except for Private Keys to be used with Roaming Certificates. Such keys, although generated in an HSM, can be retrieved for export to a Directory which is remotely accessible.

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.

6.2.7 Method of activating Private Key
The Private Key shall be protected from exposure and unauthorised usage by End-User specific Activation Data. Each invocation of an algorithmic function requires insertion of the Activation Data associated with the Key Pair.

End user cryptographic modules shall lock themselves after three consecutive failed attempts at inserting the correct Activation Data. In such case, the cryptographic module can only be unblocked by ING upon a formal request of the End-User. For authentication of such a request, the same procedure applies as that used for Suspension or Revocation.

6.2.8 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.

6.2.9 Method of destroying Private Key
Upon termination of the usage of a CA's 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 area, with physical and procedural controls in accordance with section 5. The log of the personalisation system shall contain a reference to the order, and list the corresponding chip numbers, Smart Card numbers, and Certificates.

6.3.1 Public Key archival
Not stipulated.

6.3.2 Usage periods for the public and Private Keys
- Key Pairs used to perform CA functions have a maximum validity of twenty (20) years
- Key Pairs used for Extended Validation SSL Certificates will have a maximum validity of fourteen (14) months, according to the WebTrust EV Criteria
- All other Key Pairs will have a maximum validity of five (5) years.

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 PKI, they may be revoked and reissued at any time before their expiry.

6.4. Activation Data
A PIN protecting the usage of Key Pairs contains at least five (5) digits and will be delivered to End-Users in accordance with the applicable CP.

Unblocking codes for cryptographic tokens consist of at least five (5) digits and will be securely stored by ING.

6.4.1 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.

6.4.2 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.

6.4.3 Other aspects of Activation Data
No stipulation.

6.5. Computer Security Controls

6.5.1 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
- dentification and authentication of Trusted Roles and associated identities
- Use of cryptography for session communication and database security
- Archival of CA and End-User 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.

6.5.2 Computer security rating

No stipulation.

6.6. Life Cycle Technical Controls

6.6.1 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.

6.6.2 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.

6.6.3 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 6.2.1 and 6.6.1.

7. Certificate and CRL Profiles

7.1. Certificate Profile

Certificates issued under this CPS are constructed according to X.509 and the PKIX Certificate profile (RFC2459).
The Certificate profile per type of Certificate is determined by the applicable CP.

7.1.1 Version number(s)

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

7.1.2 Certificate extensions

Certificate extensions are processed in accordance with RFC2459.

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. Private extensions are not used.

7.1.3 Algorithm object identifiers

7.1.3.1 Signature Algorithm OID
For signatures, either SHA-1 hashing with RSA Encryption (OID 1.2.840.113549.1.1.5) or SHA-2 hashing with RSA Encryption (OID 1.2.840.113549.1.1.11) is being used.

7.1.3.2 Encryption Algorithm OID
For encryption, the RSA algorithm (OID 1.2.840.113549.1.1.1) is being used.

7.1.4 Name forms

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

7.1.5 Name constraints

Each distinguished name (DN) of an ING PKI Certificate Subject includes 'O = ING'.

7.1.6 Certificate Policy Object Identifier

See section 1.3.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

Each CA populates the policy qualifiers extension with a general disclaimer and reference to the URL and e-mail address through which the CP, this CPS and other related documents can be obtained. The user notice extension will be populated with the text described in Section 1.3.

7.1.9 Processing semantics for the critical Certificate policy extension

See section 1.5.

7.2. CRL Profile

7.2.1 Version number(s)

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

7.2.2 CRL and CRL entry extensions

All software within the ING PKI correctly processes CRL extensions as specified in RFC2459.

8. Specification Administration

8.1. Specification change procedures

8.1.1 Items that can change without notification

Typographical corrections may be made to this CPS, the CP's and the ING PKI Glossary without prior notification of End-Users and without creating a new version.

Editorial changes may be made to this CPS, the CP's and the ING PKI Glossary without notification of End-Users and with creating a new version, insofar as the changes don't materially affect the contents of this CPS.

8.1.2 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, the CP's and the ING PKI Glossary 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 8.1.2 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.

All changes as referred to in 8.1.1. may be made without the implicit or explicit approval of 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 (1) week after the notification date.

8.3. Applicability and acceptance of changes

All changes to this CPS shall become effective one (1) 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

[ABA] American Bar Association, Electronic Commerce Division: **PKI Assessment Guidelines**, PAG v0.30, Public Draft for Comment. June 18, 2001

[CARAT] National Automated Clearing House Association (NACHA), The Internet Council, Certification Authority Rating and Trust (CARAT) Task Force: **CARAT Guidelines**, Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates. January 14, 2000

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

[PKIFOR] J. Sabo, Y. Dzambasov, **PKI Policy White Paper**, PKI Forum, March 2001. Available online at http://www.pkiforum.org/resources/.

[POVER] B. Albert, **ING PKI Overview**, ING PKI Programme Document, March 2002.

[RFC2510] C. Adams, S. Farrell. **Internet X.509 Public Key Infrastructure Certificate Management Protocols**, Internet Engineering Task Force (IETF) RFC 2510, Security Area, Public-key Infrastructure (X.509) working group, March 1999. Available online at http://www.ietf.org/rfc/rfc2510.txt.

[RFC2511] M. Myers, C. Adams, D. Solo, D. Kemp. **Internet X.509 Certificate Request Message Format**, Internet Engineering Task Force (IETF) RFC 2511, Security Area, Public-key Infrastructure (X.509) working group, March 1999. Available online at http://www.ietf.org/rfc/rfc2511.txt.

[RFC2527] S. Chokhani, W. Ford, **Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework**, Internet Engineering Task Force (IETF) RFC 2527, Security Area, Public-key Infrastructure (X.509) working group, March 1999. Available online at http://www.ietf.org/rfc/rfc2527.txt.

[RFC2459] R. Housley, W. Ford, W. Polk, and D. Solo, **Internet X.509 Public Key Infrastructure Certificate and CRL Profile**, Internet Engineering Task Force (IETF) RFC 2459, Security Area, Public-key Infrastructure (X.509) working group, January 1999. Available online at http://www.ietf.org/rfc/rfc2459.txt.

[RFC2560] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, **X.509 Internet Public Key Infrastructure Online Certificate Status Protocol** – OCSP Profile, Internet Engineering Task Force (IETF) RFC 2460, Security Area, Public-key Infrastructure (X.509) working group, June 1999. Available online at http://www.ietf.org/rfc/rfc2460.txt.

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

More information

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

ING