



Australian Government

Information Management Office

Australian Government Electronic Authentication Framework

Exposure Draft

This is an exposure draft of the Australian Government Electronic Authentication Framework. The Australian Government Information Management Office would be grateful for your comments on this draft by Friday 21 May 2004.

Comments may be forwarded to:
agaf@agimo.gov.au, or call 02 6271 1317.

Introduction

Online transactions between business and government are becoming more common.

Australian businesses frequently interact with Australian Government departments and agencies on a wide range of matters. These interactions range from general information enquiries, making applications and payments, lodging tenders, and providing services on behalf of government.

Increasingly, businesses are interacting with government agencies via electronic and digital environments—such as the internet or phone based services. This provides advantages to both businesses and government, for example, around the clock services, shorter waiting times for services, paperless interaction with government, and streamlined processes. Businesses are now able to complete many government administrative requirements online, whether it be form-filling, seeking access to business assistance programs, undertaking a transaction or submitting tax returns.

Businesses are taking advantage of the benefits of transacting online.

The volume of e-commerce and online transactions is increasing rapidly. Latest statistics from the Australian Bureau of Statistics indicate that in 2002-03, 485 000 Australian businesses (or 71% of all businesses) used the internet. Business internet income was \$24.3 billion in 2002-03, up from \$11.3 billion in the previous year.¹ The number of businesses who have received orders via the internet has doubled in the past year. During 2002-03:

- 71% of businesses using the internet accessed a government service online
- 21% of businesses using the internet lodged taxation forms online
- 28% of businesses using the internet made payments online
- 42% of businesses using the internet sought information or services related to taxation
- 35% of businesses using the internet sought information on regulations, and
- 26% of businesses using the internet sought information on employment.²

¹ Australian Bureau of Statistics, *Business Use of Information Technology 2002-03*, 8129.0, 17 March 2004, p.3.

² *Ibid.*, p.12.

An e-government Benefits Study³ published in April 2003 examined the attitudes of both businesses and individuals, as users of e-government services. It found that businesses saw improvements in costs and decision-making from undertaking online transactions with government.

However, business and government need assurance that these transactions are authentic.

When transacting online, there will be occasions where businesses and the government agency will need to be completely assured of each other's identity and the legitimacy of the assertions that are being made. These assertions may relate to a range of attributes such as identity, professional qualification, or that a person is authorised to conduct a specific transaction. The need for assurance is particularly important when funds or sensitive information is involved. The process of establishing the legitimacy of assertions, be they identity or other attributes, is the key element of **business authentication**.

Broadly speaking, business authentication relies on one or both of the following:

- something that a business knows, such as a password or PIN
- something that a business has, such as a smart card or a token.

The risks of not authenticating the claims of each party may be high.

If users are not properly authenticated, situations such as illegal transfer of funds, unauthorised ordering of goods, or the mischievous alteration of data may occur. Authentication underpins confidence and builds trust in electronic transactions and is a vital component of e-commerce.

As digital and phone based transactions increase in complexity, and practices such as "spoofing" (fake websites) and identity fraud have an increased impact, the risks and exposures to businesses and government increase. Government and business both need to assess the risks associated with these transactions, and implement appropriate processes and solutions on access and authorisation.

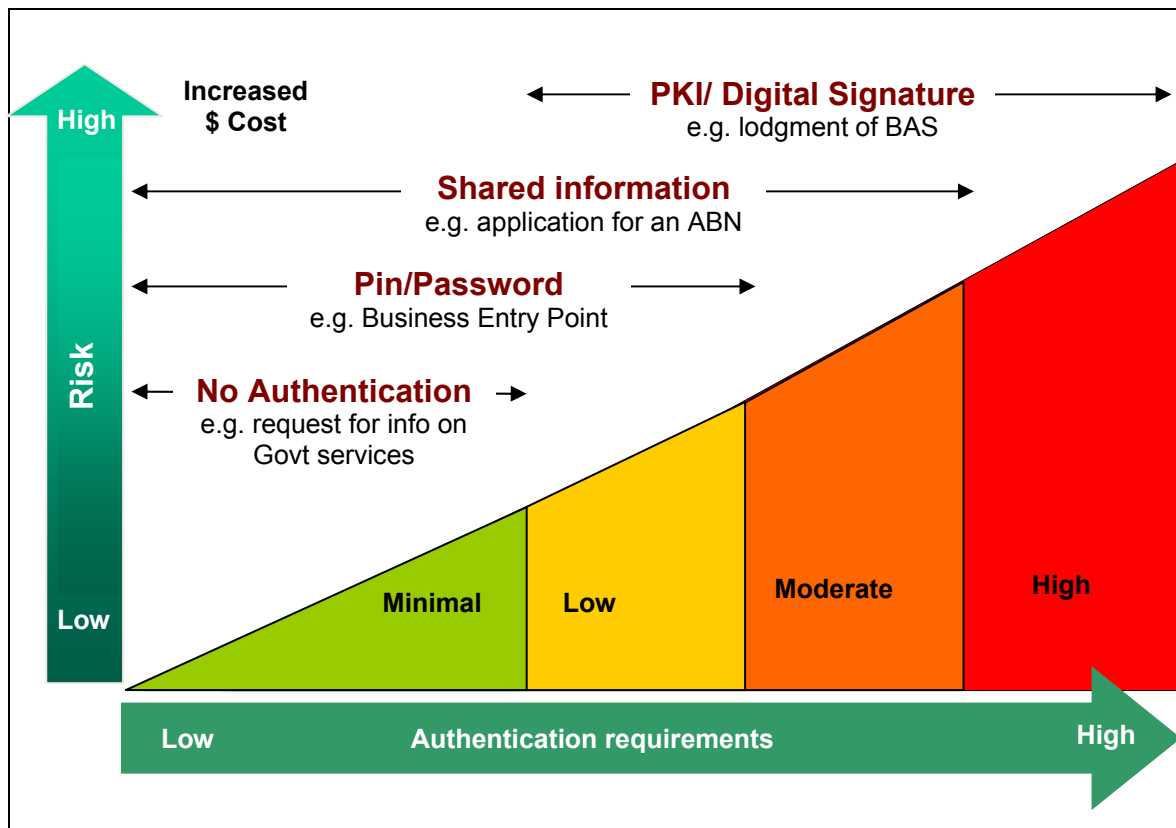
³ National Office for the Information Economy, *e-Government Benefits Study*, April 2003, p.8.

The AGAF will provide a consistent approach to government authentication.

The Government is working towards the implementation of an *Australian Government Authentication Framework* (AGAF) that provides a whole-of-government approach to authentication. The Australian Government recognises that different authentication techniques are needed for different types of transactions, depending on how much risk is involved. The AGAF aims to ensure that Australian Government agencies apply a consistent approach when making decisions about appropriate authentication methods. The AGAF will ensure that Australian Government agencies implement authentication mechanisms that correspond with the level of risk in the transaction.

Diagram 1, *Business Risks and Authentication Requirements*, highlights how the level of authentication should increase as the risks inherent in a transaction increase to either the businesses or the government.

Diagram 1: Business Risks and the range of Authentication Requirements and Techniques



What is the Australian Government Authentication Framework?

By adopting a consistent approach for selection of authentication mechanisms, the Australian Government will:

The AGAF provides consistency, trust and is cost effective.

- provide consistency of experience and expectation for businesses using government online services
- build trust within the business and government community by providing online services supported by authentication structures which are useful, safe and do not impinge upon privacy
- ensure consistent and auditable risk management is applied to authentication across government
- provide simple and lowest cost options for businesses to deal securely online with government, and for government to transact with business.

The AGAF does not propose a national ID system, or a central registry of personal or commercial information and attributes.

The AGAF proposes an approach to authentication based around four levels of risk that are matched to the risk of the transaction. For a more detailed discussion of each level see **Appendix A**.

Diagram 2: Australian Government levels of risk assurance

Level 1	Level 2	Level 3	Level 4
Minimal risk	Low risk	Moderate risk	High risk
No requirement for confidence in the assertion	Some confidence in the assertion	Moderate confidence in the assertion	High confidence in the assertion

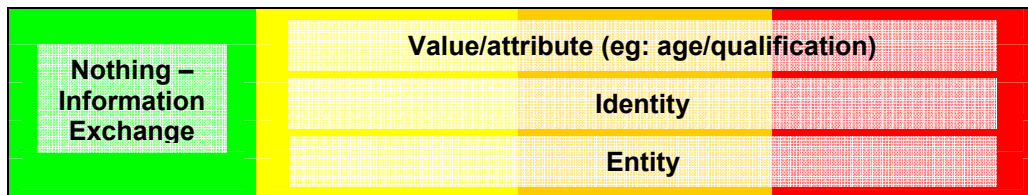
Diagram 3 illustrates the different types of risk levels, authentication categories, and authentication methodologies. It outlines three steps that government agencies will go through when determining the sort of authentication mechanism it will use.

Diagram 3: The AGAF

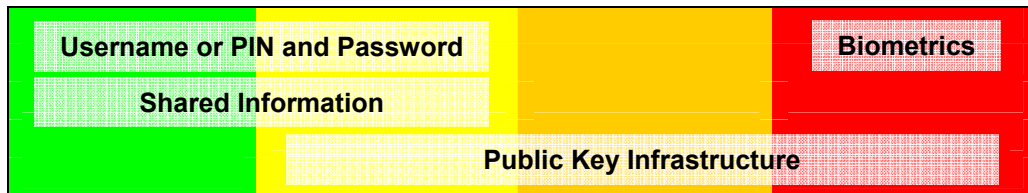
STEP 1: RISK OF TRANSACTION



STEP 2: WHAT IS BEING AUTHENTICATED?



STEP 3: AUTHENTICATION MECHANISMS



After assessing the level of risk inherent in the transaction, the government agency would examine what needs to be authenticated in order to guarantee trust in the transaction. Once these have been determined, an appropriate authentication mechanism would be selected.

Diagram 3 illustrates that low risk transactions will use low level authentication mechanisms such as username and password. Highly sensitive or high risk transactions will require high level authentication mechanisms such as Public Key Infrastructure. For example:

- a simple online enquiry that seeks information on a government program would constitute a minimal level of risk, therefore no authentication would be required
- payment for goods or services online usually requires that an attribute of the business (e.g. a valid credit card) be authenticated. Should information about the identity of the buyer or seller be false, this would constitute a moderate risk to the receiver of the false information. Accordingly, an appropriate authentication method requiring moderate assurance is applied, such as username and password
- quarterly business activity statements are lodged with the Tax Office. In this example, the need for assurance that the person is authorised to transact on behalf of the business entity is moderate to high. There is a risk that substantial damage could arise if financial data is intercepted and altered by a third party. A high assurance authentication methodology, e.g. Public Key Infrastructure, is used.

As illustrated in Diagram 3, techniques to authenticate are capable of operating across a range of risk levels. PIN and passwords as well as Public Key Infrastructure can provide authentication across a range of risk levels.

Businesses should be aware, however, that the overall security of their systems will rely on them having appropriate authentication methods, adequate and up-to-date virus protection software and firewalls.

Current practices

Currently, most users of online services employ a username/password approach to authentication. As the environment becomes more complex, the exposure to risk increases for all parties. Therefore, there is a need for the Australian Government to implement an approach to online authentication which allows multiple authentication techniques that can respond to different levels of risk.

Implications for business will be considered when choosing an authentication mechanism

The AGAF provides guidance to help government agencies decide on a particular authentication technique. It also helps the business community see how that decision was arrived at. Issues that will be considered when a government agency decides on a technique will include:

- the potential harm that would arise if the assertion being authenticated were accepted as true when it was actually false

The AGAF will ensure that businesses are not subject to time-consuming authentication processes if the risks are low

- the legal and public policy issues (including privacy) that would affect the use of the technique
- whether the technique is widely understood and used by the business community
- the willingness of the businesses to participate in the required authentication process
- the availability and reliability of the enabling infrastructure, services and solutions to support the authentication technique
- the financial implications of the technique for business clients, and for the Australian Government, and whether this is acceptable
- whether any negative impacts of the technique are justified by benefits.

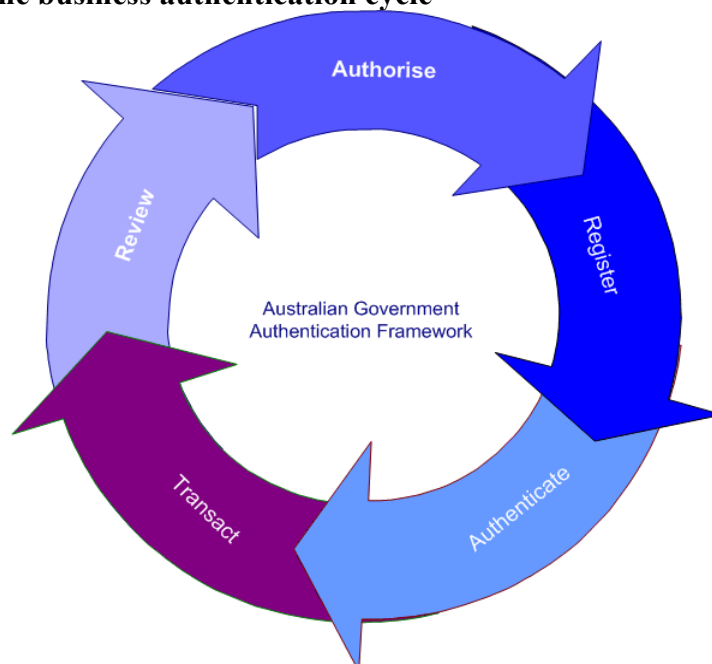
Appendix B outlines some examples of current types of online transactions undertaken with government, and the authentication techniques used.

What steps must businesses take to interact with Government?

To transact in an environment that requires authentication, businesses will need to establish access and authorisation processes so that their designated office holders can transact with government on behalf of the company. Specifically, businesses will need to:

1. **Provide Authority**—businesses will select an office holder(s) and provide them with the authority to transact online on behalf of the company to access specific government applications
2. **Register**—businesses will register these officers with government agencies allowing them to make transactions using the appropriate authentication process
3. **Authenticate**—the business representative’s right to transact is checked through an authentication mechanism, e.g. PIN/password. The government agency may then check that the representative has the authority to access specific applications
4. **Transact**—the business representative proceeds to transact online with the government
5. **Review**—the business reviews its authorised office holder position, in line with its normal business practices, to ensure that the position should continue to function as the business’s authorised officer.

Diagram 4: The business authentication cycle



The process involved in registering and authenticating businesses will differ according to the requirements of each government agency. Generally, the requirements on businesses will rise as the risks rise. This is a safeguard for both business and government. As a matter of good governance, businesses should keep registers of their employees' access rights to government online applications as part of a business's delegations systems.

Authentication mechanisms

The online services that the Australian Government provides involve different levels of risk to business and government, and require different authentication mechanisms. The key is to choose the most appropriate and effective method while minimising costs for both business and government. The different types of authentication techniques proposed by the framework are set out in Table 1:

Table 1: Authentication mechanisms

<p>Shared Information (also called a challenge/response system)</p>	<p>Business users wishing to be authenticated provide answers to a series of questions posed by the government agency involved in the transaction. The questions should represent information which only the valid user should know. The information is shared only between the specific agency and the business. The information could be of three types:</p> <ul style="list-style-type: none"> • fixed data on file (e.g. date of birth) • variable data (e.g. date and amount of last payment/receipt/claim) • specifically designed shared secrets (where the user provided a series of questions and answers to the agency). <p>Risk levels: Minimal to moderate.</p> <p>Expected implications for businesses: relevant staff will need to keep a record of information supplied and keep this secure.</p> <p>Current Government applications: application for an Australian Business Number.</p>
<p>Username/Password</p>	<p>Authentication occurs by business users presenting a username and password. These passwords are valid only with one agency. It does not allow businesses to use the same password with other agencies.</p> <p>Risk levels: Low to moderate – however it is becoming more widely used in higher risk applications, especially if it is used in conjunction with another authentication mechanism such as shared information.</p> <p>Expected implications for businesses: relevant staff will need to keep a record of usernames/passwords and keep this secure.</p> <p>Current Government applications: Customs lodgements and payments, some Job Network transactions, business visas, patent applications, Business Entry Point, some Centrelink transactions.</p>
<p>One-time passwords</p>	<p>A one-time password is a system that generates unique and different passwords each time an application or service is accessed. It uses a hardware device to generate the unique password which must match the username. Businesses would pre-register and be issued with a username and the hardware device. When a user enters a website protected by a</p>

	<p>one-time password, they would be asked for the latest password displayed on the device. The agency would know which password is valid at that time for that user. The synchronised password would change periodically.</p> <p>Risk levels: Moderate to high.</p> <p>Expected implications for businesses: relevant staff would need to safeguard the hardware device to ensure that it isn't lost or stolen. Costs can be high.</p> <p>Current Government applications: Members of Parliament utilise one time passwords.</p>
<p>Public Key Infrastructure (PKI)</p>	<p>PKI is a technology and set of procedures that enables users to authenticate their identity, and to securely and privately exchange information through the use of public key cryptography.⁴ To achieve this, public and private keys and a digital certificate are obtained through a trusted third party authority, known as a Certification Authority (CA).⁵</p> <p>The Certification Authority then links the public key to the digital certificate and vouches for the identity of the key holder. Registration Authorities then collect appropriate levels of Evidence of Identity from business users.</p> <p>Business users are issued with a public key which everyone can see, and a private key which encrypts a set of information to attest to the authenticity of the sender and the data integrity of the information sent. The business user sends information signed with their private key. The receiver verifies the message by checking the data with the business's public key. If the message has been tampered with, or if a third party is trying to pose as the user, the receiver will not be able to read it if it has been encrypted, nor validate the signature. This ensures that information flowing between a PKI-enabled business and a PKI-enabled government agency has a high level of non-repudiation, which means that neither party can deny that a transmission was sent or received. Also, the information cannot be read if encrypted, or surreptitiously altered.</p> <p>PKI authentication credentials are capable of being used in multiple government agencies, however, the costs to the business user are currently high.</p> <p>Gatekeeper is the Government's strategy for evaluating trust in PKI services provided to or employed by government. The Gatekeeper accreditation process for Certification Authorities and Registration Authorities provides high certainty and trust for all parties involved in the use of Gatekeeper accredited digital certificates. The Australian Business Number Digital Signature Certificate (ABN-DSC) is intended for business-to-government use. Australian Government agencies intending to use PKI for supporting online transactions are required to use Gatekeeper accredited PKI capabilities and services.</p> <p>Risk levels: Low to high, however PKI is currently used in mainly high risk transactions due to its current cost.</p> <p>Expected implications for businesses: Special software will be required</p>

⁴ A "key" is a string of characters used with a cryptographic algorithm to encrypt and decrypt.

⁵ For a full list of Gatekeeper accredited Certification Authorities and Registration Authorities, see www.agimo.gov.au/infrastructure/gatekeeper/accreditation

	<p>and staff members will have to undergo an evidence of identity exercise before keys and certificates are activated. Costs will vary.</p> <p>Current Government applications: Defence suppliers, healthcare provider systems, Pharmaceutical Benefits Scheme, the ATO Business Portal and Electronic Commerce Interface for lodgement of Business Activity Statements and a range of other business transactions.</p>
Biometrics	<p>A representation of a fingerprint, hand, iris-scan, voice pattern, etc. is used to identify the user. A biometric identifier can be used in a similar way to passwords to demonstrate ownership of a token or smartcard.</p> <p>Risk levels: Moderate to high.</p> <p>Expected implications for businesses: Relevant staff would need to be comfortable about registering their physical attributes and have trust in the security of this data.</p> <p>Current Government applications: None. However, Australians wishing to visit the US on business or leisure without a visa will be required to have a biometric identifier in their passports by the end of 2004. In addition, Customs and Immigration are trialling “Smartgate” which is a biometric facial recognition system for international air passengers and crew.</p>

The future of authentication

If risks rise, authentication will become more important.

Currently, most users of online services are authenticated via simple usernames and passwords in both government and the private sector. Transactions requiring high assurance authentication protocols represent only a small segment of market activity. How sustainable this will be in the longer term is an open question as practices such as “spoofing” (fake websites) and identity fraud have an increased impact. If fraudulent practices become more prevalent and serious, or the complexity of transactions deepens, there may be a need for more rigorous authentication solutions. Government and business need to be prepared to raise authentication levels based on their assessment of the evolving risks.

Therefore, government and business must be ready to respond to any increasing risk

There are many different authentication mechanisms that can meet this need, depending upon the specific nature of the risk, and the broader environment in which the transaction is undertaken. It is in the interests of all parties that the government now considers the way it needs to interact with businesses, and that its authentication mechanisms are aligned to the level of risk in each transaction.

This approach is consistent with developments overseas.

The AGAF is consistent with developments internationally where governments are working towards building mutual trust to support wide spread use of electronic interactions between business and government. This is now accelerating and recent international agreements have contained references to the need for global cross-recognition of electronic transactions. This is in response to global trade requirements for the facilitation of faster processing and surety of trading documents. While these arrangements are not yet active, Australia is preparing to transact with two of our trading partners, Singapore and the USA. There are also other developments underway with APEC countries and other trading partners.

Concluding comments

The AGAF ensures that Government keeps authentication requirements simple.

The proposed AGAF recognises that in the future, as more services are provided online, there will be some re-jigging of the way that business users of online services are authenticated. The adoption of the AGAF by government agencies will ensure that businesses do not have to undergo cumbersome and expensive authentication processes for simple or low risk transactions, and that the Government is being realistic and consistent when asking businesses to authenticate themselves. Similarly, businesses will be able to utilise the risk management techniques outlined in the AGAF to determine an appropriate level of authentication for their own business practices.

Authenticating identity and user information is an evolving landscape. Accordingly, the Australian Government intends to continue to work with business on their future authentication needs.

Risk assurance levels of the AGAF

<p>Level 1 – Minimal risk</p> <p>Level 1 authentication is appropriate for e-Government transactions in which minimal damage might arise from the assertion being accepted as true when it is actually false. The damage might cause the following situations:</p> <ul style="list-style-type: none"> • minimal inconvenience to any party • no risk to any party’s personal safety • no release of personally or commercially sensitive data to third parties • minimal financial loss to any party • no damage to any party’s standing or reputation • no distress being caused to any party • no threat to government agencies’ systems or agencies' capacity to conduct their business • would not assist a serious crime or hinder its detection.
<p>Level 2 – Low risk</p> <p>Level 2 authentication is appropriate for e-Government transactions in which minor damage might arise from the assertion being accepted as true when it is actually false. The damage might cause the following situations:</p> <ul style="list-style-type: none"> • minor inconvenience to any party • no risk to any party’s personal safety • no release of personally or commercially sensitive data to third parties • minor financial loss to any party • minor damage to any party’s standing or reputation • minor distress being caused to any party • no threat to government agencies’ systems or agencies' capacity to conduct their business • would not assist a serious crime or hinder its detection.
<p>Level 3 – Moderate risk</p> <p>Level 3 authentication is appropriate for e-Government transactions in which moderate damage might arise from the assertion being accepted as true when it is actually false. The damage might cause the following situations:</p> <ul style="list-style-type: none"> • significant inconvenience to any party • no risk to any party’s personal safety • the release of personally or commercially sensitive data to third parties • significant financial loss to any party • significant damage to any party’s standing or reputation • significant distress being caused to any party • moderate threat to government agencies’ systems or agencies' capacity to conduct their business • could assist a serious crime or hinder its detection.
<p>Level 4 – High risk</p> <p>Level 4 authentication is appropriate for e-Government transactions in which substantial damage might arise from the assertion being accepted as true when it is actually false. The damage might cause the following situations:</p> <ul style="list-style-type: none"> • substantial inconvenience to any party • risk to any party’s personal safety • the release of personally or commercially sensitive data to third parties • substantial financial loss to any party • substantial damage to any party’s standing or reputation • substantial distress being caused to any party • significant threat to government agencies’ systems or agencies' capacity to conduct their business • could assist a serious crime or hinder its detection.

Example 1

Application for an Australian Business Number – Shared Information.

The Australian Business Number (ABN) is an 11 digit business identifier that facilitates easier transactions with the Australian Taxation Office, and other areas of government.

Businesses can apply for an ABN online using Secure Sockets Layer (SSL) to ensure security and privacy. Each new application generates a unique reference number which businesses must remember if they want to save their application and complete it later. Businesses then nominate a password. The Tax Office then requires the applicant to provide proof of their identity, and of their associates.

The Tax Office compares information provided by applicants to existing government agency data as a means of verification, for example, Australian Company Numbers (ACNs) with the Australian Securities and Investments Commission (ASIC) .

Once an ABN is issued, a business must use a Digital Certificate issued by the Tax Office, a Public Key Infrastructure mechanism, to access their details.

Further information on the authentication and security protocols used by the Tax Office can be found at www.abr.gov.au .

Example 2

Business Entry Point - Username/Password – SSL

The Business Entry Point (BEP) is an online government resource for the Australian small business community. It provides businesses with a wide range of services and information about start-up, taxation, licensing and legislation, as well as allowing significant online transactions such as taxation compliance and licence applications.

The BEP's Transaction Manager facility is protected by Secure Socket Layer (SSL) encryption while the user remains on the site. The authentication process under SSL uses public key encryption and digital signatures to confirm that a server is in fact the server it claims to be. It does not authenticate the user. Once the server has been authenticated, the client and the server use techniques of symmetric key encryption to encrypt the information they exchange. A different session key is used for each transaction, impeding a hacker's ability to decrypt messages. Businesses employ a username/password to access the BEP.

Further information on authentication and security protocols used in the BEP can be found at www.business.gov.au

Example 3

The SecureNet Health E-Signature Authority (HeSA) Health PKI

The SecureNet-HeSA Health PKI provides Public Key Infrastructure (PKI) for the Australian healthcare sector. PKI is used for the transfer of health-related information across the internet, thus ensuring no compromise of patient information.

Healthcare providers who are interested in obtaining their own digital keys and certificates need to register through the Health eSignature Authority (HeSA).

HeSA offers two types of certificate:

- ‘Individual’ certificates allow someone to encrypt and exchange messages electronically with other certificate subscribers. They also allow for electronic signing at the individual level, which provides a strong level of surety about the identity of the person sending the information
- ‘Location’ certificates allow a number of people at the same location to encrypt, sign and exchange messages electronically with other certificate subscribers. Signing a message using the Location certificate confirms the location that the message came from, but not which individual.

All subscribers receive two sets of key pairs:

- Private and public authentication keys for authentication and data integrity. The sender uses their private authentication key to digitally sign their messages, while the party receiving the message uses the sender’s public authentication key to verify the digital signature of the sender once they receive the message
- Private and public confidentiality keys to protect the confidentiality of an electronic message. The sender uses the recipient’s public confidentiality key to encrypt the message before sending, while the recipient uses their private confidentiality key to decrypt the message once received.
- To register for digital keys and certificates, all applicants go to HeSA’s website and employ a user ID/password approach during the application process—much the same as the application for an ABN. Applicants respond to a series of questions, providing information that is necessary for HeSA to arrange for certificate issuing. To complete the registration process, all applicants must then provide hard copies of identity related documentation, as indicated during the web-based application process.

For further information on authentication and security protocols used by HeSA can be found at www.hesa.com.au

Appendix C

GLOSSARY: AGAF - AN OVERVIEW FOR BUSINESS	
TERM	DEFINITION
Attribute	<p>A characteristic of an Entity. Entities may include people or organisations.</p> <p>Attributes of a 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. Attributes of a business may include ASIC company numbers, an Australian Business Number, etc.</p>
Authentication	The process of testing a statement or claim, in order to establish a level of confidence in the statement's or claim's reliability.
Biometrics	Biometric technologies use physiological or behavioural characteristics to identify an individual. Examples include iris scans, retina scans, facial scans, finger scans, hand geometry, voice verification and dynamic signature verification.
Business to Government (B2G)	Online interaction between business enterprises and government agencies.
Certification Authority (CA)	An organisation that issues Digital Certificates, vouches for their contents, is trusted by the government to do so, and may provide warranties to that effect, and even some level of indemnity.
Challenge-Response	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').
Credential	<p>A document or another agent that has physical or digital existence, and that assists in the process of Authentication of a statement or claim.</p> <p>Examples include an Identity Document and a Token.</p>
Cryptography	A field of study concerning the principles, means, and methods for rendering plaintext unintelligible to an unauthorised recipient by converting it into 'ciphertext', and for restoring such encrypted 'ciphertext' into intelligible form.
Decryption	Cryptographic transformation of ciphertext in order to recover the 'plaintext' form that it had prior to encryption being performed on it. See also Encryption and Cryptography.

GLOSSARY: AGAF - AN OVERVIEW FOR BUSINESS	
TERM	DEFINITION
Digital Certificate	An electronic document signed by the Certification Authority which: <ul style="list-style-type: none"> • Identifies a key holder and the business entity they represent; • Binds the key holder to a key pair (a public key and a private key) by specifying the public key of that key pair; and • Should contain any other information required by the certificate profile.
Digital Signature	A digital signature functions for electronic documents like a handwritten signature for printed documents. The signature is an unforgeable piece of data that asserts that a named person wrote or otherwise agreed to the document to which the signature is attached.
E-Government	The application of telecommunications-based tools to the dealings of government agencies with other Entities.
Encryption	Cryptographic transformation of plaintext data into a form (ciphertext) that conceals the data's original meaning to prevent it from being known or used. See also Decryption and Cryptography.
Entity	An organisation or person to be authenticated, including corporations, trusts, superannuation funds, and incorporated associations.
Evidence of Identity (EOI)	Evidence that assists in Authentication of a statement or claim relating to Identity.
Gatekeeper Accreditation	Accreditation of PKI systems for use in government. Accreditation is granted on the basis that the Certification Authority or Registration Authority meets the published Gatekeeper accreditation criteria.
Hard Token	A physical authentication device such as a smart card
Identity Authentication	The process of testing a statement or claim that a particular Entity is appropriately using an Identity, in order to establish a level of confidence in the statement or claim's reliability.
Identity Document	A credential comprising writing or printing on paper, or its equivalent in electronic form, eg: birth certificates, passports, drivers' licences, employer-issued building security cards, etc.
Key	A data element used to encrypt or decrypt a message.

GLOSSARY: AGAF - AN OVERVIEW FOR BUSINESS	
TERM	DEFINITION
Non-Repudiation	A condition in which an Entity is precluded from repudiating or denying a particular statement or claim.
One time password	An authentication system that requires a new password every time a user authenticates themselves. This is usually achieved through use of a hardware device that generates a unique password to be entered each time the application is assessed.
Password	An arbitrary string of characters chosen by a user or an IT administrator and used to authenticate the user when they attempt to log on. See also Personal Identification Number (PIN).
Personal Identification Number (PIN)	A string of characters that is used to assist in the Authentication of the statement or claim that a person has the right to use a Username. See also Password.
PKI	See Public Key Infrastructure.
Private Key	The secret component of a pair of Cryptographic Keys used to digitally sign messages on behalf of an entity.
Public Key	The publicly-disclosable component of a pair of Cryptographic Keys used to digitally sign messages on behalf of an entity.
Public Key Cryptography	A form of Cryptography that involves two related keys, referred to as a Key Pair, one of which only the owner ever needs to know (the Private Key) and the other which anyone can know (the Public Key).
Public Key Infrastructure (PKI)	A secure method of exchanging information. PKI uses the “public/private key” method, for encrypting IDs and documents/messages. It starts with the Certification Authority which issues digital certificates that authenticate the identity of people and organisations over a public system.
Registration	A process comprising a series of steps intended to simplify subsequent Authentication processes. Also referred to as Enrolment.
Registration Authority (RA)	An Entity that conducts a Registration process on behalf of a Certification Authority (CA).

GLOSSARY: AGAF - AN OVERVIEW FOR BUSINESS	
TERM	DEFINITION
Risk Management	A process whereby threats, vulnerabilities and risks are assessed, and a balance sought between costs and benefits.
Shared information	A series of questions are asked which only the legitimate user can answer, eg: mother's maiden name.
Smart Card	A credit card-like device with a built-in microprocessor and memory used for identification or financial transactions. When inserted into a reader, it transfers data to and from a central computer.
Soft Token	An authentication device that is stored in a computer.
Token	<p>An authentication device issued by a Legal Entity to another Legal Entity in which a third Entity places some degree of trust. A Token is likely to include security features intended to render it difficult to forge, and tying it in some manner with the particular Entity.</p> <p>Examples include 'identity cards' (especially 'photo-id'), and smartcards.</p>
User ID	See Username.
Username	A name used to access a computer system. This is usually a string of characters issued to a user by an IT administrator.
Value	See Attribute