Tasmanian Government Identity and Access Management Toolkit

Summary

January 2010

Department of Premier and Cabinet

Tasmania
Explore the possibilities

For further information on the Toolkit, contact the Office of eGovernment:
egovernment@dpac.tas.gov.au| www.egovernment.tas.gov.au

Contents

Identity and Access Management Toolkit

1 Introduction

The Tasmanian Government provides a wide range of services to the public, public sector staff, business and other arms of government. The implementation of electronic service delivery has accelerated the need for a consistent approach to identity and access management, particularly as government agencies seek to integrate electronic business transactions to improve client service.

Government agencies have an obligation and responsibility to:

- Provide a duty of care and protection to their staff and clients
- To maintain staff and client confidentiality
- To establish and maintain the security and integrity of information and systems.

The need to improve identity and access management practices within government agencies was recognised by the Council of Australian Governments (COAG) when it endorsed the National Identity Security Strategy (the Strategy) at a special meeting on counter-terrorism held in 2005[1].

The Strategy covers six aspects:

1. A nationally consistent approach to establishing identity and client enrolment practices
2. Security features for common identity documents
3. Identity document verification
4. Integrity of identity data
5. Authenticating identity document holders
6. Interoperability of biometric technologies

An Inter-governmental Agreement (IGA) to implement the National Identity Security Strategy was signed by COAG in 2007. The *Tasmanian Government Identity and Access Management Toolkit* (the Toolkit) represents the Tasmanian Government's implementation of that Agreement.

The Toolkit was developed by the Office of eGovernment, Department of Premier and Cabinet (formerly the Inter Agency Policy and Projects Unit), in consultation with Tasmanian Government agencies.

---

[1] For details, see Australian government – Attorney-General's Department:
http://www.ag.gov.au/www/agd/agd.nsf/Page/Crimeprevention_Identitysecurity

2   What is the Toolkit?

The *Tasmanian Government Identity and Access Management Toolkit* provides a process and a set of definitions that allow Tasmanian Government Agencies, as service providers, to evaluate the risks 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 its staff[2].

The Toolkit is made up of four parts:

1.   Assessing Identity Risk Guidelines – provides guidance for the seven step process for applying a risk management approach to identity and access management practice
2.   Identity Registration Guidelines and Standards – covering client identity enrolment or registration practice
3.   Identity Credential Management Guidelines and Standards – covering secure credential management practice
4.   Access Management Guidelines – covering ongoing secure access management practice

It is evident that different types of services require different levels of assurance. For example, services involving sensitive information or financial transactions require a higher level of assurance about the identity of a client than services which do not. Accordingly, each part of the Toolkit provides guidelines in each part for the separate risk categories that can be applied by agencies to the range of services they provide. Where relevant, specific standards are included, providing specifications for a particular process or activity.

The Toolkit expands and deepens the guidance provided to agencies through the *Tasmanian Government Information Security Framework*[3], and forms a part of that Framework.

---

[2]   The term 'staff' includes employees, officers, contractors and volunteers
[3]   See www.egovernment.tas.gov.au

3   Why use the Toolkit?

The purpose of the *Tasmanian Government Identity and Access Management Toolkit* is to guide agencies in the determination of identity registration, identity credential issuing (or authentication), and credential verification requirements for services. It applies equally to:

- Staff and clients of Government
- Development of new services and review and improvement of existing services
- Electronically and non-electronically delivered services

The implementation of electronic service delivery has accelerated the need for a consistent approach to identity and access management, particularly as government agencies seek to integrate electronic business transactions to improve client service.

The Toolkit is intended to be used by personnel within Tasmanian Government agencies and will be particularly relevant to:

- People 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

Security functions that are not directly related to identity and access management practices are outside the scope of the Toolkit and should be addressed through the implementation of the relevant guidelines identified in the *Tasmanian Government Information Security Framework.*

The Toolkit only provides guidance on the determination of identity and access management requirements and risks, together with the most appropriate assurance levels for identity registration (enrolment), credential verification (authentication) and access policy. Other security functions that are not directly related to the identity and access management aspects of a service (eg broader information security, availability and auditing) are outside the scope of the Toolkit. It should also be noted that the Toolkit 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 Toolkit will be incorporated within the *Tasmanian Government Information Security Framework* as the process to be applied by all Tasmanian Government agencies when implementing identity and access management mechanisms.

The Framework incorporates a number of documents, as shown in the following table. One of those documents is the *Tasmanian Government Information Security Charter* (the Charter), which was approved by Cabinet in May 2003. The Charter outlines information security principles and policies that are to be applied by agencies to achieve appropriate information security within the Tasmanian Government. The Charter establishes:

- Information Security Policy Principles that agencies are to adhere to

- Information Security Policies that agencies are to adhere to

- Important legislative requirements

- Primary roles and responsibilities for information security

Document Name	Contents Outline
Tasmanian Government Information Security Charter	Legislative requirements Information security policy principles Information security policies Primary roles and responsibilities
Tasmanian Government Information Security Guidelines	Overview of the Tasmanian Government Information Security Framework Information security governance Record security Physical security Personnel General ICT Incident management Information security risk management
Tasmanian Government WAN and Internet Services: Information Security Policies and Standards	A whole-of-government implementation of the framework, with polices and standards specific to this topic
Identity and Access Management Toolkit	*Overview and context of the Toolkit* *Assessing Identity Risk* *Identity Registration Guidelines & Standards* *Credential Management Guidelines & Standards* *Access Management Guidelines*

As it forms part of the *Information Security Framework*, the *Identity and Access Management Toolkit* is to be applied by agencies on an 'opt in – argue out' basis.

4   When to use the Toolkit

The *Tasmanian Government Identity and Access Management Toolkit* is intended to be used by all Tasmanian Government agencies to evaluate the identity and access management aspects of their client services, including internal staff services. Ideally, the Toolkit should be applied to all services and systems. However, it is recognised that this may be impractical and potentially disruptive as well as cost-prohibitive for many existing systems and services. It is therefore recommended that the Toolkit be applied in the following order:

- All new systems and services should be evaluated against the Toolkit during development or implementation
- Existing systems and services requiring cross-agency authentication should be evaluated against the Toolkit
- Existing systems and services should be evaluated against the Toolkit, 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, retro-fitting of existing ICT applications to support the higher levels of identity and access management that may be indicated by the Toolkit process might 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, could choose to accept a risk of having weak identity and access management processes for systems containing security classified information. In which case, it should take other precautions to minimise the risk of inappropriate access to or release of that information.

It is strongly recommended that a second person or group verify all initial assessments of identity and access management levels to ensure that they are appropriate and in accordance with the Toolkit. Additionally, as indicated by the review step in Part 1 of the Toolkit, 'Assessing Identity Risk Guidelines', it is strongly recommended that agencies establish procedures to periodically review and verify that the correct identity and access management levels are in use and remain valid from initial assessment, particularly for applications that have external access.

5   How to use the Toolkit

The *Tasmanian Government Identity and Access Management Toolkit* has been developed as a practical resource business units can work through to determine the identity and access management requirements for a particular service.

The Toolkit is made up of four different parts, which relate to the four key business processes for the service:

Assessing identity risk (Part 1)

Identity registration (Part 2)

Identity credential management (Part 3)

Access management (Part 4)

Part 1 of the Toolkit, 'Assessing Identity Risk Guidelines', provides a set of seven risk assessment steps to determine the form of identity and access management processes to be applied to the delivery and management of a particular service.

Part 1 has been developed as a workflow. By working through the seven steps, the user can ascertain the relevant risk level and corresponding procedures that should be applied to the stages of client registration, credential issue and ongoing identity and access management that will be implemented for the service or process.

In Part 1, users are guided to determine the appropriate assurance levels for the service they are assessing. There are three assurance levels to be assessed – the Access Assurance Level, the Identity Registration Assurance Level, and the Credential Assurance Level. Each of these levels is expressed in the form of a number from zero to 4, with 4 representing the highest risk. The following table provides a summary of the seven steps covered in Part 1 of the Toolkit.

Once the relevant assurance levels are determined, Part 1 guides the user to the corresponding sections of Parts 2, 3 and 4 for the guidelines and standards that are to be used to develop appropriate business procedures for the identity registration, credential management and ongoing access management procedures to be applied to the particular service being assessed.

Step 1 **Determine business requirements**	The logical first step is to define what the service is, how it is planned to be delivered, and what other factors impact on the delivery of that service The way a service is to be provided will impact on the level of assurance that will be required (eg assurance needs will differ for physical and online delivery) General or specific legislative requirements may impact on the level of assurance that needs to be applied
Step 2 **Determine access assurance level**	This step is concerned with determining the level of risk that is applicable to the particular service How confident do you need to be that the person registering for the service is in fact who they claim to be? How critical is it that the service is delivered to the same person who was registered? What are the consequences that the service is delivered to the wrong person?
Step 3 **Determine identity registration assurance level**	Allows for matching the assessed risk determined in Step 2 with the level of confidence required in relation to the registration process for that service By determining the business requirements, the level of assurance can be decided – ie the greater the need to confirm the identity of an applicant, the higher the assurance level required in the registration process Once the Identity Registration Assurance Level (IRAL) has been determined, the equivalent section in Part 2 Identity Registration Guidelines and Standards would be consulted in developing the business procedures to be applied For example, if this step determines that a High, or Level 4 assurance level is applicable, you would refer to the Level 4 guidelines in Part 2 of the Toolkit to develop the appropriate business procedures
Step 4 **Determine the credential assurance level**	Similarly to the previous step, this also provides for the matching of the assessed risk and assurance levels determined by Steps 2 and 3 in relation to the level of assurance required in the issuing and management of any associated credential As with Step 3, once the credential assurance level has been determined, the equivalent section in Part 3 Credential Management Guidelines and Standards would be consulted in developing the business procedures to be applied Generally, the assessed credential assurance level will be the same as the overall assurance level (Step 1) and the identity registration assurance level (Step 3) However, there may be instances where the three levels may not match – eg the credential is intended to be used to access specific entitlements, but the eligibility for that entitlement may be based on a physical or social condition where the assurance level for assessing the identity of the person to whom the credential was issued is determined to be minimal or low risk
Step 5 **Perform cost benefit analysis**	This is intended to provide a final check of the assessed risk levels determined by the previous steps to ensure a suitable balance between the cost of implementing procedures at the identified assurance levels and the relevant business requirements For example, while it may be desirable to apply the highest risk level to the issuing and ongoing management of a credential, the actual cost of doing that may be far in excess of the actual delivery cost of the service, or the risk applying to the failure of the credential

Step 6 **Implement registration and authentication mechanisms**	Once the required assurance levels and the corresponding business processes have been determined (ie by reference to Parts 2, 3 and 4) and documented, the next step is to implement the service
	This step involves a number of practical considerations, including:
	– Updating the agency asset register with details of the service
	– Selecting the type of credential to be issued in line with the associated business processes
	Part 4 of the Toolkit, *Access Management Guidelines*, should be consulted when determining the procedures for the ongoing management of all registered identities and credentials, including the establishment of the directory, or client database for the service
Step 7 **Review**	All business processes need to be regularly reviewed to ensure ongoing compliance with relevant legislative and business requirements
	Reviewing a service also ensures that the assessed assurance levels for all aspects of the delivery of the service continue to be relevant and reflect changes in the environment in which it is operating
	The review would involve repeating Steps 1 to 6 above

6   Interpretation

As noted above, the *Tasmanian Government Identity and Access Management Toolkit* forms part of the *Tasmanian Government Information Security Framework* and agencies are expected to apply it as part of their compliance with that Framework.

To be consistent with the *Tasmanian Government Information Security Framework*, the same key words have been used to indicate the degree to which the proposed guidelines and standards are to be applied. These key words are directly linked to the identified assurance level.

For example, guidelines for risk assurance Level 4 transactions will be more prescriptive: 'The registering agency **will** …'. This reflects the intention that the guideline is obligatory in order to meet the level of risk involved.

However, for a risk assurance Level 3 transactions, the equivalent guideline states: '**It is desirable** that the registering agency …'. This reflects the intention that the stated guideline be applied, but allows for some flexibility. However, a decision not to comply with the guideline must be carefully considered before being made and acted upon.

The following may be of assistance in this regard:

Key words	Interpretation
WILL	The item is considered to be obligatory
WOULD, DESIRABLE	The item is considered to be important, and while there may be valid reasons for deviating from the provisions, the full implications for doing so need to be fully considered
SHOULD, COULD, MAY, MIGHT	The item is considered important, but its application is for the agency to determine As for the previous entry, deviating from this course of action needs to be fully considered
SHOULD NOT	Valid reasons for taking this approach may exist in particular circumstances, but the full implications for doing so need to be fully considered
NOT ESSENTIAL	Implementing the item is not considered necessary, but may be implemented if considered appropriate in particular circumstances

It should also be noted that, within a particular risk assurance level, some leeway is allowed in the application of the guidelines and will contain both obligatory and optional elements within the same assurance level. That is, some suggested actions within a particular risk assurance level are considered to be critical regardless of the assurance level, while others are not deemed to be as critical and may be implemented at the discretion of agencies.

While acknowledging that the Toolkit can appear complex, the Office of eGovernment will, wherever possible, assist agencies upon request with the assessment of agency services against the Guidelines.

7   Acknowledgments

Work undertaken in other jurisdictions was referenced in the development of the *Tasmanian Government Identity and Access Management Toolkit*.

In particular, the Project acknowledges the work undertaken by the following:

- The Australian Government Information Management Office – Australian Government e-Authentication Framework / National e-Authentication Framework
  (See www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html)
- The Queensland Government Chief Information Office – Queensland Government Authentication Framework
  (See www.qgcio.qld.gov.au/QGCIO/ARCHITECTUREANDSTANDARDS/Pages/security.aspx)
- The Western Australian Office of eGovernment – Identity and Access Management Framework
  (See www.sr.egov.wa.gov.au/StandardsRepository/Pages/DocumentDetails.aspx?ItemId=33&tab=oeg)

The guidelines have been based upon the *Australian Government Authentication Framework*, developed by the Australian Government Information Management Office (AGIMO) at the direction of the Online and Communications Council.
(see www.agimo.gov.au/infrastructure/authentication/agaf_b)

Part 1

Assessing identity risk guidelines

Different types of government services face different levels of risk. For example, services involving sensitive information or financial transactions face the risk of more severe consequences if the information is misused than other less sensitive services.

The higher the risk a service faces, the more assured the service owner needs to be that only authorised people are accessing the service delivery information. This concept is expressed in the *Tasmanian Government Identity and Access Management Toolkit* as the Access Assurance Level, which must be commensurate with the level of risk identified for the particular service.

It is important for Government agencies to provide a level of access assurance that is appropriate for the service involved. 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.

The process steps for the application of the *Identity and Access Management Toolkit* align with the *Australian Government Authentication Framework* (AGAF) in seeking to determine an appropriate overall assurance level for services.

In most cases, agencies will undertake two processes to ensure an applicant meets the required level of assurance to utilise their service – initial registration and subsequent verification. In assessing these aspects, an agency must ensure that the level of registration assurance and the level of verification assurance are equal to or higher that the required level of access assurance.

On this basis, the Toolkit involves establishing the level of risk for a service and translating this level across three areas:

1. Access assurance
2. Identity registration assurance
3. Credential assurance (ie subsequent verification)

Part 1 of the Toolkit is intended to be applied by an agency business unit in assessing the business processes to be applied for a particular service. It provides the guidelines for completing each of the 7 steps in establishing the assurance levels.

In addition, Parts 2, 3 and 4 provide specific guidelines to assist agencies in developing the identity registration, credential issuing, and ongoing access management business processes for services offered by government agencies.

Part 2

Identity registration guidelines and standards

The *Identity Registration Guidelines and Standards* (this section) forms part of the *Tasmanian Government Identity and Access Management Toolkit* and provides minimum policies, guidelines and standards for agencies to follow in the implementation of identity and access management practices.

The guidelines and standards detailed in Part 2 have been based upon the Gold Standard Enrolment Framework (GSEF), which is part of the National Identity Security Strategy. The GSEF sets the best practice standards for the enrolment of individuals for the purpose of issuing high-integrity government documents or credentials that may function as key documents for proof of identity purposes.

Using the GSEF, guidelines have been developed for the five identity registration assurance levels. The processes to be applied to registering or enrolling an identity are risk-based. Therefore, the level of confidence required in relation to a particular service will be reflected in the identity registration process.

Part 2 incorporates three standards that will be applied in conjunction with one another to determine the form of evidence to be provided by an applicant for a specific government service.

These standards are:

Identity Registration Standard	Designates the points value associated with each of the five identity risk levels and the equivalent number and type (in terms of their objective value, as designated in Standard 2) of the identity documents or credentials required to be provided by a registering person
Proof of Identity Document Standard	Designates the accepted documents or credentials that a registering person is required to provide to meet six proof of identity objectives
Proof of Identity Document Points Standard	Details accepted identity documents or credentials and the equivalent points value allocated to them

Part 3

Credential management guidelines and standards

This Part provides guidelines to assist agencies in selecting the best form of credential that is fit for purpose and matches the level of risk associated with the service and the intended use of that credential.

A credential might take different forms, depending on the nature of the service and the need for registered users of that service to provide evidence of that registration. Examples of credentials issued by the Tasmanian Government include plastic cards (eg a driver licence, Seniors Card), a paper document (eg registration certificate, birth certificate), vehicle stickers (eg an endorsed registration sticker showing a receipt number), or a certificate of competency (eg education certificate, business affairs certificate).

Similarly to identity enrolment or registration, the processes to be applied to the issuing and management of credentials, is risk-based.

Similarly to Part 2, Part 3 provides guidelines for each credential assurance level, together with standards in relation to both electronic and non-electronic credentials.

Part 4

Access management guidelines

After determining the relevant Access Assurance Level, Identity Registration Assessment Level and Credential Management Level for a particular service, the final stage is to determine ongoing access management practices to be applied.

Part 4 provides guidelines to assist agencies in this regard. As with Parts 2 and 3, Part 4 provides separate guidelines for each of the five access assurance levels (ie levels zero to 4).