ING Public Key Infrastructure Glossary

Version 5.4 - November 2015

Term	Definition
Acceptance	The action of demonstrating approval of a Certificate while knowing or having notice of its informational contents. Among others, usage of a Certificate demonstrates approval of that Certificate's contents.
Activation Data	Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a pass phrase, or a manually-held key share).
Application	A computer program or set of computer programs implementing business processes (e.g. banking, insurance or management information functions).
Application Agreement	The overall agreement between ING Bank NV and an ING Entity in which the relation between the two parties is stipulated, based on which the ING Entity will be using the ING PKI services.
Associate	A person working for ING within our regulation (following our internal ING rules). The person is employed by ING, or contracted by ING or employed or contracted by a subcontractor of ING and assigned to work for ING within our regulation. • Also see 'Employee'
Audit	A procedure used to validate that controls are in place and adequate for their purposes.
Authentication	A process used to confirm the identity of a person or to prove the integrity of specific information.
Biometrics	Authentication techniques that rely on biological phenomena, such as the individual characteristics of a person's finger, hand or eye geometry.
CA (Certification Authority)	An entity that is responsible for the generation, issuance, management, Suspension and Revocation of Certificates.
CA System	All hardware and software used to support the issuance or management of Certificates and keys, including any workstations, cryptographic hardware modules, Smart Cards and storage media.
Certificate	The Public Key of an End-User and his identifying information rendered un-forgeable by encoding with the Private Key of a Certification Authority.
Certificate Policy (CP)	A named set of rules that indicates the applicability of a Certificate to a particular community and/or class of Application with common security requirements.
Certificate Revocation List (CRL)	A list of Certificates that have an inactive status due to Suspension or Revocation, signed by the Certification Authority.
Certificate Subject	A person or entity that has its Public Key and identity certified in a Certificate by a Certification Authority.
Certification Path	An ordered sequence of Certificates which, together with the Public Key of the initial object in the path, can be processed to obtain that of the final object in the path, the Root.
Certification Practice Statement (CPS)	A statement of the practices, processes and procedures which a Certification Authority employs in delivering its services.
Cipher text	Data that has been encrypted in order to protect the Confidentiality of its contents.
Code of Conduct	A set of rules describing a specific type of appropriate behaviour.
Communication	All exchanges of information between two or more parties, independent of the medium used.
Confidential Information	All information that is exchanged between parties and that at the time of exchange was not public knowledge or publicly available, nor already in possession of or known to the receiving party.
Confidentiality	The condition in which data is kept secret and disclosed only to authorized parties.
Term (ctd – I)	Definition (ctd – I)
Cross-certification	A condition in which a Certification Authority within the ING PKI and one outside the ING PKI issues a Certificate having the other as the Certificate Subject.
Cryptography	Mechanisms and practices used to encode data for security purposes.
Customer, ING Customer	An ING entity that requests provision of ING PKI services from ING Bank NV and that is as such identified in the Application Agreement. When 'Customer' is written in any ING PKI documentation, always ING Customer is meant. • Also see 'End-user'
Customer, Commercial Customer	A Customer of an ING Entity that will be using the ING PKI in combination with an Application of that specific ING Entity. When a Commercial Customer is meant in any ING PKI documentation, this is always written in full ('Commercial Customer') • Also see 'Customer, ING Customer'
Data	Programs, files, and other information stored in, communicated, or processed by a computer.
Decryption	The process of turning cipher text back into plaintext.
Delegated Registration Authority Officer (DRAO)	The security officer who is appointed to perform the user management of those who want to make use of an ING Certificate, either Customer or Employee.
Digital Signature	A digital code attached to an electronic Communication that distinctly identifies the sender of that Communication and confirms that its contents have not been altered during transmission.

Directory A look-up table within an electronic storage environment.

Distinguished Name A globally unique Identifier representing an identity.

Employee A person working for ING within our regulation (following our internal ING rules). The person is employed by ING, or contracted by ING or employed (contracted by a subcontractor of ING) and assigned to work for ING within our regulation.
- Also see 'Associate'

Encryption The scrambling of data for Confidentiality purposes; a practice that allows only intended recipients to decode information.

End-User A person or entity who or which will be using the Certificate.

EV Certificates (Extended Validation certificates) Extended Validation Certificates (EV) are a special type of X.509 certificate which requires more extensive investigation of the requesting entity by the Certificate Authority before being issued. The criteria for issuing EV certificates are defined by the Guidelines for Extended Validation Certificates, currently at version 1.1. The guidelines are produced by the CA/Browser Forum, a voluntary organization whose members include leading CAs and vendors of Internet software, as well as representatives from the legal and audit professions.

Expiry Date The time and date specified in the Certificate when the operational period of that Certificate ends.

Extension Field in an X.509v3 Certificate that provides methods for associating additional attributes with End-Users or Public Keys and for managing the certification hierarchy.

Hardware Security Module A tamper-proof processing and storage device.

Help Desk A support entity supplied by ING Bank NV for the suspension of Certificates.

Identifier A string of bits or characters that names an entity, such as a person, program, or device.

Term (ctd – II) Definition (ctd – II)

ING All legal entities that are part of the group of companies of ING Group.

Integrity A condition in which data has not been altered or destroyed in an unauthorized manner

Intellectual Property Rights All patents, trademarks, trade name rights, database rights, copyright, model rights, design rights, know-how and other legal claims to intellectual property.

Key Pair The Private Key and the corresponding Public Key.

Non-repudiation The inability to deny the transmission and/or contents of an electronic Communication.

Object Identifier (OID) An Identifier representing a given object.

Personalization The process by which specific information – such as Applications and personal information – are loaded onto a Smart Card.

Plaintext Data that has not been encrypted and that is therefore readable by human beings.

Policy Qualifier Policy-dependent information that accompanies a Certificate Policy Identifier in an X.509 Certificate.

Power of Attorney Formal document stating the legal authority of one or more parties.

Private Key That key of an End-User's Key Pair which is known only by that End-User.

Public Key That key of an End-User's Key Pair which is publicly known and which is included in the Certificate.

Public Key Infrastructure (PKI) A system that uses Signing and Encryption techniques to provide trust services based on certification of asymmetrical Key Pairs.

RA System All hardware and software used to support the validation and requesting of Certificates and keys, including any workstations, cryptographic hardware modules, Smart Cards and storage media.

Registration Authority (RA) An entity that is responsible for identification and authentication of Certificate Subjects.

Registration Authority Officer (RAO) The security officer who is appointed to perform the user management of the DRAO's.

Regulation The possibility to give instruction how the work needs to be carried out, and to sanction this.

Relying Party An entity who acts in reliance on a certificate.

Repository A Directory for storing and retrieving Certificates and other related information such as Certificate Revocation Lists.

Revocation Designating a Certificate as permanently invalid.

Roaming Certificate A Certificate of which the Private Key is stored in an online Directory, enabling the End-User to securely access the Private Key from any remote location.

Root A Certification Authority with a self-signed Certificate that forms the single trust foundation for a PKI.

Smart Card A plastic card with an embedded integrated circuit which offers memory and micro-processing capabilities and that possesses some inherent resistance to tampering.

Smart Card Reader Hardware capable of activating and interfacing with a Smart Card for purpose of data exchange.

Software Token Software that stores or generates Public and Private Keys.

Suspension Designating a Certificate as temporarily invalid, with the option of restoring its active status within the initial Validity term.

Terms and Conditions A set of legal requirements and/or restrictions applicable to the delivery of selected ING PKI services.

Term (ctd – III) Definition (ctd – III)

Trusted Registrar A person who requests Certificates on behalf of an organisation or organisational unit.

Trusted Role All Employees with access to or control over cryptographic operations that may materially affect the issuance, use, suspension, or revocation of Certificates.

Validity The fatal term within which a Certificate can be used.

Validation The process that checks if a Certificate is still valid or not.

X.509 The ITU-T standard for Certificates.

X.509v3 The ITU-T standard for Certificates containing or capable of containing extensions.