



The World Internet Security Company

**Solutions for Security**

# **WIS@key CertifyID Product Glossary**

Date: October 2007  
Version: 0.1.2  
Authors: WIS@key SA

## Terminologies Used in the WISeKey Product Documentation

The following table lists the meaning of key terms used in User Guides of WISeKey CertifyID Products.

Term	Description
Access Control	Refers to the practice of restricting access to a system, resource, or physical area to authorized entities.
Applicant	The entity that has applied to be issued a certificate within the WISeKey PKI. The verification processes vary in accordance with the nature and, where applicable, the operational role within the PKI corresponding to the certificate the entity is applying.
Archive	To store records and associated journals for a given period of time for security, backup, or auditing purposes.
Asymmetric Algorithm	Asymmetric algorithms are algorithms used in cryptography that use two different keys to encrypt and decrypt the plaintext. The two keys are related mathematically; a message encrypted by the algorithm using one key can be decrypted by the same algorithm using the other.
Asymmetric Key Pair	A pair of cryptographically related keys, the private key and public key as used in public-key cryptography.
Audit	Audit is defined as a review and examination of system records and activities to assess the adequacy and effectiveness of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Audit Event	An action, detected internally by the system which may generate an audit record. If an event causes an audit record to be generated [for recording in the audit trail], it is a "recorded event". Otherwise, it is an "unrecorded event". The set of audit events is based upon a system's security policy.
Audit Level	A series of requirements and regulations associated with Policy Types as provided in this CPS against which a specific certification services providers are audited.
Audit Record	The discrete unit of data recorded in the audit trail on the occurrence of a recorded event.
Authentication	A process used to confirm the identity of a person or to prove the integrity of specific information.
Authorization	The granting of rights, including the ability to access specific information or resources.
Availability	The property of information being accessible and usable upon demand by an authorised entity or process.
Backup	The process of copying critical information, data and software for the purpose of recovering essential processing back to the time the backup was taken.
Certificate	Also referred to as a Digital Certificate. It is a data structure, using the CCITT ITU X.509 standard, containing the public key of an entity, together with associated information, and rendered

	un-forged by being digitally signed by the Certification Authority which issued it.
Certificate Chain	A chain of multiple certificates needed to validate a certificate. Certificate chains are built by linking and verifying the digital signature on a certificate with a public key on a certificate issued by the a Root Certification Authority, such as the OISTE WISeKey Root CA.
Certificate Expiration	The time and date specified in the Digital Certificate when the operational period ends, without regard to any earlier suspension or revocation.
Certificate Extension	An extension field to a Digital Certificate which may convey additional information about the public key being certified, the certified subscriber, the Digital Certificate issuer, and/or the certification process. Standard extensions are defined in Amendment 1 to ISO/IEC 9594- 8:1995 (X.509). Custom extensions can also be defined by communities of interest.
Certificate Generation	Certificate generation is the process of creating a certificate from inputs specific to the application and the user.
Certificate Management	Certificate management includes, but is not limited to, storage, distribution, dissemination, accounting, publication, compromise, recovery, revocation, suspension and administration of Digital Certificates. A Certification Authority designates issued and accepted Digital Certificates as valid by publication.
Certificate Policy (CP)	A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of mobile communication transactions for the trading of goods within a given price range.
Certificate Request	Authenticated request by an entity for its parent authority to issue a certificate which binds the identity of that entity to its public key.
Certificate Revocation	Certificate revocation is the process of changing the status of a certificate from valid or suspended to revoked. The status of a certificate as revoked means that it should not longer be relied upon by any entity for whatever purpose.
Certificate Revocation List	A signed list of the certificates which have been revoked by a CA.
Certificate Serial Number	A value that unambiguously identifies a Digital Certificate generated by a Certification Authority.
Certification / Certify	The process of issuing a Digital Certificate by a Certification Authority.
Certification Authority (CA)	An authority trusted by one or more users to create, issue and manage the life-cycle of certificates.
Certification Practice Statement (CPS)	A statement of the practices which a certification authority employs in issuing certificates and managing the life-cycle of such certificates.
Certification Services	Any of the services that can be provided in relation to the lifecycle management of certificates at any level of the PKI hierarchy, including ancillary services such as OCSP services, time-stamping services, identity verification services, CRL hosting, etc.
Compliance Audit	A review and examination of system records and activities in

	order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred.
Computer Data Base	Means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network.
Confidentiality	Ensuring that information is accessible only to those authorized to have access.
Controls	Measures taken to ensure the integrity and quality of a process.
Critical Information	Data determined by the data owner as mission critical or essential to business purposes.
Cross-Certificate	A Certificate used to establish a trust relationship between two Certification Authorities.
Cryptographic Algorithm	A clearly specified mathematical process for computation; a set of rules that produce a prescribed result.
Cryptographic Key	A parameter used in conjunction with an algorithm for the purpose of validation, authentication, encipherment or decipherment.
Cryptography	The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use.
Data Integrity	The quality or condition of being accurate, complete and valid, and not altered or destroyed in an unauthorised manner.
Data Security	The practice of protecting data from accidental or malicious modification, destruction, or disclosure.
Digital Certificate	A digital certificate is a data structure used in a public key system to bind an authenticated individual to a particular private key. See also Certificate.
Digital Signature	Data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.
Distinguished Name	A set of data that identifies a real-world entity, such as a person in a computer-based context.
Document	A record consisting of information inscribed on a tangible medium such as paper rather than computer-based information.
Electronic Form	With reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro-film, computer generated micro fiche or similar device.
Electronic Mail (E-Mail)	Messages sent, received or forwarded in digital form via a computer-based communication mechanism.
Electronic Record	Means data, record or data generated, image or sound stored, received or sent in an electronic form or computer readable form.

Encryption	The process by which plain text data are transformed to conceal their meaning. Encryption is a reversible process affected by using a cryptographic algorithm and key.
End User	These are entities (legal, natural, mechanical or electronic) that have been issued certificates within a PKI but are not subordinate PKI entities.
Entity	Any person (legal or natural) or system (mechanical or electronic).
Evaluation	Assessment against defined criteria in order to give a measure of confidence it meets the corresponding requirements.
Extensions	Extension fields in X.509 v3 certificates.
File Transfer Protocol (Ftp)	The application protocol that offers file system access from the Internet suite of protocols.
Generation of Key Pair	A trustworthy process of creating private keys during Digital Certificate application whose corresponding public keys are submitted to the applicable Certification Authority during Digital Certificate application in a manner that demonstrates the applicant's capacity to use the private key.
Hard Copy	A copy of computer output that is printed on paper in a visually readable form; e.g. printed reports, listing, and documents.
Hash (Hash Function)	An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that : i) A message yields the same result every time the algorithm is executed using the same message as input. ii) It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm. iii) It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.
Identification information	The information obtained or presented to positively identify an entity and provide the certification services requested by it.
Identity	A unique piece of information that marks or signifies a particular entity within a domain. Such information is only unique within a particular domain.
Information	Includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro-film or computer generated micro fiche.
Information Assets	Means all information resources utilized in the course of any organisation's business and includes all information, application software (developed or purchased), and technology (hardware, system software and networks).
Information Technology Security	All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, authenticity, and reliability.
Information Technology Security Policy	Rules, directives and practices that govern how information assets, including sensitive information, are managed, protected and distributed within an organization and its Information Technology systems.
Interoperability	Interoperability implies that equipment and procedures in use by two or more entities are compatible, and hence that it is possible to undertake common or related activities.
Key	A sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature generation,

	or signature verification).
Key Archiving	Key archiving is the process of storing used key or their ID, and/or certificates as a record in long term storage for future retrieval.
Key Destruction	Key destruction is the process of removing all copies of a key throughout the key management system.
Key Generation	Key generation is the process by which cryptographic keys are created. It is the function of generating variables required to meet particular key attributes.
Key Management	The administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy.
Key Pair	The keys in an asymmetric cryptosystem having the property that one of the pair will decrypt what the other encrypts.
Message	A digital representation of information; a computer-based record.
Name	A set of identifying attributes purported to describe an entity of a certain type.
Non-Repudiation	Provides proof of the origin or delivery of data in order to protect the sender against a false denial by the recipient that the data has been received or to protect the recipient against false denial by the sender that the data has been sent. Note: Only a trier of fact (someone with the authority to resolve disputes) can make an ultimate determination of non-repudiation. By way of illustration, a digital signature verified pursuant to this Certification Practice Statement can provide proof in support of a determination of non-repudiation by a trier of fact, but does not by itself constitute non-repudiation.
OCSP	A protocol which is used to provide real-time validation of a certificate's status. An OCSP responder is used to respond to certificate status requests and can issue one of three responses: Valid, Invalid, and Unknown. An OCSP responder replies to certificate status requests on the basis of CRLs (Certificate Revocation Lists) provided to it by certification authorities.
OCSP Request	An OCSP Request contains the following data: protocol version, service request, target certificate identifier, optional extensions which may be processed by the OCSP Responder
OISTE WISeKey Root CA (OWRCA)	It is the apex of the PKI hierarchy which is provided by the OISTE WISeKey Root within the OISTE WISeKey Root PKI.
OISTE WISeKey PKI	It is the public key infrastructure made up of the OISTE WISeKey Root CA and the CAs subordinated to it.
Operational Infrastructure	The technological infrastructure by which the certification services are provided. This infrastructure does not necessarily coincide with the legal infrastructure or relationships that exist or that develop between entities that form part of the WISeKey PKI or that use the WISeKey PKI certification services in any way.
Password (Pass Phrase; PIN Number)	Confidential authentication information usually composed of a string of characters used to provide access to a computer resource.
Physical Security	The measures used to provide physical protection of resources against deliberate and accidental threats.
PKI (Public Key Infrastructure)	The infrastructure needed to generate, distribute, manage and archive keys, certificates and certificate revocation lists, and

	OCSP responders.
Policy Certification Authority	A Certification Authority that has been issued its CA certificate by the Root Certification Authority, and designated by the Policy Approval Authority as a Policy Certification Authority..
Post-Suspension Investigation	Investigation performed by the WPAA after a certificate has been suspended in order to determine whether such certificate should be revoked or reinstated as valid.
Private Key	The key of an entity's asymmetric key pair which shall normally only be known by that entity.
Proxy Server	A proxy server operates between a client application (e.g. web browser) and a destination server. The proxy intercepts all requests to the destination server to see if it can fulfill the request itself. If it cannot, it forwards the request to the destination server.
Public Key	The key of an entity's asymmetric key pair which can be made public, although not necessarily available to the public in general, as it may be restricted to a pre-determined group.
Public Key Certificate	A digital certificate that binds un-forgeably the public key of an entity to the entity's distinguishing identifier, and which indicates a specific validity period.
Recipient (of a Digital Signature)	The entity that gets (receives or retrieves) a message.
Registration Authority	An entity whose purpose is to provide local support to a set of Subordinate PKI Entities or End Users that are physically far from their immediate superior certification authority. A Registration Authority performs a subset of the functions available to a certification authority administrator responsible for directly managing a set of Subordinate PKI Entities and End Users. The functions of Registration Authorities within the WISeKey PKI are provided for under § 1.3 of this CPS and under the corresponding CPS of its parent ACA.
Rekey	The act of replacing an expired Certificate by providing a new set of keys.
Rely / Reliance (on a Certificate and Digital Signature)	To accept a digital certificate or signature
Relying Party	Any entity relying on a certificate that: (1) has agreed to a Relying Party Agreement within the WISeKey PKI or other similar agreement containing Relying Party provisions within the WISeKey PKI or (2) is designated as such by an approved Certificate Policy, despite not having signed a Relying Party agreement.
Renewal	The process of obtaining a new Digital Certificate of the same class and type for the same subject once an existing Digital Certificate has expired.
Repository	A Certificate Repository is a database of Digital Certificates and other relevant information accessible on-line.
Repudiation	The denial or attempted denial by an entity involved in a communication of having participated in all or part of the communication
Responder	In an OCSP context, a Responder is generally a reference to an OCSP Server. An OCSP Server can be contacted to obtain the revocation status of certificates
Revoke A Certificate	The act of changing the status of a valid or suspended certificate to "Revoked" from a specified time and forward

Root	The CA that signs its own certificate, and is the first certificate in a certificate chain. The root's public key must be known in advance by a certificate user in order to validate a certificate chain. The root's public key is made trustworthy by some mechanism other than a certificate, such as by secure physical distribution.
RSA	A public key cryptographic system invented by Rivest, Shamir & Adelman.
S/MIME	A specification for E-mail security exploiting cryptographic message syntax in an Internet MIME environment.
Security	The quality or state of being protected from unauthorized access or uncontrolled losses or effects. Absolute security is impossible to achieve in practice and the quality of a given security system is relative. Within a state-model security system, security is a specific "state" to be preserved under various operations.
Security Policy	A document which articulates requirements and good practices regarding the protections maintained by a trustworthy system.
Self-Signed Public Key	A data structure that contains a Public Key that has been signed by its corresponding Private Key.
Sign	To create a digital signature for a message, or to affix a signature to a document, depending upon the context.
Signer	A person who creates a digital signature for a message, or a signature for a document.
Smart Card	A hardware token that incorporates one or more integrated circuit (IC) chips to implement cryptographic functions and that possesses some inherent resistance to tampering.
Subject (of a Certificate)	The holder of a private key corresponding to a public key. The term "subject" can refer to either the equipment or device that holds a private key and to the individual person, if any, who controls that equipment or device. A subject is assigned an unambiguous name, which is bound to the public key contained in the subject's Digital Certificate.
Subject Name	The unambiguous value in the subject name field of a Digital Certificate, which is bound to the public key.
Subordinate PKI Entity	Any entity that has the authority to operate or provide certification services under the OISTE WISeKey Root PKI. Natural persons may not be Subordinate PKI Entities under the WISeKey Root CA.
Subscriber Agreement	The agreement executed between a subscriber and a Certification Authority for the provision of designated public certification services in accordance with this Certification Practice Statement.
Summary Information	The basic information required for the production of a public key certificate, for the verification of a digital signature, for the validation of a certificate's status as well as the information produced as a result of such verification and validation.
Suspend a Certificate	A temporary "hold" placed on the effectiveness of the operational period of a Digital Certificate without permanently revoking the Digital Certificate. A Digital Certificate suspension is invoked by, e.g., a CRL entry with a reason code.
Time Stamp	A notation that indicates (at least) the correct date and time of an action and identity of the person or device that sent or received the time stamp.

Token	The medium in which a key is stored (e.g. smart card, cryptographic key).
Trust	Generally, the assumption that an entity will behave substantially as expected. Trust may apply only for a specific function. The key role of this term in an authentication framework is to describe the relationship between an authenticating entity and a Certification Authority. An authenticating entity must be certain that it can trust the Certification Authority to create only valid and reliable Digital Certificates, and users of those Digital Certificates rely upon the authenticating entity's determination of trust.
Trusted Third Party	In general, an independent, unbiased third party that contributes to the ultimate security and trustworthiness of computer-based information transfers. A trusted third party does not connote the existence of a trustor-trustee or other fiduciary relationship.
Uniform Resource Locator (URL)	A standardized device for identifying and locating certain records and other resources located on the World Wide Web.
User	An authorized entity that uses a certificate as applicant, subscriber, recipient or relying party, but not including the Certification Authority issuing the Digital Certificate.
Valid Certificate	A Digital Certificate issued by a Certification Authority and accepted by the subscriber listed in it which is neither expired nor revoked/suspended.
Validate a Certificate	The process of checking the validity of a Certificate in terms of its status (i.e. suspended or revoked), and its certificate chain.
Verify (a Digital Signature)	A process which takes as input the signed message, the verification key and the domain parameters, and which gives as output the result of the signature verification: valid or invalid.
Web Browser	A software application used to locate and display web pages.
World Wide Web (WWW)	A hypertext-based, distributed information system in which users may create, edit, or browse hypertext documents. A graphical document publishing and retrieval medium; a collection of linked documents that reside on the Internet.
X.509	The ITU-T (International Telecommunications Union-T) standard for Digital Certificates. X.509 v3 refers to certificates containing or capable of containing extensions.