

Queensland Government Authentication Framework

Final

November 2010

v2.0.1

PUBLIC

Queensland Government Enterprise Architecture

ICT Policy and Coordination Office
Department of Public Works

Queensland Government

Document details

Security classification	PUBLIC		
Date of review of security classification	November 2010		
Authority	Queensland Government Chief Information Officer		
Author	ICT Policy and Coordination Office		
Documentation status	Working draft	Consultation release	☑ Final version

Contact for enquiries and proposed changes

All enquiries regarding this document should be directed in the first instance to:

Director, Policy Development
ICT Policy and Coordination Office
ICTPolicy@qld.gov.au

Acknowledgements

This version of the *Queensland Government Authentication Framework* was developed and updated by the ICT Policy and Coordination Office.

Feedback was also received from a number of staff from various agencies, including members of the Information Security Reference Group, which was greatly appreciated.

It is based on the Australian Government Authentication Framework, developed by the Australian Government Information Management Office. It was developed in consultation with the Distributed Systems Technology Centre (DSTC) of the University of Queensland, the Information Security Research Centre (ISRC) of the Queensland University of Technology, and the Department of Justice and Attorney-General's Privacy Manager. The Queensland Government would like to acknowledge the important contribution made by these organisations and individuals.

Copyright

Licence

Information security

This document has been security classified using the Queensland Government Information Security Classification Framework (QGISCF) as PUBLIC and will be managed according to the requirements of the QGISCF.

Contents

Figures

Tables

1 Introduction

The Queensland Government provides a wide range of services to the public, internal staff, business and other jurisdictions of government. Government agencies have an obligation and responsibility to provide a duty of care and protection to their clients, to maintain client confidentiality, and to establish and maintain the security and integrity of information and systems.

Authentication is the process of verifying an identity which has previously been registered to use a service. Authentication is an essential process of many services in meeting the above obligations, and provides a level of confidence in the identity of those involved in the use of a service, thus reducing opportunities for identity misuse such as identity fraud, and ensuring the security of services and systems.

1.1 Purpose

The purpose of the Queensland Government Authentication Framework (QGAF) is to provide a framework for agencies to use when determining authentication requirements. The QGAF applies to all services that require user authentication.

Authentication is accomplished using something the user knows (eg. a password, or secret questions and answers), something the user has (eg. a security token) or something the user is (eg. a biometric) or a combination of these.

The QGAF applies equally to the development of new services and when reviewing and improving existing services, and applies to both electronically and non-electronically delivered services. The implementation of electronic service delivery has accelerated the need for a consistent approach to authentication, particularly as government agencies seek to integrate electronic business transactions to improve client service.

The QGAF seeks to:

- facilitate improved interoperability across the sector by establishing a consistent approach to authentication for Queensland Government
- promote an understanding of the importance of authentication in the overall operation of Government services
- help agencies position their approach to authentication for service delivery across different types of service delivery channels
- position agencies to take advantage of future whole-of-Government authentication initiatives
- ensure that the Queensland Government is aligned with the *Australian Government National e-Authentication Framework* (NeAF).

The QGAF provides:

- an introduction and overview of authentication and related processes
- a process that agencies can use to determine their authentication needs based on an approach that considers a risk assessment and information security classification
- a process which provides transparency and openness regarding decisions surrounding authentication which will encourage better and more easily understood decision making
- guidance on determining appropriate technologies to meet authentication needs, taking into account cost, technology and usability issues

- improved cost-effectiveness for authentication solutions by ensuring that solutions implemented are not over-specified but are based on business need and risk
- background information on authentication related technologies and architectures.

The QGAF is intended for the use of staff within Queensland Government agencies. It will be of particular relevance to:

- any people who are designing agency services such as service designers and system architects
- business managers and service stakeholders
- risk managers
- information security managers and auditors who may assess the security of services
- Chief Information Officers and other ICT managers and staff responsible for the supply and operation of systems supporting service delivery.

1.2 Scope

The QGAF applies to all services that require user authentication – ie. services where access is restricted by something the user knows (eg. a password, or secret questions and answers), something the user has (eg. a security token) or something the user is (eg. a biometric) or a combination of these.

The QGAF provides a framework to assist in determination of authentication requirements and risks, and the most appropriate assurance levels for registration, identification and authentication. Other security functions that are not directly related to the authentication aspects of a service (eg. access control, availability, auditing) are outside the scope of this framework, and should be addressed through the implementation of the Queensland Government information standards, other information security frameworks, and relevant elements of the Queensland Government Enterprise Architecture (QGEA). In particular, it should be noted that the QGAF does not provide advice on authorisation and access control. The following definitions are helpful in distinguishing these areas of security:

- authentication – ensuring that users are the persons they claim to be
- access control – ensuring that users access only those resources and services that they are entitled to access and that qualified users are not denied access to services that they legitimately expect to receive.

The QGAF applies to systems and services which are delivered both within an agency to internal staff and clients, and outside an agency to other business partners and the public.

The security context of the authentication framework within an information delivery model is illustrated in Figure 1. It shows the processes of authentication (registration, identification and authentication) are independent of other security functionality within the delivery model.

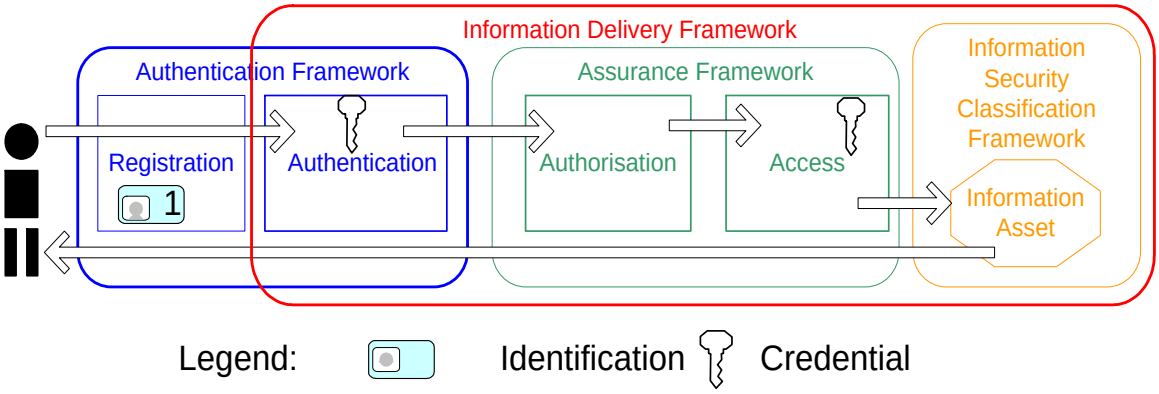

Figure 1: Security context for the delivery of services

1.3 Context

This framework has been developed to align with appropriate Queensland Government legislation and regulation, Australian Government standards, Australian Standards, and Queensland Government ICT Strategy and Policy. Each of these are listed in table 1.

Author	Resources
Queensland Government Legislation	• *Public Records Act 2002* • *Right to Information Act 2009* • *Information Privacy Act 2009*
Queensland Government Policy	• Information Security (IS18) • Retention and Disposal of Public Records (IS31) • Recordkeeping (IS40) • Information Asset Custodianship (IS44)
Australian Government Standards	• Protective Security Policy Framework (PSPF) • Information Security Manual (ISM) • National e-Authentication Framework
Australian and International Standards	• ISO/IEC 27000:2009 Information technology - Security techniques - Information security management systems - Overview and vocabulary • AS/NZS ISO/IEC 27001:2006 Information technology - Security techniques - Information security management systems – Requirements • AS/NZS ISO 31000:2009 Risk management - Principles and guidelines
Queensland Government ICT Strategy and Policy	• DIGITAL1ST • Queensland Government Enterprise Architecture (QGEA) • Queensland Government Information Security Policy Framework (QGISPF)

Table 1: QGAF context

1.4 Supporting documentation

The QGAF has three supporting documents:

- *QGAF Identity and Registration Concepts*. This document explains the concepts surrounding identity, evidence of identity and the processes that can be applied to register an identity and issue authentication credentials.
- *QGAF Authentication Concepts.* This document explains the concepts surrounding authentication and provides advice on authentication mechanisms and their fit to required assurance levels and the business requirements of the service being provided.
- *QGAF Case Studies*. This document provides examples of real world QGAF implementation by some Queensland Government agencies.

To support the QGAF process, a spreadsheet has been developed which assists with implementing the framework. By answering the various questions posed by the spreadsheet, the risk, identity, registration and assurance levels are calculated.

The spreadsheet also allows for some sensitivity analysis/moderation to occur by enabling the answers to the questions posed to be changed and allowing for observation of the effect of these changes on the Authentication Assurance Level.

It is strongly recommended that this spreadsheet be used when applying this framework.

Additionally, QGAF is based on the NeAF. QGAF has maintained a close relationship with NeAF. The QGAF enables an authentication framework to be implemented by Queensland Government agencies providing a sufficient assurance and confidence for services, whilst meeting NeAF processes.

QGAF is also consistent wherever possible with other related Australian and international standards for authentication and risk management (See appendix A for a brief comparison of QGAF with other authentication frameworks).

1.5 QGAF Requirements

Queensland Government IS18 mandates this framework as the process to be applied by all Queensland Government agencies when implementing authentication mechanisms.

This framework requires that agencies must:

- comply with the 11 Information Privacy Principles of the *Information Privacy Act 2009*
- perform a privacy impact assessment for the service
- ensure that all service delivery channels support the same level of service for clients
- determine an authentication assurance level (AAL) for each service based on the risks associated with authentication
- assign an identify registration assurance level (IRAL)
- set a minimum evidence of identity (EOI) requirement that reflects the IRAL for the service
- determine an identity authentication assurance level (IAAL) for each service based on the service's identity registration and authentication assurance level
- select an authentication mechanism that reflects the IRAL and IAAL associated with the service
- review the service and its associated authentication assurances

In the short term, this will lead to suitable levels of authentication being provided for Government services and protection for its clients. In the long term, it will enable consistent authentication across Government services. This also supports any potential future implementation of whole-of-Government approaches to authentication that could improve efficiency, reduce costs, and provide a higher level of service for clients.

1.6 Implementation guidance

This framework must be used by all Queensland Government agencies to evaluate the authentication aspects of their services. Ideally the QGAF should be applied to all services and systems. It is however recognised that this is impractical and potentially disruptive and cost-prohibitive for many existing systems and services. Therefore, agencies must apply QGAF in the following order:

1. All new systems and services must be evaluated against QGAF during development or implementation.
2. Existing systems and services must be evaluated against QGAF based on an assessment of risk, with high risk systems and services being considered a priority for evaluation.

It should also be noted that in many cases, retrofitting of existing ICT applications to support the higher levels of authentication which may be indicated by the QGAF process may be either technically impossible, or highly cost-prohibitive. In these circumstances, as for all things related to information security, a risk management approach is required. An agency, through its risk management processes, can choose to accept a risk of having weak authentication processes on systems containing security classified information, and should take other precautions to minimise the risk of inappropriate access to or release of security classified information.

A register of existing authentication processes, mechanisms and issued credentials may also prove useful to agencies in managing their authentication solutions.

All initial assessments of authentication levels must be verified by a second person or group to ensure that the assessment is appropriate. Additionally, as indicated by the Review step in the QGAF process, agencies must establish procedures to periodically verify the correct security classification and authentication levels are in use and remain valid from initial assessment, particularly for applications that have external access.

Acknowledging that this framework can appear complex, the ICT Policy and Coordination Office will, wherever possible, assist agencies upon request with the assessment of services against this framework.

1.7 Overview

The QGAF provides a process and a set of definitions which allow agencies, as service providers, to evaluate the risk associated with their services and determine the appropriate level of authentication assurance required. This in turn enables agencies to implement systems that manage and reduce the impact of authentication failures to acceptable levels (ie. to levels commensurate with the risks involved) to ensure appropriate protection for the Government, its clients, and the public.

This framework should be applied to all services that are provided for the use of government clients and staff. Whilst it can and should be applied to existing services, ideally, it should be applied during the design phase of a service. This is important because authentication is an inherent property of a service. Considering authentication related issues only after service design is complete may cause undue expense and could potentially make the service unusable or unviable without redesign being required.

It should also be noted, that whilst this framework is intended to apply to each and every transaction provided by a system or even an agency, in practical terms, authentication is usually implemented in such a way that a single authentication process is implemented which will cover all likely transactions that a client wishes to perform during a business interaction. More information on the treatment of multiple services is contained in section 2.6.2 of this document.

2 The QGAF process

The process steps for the application of QGAF to a particular service are illustrated in Figure 2. The remaining sections of this document provide more information about each step in the process.

Different types of services require different levels of authentication assurance. For example, services involving sensitive information or financial transactions would require a higher level of assurance about the identity of a client than services which do not. It is important for government agencies to provide a level of authentication assurance that is appropriate for the service. This is necessary for the proper functioning of the service, as well as for preventing improper use and fraud. It is also necessary to ensure that agency risks are managed and clients are protected.

QGAF aligns with the NeAF in seeking to determine an appropriate overall Authentication Assurance Level for services. As two separate processes are involved in an authentication process (registration and subsequent authentication), the overall AAL achieved for a service is dependent on both the registration process and the subsequent authentication process which occurs during each service request. That is, the assurance or confidence that can be held in these two processes, combine to provide an overall authentication assurance level.

This authentication framework provides processes to aid the identification of two sub-assurance levels, the IRAL and the IAAL. Further explanations of these levels are provided in later sections of this document.

As indicated in the QGAF process diagram below, the service authentication levels derived by following this framework must be reviewed prior to final acceptance of the service, and periodically throughout the lifetime of the service. This is to ensure that no changes have occurred to the service or its environment which require adjustments to the implementation of the authentication mechanisms of the service.

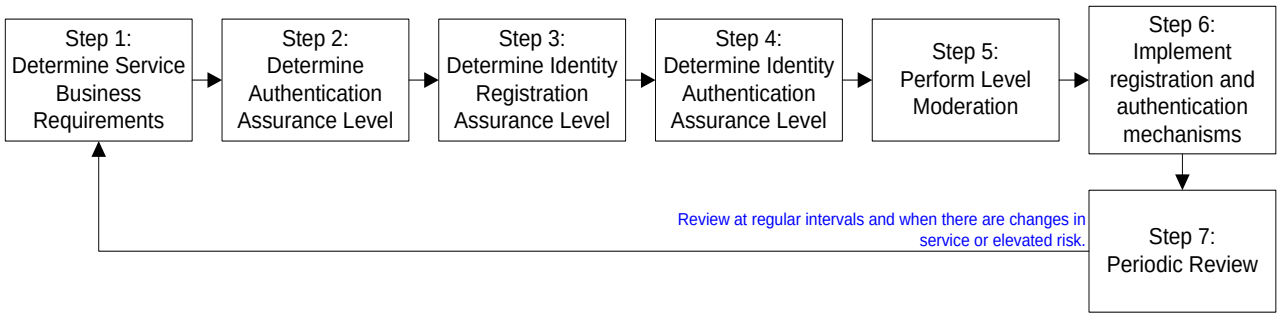

Figure 2: The QGAF process

2.1 Determine Service Business Requirements

The first step in implementing authentication for a service is to ensure that the business requirements for the service are accurately identified. All future steps in the QGAF process are reliant upon the service business requirements and the determination of the correct authentication levels for the service is dependent on the accuracy and completeness of the business requirements. Failure to identify the business requirements correctly can result in a higher or lower level of assurance being implemented than should be, which could result in an unwarranted increase in implementation and maintenance costs, or an increase in the authentication risk associated with a service.

It is also important when implementing QGAF that the service provider has identified all services that are being offered as part of a business process, so appropriate consideration

can be given to the use of a single or graduated approach to authentication services (see Section 2.6.2 for more information).

Section 0 provides considerable guidance on the many business requirements which can influence assurance levels, and these requirements need to be assessed and understood when applying this framework. The remainder of this section deals with additional requirements which impact design of service delivery channels and privacy considerations.

2.1.1 Service delivery channels

A service delivery channel is a conduit through which services are provided or transactions are conducted. There are three main types of channels:

- Physical Delivery Channels
- Voice Delivery Channels
- Data Delivery Channels

Public preferences for service channels have been explored as part of the Queensland Household Survey (QHS). Appendix A outlines different channel types and contains survey highlights from 2004 to 2007. These statistics indicate the Internet is increasingly seen as the preferred channel for government services. However, there remains a significant element of preference for many Queensland households for the use of 'traditional' service delivery channels (mail, over the counter and phone). When developing a new service, findings from the Queensland Government Household Survey (or similar material) can assist with service delivery channel selection, to ensure that the services are delivered using a suitable channel which can and will be accessed by those seeking the service.

2.1.2 Privacy

Agency authentication activities must comply with the 11 Information Privacy Principles (IPPs). The IPPs specify how individuals' personal information[1] is collected, stored, used and disclosed. The IPPs are:

- IPP 1 – Collection of personal information (lawful and fair)
- IPP 2 – Collection of personal information (requested from individual)
- IPP 3 – Collection of personal information (relevance etc)
- IPP 4 – Storage and security of personal information
- IPP 5 – Providing information about documents containing personal information
- IPP 6 – Access to documents containing personal information
- IPP 7 – Amendment of documents containing personal information
- IPP 8 – Checking of accuracy etc. of personal information before use by agency
- IPP 9 – Use of personal information only for relevant purpose
- IPP 10 – Limits on use of personal information
- IPP 11 – Limits on disclosure

Further information on the privacy and the IPPs can be found in Appendix E.

[1] ***Personal information*** is information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

2.2 Determine desired Authentication Assurance Level

Authentication assurance indicates the level of confidence the service provider has in the premise that the client using a service is in fact the client registered to access the service. In addition, the higher the level of assurance the greater the level of confidence can be held that the real world identity of the client is known.

The QGAF establishes five levels of assurance as shown in Table 2.

Authentication Assurance Level (AAL)				
Level 0	Level 1	Level 2	Level 3	Level 4
No Assurance	Minimal Assurance	Low Assurance	Moderate Assurance	High Assurance
No confidence is required in the client's identity	Minimal confidence is required in the client's identity	Low confidence is required in the client's identity	Moderate confidence is required in the client's identity	High confidence is required in the client's identity

Table 2: Authentication Assurance Levels

Authentication assurance levels are a composite of many factors. This framework provides a methodology for setting the appropriate levels based on an assessment of the risk associated with an authentication failure, and on the information security classification level, as described in the following sub-sections, and on performing a final moderation step to ensure business needs are being appropriately met. When reading this section it may be useful to refer to the supporting documentation Queensland Government Authentication Framework: Authentication Concepts for further clarification.

2.2.1 Information security classification level

Many services provide information to clients, or the ability to change information recorded in systems. When the information involved in these services has been assessed for an information security classification level, it can be used to guide the AAL (see the Queensland Government Information Security Classification Framework (QGISCF) for more information).

The greater the information security classification level, the higher the level of authentication assurance is required.

Table 3 (page 9) shows the determination of the Authentication Assurance Level based on the information security classification assessment. Note that this assessment **must** be performed based on the most highly classified information accessed by the service.

Highest Information Security Classification Level				
Public	Unclassified	In Confidence	Protected	Highly Protected
⇩	⇩	⇩	⇩	⇩
AAL-0[2]	AAL-1	AAL-2	AAL-3	AAL-4
Authentication Assurance Level (AAL)				

Table 3: Determination of AAL based on Information Security Classification Level

2.2.2 Risk Assessment

Where information security classification has not been performed on the information provided by the service, the AAL can be determined using agency risk assessment processes. A sample process is provided in Appendix D.

2.2.3 Final authentication assurance level

The final authentication assurance level to be used in the remainder of the QGAF process is determined by comparing the authentication assurance level from the risk assessment with that from the information security classification assessment (see section 2.2.1) and selecting the highest authentication assurance level determined by these two processes.

Table 4 shows the determination of the AAL based on the risk assessment.

Authentication Risk Level				
Negligible	Minimal	Low	Moderate	High
AAL-0	AAL-1	AAL-2	AAL-3	AAL-4
Authentication Assurance Level				

Table 4: Determination of Authentication Assurance Level based on Risk Assessment

Some examples may help to explain why both measures (risk and information security classification) are used. A service which licences someone to operate heavy equipment may only contain information of an in-confidence classification (some personal details, perhaps, but nothing which needs a protected level of security classification), which would lead to an AAL-2 using the information security classification assessment. However, due to the potential for harm which may occur if a person were incorrectly licensed to operate this equipment, the risk assessment may indicate moderate risk (due to the potential of someone being incorrectly granted and using a licence), which would thus in turn indicate an AAL-3 was required.

Likewise, it is also possible that a service may be evaluated with a low risk assessment, but in fact it provides information classified as highly protected. In theory, this would be unlikely to occur often, as the classification of information is based itself on a similar risk assessment process.

[2] Some PUBLIC information may be available only via a service that requires registration. If this is the case, AAL-1 may be more appropriate.

2.3 Determine the Identity Registration Assurance Level

As described in the overview to QGAF, the overall authentication assurance achieved for a given service is a combination of the assurance provided by the registration process, and that provided by authentication process that occurs with each service delivery process.

The IRAL determines the level of confidence a service provider requires in the registration of a client. The higher the level of confidence required, the higher the level of identity verification the service provider needs during the registration process to be confident that the identity being registered is in fact a given real world entity.

More information on registration is contained in the Identity and Registration Concepts document. Depending on the level of authentication assurance required, the registration process needs to defend itself against applicants impersonating an identity, and possibly against repudiation of registration.

Table 5 indicates the IRAL of this framework. These levels are determined based on the business requirements, and consideration of the overall AAL determined in the previous step. Whilst there is some level of independence in the various assurance levels, in effect, the previously determined Authentication Assurance Level will affect the minimum required IRAL.

IRAL and Confidence Provided	Description	Usage
IRAL-4 High Confidence	High level verified identity Substantial evidence of the real-world identity is required, and verified. External checks **must** be performed on the evidence of identity, and the person is required to be physically present at the registration authority during registration. Requires the taking of a biometric (such as a photograph) during registration to ensure non-repudiation of the registration process.	Used when a high level of confidence is required in the registration process, the identity needs to be linked to a real world client, and non-repudiation of the registration process is required. Does not support remote registration (ie. registration conducted electronically or over the phone), due to the need for the client to be physically present at the registration authority.
IRAL-3 Moderate Confidence	Moderate level verified identity Moderate evidence of the real-world identity is required, and verified. External checks **must** be performed on the evidence of identity.	Used when the identity needs to be directly linked to a real world client and the transaction indicates it is legally binding (ie. service delivery non-repudiation is supported at a moderate level).
IRAL-2 Low Confidence	Low level or Basic identity Some minimal evidence of real-world identity is provided during the registration process. The client's real world identity is known to the registration authority and hence transactions can be verified against a real world identity if required.	This level of registration is used when the service requires that client is to be specifically identified during the conduct of transactions or the registration process, and only low levels of authentication assurance are required. Used, for example, when registering for a low risk service which requires eligibility criteria to be met (age, qualifications, etc).

IRAL and Confidence Provided	Description	Usage
IRAL-1 Minimal Confidence	Pseudonymous or Self-Registered identity Registration is performed but no proofing is carried out on the data. The registration would usually be performed by the client (self-registered) but may be performed by the service provider or third party registration authority. Does not require real-world identity registration data. The client could identify using any name or data they wished and thus create a pseudonym.	This level of registration is useful for recognising return visits to the service, even though the individual entity remains unknown – eg where a client's return visits automatically load personal preferences linked to a pseudonym. This level also supports a form of further contact so the client can be further contacted if required, but there is no support for non-repudiation or for knowledge of the real-world identity of the client. An example would be where a client has registered an email address that can not be converted to a real world identity but is sufficient to allow information to be sent or continue further interaction.
IRAL-0 No Confidence	Not Identified – anonymous No registration and hence no identification is performed.	Supports requests for information that is freely available, such as access to online information about government programs or services. Generally applies to public information that is freely available, and excludes interactions that alter information.

Table 5: Identity Registration Assurance Levels

2.3.1 Business requirements analysis

There are specific business requirements which need to be established before a service provider can fully establish the required service identity registration level as they guide the appropriate choice of registration level.

Higher levels of IRAL generally imply more invasive registration processes, which may hinder the take-up of a service by clients, and may limit the choice of service delivery channels. For example, in the case of the provision of information on a web site, clients are generally happy to download information where it is available without any registration. Many clients will be happy to provide a simple email address before downloading the requested information, although some will not be, but a great number will not be willing to provide information such as home phone numbers, name, and street address before gaining access to the information.

When deciding on what type of identity registration is required the following should be taken into consideration:

- Is there a legislative or policy need to ensure anonymity? Is it important that you, as service provider, are unable to identify the real world identity of the client?
- Does the service provider need to make future contact with the client?
- Is the information being provided restricted in anyway? Are there privacy considerations? Is it acceptable if the information is provided to anyone / everyone?
- Is there a need for payment? Does the payment need an official receipt? Does the receipt require identifying data? Does the service provider need to keep a record of

payments made by a client? Payments and receipting may require knowledge of the real world identity of the client.

- Is there a need to store and retrieve a history of dealings with a specific client?
- Is the transaction legally binding? Is non-repudiation required?
- Does the client require access to a particular transaction or a piece of information?

Table 6 shows how the different IRAL support different business requirements. This table can be used as a basis for the selection of the correct identity registration assurance level based on the gathered business requirements and the previous assessment of Authentication Assurance Level. Further detail on each of these business requirements is provided below. There can be more than one suitable IRAL for a given set of business requirements, particularly where the business requirements are not particularly demanding, and on these occasions an informed choice can be made.

Terms used in Table 6 are expanded and explained in the following sub-sections.

IRAL	Client Anonymity Maintained	Allows Contactability and Service History and Personalisation	Real World Identity link, service delivery non-repudiation	Supports overall AAL > 2	Supports Non-repudiation of registration
IRAL-4 High	No	Yes	Yes	Yes	Yes
IRAL-3 Moderate	No	Yes	Yes	Yes	No
IRAL-2 Low / Basic	No	Yes	Yes	No	No
IRAL-1 Pseudonymous or Self Registered	Yes by Pseudonym	Yes	No	No	No
IRAL-0 No registration	Yes	No	No	No	No

Table 6: QGAF Identity Registration Assurance Levels Business Capabilities

Third party registration authorities

A service provider is not constrained to registering clients themselves, and may use a third party to perform the registration process. The third party registration authority will receive all evidence of identity on behalf of the client and verify their authenticity against the requirements of the service provider. The service provider is provided with an identity that has been fully verified by the third party, allowing the service provider to trust the identity without having to perform the identity registration phase themselves.

It should be noted that third party registration is allowable at all appropriate levels (1, 2, 3 and 4), though appropriate trust must be established between the third party registration authority and the service provider, particularly at the higher levels of registration.

Anonymity

When providing a service it must be clearly defined whether the transaction requires a real world identity to be known or not known to the service provider. Where a real world identity is not required then an IRAL-0, which involves no registration, and hence no authentication, is simple and cheap to implement. Anonymous services can also assist in attracting public participation of a service that may have a social stigma attached, hindering the public from partaking in the service.

Note that absolute anonymity can be supported by identity registration assurance levels 0 (no registration required) and 1 (pseudonymous registration), but not by levels 2, 3 or 4, which all require the real-world identity to be know by the registration authority (see Identity Escrow for more). If IRAL-0 is the identified registration assurance level required, the following check list **must** be reviewed to ensure the selection is correct.

- Confirm that the information provided by the transaction should be viewable to anyone – ie. is it public domain?
- Confirm that there is no need to know who the client is using the service, because there is no need for client follow up, no relation to other transactions, no history of transactions required, and there is no harm in communicating with an unknown client.
- Confirm there is no need for the client to have a particular attribute to use the transaction (eg. does the client need to be of a certain age, or have certain licences or qualifications).

Pseudonym

A pseudonym is an identity where only the entity that generated the pseudonym knows the real world identity. As the real world identity of the client using a pseudonym is not known to the service provider, a pseudonym may be used in some systems for privacy reasons, as it provides an effective form of anonymity.

Some transactions are able to be operated successfully through the use of a pseudonym. Pseudonyms are used for transactions that require the service provider to be able to remain in contact with the client without needing to know the details of the real world entity (see *Contactability* page 14). A typical example is a transaction which may involve registering to receive newsletters or information. In these cases the client may create their own user-id and password, which allows them to return and modify their preferences or remove themselves from the service, but there is no need for the service provider to know the real name of the recipient of the information. The created user-id forms a pseudonym identity, and maintains client anonymity as the identity does not provide any link to a real world identity.

Alias or identity escrow

Identity Escrow in the QGAF context occurs when a client uses a third party registration authority to establish and register their identity, and the third party passes on to the service provider an alias for the client (ie. they keep the clients real-world identity hidden from the service provider, and provide some other identifier such as a client id number). This form of identity escrow may be used for various reasons, including the preservation of client anonymity whilst allowing the service provider to know that a real world entity does actually exist, even if the service provider does not know that identity.

Thus, an alias in the QGAF context, is an identity where the registration authority that generated the alias knows the real world identity of the entity, but provides the client with an identity (termed here as an ‘alias’, but is in fact a form of pseudonym) which hides this real world identity. It is possible for an alias to be used at identity registration levels 2, 3 and 4,

though this would be at the discretion of the agreement between the third party registration authority and the service provider. An alias may be used in some systems for privacy reasons or where the sharing of information is occurring with parties or organisations that are separate from the service provider.

It is important to note that the service provider may only know the client by an alias but, if required, there is a mechanism to gaining access to the real-world identity of the client through the third party. Thus, the main difference between an alias and a pseudonym is that an alias *is* able to be traced back to a real world identity, so anonymity is not absolute, and the service provider can safely assume that the client identity has been verified by the registration authority.

Contactability

Contactability is where the service provider requires a mechanism to be in place to enable further correspondence with the client. In other words, does the service provider need to provide the client with further related material and/or regular updates or news?

This may be achieved as simply as storing and using an email address or a postal address, and may not require the client to use their real-world identity, though some process to capture the contact information is required.

This may not technically require a registration process, which typically involves the creation of a unique client identifier (userid). The data collected may not necessarily need to be retained. For example, if a web-site is used to request information be posted to a postal address, the address provided could be deleted once the information has been sent. In a case like this, no registration or client identifier needs to be performed, though not doing so will prevent service history and personalisation functionality as described below.

It is important to know if the transaction you are analysing requires a contact capability, because a requirement for being contactable necessitates some identity registration and authentication to occur. In other words, the transaction cannot be completely anonymous if there is a need for further contact, as the service provider must know who it is interacting with. If there is no need for further contact, there *may* be no need for the client to identify themselves at all, which leads to the possibility of an anonymous identity category.

Service history

Similar in many ways to contactability, is a requirement to maintain a service history. In other words, do either the service provider or the client need the ability to trace repeat uses of the service, so that a history of all services provided is required. If so, the service cannot be completely anonymous, and some level of registration, allocation of a unique client identifier, and subsequent authentication is required. In essence, by providing a unique client identifier, a method of associating multiple interactions is enabled.

Personalisation

Similar to service history is a requirement to offer service personalisation. This would allow a client's preferences to be automatically loaded on repeat visits, or would allow the service provider to customise future interactions with the client to their specific needs or interests. In these cases this will imply a minimal level of registration requiring identification of the client. A common example of a basic level of personalisation is used by many Pizza delivery businesses, where the client provides a telephone number, and this is stored in the service provider's database to provide information on the client's name, address, and even personal preferences.

Real world identity

Many transactions will require the service provider to know the real world identity of the client. This may be due to the need to provide an official receipt for payment which identifies the client, a need to know something about the client (such as their age) in order to qualify for the service, or for various other legal reasons. If a real-world identity link is required, in order to prevent fraud or misrepresentation, registration at a minimum level of IRAL-2 must be performed by the service provider or trusted third party registration authority, and self registration is unable to be used.

Non-repudiation of registration

Some transactions may require undeniable proof that the transaction has occurred involving a specific client. Non- repudiation controls are controls that are designed to prevent a client from being able to deny receipt or transmission of information or participation in a transaction.

For the purposes of QGAF, the aspect of non-repudiation of interest is non-repudiation of the registration process itself. What is required is sufficient evidence to prevent the client from repudiating the registration, that is, to claim that they were not the client who was registered by the registration authority. This may occur if there is a dispute about a later authentication using an authentication token provided to the client. A possible denial used by the client could be that they were not the client who underwent the registration process (in other words someone else was impersonating them in the registration process). To prevent this, a biometric of some sort should be taken during registration (most often this would be a photograph). If a dispute arises, the biometric can be checked against the client to determine if the client was the person who was registered by the registration authority.

Such levels of protection would be rarely required, and hence the taking of a biometric during registration is only required at the highest level of registration, IRAL-4.

Service delivery non-repudiation

Service delivery non-repudiation is classed as non-repudiation that validates that the originator sent the transaction, the transaction was not interrupted or corrupted in transit and the receiver received the transaction with full integrity. This does not necessarily imply that the transaction is conducted electronically. This can be achieved through the physical delivery of documents that have been signed by either party.

From a QGAF perspective, IRAL-0 and 1 do not provide service delivery non-repudiation, as there is no knowledge of who the client is. IRAL-2, 3 and 4 provide increasingly higher levels of confidence in the identity of the client who conducted a transaction. A high level registration process combined with a high level Identity Authentication Assurance Level (see section 2.4) would provide a high level of service-delivery non-repudiation. In other words, this would make it difficult for a client or service provider to deny involvement in a particular service transaction.

2.3.2 Documentary evidence required

In registering clients, the service provider or registration authority must assess that the EOI provided meets the identity registration assurance level required. Issues which should be considered when choosing to use such evidence are:

- the trustworthiness of the authentication process used by the issuing agency
- situations where the client may not be able to provide the evidence (eg. people who don’t hold a drivers licence)
- possibility of forgery.

For individuals, biometric data can also be collected during the registration process and used later as evidence of who was registered and received the credentials (for example, as mentioned earlier, this could possibly support non-repudiation of registration). To achieve the identity registration assurance levels, there must be a minimum EOI contained in establishing the identity.

Table 7 outlines the suggested EOI requirements to establish the required identity registration assurance levels for individuals. The associated Queensland Government Authentication Framework: Identity and Registration Concepts document provides more information about Category documents and other information used as evidence of identity.

The suggested documentary requirements are those provided by the NeAF and as specified within the Gatekeeper PKI Framework, and agencies may wish to vary those requirements, provided the overall intent of the assurance level is maintained.

A comparison of the suggested EOI requirements with previous versions of the QGAF and the Commonwealth's *Financial Transactions Report Act (1988)* is provided in Appendix F.

IRAL	Suggested Documentary Requirements for Individuals
IRAL-4	One Category A document AND one Category B document AND one Category C document OR One Category A document AND two Category B documents
IRAL-3	One Category A document AND one Category B document OR Two Category B documents AND one Category C document
IRAL-2	One Category B document OR Two Category C documents
IRAL-1	Self registered or pseudonymous registration (IRAL-1) OR No registration process (IRAL-0) – No evidence required.
IRAL-0	

Table 7: Evidence of Identity Required

The documentary evidence categories are described in Table 8 (page 17).

Category	Documents Satisfying the Category
A. Evidence of commencement of Identity in Australia	• Birth Certificates • Record of Immigration Status: • Foreign passport and current visa • Travel Documents and current Australian visa • Certificate of Evidence of Residence Status • Citizenship Certificate

Category	Documents Satisfying the Category
B. Linkage between Identity and Person (photo and signature)	• Australian Drivers Licence (current and original) • Australian Passport (current) • Firearms licence (current and original) • Foreign Passport • Current Queensland Government public service ID card with photo and signature • Current commonwealth public service ID card with photo and signature
C. Evidence of Identity Operating in the Community (could be another Category A or B document)	• Medicare card • Change of Name Certificate • Credit or Account Card or bank passbook • Centrelink or Department of Veterans Affairs card • Security guard/crowd control licence • BSM issued Marriage Certificate • Tertiary ID card (less than one year old and issued by an Australian university only) • Australian Exam Report (persons under 16 years of age only) • Australian Record of Achievement (persons under 16 years of age only) • Australian Secondary school Exam Certificate (persons under 16 years of age only) • Council rates notices • Letter from employer • Telephone directory • The Electoral Roll

Table 8: Documentary Evidence categories

2.3.3 Third party collaboration

In some instances, the evidence of identity can be a statement provided by a trustworthy third party. The third party must have a formal relationship with the client. However, they must be impartial and independent (eg. they must not be related).

Examples of third parties are an employer of the applicant, a police service, a government department or agency, a bank or other financial institution, a medical practitioner or solicitor with whom the client has a formal relationship, and a justice of the peace. The third parties which will be trusted needs to be established by the registration authority, and may vary from authority to authority.

2.3.4 Known customer scenario

In some cases clients may already be a registered with the service provided; this is described as the known customer scenario. In some cases providers may choose to recognise known customers rather than requiring re-registration of clients.

In this situation, service providers should evaluate if the known customer's previous registration meets the required IRAL, and if any authentication credentials are suitable for use with the new service. This will ensure that the desired AAL is maintained if known customers are recognised.

2.4 Determine the Identity Authentication Assurance Level

During the process of implementing the QGAF, a service provider has determined the Identity Registration Assurance Level and the desired overall AALs. The third assurance level is the IAAL.

The IAAL is the measure used for the level of assurance provided by the authentication process which occurs each time a service is used. That is, it is the level of assurance or confidence the service provider has that when a client returns to a service, that the client is in fact the same entity which was previously registered.

The higher an IAAL, the higher the level of confidence that can be placed in a claimant's assertion of their identity during an authentication process. Table 9 details the IAALs, and the level of confidence achieved through each level. Further the table provides guidance on the capabilities of related authentication credentials to ensure the level of confidence is met, though a more complete discussion of appropriate authentication credentials, two and three factor authentication, and authentication mechanisms is contained in the supporting Authentication Concepts document.

Identity Authentication Assurance Level	Confidence Provided	Description
IAAL-4	High confidence	The highest practical authentication assurance is required. Strong cryptographic authentication mechanisms must be used and authentication will require at least two factors.
IAAL-3	Moderate confidence	A moderate level of confidence in the authentication mechanism is required. Strong cryptographic authentication mechanisms must be used. Generally speaking this level of authentication will require two factors.
IAAL-2	Low confidence	A low level of confidence in the authentication mechanism is required. The mechanism needs to prevent common forms of attack, such as: eavesdropper, replay, and online guessing attacks. For example, a password over an encrypted link. However, strong cryptographic authentication is not mandatory.
IAAL-1	Minimal confidence	Authentication is performed, but there is little assurance placed upon it. For example, a challenge-response password mechanism.
IAAL-0	No confidence	No authentication is performed. Included for completeness only, but does not represent any authentication process.

Table 9: Identity Authentication Assurance Levels

The appropriate IAAL to support the desired AAL and the identified IRAL is shown in Table 10 (page 19).

The table identifies the minimum IAAL required, and higher level IAALs may be able to be used (provided the client has been given sufficient authentication credentials in the registration process).

Any unnecessary increase in the Identity Authentication Assurance Level will increase the costs of implementation without offering any significant benefit. The decision to increase the IAAL **should** be carefully considered by the service provider. During the Cost/Benefit phase the service provider can assess if a higher level of IAAL is desired or warranted.

Registration Assurance Level	Required Authentication Assurance Level				
	AAL-0 None	AAL-1 Minimal	AAL-2 Low	AAL-3 Moderate	AAL-4 High
IRAL-0 - None	IAAL-0	N/A[3]	N/A[3]	N/A[3]	N/A[3]
IRAL-1 - Minimal	IAAL-0 (1)[5]	IAAL-1	(IAAL-3)[4]	(IAAL-4)[4]	N/A
IRAL-2 - Low	IAAL-0 (1)[5]	IAAL-1	IAAL-2	N/A	N/A
IRAL-3 - Moderate	IAAL-0 (1)[5]	IAAL-1	IAAL-2	IAAL-3	N/A
IRAL-4 - High	IAAL-0 (1)[5]	IAAL-1	IAAL- 2	IAAL-3	IAAL-4

Table 10: Minimum Identity Authentication Assurance Level Matrix

2.4.1 IAAL Examples

Consider a service which is evaluated with a desired AAL-1 (because of minimal risk), and with an IRAL-2 (because there is a need for the real world identity of the client to be established in some manner). The above table indicates that an IAAL-1 is the required minimum for authentication. As illustrated in the *Authentication Concepts* supporting document, a simple PIN or password would be sufficient as an authentication mechanism for conducting this service electronically.

If considering a service with an evaluated IRAL-2 and an AAL-2, the above table shows that IAAL-2 would be valid to achieve the required overall authentication assurance.

There may be occasions where the business requirements simply do not match. For example, a service is proposed which is designed and intended for self registration (IRAL-1), but the information which is being requested to be shared is classified 'in-confidence' (AAL-2). Self-registration means that the client can use any name or identifier they like (for example, Mickey Mouse), and are thus essentially anonymous. There is no circumstance where 'in-confidence' information can be shared with an anonymous client.

In cases like this the business requirements may need to change, or the classification of the information may be wrong. In either case, further discussion needs to occur with the business and information stakeholders to resolve the situation. An alternative may be to redesign the service, perhaps removing potentially harmful information which may not be required by all clients and allowing anonymous access to the information. A second transaction could be created for the clients who do need to access the 'in-confidence' information and implemented using an appropriate registration process. These clients are likely to not mind the imposition of the more onerous registration process given the information they are being granted access to.

[3] IRAL-0 means no registration has occurred. In this case, no authentication can be possible.

[4] It is possible for a pseudonymous registration process to be supported by high levels of IAAL. Whilst this has been included on this table as supporting higher levels of overall authentication assurance (AAL), it only does so to a certain extent – ie. a consideration of the impacts that led to a need for a higher AAL level is important, and these shaded positions should only be used when anonymity is vital, and a high level of certainty that the entity which originally registered is the one which subsequently uses the service is also required. By providing high authentication, some of the impacts which could lead to higher levels of risk (primarily those associated with impact on the client themselves), can be dealt with. However, if, for example, a service assessment indicates that information could prejudice or impede investigations or facilitate crime, it would be inappropriate to allow access to this information at a registration level of 1 (which is essentially anonymous) regardless of the level of the subsequent authentication process. See the text under the sub-section 2.5.2 for a further example.

[5] IAAL-1 is the required minimum level if contactability, personalisation or service history support is required, even where overall authentication levels do not require registration.

Once the IAAL has been determined, agencies should verify the results (AAL, IRAL and IAAL) with a second person or group to ensure that the assessment is appropriate. This activity is separate from on-going review of the service authentication requirements outlined in section 2.7.

2.5 Perform level moderation

The three main levels determined by the authentication framework are the Authentication Assurance, Identity Registration Assurance and the Identity Authentication Assurance Levels. It is important when implementing an authentication framework that the service provider can have some flexibility in applying authentication, identity registration and identity authentication assurance levels.

It is paramount to note, however, that the already determined AAL should, in virtually all circumstances, never be reduced to a lower level of assurance, as doing so will significantly increase the risk of harm arising from the service. However, an agency would have the ability to accept and manage residual risks that accrue solely to itself. In other words, if the risk assessment of a service indicates that the highest level risks identified affect the service providing agency only, and not its clients, the agency could choose to accept risk, and adopt a lower level of Authentication Assurance for this service. This does not allow an agency to reduce the AAL when the harm identified would accrue to other parties, and any decisions to lower overall Authentication Assurance Levels must be taken with extreme care.

2.5.1 Cost and benefit

A main consideration when implementing the authentication framework is to consider the costs of authentication mechanisms against the benefit gained. At this stage an assessment has been made that identifies the **minimum requirements** for authentication implementation. A service provider can consider the costs of an increased implementation against the benefit gained, and the fit to the requirements of other services being offered.

As a general guideline, the cost and inconvenience related to a particular authentication solution increases as a function of the assurance level. This is reflected in the increased costs of collection and proofing of data during registration (and re-registration); and also in the increased implementation and/or operating costs of the authentication controls.

The key cost considerations are:

- the number of potential and likely clients
- the cost of the registration process (self registering versus registering in person)
- the cost and lifespan of any credentials issued (certain credentials may only last a couple of days, such as one-time passwords)
- the cost of credential management (requirement for manual versus automatic management such as password resets)
- any existing authentication infrastructure that can be leveraged (existing username/password combinations)

- the expected life of the service (short lifespan with costly authentication management may not be feasible)
- other security costs associated with the service, such as access controls and authorisation mechanisms.

2.5.2 Moderation

An example using Table 10 (page 19) will help explain the moderation process. During evaluation of a service, a service provider identifies a need for an overall AAL of level 3, and an IRAL of level 3. This would indicate a required IAAL of level 3, which would generally involve a two factor authentication process. However, the nature of the service is such that this level of authentication is going to be expensive.

To decrease the AAL a service provider would have to change the service delivery proposal, considering aspects such as reducing the amount of sensitive information being provided over the transaction, which may in turn reduce the authentication failure risk level, reducing the AAL.

It is also possible for a service provider to increase the AAL directly, although this will significantly increase the implementation costs without any real additional benefit to the service. A service provider may wish to increase the AAL if it is expecting to change the service in the future in a way which may require a higher level of AAL, or to take advantage of existing processes or issued authentication credentials already operating at a higher level. It may be feasible and more cost effective to implement the final solution in the first instance, so an assessment of future services may be useful.

Other considerations may come into play during moderation. The identity authentication assurance level matrix of the previous section indicates the minimum IAAL required. There are cases where the business requirements may drive the need to implement high IAALs. This can occur where a client wishes to use a service anonymously, such as for receiving personal test results for a pathology, an aptitude test, or for making human resource enquiries or complaints, and many other business scenarios. In these sorts of services, it may not be important that the client provide a real world identity, but the service provider needs to be certain that the client who made the initial inquiry or request is the same individual who receives the results or response.

Take a hypothetical pathology test scenario. A client registers under a pseudonym, but is provided with sufficient authentication credentials to support an IAAL of level 3. This will ensure that the client can anonymously (through the pseudonym) retrieve the correct results. Although the overall authentication assurance level is minimal, due to the pseudonymous registration, the confidence that can be had that the client who receives the results is the one who originally registered can be high.

2.6 Implement registration and authentication mechanisms

The IRAL and IAAL levels determined by QGAF must be used to implement appropriate registration and authentication processes, controls and mechanisms.

After completing the QGAF assessment process for the assurance levels, the next step is to select appropriate registration and authentication processes and mechanisms for implementation. This section provides a short overview of:

- selecting authentication mechanisms
- approaches to dealing with multiple transactions in a single system; and
- expiry of identities and authentication credentials.

More information regarding these implementation issues (including appropriate authentication mechanisms) can be found in the supporting documents *Authentication Concepts* and *Identity and Registration Concepts*.

2.6.1 Authentication Mechanism Selection

There are potentially several different mechanisms for each IAAL. The difficulty in choosing an appropriate authentication mechanism is significant, given the array of options available and the number of variables which enter into the decision making process. This decision needs to balance the three elements of Security, Cost and Convenience. When selecting an approach to authentication the service provider should consider the following:

- ease of use and registration for users
- ease of implementation by a service provider including consideration of credentials that is already supported by the service provider
- credentials that the client community commonly has
- the likelihood that clients will be able to use the credential with other service providers
- cost per client (to both the service provider and the client)
- setup costs for verification systems for this type of credential
- ongoing costs for verification systems for this type of credential, including software licences, administration.

To ensure consistent evaluation of authentication credentials, a structured approach is recommended. Table 11 below outlines ten attributes across three categories that may assist mechanism selection[6].

RSA Authentication Scorecard		
Total Cost of Ownership	Acquisition cost	What are the initial acquisition costs? Include all additional hardware, software, servers, readers, services, associated with acquiring the authentication solution.
	Deployment cost	What does it cost to deploy the authentication solution? This includes the distribution of any necessary hardware or software; ease of installation; ease of set-up and configuration; training of end-users.
	Operating cost	What are the ongoing operating costs? This may include costs for replacement (eg. expired/lost/ stolen/broken) authentication devices; ongoing management; upgrades; vendor support; help desk support.
Strategic Fit (users)	Convenience/ ease-of-use	How easy is it for end-users to learn how to use the authentication method? How convenient is it for end-users to use the authentication method, day in and day out?
	Portability	How portable is the authentication method? Can it reliably be used to gain access from multiple locations (office, home, airport hotel, kiosk)?

[6] Based on the RSA Security Inc White Paper, The Authentication Scorecard, 2004

	Multi-purpose	Can the authentication method be used for more than one purpose? eg. network access, physical access, application access, photo ID badge, electronic signature, stored value. Does the authentication method leverage a device that is itself used for multiple purposes? eg. PC, PDA, phone.
Strategic Fit (corporate/ system)	Relative security	How strong is the authentication? How secure is the implementation? Is it adequate for the information being protected? Does it meet regulatory requirements (if any) for the protection of information?
	Interoperability/ Back-end integration	Does the authentication solution work natively with multiple products? Does it work only with the installation of additional software? How easy is it to integrate with back-end resources or applications? What resources and applications need to be supported?
	Robustness/ scale	Does the authentication solution scale to the degree required now? Three years from now?
	Future flexibility	What future options may be available from the selection of this authentication solution (whether you currently intend to use them or not)? What future options might be of interest?

Table 11: RSA Authentication Mechanism Scorecard (Part 1)

2.6.2 Approaches to multiple transactions in a system

When dealing with a number of transactions within a single system, two approaches are possible – single or graduated.

Single Authentication method

A single strong method of authentication for all transactions is used where it is decided that the same level of authentication will be used for all transactions. This is regardless of the risk of the individual transaction, and in essence means that the authentication levels selected and used should provide protection for the most sensitive transaction in the system.

If during the conduct of business, a client is likely to use transactions which require different authentication levels, it may make sense to simply authenticate the client at the commencement of the business process to the highest required level, and then allow the client access to the appropriate transactions.

Thus, after analysing the required authentication levels for all transactions, or for the transactions which are known to be most sensitive, the final authentication assurance, identity registration and identity assurance levels should be set to those of the transaction that returns the highest levels. By forcing all authentication requests to be at this level, a single authentication process can provide access to all transactions. This is commonly the approach used for systems which staff access internally.

A common scenario where this approach is applicable is where an agency is deploying a new internal application which consists of many transactions. Generally the authentication

and registration process will be implemented once only at 'login' stage when the application is first started. In this instance the authentication needs to be designed to protect the transaction with the need for the highest assurance levels.

The negatives of this approach become obvious if the individual transactions vary in the authentication levels required. For example, if a system has a number of transactions that require little or no authentication, but one or two which require very high levels of authentication assurance, all users will be forced to be registered and authenticated at the higher levels, even if they may never use the sensitive transactions. This will incur undue cost and inconvenience.

Graduated Authentication method

The graduated method is based on the level of risk involved in each transaction, whereby the authentication mechanism used is matched to the level of risk the transaction entails. Thus, a single system may support multiple levels of authentication. This approach is more commonly used for systems which are made available to external clients, as it ensures the cost of registration and subsequent authentication (and the associated authentication tokens) is kept to the minimum required, but this comes at the increased complexity of requiring the system to support multiple levels of authentication, and checking that appropriate authentication has been achieved before each transaction is allowed.

The delivery of web based transactions and services to the public is a good example of a system which generally takes this approach. Typically such systems allow a more random access to transactions, and here a balance needs to be struck between the need to ensure appropriate assurance levels are maintained, and not requiring too invasive a registration and authentication process for clients. Clients, particularly when using the web to access a service, will often abandon a transaction if the registration process asks for more information than the client thinks is reasonable.

In these circumstances transactions which require little or no authentication assurance should be allowed without requiring a heavier registration and authentication process, even when most clients will later proceed to using a transaction which does require high level of authentication assurance and the registration and authentication process should be implemented only when needed.

A common example of this approach is web-based shopping sites. Good sites will allow the user to browse the catalogue, put items in the shopping basket, and perform other transactions without any form of authorisation. Only when the client wishes to complete the purchase process are they required to supply their full details. A site which requests full details up front including credit card numbers before allowing the user to browse the catalogue will see very high rates of clients leaving without completing the requested information or using the service.

2.6.3 Expiry of identities and authentication credentials

The expiry of identities created by the registration process requires careful consideration at this stage. The length of time that an identity should remain valid is dependent on a range of business requirements, and an expiry policy will need to be created to cover both the expiry of identities and of authentication credentials. Note that expiration of an identity should result in a deactivation of the identity[7]. Identities which are expired will be required to undergo a reactivation process should they need to be restored. Authentication credentials which are expired will need to be reissued.

[7] See Section 4 *QGAF: Identity and Registration Concepts* for more information of deactivation and reactivation processes.

For many organisations, an identity never expires, but only the associated authentication credentials are expired. This commonly occurs with passwords, with many organisations requiring passwords to be reset on a regular basis (for example every 60 days). It is however possible to expire the identity itself, which will in turn automatically prevent the use of any authentication credential in use. This may be the most practical approach when authentication credentials in use do not have an easy means of expiry (a biometric for example).

Where identities are not given an indefinite active life, there are two common approaches to expiry:

1. An identity has a set life based on the date of registration. Typically expiry in these circumstances is set in years.
2. An identity's active life is refreshed by use of the identity, but expires after a certain period on non-use. Typically expiry in these circumstances is set in much shorter periods such as days or weeks. An example may be where a client has not 'logged-in' to a service for 12 weeks, the identity is automatically deactivated, and a re-registration or re-activation process must be conducted to re-activate the identity.

Likewise, similar approaches can be taken to the expiry of authentication credentials.

2.7 Review

Before finalising the design of a service, the results of applying the QGAF must be reviewed to ensure they are appropriate to the intent of the service and associated risks. This should occur before the final service design is endorsed.

Regular review of the authentication requirements of services must be conducted, either:

- After a predetermined period, to ensure that the assurance requirements have not altered from the original scope. This review will identify any changes in information sensitivities and highlight if there are to be any changes to be made to the various authentication levels discussed in this document, and the subsequent authentication implementation.
- When additional transactions are added to the same system. The purpose of this review is to ensure that there are no other flow-on transactions resulting from a service implementation. It is possible that one service may result in further transactions that are of a different nature. These additional transactions must be independently reviewed to determine their authentication assurance levels. The implementation of a set of related levels will often mean the highest level of authentication assurance required is implemented for all services/transactions.

Appendix A Comparison of authentication assurance levels

This section presents a comparison of acceptable assurance levels that a range of authentication mechanisms can support according to the following framework documents[8]:

- NeAF[9]
- NIST, Electronic Authentication Guideline [NIST SP800-63][10]
- IDA, Interchange of Data between Administrations, European Commission Directorate General Enterprise[11]
- UKOnline, Registration and Authentication, e-Government Strategy Framework Policy and Guidelines, v.3.0, UK Office of the e-Envoy [12].

	Assurance Levels				
QGAF	0 None	1 Minimal	2 Low	3 Moderate	4 High
NeAF	0 None	1 Minimal	2 Low	3 Moderate	4 High
NIST	1 Little or None		2 Some	3 High	4 Very High
IDA	N/A	1 Minimal	2 Low	3 Substantial	4 High
UKOnline	0 Minimal	1 Minor	2 Significant	3 Substantial	

Table 12: Assurance levels in four international authentication frameworks

[8] Australian Government Information Office (AGIMO), January 2009. The New Zealand Authentication best practice framework [NZ 2004] was also reviewed but it does not provide guidance on mechanism assurance levels.

[9] Unlike the other frameworks, the NeAF does not specifically distinguish registration assurance from authentication assurance.

[10] Electronic Authentication Guideline. National Institute of Standards and Technology (NIST) Special Publication 800-63, version 1.0.1, September 2004

[11] Interchange of Data between Administrations (IDA), European Commission Directorate General Enterprise, July 2004

[12] Minimum Requirements for the Verification of the Identity of Individuals and Organisations in force, Office of the e-Envoy [UK] version 2.0, January 2003. Even though authentication level 0 applies to minimal damage, section 4.2.3 states that authentication is not required. Minimal damage in the other frameworks indicates some requirement for authentication.

Appendix B Queensland Household Survey 2004 to 2007 (summary)

The following information from the Queensland Household Survey (QHS) conducted by the Office of the Government Statistician within the Office of Economic and Statistical Research (OESR) may be of use when considering the design and delivery of a business service, and the selection of appropriate service delivery channels. These statistics provide detailed information on household computer and internet access and usage, particularly on a regional basis. Statistics collected from 2004 to 2007 included questions regarding citizens' preferences for accessing Government information and services. Further statistical information can be accessed by contacting OESR.

Table 13 contains survey highlights from 2004 to 2007. These statistics indicate that over the 4 year period, use of the internet is increasingly being the preferred channel for government services. However, there remains a significant preference for many Queensland households for the use of 'traditional' service delivery channels (mail, over the counter and phone). While these preferences will continue to change over time, it is recommended when developing a new service that the designers consult the latest findings from the Queensland Government Household Survey, or similar material, to assist with service delivery channel selection, and ensure that the services are delivered using a suitable channel which can and will be accessed by those seeking the service.

Internet access in Queensland	approx % of adult population (18+)			
	2004	2005	2006	2007
Total (whole-of-state)	60	67	77	80
Preferred method of finding information on government services, laws or policies [13]				
Face-to-face over a counter	36	34	30	31
By mail	22	14	18	24
Over the phone to a person	33	29	28	25
Over the internet	35	42	44	50
Preferred method of doing other things with government such as pay bills, make bookings, apply for permits etc				
Face-to-face over a counter	47	42	38	41
By mail	11	7	9	11
Over the phone to a person	19	20	19	22
Over the phone using an automatic bill paying system	26	20	23	22
Over the Internet	24	35	37	49

Table 13: Summary Information from Queensland Household Survey 2004 to 2007

Physical Delivery Channels

Physical delivery channels are those that involve human interaction by the client and the service provider or use the movement of physical documents. These channels usually

[13] Can add to more than 100% as more than one answer was permitted.

involve paper based forms and means of authentication such as signatures, or may require authentication mechanisms that are visual or knowledge based. The primary physical delivery channels are the service counter and mail.

Voice Delivery Channels

These are phone based service delivery channels, which can use operators, or be automated through voice recognition and response systems, or through the use of interactive menus.

Data Delivery Channels

Data based delivery channels are those that are delivered through computers or similar data based devices, and generally do not require any human interaction on behalf of the service provider. Common channels include the internet, private networks, public kiosks or mobile links. These channels require the user to have an authentication mechanism that can be remotely verified, typically using the data channel. It is vitally important to consider the security of the information being delivered on these channels as the threats to electronic data delivery channels can be significant.

A multi-channel environment is one where a single business service is made available through several different channels. For many reasons, it is important that government clients have a choice of the service delivery channel, and to ensure that services are not restricted by being offered using only one channel. Consequently, many government services are available through multiple channels (service counter, call centre, and web being a common combination). The identification of the service delivery channel composition is important in determining appropriate authentication mechanisms.

Authentication mechanisms[14] can differ for different channels. For example, a different mechanism may be used to authenticate a client using a Web channel (eg. userID and password) from that used for over-the-counter services (eg presentation of a photo identification card and check of a signature). These different authentication mechanisms may provide different levels of assurance. What is important is that the different authentication mechanism used for different channels ensure the same *minimum* required assurance levels are met across all channels. For example, the authentication assurance gained from showing a photo identification document (such as a driver's licence) in person may be higher than actually needed, but this does not mean that other channels have to meet this higher standard if it is higher than the minimum required, provided all channels provide a standard of authentication that meets the minimum assurance levels identified for the service.

[14] See the *Authentication Concepts* document for more information on authentication mechanisms

Appendix C Sample risk assessment process

The level of authentication assurance required by a service is influenced by the impacts which may arise as a result of an authentication failure. The greater the level and probability of an impact occurring, and the greater the impact, the higher the level of authentication assurance that has to be achieved in order to reduce the risks and impacts which may be caused by a failure in the authentication aspects of a service to an acceptable level. Because increased levels of authentication assurance will likely increase the cost of the authentication solution, it is important to ensure that the level of assurance is appropriate to the business service.

The risk assessment process outlined below will help ensure the correct authentication levels can be determined, and help to balance the cost of implementation against the benefit gained. Risk is determined by considering two dimensions – impact and probability.

A total security risk assessment of a service or system conducted by risk practitioners is concerned with assessing the likelihood of harm arising from a threat, and considers many more things than an authentication risk assessment does. It is paramount that the following authentication risk assessment is not used to replace a comprehensive security risk assessment of services, and that the difference between these two risk assessments is understood.

The authentication risk assessment described in QGAF is based on the ordinal risk model outlined by *AS/NZS ISO 31000:2009*. This risk assessment should be incorporated into a service provider's overall risk management process and is only part of a whole service risk assessment.

The QGAF risk assessment estimates the 'severity of harm' that may result from authentication failure, and the probability of there being an occurrence of harm as a result of the failure. The severity, in combination with the corresponding probability, determines the level of authentication assurance required.

The risk assessment attempts to identify any event or circumstance that has the potential to cause harm (ie. a consequence or impact) that may arise due to an authentication failure. The severity of the potential harm is estimated using the impact rating matrix. For each circumstance the probability of its occurrence is estimated using the consequence probability rating matrix. These two values (the impact severity rating and its probability rating) are combined to obtain the overall risk level associated with an authentication failure on the service being evaluated.

C.1 Threats

Included below is a discussion of the possible authentication related threats involved in service delivery, which should help inform assessments of impacts and the probability of those impacts occurring.

There are a number of threats to information stored by service providers. When assessing the authentication related risk of a service it is important to consider the boundaries of a service provider's authentication framework. The authentication processes of a system / business process are only responsible for ensuring the successful registering, identification and authentication of a client to begin a service transaction.

There are two main categories to be considered when assessing the level of threat to information in the event that a service provider's authentication process fails. They are intentional and non-intentional.

Intentional threats

Intentional threats can include fraudulent activities that are intentionally trying to gain unauthorised access to information in order to conduct a range of illegal activities. Fraudulent activities have been conducted for, amongst other things, personal financial gain, to discredit the reputation of a third party or cause distress, embarrassment and inconvenience to others, to commit violent acts, and to illegally establish an identity to conduct criminal activities[15].

It is important to note that a service provider may be the key target of fraudulent activity or could be subjected to attacks and information gathering in order to conduct a fraudulent activity against client. As well as fraud, other intentional threats can be intended to cause embarrassment, distress, and inconvenience.

Non-intentional threats

Generally, within the context of authentication, non-intentional threats relate to an authorised client who is registered, identified and authenticated to transact with a service provider, but who receives information not related to their transaction as a result of an accidental disclosure due to mistaken identity. An example could be where a staff member of the service provider unintentionally provides information to a client who has similar attributes to another client.

The main difference to intentional threats is that the entity who receives unauthorised information in this non-intentional manner may or may not use that information for a purpose other than it was initially collected. This may depend on who received the information, the level of sensitivity surrounding the information and the probability for personal gain as a result of receiving the information.

C.2 Impact assessment

Within the context of this framework, when determining risk, the approach is to assume that there is no authentication currently protecting the service, and to evaluate the risk that this 'open door' would pose. This is very important, since if suitable authentication is factored in and operating correctly, then there should always be 'negligible risk' from the authentication related aspects of a service, and such a result would be meaningless for determining the correct AAL.

Thus, consider an unprotected service when performing the following risk assessments. The questions to be evaluated are 'if access to this service/transaction was to be given to a person who should not have had the access, what impact could result, and what probability will there be that the identified impact may actually occur?

It also needs to be noted that the impacts being examined can also involve more than just those involved in the service or transaction, and this needs to be considered when making these assessments. The probability or likelihood of the consequence is not taken into account when determining impacts. This is dealt with later.

Table 14 (page 32) should be used when assessing the severity of impacts which may arise for a service as a result of an authentication failure. The impact severity ratings used here are based on similar information contained in the NeAF 2005. The main difference is that this table adds a 'no impact' level, so that services which do not require any form of authentication can be addressed by the framework. The shaded areas indicate at which point the outcome cannot be realised.

[15] Carey, C. (2002) ID related Fraud Strategic Learning Workbook, Australian Institute of Criminology, Canberra.

Please note that the risk levels and descriptors (eg. minimal, minor etc) used throughout QGAF are those used in the NeAF and may vary from those used in other risk assessments within Queensland Government agencies. The use of the NeAF levels is deliberate to ensure alignment between NeAF and QGAF.

It is important to ensure that agencies assess the impact of both the release of information, and also of allowing an unauthorised person to modify or change information stored in systems.

Table 14 below is based on the NeAF table 'Illustrative consequences and severity', and is provided as a guide only. For example it is not possible to provide clear definitions applicable in all circumstances of assessments such as 'short term distress' or 'limited long term distress'. These descriptions are provided to assist agencies in their consideration of severity, but cannot be prescriptive.

It should also be noted that the impacts identified are generic in nature so as to have the broadest possible application. Agencies may find that some impact types are not relevant to their particular business, and that other impact types which are relevant are not included within the table. Agencies are encouraged to adapt the table to suit agency business and risk management requirements, whilst being mindful of the need to preserve the original intent of the impact assessments.

The assessment of risk can also make use of existing information, statistics or trends from pertinent information which may be available from an agency's own data or another source known to an agency. Regardless of the availability of qualitative information, it will never be possible to provide a completely qualitative assessment of all impact types, and in particular impacts such as public order or government policy.

It is also important to note that the determination of risk is not merely a mechanical computation. Stakeholders need to apply their judgement based on the unique factors associated with the agency's business, the nature of the user base, the overall environment and the transaction aspects[16].

[16] This paragraph substantially reproduced from the *AGAF Implementation Guide for Government – Volume 3* – Part 3, Page 11

IMPACT Type	Severity				
	Lowest				Highest
IMPACT rating	None/ Insignificant	Minor	Moderate	Major	Severe
Risk to any party's safety	None			Any risk to personal safety	Threaten life directly
Distress caused to any party[17]	None		Minor - Short term distress	Limited long term distress	Substantial long term distress
Damage to any party's standing or reputation	None		Minor - Short term damage	Limited long term damage	Substantial long term damage
Inconvenience to any party	None	Minimal inconvenience	Minor inconvenience	Significant inconvenience	Substantial inconvenience
Public order	No Impact		Impact	Prejudice	Seriously prejudice
Release of personally or commercially sensitive data to third parties without consent	No impact	Would have no significant impact	Measurable impact, breach of regulations or commitment to confidentiality	Release of information would have a significant impact	Would have major consequences to a person, agency or business
Impact on Government finances or economic and commercial interests	No Impact		Cause financial loss or loss of earning potential	Work significantly against	Substantial Damage
Financial loss to any client of the service provider[18] or other third party	None	Minimal	Minor	Significant	Substantial
Financial Loss to Agency / service provider	None	Minimal < 2% of monthly agency budget	Minor 2% – < 5% of monthly agency budget	Significant 5% – < 10% of monthly agency budget	Substantial ≥ 10% of monthly agency budget
Threat to government agencies' systems or	No threat			Agency business or	Agency business halted

[17] An outcome that causes distress to any party can not occur at the 'Minimal' rating. Due to the impact of such an event, any realisation of the outcome will automatically result in there being an impact rating at least at the minor level.

[18] The amounts to be considered are suggested as: Minimal <$50, Minor $50-<$200, Significant $200-<$2000 and Substantial ≥ $2,000, but these figures here guidelines only based on impact on an 'average' individual. Where the client is known to be a corporation of other similar entity, these figures would need to be adjusted to something more akin to the figures used for financial loss to the service provider. If multiple clients will suffer the loss, the impact level should be adjusted accordingly to reflect the total losses to clients.

IMPACT Type	Severity				
	Lowest				Highest
capacity to conduct their business				service delivery impaired in any way	or significantly impaired for a sustained period[19]
Assistance to serious crime or hindrance of its detection	Would not assist in, or hinder detection of unlawful activity		Prejudice investigation or facilitate commission of violations that will be subject to enforcement efforts	Impede investigation or facilitate commission of serious crime	Prevent Investigation or directly allow commission of serious crime
Impact on development or operation of major government policy	No impact		Impede effective development or operation	Seriously Impede	Substantially Impede
Impact on the environment	None/ Negligible	Minor impact on the environment.	Measurable short term damage to the environment	Limited long term damage to the environment	Substantial long term damage to the environment
Impact on agency or Queensland Government workforce	None/ Neglible	Minor impact	Measurable impact	Limited long term impact	Substantial long term impact
Impact on risk of litigation	None/ Neglible	Minor impact	Measurable impact	Significant impact	Substantial impact

Table 14: Impact Assessment Matrix

[19] The period here may vary from agency to agency – some agencies may be able to endure a halt in business for a number of days without serious impact on the government or society. Others more directly involved in public safety and similar services would be less tolerant of outages.

To provide some assistance in completing the impact assessments, the following table provides examples of considerations agencies may make when assessing each impact type. Agencies may have other considerations when assessing impacts, and it may be useful for agencies to develop their own guidelines as to the considerations which may apply to each impact type.

Impact type	Possible considerations
Risk to party's safety?	Consider any risk of any injury or impact on safety at all, as well as the possibility of loss of life. An example could someone being registered for a job which they should not have been because they were not appropriately qualified (eg. unqualified truck driver who causes an accident which injures or kills someone), or are prevented by previous criminal history. Other examples could include release of names or locations of under-cover officers, people under protection orders.
Distress caused to any party?	From the client's or public's point of view, distress could be caused by many things, including denial of expected services. From a service provider's point of view, potential impacts could be minor or major re-work or re-processing of the transaction, through to stress impacts on employees and possible loss of jobs or major reorganisation forced by the inappropriate access.
Damage to any party's standing or reputation?	Issues to consider include potential for adverse publicity, either locally or wider, and the potential to damage of either the service provider's or client's ongoing reputation. If an incorrect decision was made or inappropriate access to information was granted etc, would it be of interest to the media?
Level of inconvenience to any party?	From a client's point of view consider factors such as causing client to re-apply for a service or entitlement, denial of service provision, delays in service provision. From a service provider's point of view consider factors such as job stress caused by the failure, loss of jobs, re-work or re-processing. Examples may be the need to recall and reissue licences / tickets or registrations.
Public Order	Need to consider whether disclosure of information could pose a threat to community relations and public order. This may occur when information is released that can cause 'alarm' in a way that then results in damage to public order. An example would be disclosure of an offender's identity or whereabouts where the community could then react and disturb public order.
Release of personally or commercially sensitive data to third parties?	Could information which should not be made public be released? Examples include medical records, commercially sensitive information that could impact on current or future business, personal information which should be protected from release.
Impact on Government finances or economic and commercial interests	Would disclosure of information result in financial or economic consequences to government. Release of information may result in financial gain or loss. Disclosure of planning decisions which could result in changing valuations would be an example
Financial Loss to any client of the service provider or other third party	Consider this from the clients perspective - what losses could they incur? Consider the possibility of fraud, a party illegally transferring money, a party gaining control of assets they don't legally own (eg by changing ownership details), payments being made to the wrong party (eg a grant or benefit), etc.

Impact type	Possible considerations
Financial Loss to service provider?	Consider this from the service providers perspective - what losses could they incur? Considerations include possibility of fraud, a party illegally transferring money, a party gaining control of assets they don't legally own (eg by changing ownership details), payments being made to the wrong party (eg a grant or benefit) etc.
Threat to government agencies' systems or capacity to conduct their business?	Would an authentication failure of this transaction have the potential to reduce or prevent an agency or external party conducting their business? For how long would this reduction / prevention last? Could data be inappropriately damaged? How extensively? Could systems be made inoperable?
Assistance to serious crime or hindrance of its detection?	Would an authentication failure of this transaction have the potential to assist in the conduct of a crime? This could include release of information enabling the planning of a crime, the creation of a false identity, or change to information which may help prevent the detection of a crime.
Impact on development or operation of major government policy	Would disclosure cause embarrassment to government in the stages where policy is being formulated? The impact may be that a major policy initiative will not proceed.
Impact on the environment	Would inappropriate disclosure of or unauthorised changes to the information be damaging to the environment?
Impact on agency or the Queensland Government workforce	Would inappropriate disclosure of information result in a negative impact on agency or the Queensland Government workforce? For example could there be a damaging effect on: • staff morale? • workplace health and safety? • enterprise bargaining agreement negotiations?
Impact on risk of litigation	Would disclosure of the information result in a breach of legal, regulatory or contractual obligations?

Table 15: Sample impact considerations

C.3 Probability of harm

Whether an individual or group receives unauthorised information through intentional or non-intentional means, harm may or may not result, depending on the nature of the information released, and the intent and actions of the recipient of this information. Thus, when assessing the level of risk from a threat it is necessary to assess the probability of there being any harm from each impact as a result of the authentication framework failing. In other words, how likely is it that the possible impact identified will actually occur.

The probability rating shown in Table 16 must be used in this assessment. Each probability rating has been given a guideline percentage to assist its application, and is a rating of the likelihood that someone (client, service provider, member of the public, other organisation) will suffer harm as a consequence of a failure in authentication. In other words, the question being asked is ‘Given an instance of authentication failing, how likely is it that the impact identified will actually be incurred?’ This is a different style of probability assessment than that commonly used in an information security context.

In making an assessment, it should be noted that the probability of an impact occurring may be linked to a person's motivation. In other words, where there is a potential for financial gain, the probability of that impact occurring is likely to be high.

Probability Rating	Definition	Guideline Percentage
Almost Certain	It is almost certain that an impact will occur from a failure in authentication	95-100%
Likely	It is likely that an impact will occur from a failure in authentication.	50-95%
Possible	It is possible that an impact will occur from a failure in authentication.	10-49%
Unlikely	It is unlikely that an impact will occur from a failure in authentication.	1-9%
Rare	It would be rare that an impact will occur from a failure in authentication.	<1%

Table 16: QGAF consequence probability rating

C.4 Authentication risk level

Table 17 determines the Authentication Risk Level. For each consequence, determine the risk level by locating the intersection of the Impact Severity and Probability.

		Impact severity				
		None	Minor	Moderate	Major	Severe
Probability	Almost certain	Negligible	Minimal	Low	Moderate	High
	Likely	Negligible	Minimal	Low	Moderate	High
	Possible	Negligible	Minimal	Low	Moderate	High
	Unlikely	Negligible	Minimal	Minimal	Low	Moderate
	Rare	Negligible	Minimal	Minimal	Low	Moderate

Table 17: Determining the Authentication Risk level

When determining the overall Authentication Risk Level, each individual impact **must** be subjected to the risk assessment process. It is possible for lower impacts to be a higher risk due to a higher probability. The final authentication risk level to be used in subsequent steps of the authentication framework is the highest risk level indicated by any of the impacts.

Table 18 provides a sample risk assessment for a service. In this fictitious example, there is one consequence which has been rated as High risk. Therefore, the authentication risk level which needs to be treated, and therefore should be used in the rest of the framework is High.

Consequence	Impact severity	Probability	Risk
Risk to any party's safety	None	Rare	Negligible
Distress caused to any party	Major	Almost Certain	Moderate
Damage to any party's standing or reputation	Major	Likely	Moderate
Inconvenience to any party	Severe	Possible	High
Impact on Public Order	Moderate	Possible	Low
Release of personally or commercially sensitive data to third parties	None	Rare	Negligible
Impact on Government Finances	Minor	Unlikely	Minimal
Financial loss to any client or third party	None	Rare	Negligible
Financial loss to service provider	Minor	Possible	Minimal
Threat to government agencies' systems or capacity to conduct their business	None	Rare	Negligible
Assistance to serious crime or hindrance of its detection	None	Rare	Negligible
Impact on government policy	Minor	Possible	Minimal

Table 18: Example Risk Assessment

Appendix D Privacy

An entity's privacy is an important consideration when establishing a service. Although not all of the information privacy principles relate directly to authentication, it has been incorporated into QGAF as privacy is an important factor which affects business decisions when establishing services that collect individual personal information.

The Queensland Government has committed its agencies to the responsible and transparent collection and management of citizens' personal information. Limits on the transfer of personal information between agencies, other levels of government and the private sector are included within this commitment.

The *Information Privacy Act 2009* ('the IPA Act'), provides safeguards for the handling of personal information in the public sector environment, and to allow access to and amendment of personal information. Agencies must comply with the 11 Information Privacy Principles (IPPs) about how individuals' personal information is collected, stored, used and disclosed. The IPPs are set out as follows:

- IPP 1 – Collection of personal information (lawful and fair)
- IPP 2 – Collection of personal information (requested from individual)
- IPP 3 – Collection of personal information (relevance etc)
- IPP 4 – Storage and security of personal information
- IPP 5 – Providing information about documents containing personal information
- IPP 6 – Access to documents containing personal information
- IPP 7 – Amendment of documents containing personal information
- IPP 8 – Checking of accuracy etc. of personal information before use by agency
- IPP 9 – Use of personal information only for relevant purpose
- IPP 10 – Limits on use of personal information
- IPP 11 – Limits on disclosure.

The IPA Act defines 'personal information' as follows:

> '***Personal information*** is information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.'

The Information Privacy Principles provide an important perspective for the implementation of sound authentication mechanisms. For example, IPP 11 provides that an agency having control of a document containing an individual's personal information must not disclose the personal information to an entity other than its subject unless one or more of the conditions set out in the IPA Act is satisfied. Similarly, IPP 4 provides that documents containing personal information must be to protected by employing security safeguards against loss, unauthorised access, use or disclosure. Using an appropriate authentication mechanism for a given type of transaction helps the agency fulfil these principles. By reaching the requisite level of confidence concerning the validity of a claimed identity, an agency can be sure that a proposed disclosure of personal information will be made to the subject of the information - and not to a third party-impostor or a third party inadvertently mistaken for the subject of the personal information.

The Information Privacy Principles also present challenges for authentication practices. When determining an appropriate identity registration assurance level under QGAF, agencies must consider whether collection of real world identifiers (such individuals' real names, residential addresses, dates of birth, etc, for linkage with an assigned unique identifier) accords with IPP 1. IPP 1 states that:

'(1) An agency must not collect personal information for inclusion in a document or generally available publication unless –

(a) the information is collected for a lawful purpose directly related to a function or activity of the agency; and

(b) the collection of the information is necessary to fulfil the purpose or is directly related to fulfilling the purpose.'

The choice of an pseudonymous identifier (IRAL-1) (for example, for the purpose of recognising return visits to a counselling service) is appropriate in terms of IPP 1 whenever real world identifiers are not needed in order to perform the function or activity.

The assignment of a pseudonymous identifier meets the authentication mechanism that requires some identity credential to be provided – in the example for recognising return visits to the counselling service – but there is no unnecessary collection of personal information comprising real world identifiers. This example provides maximum privacy protection, but for some types of counselling or treatment services a pseudonymous identifier linked to escrowed real world identity may be more appropriate. Once again the agency must include in its assessment the text and spirit of the IPPs and the means available of affording privacy protection, but without ignoring other important interests and values, for example, the need for security and to protect public health.

D.1 Privacy impact assessment

When assessing the impact of the selected authentication model on privacy the following points must be considered as part of the analysis (Kreizman 2004):

- Does the service require identity and authentication?
- Are multiple identities allowed (Not possible if the identity is required to be linked to a real world identity)?
- What information is collected as evidence of identity, and how is that evidence managed?
- What personal information is stored along with the user's system identity?
- What information is collected and stored when identity credentials are used?

D.2 Opt In/out and information accessibility

Generally speaking, it is the client's choice as to whether they choose to use a certain service delivery channel. As electronic service delivery becomes more pervasive, agencies must ensure that clients choosing not to use such channels (due to lack of infrastructure or concerns regarding privacy) are not disadvantaged. When a client chooses to opt out or not opt into a service delivery channel they must be capable of having the same level of access to information no matter which service channel they choose.

It should be noted that the choice of service delivery channel can be related to privacy issues. For example, some people may feel the need to register for electronic service delivery can invade their privacy (for example because they need to supply an email address to receive information), particularly if the same service delivered over a counter does not require them to leave an email or contact address.

D.3 Information sharing

When registering users, (which involves collecting personal identification and contact information), agencies must adhere to the information privacy principles contained in the IPA Act noted above. In line with these principles, information gathered during the

registration process must not to be shared with other agencies or business partners unless the client's permission to do so had been gained. Likewise, when recording transaction detail on services provided, agencies must protect this data and not make it available to other agencies or commercial entities such that a client's transaction profile can be constructed. Any data shared with another agency must be de-personalised or aggregated such that an individual's identity is not discernable.

Additionally, where multiple service providers are using the one authentication mechanism infrastructure, each service provider must only access the identity information they have collected, and the ability to access other client information not collected by the service provider must be prohibited unless the client's permission to do so has been gained.

Appendix E Evidence of Identity Comparisons

The following tables compare the Evidence Of Identity (EOI) requirements of the current and previous versions of QGAF. The tables also provide a comparison between against the Commonwealth's *Financial Transaction Reports Act (1988) (FTRA)* document categories and likely points values. Please note that this is not intended to be an exhaustive list, and agencies should verify that the mappings support their authentication needs as part of the QGAF process.

Documents	Current QGAF	Previous QGAF	AUSTRAC EOI Check (Form 201)	FTRA document type
Type	**Category**	**Category**	**Point Value**	**Category**
Australian Birth Certificate (full)	A	A	70	Primary
Australian Citizenship Certificate or Naturalisation Certificate	A	A	70	Primary
Australian Defence Force (excluding civilian) Photo ID card	N/A	A	40	Primary
Australian Drivers License with Photo ID (current or expired <2 years)	B	A	40	Secondary
Australian Exam Report (persons under 16 years of age only)	C	N/A	25	Secondary
Australian Passport (current or expired < 2 years)	B	A	70	Primary
Australian Record of Achievement (persons under 16 years of age only)	C	N/A	25	Secondary
Australian Secondary School Exam Certificate (persons under 16 years of age only)	C	N/A	25	Secondary
BSM issued Marriage Certificate	C	N/A	25	Secondary
Centrelink or Department of Veterans Affairs Card	C	B	N/A	Secondary
Certificate of Evidence of Resident Status	A	N/A	40	Primary
Change of Name Certificate	C	N/A	N/A	Secondary
Council rates notices	C	N/A	25	Secondary
Credit or Account card with signature and embossed name, bank passbook, or bank statement	C	B	25	Secondary

Documents	Current QGAF	Previous QGAF	AUSTRAC EOI Check (Form 201)	FTRA document type
Current commonwealth public service ID card with photo and signature	B	N/A	40	Secondary
Firearms license (Australian issued - current and original)	B	B	N/A	Primary
Foreign Passport	B	A	70	Primary
Foreign Passport and Current Visa	A	N/A	70	Primary
Letter from employer (current or within last 2 years)	C	N/A	35	Secondary
Medicare card	C	B	25	Secondary
Record of immigration status (certificate of evidence of resident status)	A	A	N/A	Primary
Security guard/crowd control license (Australian Issued)	C	B	N/A	Secondary
State 18+ Photo ID card	N/A	A	40	Secondary
State or Federal Police Officer Photo ID	N/A	A	40	Secondary
State Transport Driver Authorisation (current or expired < 2 years)	N/A	A	40	Secondary
State Transport Rider or Driver Trainer Accreditation (current or expired < 2 years)	N/A	A	40	Secondary
Telephone directory	C	N/A	N/A	Secondary
Tertiary ID card (less than one year old and issued by an Australian university only)	C	B	40	Secondary
The Electoral Roll	C	N/A	N/A	Secondary
Travel documents and current Australian Visa	A	A	N/A	Primary

Table 19: Comparison of EOI between the current and previous QGAF, and the FTRA

	Current QGAF		Previous QGAF	
Identity Registration Assurance Level	Possible 'Points' range (cf. AUSTRAC Form 201 EOI check)	Document Requirements	'Points' & Currency	Document Requirements
IRAL-4	210 -105 points	1 x A + 1 x B + 1 x C **OR** 1 x A + 2 x B	Minimum 150 Points Currency of EOI = not older than 3 years	2 x A + 1 x A or B (minimum 3 docs)
IRAL-3	175-80 points	1 x A + 1 x B **OR** 2 x B + 1 x C	Minimum 100 points Currency of EOI = not older than 3 years	1 x A + 1 x B + 1 A or B (minimum 3 docs)
IRAL-2	70-40 points	1 x B **OR** 2 x C	Minimum 50 points Currency of EOI = not older than 3 years	1 x A + 1 x B (minimum 2 docs)
IRAL-1	Not applicable	No evidence required	No Minimum	No evidence required
IRAL-0				

Table 20: Comparison of IRAL requirements between current and previous QGAF