Citizen Identity Management

Policy

> Where identity credentials are required for external users of Victorian Government online services, agencies will provide use of the Victorian Government federated identity infrastructure as an option for sign-on.

Keywords:	Citizen, IDAM, identity, NeAF.		
Identifier: IDAM POL 02	**Version no.:** 1.0		**Status:** Final
Issue date: 1 January 2014	**Date of effect:** 1 January 2014		**Next review date:** 1 January 2015
Authority: Victorian Government CIO Council		**Issuing authority:** Victorian Government Chief Technology Advocate	

DEPARTMENT OF
PREMIER AND CABINET

State Government
Victoria

Overview

Policy context

Trust between government and users is a key foundation for online service delivery. For users to have access to government services through web and mobile media, they must be able to confirm their identity online as required.

For this reason, the enabling of citizen identity and access management was identified as a priority in the 2013 *Victorian Government ICT Strategy*. This policy aims to simplify user engagement with Victorian Government online services by enabling the use of a simplified sign-on when accessing services across multiple agencies.

Policy statement

Where identity credentials are required for external users of Victorian Government online services, agencies will provide use of the Victorian Government federated identity service as an option for sign-on.

Rationale

The identity management framework will enable the delivery of Victorian Government services to users across multiple agencies using a simplified sign-on (SSO). This will be based on federated identity services where agencies accept the registration (including identification) completed by, and authentication mechanism issued by, other organisations including the Australian Government *Reliance Framework* and approved *Third Party Identity Services Assurance Framework*, including social media web sites.

Scope

All agencies with existing or planned citizen online service delivery requiring user identification.

Requirements

Service requirements

The federated identity service must comply with:

- Victorian Government security standards including *SEC POL 01 Information Security Management Policy* which requires compliance with the Australian Government *Protective Security Policy Framework* (PSPF), *Information Security Manual* (ISM) and *National eAuthentication Framework* (NeAF),
- VG IDAM standards (*IDAM STD 01 Identity and Access Management*, *IDAM STD 02-2 Strength of Registration for Citizens and Organisations* and *IDAM STD 03 Strength of Authentication Mechanism*),
- the VG *Information Privacy Act (2000)* and *Health Records Act (2001)*
- appropriate identity management frameworks and agreements for facilities integrated into the federated identity service including the national Document Verification Service, the Australian Government *Reliance Framework* and *Third Party Identity Services Assurance Framework*, etc.,

Agency requirements

Victorian Government agencies will:

- consider use of the federated identity service and its associated SSO / identity as the first preference for any new online services they may be considering, once the federated identity service and SSO service is available,
- comply with *IDAM STD 01 Identity and Access Management* – i.e. all services delivered through the federated identity service must have their Authentication Assurance Level (AAL) assessed in accordance with NeAF. This will determine the strength of registration and the strength of authentication mechanism required for the agency service.
- use a registration level, and an authentication mechanism, as provided through the federated identity service, which meet the requirements of the AAL derived above,

For any services delivered through the federated identity service which only require pseudonymous access i.e. a sign-on, but no identification of the user, agencies should use an email address for the user ID together with a password (see NeAF Level 1, *IDAM STD 03 Strength of Authentication Mechanism.*) Alternatively, agencies may choose to accept approved social media credentials, provided the service is not a high availability service.

For services delivered through the federated identity service which require the real identity of the user to be known and verified, the strength of registration must meet the requirements specified in *IDAM STD 02-2 Strength of Registration for Citizens and Organisations.* In particular:

- The minimum registration requirement for identified users is NeAF Level 2 (Low.)
- For any service involving PROTECTED information, the registration requirement is NeAF Level 3 (Moderate.)

Compliance

Timing

This policy will come into effect upon the date noted. Agencies should incorporate this policy requirement into their planning timelines.

References

VG IDAM policies, standards and guidelines:

- https://www.vic.gov.au/identity-and-access-management-policies-and-standards

VG Security standard(s):

- https://www.vic.gov.au/digital-strategy-transformation

NeAF:

- http://agimo.gov.au/policy-guides-procurement/authentication-and-identity-management/national-e-authentication-framework/

Reliance Framework

- http://www.finance.gov.au/publications/reliance-framework/

- https://my.gov.au/

Further information

For further information regarding this Policy, please contact [digital.transformation@dpc.vic.gov.au.](mailto:digital.transformation@dpc.vic.gov.au)

Glossary

Term	Meaning
AAL	Authentication Assurance Levels as defined in the National eAuthentication Framework
Federated identity infrastructure	Identity infrastructure which allows linking a person's identity and attributes, across multiple distinct identity management systems. This includes agencies accepting the registration (including identification) completed by, and authentication mechanism issued by, other organisations including those issued under the Australian Government *Reliance Framework* and *Third Party Identity Services Assurance Framework*, and by social media web sites.
ICT	Information and communications technology
IDAM	Identity and access management
Identification	The process whereby data (evidence of identity) is associated with a particular user. It occurs through acquiring data that identifies that user.
NeAF	National eAuthentication Framework
Registration	The processes associated with the initial unique identity record and allocation of credentials to a user. Registration encompasses identification processes.
Simplified Sign-on (SSO)	The use of a simplified or single set of authentication credentials across multiple systems or organisations
VG	Victorian Government

Version history

Version	Date	Details
0.1	9 July 2013	Initial draft
0.2	17 July 2013	Minor updates to draft
0.3	27 July 2013	Updates based on feedback received.
0.4	4 August 2013	Updates based on feedback received.
0.5	7 October 2013	Updates to reflect a federated identity model.
1.0	30 November 2013	Submission to CIO Council