

Annex 0.5.2 – ABBREVIATIONS AND TERMS – PKI

Table 1 – ABBREVIATIONS

Abbreviation	Meaning
CA	Certification Authority
CARL	Certificate Authority Revocation List
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
BCA	Bridge Certification Authority
IPKI	Israel Public Key Infrastructure
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
OID	Object Identifier
PCA	Principal CA
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-1	Secure Hash Algorithm, Version 1
S/MIME	Secure Multipurpose Internet Mail Extension
SST	Secure Sockets Layer
URL	Uniform Resource Locator

Table 2 – Glossary of Terms

Term	Description
Access	The ability to make use of any information system (IS) resource.
Access Control	Process of granting access to information system resources only to authorized users, programs, or other systems.
Accreditation	Formal declaration by a designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Agency	Any department or subordinate element of a department, or independent organizational entity that statutorily or constitutionally is recognized as being part of Israeli Government.
Agency CA	A CA that acts on behalf of an agency, and is under the operational control of an agency.
Applicant	An organ, after applying to a Certification Authority for a certificate, but before the certificate issuance procedure is completed.
Attribute Authority	An entity recognized by the IPKI, as having the authority to verify the association of attributes to an entity.
Authenticate	To confirm the identity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, messages, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
Biometrics	A physical or behavioral characteristic of a human being.
Certificate	A digital representation of information which at least (1) identifies the Certification Authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARL' s or CRL' s.
Certification Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.

Term	Description
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to subscribers.
Certificate Policy (CP)	A Certificate Policy is a specialized form of an administrative policy tuned to electronic transaction performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communication system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements.
Certificate - Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates, which it has issued that are revoked prior to their stated expiration date.
Certificate Status Authority	Trusted entities that provide on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities.

Term	Description
Data Integrity	Assurance that the data is unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
Duration	A field within a certificate which is composed of two sub-fields; "date of issue" and "date of expiration".
Employee	Any person employed by an Agency as described above.
Integrity	Protection against unauthorized modification or destruction of information. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intermediate CA	A CA that is subordinated to another CA, and has a CA subordinated to itself.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement.
Key Exchange	The process of exchanging public keys in order to establish secure communication.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (2) even knowing one key, it is computationally infeasible to discover the other key.
Local Registration Authority (LRA)	A Registration authority with responsibility for a local community.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Naming Authority	An organizational entity responsible for assigning distinguished names (DN' s) and for assuring that each DN is meaningful and unique within its domain.
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny

Term	Description
	having processed the data.
Policy Management Authority (PMA)	Body established to oversee the creation and update of certificate policies, review Certification practice Statements, review the result of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
Principal CA	The Principal CA is a CA designated by an Agency to inter-operate with the BCA.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain and revoke key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Re-Key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally involves issuing a new certificate on the new public key.
Relying Party	A person or Agency who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates; may also be referred to as a “directory”.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specified date and time.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than

Term	Description
	encrypting data or performing any other cryptographic functions.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See also Superior CA).
Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) hold a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificate to another party. This includes, but is not limited to, an individual or a network device.
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See also Subordinate CA).
Update (a certificate)	The act of process by which data items bound in an existing key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.