



Australian Government

Department of Finance and Deregulation

Australian Government Information Management Office

National e-Authentication Framework



January 2009

Glossary of Terms

Disclaimer

This document has been prepared by the Department of Finance and Deregulation (Finance) to provide information to government bodies in relation to the use of e-Authentication for government transactions.

While every effort has been made to ensure that the document is accurate, no warranty, guarantee or undertaking is given regarding the accuracy, completeness or currency of the document. This document should not be relied upon as legal advice. Users are encouraged to seek independent advice relevant to their own circumstances.

Links to other websites are inserted for convenience only and do not constitute endorsement of material at those sites, or any associated organisation, product or service.

ISBN 0 9758173 7 X

Department of Finance and Deregulation

Australian Government Information Management Office

© Commonwealth of Australia 2009

This work is copyright. Apart from any use as permitted under the Copyright Act 1968, no part may be reproduced by any process without prior written permission from the Commonwealth.

Requests and inquiries concerning reproduction and rights should be addressed to the:

Commonwealth Copyright Administration,

Attorney General's Department,

Robert Garran Offices,

National Circuit,

Barton ACT 2600

or posted at <http://www.ag.gov.au/cca>

Acknowledgements

Photographs taken by Steve Keough, Steve Keough Photography

Copyright: Department of Finance and Deregulation

National e-Authentication Framework Glossary of Terms¹

Term	Meaning (within NeAF context)
100-Point Check	<p>A process for evaluating Evidence of Identity for an individual, as defined by the <i>Financial Transaction Reports Act 1988</i> and administered by AusTrac.</p> <p>This process has been replaced by the National Identity Security Strategy – Proof of Identity Framework, as adopted into the Gatekeeper Evidence of Identity Policy.</p> <p>See also: Evidence of Identity</p> <p>Source: <i>Financial Transaction Reports Act 1988</i>, Gatekeeper Evidence of Identity Policy</p>
150-Point Check	<p>A process for evaluating Evidence of Identity for an individual, as defined by the <i>Financial Transaction Reports Act 1988</i> and administered by AusTrac.</p> <p>This process has been replaced by the National Identity Security Strategy – Proof of Identity Framework, as adopted into the Gatekeeper Evidence of Identity Policy.</p> <p>See also: Evidence of Identity</p> <p>Source: <i>Financial Transaction Reports Act 1988</i>, Gatekeeper Evidence of Identity Policy</p>
Access Authorisation (or 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> <p>For more detail: Dennis C. Brewer. <i>Security Controls for Sarbanes-Oxley Section 404 IT Compliance: Authorization, Authentication, and Access</i>. Wiley. 2005</p>

¹ Sources used for definitions provided in this glossary are noted in each term. Where no source is listed the definition is sourced from the original AGAF Glossary (located at <http://www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html>)

National e-Authentication Framework
Glossary of Terms

Term	Meaning (within NeAF context)
Access Control	<p>Access Control is 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) and information assets.</p> <p>Strictly speaking, Access Control is usually seen as the amalgam of Authentication, Authorisation and Audit (known as 'AAA'). However the term is often used as a synonym for authorisation or permissions management as well.</p> <p>An entity's identity claims must first be authenticated to verify that they are recognised in the system. Once the entity has been recognised, the access rights, permissions, entitlements or privileges associated with that entity are then available for use.</p> <p>Source: AGAF Glossary, RSA Glossary</p>
Access Control Rules	<p>Access Control Rules are defined and enforced within an access control system. These may examine attributes associated with an authenticated identity – e.g. role, delegation.</p>
Accreditation	<p>The act of granting credit/recognition, or certifying, that an entity has met specific requirements. This proof requires both a recognised set of requirements and a testing regime to exercise a body nominated for Accreditation against such requirements.</p> <p>In this use, the relevant example is for the through Gatekeeper Accreditation of Service Providers (Registration Authorities and Certification Authorities), which includes evaluation of their operational policies and procedures and secure facilities against Gatekeeper Policy and Criteria.</p> <p>Source: Gatekeeper PKI Framework</p>
Agency	<p>An Agency can be:</p> <ul style="list-style-type: none"> (a) a Department of State, or a Department of the Parliament, of the Commonwealth, a State or a Territory; (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); (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 (d) an incorporated company over which the Commonwealth, a State or a Territory has a controlling interest. <p>Source: Gatekeeper Glossary</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>

National e-Authentication Framework
Glossary of Terms

Term	Meaning (within NeAF context)
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.</p> <p>Source: Australian Government Protective Security Manual</p>
Agent	<p>A Legal Entity that has the capacity to act for, in the place of, or on behalf of another Legal Entity by authority from that other Legal Entity. The Legal Entity that is represented is referred to as a Principal.</p>
Assertion	<p>A statement made that purports to be true. This is the claim being made that the relying party wishes to authenticate. The term 'claim' implies that the information about the entity must be validated before being accepted</p> <p>Commonly the assertion is one of identity, but other categories of Assertion that may be subjected to Authentication include Agents, Attributes, Credentials, Data Integrity, 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> <p>A collection of Assertions (along with associated relationships) which refer to a single entity in a particular context collectively form an identity.</p> <p>Assertions can relate to 'attributes' which a subject has; 'traits' which a subject has acquired; and 'preferences' a subject stipulates.</p> <p>Source: AGAF Glossary, NEHTA Identity Management Terminology Guide</p>
Assurance	<p>A process to confirm one of several security goals to protect information and information systems, including authentication, integrity, availability, confidentiality, and accountability. Assurance is not absolute: it is a defined level of confidence. Assurance levels relating to authentication may be approached from various points of view – one of them being risk management practices and the other suitable technological solutions.</p> <p>Source: OECD Guidance for Electronic Authentication</p>
Assurance Level	<p>The level of trust that is required from e-authentication and/or the level of trust related to a particular approach to e-authentication.</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</p>

National e-Authentication Framework
Glossary of Terms

Term	Meaning (within NeAF context)
Attribute	<p>An 'Attribute' is a distinct, physical or abstract, named property belonging to an Entity or Identifier.</p> <p>Attributes are one of three types of claim which can form of an identity definition, and have an association with an identity provider to authenticate a claim about the subject being identified.</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> <p>Source: AGAF Glossary, NEHTA Identity Management Terminology Guide</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).</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>
Australian Government Protective Security Manual	<p>The Australian Government's Protective Security Manual (PSM) is Australian Government policy.</p> <p>It is the principal means for disseminating Australian Government protective security policies, principles, standards and procedures, to be followed by all Australian Government agencies for the protection of official resources.</p> <p>Source: Attorney General http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_ProtectiveSecurityManual(PSM2005)#A</p>

National e-Authentication Framework
Glossary of Terms

Term	Meaning (within NeAF context)
Authentication	<p>A function for establishing the validity and assurance of a claimed identity of a user, device or another entity in an information or communications system, by testing the credentials supplied by the entity making the claim/assertion.</p> <p>Source: OECD Guidance for Electronic Authentication, Gatekeeper Glossary</p>
Authentication Assurance Level	<p>The level of trust or confidence in the chosen Authentication Technique.</p> <p>The NeAF proposes five assurance levels (0-4): Null, Minimal, Low, Moderate, High. In this scale, the range is from level 0 (no confidence in the identity presented) to level 4 (very high degree of confidence in the identity presented).</p> <p>The assurance level is arrived at by testing the impacts of getting e-authentication wrong.</p> <p>Sources: AGAF Glossary, GSA E-Authentication Initiative²</p>
Authentication Protocol	<p>The authentication protocol addresses issues of exchange of information between the relying party and the user, protection of secret information by the user, relying party or trust-broker, etc.</p>
Authorisation	<p>Authorisation is 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 has checked if the Entity is who they claim to be, then authorisation checks what the Entity is allowed to do.</p> <p>Note that the act of Authorisation does not provide the results of a request – it merely endorses the rights of the requester to be able to receive the information.</p> <p>Source: AGAF Glossary, GSA E-Authentication Initiative</p>
Authority	<p>Permission to perform a specified act, eg: access and/or modify data; approve the registration and/or enrolment of users. This is then controlled by Authorisation systems.</p> <p>See also: Authorisation</p>
Binding	<p>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.</p> <p>With respect to EOI it is the process of establishing a linkage between an individual or entity and their claimed or documented identity in an assured manner.</p> <p>Source: Gatekeeper Glossary</p>

² <http://asc.gsa.gov/portal/template/terminology.vm>

National e-Authentication Framework
Glossary of Terms

Term	Meaning (within NeAF context)
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	<p>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.</p>
Business Entity	<p>An entity entitled to have an ABN within the meaning of s.8 of the A New Tax System (Australian Business Number) Act 1999.</p> <p>Source: A New Tax System (Australian Business Number) Act 1999</p> <p>Also refers to any entity conducting business that may or may not have an ABN, but which has a need to authenticate itself to government.</p>
Business to Business (B2B)	<p>eBusiness among Legal Persons in the form of business enterprises.</p>
Business to Government (B2G)	<p>eBusiness among Legal Persons in the form of business enterprises on the one hand, and government agencies on the other.</p>
Call-Back	<p>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).</p>
Certificate	<p>See Digital Certificate</p>
Certificate Profile	<p>The specification of the fields to be included in a Digital Certificate and the contents of each.</p> <p>Source: Gatekeeper Glossary</p> <p>For more detail: http://www.gatekeeper.gov.au.</p>
Certification Authority (CA)	<p>An important player within a Public Key Infrastructure – a service provider responsible for generating and issuing digital certificates based upon requests received from a Registration Authority (RA).</p> <p>With endorsement from a trusted CA (which is physically a digital signature from the CA on the issued certificate), users of the certificate can have confidence that this certificate has been validly issued.</p>

National e-Authentication Framework
Glossary of Terms

Term	Meaning (within NeAF context)
Challenge-Response	<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> <p>Responses may also be generated by specialised devices or Tokens held by a User. These Responses are typically generated using cryptographic processes.</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> <p>Sources: Australian Government Protective Security Manual, ACSI-33</p>
Clearance Level	<p>The formal Classification associated with a person - eg cleared to 'Highly Protected' level.</p> <p>Sources: Australian Government Protective Security Manual, ACSI-33</p>
Claim	See Assertion.
Client	<p>A generic short-form way of describing the software used by an end-user. See 'thin client' and 'fat client'.</p> <p>The term is also used by some agencies synonymously with term customer.</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>

National e-Authentication Framework
Glossary of Terms

Term	Meaning (within NeAF context)
Credential	<p>A Credential is the technology used to authenticate a user's identity. The user possesses the Credential and controls its use through one or other authentication protocols. A Credential may incorporate a password, cryptographic key or other form of secret.</p> <p>To use a digital identity in requesting access to a resource, a subject presents 'Credentials'. The Credentials (once authenticated) are taken as proof that the subject owns the digital identity being presented, and that the subject is permitted to access the resources/services which are associated with their digital identity.</p> <p>The distinction between using Credentials to establishing an identity and using Credentials as a way of establishing rights is important. It is common for a subject to own Credentials which hold both identity claims and access rights.</p> <p>A Credential may be a physical device such as a one-time-password token, a smartcard, a code book, or simply, as in the case of a username+password, the user's knowledge of the secret. It can also be 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.</p> <p>Sources: INFOSEC-99, ANSI X9.69, RSA Glossary</p>
Credential Issuer	<p>A credential issuer issues a credential to a subscriber registered by a Registration Authority. In the NeAF context, credential issuers could include government agencies and external organisations that are accredited issuers of Gatekeeper compliant certificates.</p>
Credential Management	<p>The 'lifecycle' approach associated with a credential including creation, initialisation, personalisation, issue, maintenance and cancellation.</p>
Credential Store	<p>The systems-based repository that holds electronic records of user credentials. Common credential stores include databases, directories and smart cards.</p> <p>Source: RSA Glossary</p>
Data Classification	<p>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.</p> <p>For more detail: : Australian Government Protective Security Manual</p>
Data Confidentiality	<p>The condition in which data is protected against Access by unauthorised parties, whether such data is stored or is in transmission.</p>
Data Integrity	<p>The condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.</p>

National e-Authentication Framework
Glossary of Terms

Term	Meaning (within NeAF context)
De-provisioning	<p>The withdrawing of access permissions by the alteration of 'control' records on systems relating to the authentication credentials and/or access permissions of users.</p> <p>See also: Provisioning</p>
Digital Certificate	<p>An electronic document that asserts a connection between an Identity and a cryptographic Public Key. A digital certificate is signed by the Certification Authority and:</p> <ul style="list-style-type: none"> (a) Identifies either a Key Holder and/or the business entity that he/she represents; or a device or application owned, operated or controlled by the business entity (b) binds the Key Holder to a Key Pair by specifying the Public Key of that Key Pair (c) contains the information required by the Certificate Profile. <p>There are a number of formats for Digital Certificates – X.509 and PGP are two of the most common. These two standards differ mainly in how they inter-relate to provide trust for their users.</p> <p>Sources: Gatekeeper Glossary, AGAF Glossary, RSA Glossary</p>
Digital Signature	<p>An electronic signature created using a Private Signing Key. A string of characters (or very large number) appended to a digital object that demonstrates that the originating device had access to a particular Private Key. It is 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.</p> <p>The relevant 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.</p> <p>See also: Public Key Infrastructure.</p> <p>Sources: AGAF Glossary, Gatekeeper Glossary, RSA Glossary</p>
[national] Document Verification Service	<p>The DVS is a service to be accessible to all Australian, State and Territory government document issuing agencies to strengthen and enhance existing proof of identity (POI) processes and systems.</p>
e-Authentication	<p>The process that delivers (a level of) assurance of an assertion made by one party to another in an electronic environment. In NeAF the focus is on the assurance of identities of individuals and businesses.</p>
e-Authentication Mechanism	<p>The term used to describe the combination of the credential and the credential management approach.</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>

National e-Authentication Framework
Glossary of Terms

Term	Meaning (within NeAF context)
eGovernment	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.
Encryption	Encryption, which forms part of cryptography, is the process of transforming information using an algorithm (formula) to make it unreadable to anyone except those possessing the key (cipher) used by the algorithm, or a matching/complimentary key. Two forms of encryption are commonly used for information security, symmetrical encryption and public key-based encryption (PKI). The latter is most commonly used for e-authentication.
Enrolment	<p>The act of binding of an e-authentication credential to a known instance of a user within an IT resource context (e.g. network, website, application system) in order to enable access by the user. This includes setting up permissions that enable a known user to gain:</p> <ul style="list-style-type: none"> - access to a system; - eligibility for a service; - entitlement to a service., <p>Eg a an entity, issued with a credential enrolls to transact with certain government agencies</p> <p>Multiple enrolments into various systems may occur after a user has been Registered.</p> <p>Once an identity has been created by a Registration Authority, this identity needs to be enrolled with a service provider to use a particular service. In many cases this enrolment is built into the registration process, however it is in fact a separate process from a logical point of view at least.</p> <p>Sources: AGAF Glossary, Queensland Government Authentication Framework Identity and Registration Concepts</p>
Entity	<p>An entity is the person or 'subject' (e.g. corporations, trusts, superannuation funds, and incorporated associations) associated with a digital identity. An entity may have multiple digital identities.</p> <p>Categories include objects, animals, artefacts, natural persons, and legal persons (such as corporations, trusts, superannuation funds, and incorporated associations).</p>
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>In a service delivery model credentials, if issued, are issued at the time that eligibility for a service is established rather than at point of registration. These Credentials can then be used as evidence of eligibility.</p> <p>See also: Evidence of Relationship</p>

National e-Authentication Framework
Glossary of Terms

Term	Meaning (within NeAF context)
Evidence of Relationship	<p>Evidence (e.g. in the form of shared knowledge/secrets, or documentary) used to substantiate that the presenting party has an existing relationship with the relying party (ie is already the 'owner' of a digital identity on the relying party's system).</p> <p>This may be used when existing customers are provided with a credential to enable them to undertake online dealings with a party with whom they already have an offline relationship.</p> <p>Source: NEHTA Identity Management Terminology Guide</p>
Fat Client	<p>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.</p>
Gatekeeper	<p>Gatekeeper is the Australian Government's policy and accreditation framework for the use of PKI by Australian Government agencies.</p>
Gold Standard e-Authentication Requirements	<p>The GSAR describes a gold standard approach to electronic authentication.</p> <p>This approach should be applied by government agencies where:</p> <ul style="list-style-type: none"> - the identity of an individual engaging in a transaction needs to be authenticated, and the authentication process is either wholly electronic or supported electronically; - an electronic credential issued as an output from the Gold Standard Enrolment Framework (GSEF) is employed in that authentication process; and - the risks associated with the transaction require level 4 (high) assurance under the Australian Government e-Authentication Framework (AGAF). <p>Source: Australian Government Attorney-General's Department (National Identity Security Strategy)</p>
Gold Standard Enrolment Framework	<p>The GSEF describes a premium or "gold standard" approach for use by government agencies who enrol individuals for the purpose of issuing government documents that also may function as key documents for evidence of identity purposes.</p> <p>The Gold Standard Enrolment Framework defines a high quality approach to enable the consistent and robust registration of individuals and give a strong assurance of individuals' identities.</p> <p>See also: Registration</p> <p>Source: Australian Government Attorney-General's Department (National Identity Security Strategy)</p>
Hard Certificates	<p>Digital certificates stored on a hardware token (e.g. smartcard) together with the associate private key.</p>
Identification	<p>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.</p>

Term	Meaning (within NeAF context)
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 brand names), and multiple 'id numbers' and 'id codes' assigned by other Entities that the Entity interacts with.</p>
Identities Directory	<p>Directory in which core information is held relating to identities.</p>
Identity	<p>An 'Identity' is a particular presentation of an Entity. An Identity may be an analogue for the Entity themselves, or may correspond to a Role played by the Entity, or a representative, delegate etc.</p> <p>An Identity may be used by the Entity in its dealings with one other Entity, or with many other Entities. Equally, an entity can have multiple Identities for use in different contexts.</p> <p>An organisation may maintain an Account within its records that corresponds to an Identity.</p> <p>An 'Identity' is underpinned by two types of information, as illustrated below:</p> <ul style="list-style-type: none"> - A set of 'claims' which describes a person or object (termed the subject or entity); and - A relationship/s between the subject and one or more other entities. <p>An entity may re-use the same claims for multiple identities – e.g. name and date of birth are common claims which are used to underpin many Identities which a person may hold.</p> <p>An Identity should ideally be the minimum collection of claims and relationships needed to fulfil the identification requirements for the service/system in use.</p> <p>For practical reasons, it is sometimes useful to include some additional information into an Identity record to allow use in typical situations (eg address and demographic data).</p> <p>Note that an Identity is typically only recognised by a single Identity provider. For example a Identity used to log-in to a hospital system is not a valid Identity to be used for access to the user's Internet banking system.</p>

Term	Meaning (within NeAF context)
Identity Management	<p>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.</p> <p>There are three core work and process streams in Identity Management:</p> <ul style="list-style-type: none"> - Lifecycle activities for creation, use and destruction of digital identity credentials, as outlined in the diagram below; - Procedures and policies governing the actions around the lifecycle processes; and - Technical solutions to allow the identity lifecycle activities to be performed. <p>Identity Management (or, more specifically, Digital Identity Management) is implemented by systems that support the creation, distribution, usage and ultimately destruction of the electronic records that allow the identification of entities of interest.</p> <p>An Identity Management system enables organisations to facilitate and control their users' legitimate access to resources, while protecting information from unauthorised access or use.</p> <p>Typical areas considered to be part of an Identity Management system include:</p> <ul style="list-style-type: none"> ▪ Registration ▪ Enrolment; ▪ Provisioning; and ▪ Authentication. <p>A number of other common business activities are enabled by the Identity Management system (such as Access Control), but are not generally within the core charter of Identity Management itself.</p>
Identity Provider	<p>An 'Identity Provider' offers services to enrol, provision, propagate, use, maintain and remove digital identities through a set of published mechanisms and controlled by known governance policies.</p> <p>An Identity Provider is a trusted source for identity credentials. Identity Providers can frequently also offer authentication systems for credentials issued by the system to allow identity claims using those credentials to be processed.</p> <p>Source: NEHTA Identity Management Terminology Guide .</p>
Integrity	<p>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.</p>
Intrinsic Risk	<p>The fundamental risk associated with a transaction (ie before consideration of mitigating factors).</p> <p>Source: AS/NZS 4360</p>

National e-Authentication Framework
Glossary of Terms

Term	Meaning (within NeAF context)
ISM	The document developed by the Defence Signals Directorate (DSD) to provide policies and guidance to Australian Government Agencies on how to protect their ICT systems. For more detail: http://www.dsd.gov.au/library/infosec/ism.html
Issuance	The process involved in providing a user with an authentication credential. This will be undertaken in conjunction with or following the Registration process, or in a service delivery context it will occur when eligibility is determined. See also: Provisioning
IT Security Adviser	A person nominated by the agency head to provide advice on information technology-related security issues within his or her agency. Source: ISM
Key	A string of characters used with a cryptographic algorithm to encrypt and decrypt. Source: Gatekeeper Glossary
Key Holder	An individual who holds and uses Keys and Certificates on behalf of an Organisation, or in his/her own right in the case of Individual Certificates. Source: Gatekeeper Glossary
Key Pair	A pair of asymmetric cryptographic Keys (e.g. one decrypts messages which have been encrypted using the other) consisting of a Public Key and a Private Key. Source: Gatekeeper Glossary
Knowledge-Based Authentication	A method to authenticate an individual based on knowledge of pre-existing, authenticated personal information (or other knowledge), substantiated by a real-time interactive question and answer process. Source: AS 4860-2007, RSA Glossary
Known-Customer Basis	An approach to registration which requires individuals to establish they have an existing relationship with the agency. In most circumstances, the establishment of the original relationship would have encompassed an EOI process. The 'Known Customer' approach to registration usually involves the presentation of documentary or 'knowledge' based evidence.
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. See Enrolment
Legal Entity	An Entity that is recognised at law as having the capacity to act. See Natural Person and Legal Person.

National e-Authentication Framework
Glossary of Terms

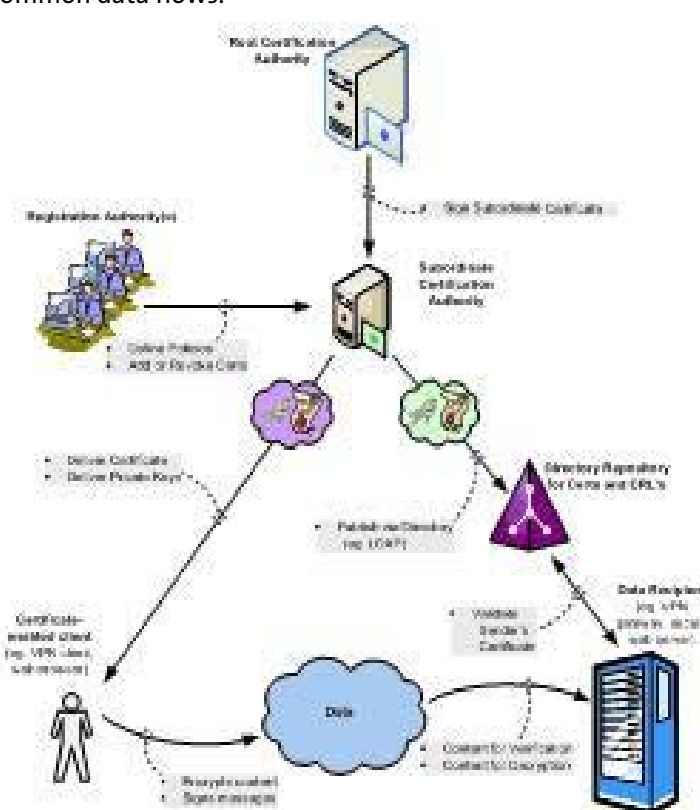
Term	Meaning (within NeAF context)
Legal Person	<p>A Legal Entity that is recognised at law, but is not a Natural Person. Examples include corporations, incorporated associations and trusts. Some government agencies are Legal Persons, in particular those established under statute, and those formed under the Corporations Law. All other government agencies form part of a single Legal Person called a body politic, such as the Australian Government of Australia, and the State of N.S.W.</p> <p>A Legal Person may perform Roles, including as Agent for other Legal Entities.</p>
Login	<p>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.</p>
LoginId	See User Name.
Malware	Software deliberately designed to damage or subvert computer process (eg Worms, viruses).
Masquerade	<p>Behaviour by an Entity as though it were another Entity. Also referred to as Impersonation or Spoofing.</p>
Mitigating Factors	<p>Factors that may reduce the level of Intrinsic Risk.</p> <p>Source: AS/NZS 4360</p>
Multi Factor Authentication	<p>An Authentication process in which multiple forms of Evidence of Identity are used, in order to increase the level of confidence in the Assertion.</p> <p>In the case of Identity Authentication, this involves two or more of the following:</p> <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').

National e-Authentication Framework
Glossary of Terms

Term	Meaning (within NeAF context)
National Identity Security Strategy	<p>A strategy of the Australian and State/Territory Governments, co-ordinated by the Australian Government Attorney Generals Department.</p> <p>The key objectives of the Strategy, as set out in the IGA and detailed in the reports to COAG, include:</p> <ul style="list-style-type: none"> - improving standards and procedures for enrolment and registration for the issue of proof of identity documents (POI) - enhancing the security features on POI documents to reduce the risk of incidence of forgery - establishing mechanisms to enable organisations to verify the data on key POI documents provided by clients when registering for services - improving the accuracy of personal identity information held on organisations' databases - enabling greater confidence in the authentication of individuals using online services, and - enhancing the national inter-operability of biometric identity security measures. <p>The strategy covers six areas:</p> <ul style="list-style-type: none"> – The Gold Standard Enrolment Framework – Security Standards For Proof-Of-Identity Documents – Gold Standard E-Authentication Requirements – The National Document Verification Service – Improving The Integrity Of Identity Data – Biometric Interoperability
Natural Person	<p>A human being, and a particular category of Legal Entity. Distinguished from a Legal Person.</p> <p>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.</p>
Non-Repudiation	<p>Strong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message or the integrity of its contents.</p> <p>Paper signatures are the traditional means of providing Non-Repudiation. Digital Signatures are a strong electronic means of providing Non-Repudiation.</p> <p>Source: American Bar Association Digital Signature Guidelines, ISO Non-repudiation Framework</p>
Onboarding	The process of Registering and Enrolling online users.

National e-Authentication Framework
Glossary of Terms

Term	Meaning (within NeAF context)
One-Time Password	Secures systems using a constantly changing password. Common implementations include using a hashing algorithm to continuously re-encode the password, or linking the password to a timer. Source: IETF RFC2289 (located at: http://www.ietf.org/rfc/rfc2289.txt)
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.
Outreach	The process of publicising agency electronic services to potential users including advising them of requirements in relation to eg e-authentication.
Password	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. 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). If a Password is disclosed or shared, Accountability is compromised. Synonyms/similar concepts are Passphrase, Personal Identification Number (PIN), Memorised Password See also: Strong Password
Permissions	A Capability, associated with an Identity, which enables Access to System Resources. Authorisation and Privilege are used as synonyms for Permission.
Permissions Management Infrastructure	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.
Permissions Store	The systems-based repository that holds the authoritative records of valid user permissions.
Phishing	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 theft.

Term	Meaning (within NeAF context)
<p>Public Key Infrastructure (PKI)</p>	<p>The comprehensive set of measures, a combination of hardware, software, people, policies and procedures, needed to create, manage, store and distribute Keys and Certificates based on public Key cryptography. This enables Public Key Technology to support the Authentication of Assertions.</p> <p>The diagram below shows a typical PKI system, along with some of the common data flows.</p>  <p>The diagram illustrates a PKI system with the following components and flows:</p> <ul style="list-style-type: none"> Root Certification Authority (top): Issues Root Subordinate Certificates to the Subordinate Certification Authority. Registration Authority(s) (left): Interacts with the Subordinate CA. Flows include Online Protocol and ADD of Eligible Certs. Subordinate Certification Authority (middle): Issues Derive Certificate and Derive Private Key to the Certificate-Enabled Client. Directory Registry for Certificate CRL's (right): Publishes Directory (eg LDAP) and provides Verify Sender's Certificate to the Data Recipient. Certificate-Enabled Client (eg VPN client, subresource) (bottom left): Encrypts content and Signs messages. Data (cloud): Contains Content for Verification and Content for Disruption. Data Recipient (eg. e-PKs, e-Forms, etc. etc. web browser) (bottom right): Receives data and performs verification.
<p>Privacy</p>	<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>

National e-Authentication Framework
Glossary of Terms

Term	Meaning (within NeAF context)
Private Key	<p>The Private Key in asymmetric Key Pair that must be kept secret to ensure confidentiality, integrity, authenticity and non-repudiation, as the case may be.</p> <p>Source: Gatekeeper Glossary</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>
Pseudonymous e-Authentication	<p>Persistent e-authentication of an entity based upon a pseudonymous credential. While the individual or business is not directly identifiable, it is possible to determine that the electronic transaction has a high probability of origination from the same user as before.</p>
Public Domain Information	<p>Official information that is authorised for unlimited public access and circulation (for example, agency publications or web sites).</p>
Public Key	<p>The Key in an asymmetric Key Pair which may be made public.</p> <p>Source: Gatekeeper Glossary</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>
Registration	<p>The processes associated with the initial unique identity record and allocation of an e-authentication credential to a user. Registration can encompass EOI and/or EOR processes..</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> <p>See also: Registration Authority, Enrolment</p>

National e-Authentication Framework
Glossary of Terms

Term	Meaning (within NeAF context)
Registration Authority (RA)	<p>A registration authority verifies the identity of a subscriber and requests a credential issuer to issue a credential to the subscriber. Whilst the term “registration authority” is most usually used in the respect to PKI environments, it is a general term and may be applied in the context of any authentication regime.</p> <p>In a PKI environment, a registration authority is an Entity that conducts a Registration process on behalf of a Certification Authority (CA).</p> <p>In Gatekeeper terms, the RA is a Service Provider that:</p> <ul style="list-style-type: none"> - is responsible for the registration of applicants for Digital Certificates by checking Evidence of Identity (EOI) documentation submitted by the applicant for its compliance with Gatekeeper EOI Policy; - is responsible for the provision of completed and authorised application form including copies of the submitted EOI documents to the relevant CA; and - may be responsible for the secure distribution of signed Digital Certificates to Subscribers. <p>An RA is an optional PKI component, separate from the CA. Alternatively, the CA may itself perform the Registration process. It is usual for there to be many RAs for one CA.</p> <p>Sources: AGAF Glossary, Gatekeeper Glossary</p>

Term	Meaning (within NeAF context)
Relationship	<p>A set of information or attributes that comprise an identity, and help bind a set of identity claims into an Identity Management context by providing linkages between the claims and other entities.</p> <p>Layering a set of Relationships over a set of claims ensures the uniqueness of a particular identity. For example, an entity may use the same name and date of birth for multiple identities. The core set of claims are identical, but the Relationships to the contexts that hold the identity account details ensures that the identities are able to co-exist.</p> <p>Tier 1: Fundamental – These types of Relationships govern the identities owned as true and personal by entity. Fundamental relationships are generally established when the identity is created, and are never changed. An example of fundamental relationship is a person’s parents.</p> <p>Tier 2: Shared – Shared Relationships are established between an entity and a service provider. Most identities used in digital context are based around shared Relationships, and these Relationships can be established and broken by the entity. Common examples of shared Relationships for an identity are customer accounts with Medicare, public utilities, membership information in airline rewards plans and so on.</p> <p>Tier 3: Abstract - These types of Relationships are generally established by the identity provider, and can be regarded collectively as demographics, most influenced by the way an entity behaves in an Identity Management context. For example, a credit card program may nominate high spend customers to gain elite rights, and may establish extra channels to facilitate this.</p> <p>Source: NEHTA Identity Management Glossary</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>
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> <p>Source: AS/NZS 4360</p>

National e-Authentication Framework
Glossary of Terms

Term	Meaning (within NeAF context)
Revocation	The process of removing a user's access rights. This will always involve changes to the system files that hold user's authentication records and details of access permissions. It may also involve having similar records amended by trusted third parties (eg CAs) and retrieval or destruction of a physical authentication token (eg smartcard).
Risk Management	A process whereby threats, vulnerabilities and risks are assessed, and a balance sought between predictable costs and uncertain benefits. 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. Source: AS/NZS 4360
Role	A pattern of behaviour adopted by an Entity. An Entity may adopt one Identity in respect of each Role, or may use the same Identity when performing multiple Roles. 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.
Role-Based Access Control (RBAC)	An approach to Access Control whereby Usernames are associated with Roles (or functional positions), within an organisation or process, rather than with individual Users.
Security	When a system is secure, users of the system know that an appropriate set of policies and controls are in place to prevent system data from being inappropriately accessed. Approaches to IT security can range from password protecting a sensitive file directory through to requiring a system of strong authentication and access controls for highly confidential information.
Shared Information	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. eg date/amount of last payment; address; date of birth
Shared Secrets	Information specifically stored in order to enable authentication. eg mother's maiden name; favourite colour; etc

National e-Authentication Framework
Glossary of Terms

Term	Meaning (within NeAF context)
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).
Single Sign-On	<p>The act of signing on once (providing a credential, (eg. UserID and Password) thereby achieving access to multiple systems or e-services without having to re-establish the identity of the person.</p> <p>SSO requires just a single authenticated connection to it from the user, and it will then handle login to downstream services automatically.</p> <p>Source: NZ Government Best Practice Framework for Authentication</p>
Smartcards	<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>
Spoofing	<p>Website 'spoofing' occurs when users are directed, usually via an email, to a fake web site which looks exactly like the real web site.</p> <p>Source: National Computer Security Center, Trusted Network, Glossary of Computer Security Terms, NCSC-TG-004, Oct. 1988</p>
Standard Business Reporting Program	<p>A multi-agency initiative that will simplify business-to-government reporting by:</p> <ul style="list-style-type: none"> - making forms easier to understand - using accounting/record keeping software to automatically pre-fill government forms and - introducing a single secure way to interact on-line with participating agencies. <p>Source: Small Business Reporting Program</p>

National e-Authentication Framework
Glossary of Terms

Term	Meaning (within NeAF context)
Step-up e-Authentication	An e-Authentication approach that seeks to achieve increased level of assurance by requesting further authentication as the assurance level of transactions increases – e.g. initial e-authentication may only require user-id and password in order for the user to view some account details, but if the user wishes to update information or view more sensitive information they may be required to enter a range of shared secrets to provide an additional level of e-authentication.
Strength of Credential	Degree of confidence that the credential type cannot be tampered with, thus that the details of the identity being authenticated by the credential are the ones that were placed on the credential.
Strong Password	A password that is difficult to guess by both humans and computer programs, effectively protecting data from unauthorised 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 name.
Subscribers	<p>An Entity who has been provisioned with an identity (eg. Private Key or Certificate) to access a system protected by access controls and open only to authenticated users.</p> <p>The notion of a subscription implies that there is an ongoing relationship to be maintained once established – whether by maintenance of business relationship, payment of dues, maintenance of skills or minimum usage.</p> <p>Source: Gatekeeper Glossary, US Government Federal Identity Management Handbook</p>
Symmetric Key Cryptography	An encryption system in which the sender and receiver of a message share a single, common key that is used to secure the message.
Thin Client	Generic user-interface software, not specific to a particular application that supports execution of applications delivered over the network. Examples include a web-browser.
Threat and Risk Assessment	<p>Formal evaluation of risk.</p> <p>First possible Threats are identified, then for each Threat its likelihood, and consequences 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>Source: AS/NZS 4360, HB231 and HB436 from Standards Australia.</p>

National e-Authentication Framework
Glossary of Terms

Term	Meaning (within NeAF context)
Token	<p>A hardware device (e.g. smart card, specialised hardware device, mobile phone), issued as a credential, that stores authentication information and may be able to perform programmatic functions (e.g. encryption).</p> <p>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>A Token most commonly takes the form of a physical object, but electronic data such as a digital certificate can also be considered a type of Token.</p> <p>Examples include 'identity cards' (especially 'photo-id'), smartcards, one-time-password devices and 'dongles'.</p>
Trojan	<p>A destructive computer program that masquerades as a harmless application - usually associated with the Internet.</p>
Trust	<p>Trust is qualified reliance on information, based on factors independent of that information.</p> <p>A Trust relationship between two organisations is generally established when a third party can 'vouch' for the organisation asking to be trusted. The level of Trust conferred will be dictated by the type of proof the third party can provide about the organisation requesting Trust.</p> <p>Trust is based not just on the entities involved in a transaction, but also their roles and the type of transaction being conducted. Trust is controlled by one party – it can be granted to, adjusted or revoked without being controlled by the other party in the relationship.</p> <p>Thus it is important to consider that in an electronic authentication context, trust is not transitive, thus is localised to the original entities.</p> <p>See also Trust Broker</p>
Trust Broker	<p>A trust-broker is a party that vouches for the user to the relying party. This could be eg a CA in the case of PKI, another organization in the case of a federated authentication scheme, a bank or credit card company, etc. A synonym for trust-broker is 'credential issuer'.</p>
Unclassified Information	<p>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.</p>
Unique Identifier	<p>A code that is assigned by a public sector organisation to identify a person for the purposes of the operations of the organisation. It includes things like a driver's licence number.</p> <p>Source: NT IPP's, Vic IPP's,</p>
User	<p>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.</p>

National e-Authentication Framework
Glossary of Terms

Term	Meaning (within NeAF context)
Username	<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 UserID.</p> <p>Normally used in conjunction with a Password or PIN, and possibly also a Token or biometric, in order to enable Authentication.</p>
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>
Validation Authority	<p>The role of a 'Validation Authority' within a PKI is to confirm that digital certificates proffered by users are not invalid, nor have been revoked by the issuing CA.</p> <p>A Validation Authority role generally acts as an abstraction layer over services which implement the tests. There are a number of mechanisms for testing certificate validity, with Online Certificate Status Protocol (OCSP) being the most widely deployed.</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>
Verifier	<p>A verifier determines, through the execution of an authentication protocol, the bonafides of a credential presented in support of a subscriber's identity claim.</p> <p>In the NeAF context, a verifier could be an agency that is also the relying party, an agency providing verifier services to other agencies, or an external party.</p>