

Australian Government e-Authentication Framework Glossary

100-Point Check	<p>A process for evaluating Evidence of Identity for an individual, as defined by the Financial Transactions Reporting Act 1988 and administered by AusTrac. It requires the presentation of sufficient original documents from an approved list of document-types, with associated point values, such that the total of the points associated with the presented documents is at least 100 points.</p> <p>See also Evidence of Identity</p>
Access Authorisation	<p>The system controls and surrounding processes that provide or deny parties the capability and opportunity to access systems (i.e. gain knowledge of or to alter information or material on systems).</p> <p>In practice, the act of authorising access usually occurs after authentication has been successful. Authentication checks if the party is who they claim to be. Access authorisation checks what the party is allowed to do.</p>
ACSI 33	<p>Old name for the Australian Government's "Information Technology Security Manual" published by the Defence Signals Directorate. Previously called "Australian Communications-Electronic Security Instruction 33".</p>
AGAF	<p>The Australian Government e-Authentication Framework.</p> <p>The Framework covers the rules to be applied to authentication of external (ie non-Commonwealth Government) entities when dealing with them online.</p> <p>The Framework provides a risk management approach to authentication that aligns business needs and processes with appropriate authentication solutions and technologies.</p>
Agency Security Plan	<p>The plan of action the agency intends to use to address its security risk based on the context in which the agency operates and a thorough risk review. It is one of the means by which an agency will demonstrate a commitment to general risk management.¹</p>
Agency Security Adviser	<p>The person nominated by the agency for the day-to-day performance of the protective security function within the agency.</p>
Agent	<p>A Legal Entity that has the capacity to act on behalf of another Legal Entity. The Legal Entity that is represented is referred to as a Principal.</p>
ASA	<p>See Agency Security Adviser</p>

¹ Source: Australian Government Protective Security Manual

Assertion	<p>A statement made that purports to be true.</p> <p>Categories of Assertion that may be subjected to Authentication include Agents, Attributes, Credentials, Data Integrity, Entities, Identities, Location, and/or Value.</p> <p>Eg – “I am Sheila Smith”, “I am an authorised signatory”, “I am the authorised agent of Bob Black”, “This communication is coming from Geelong”.</p>
Asymmetric Key Cryptography	<p>Technology that enables a message to be encrypted with one Key, and decrypted with another Key. The two keys are mathematically related and are generated as a pair. One Key of each key-pair is kept secret (the Private Key). The other can be made public (the Public Key). It is infeasible to determine a Private Key from knowledge of its related Public Key.</p> <p>See also: Public Key Technology; PKI</p>
Attribute	<p>A characteristic of an Entity or Identifier.</p> <p>Attributes of a Natural Person include the person’s gender, age-range, qualifications (such as being a registered counsellor), and capacity to act as an Agent for another Entity.</p>
Audit	<p>Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.</p>
Australian Business Number (ABN)	<p>The Australian Business Number (ABN) is a single identifier for dealings with the Australian Taxation Office (ATO) and for future dealings with other government departments and Agencies.</p>
Australian Business Register (ABR)	<p>The Australian Business Register (ABR) contains all the publicly available information provided by businesses when they register for an Australian Business Number (ABN). The Australian Business Register was established under s.24 of the A New Tax System (Australian Business Number) Act 1999.</p>
Authentication	<p>The process of testing of an Assertion, in order to establish a level of confidence in the Assertion’s reliability.</p>
Authentication Assurance Level	<p>The level of trust/certainty associated with the Authentication Technique.</p> <p>The AGAF propose four assurance levels (1-4): Minimal, Low, Moderate, High.</p>
Authority	<p>Permission to perform a specified act.</p> <p>Eg: access and/or modify data; approve the registration and/or enrolment of users.</p>

Authority to deal	Broadly based permissions that can be associated with an identity – eg those based upon role, financial delegation
Binding	The process of linking a credential to an identity in an assured manner. Eg. When a CA uses a Digital Signature to bind together a Subject and a Public Key in a Digital Certificate.
Biometrics	<p>A measure of an Attribute of a Natural Person's physical self, or of their physical behaviour. In principle at least, a Biometric can be used:</p> <ul style="list-style-type: none"> • to validate an entity (where the entity is a Natural Person); • as an Authenticator for an Assertion involving an Entity; and • as a means of restricting the use of a personalised Token to the appropriate Natural Person. <p>Examples include: fingerprint, voice-print, iris-scan</p>
Browser-based	A (web) browser is a software application used to locate and display web pages (eg. Microsoft Internet Explorer). A browser-based authentication mechanism is one that makes use of the web browser and its inbuilt functionality or plug-ins/add-ons to do the authentication processes.
Business Entity	An entity entitled to have an ABN within the meaning of s.8 of the A New Tax System (Australian Business Number) Act 1999.
Business to Business (B2B)	eBusiness among Legal Persons in the form of business enterprises.
Business to Government (B2G)	eBusiness among Legal Persons in the form of business enterprises on the one hand, and government agencies on the other.
CA	See Certification Authority.
Call-Back	A technique whereby a System does not permit Access by a User directly, but only accepts from a User a request for Access, and then initiates a connection to a contact point previously recorded for that User (e.g. a telephone-number or IP-Address).
Certificates	See Digital Certificate
Certification	An Assertion by a Legal Entity that a particular Public Key is associated with (or 'bound' to) a particular Legal Entity.
Certification Authority (CA)	An Entity that issues Digital Certificates (especially X.509 certificates), vouches for their contents, is trusted by Relying Parties to do so, and may provide warranties to that effect, and even some level of indemnity.

Challenge-Response (general meaning)	<p>An authentication technique whereby a System does not permit Access by a User, until the User has given the correct answer ('response') to a question (or 'challenge').</p> <p>A Password is a form of Challenge-Response authentication. Other examples include requests for date of birth, invoicing address, and the most recent transaction on the User's account.</p>
Challenge-Response (2) (Used in relation to a particular technology implementation)	<p>A cryptographic authentication technique which tests knowledge of a secret without exposing that secret.</p> <p>A randomised one-off Challenge is presented to the party to be authenticated, which answers with a Response. The correct Response is a function of both the Challenge and a secret (cryptographic key). The response is often generated in a separate hardware device (smart card, token) which securely contains the cryptographic key. Access to the device would typically be via an access code or biometric.</p> <p>TLS (SSL) implements challenge – response as a core part of its authentication protocol.</p>
Classification	<p>Determining the 'status' of a user or information resource for security purposes. The matching of the two then provides a capacity to determine user access rights to the information resource.</p> <p>See Data Classification.</p>
Clearance Level	<p>The formal Classification associated with a person – eg cleared to 'Top Secret' level.</p>
Client	<p>A generic short-form way of describing the software used by an end-user. See 'thin client' and 'fat client'.</p>
Confidentiality	<p>The obligation of a recipient of information to not disclose it to parties other than those explicitly agreed to by the subject/owner of the information. The obligations are regulated by the common law of confidence.</p>
Credential	<p>A Credential is something used to authenticate a user's identity. The user possesses the Credential and controls its use through one or other authentication protocols. A Credential incorporates a Password, cryptographic key, or other form of secret.</p> <p>The form factor of the Credential may be a physical device such as a one-time-password token, a smart card, a code book, or simply, as in the case of a password, the user's knowledge of the secret.</p>
Credential 2	<p>Information, passed from one entity to another, used to establish the sending entity's access rights².</p>

² Source: INFOSEC-99

Credential 3	A set of access permissions. Media independent data attesting to, or establishing, the identity of an entity, such as a birth certificate, driver's license, mother's maiden name, social security number, finger print, voice print, or other biometrics. ³
Credential Store	The systems-based repository that holds electronic records of user credentials.
Data Classification	Classification of data (eg documents, computer records) according to defined 'security' rules. This enables access to such data to be provided or refused based upon the 'security' classification of the party seeking access.
Data Confidentiality	The condition in which data is protected against Access by unauthorised parties, whether such data is stored or is in transmission.
Data Integrity	The condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.
De-provisioning	The withdrawing of access permissions by the alteration of 'control' records on systems relating to the authentication credentials and/or access permissions of users.
Digital Certificate	A character string that has been digitally signed by an Entity (a Certification Authority) and that makes one or more Assertions about a Public Key and another Entity, as specified by the relevant terms of contract.
Digital Certificate 3	<p>An electronic document that asserts a connection between an Identity and a cryptographic Public Key. A digital certificate is tamper-resistant and cannot be readily forged, because it is Digitally Signed by the Private Key of the Certification Authority which issued it</p> <p>In an X.509-based scheme, it is an an electronic document signed by the CA which:</p> <ol style="list-style-type: none"> (1) identifies a Key Holder and the Business Entity he or she represents; (2) binds the Key Holder to a Key Pair by specifying the Public Key of that Key Pair; and (3) should contain any other information required by the Certificate Profile.

³ Source: ANSI X9.69

Digital signature	<p>A string of characters appended to a digital object that demonstrates that the originating device had access to a particular Private Key.</p> <p>An important use is to enable Authentication of the Identity that generated, sent, or takes responsibility for that digital object. This assumes that a considerable number of conditions hold. See Public Key Infrastructure.</p> <p>The technique applies Public Key Technology as follows:</p> <ul style="list-style-type: none"> • a relatively short string of bits is generated from the content of the digital object, by applying an agreed one-way Hash Function to it; • that string is then encrypted with the signer's Private Key, and appended to the digital object; • any other party that has Access to the digital object can also generate that string by applying the same Hash Function to it; • any other party that has Access to the signed digital object can decrypt the Digital Signature by applying the putative signer's Public Key to it; • if the generated string and the decrypted signature are equal, then the signature was generated by a device that had Access to the appropriate Private Key.
Digital signature 2	<p>A very large number created in such a way that it can be shown to have been done only by somebody in possession of a (secret) key and only by processing a document with a particular content. It can be used for the same purposes as a person's handwritten signature on a physical document. Something you can do with public key cryptography.⁴</p>
eAuthentication	<p>Authentication performed in the context of electronic services delivery in an online environment.</p>
eBusiness	<p>The application of telecommunications-based tools to the business of Natural Persons and/or Legal Persons. It encompasses all segments of electronic interaction, including business-to-consumer (B2C), business-to-business (B2B), business-to-government (B2G), government-to-business (G2B), government-to-government (G2G), consumer-to-consumer (C2C), eGovernment and Electronic Services Delivery.</p>
eGovernment	<p>The application of telecommunications-based tools to the dealings of government agencies with other Entities, including Natural Persons, Legal Persons in the form of business enterprises, and other government agencies.</p>

^{4 4} Source: www.w3.org/People/Berners-Lee/Weaving/glossary.html

Enrolment	<p>The act of setting up permissions that enable a known user to gain knowledge of or to alter information or material on systems.</p> <p>Eg a known user will be enrolled into the email, HR, Financial etc systems.</p> <p>Multiple enrolments into various systems may occur after a user has been Registered.</p> <p>Although 'Registration' and 'Enrolment' are sometimes used as synonyms, a distinction is being drawn here between the two terms.</p>
Entity	<p>A real-world thing.</p> <p>Categories include objects, animals, artefacts, natural persons, and legal persons (such as corporations, trusts, superannuation funds, and incorporated associations).</p>
EOI	See Evidence of Identity
Evidence of Identity	<p>Evidence (eg in the form of documents) used to substantiate the identity of the presenting party, usually produced at the time of Registration (ie when authentication credentials are issued).</p> <p>See also 100-Point Check.</p>
Fat client	A client software application (or client machine running the application) that performs the data processing operations, rather than those operations happening at the server end.
FTRA	Financial Transactions Reporting Act (1988)
Hard certificates	Digital certificates stored on a hardware token (eg smartcard) together with the associate private key.
Identification	The process whereby data is associated with a particular Identity. It is performed through the acquisition of data that constitutes an Identifier for that Identity.
Identifier	<p>One or more data-items concerning an Identity that are sufficient to distinguish it from other Identities, and that are used to signify that Identity.</p> <p>Identifiers include names. A natural person may use more than one name, and variants of each name.</p> <p>Identifiers also include 'id numbers' or 'id codes' issued by other Entities that the Entity interacts with. An Entity may be assigned many such numbers and codes.</p> <p>A legal person may have many names (e.g. associated with business units, divisions, branches, trading-names, trademarks and brandnames), and multiple 'id numbers' and 'id codes' assigned by other Entities that the Entity interacts with.</p>

Identities Directory	Directory in which core information is held relating to identities.
Identity	<p>A particular presentation of an Entity.</p> <p>An Identity may correspond to a Role played by the Entity.</p> <p>An Identity may be used by the Entity in its dealings with one other Entity, or with many other Entities.</p> <p>An organisation may maintain an Account within its records that corresponds to an Identity.</p>
Identity Authentication	<p>The process of testing an Assertion that a particular Entity is appropriately using an Identity, in order to establish a level of confidence in the Assertion's reliability.</p> <p>In particular, the process of cross-checking, against additional Evidence of Identity (EOI), the Identity signified by an Identifier acquired during an Identification process.</p>
Identity Management	The policies, rules, processes and systems involved in ensuring that only known, authorised Identities gain access to networks and systems and the information contained therein.
Integrity	The term used in relation to data/messages to indicate the situation under which these are transmitted from point-to-point and/or application-to-application without the content being altered.
Intrinsic Risk	The fundamental risk associated with a transaction (ie before consideration of mitigating factors).
IT Security Adviser	A person nominated by the agency head to provide advice on information technology-related security issues within his or her agency.
ITSA	See IT Security Adviser
KBA	See Knowledge Based Authentication
Knowledge Based Authentication	An authentication approach in which a user is challenged to provide one or more answers to questions/challenges provided by the party undertaking the authentication. The information sought could be 'shared secrets' provided by the user during a registration process and/or personal information (eg address, date of birth, mothers maiden name, etc) and/or transactional data (eg date, amount, reference number of last payment).
Late Binding	The process of linking a Credential to an Identity in an assured manner at a point in time after the Credential is created, ie. a Credential is created absent of any identification information and later linked to an individual/organisation's Identity.

Legal Entity	An Entity that is recognised at law as having the capacity to act. See Natural Person and Legal Person.
Login	An action by an Entity whereby they seek Access to System Resources. Usually involves the provision of a Username/Password pair to an Access Control System.
LoginId	See User Name.
Malware	Software deliberately designed to damage or subvert computer process (eg Worms, viruses).
Masquerade	Behaviour by an Entity as though it were another Entity. Also referred to as Impersonation or Spoofing.
Mitigating Factors	Factors that may reduce the level of Intrinsic Risk.
Multi factor authentication	An Authentication process in which multiple forms of Evidence are used, in order to increase the level of confidence in the Assertion. In the case of Identity Authentication, this involves two or more of the following: <ul style="list-style-type: none"> • an additional authenticator provided by the person; • knowledge demonstrated by the person ('something you know'); • an act performed by the person ('something you can do'); • a Credential provided by the person ('something you have'); • a Biometric surrendered by the person ('something you are' or 'something you do').
Natural Person	A human being, and a particular category of Legal Entity. Distinguished from a Legal Person. A Natural Person performs social, economic and political functions in various Roles, e.g. as citizens, consumers, sole traders, and members of partnerships and unincorporated solutions; and as Agents both for other Natural Persons and for Legal Persons.

Non-Repudiation	<p>Strong evidence, verifiable by a third party, that a transaction has been sent/authorised by the purported sender. This provides protection against the sender later falsely denying having sent the transaction.</p> <p>The concept is inconsistent with the notion of risk-managed security. The concept of Repudiability is to be strongly preferred, because it brings to attention that an Assertion may be able to be subsequently denied, but with varying degrees of credibility.</p> <p>Paper signatures are the traditional means of providing Non-Repudiation. Digital Signatures are a strong electronic means of providing Non-Repudiation, but other approaches can be used. These typically involve a neutral third party in a transaction, in addition to the sender and receiver, so the third party can later adjudicate in event of a dispute.</p>
Nym	<p>A class of identifier used by an entity that enables the entity to remain fully or partially anonymous (the latter being pseudonymous).</p> <p>See also: Persistent Nym</p>
OFPC	Office of the Federal Privacy Commissioner
Onboarding	The process of Registering and Enrolling online users.
Out-of-band	The use of an alternative channel for transmitting information – eg post to send a PIN; SMS to send a one-time password.
Password	<p>A form of Authentication in which a string of characters is used to assist in the Authentication of the Assertion that a person has the right to use a particular User-ID.</p> <p>The effectiveness of the technique depends upon the assumption that the Password is known only by the appropriate Entity (and, in less secure schemes, also by the System conducting the Authentication).</p> <p>If a Password is disclosed or shared, Accountability is compromised.</p> <p>Synonyms/similar concepts are Passphrase, Personal Identification Number (PIN).</p> <p>(See also <i>Strong Password</i>)</p>

Password 2	<p>A secret series of characters that enables a user to access a file, computer, or program. On multi-user systems, each user must enter his or her password before the computer will respond to commands. The password helps ensure that unauthorized users do not access the computer. In addition, data files and programs may require a password.</p> <p>Ideally, the password should be something that nobody could guess. In practice, most people choose a password that is easy to remember, such as their name or their initials. This is one reason it is relatively easy to break into most computer systems.⁵</p>
Permissions	<p>A Capability, associated with an Identity, which enables Access to System Resources.</p> <p>Authorisation and Privilege are used as synonyms for Permission.</p> <p>See also Restriction.</p>
Permissions Management Infrastructure (PMI)	<p>The systems (hardware, software and networks) that enable the management of Permissions in relation to user access to application systems resources. The term is generally used only where the PMI is infrastructure supporting multiple application systems, rather than each of those systems providing Permissions management functionality for itself.</p>
Permissions store	<p>The systems-based repository that holds the authoritative records of valid user permissions.</p>
Persistent Nym	<p>A class of identifier used to enable a user to remain anonymous or pseudonymous, but that nonetheless enables a persistent conversation to be held between the credential owner and a relying party.</p> <p>See also: Nym</p>
Phishing	<p>The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft⁶.</p>
PKI	<p>Public Key Infrastructure.</p> <p>The comprehensive set of measures needed to enable Public Key Technology to support the Authentication of Assertions. For a detailed list of measures required, see http://www.anu.edu.au/people/Roger.Clarke/EC/Bled03.html#App2</p>

⁵ Source: <http://www.webopedia.com/TERM/P/password.html>

⁶ Source: www.webopedia.com

Privacy	<p>The interests that Natural Persons have in sustaining a 'personal space', free from interference by other people and organisations, and in controlling information about themselves.</p> <p>It has multiple dimensions, including privacy of the physical person, privacy of personal behaviour, privacy of personal communications, and privacy of personal data.</p> <p>A variety of privacy rights are conferred by international instruments, and by the laws of most jurisdictions.</p> <p>The term is often misused to mean the protection of data during transmission or storage. Privacy is a much broader concept, involving issues such as what data to collect, when to destroy it, and access rights by the subject, not just how to protect it.</p>
Provisioning	<p>The process (whether manual or automated) of supplying services to and enabling features for a subscriber, in this context, access permissions. It includes Registration, issuing of Credentials, and initial Enrolments.</p>
PSM	<p>The Australian Government's <i>Protective Security Manual</i> published by the Attorney-General's Department. The PSM sets out the policies, practices and procedures that provide a protective security environment for Government resources.</p>
Public Key Technology	<p>Technology based on public key cryptography, that enables a message to be encrypted with one Key, and decrypted with another Key. Also known as Public Key Cryptography (PKC).</p> <p>PKI is distinguished from secret-key (or symmetric) technologies, which use a single key that both parties must possess, and that therefore has to be communicated from whomever creates it to whomever needs it, and therefore has to be exposed to the risk of interception.</p> <p>With public key technologies, on the other hand, one of the key pair can be kept securely by one party, and never exposed to the risk of interception by a third party.</p>
Public Domain Information	<p>Official information that is authorised for unlimited public access and circulation (for example, agency publications or web sites).</p>
RA	<p>See Registration Authority.</p>
Registration	<p>The process of establish a user's Authentication Credentials. This may involve eg requirement for production of Evidence of Identity and the issuing of one or more Credentials.</p> <p>Multiple enrolments may occur after a user has been registered.</p> <p>Although 'registration' and 'enrolment' are sometimes used as synonyms, a distinction is being drawn here between the two terms.</p>

Registration Authority (RA)	<p>An Entity that conducts a Registration process on behalf of a Certification Authority (CA).</p> <p>An RA is an optional PKI component, separate from the CA. Alternatively, the CA may itself perform the Registration process.</p>
Relying Party	<p>An Entity that relies on an Assertion.</p> <p>Of particular importance is an Assertion that another Assertion (e.g. of Value, Identity, Attribute or Agency) has been subjected to particular Pre-Authentication or Authentication processes.</p>
Repudiability	<p>The capacity for an Entity to repudiate a particular Assertion.</p>
Repudiation	<p>A denial by a Legal Entity that an act attributed to them was performed by them.</p> <p>Examples of such an act include an Assertion, a declaration and a transaction.</p>
Reputation	<p>An arrangement whereby trust in an Identity's behaviour is based on the opinions held about it by other Entities, and/or on its previous behaviour as perceived by other Entities.</p>
Residual Risk	<p>In Threat and Risk Assessment, the risk derived after applying Mitigating Factors to the Intrinsic Risk.</p>
Risk Management	<p>A process whereby threats, vulnerabilities and risks are assessed, and a balance sought between predictable costs and uncertain benefits.</p> <p>The aim of Risk Management is to expend on safeguards the effort and cost that are warranted in order to provide an appropriate level of protection against identified threats.</p>
Role	<p>A pattern of behaviour adopted by an Entity.</p> <p>An Entity may adopt one Identity in respect of each Role, or may use the same Identity when performing multiple Roles.</p> <p>Examples of Roles played by Legal Entities include seller/buyer, supplier/receiver, debtor/creditor, payer/payee, principal/agent, franchisor/franchisee, lessor/lessee, copyright licensor/licensee, employer/employee, contractor/contractee, trustee/beneficiary, tax-assessor/tax-assessee, business licensor/licensee, plaintiff/respondent, investigator/investigatee, and prosecutor/defendant.</p>
Role-Based Access Control (RBAC)	<p>An approach to Access Control whereby Usernames are associated with Roles (or functional positions), within an organisation or process, rather than with individual Users.</p>

Single factor authentication	<p>An Authentication process in which a single form of Evidence is used to authenticate the user.</p> <p>In the case of Identity Authentication, this involves one of the following:</p> <ul style="list-style-type: none"> • an Identifier provided by the person; • knowledge demonstrated by the person ('something you know'); • an act performed by the person (something you can do); • a Credential provided by the person ('something you have'); • a Biometric surrendered by the person ('something you are' or something you do).
Shared Information	<p>Information known to the user and the party seeking to authenticate the user. This is often not information that has been specifically collected to enable authentication.</p> <p>eg date/amount of last payment; address; date of birth</p>
Shared Secrets	<p>Information specifically stored in order to enable authentication.</p> <p>eg mother's maiden name; favourite colour; etc</p>
Smart cards	<p>A hardware token, usually taking the form of a credit-card sized plastic card with an embedded chip.</p> <p>May be used as a hardware token to carry information for authentication including digital certificate.</p>
Soft certificates	<p>Digital certificate and associated private key stored on a medium that enables it to be copyable-eg computer hard-disk, diskette or other form of removable media, etc.</p>
Strong Password	<p>A password that is difficult to guess by both humans and computer programs, effectively protecting data from unauthorized access. A strong password consists of at least six characters (and the more characters, the stronger the password) that are a combination of letters, numbers and symbols (@, #, \$, %, etc.) if allowed. Passwords are typically case-sensitive, so a strong password contains letters in both uppercase and lowercase. Strong passwords also do not contain words that can be found in a dictionary or parts of the user's own name⁷.</p>
Symmetric Key Cryptography	<p>An encryption system in which the sender and receiver of a message share a single, common key that is used to secure the message.</p>
Thin Client	<p>Generic user-interface software, not specific to a particular application that supports execution of applications delivered over the network. Examples include a web-browser.</p>

⁷ Source: http://www.webopedia.com/TERM/S/strong_password.html

Threat and Risk Assessment	<p>Formal evaluation of risk.</p> <p>First possible Threats are identified, then for each Threat its</p> <ul style="list-style-type: none"> a) likelihood, and b) consequences <p>are evaluated to arrive at an Intrinsic Risk for each Threat.</p> <p>Mitigating Factors can then be considered. The Residual Risk of each Threat is the remaining risk after Mitigating Factors are applied.</p> <p>See Australian Government's Protective Security Manual and "Information Technology Security Manual" (ACSI 33), and AS/NZS 4360, HB231 and HB436 from Standards Australia.</p>
TRA	Threat Risk Assessment
Token	<p>A physical thing, issued as a Credential. A Token is likely to include security features intended to render it difficult to forge, and tying it in some manner with the particular Entity.</p> <p>Examples include 'identity cards'(especially 'photo-id'), smartcards, one-time-password devices (eg RSA SecurID) and 'dongles'.</p>
Trojan	A destructive computer program that masquerades as a harmless application – usually associated with the Internet.
Unclassified Information	Official information that is not security classified. It may be unlabelled or it may be marked UNCLASSIFIED. Disclosure of this information must be authorised. This type of information represents the bulk of official information ⁸ .
User	In the context of Usernames and Access Control, an Identity (eg Natural Person, device (eg another client or server application)) that seeks Access to System Resources.
User-ID	<p>A string of characters that is issued to an Identity, and is included within an Access Control List, and which thereby has Permissions, and is subject to Restrictions, in relation to Access to System Resources.</p> <p>Also referred to as LoginID and User Name.</p> <p>Normally used in conjunction with a Password or PIN, and possibly also a Token or biometric, in order to enable Authentication.</p>

⁸ Source: Australian Government Protective Security Manual

Validation	<p>The process of establishing the truth of an Assertion to some pre-determined degree of assurance.</p> <p>In PKI, used to mean to the process of checking a chain of Digital Certificates to ensure that none of the certificates have been revoked, etc.</p> <p>See also Verification.</p>
Verification	<p>The process of establishing the truth of an Assertion to some pre-determined degree of assurance.</p> <p>In PKI, the process of checking a Digital Signature.</p> <p>See also Validation.</p>