SUBMISSION NO. 27

The House of Representatives Communications Committee

Inquiry into Cyber Crime

A submission by Australia Post
July 2009

AUSTRALIA POST

Table of Contents

Executive Summary

The purpose of this submission is to advise the Standing Committee on Communications of the important role that Australia Post plays in combating online fraud through its existing identity services.

Australia Post is investing significantly in its growing identity services business to expand its role as a trusted intermediary to build confidence between trading partners and consumers in both physical and electronic channels.

Government departments, agencies and businesses have the ability to mitigate key risks of physical and digital identity fraud by leveraging Australia Post's existing identity management services.

This submission outlines the following Australia Post services and initiatives that have direct relevance to three of the Inquiry's terms of reference:

(1) Measures currently deployed to mitigate e-security risks by Australian consumers:

Australia Post's **VIP Online Security** currently provides online service providers and their customers with access to a solution to deal with the problem of unauthorised access to and use of online services. It incorporates a unique combination of features that differentiates it from conventional approaches and offers a low cost, whole-of-community solution available to Australian citizens, businesses and government agencies.

(2) Future initiatives that will further mitigate the e-security risks to Australian internet users; and

(3) Emerging technologies to combat these risks:

Australia Post is expanding its existing **identity and verification services** to include:

- A multi-channel solution to support identity management services integrating workflows across online, in person and telephone channels;
- Visual document inspection combined with electronic verification of documents (back to source) and/or background list screening to reflect the risk level of the transaction; and
- Biometric capture systems (digital cameras, signature capture, etc), which will be progressively rolled out nationwide, starting July 2009, to allow additional security features to be incorporated into credentials.

Together, these initiatives will reduce online identity fraud, build trust within the online community and assist government and business to fully realise the benefits that flow from the online delivery of services.

Introduction

Australia Post is held in high regard in the Australian community and is one of Australia's most trusted brands.[1] In 2009, Australia Post ranked first for reputation in a study of Australia's 60 biggest companies.[2]

Much of this trust has been earned by Australia Post over the past 200 years by acting as a neutral intermediary between the senders and receivers of letters and parcels. This has culminated in the privileged position that Australia Post holds today in the delivery of banking, bill payment and money transfer services on behalf of the business sector nationwide. Australia Post's trusted reputation also underpins its solid track record as a provider of face-to-face identity and verification services.

Today, Australia Post performs more than 3 million physical identity checks each year. It undertakes a wide range of identity services on behalf of both federal and state government agencies, including more than 90% of Australian Passport interviews, British Passport applications, Working with Children Checks, Maritime Security Industry Checks, WorkSafe Applications for High Risk Work and Drivers Licence Applications. As an experienced provider of identity services, Australia Post has a sound understanding of the identity landscape in Australia and the underlying issues that confronts the government and business sectors. Australia Post is an accredited Registration Authority under the government's Gatekeeper scheme.

This submission outlines key areas within Australia Post's identity services which have direct relevance to the Inquiry's terms of reference:

(1) Options to leverage Australia Post's existing Identity Services Business

(2) Australia Post's Electronic Authentication Service (VIP Online Security)

[1] Eye on Australia, 2008
2 AMR Interactive, 2009

(1) Options to leverage Australia Post's Identity Services Business

International terrorism, increased demand for access to secure online services, concerns about identity-related crimes, and increasingly sophisticated demands for the protection of personal information and privacy are driving the need for more robust identity procedures. Governments are responding with a range of measures including stronger cross-border collaboration, stronger legislation and regulation around granting and protection of identities, and the adoption of new technologies, designed to more effectively collect, manage and protect identity-related information.[3]

Australia Post has observed a number of key changes in the business sector in response to national regulatory and industry changes:

- The drive for cost reduction while expanding access to services has driven significant growth in on line transactions between government and business, business and business and business and consumers;
- As the 100 point check is superseded by new Anti Money Laundering/ Counter Terrorism Financing Act 2006 legislation, identity requirements are extended to approximately 8,000 registered entities;
- Major financial institutions have started to issue smartcards to combat credit card fraud and increase on line payment security. Smart cards can be used in person or on line for authentication purposes and depending on the transactional risk levels, may incorporate biometric identifies in the future;
- Increased employment vetting is being driven by greater employment mobility, increases in employer regulatory requirements for warranty and liability regarding employees and contractors.

Australia Post has identified a number of key themes emerging in the Australian marketplace:

- A new emphasis on identity credential enrolment procedures which reflect the transactional risk level associated with the credential (driven by the Australian Government's National e-Authentication Framework 2009 and Risk Standard AS/NZS 4360);
- The need to ensure that people can 'appropriately' enrol for services via a range of channels (online, in person and telephone) or an integrated set of channels (e.g. start in one, finish in another);
- The importance of creating trusted technology and human interfaces across multiple parties, including governments, businesses and consumers;
- The need to be able to re-issue credentials and to provide accessible, effective support in the event credentials are lost, stolen, faulty etc ;
- The need to provide citizens and consumers with strong assurances on data privacy and security as well as choices and easy paths to adoption and use.

In May 2009, Australia Post commenced the first phase of investment in:

- A multi-channel solution to support identity management services integrating workflows across online, in person and telephone channels. This helps to achieve cost savings by matching the appropriate process rigour with the risk profile of the transaction;
- Visual document inspection will be combined with electronic verification of documents (back to source) and/ or electronic identity verification using background list screening to reflect the transactional risk level of the enrolment;
- Biometric capture systems (digital cameras, signature capture, etc) will be installed in key outlets to allow integration of additional security features into credentials. Future work is planned around voice-print enrolment for authentication solutions based on speech recognition.

These capabilities have been designed to address key needs associated with:

- Compliance to legislation and regulation;

[3] Based on Market Trend research and analysis commissioned by Australia Post

- Channel extension and/ or integration, recognising some businesses and government agencies either have little or no service delivery channels;
- Work flow management processes to ensure management and transparency across channels;
- Cost effectiveness by supporting the relevant combination of 'channel' activities to deliver a streamlined, secure process;
- Support and recognition of a risk based approach to process design, although it is recognised that many are still unclear on where their particular activity sits in the risk context.

Australia Post has also sought to support the key Federal Government principles and frameworks reflected in:

- The National identity Security Strategy, specifically the Australian Government e-Authentication Framework 2009, the Risk Standard AS/NZS 4360) and the Gold Standard Enrolment Framework;
- e-government strategies;
- emerging channel management objectives.

Online Forms

Australia Post's Online Forms Management service is a complete approach to online data capture including form design, hosting and systems to facilitate convenient, accurate, efficient collection and processing of information.

Well designed Online Forms means convenient access for customers and guidance to assist them to provide accurate, complete and correctly formatted data. This enhances the customer experience and offers business and government improved data quality, reduced compliance costs and more timely business processes.

Australia Post can design online form solutions to meet specific business requirements and can draw on a range of supporting options including online help, data validation, secure hosting, version control, print options, 2D bar codes and talking forms. The solutions design can, where appropriate, incorporate Australia Post's network of Post Offices to provide face-to-face identity checks, document verification, form lodgement and payment services. Electronic integration with both upstream and downstream systems enables data to be handled efficiently according to programmed business policies and procedures.

Electronic Screening

Australia Post's face-to-face identity checks (including 100-point and AML ID checks), have recently been expanded to include Australia Post's Electronic Screening service. This turn-key, managed service incorporates the electronic screening of individuals against proprietary and public access data-sets to verify identities and flag potentially high-risk applicants.

The combination of Australia Post's physical and electronic channels offers a comprehensive solution assists business and government reporting entities in meeting their AML/CTF requirements.

Australia Post's Electronic Screening service has been developed in conjunction with leading providers of electronic screening systems and uses well proven data sources. The service involves the screening of individuals against agreed databases to confirm basic identity (name and address, D.O.B, as well as other data as required). It also screens against exception and watch-lists (such as DFAT and politically exposed persons).

The solutions design can incorporate Australia Post's network of Post Offices to provide face-to-face identity checks, document verification, form lodgment and payment services. It can be integrated with client systems to facilitate efficient and timely processing that is scalable to meet volume fluctuations.

(2) VIP Online Security Two Factor Authentication

Another of Australia Post's identity related services that has direct relevance to the Terms of Reference of this inquiry is VIP Online Security, a robust, long term solution backed by the combined stability, strength and trusted reputation of Australia Post and VeriSign. It provides a solution to the problem of unauthorised access to online services and accounts. It is currently being used by 25 businesses in Australia (17 financial institutions for internet banking) and 47 businesses globally (including eBay and PayPal). Almost 100,000 VIP credentials are already in the hands of Australians and over 1.8 million have been issued globally.

Two factor authentication is a well established authentication protocol that adds an extra layer of security when accessing online services and accounts. It requires the end user to present two factors. The first factor is something the person knows such as user name and password. The second factor is something the person has such as a credential (or token) that displays a one-time password (OTP). Attacks such as phishing or spyware may successfully steal the first factor, however, without the second factor, the cyber criminal cannot gain access to the account or service.

Two factor authentication has been used for many years in closed enterprise environments. However, its potential for widespread adoption has been limited by the cost of purchasing and distributing credentials and more so by the necklace of tokens problem. This name is commonly given to the problem that arises when the end user is required to keep multiple credentials (or tokens) on hand in order to access various online service providers. Australia Post's VIP Online Security overcomes both of these long standing barriers to the widespread use of two factor authentication. Through an innovative shared network concept, VIP Online Security shares both the back end infrastructure and the front end credential without compromising the security integrity of the solution. This allows the customer to use one credential (e.g. mobile phone) for access to multiple online accounts.

A Whole-of-Community Approach

The combination of the shared network and the reduced reliance on tokens is unique in the Australian marketplace and provides the foundation for the creation of a ubiquitous open, low cost, authentication network accessible to the online community across Australia. Business and government online service providers will have access to a widespread community of end users who are already enabled to use the VIP network.

The VIP Online Security solution incorporates a downloadable application that transforms the mobile handset into a one-time-password (OTP) generator (equivalent to the traditional token). This overcomes the need for the end users to carry a separate device and reduces the online service provider's need to purchase and deliver tokens. There is no charge to end users or VIP network members to download the mobile credential download.[4] Physical tokens will continue to be a part of the credential mix for most VIP network members but their use will decline as free mobile phone credentials become more widely used in the community.

VIP Online Security is a security-as-a-service model that requires no upfront investment and no joining fees. Once registered, online service providers pay a monthly fee based on the number of credentials activated by their customers. This fee includes unlimited validations of their customers' one-time passwords. The VIP Online Security business model transforms the acquisition cost of online security from a significant capital expenditure commitment to a minimal operating expense.

Although back end infrastructure is shared, all VIP network members maintain control over their own business rules and their customers' online experience. End users and VIP network members remain protected, as the service does not store any user account or identity information and no data is, or can be, transferred between VIP network members.

[4] A fee may be charged by the mobile phone carrier for the initial download

Based on the National e-Authentication Framework (NeAF) "Better Practice Guidelines Vol 1", VIP Online Security is an authentication mechanism appropriate for applications requiring "Moderate" assurance levels and has a credential strength rated Level 3 according to the methodology. It meets a range of the NeAF stated objectives including:

- enhanced community confidence
- consistency across agencies and jurisdictions
- re-use of credentials
- sharing of infrastructure
- extensibility

The Technology

VIP Online Security is enabled by an exclusive partnership with VeriSign®. VeriSign is a leading international provider of Internet infrastructure services (www.verisign.com.au). Further technical details of the VIP platform and information about the VIP Access for Mobile can be found at: https://vipdeveloper.verisign.com/vip/home.jsp. IT specialists can examine and test all technical aspects of the VIP Online Security two factor solution and download software development kits (SDKs), FAQs and white papers.

Conclusion

Australia Post is assisting government and business to mitigate the risk of identity fraud through the following service initiatives:

1. The expansion of Australia Post's Identity and Verification Services; and
2. VIP Online Security.

Raising awareness of Australia Post's capabilities and assistance in engaging with relevant government agencies on common industry issues is always appreciated. As an experienced provider of identity services, Australia Post can make a meaningful contribution to the development of trusted national identity solutions.

These initiatives address the terms of reference for the committee:

1. Measures currently deployed to mitigate e-security risks by Australian consumers;
2. Future initiatives that will further mitigate the e-security risks to Australian internet users; and
3. Emerging technologies to combat these risks.

Contact Information

Any inquiries about this submission should be forwarded to:

Paul Burke
Manager, Board & Shareholder Liaison
Australia Post
Telephone: +61 3 9204 7115
Fax: +61 3 9204 7478
E-mail: paul.burke@auspost.com.au

Glossary of Terms

Term	Meaning in the context of this submission
100 point check	A process for evaluating Evidence of Identity for an individual, as defined by the Financial Transaction Reports Act 1988 and administered by AusTrac. Source: NeAF Glossary
Access Authorisation	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). 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. Source: NeAF Glossary
Access Control	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. 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. 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. Source: NeAF Glossary
Accreditation	The act of granting credit/recognition, or certifying, that an entity has met specific requirement. This proof requires both a recognised set of requirements and a testing regime to exercise a body nominated fro Accreditation against such requirements. In this use the relevant example is the 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. Source: Gatekeeper PKI Framework. Source: NeAF Glossary
Agency	An Agency can be: (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. Source: Gatekeeper Glossary

Assurance	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. Source: NeAF Glossary
Assurance Level	The level of trust that is required from e-authentication and/or the level of trust related to a particular approach to e-authentication. Source: NeAF Glossary
Attribute	An 'Attribute' is a distinct, physical or abstract, named property belonging to an Entity or Identifier. 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. 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. Source: NeAF Glossary
Authentication	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. Source: OECD Guidance for Electronic Authentication, Gatekeeper
Authentication Assurance Level	The level of trust or confidence in the chosen Authentication Technique. 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). The assurance level is arrived at by testing the impacts of getting e-authentication wrong. Sources: NeAF
Authentication Protocol	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. Source: NeAF Glossary
Biometrics	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: • 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. Examples include: fingerprint, voice-print, iris-scan. Source: NeAF Glossary

Credential	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. 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. 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. 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. Source: NeAF Glossary
Credential Issuer	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. Source: NeAF Glossary
Document Verification Service	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. Source: NeAF Glossary
e-Authentication	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. Source: NeAF Glossary
eBusiness	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. Source: NeAF Glossary
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. Source: NeAF Glossary

Enrolment	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: • access to a system; • eligibility for a service; • entitlement to a service. Eg a an entity, issued with a credential enrols to transact with certain government agencies. Multiple enrolments into various systems may occur after a user has been Registered. 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. Sources: NeAF
Evidence of Identity	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). 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. Source: NeAF Glossary
Gatekeeper	Gatekeeper is the Australian Government's policy and accreditation framework for the use of PKI by Australian Government agencies. Source: NeAF Glossary
Gold Standard e-Authentication Requirements	The GSAR describes a gold standard approach to electronic authentication. This approach should be applied by government agencies where: • 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). Source: NeAF Glossary
Gold Standard Enrolment Framework	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. 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. Source: NeAF Glossary
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. Source: NeAF Glossary

Identity	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. 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. An organisation may maintain an Account within its records that corresponds to an Identity. An 'Identity' is underpinned by two types of information, as illustrated below: • 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. 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. An Identity should ideally be the minimum collection of claims and relationships needed to fulfil the identification requirements for the service/system in use. 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). 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. Source: NeAF Glossary
Identity Provider	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 polices. 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. Source: NeAF Glossary
Mitigating Factors	Factors that may reduce the level of Intrinsic Risk. Source: AS/NZS 4360
Multi Factor or Two Factor Authentication	An Authentication process in which multiple forms of Evidence of Identity 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: • 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'). Source: NeAF Glossary

National Identity Security Strategy	A strategy of the Australian and State/Territory Governments, co-ordinated by the Australian Government Attorney Generals Department. The key objectives of the Strategy, as set out in the IGA and detailed in the reports to COAG, include: • 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. The strategy covers six areas: • 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 Source: NeAF Glossary
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: NeAF Glossary
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. Source: NeAF Glossary
Privacy	The interests that Natural Persons have in sustaining a 'personal space', free from interference by other people and organisations, andin controlling information about themselves. It has multiple dimensions, including privacy of the physical person, privacy of personal behaviour, privacy of personal communications, and privacy of personal data. A variety of privacy rights are conferred by international instruments, and by the laws of most jurisdictions. 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. Source: NeAF Glossary
Provisioning	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. Source: NeAF Glossary

Registration	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.. Multiple enrolments may occur after a user has been registered. Although 'registration' and 'enrolment' are sometimes used as synonyms, a distinction is being drawn here between the two terms. See also: Registration Authority. Source: NeAF Glossary
Registration Authority (RA)	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. In a PKI environment, a registration authority is an Entity that conducts a Registration process on behalf of a Certification Authority (CA). In Gatekeeper terms, the RA is a Service Provider that: • 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. 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. Sources: AGAF Glossary, Gatekeeper Glossary
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
Single factor authentication	An Authentication process in which a single form of Evidence is used to authenticate the user. In the case of Identity Authentication, this involves one of the following: • 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). Source: NeAF Glossary
Smartcards	A hardware token, usually taking the form of a credit-card sized plastic card with an embedded chip. May be used as a hardware token to carry information for authentication including digital certificate. Source: NeAF Glossary

Token	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). 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. 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. Examples include 'identity cards' (especially 'photo-id'), smartcards, one-time-password devices and 'dongles'. Source: NeAF Glossary
Trust	Trust is qualified reliance on information, based on factors independent of that information. 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. 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. Thus it is important to consider that in an electronic authentication context, trust is not transitive, thus is localised to the original entities. Source: NeAF Glossary
Trust Broker	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'. Source: NeAF Glossary
Validation	The process of establishing the truth of an Assertion to some pre-determined degree of assurance. 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. Source: NeAF Glossary
Verification	The process of establishing the truth of an Assertion to some pre-determined degree of assurance. In PKI, the process of checking a Digital Signature. Source: NeAF Glossary