Strength of Registration – Citizens and Organisations

Identity and Access Management

Standard

Departments and agencies must meet the requirements in this standard when registering Victorian Government citizens and organisations for access to Victorian Government networks and information systems.

Keywords:	Evidence of identity; EOI; user authentication; IDAM.	
Identifier: IDAM STD 02-2	**Version no.:** 1.1	**Status:** Final
Issue date: 30 November 2013	**Date of effect:** 1 January 2014	**Next review date:** 1 July 2017
Authority: Victorian Government CIO Leadership Group	**Issuer:** Enterprise Solutions, Department of Premier and Cabinet, Victorian Government	

Exemptions – Any exemptions to this standard must be reported to departmental / agency governance bodies.

Overview

The National e-Authentication Framework (NeAF) has been developed as a national framework, addressing the needs of Commonwealth, State, Territory and local government departments and agencies (referred to collectively as 'agencies' hereafter) and is managed by the Australian Government Digital Transformation Office (http://DTO.gov.au/).

The scope of NeAF covers two aspects of authentication:

- electronic authentication of the identity of individuals and businesses; and
- authentication of government websites.

Central to the framework is the concept of assurance levels. An assurance level is determined through a comprehensive risk assessment process to determine the severity of the impact of getting e-authentication wrong. The focus is on answering the question: *Do we have the correct party at the other end of the line – i.e. are they who they purport to be?*

To determine an agency's assurance level and authentication requirements, the NeAF provides:

- A standardised set of (five) e-authentication assurance levels and a recommended set of criteria for determining the level of assurance required for a particular e-transaction.
- A standardised approach to determining the e-authentication solution required to satisfy the e-authentication assurance level, including registration approaches, and e-authentication mechanism.

Requirements

Each agency will ensure that, as part of the registration process and ongoing management of a user being granted access to a Victorian Government (VG) network and/or information system, appropriate evidence of identity (EoI) and, where applicable, evidence of relationship (EoR) is presented to a registration authority, and validated and verified as required, and recorded in accordance with the following minimum documentation.

Unless a risk assessment determines otherwise, agencies are required to select authentication mechanisms (i.e. credentials and processes for the management of credentials) which are consistent with the levels of strength specified in this standard.

Note that a document may only be presented once to satisfy a single category i.e. the same document cannot be used to satisfy multiple categories.

Individual Identification (e.g. Customers, Consumers, Citizens)

NeAF determines the Authentication Assurance Level (AAL) required for the network or system being accessed by the user (refer to IDAM STD 01 and GUIDE 01 for guidance on how to assess this). The minimum registration requirements for each AAL are outlined in the table below.

Authentication Assurance Level:	**None Level 0**	**Minimal AA Level 1**	**Low AA Level 2**	**Moderate AA Level 3**	**High AA Level 4**
Identity:	None	Identity Asserted (Pseudonym acceptable)	Identity Tested (Real Identity)	Identity Verified (Real Identity)	Identity Vetted (Real Identity)
Validated?	No	No	Yes	Yes	Yes
Verified?	No	No	No	Yes	Yes

Strength of Registration:	None	None	Known Customer, Threat/ Risk, or General (new customers)	General	High Assurance

Known Customer (AAL2)

Departments or agencies may already have existing clients or customers that they have previously performed an EoI check on, either as an individual or an organisation. This is referred to as 'known customer' EoI. In this instance, the agency should evaluate the currency and adequacy of its EoI information in deciding whether to use it as a basis for identifying its customers. If considered current and adequate, then the identity provided in the past can be accepted, and no further EoI is required.

However, new customers must comply with the General EoI requirements specified below.

Threat/ Risk (AAL2)

In some cases, departments or agencies may rely on identification performed by a third party organisation, provided a threat and risk assessment has been performed on the currency and adequacy of the third party's EoI processes and documentation. This is referred to 'threat/ risk' EoI. If the assessment determines that the risks of using this approach are acceptable, then the department or agency can rely on the third party's EoI rather than performing its own EoI.

Examples could include EoI completed by Australia Post on behalf of the agency, or EoI completed by an authorised representative of an organisation (see under *Access by Organisations* below.)

General EoI (New AAL2 Customers, and AAL3)

General EoI involves a formal identity verification process that complies with presentation, validation and face-to-face verification of one of the following specified EoI documentation options, together with EoR for users that are not direct employees (i.e. are representing an organisation such as contractors, third party consultants, etc.). Where representing an organisation, evidence of identity of the organisation is also required (see *Access by Organisations* below.)

The categories of documents included in the options below refer to the categories described in Attachment 1.

1. **Option one:**
   - one Category A document establishing evidence of commencement of identity in Australia; and
   - one Category B document establishing a linkage between identity and person (photo and signature);

2**. Option two:**
   - two Category B documents establishing a linkage between identity and person (photo and signature); and
   - one Category C document establishing the operation of that identity in the community.

3. **Option three:**
   - present identification documentation that would satisfy a Victoria Police Check to a registration authority.

For all options, a registration authority must validate the identity by

- ensuring the applicant's name is on every document (where the EoI documents bear a different name then the linkage between that EOI document, the name to be enrolled and the applicant must be clearly established),
- the applicant's address is on at least one of the documents,
- the applicant's date of birth is on at least one of the documents,

- the applicant's signature is on at least one of the documents, and a signature verification check confirms the applicant's signature, and
- a recognisable photograph of the applicant is on at least one of the documents, and the photo bears a reasonable resemblance to the user.

High Assurance Strength of Registration (AAL4)

High Assurance strength of registration involves the same formal identity verification process as for General EoI, but requires one additional document from one of the following document options (see categories described in Attachment 1.)

1. Option one:

- one Category A document establishing evidence of commencement of identity in Australia; and
- one Category B document establishing a linkage between Identity and Person (photo and signature); and
- one Category C document establishing the operation of that identity in the community

2. Option two:

- one Category A document establishing evidence of commencement of identity in Australia; and
- two Category B document establishing a linkage between Identity and Person (photo and signature).

For all options, a registration authority must validate the identity by:

- ensuring the applicant's name is on every document (where the EoI documents bear a different name then the linkage between that EoI document, the name to be enrolled and the applicant must be clearly established),
- the applicant's address is on at least one of the documents,
- the applicant's date of birth is on at least one of the documents,
- the applicant's signature is on at least one of the documents, and a signature verification check confirms the applicant's signature, and
- a recognisable photograph of the applicant is on at least one of the documents, and the photo bears a reasonable resemblance to the user.

Vetting and Authorisation

In many cases, identity is not the only assertion that needs to be authenticated.

Other assertions may require

- vetting of the user e.g. a Police Check, Working With Children Check, or even a security clearance if access is being granted to information classified PROTECTED or higher, and
- checking the person's authorisation to access the information i.e. approval by the system/ application owner or other relevant authority.

Agencies should check VG policies and legislative and regulatory requirements for vetting, and comply with these requirements as part of the identification process.

Evidence of Relationship (EoR)

If a user is representing an organisation, the person must fulfil the appropriate EoI (as specified in the table above) and show EoR. EoR will show a linkage between the person and the organisation they are representing.

This is required in the form of an authorisation signed/issued by an owner, chief executive or other officer or employee with clear capacity to commit the organisation. The EoR document can be in the form of a letter on the organisation's letterhead, or an email displaying the organisation's logo from an email address within the organisation's domain name, or other suitable document.

Where required, the EoR document must authorise the person to act on the organisation's behalf and agree to appropriate terms and conditions e.g. in the case of a person who is authorised to register other persons in the organisation for access to VG systems (see below.)

The EoR must be independently verified. For example, the organisation's telephone number can be sourced from the White or Yellow pages, the number can be called, and the person with clear capacity to commit can asked to confirm the EoR provided, and where appropriate, confirm the representative's authority to act on the organisation's behalf.

Organisational Identification

In some cases agencies need to register organisations. For example, these could be downstream non-government organisations that deliver services on behalf of a department or agency on a funded basis, or it could be an upstream supplier of products and services to government, etc.

This may also involve registering an authorised representative of that organisation, who may in turn be responsible for registering other staff from within the organisation. Identification of authorised representatives should be completed using the High Assurance strength of registration described above, as this is a position of trust. Identification of other employees within the organisation will be determined by the AAL, as shown in the table above.

The standard below deals with registration of the organisation itself. Each agency will ensure that, as part of the registration and ongoing management of an organisation which is granted access to government systems, appropriate EoI of the organisation will be collected, validated, verified, and recorded in accordance with the following minimum documentation requirements:

The Organisation identity documentation must comprise:	Additional validation/ verification
• an original or certified copy of the notice issued by the Registrar of the Australian Business Register (ABR) bearing the business entity's name and the Australian Business Number (ABN).	An online verification with the ABR to link the organisation's ABN to its business name must be completed.

The Organisation identity documentation must comprise:	Additional validation/ verification
OR where a notice issued by the ABR cannot be provided: • a statement of transactions issued by a financial institution in the name of the organisation, which is less than one year old, • a signed contract for the purchase of the organisation, • a lease agreement for property bearing the organisation's name, • a rates notice for property bearing the organisation's name, • an original or certified copy of the Articles of Incorporation or Articles of Association, • an original or certified copy of a Partnership Agreement, • an original or certified copy of a Deed of Trust specifying the Trustees of a Trust, or the appointment of a Trustee, • Articles of Association of an unincorporated association, • a certified extract of the Chief Executive Instructions specifying the position and delegation of a public servant, • a document issued by the ATO (Australian Taxation Office) bearing the organisation name and tax file number.	Other relevant online or telephone checks must be completed to confirm the identity of the organisation e.g. ABR (Australian Business Registration) search, ASIC (Australian Securities and Investment Commission) search; search of Dun & Bradstreet Online Directory, telephone verification etc.

Provisioning requirements

New User (not Known Customer)

New users are required to present the originals and certified copies of EoI and EoR (if required) identification documentation (with the exception of copies of credit cards), in person, to a registration authority that can verify that the documentation being sighted is for the user that was intended to be hired.

To determine the appropriate strength of EoI, the registration authority must determine what information systems the user needs access to. The registration authority must then determine the AAL for each of the information systems. The required strength of EoI should match the highest AAL of the information systems to be accessed.

After the registration authority has made a decision on the required strength of EoI, they must complete it, as described above.

A user is required to supply on request the following key identifying information attributes for recording in agency registration systems to ensure accurate identity matching and user account uniqueness:

- First Name
- Last Name
- Date of Birth
- Gender

The certified copies of documents and outcome of the EoI check is to be recorded against the user record with the following information elements recorded:

1. strength of registration achieved (Known Customer, Threat/ Risk, General, High Assurance)
2. registration authority's name that sighted the EoI/EoR documentation; and
3. date the documentation was sighted.

Existing User

If an existing user with access granted at a lower AAL needs access to information systems that require a higher AAL, the user must present, in person, all documentation (originals and certified

copies, with the exception of copies of credit cards) that is required to satisfy the higher AAL's strength of EoI requirements to a registration authority.

The certified copies and the new EoI and AAL achieved is to be formally recorded along with the name of the registration authority and date of registration.

Rationale

The requirement to record for each user the strength of EoI that has been satisfied, the name of the registration authority and date of registration is essential to

- ensure traceable accountability of authorised access, and
- build a 'trusted' identity and access management system where credentials can be reused/shared across VG departments and agencies (e.g. single sign-on or centralised government portal).

The Australian Government's EoI processes including the Attorney General's *National Identity Security Strategy* (NISS) have been adopted as they are relatively simple, already codified and widely agreed and adopted. To propose an alternative EoI would be impractical and increase the complexity of sharing of information between jurisdictions and with the Commonwealth.

The adoption of this standard will

- enable a common trusted framework for the sharing of credentials and information,
- engender a high degree of confidence that users who access VG information are who they say they are,
- provide an auditable, traceable record of EoI due diligence and decision-making,
- align with the Commonwealth *National Identity Security Strategy – Proof of Identity* framework, and
- align with the NeAF (refer IDAM STD 01) and associated strength of registration requirements.

Scope

The use and adaptation of Victorian Government (VG) ICT policies, standards, guidelines and other supporting material is open to all, under the appropriate Creative Commons license of the document in question.

Use of VG ICT policies and standards is mandated to:

All departments

- Department of Economic Development, Jobs, Transport and Resources
- Department of Education and Training
- Department of Environment, Land, Water and Planning
- Department of Health and Human Services
- Department of Justice and Regulation
- Department of Premier and Cabinet
- Department of Treasury and Finance

Agencies

- Ambulance Victoria
- CenITex
- Country Fire Authority
- Court Services Victoria
- Emergency Services Telecommunications Authority
- Environment Protection Authority
- Metropolitan Fire and Emergency Services Board
- Public Transport Victoria
- State Revenue Office
- Victoria Police
- VicRoads
- Victoria State Emergency Service

Where applicable, legal and or regulatory compliance obligations take precedence over this policy and related standards. Departments and agencies may have additional legal and or regulatory information protection compliance requirements. Examples include (but are not limited to) Victoria Police and the Commissioner for Law Enforcement Data Security (CLEDS), credit card processing contract obligations of the Payment Card Industry Data Security Standard (PCI DSS) and the Information Privacy Act 2000.

This standard applies to external users of VG systems including consumers, citizens, customers, and (where relevant) the organisations they are associated with.

This standard is the minimum requirement. Agencies may, at their discretion, apply more rigorous EoI processes and apply them retrospectively.

Compliance and reporting requirements

Completion and submission of the IDAM items in the ISMF self-assessment report, as required by SEC STD 01 *Information Security Management Framework*, reporting cycle.

References

VG Information Security Policy and standards:

http://www.enterprisesolutions.vic.gov.au/business-systems/information-security/

VG IDAM Policy and Standards
http://www.enterprisesolutions.vic.gov.au/business-systems/identity-and-access-management/

Australian Commonwealth Government initiatives, including:

Protective Security Policy Framework (PSPF), 2012

- Australian Government Attorney General's Office
- http://www.protectivesecurity.gov.au/Pages/default.aspx

National Identity Security Strategy (NISS), April 2007 and updated in 2012:

- Australian Government Attorney General's Office
- http://www.ag.gov.au/rightsandprotections/identitysecurity/pages/nationalidentitysecuritystrategy.aspx

National e-Authentication Framework (NeAF), January 2009

- Australian Government Digital Transformation Office
- http://www.finance.gov.au/policy-guides-procurement/authentication-and-identity-management/national-e-authentication-framework/

Gatekeeper Public Key Infrastructure Framework, December 2015

- Australian Government Digital Transformation Office
- https://www.dto.gov.au/standard/design-guides/authentication-frameworks/gatekeeper-public-key-infrastructure-framework/

National Identity Proofing Guidelines, 2014

- Australian Government Digital Transformation Office
- https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/NationalIdentityProofingGuidelines.pdf

Australian Government Identity Security Guidelines and Standards

- https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/default.aspx

Further information

For further information regarding this standard, please contact the Department of Premier and Cabinet, at enterprisesolutions@dpc.vic.gov.au

Glossary of terms and abbreviations

Term	Meaning
AAL	Authentication Assurance Level – a level of assurance set by the Australian Government National e-Authentication Framework (NeAF.)
Access management	The capability and processes that permit or deny access to systems, thus controlling the ability to read, modify or remove information.
Authentication	The process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access (Authorisation) to resources in an information system, and often via a credential.
Authorised representative	An authorised representative is a person who is authorised by an organisation to perform the EoI task for other people within the organisation. This authorised person must t complete High Assurance strength of registration, and EoR, if required, for the registration authority to sight.
Entity	A real-world thing. Categories include objects, animals, artefacts, natural persons, and legal persons (such as corporations, trusts,

Term	Meaning
	superannuation funds, and incorporated associations).
Evidence of identity	A predetermined process whereby an entity establishes the right to use an identity, by presenting appropriate documentation supporting that right.
Identity	A particular presentation of an entity. An identity may correspond to a role played by the entity. An identity may be used by the entity in its dealings with one other entity, or with many other entities. An organisation may maintain an account within its records that corresponds to an identity.
Identification	The process whereby data is associated with a particular user. It occurs through acquiring data that identifies that user.
IDAM	Identity and Access Management.
Identity Management	The policies, rules, processes and systems involved in ensuring that only known, authorised users gain access to systems and information.
Registration authority	A registration authority is one who is authorised by the application owner to perform this EoI task. This registration authority must themselves produce High Assurance strength of registration (and EoR, if required), for the application owner to sight. Typically, the registration authority will be the line manager/supervisor of the EoI applicant.
Remote Access Technologies	VPN Dial-Up; Citrix, external facing websites/portals, etc.
Simplified Sign On (SSO)	SSO is a property of access control of multiple, related, but independent software systems. With this property a user logs in once and gains access to all systems (for which they are authorised), without being prompted to log in again at each of them.
User	Any person who is eligible to access a Victorian Government network and / or Victorian Government information system.
Validation	Validation is the process that checks that the claimed identity exists. It does not provide any assurance that the claimed identity belongs to the claimant.
Verification	Verification is the process of checking that the claimant is the individual to which the claimed identity belongs e.g. photograph and signature comparison
Victorian network	A Victorian Government network is defined as any Victorian Government ICT network infrastructure used to carry electronic information between systems.

Version history

Version	Date	GSD TRIM Ref	Details
0.1	1 March 2013	n/a	Initial draft
0.2	22 April 20`13		Updated with feedback from ISAG
0.3	July 2013		Updated feedback from ISAG working group
0.4	Sept 2013		Updated feedback from ISAG members
0.5	26 November 2013		Final updates, review links and dates.
1.0	30 November 2013		Submission to CIO Council
1.1	7 July 2016		Reviewed – no substantive changes. Update to reference links, next review date, and to reflect Machinery of Government changes.

Attachment 1[1]

Categories	Documents satisfying the categories

A. Evidence of commencement of identity in Australia **(Mandatory)**	• Birth certificates (issued by births deaths and marriages (BDM) authorities within Australia)
	• Australian passport (current)
	• Record of immigration status:
	  o foreign passport and current visa
	  o travel document and current Australian visa
	  o certificate of evidence of residence status
	  o citizenship certificate

B. Linkage between identity and person (photo and signature) **(Mandatory)**	• Australian drivers licence (current and original) • Australian passport (current) • Firearms licence (current and original) • Foreign passport • Current Commonwealth or state public service ID card with photo and signature
C. EoI operating in the community (can be used as another Category A or B document)	• Medicare card • Change of name certificate: non-standard EoI (for marriage or legal name change, showing link with previous name/s) • Credit or account card or bank passbook • Centrelink or Department of Veterans' Affairs card • Security guard/crowd control licence • BDM-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 examination certificate (persons under 16 years of age only) • Certificate of trusteeship • Council rates notices (where name and address match those on the application form) • Letter from employer (current or within last two years) • Telephone directory (verified by telephone call) (where name and address match the application form) • The electoral roll
D. Evidence of residential address (used only to provide evidence of residential address if not provided by a	• Utilities notice (where name and address match the application form) • Rent details (where name and address match the application form) • A bank, building society, credit union, or other financial institution account statement less than one year old (where name and address match the application form) • Council rates notices (where name and address match those on the application

[1] Attachment 1 is an extract from The Report to the Council of Australian Governments on the Elements of the National Identity Security Strategy, April 2007 together with the addition of Australian Passport.

category B or C document)	form) • Title or deed to real estate, or registered mortgage papers on a home or property