



Baltimore Certificates On-Line

CAPL - 007 (GL – TE) - Glossary of Terms

Information in this document is subject to change without notice.

No part of it may be copied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior written permission from Certificates Australia Pty Limited.

Written and published in Sydney, Australia, by Baltimore Certificates Australia Pty Limited.

Copyright © 2000, Baltimore Certificates Australia Pty Limited,
ACN 075 8788 67.

All Rights Reserved.

Table of Contents

PURPOSE OF PAPER	3
Amendment procedure.....	3
References.....	3
GLOSSARY of TERMS	4

IMPORTANT NOTE ABOUT THIS DOCUMENT

The information contained in this document is intended for personnel charged with the management and operation of the Certification Authorities owned and operated as Baltimore Certificates Australia Pty Ltd (CAPL), those persons named as recipients or those persons nominated in the circulation list.

It may contain privileged and confidential information and if you are not the intended recipient you must not copy, distribute or take any action in reliance on it.

If you have received this document in error, please notify the author immediately by reverse charge telephone call and return the original to the sender by mail. You will be reimbursed for postage.

This policy document has been produced in accordance with the general provision of the Commonwealth's policy and guidelines on the protection of information and information technology environments.

Contact:

General Manager – BCOL
Baltimore Certificates Australia Pty Ltd
Level 5, 1 James Place
NORTH SYDNEY NSW
AUSTRALIA
Ph +61 2-9409-0300

The presence of the signature below indicates that personnel charged with operating the Certification Authority Services on behalf of CAPL will abide by the policies contained herein.

PURPOSE OF PAPER

The purpose of this document is to provide definitions to terms used throughout the entire CAPL documentation suite. These definitions are based on:

- ISO Glossary of IT Security Technology; and,
- GPKA Glossary of Terms.

The definitions in the CAPL documentation suite differ from these glossaries only in so far as it is necessary for clarity within the framework of the CAPL PKI hierarchy.

Amendment procedure

As new standards emerge, or policy matters are identified for improvement, this policy will be amended.

The responsibility for amending this document rests with the General Manager – BCOL. The naming convention for amendment notices shall be:

YY indicating the year the amendment was issued;

XXX where XXX represents a sequential number beginning with 000.

References

- Glossary of IT security terminology prepared by JTC1 SC 27 at <http://www.iso.ch:8080/jtc1/sc27/27sd698a.htm>
- Government Public Key Authority web site at <http://www.govonline.gov.au/>

GLOSSARY OF TERMS

Term or Acronym	Explanatory notes
Access	Obtaining knowledge or possession of classified material, or access to a designated secure area.
Access control list*	A list of entities, together with their access rights, which are authorised to have access to a resource.
Access control*	The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner.
Accountability*	The property that ensures that the actions of an entity may be traced uniquely to the entity.
Accredited Documents	<p>The documentation set required to be evaluated in order to achieve Gatekeeper Accreditation. These include the following:</p> <ul style="list-style-type: none"> • Concept of Operations (Public) • Privacy Policy (Public) • Business Continuity Policy (Public) • Certificate Practice Statement (Public) • CAPL RCA Certificate Policy (Public) • Information Systems Security Policy (Public) • Protective Security Risk Review (Protected) • System Security Plan (Protected) • Contingency and Disaster Recovery Plan (Protected) • Key Management Plan (Protected) • Configuration Baseline (Protected) • CAPLFW1 Firewall Baseline Configuration (Protected)
ACSI	Australian Communications – Electronic Security Instruction.
Administrative Security	Any procedural system that is established to ensure that classified material or valuable asset is protected against loss, damage or unauthorised access.
Adverse Security Assessment	<p>A security assessment in respect of a person that contains:</p> <p>(a) any opinion or advice or any qualification of any opinion or advice, or any information, that is or could be prejudicial to the interests of the person; and;</p> <p>(b) a recommendation that prescribed administrative action be taken or not be taken in respect of the person, being a recommendation the implementation of which would be prejudicial to the interests of the person.</p>

Term or Acronym	Explanatory notes
Agency	<p>(a) a Department of State, or a Department of the Parliament, of the Commonwealth, a State or a Territory;</p> <p>(b) a body corporate or an unincorporated body established or constituted for a public purpose by Commonwealth, State or Territory legislation, or an instrument made under that legislation (including a local authority);</p> <p>(c) a body established by the Governor-General, a State Governor, or by a Minister of State of the Commonwealth, a state or a Territory; or</p> <p>(d) an incorporated company over which the Commonwealth, a State or a Territory exercises control.</p>
Agency Assessment / Recommendation	The final interpretation formulated by the agency of the results of all checking and assessment action – including the ASIO Security Assessment, where sought culminating in a recommendation to the Agency Head or his/her delegate to grant, withhold, continue, rescind, or otherwise vary a proposed or existing security clearance.
Agency Evaluation	The assessment by agency security personnel, prior to submission of any request to ASIO for a Security Assessment, of the results of all checking and character assessment action, with a view to determining in consultation with agency management whether or not to cease all such action, consult with ASIO, and/or proceed with further clearance action, including for DSAPs submitting a request to ASIO for a Security Assessment (with or without a memorandum of information of possible security significance obtained through agency checking action, as deemed appropriate).
Agency Head	Means the head of a Department of State or a Department of the Public Service or the Chief Executive Officer of any other authority or agency of the Australian Government, including the Chief of the Defence Force, and the Chiefs of Staff for the Navy, Army and Air-Force.
Agency Security Advisers	That person nominated by the Agency Head to perform the day-to-day protective security functions within his/her agency.
Agency Security Instructions	Instructions issued by an Agency providing protective security policy and procedural advice to all staff within that agency. These instructions should preferably be issued under the authority of the Agency Head.
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ANAO	Australian National Audit Office
Approved CP	A Certificate Policy that has been evaluated by an Authorised Evaluator and approved by the CEO, NOIE for use within Gatekeeper.
ASIO	The Australian Security Intelligence Organisation.
Asset*	Anything that has value to the organisation.
Assets*	Information or resources to be protected by technical or non technical countermeasures of a TOE.
Assurance*	Confidence that an entity meets its security objectives.
ASVS	Australian Security Vetting Service
Asymmetric authentication method*	A method of authentication, in which not all authentication information is shared by both entities.

Term or Acronym	Explanatory notes
Asymmetric cryptographic technique*	<p>A cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation.</p> <p>NOTE – A system based on asymmetric cryptographic techniques can either be an encipherment system, a signature system, a combined encipherment and signature system, or a key agreement system. With asymmetric cryptographic techniques there are four elementary transformations: sign and verify for signature schemes, encipher and decipher for encipherment systems. The signature and decipherment transformation are kept private by the owning entity, whereas the corresponding verification and encipherment transformation are published. There exist asymmetric cryptosystems (e.g. RSA) where the four elementary functions may be achieved by only two transformations: one private transformation suffices for both signing and decrypting messages, and one public transformation suffices for both verifying and encrypting messages. However, since this is not the general case, throughout this International Standard the four elementary transformations and the corresponding keys are kept separate.</p>
Asymmetric encipherment system*	A system based on asymmetric techniques whose public transformation is used for encipherment and whose private transformation is used for decipherment.
Asymmetric key pair*	A pair of related keys where the private key defines the private transformation and the public key defines the public transformation.
Asymmetric signature system*.	A system based on asymmetric techniques whose private transformation is used for signing and whose public transformation is used for verification.
Authenticated identity*	A distinguishing identifier of a principal that has been assured through authentication.
Authentication	The process whereby a service provider satisfies him/her self to an appropriate level of confidence that a service requester is entitled to the service sought.
Authentication certificate*	A security certificate that is guaranteed by an authentication authority and that may be used to assure the identity of an entity.
Authentication data*	Information used to verify the claimed identity of a subject
Authentication exchange*	<p>(i) A mechanism intended to ensure the identity of an entity by means of information exchange.</p> <p>(ii) Information used for authentication purposes.</p>
Authentication initiator*	The entity that starts an authentication exchange.
Authentication private key	The key used to digitally sign a message.
Authentication public key	The key used to verify a digital signature.
Authentication token (token)*	Information conveyed during a strong authentication exchange, which can be used to authenticate its sender.
Authentication*	The provision of assurance of the claimed identity of an entity.
Authenticity*	The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information.
Authorised	Authorised by the Agency Head or his/her delegate.

Term or Acronym	Explanatory notes
Authorised administrator*	A user to whom authorisation has been granted to perform administrative operations which may affect the enforcement of the TSP.
Authorised Auditor	A person or organisation (including an employee of that organisation) authorised in writing by the CEO, NOIE, to audit the Contractor's ongoing compliance with the Accredited Documents, Criteria and Policies.
Authorised Evaluator	A person or organisation (including an employee of that organisation) authorised in writing by the CEO, NOIE, to evaluate the Contractor's compliance against the Criteria and with the Accreditation Process.
Authorised Third Party	A third party authorised by law to be able to request revocation or suspension of a Certificate. (e.g. A Court of New South Wales)
Authorised user*	A user who may, in accordance with the TSP, perform an operation
Authorisation*	The granting of rights, which includes the granting of access based on access rights.
Background Checking	That activity which is concerned primarily with verification of the personal, family, and other details stated in forms and related documents completed by an individual under consideration for possible employment in a Position of Trust (POT).
Biometrics	Technology that measures a presented human anatomical part and which then compares that against a known measure. E.g. fingerprint comparison.
CA	Certification Authority.
Cabinet Document	Those documents as defined and described in the Cabinet Handbook.
CAPL PKI Hierarchy	The PKI infrastructure which consists of, at its apex the Certificates Australia Pty Limited (CAPL) Root Certification Authority under which subordinate elements identified by Object Identifiers (OID) may exist which in turn may have further subordinate OID.
CAPL X.500 Directory	The repository used by CAPL to store Public Certificates corresponding with Private keys issued by CAs operating within the CAPL PKI Hierarchy. This repository is also used to post CRLs.
CASP	A Certification Authority Service Provider.
CBC	Cipher Block Chaining
CEO, NOIE	The Chief Executive Officer, National Office for the Information Economy
Certificate ¹	A set of information which at least: <ul style="list-style-type: none"> - identifies the Certification Authority issuing the certificate; - unambiguously names or identifies its owner; - contains the owners public key; and - is digitally signed by the Certification Authority issuing it.
Certificate (user certificate)*	The public keys of a user, together with some other information, rendered unforgeable by encipherment with the secret key of the certification authority which issued it.
Certificate of Accreditation	A certificate issued by the GPKA endorsing the holder to provide CA services to users on behalf of an agency.
Certificate Policy Statement (CP)	The suite of policies that support a Certification Authority in generating certificates and the binding of certificates to an individual.
Certificate Practice Statement (CPS)	A statement of the practices that a Certification Authority employs in issuing certificates.

¹ Definition from SAA MP75 (Standards Australia).

Term or Acronym	Explanatory notes
Certificate Revocation List (CRL)	The process of retracting the guarantees associated with a public key pair. In particular the guarantee that the entity and the public key pair are mutually identified bound. Revocation may occur where a public key pair: <ul style="list-style-type: none"> - has been compromised; - has outlived its intended life; - is no longer fit for purpose; - use has been proven to be fraudulent; - at the request of the owner; - in accordance with the policies of the CA
Certificate serial number*	An integer value, unique within the issuing CA (certification authority), which is unambiguously associated with a certificate issued by that CA.
Certificate*	An entity's data rendered unforgeable with the private or secret key of a certification authority.
Certification authority (CA)*	(i) A centre trusted to create and assign public key certificates. Optionally, the certification authority may create and assign keys to the entities. (ii) An authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the user's keys. (iii) A trusted entity that verifies the identity of a user, allocates a Distinguished Name to that user, and verifies the correctness of information concerning that user by signing the data which constitutes the digital signature for that user. ²
Certification Authority Service Provider	A body which has achieved Gatekeeper Accreditation and has been authorised by the CEO, NOIE to supply Certification Authority services.
Certification chain	See Certification path
Certification path*	An ordered sequence of certificates of objects in the DIT (directory information tree) 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
Certification Request	means an electronic document containing the details of the Certificates which are to be created by the CA, completed and digitally signed by the RA, and sent by the RA to the CA.
CGIO	Chief Government Information Officer
Character Assessment	The balanced and informed estimation of an individual's reliability and trustworthiness which is derived from comprehensive checks on identity, background, personal values and behaviour. Checks of Police Records are an integral part of this activity.
Classified Material	Official information which, for reasons of security, requires protection to prevent its being acquired by people, organisations or governments not authorised to receive it. Classified material may be either 'national security' or 'non national security' material.
Commonwealth Contractor	A person performing work or rendering services for a Commonwealth agency, other than as a employee of the agency, including a person performing such services as a sub-contractor or as an adviser or consultant.

² Ibid.

Term or Acronym	Explanatory notes
Communications Security (COMSEC)	All measures applied to the protection of telecommunications from unauthorised interception and exploitation. Communications Security includes: <ul style="list-style-type: none"> (a) Crypto security – That component of communications security which results from the provision of technically sound cryptosystems and their proper use; (b) Physical security – That element of communications security which results from all physical measures necessary to safeguard classified equipment, material and documents from access or observation by unauthorised people; and (c) Transmission Security – That component of communication security which results from all measures designed to protect transmissions from unauthorised interception, traffic analysis and imitative deception (the latter term relates to attempts to introduce bogus transmissions into a communications system).
Concept Of Operations (CONOPS)	A high level description of the process or procedures under which a system operates. Includes a description of inputs, processing and outputs.
Confidentiality private key	The key used to decipher or decode the contents of a message.cipher
Confidentiality public key	The key used to encipher or encode a the contents of a message.cipher
Confidentiality*	The property that information is not made available or disclosed to unauthorised individuals, entities, or processes
CONOPS	See Concept of Operations.
COTS	Commercial off the shelf product
CP	See Certificate Policy Statement.
CPS	See Certificate Practice Statement.
Credentials*	Data that is transferred to establish the claimed identity of an entity.
CRL	Certificate Revocation List
Cross certification	Practice of mutual recognition of another Cas certificates to an agreed level of confidence. Usually evidenced in contract. GPKA endorsed Cas shall only cross certify with other GPKA Cas.
Cryptographic algorithm*	A cryptographic algorithm is defined as an algorithm which transforms data in order to hide or reveal its information content and which uses at least one secret parameter. This definition includes both symmetric algorithms (e.g. DES and FEAL) and asymmetric algorithms (e.g. RSA and Rabin). In the case of a symmetric algorithm the data is hidden and revealed using a secret parameter. In the case of an asymmetric algorithm the data is hidden using a public parameter and revealed using a secret parameter.
Cryptographic equipment*	Equipment in which cryptographic functions (e.g. encipherment, authentication, key generation) are performed.
Cryptographic Information	Information, including crypto-material, significantly descriptive of cryptographic techniques and processes, or of cryptosystems and equipment or their functions and capabilities, the disclosure of which would assist the cryptanalytic solution of an encrypted text or a crypto-system.
Cryptographic key; key*	A parameter used in conjunction with an algorithm for the purpose of validation, authentication, encipherment or decipherment.

Term or Acronym	Explanatory notes
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.
DAP	Directory Access Protocol
Data integrity*	The property that data has not been altered or destroyed in an unauthorised manner.
Data storage*	A means for storing information from which data is submitted for delivery, or into which data is put by the delivery authority
Data string (data)*	The string of bits which is the input to a hash-function.
DEA	Data Encryption Algorithm
Decrypt	Practice of recovering an encrypted message by reverting from cipher text to plain language.
Defence Signals Directorate	The Commonwealth authority in matters pertaining to communications and computer security. It is located within the Department of Defence.
DES	Data Encryption Standard
Digest	The result from the application of a hashing algorithm to message text to a defined data. It is just a quotient.
Digital signature ³	A digital signature is a mathematical construct that creates a unique and unforgeable identifier of the owner of the Distinguished Name.
Digital signature*	Data appended to, or a cryptographic transformation (see cryptography) 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
Director General	The Director General of Security holding office under the ASIO Act 1979 (i.e. the Head of ASIO).
Directory	An online database containing public keys, Public Key Certificates and CRLs.
DISP	Defence Industrial Security Program.
Document	Anything on which information is recorded by any means, including words, symbols, images or electro-magnetic impressions.
DSA	Digital Signature Algorithm. Directory Service Agent.
DSD	Defence Signals Directorate.
DSD Certified	Software and/or Hardware that has been evaluated by the Australian Defence Signals Directorate and has achieved ITSEC certification.
DSS	Digital Signature Standard.
Dual control*	A process of utilising two or more separate entities (usually persons), operating in concert, to protect sensitive functions of information whereby no single person is able to access or utilise the materials, e.g. cryptographic key.
EDI	Electronic Data Interchange.
EDP	Electronic Data Processing.
Emergency Key Recovery	A method for retrieving private confidentiality keys from an authorised archive in an emergency.
Enablers	Small applications that allow a user to access and use a public key in an electronic service.

³ Ibid.

Term or Acronym	Explanatory notes
Encrypt	Practice of converting plain language to cipher text.
End Entity	Means a party who has been issued with private keys and Certificates by an Organisation CA under the terms of a recognised Certificate Policy, who receives or relies on cryptographic keys to authenticate themselves, or another End Entity, and/or to protect confidential information.
Entity authentication*	The corroboration that an entity is the one claimed.
EPL	DSD Evaluated Products List (List of products that have undergone a review process through the national authority.)
Evaluation authority*	A body which implements the criteria for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community.
Evaluation scheme*	The administrative and regulatory framework under which the criteria are applied by an evaluation authority within a specific community.
Evaluation*	Assessment of an IT system or product against defined criteria.
Explicit key authentication to A*	The assurance for one entity A that only another identified entity is in possession of the correct key. NOTE – Implicit key authentication to A and key confirmation to A together imply explicit key authentication to A.
GATEKEEPER	Project name for the implementation of a whole of Government Public Key Infrastructure.
Gatekeeper Accredited	A body that has been granted accreditation by the CEO, NOIE following a successful evaluation by a team of Authorised Evaluators against the Gatekeeper Criteria for the Accreditation of Certification Authorities. These criteria may be found at: http://www.govonline.gov.au
Gatekeeper Head Agreement	Contractual instrument for the provision of Whole Of Government Telecommunications services.
GOLD	Government On Line Directory.
GPKA	Government Public Key Authority.
GPKI	Government Public Key Infrastructure.
Hash	A computed number. A hash is used to compare versions of a calculated piece of data. If the hash results match, an assurance can be drawn that the data has not been tampered with.
Hash field*	Field of the intermediate string which conveys the hash-code.

Term or Acronym	Explanatory notes
Hash function*	<p>(i) A (mathematical) function which maps values from a (possibly very large) domain into a smaller range. A “good” hash function is such that the results of applying the function to a (large) set of values in the domain will be evenly distributed (and apparently at random) over the range.</p> <p>(ii) A function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties:</p> <ul style="list-style-type: none"> - it is computationally infeasible to find for a given output an input which maps to this output. - it is computationally infeasible to find for a given input a second input which maps to the same output. <p>[ISO/IEC 10118-1: 1994] [FCD ISO/IEC 14888-1 (12/1997)] The following notes are contained in ISO/IEC 10118-1. The second note is also contained in ISO/IEC 14888-1. NOTES 1. The literature of the subject contains a variety of terms which have the same or similar meaning as hash-function. Compressed encoding and condensing function are some examples. 2. Computational feasibility depends on the user’s specific security requirements and environment.</p>
Hash-code*	The string of bits which is the output of a hash-function.
Head Agreement	See Gatekeeper Head Agreement.
HIC	Health Insurance Commission
Hierarchy	See CAPL PKI Hierarchy
HIGHLY PROTECTED	The highest level of non national security classification.
HTTP	Hypertext Transfer Protocol
ICA	Intermediate Certification Authority – An entity on the second level of the PKAF hierarchy and which is immediately subordinate to the PARRA
Identification data*	<p>(i) A sequence of data items, including the distinguishing identifier for an entity, assigned to an entity and used to identify it. NOTE – Examples of data items which may be included in the identification data include: an account number, expiry date, serial number, etc.</p> <p>(ii) A sequence of data items, including the distinguishing identifier for an entity, assigned to an entity and used to identify it. NOTE – The identification data may additionally contain data items such as identifier of the signature process, identifier of the signature key, validity period of the signature key, restrictions on key usage, associated security policy parameters, key serial number, or domain parameters. [FCD ISO/IEC 14888-1 (12/1997)]</p>
Identity*	A method for identifying the user, which can either be the real name of that user or a pseudonym. [2 nd CD ISO/IEC 15408-1 (11/1997)]
Identity-based security policy*	A security policy based on the identities and/or attributes of users, a group of users, or entities acting on behalf of the users and the resources/objects being accessed.
IMAP	Information Management Access and Policy Branch

Term or Acronym	Explanatory notes
-IN-CONFIDENCE-	The classification given to material and resources, other than national security classified information or Cabinet documents, which require a limited degree of protection (i.e. the lowest level of non national security classification).
Intellectual Property Rights	All copyright and neighbouring rights, all rights in relation to inventions (including patent rights), plant varieties, registered and unregistered trademarks (including service marks), registered designs, confidential information (including trade secrets and know how), databases, and circuit layouts, and all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields.
ISO	International Organisation for Standardisation
IT security policy*	Rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organisation and its IT systems.
IT security*	All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, authenticity, and reliability.
IT/12/4/1	Standards Australia Committee for PKAF related standards
ITSEC	Information Technology Security Evaluation Criteria
Key establishment*	The process of making available a shared secret key to one or more entities. Key establishment includes key agreement and key transport.
Key generating function*	A function which takes as input a number of parameters, at least one of which shall be secret, and which gives as output keys appropriate for the intended algorithm and application. The function shall have the property that it shall be computationally infeasible to deduce the output without prior knowledge of the secret input.
Key generator*	A type of cryptographic equipment used for generating cryptographic keys and, where needed, initialisation vectors.
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	Expression used to describe the public and private keys of Public Key Technology
Key token*	Key management message sent from one entity to another entity during the execution of a key management mechanism
Key transport*	The process of transferring a key from one entity to another entity, suitably protected
Key*	(i) 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). (ii) A sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment).
Keying material*	The data (e.g. keys, initialisation values) necessary to establish and maintain cryptographic keying relationships
LDAP	Lightweight Directory Access Protocol
Masquerade*	The pretence by an entity to be a different entity.

Term or Acronym	Explanatory notes
Message*	(i) String of bits of limited length. (ii) A string of bits of any length. (iii) String of bits of any length, possibly empty.
Message authentication code (MAC)*	(i) A code in a message between a sender and a receiver used to validate the source and part or all of the text of a message. The code is the result of an agreed calculation. (ii) A data item derived from a message using symmetric cryptographic techniques and a secret key. It is used to check the integrity and origin of the message by any entity holding the secret key.
MOA	Memorandum Of Agreement
Monitor (Monitoring Authority)*	A trusted third party monitoring the actions and events and trusted to provide evidence about what was monitored.
MOU	Memorandum Of Understanding
NATA	National Association of Testing Authorities
National Security Classifications	Those classifications used to designate classified national security material. The classifications are TOP SECRET, SECRET, CONFIDENTIAL and RESTRICTED.
National Security Clearance	A clearance issued by an agency to enable a person to have access to national security material or a designated secure area.
National Security Material	Material in any form pertaining to Australia's security and defence, to some international relations and some matters affecting the national interests.
Need-to-Know	A criterion which requires the custodian of classified matter to establish, prior to disclosure, that the intended recipient needs access to the material to perform his/her official duties.
NOIE	National Office of the Information Economy. The administrative unit of the Commonwealth responsible for administering whole-of-government business arrangements for information technology services, including Certification Services, and any agent appointed by NOIE.
Non-repudiation exchange*	A sequence of one or more transfers of non-repudiation information (NRI) for the purpose of non-repudiation.
Non-repudiation information*	A set of information that may consist of the information about an event or action for which evidence is to be generated and validated, the evidence itself, and the non-repudiation policy in effect.
Non-repudiation policy*	A set of criteria for the provision of non-repudiation services. More specifically, a set of rules to be applied for the generation and verification of evidence and for adjudication.
Non-repudiation token*	A special type of security token as defined in ISO/IEC 10181-1 consisting of evidence, and, optionally, of additional data.
NRT token*	Non-repudiation of transport token. A data item which allows either the originator or the delivery authority to establish non-repudiation of transport for a message.
OCA	Organisation Certification Authority.
OECD	Organisation for Economic Co-operation and Development.
ORA	Organisation Registration Authority – An entity which establishes the identities of subordinate users and registers their certification requirements with a Certification Authority.
Organisational security policy*	A set of security rules, procedures, practices, and guidelines imposed by an organisation upon its operations.

Term or Acronym	Explanatory notes
PAA	Policy Approval Authority.
PARRA	Policy and Root Registration Authority – An entity which creates and monitors compliance with the overall guidelines that all users, associations of users, tiered levels of Certification Authorities and subordinate policy making authorities must follow.
Personal Identification Code	An access control mechanism used during key transport to import private keys into an end user application.
Personnel Security	The protective measures used to ensure that only suitable people are given access, remain suitable for access and are made aware of their security responsibilities.
Physical Security	(i) That part of protective security concerned with physical measures designed to prevent unauthorised access to resources, and to safeguard them against espionage, deliberate damage, alteration or theft (e.g. locks, alarms, safes, etc). (ii) The measures used to provide physical protection of resources against deliberate and accidental threats.
PIC	See Personal Identification Code.
PKAF	Public Key Authentication Framework – A framework that, if followed, allows for the establishment of a trusted public key system. This system will allow any entity to determine the trust and validity of a digital signature claimed to be associated with another entity.
PKI	Public Key Infrastructure.
PKT	Public Key Technology.
POI	Proof of Identity.
Police Records Checks	A check, in the proper form, of records of police forces for any conviction, charges pending or other criminal activity regarding the vettee.
Position of Trust (POT)	A position on the establishment of an agency the duties of which are likely to involve access to sensitive material, and/or valuable or attractive resources, or a position in which the occupant may exercise considerable authority/responsibility – e.g. the granting of major contracts.
Position of Trust Clearance	A clearance issued by an Agency to enable a person to have access to sensitive material or resources of a valuable or attractive nature.
Preferred Candidate	The candidate for appointment, promotion, transfer to a designated security assessment position or position of trust who, subject to the granting of a clearance, will be appointed, promoted or transferred to the position.
Privacy*	The right of individuals to control or influence what information related to them may be collected and stored and to whom that information may be disclosed. NOTE – Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security.

Term or Acronym	Explanatory notes
Private key*	<p>(i) Secret part, key or mathematical construct from a pair of keys which together form the basis of Public Key Technologies. (See Public key)</p> <p>(ii) That key of an entity's asymmetric key pair which shall normally only be known by that entity. NOTE – In the case of an asymmetric signature system the private key defines the signature transformation. In the case of an asymmetric encipherment system the private key defines the decipherment transformation. [2nd DIS ISO/IEC 11770-3 (08/1997)] 13888-1: 1997</p> <p>(iii) That key of an entity's asymmetric key pair which is usable only by that entity. In the case of an asymmetric signature system, the private key and the associated algorithms define the signature transformation.</p> <p>(iv) (secret key – deprecated) (In a public key cryptosystem) that key of a user's key pair which is known only by that user.</p> <p>(v) That key of an entity's asymmetric key pair which should only be used by that entity. The following note is contained in ISO/IEC 9798-1: NOTE – In the case of an asymmetric signature system the private key defines the signature transformation. In the case of an asymmetric encipherment system the private key defines the decipherment transformation. The following note is contained in ISO/IEC 11770-1: NOTE – A private key shall normally not be disclosed.</p>
Private signature key*	Private key which defines the private signature transformation. NOTE – This is sometimes referred to as a secret signature key.
PROTECTED	The classification applied to sensitive material requiring a reasonable degree of protection (i.e. the middle sensitive material classification).
Protective Security	The total concept of administrative, personnel, physical, technical, computer and communication security.
PSM	Protective Security Manual
PSRR	Protective Security Risk Review

Term or Acronym	Explanatory notes
Public key*	<p>(i) Public part, key or mathematical construct from a pair of keys which together form the basis of Public Key Technologies. (See Private key) The key of an entity's asymmetric key pair which can be made public. In the case of an asymmetric signature system, the public key and the associated algorithms define the verification transformation.</p> <p>(ii) [ISO/IEC 13888]</p> <p>(iii) (In a public key cryptosystem) that key of a user's key pair which is publicly known. [ISO/IEC 9594-8:1990] [CCITT X.509: 1988]</p> <p>(iv) That key of an entity's asymmetric key pair which can be made public. [ISO/IEC 9798-1 (2nd edition): 1997] [ISO/IEC 11770-1: 1997] [2nd DIS ISO/IEC 11770-3 (08/1997)] The following note is contained in ISO/IEC 9798-1 and in ISO/IEC 11770-3: NOTE – In the case of an asymmetric signature system the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is “publicly known” is not necessarily globally available. The key may only be available to all members of a pre-specified group.</p>
Public key certificate (certificate)*	<p>(i) The public key information of an entity signed by the certification authority and thereby rendered unforgeable. [ISO/IEC 9798-1 (2nd edition): 1997] [ISO/IEC 11770-1: 1997] [2nd DIS ISO/IEC 11770-3 (08/1997)]</p> <p>(ii) A security certificate which binds unforgeably the public key of an entity to the entity's distinguishing identifier, and which indicates the validity of the corresponding private key. [ISO/IEC]</p>
Public key derivation function*	<p>A public function, which maps strings of bits to positive integers, which is used to transform an entity's identification data to its verification key, and which satisfies the following two properties:</p> <ul style="list-style-type: none"> - It is computationally infeasible to find any two distinct inputs which map to the same output. - Either the probability that a randomly chosen value Y is in the range of the function is negligibly small, or it is computationally infeasible to find for a given output an input which maps to this output. <p>NOTE – Negligibility and computational infeasibility depend on the user's specific security requirements and environment.</p>
Public key information*	<p>(i) Information specific to a single entity and which contains at least the entity's distinguishing identifier and at least one public key for this entity. There may be other information regarding the certification authority, the entity, the public key included in the public key information, such as the validity period of the public key, the validity period of the associated private key, or the identifier of the involved algorithms.</p> <p>(ii) Information containing at least the entity's distinguished identifier and public key. The public key information is limited to data regarding one entity, and one public key for this entity. There may be other static information regarding the certification authority, the entity, the public key, or the involved algorithms, included in the public key information.</p>

Term or Acronym	Explanatory notes
Public key information*	<p>(i) Information specific to a single entity and which contains at least the entity's distinguishing identifier and at least one public key for this entity. There may be other information regarding the certification authority, the entity, the public key included in the public key information, such as the validity period of the public key, the validity period of the associated private key, or the identifier of the involved algorithms.</p> <p>(ii) Information containing at least the entity's distinguished identifier and public key. The public key information is limited to data regarding one entity, and one public key for this entity. There may be other static information regarding the certification authority, the entity, the public key, or the involved algorithms, included in the public key information.</p>
Public verification key*	Public key which defines the public verification transformation.
Qualified Security Assessment	<p>A security assessment in respect of a person that:</p> <p>(a) contains any opinion or advice, or any qualification of any opinion or advice, or any information, that is or could be prejudicial to the interests of the person; and</p> <p>(b) does not contain a recommendation of the kind referred to in paragraph (b) of the definition of "adverse security assessment", whether or not the matters contained in the assessment would, by themselves, justify prescribed administrative action being taken or not being taken in respect of the person to the prejudice of the interests of the person.</p>
RA	Registration Authority.
RCA	Root Certification Authority.
Recipient*	The entity that gets (receives or fetches) a message for which non-repudiation services are to be provided.
Registration	Process of establishing the identity of an individual and documentation of proof to a prescribed level of confidence.
Registration Authority	Registration Authority – An entity which establishes the identities of users and registers their certification requirements with a Certification Authority
Relying Party	A person or organisation who uses or relies upon information contained in a Certificate issued by a CA within the CAPL PKI hierarchy or information contained within a CRL posted in the CAPL X.500 Directory.
Repudiation*	Denial by one of the entities involved in a communication of having participated in all or part of the communication
Resource	Personnel, property or information belonging to, or in the care of an agency.
RESTRICTED	The classification allocated to national security information the unauthorised disclosure of which could possibly be harmful to the national security.
Risk analysis*	The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards.
Risk management*	The total process of identifying, controlling, and eliminating or minimising uncertain events that may affect IT system resources.
Risk*	The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets.
Role*	A predefined set of rules establishing the allowed interactions between a user and the TOE
RSA	Rivest Shamir Adleman

Term or Acronym	Explanatory notes
Signature key*	A secret data item specific to an entity and usable only by this entity in the signature process.
SOP	Standard Operating Procedures
SSP	System Security Plan
Standards Australia	An Australian organisation whose mission is to develop and promote the use of standards.
Steering Committee	Peak directional committee for Project GATEKEEPER
Subordinate CA	A CA that is underneath another CA higher in the trust hierarchy. e.g. the CAPL OCA is subordinate to the CAPL RCA.
Subscriber	A person or organisation who has been issued with a Certificate by one of the CAs within the CAPL PKI Hierarchy.
Symmetric authentication method*	A method of authentication in which both entities share common authentication information.
Symmetric cryptographic technique*	A cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation. Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation.
System integrity*	The property that a system performs its intended function in an unimpaired manner, free from deliberate or accidental unauthorised manipulation of the system.
Target of Evaluation (TOE)*	An IT product or system and its associated administration and user guidance documentation that is the subject of an evaluation
Threat*	<ul style="list-style-type: none"> (i) A potential event that could adversely affect the status of a resource, such as through loss, damage, destruction, reduced capacity, compromise, etc. (ii) A potential violation of security. (iii) A potential cause of an unwanted incident which may result in harm to a system or organisation.
Threat Assessment	A judgement of the likelihood or probability of an event taking place that could adversely affect an agency's resources.
TOE resource*	Anything useable or consumable in the TOE.
TOE Security Policy (TSP)*	A set of rules that regulate how assets are managed, protected and distributed within a TOE.
Token*	A message consisting of data fields relevant to a particular communication and which contains information that has been transformed using a cryptographic technique.
TOP SECRET	The classification allocated to national security information the unauthorised disclosure of which could cause exceptionally grave damage to the national security. It is the highest national security classification.
Trusted path*	A means by which a User and a TSF can communicate directly with necessary confidence to support the TSP.

Term or Acronym	Explanatory notes
Trusted third party*	(i) A security authority, or its agent, trusted by other entities with respect to security related activities. In the context of this multipart standard, a trusted third party is trusted either by the originator, the recipient, and/or the delivery authority for the purposes of non-repudiation, and by another party such as the adjudicator. (ii) A security authority, or its agent, trusted by other entities with respect to security related activities.
TSA	Time Stamp Authority.
TTP	Trusted Third Party.
User	Any entity (human or machine) outside the TOE that interacts with the TOE.
Validation*	The process of checking the integrity of a message, or selected parts of a message.
Verification authentication information (verification AI)*	Information used by a verifier to verify an identity claimed through exchange AI.
Verification key*	(i) A value required to verify a cryptographic check value. (ii) A data item which is mathematically related to an entity's signature key and which is used by the verifier in the verification process.
Verification process*	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.
Verifier*	(i) An entity that verifies an evidence. (ii) An entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges.
Vetting	The process of acquiring information to assess a person's suitability for access to classified and/or sensitive material or to a designated secure area.
WEMA	World Electronic Messaging Association.
Word*	A string of 32 bits.
Working Days	Monday to Friday excluding NSW public holidays.

NOTE: Terms or acronyms marked (*) have been adopted from ISO draft (subject to change) Glossary of IT security terminology prepared by JTC1 SC 27 at <http://www.iso.ch.8080/jtcl/sc27/27sd698a.htm>.