Tasmanian Government

Identity and Access Management Toolkit

Part 4

Identity Access Management Guidelines

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

ISBN:
978 0 7246 5580 8: Tasmanian Government Identity and Access Management Toolkit – PDF
978 0 7246 5586 7: Tasmanian Government Identity and Access Management Toolkit – HTML

Contents

Using the Access Assurance Level 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). These levels relate to the Access Assurance Level, which was determined at Step 2 of Part 1 of the Toolkit.

Access Assurance Level 4

Suitable for:

The following processes are relevant for any information assets assessed as Access Assurance Level 4 in Part 1 of the Identity and Access Management Toolkit.

1. Create Access Policy

- Each service provided by an agency will have a business owner
- Access policies for a service are set by the business owner
- The policy will stipulate the conditions of client access to information which may include a combination of:
  - Identity Registration Assurance Level 4
  - Credential Assurance Level 4
  - Client role, as identified in the client information store
  - Membership of a part of the agency, as identified in the client information store
  - Other specific rules based on the attributes of a client recorded in the client information store (eg clearance level)
  - Other specific rules based on things like time of day, location
- Access policies will need to take into account multiple layers of access control including:
  - Coarse grain control at the authentication layer checking credentials
  - Medium grain control at the authorisation layer such a role and group membership
  - Fine grain control within a business application relating to data fields

2. Apply Access Policy

- A client may have multiple roles or ways they interact with an agency. Agencies should assign / un-assign roles to clients as they enrol or change their enrolment with the agency
- Map privileges to roles. A role may require more than one technical privilege to be set up. By grouping multiple privileges under one role can make the implementation and reporting on access policy much simpler

3. Report on Access Policy

- It may not be possible or practical to implement very fine grain access control. At Access Assurance Level (AAL) 4, risks can be mitigated by maintaining and reviewing audit logs
- The business owner will regularly review audit logs to identify possible breaches of access policy
- The business owners will be responsible for the regular review of client access and adding and removing clients as required (it is not appropriate at this level to leave this task to internal IT teams)
- At AAL-4, it may be appropriate to monitor access attempts as a proactive method of maintain security

4. Change Access Policy

- The business owner will monitor access usage patterns and identify changes that may trigger the need for a review of access policy
- The business owner will review and change policy as business issues and needs are identified
- The business owner will ensure any change to access policy is accurately reflected in a change to the roles and mapping of privileges, as appropriate
- The business owner will ensure any changed access policy triggers a recalculation of clients and their mapping to roles. This will ensure that new access is given and old access is removed

Access Assurance Level 3

Suitable for:

The following processes are relevant for any information assets assessed as Access Assurance Level 3 in Part 1 of the Identity and Access Management Toolkit.

1. Create Access Policy

- Each information asset will have a business owner
- Access policies for an information asset are set by the business owner
- The policy will stipulate the conditions of client access to information which may include a combination of:
  - Identity Registration Assurance Level 3
  - Credential Assurance Level 3
  - Client role as identified in the client information store
  - Membership of a part of the agency as identified in the client information store
  - Other specific rules based on the attributes of a client recorded in the client information store (eg clearance level)
  - Other specific rules based things like time of day, location
- Access policies will need to take into account multiple layers of access control including:
  - Coarse grain control at the authentication layer checking credentials
  - Medium grain control at the authorisation layer such a role and group membership
  - Fine grain control within a business application relating to data fields

2. Apply Access Policy

- A client may have multiple roles or ways they interact with an agency. Agencies should assign / un-assign roles to clients as they enrol or change their enrolment with the agency
- Map privileges to roles. A role may require more than one technical privilege to be set up. By grouping multiple privileges under one role can make the implementation and reporting on access policy much simpler

3. Report on Access Policy

- It may not be possible or practical to implement very fine grain access control. At Access Assurance Level (AAL) 3, risks can be mitigated by maintaining and reviewing audit logs
- The business owners will regularly review audit logs to identify possible breaches of access policy
- The business owner will be responsible for the regular review of client access and adding and removing clients as required (it is not appropriate at this level to leave this task to internal IT teams)
- At AAL-3 it may be appropriate to monitor access attempts as a proactive method of maintain security

4. Change Access Policy

- The business owner will monitor access usage patterns and identify changes that may trigger the need for a review of access policy
- The business owner will review and change policy as business issues and needs are identified
- The business owner will ensure any change to access policy is accurately reflected in a change the roles and the mapping of privileges as appropriate
- The business owner will ensure any changed access policy triggers a recalculation of clients and their mapping to roles. This will ensure that new access is given and old access is removed

Access Assurance Level 2

Suitable for:

The following processes are relevant for any information assets assessed as Access Assurance Level 2 in Part 1 of the Identity and Access Management Toolkit.

1. Create Access Policy

- Each information asset will have a business owner
- Access policies for an information asset are set by the business owner
- The policy will stipulate the conditions of client access to information which may include a combination of:
  - Identity Registration Assurance Level 2
  - Credential Assurance Level 2
  - Client role as identified in the client information store
  - Membership of a part of the agency as identified in the client information store
  - Other specific rules based on the attributes of a client recorded in the client information store (eg clearance level)
  - Other specific rules based things like time of day, location
- Access policies will need to take into account multiple layers of access control including:
  - Coarse grain control at the authentication layer checking credentials
  - Medium grain control at the authorisation layer such a role and group membership
  - Fine grain control within a business application relating to data fields

2. Apply Access Policy

- A client may have multiple roles or ways they interact with an agency. Agencies should assign / un-assign roles to clients as they enrol or change their enrolment with the agency
- Map privileges to roles. A role may require more than one technical privilege to be set up. By grouping multiple privileges under one role can make the implementation and reporting on access policy much simpler

3. Report on Access Policy

- It may not be possible or practical to implement very fine grain access control. At Access Assurance Level (AAL) 2, risks can be mitigated by maintaining and reviewing audit logs
- The business owner will regularly review audit logs to identify possible breaches of access policy
- The business owner will be responsible for the regular review of client access and adding and removing clients as required (it is not appropriate at this level to leave this task to internal IT teams)
- At AAL-2 it may be appropriate to monitor access attempts as a proactive method of maintain security

4. Change Access Policy

- The business owners will monitor access usage patterns and identify changes that may trigger the need for a review of access policy
- The business owner will review and change policy as business issues and needs are identified
- The business owner will ensure any change to access policy is accurately reflected in a change the roles and the mapping of privileges as appropriate
- The business owner will ensure any changed access policy triggers a recalculation of clients and their mapping to roles. This will ensure that new access is given and old access is removed

Access Assurance Level 1

Suitable for:

The following processes are relevant for any information assets assessed as Access Assurance Level 1 in Part 1 of the Identity and Access Management Toolkit.

1. Create Access Policy

- Each information asset will have a business owner
- Access policies for an information asset are set by the business owner
- The policy will stipulate the conditions of client access to information which may include a combination of:
  - Identity Registration Assurance Level 1
  - Credential Assurance Level 1
  - Client role as identified in the client information store
  - Membership of a part of the agency as identified in the client information store
  - Other specific rules based on the attributes of a client recorded in the client information store (eg clearance level)
  - Other specific rules based things like time of day, location
- Access policies will need to take into account multiple layers of access control including:
  - Coarse grain control at the authentication layer checking credentials
  - Medium grain control at the authorisation layer such a role and group membership
  - Fine grain control within a business application relating to data fields

2. Apply Access Policy

- A client may have multiple roles or ways they interact with an agency. Agencies should assign / un-assign roles to clients as they enrol or change their enrolment with the agency
- Map privileges to roles. A role may require more than one technical privilege to be set up. By grouping multiple privileges under one role can make the implementation and reporting on access policy much simpler

3. Report on Access Policy

- It may not be possible or practical to implement very fine grain access control. At Access Assurance Level (AAL) 1, risks can be mitigated by maintaining and reviewing audit logs
- The business owner will regularly review audit logs to identify possible breaches of access policy
- The business owner will be responsible for the regular review of client access and adding and removing clients as required (it is not appropriate at this level to leave this task to internal IT teams)
- At AAL-1 it may be appropriate to monitor access attempts as a proactive method of maintain security

4. Change Access Policy

- The business owner will monitor access usage patterns and identify changes that may trigger the need for a review of access policy
- The business owner will review and change policy as business issues and needs are identified
- The business owner will ensure any change to access policy is accurately reflected in a change the roles and the mapping of privileges as appropriate
- The business owner will ensure any changed access policy triggers a recalculation of clients and their mapping to roles. This will ensure that new access is given and old access is removed

Access Assurance Level 0

Suitable for:

The following processes are relevant for any information assets assessed as Access Assurance Level 0 in Part 1 of the Identity and Access Management Toolkit.

1. Create Access Policy

- Each information asset will have a business owner
- As Access Assurance Level (AAL) 0 requires no access policy the business owner will only be concerned with the accuracy and availability of the service being delivered

2. Apply Access Policy

- At AAL-0, there are no access policies to apply

3. Report on Access Policy

- At AAL-0, there are no access policies to report on. The business owner may be interested in report on usage rates and availability of the service.

4. Change Access Policy

- At AAL-0, there are no access policies to change