Australian Government

Digital Identity

02 Overview

Trusted Digital Identity Framework Release

Release 4 June 2021, version 1.2

PUBLISHED VERSION

Digital Transformation Agency (DTA)

Licence

Use of the Coat of Arms

The terms under which the Commonwealth Coat of Arms can be used are detailed on the It's an Honour website (http://www.itsanhonour.gov.au)

Conventions

References to TDIF documents, abbreviations and key terms (including the words *MUST*, *MUST NOT*, and *MAY)* are denoted in italics are to be interpreted as described in the current published version of the *TDIF: 01 – Glossary of Abbreviations and Terms.*

TDIF requirements and references to *Applicants* are to be read as also meaning *Accredited Provider*, and vice versa. The scope of *TDIF* requirements are to be read as applying to the *Identity System* under *Accreditation* and not to the organisation's broader operating environment.

Contact us

The *DTA* is committed to providing web accessible content wherever possible. This document has undergone an accessibility check however, if you are having difficulties with accessing the document, or have questions or comments regarding the document please email digitalidentity@dta.gov.au.

Document management

The *DTA* has endorsed this document for release.

Change log

Version	Date	Author	Description of the changes
0.1	July 2019	SJP	Initial version
0.2	Oct 2019	SJP	Updated to incorporate feedback provided by stakeholders during the first round of collaboration on TDIF Release 4
0.3	Dec 2019	SJP	Updated to incorporate feedback provided by stakeholders during the second round of collaboration on TDIF Release 4
0.4	Mar 2020	SJP	Updated to incorporate feedback provided during the public consultation round on TDIF Release 4
1.0	May 2020		Published version
1.1	Jul 2020	SJP	Updated references
1.2	Jun 2021	JK, SJP	CRID0009 – minor grammar and style update. Updated references and added requirements subject area description table. CRID0012, CRID0013 – Update to wording to incorporate other TDIF document changes.

Document review

All changes made to the TDIF are published in the TDIF Change Log which is available at https://www.digitalidentity.gov.au/privacy-and-security/trusted-digital-identity-framework.

Contents

Introduction

The *DTA* has been developing the *TDIF* since 2015. The *TDIF* is an *Accreditation* regime which specifies the minimum requirements that *Attribute Service Providers*, *Credential Service Providers*, *Identity Exchanges* and *Identity Service Providers* are required to meet in order to achieve and maintain *TDIF* accreditation. This document provides an overview of the *TDIF* including its scope and objectives.

The intended audience for this document includes:

- *Accredited Providers*.
- *Applicants*.
- *Assessors.*
- *Relying Parties*.

What is identity

A person's identity is not a fixed concept; it is highly dependent on context. Identity is a combination of characteristics or attributes that allow a person to be uniquely distinguished from others in a specific context.

For the purpose of the TDIF, a person's identity in Australia is generally considered to be established at birth with the creation of a birth record that details unique information about the individual, such as name and date and place of birth. For people not born in Australia, their identity in Australia is generally established from personal details recorded on Australian government-issued immigration documents or records.

Australian citizens and permanent residents retain the right, enshrined in Australian privacy legislation, to act anonymously or pseudonymously when interacting with governments or businesses, unless:

- An organisation is required or authorised under Australian law to request identification, or
- It is otherwise impracticable to interact with individuals who have not identified themselves.

What is digital identity

Digital identity is an electronic representation of an entity (person or other entity such as a business) and it allows people and other entities to be recognised online. A person's digital identity is an amalgamation of personal attributes and information in electronic form that can be bound to that physical person. Digital identity provides a means for people to undertake online what they have traditionally done manually. It is seen as a critical enabler for people and business participation in the digital economy and to access government services.

What is a Trust Framework

The Open Identity Exchange[1] describes an identity *Trust Framework* as:

> *A trust framework typically defines the scope and purpose of the Identity System, determines what roles are to be included and what duties are assigned to those roles, sets the eligibility requirements for entities seeking to fulfil those roles, and establishes the rules and regulations for processing of identity information within the context of the Identity System.*

Trust Frameworks are commonly used to govern a variety of multi-party systems where participants want to engage in a common type of transaction with any of the other participants and do so in a consistent and predictable manner. Common examples include credit card systems, electronic payment systems, and the internet domain name registration system, which all rely on a set of interdependent specifications, rules, and agreements. This set of specifications, rules and agreements is referred to by various names, such as 'operating regulations', 'scheme rules,' or 'operating policies.' In the world of *Identity System*s, they are commonly referred to as a '*Trust Framework*.'

[1] Ester Makaay, Tom Smedinghoff, Don Thibeau, June 2017, *Trust Frameworks for Identity Systems*, OIXnet, https://www.oixnet.org/news-whitepaper

Trusted Digital Identity Framework

2.1 Early history

The Australian Government has been exploring the concept of online trust for several years.

In 2010 the Australian Government Department of the Prime Minister and Cabinet (*PMC*) identified a need to strengthen identity management in the digital economy and a voluntary trusted identity model was seen as a possible way to achieve this. The possible model involved the development of a market in identity authentication products which led to the development of the National Trusted Identities Framework (*NTIF*) in 2011. The aim of the framework was to make it simpler for government and business to confirm the identity of individuals they do business with and allow individuals to verify the credentials of the businesses they transact with online using the same system. *PMC* conducted two consultation sessions during 2011 and 2012 on the *NTIF*. Although the sessions identified several issues and questions related to online trust and what might be needed to address it, there was no clear consensus on what next steps should be taken to progress the *NTIF*.

In 2011 the then Department of Broadband, Communications and the Digital Economy published the National Digital Economy Strategy (*NDES*), which outlined the government's vision for Australia's digital economy. The *NDES* aimed to improve online government service delivery and engagement and built on the concepts established in the *NTIF* around online trust.

In 2013 these concepts were explored further, when the Australian Government Information Management Office (*AGIMO*) published the Third Party Identity Services Assurance Framework (*TPISAF*). This framework set out the compliance criteria and accreditation requirements for third party providers of identity services. The underlying premise of the framework is that, based on an understanding of an agency requirements, individuals will be able to choose to use the services of an accredited service provider in order to access online government services.

2.2 Recent history

The Australian Government established the *Financial System Inquiry*[1] (*FSI*) in December 2013 to examine the positioning of the financial system to meet evolving needs and support economic growth for Australia. In December 2014, the *FSI* concluded that:

> "The innovative potential of Australia's financial system and broader economy can be supported by taking action to ensure policy settings facilitate future innovation that benefits consumers, business and government".

To facilitate innovation, the *FSI's* recommendations include the aim to:

> "Strengthen Australia's digital identity framework through the development of a national strategy for a federated-style model of trusted digital identities".

In accepting the recommendations of the *FSI* in October 2015, the Australian Government agreed that a national digital identity strategy would streamline people's interactions with government and provide efficiency improvements. As per Inquiry Recommendation 15 (digital identity), the Government also agreed to:

> "Work across government and with the private sector to develop a Trusted Digital Identity Framework to support the Government's Digital Transformation Agenda".

The *TDIF* builds on previous trust framework development efforts and responds directly to the *FSI* and government commitment. The *TDIF* requires providers of identity-related services to be accredited and establishes the rules for the *Australian Government's identity federation*.

2.3 Objectives

Based on the above principles, the *TDIF* will facilitate the following outcomes:

Simple, easy to use and trusted: A *Digital Identity* that *Individuals* want to use.

1 See *References* for further information on the FSI

Accessible: *Digital Identity* that is accessible to all *Individuals* regardless of their location, circumstances, abilities or the computing devices they use.

Secure and privacy-enhancing: *Digital Identity* is secure and privacy-enhancing to embody fundamental data protection principles by minimising use of personal data, maximising data security and empowering *Individuals*. *Individuals* are given greater control over their *Personal Information* and who their *Personal Information* is shared with. Safeguards and recovery mechanisms are implemented in the event an *Individual's Digital Identity* is compromised.

Interoperability: *Accredited Digital Identity Providers* interoperate with other *Identity Systems* through the use of open standards and *Trust Frameworks*.

2.4 Guiding principles

The *TDIF* supports the following guiding principles:

User centric:

- Accessing digital services must be easy, convenient, simple, secure and trusted.
- *Individuals* can choose to create a *Digital Identity* from a range of accredited government and private sector *Accredited Providers*.
- *Individuals* can use one or more *Identity Service Providers* to maintain separate or merged personal and business *Digital Identities*.

Voluntary and transparent:

- *Individuals* choose to participate or not (i.e. opt-in).
- *Individuals* can control their *Digital Identity* in an easy and straightforward manner.
- Records of *Credential* use are maintained securely by *Accredited Providers* and easily accessible by those authorised to do so under the *TDIF*.

Service delivery focused:

- *Accredited Providers* can offer choice and convenience for *Users* when accessing government or commercial digital services.

- Participation is cost neutral for *Users*.
- The supporting business model encourages private sector participation.

Privacy enhancing:

- *Personal Information* is only collected and disclosed by *Accredited Providers* with the *Express Consent* of *Users* and in accordance with privacy laws and good privacy practices.
- Privacy enhancing technology, policy and processes are applied by *Accredited Providers* to all *Personal Information*.
- *Users* have an informed understanding of how their *Personal Information* will be used and protected.
- *Users* can view and manage their *Personal information*, correct errors and revoke their *Consent.*
- No single identifier is issued by the *Identity Exchange* to *Identity Service Providers*, *Attribute Service Providers* or *Relying Parties*.
- There is no single *Credential* or centralised database of *Personal Information*.

Collaborative:

- Active collaboration between the public and private sectors and the broader community will draw on the respective strengths and expertise of government and business.

Interoperable:

- Facilitate interconnectedness with other *Trust Frameworks* and identity services nationally and internationally.
- Scalable to grow and accommodate the needs of *Accredited Providers* and *Relying Parties*.

Adaptable:

- Promote flexibility and innovation in technology and business models.
- The *TDIF* is flexible to evolve to meet community expectations and changing business, technology, legal and social needs.
- The *TDIF* supports secure information exchanges ranging from low to high value and from pseudonymous to fully verified identity proofing.

Secure and resilient:

- *Accredited Providers* meet stringent government security standards.
- The same *Accreditation* requirements apply to organisations and government agencies.
- Cyber security threats and risks are identified and actively managed by *Accredited Providers* and *Relying Parties*.
- Effective *Fraud* management controls are implemented and maintained.

2.5 Accredited roles

The *TDIF* supports the *Accreditation* of *Attribute Service Providers*, *Credential Service Providers*, *Identity Exchanges* and *Identity Service Providers*.

2.5.1 Attribute Service Providers

Attribute Service Providers generate and manage *Attributes* and claims that are provided to *Relying Parties* to support their decision-making processes.

2.5.2 Credential Service Providers

Credential Service Providers generate, bind and distribute *Credentials* to *Individuals* or can include the binding and management of *Credentials* generated by *Individuals*. This function may also be undertaken by an IdP.

2.5.3 Identity Exchanges

Identity Exchanges conveys, manages and coordinates the flow of identity *Attributes* and assertions between members of an *Identity Federation*.

2.5.4 Identity Service Providers

An *Identity Service Provider* creates, maintains and manages identity *Information* of *Individuals* and offers identity-based services.

2.6 Unaccredited roles

Other roles within an *Identity Federation* (which are not accredited) include *Relying Parties*, *Attribute Verification Services* and *Users*.

2.6.1 Relying Parties

Relying Parties are the organisations that rely on verified *Attributes* or *Assertions* provided by *Identity Service Providers* and *Attribute Service Providers* to enable the provision of a digital service.

2.6.2 Attribute Verification Services

Attribute Verification Services (also known as an *Identity Matching Service*) are repositories recognised by the *DTA* that confirm the veracity of *Attributes* and associated information. *Attribute Verification Services* can refer to either the repositories themselves, or the methods used to access them (e.g. *Document Verification Service* and the *Face Verification Service*).

2.6.3 Users

Users are *Individuals* who establish a *Digital Identity* to obtain digital services from *Relying Parties*. This includes *Individuals* acting in their own capacity and *Individuals* who act on behalf of others.

2.7 Accreditation governance

The *DTA* and the *Accredited Provider* may sign an agreement that sets out their ongoing obligations under the *TDIF*. In time these will be replaced with a set of *Operating Rules.*

2.8 Accreditation process

TDIF Accreditation is a formal process through which *Applicants* demonstrate their ability to meet specific requirements to the satisfaction of the *DTA*. *TDIF Accreditation* covers the initial accreditation and ongoing accreditation obligations.

Initial *Accreditation*: *Accreditation* of an *Applicant's Identity System* is fundamental to its trustworthiness and its functional effectiveness. The *TDIF Accreditation Process* involves a combination of documentation, third party evaluations by *Assessors* and operational testing that *Applicants* must complete to the satisfaction of the *DTA* to achieve *TDIF Accreditation* or vary their accreditation (e.g. *Step-Up*).

Ongoing *Accreditation* obligations: *Accredited Providers* are required to continue to comply with the requirements of the *TDIF* to maintain their *Accreditation*. *Accredited Providers* are required to complete *Annual Assessments* against the *TDIF* by the anniversary of their initial *Accreditation* date and remediate any adverse findings in timeframes agreed with the *DTA*.

2.9 TDIF Accreditation Process roles

2.9.1 Applicant and Accredited *Provider*

The *Applicant* is responsible for:

- Formally requesting *TDIF Accreditation* for its *Identity System* from the *DTA*.
- Preparing all required documentation within timeframes agreed with the *DTA*.
- Obtaining all relevant internal system *Accreditations* or endorsements from the appropriate *Accountable Authority* throughout the *TDIF Accreditation Process.*
- Completing the required *Functional Assessments* by *Assessors*.
- The provision of all relevant *Accreditation* evidence to the *DTA*.
- Remediating all identified non-conformance and adverse findings to the satisfaction of the *DTA*.
- Accepting the residual risk relating to its *Identity System*. (Residual risks may be accepted by appropriate *Accountable Authority*).

- Responding to all requests for information by the *DTA* in relation to *Accreditation* matters.
- As required by the *DTA*, enter into an agreement with the *DTA* following *TDIF Accreditation*.
- Maintain *Accreditation* in accordance with its agreement.
- Undergo *Annual Assessments* on its *Identity System* by the anniversary of its initial *Accreditation* date as set out in *TDIF: 07 – Annual Assessment*.
- Formally advising the DTA of its intention to leave the *TDIF* in the event it:
    - No longer wants to undergo the *TDIF Accreditation Process* or maintain *Accreditation*.
    - Can no longer comply with *TDIF* requirements once accredited.
    - Chooses to no longer maintain its *Accreditation*.

2.9.2 Digital Transformation Agency

The *DTA* is responsible for:

- Performing the roles and functions of the *Oversight Authority* in relation to *TDIF Accreditation*.
- Ensuring that the *TDIF Accreditation Process* is conducted with due care and in accordance with the published *TDIF* documents.
- Reviewing, within agreed timeframes, all relevant *Applicant* and *Accredited Provider* evidence to ensure conformance to the published *TDIF* documents.
- Handling and treating all *Applicant* and *Accredited Provider* evidence consistent with its classification and sensitivity. Unless otherwise agreed between the *Applicant* and the *DTA*, all evidence provided to the *DTA* will be treated as ***OFFICIAL information***. All *DTA Personnel* associated with *Accreditation* activities have an appropriate need-to-know and security clearance level to handle sensitive or classified documents provided to the *DTA* in relation to *TDIF Accreditation*.
- Protecting all information provided to it by an *Applicant* (including their *TDIF Accreditation Letter* and supporting information), and *Accredited Provider* to ensure it is only available to staff directly involved with their *Accreditation*. Any documentation requested by other parties will only be shared with the express permission of the *Applicant* or *Accredited Provider*.

    - As required, DTA staff directly involved with *TDIF* accreditation will sign a Non-Disclosure Agreement.
- Considering all reports and recommendations from *Assessors*.
- Interpreting conformance against *TDIF* requirements.
- All decisions in relation to the initial *Accreditation* of an *Applicant* or ongoing accreditation of an *Accredited Provider*.
- Granting accreditation to an *Applicant*.
- Maintaining the list of *Accredited Providers*[2].
- Maintaining the *TDIF Accreditation Register*.
- Reviewing all documentation which supports an *Accredited Provider's Annual Assessment*.
- Directing *Accredited Providers* to undergo *TDIF Reaccreditation* (as required).
- Revoking the accreditation of an *Accredited Provider*.

2.9.3 Assessors

Assessors are independent evaluators of business processes, documentation, systems and services who have the required skills, experience and qualifications to determine whether an *Applicant* or *Accredited Provider* has met specific *TDIF* requirements.

As part of the *TDIF Accreditation Process*, the *Applicant* is required to undergo a series of *Functional Assessments* by suitably skilled and experienced *Assessors*. *Assessors* are responsible for assessing the *Applicant's* compliance against specific *TDIF* requirements[3] and documenting their findings.

2.10 Documents

The TDIF includes the following documents:

- ***TDIF: 01 - Glossary of Abbreviations and Terms***, which includes a list of acronyms and a definition of key terms used in the *TDIF*.

[2] Available on the TDIF website (https:///www.dta.gov.au)

[3] See *TDIF: 04 - Functional Requirements* for further information.

- ***TDIF: 02 - Overview****,* (this document) which provides a high-level overview of the *TDIF*.
- ***TDIF: 03 - Accreditation Process****,* which sets out the process and requirements an *Applicant* is required to complete to achieve *TDIF* accreditation.
- ***TDIF: 04 - Functional Requirements****,* which includes requirements applicable to the *Accredited Roles*, including fraud control, privacy, protective security, user experience and technical testing. This document also includes a series of *Functional Assessments* to be undertaken by the *Applicant* to achieve *TDIF* accreditation, including a *Privacy Impact Assessment*, *Privacy Assessment*, *Security assessment*, penetration test and an assessment against the *Web Content Accessibility Guidelines*.
- ***TDIF: 04A – Functional Guidance****,* which provides guidance to *Applicants* on meeting the requirements set out in *TDIF: 04 Functional Requirements*.
- ***TDIF: 05 - Role Requirements****,* which includes user terms and lifecycle management requirements applicable to the *Accredited Roles*.
- ***TDIF: 05A – Role Guidance****,* which provides guidance to *Applicants* on meeting requirements set out in *TDIF: 05 Role Requirements*.
- ***TDIF: 06: Federation Onboarding Requirements****,* which includes the requirements to be met when an *Applicant's Identity System* is approved to onboard to the *Australian Government's identity federation*. This document includes functional requirements, technical integration testing requirements, and obligations when reporting to the Oversight Authority[4]. An *Applicant* is not required to meet these requirements unless they are intending to onboard to the *Australian Government's identity federation.*
- ***TDIF: 06A –Federation Onboarding Guidance****,* which provides guidance to *Applicants* on meeting requirements set out in the *TDIF: 06 Federation Onboarding Requirements*.
- ***TDIF: 06B - OpenID Connect 1.0 Profile****,* which describes how OpenID Connect 1.0 is used within the *Australian Government's identity federation*.
- ***TDIF: 06C - SAML 2.0 Profile****,* which describes how *SAML* 2.0 is used within the *Australian Government's identity federation*.

[4] The *Oversight Authority is responsible for administering the Australian Government identity federation, including undertaking fraud and cyber security investigations.*

- ***TDIF: 06D – Attribute Profile***, which describes the *Attributes* used within the *Australian Government's identity federation* and how these are mapped in the OpenID Connect 1.0 Profile and *SAML* 2.0 Profile.
- ***TDIF: 07 - Annual Assessment***, which sets out the process and requirements an *Accredited Provider* is required to complete by the anniversary of their initial accreditation date to remain *TDIF* accredited.

2.11 Requirements schema

The following is an example of a *TDIF* requirement:

TDIF Req: ACCRED-03-01-01; **Updated**: Jun-21; **Applicability**: A, C, I, X
The *Applicant* *MUST* formally request *TDIF* accreditation with a *TDIF Application Letter*.

Each *TDIF* requirement includes the following information.

- ***TDIF* Req**: The unique identifier for each *TDIF* requirement.
  Each *TDIF* requirement uses the following schema
  [*Subject Area -Document Section – Requirement -Sub Requirement].*
  - *Subject Area:* A shorthand of the subject area. See Section 2.12 for a list of these.
  - *Document Section:* Denoted by the four left-hand digits in the schema. For example, the '03-04' in PRIV-03-04-01a means section 3.4 of the privacy requirements (set out in *TDIF: 04 - Functional Requirements)*.
  - *Requirement:* Denoted by the two right-hand digits in the schema. For example, the '01' in PRIV-03-04-01a means requirement 01 in section 3.4 of the privacy requirements.
  - *Sub-Requirement:* Denoted by a unique letter at the right-hand side of the schema. For example, the 'a' in PRIV-03-04-01a means the first sub-requirement linked to requirement 01 in section 3.4 of the privacy requirements.
- **Updated**: The month/year the requirement was last updated.
- **Applicability**: The *Accredited Role* to whom the requirement applies. The roles include:

- *Attribute Service Providers*, denoted by an ‘A’
- *Credential Service Providers*, denoted by a ‘C’
- *Identity Service Providers*, denoted by an ‘I’
- *Identity Exchanges* denoted by an ‘X’.

- **Requirement text**: The requirement to be met.

2.12 Subject area description

The following table sets out the shorthand descriptions for the TDIF requirements subject areas.

TDIF Document	Section	Shorthand
03 Accreditation Process	All Sections	ACCRED
04 Functional Requirements	2 – Fraud control requirements 3 – Privacy Requirements 4 – Protective Security Requirements 5 – User Experience Requirements 6 – Technical Testing Requirements 7 – Functional Assessments	FRAUD PRIV PROT UX TEST ASSESS
05 Role Requirements	2 – Common Role Requirements 3 – Identity Service Provider Requirements 4 – Credential Service Provider Requirements 5 – Attribute Service Provider Requirements 6 – Identity Exchange	ROLE IDP CSP ASP IDX
06 Federation Onboarding Requirements	All Sections	FED
06B OpenID Connect 1.0 Profile	All Sections	OIDC
06C SAML 2.0 Profile	All Sections	SAML
07 Annual Assessment	All Sections	ANNUAL

2.13 What is not covered in the TDIF

The scope of the *TDIF* is limited to the accreditation of *Applicants* and maintenance of *Accredited Provider's* accreditations. There are several items not covered by the *TDIF*, including:

- Cost or fee schedules for the provision of identity services.
- Liability arrangements for *Accredited Providers*.
- Information regarding the *Australian Government's Identity Federation*[5].
- Requirements to be met by *Relying Parties* to join the *Australian Government's Identity Federation*.
- A catalogue of participating services available through the *Australian Government's Identity Federation*.
- Technical details or other information related to the *Australian Government's Identity Federation* test environments.
- Operational functions of the *Australian Government's Identity Federation*.
- Service level agreements.
- Governance arrangements for the *Australian Government's Identity Federation*.

[5] Information about the Australian Government's Digital Identity program is available at https://www.digitalidentity.gov.au/

References

In developing the *TDIF* the following sources have been considered[6].

1. Agarwal N and Bradley J (2015) *Proof Key for Code Exchange by OAuth Public Clients [RFC 7636],* Internet Engineering Task Force, Sakimura N (ed).
2. Anderson M, Fergus N, Gibson C, Kilgour J, Love G, Parsons and Tarrant M (2006) *Security risk management handbook (HB 167:2006)*, Standards Australia and New Zealand, Sydney and Wellington
3. *Archives Act 1983* (Cth)
4. Attorney-General's Department (2011) *Australian Government Investigation Standard* [online document], Australian Government Attorney-General's Department.
5. Attorney-General's Department (2017) *Commonwealth Fraud Control Framework* [online document], Australian Government Attorney-General's Department.
6. Attorney-General's Department (2011) *Improving the integrity of identity data: recording of a name to establish identity – better practice guidelines for Commonwealth Agencies* [PDF], Australian Government Attorney-General's Department.
7. Attorney-General's Department (2016) *National Identity Proofing Guidelines (NIPGs)* [PDF], Australian Government Attorney-General's Department.
8. Attorney-General's Department (2018) *Protective Security Policy Framework* [website], Australian Government Attorney-General's Department.
9. Auditing and Assurance Standards Board (2015) *Auditing Standard ASA 700 – Forming an Opinion and Reporting on a Financial Matter* [PDF], Australian Government Auditing and Assurance Standards Board.
10. Australian Signals Directorate (ASD) (2018) *2018 Australian Government Information Security Manual: Controls (ISM),* Australian Government ASD.
11. Australian Signals Directorate (ASD) (2019) *Essential Eight Explained*, Australian Government ASD.
12. Bartel M, Boyer J, Fox Bm LaMacchia B and Simon E (2013) *XML Signature Syntax and Processing [Version 1.1]* [XMLSig], W3C XML Schema Working Group, World Wide Web Consortium (W3C).
13. Beech D, Thompson H, Maloney M and Mendelsohn N (eds) (2004) XML Schema Part 1: Structures *[Second Edition].* W3C XML Schema Working Group, World Wide Web Consortium (W3C).
14. Biron P V and Malhotra A (eds) (2004) *XML Schema Part 2: Datatypes [Second Edition].* W3C XML Schema Working Group, World Wide Web Consortium (W3C).
15. Biometrics Evaluation and Testing (BEAT) (n.d.) https://www.beat-eu.org/, Idiap Research Institute.
16. Bradley J, Sakimura N, Jones M, de Medeiros B and Mortimore C (2014) *OpenID Connect Core 1.0* [OpenID.Core], The OpenID Foundation.
17. Bradley J, Sakimura N, Jones M and Jay E (2015) *OpenID Connect Discovery 1.0 incorporating errata set 1,* The Open ID Foundation.
18. Bradley J, Sakimura N, Jones M (2014) *OpenID Connect Client Registration 1.0 incorporating errata set 1*, The Open ID Foundation.

[6] Some sources contain hyperlinks.

19. Bradner S (1997) *Key words for use in RFCs to Indicate Requirements Level*, Internet Engineering Task Force.
20. Campbell A, Cooper M, Kirkpatrick A and O'Connor J (2018) *Web Content Accessibility Guidelines (WCAG) 2.1*, World Wide Web Consortium (W3C).
21. Caldwell B, Cooper M, Reid L G, and Vanderheiden G (2008) *Web Content Accessibility Guidelines (WCAG) 2.0*, World Wide Web Consortium (W3C).
22. Campbell B, Jones M, Mortimore C and Goland Y (2015) *Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants [RFC 7521].* Internet Engineering Task Force (IETF).
23. Campbell B, Jones M and Mortimore C (2015) *JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants [RFC 7523]*. Internet Engineering Task Force (IETF).
24. Canadian Government Digital ID & Authentication Council of Canada (DIACC) (2016) *Pan-Canadian Trust Framework – Identity Establishment Conformance Criteria*, Canadian Government DIACC.
25. Cannon G, Karlsson M, Newton E, Schuckers S, Tabassi E (eds) (2019) *FIDO Biometrics Requirements*, Fast IDentity Online (FIDO) Alliance.
26. Cantor S, Kemp J, Maler E, Philpott R (eds) (2005) *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0* [SAML2Core] [PDF], OASIS Security Services Technical Committee.
27. Cantor S, Kemp J, Maler E, Philpott R (eds) (2005) *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0* [SAML2Meta] [PDF], OASIS Security Services Technical Committee.
28. Cantor S, Kemp J, Maler E, Philpott R (et al.) (eds) (2005) *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0* [SAML2Prof] [PDF], OASIS Security Services Technical Committee.
29. Cantor S (ed) (2017) *SAML V2.0 Subject Identifier Attributes Profile Version 1.0*, OASIS Security Services.
30. Committee IT-012 (Information Technology Security Techniques) (2012) *Information technology - Security techniques - Information security risk management (AS/NZS ISO/IEC 27005:2012)*, Standards Australia and New Zealand, Sydney and Wellington.
31. Committee IT-015 (Software and Systems Engineering) (2009) Risk management - principles and guidelines (AS/NZS ISO/IEC 31000:2009), Standards Australia and New Zealand, Sydney and Wellington.
32. Committee IT-015 (Software and Systems Engineering) (2015) Software and systems engineering – software testing – *Part 1:* concepts and definitions (AS/NZS ISO/IEC/IEEE 29119.1:2015), Standards Australia and New Zealand, Sydney and Wellington.
33. Committee IT-015 (Software and Systems Engineering) (2015) *Software and systems engineering – software testing – Part 2: test processes (AS/NZS ISO/IEC/IEEE 29119.2:2015)*, Standards Australia and New Zealand, Sydney and Wellington.
34. Committee IT-015 (Software and Systems Engineering) (2015) *Software and systems engineering – software testing – Part 3: test documentation (AS/NZS ISO/IEC/IEEE 29119.3:2015)*, Standards Australia and New Zealand, Sydney and Wellington.
35. Committee QR-015 (Complaints Handling) (2014) *Guidelines for complaint management in organisations (AS/NZS 10002:2014)*, Standards Australia and New Zealand, Sydney and Wellington.
36. Commonwealth Ombudsman (2017) *Better practice guides* [website], Australian Government Commonwealth Ombudsman website.

37. Council of Registered Ethical Security Testers (CREST) (2020) *Implementation & Procurement Guides* [website], CREST.
38. *Crimes Act 1914* (Cth)
39. *Criminal Code Act 1995* (Cth)
40. Davis M and Phillips A (eds) (2009), *Tags for Identifying Languages [RFC 5646],* Network Working Group.
41. Department of Finance (2016) *Implementing the Commonwealth Risk Management Policy - Guidance. Resource Management Guide 211*, Australian Government Department of Finance website.
42. Department of Finance (2009) *National e-Authentication Framework (NeAF),* Australian Government Department of Finance website [archived].
43. Department of Industry, Science, Energy and Resources (DISER) (2020) *How to prepare an emergency management plan* [website], DISER business.gov.au.
44. Department of Internal Affairs (2009) *Evidence of Identity Standard*, New Zealand Government Department of Internal Affairs.
45. Digital Transformation Agency (DTA) (2015) *Gatekeeper Public Key Infrastructure (PKI) Framework*, Australian Government DTA.
46. Digital Transformation Agency (DTA) (2017), *Digital Service Standard* [website], Australian Government DTA.
47. Digital Transformation Agency (DTA) (2017) *GOV.AU content guide* [website], Australian Government DTA.
48. Digital Transformation Agency (2020) *Australian Government Style Manual* [website], https://stylemanual.gov.au.
49. Dillaway B, Imamura T, Simon E, Yiu K and Nystrom M (2013) *XML Encryption Syntax and Processing [Version 1.1]* [XMLEnc]. W3C XML Schema Working Group, World Wide Web Consortium (W3C).
50. *Disability Discrimination Act 1992* (Cth)
51. Eastlake D (3rd) (2005) *Additional XML Security Uniform Resource Identifiers (URIs) [RFC 4051]* DOI 10.17487/RFC4051.
52. Fielding R, Gettys J, Mogul J, Frystyk H, Mastiner L, Leach P and Berners-Lee T (1999) *Hypertext Transfer Protocol – HTTP/1.1 [RFC 2616]*, Network Working Group.
53. Government Digital Service (2016) '*Measuring user satisfaction'*, *Gov.UK Service Manual*, https://www.gov.uk/service-manual.
54. Government Digital Service (2016) '*Measuring digital take-up'*, *Gov.UK Service Manual*, https://www.gov.uk/service-manual.
55. Government Digital Service (2016) *Measuring completion rate*', *Gov.UK Service Manual*, https://www.gov.uk/service-manual.
56. Government Digital Service (2016) '*Measuring const per transaction'*, *Gov.UK Service Manual*, https://www.gov.uk/service-manual.
57. Government of Canada (2012) '*Guideline on Defining Authentication Requirements*', *Government of Canada*.
58. Grassi P, Varley M (eds) (2017) *International Government Assurance Profile (iGov.OIDC-1.0) for OpenID Connect 1.0 – Draft 02*, OpenID Foundation (OIDF).
59. Grassi P, Richer J and Varley M (2017) *International Government Assurance Profile iGov Profile for OAuth 2.0*, OpenID Foundation (OIDF).

60. Hardt D (ed) (2012) *The Oauth 2.0 Authorization Framework [RFC 6749]*, Internet Engineering Task Force (IETF), Microsoft.
61. Hardt D and Jones M (2012) *The OAuth 2.0 Authorization Framework: Bearer Token Usage [RFC 6750]*. Internet Engineering Task Force (IETF).
62. Hoehn W et al. (2017) *SAML V2.0 Implementation Profile for Federation Interoperability V1.0*. Kantara Initiative.
63. Holz R, Sheffer Y and Saint-Andre P (2015) *Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS) [RFC 7457],* Internet Engineering Task Force (IETF).
64. International Organization for Standardization (2004) *Data elements and interchange formats – Information interchange – Representation of dates and times (ISO 8601:2004)*, ISO/TC 154 Processes, data elements and documents in commerce, industry and administration.
65. International Organization for Standardization (2019) Date and time – representations for information interchange – Part 1: Basic rules (ISO 8601-1:2019), ISO/TC 154 Processes, data elements and documents in commerce, industry and administration.
66. International Organization for Standardization (2010) Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems (ISO 9241-210:2010), ISO/TC 159/SC 4 Ergonomics of human-system interaction.
67. International Organization for Standardization (2011) Information technology – Security techniques – information security risk management (ISO/IEC 27005:2011), ISO/IEC JTC1/SC 27 IT Security techniques.
68. International Organization for Standardization (2012) Information technology – Security techniques – security requirements for cryptographic modules (ISO/IEC 19790:2012), ISO/IEC JTC 1/SC 27 IT Security techniques.
69. International Organization for Standardization (2015) *Software and systems engineering – software testing – test processes* (ISO/IEC/IEEE 29119.4:2015), ISO/IEC JTC1/SC7 software and systems engineering.
70. International Organization for Standardization (2016) Information technology – Biometric presentation attack detection – Part 1: Framework (ISO/IEC 30107-1:2016), ISO/IEC JTC 1/SC 37 Biometrics.
71. International Organization for Standardization (2017) *Information technology – Vocabulary- part 37: Biometrics (ISO/IEC 2382-37:2017)*, ISO/IEC JTC 1/SC 37 Biometrics
72. International Organization for Standardization (2018) *Information technology - Security techniques – Identity proofing (ISO/IEC TS 29003:2018)*, ISO/IEC JTC 1/SC 27 IT Security techniques.
73. International Organization for Standardization (2018) *Information technology – Service management – Part 1: Service management system requirements (ISO/IEC 20000-1:2018)*, ISO/IEC JTC 1/SC 40 IT Service Management and IT Governance.
74. International Telecommunication Union (ITU) (2010) *E.164: The international public telecommunication numbering plan*, ITU.
75. Jones M (2015) *JSON Web Key (JWK) [RFC 7517].* Internet Engineering Task Force (IETF).
76. Jones M (2015) *JSON Web Algorithms [RFC 7518]*. Internet Engineering Task Force (IETF).
77. Klensin J (2001) Simple Mail Transport Protocol [*RFC 2821]*, Network Working Group.
78. Leach P, Mealling M, Salz R (2005) Universally Unique IDentifier (UUID) URN Namespace (*RFC 4122)*, Internet Engineering Task Force.
79. Lodderstedt T, Dronia S, Scurtescu M (2013) *OAuth 2.0 Token Revocation [RFC 7009]*, Internet Engineering Task Force.

80. Lodderstedt T, McGloin M and Hunt P (2013) *OAuth 2.0 Threat Model and Security Considerations [RFC 6819].* Internet Engineering Task Force.
81. Makaay E, Smedinghoff T and Thibeau D (2017) *Trust Frameworks for Identity Systems*, Open Identity Exchange (OIX).
82. National Institute of Standards and Technology (NIST) (2017) *Digital Identity Guidelines [NIST SP 800-63-3]*, Government of the United States NIST.
83. National Institute of Standards and Technology (NIST) (2017) *Digital Identity Guidelines – Enrollment and Identity Proofing [NIST SP 800-63-3a]*, Government of the United States NIST.
84. National Institute of Standards and Technology (NIST) (2017) *Digital Identity Guidelines – Authentication and Lifecycle Management [NIST SP 800-63-3b],* Government of the United States NIST.
85. National Institute of Standards and Technology (NIST) (2017) *Digital Identity Guidelines – Federation and Assertions [NIST SP 800-63-3c]*, Government of the United States NIST.
86. National Institute of Standards and Technology (NIST) (2008) *Technical Guide to Information Security Testing and Assessment [NIST SP 800-115]*, Government of the United States NIST.
87. Nielsen J (1994) *How to Conduct a Heuristic Evaluation* [website], Neilson Norman Group.
88. Nielsen J (2012) *Usability 101: Introduction to Usability* [website], Neilson Norman Group.
89. Lebson C (2014) *Usability: What a Project Manager Needs to Know – Part 2,* usability.gov, U.S. General Services Administration.
90. OASIS Security Services (2005) https://docs.oasis-open.org/security/saml/v2.0/saml-schema-assertion-2.0.xsd [saml-schema-assertion-2.0].
91. OASIS Security Services Technical Committee (2008) *Identity Provider Discovery Service Protocol and Profile* [IdPDisco] [PDF], OASIS.
92. OASIS Security Services Technical Committee (2009) *SAML V2.0 Metadata Extension for Entity Attributes Version 1.0* [MetaAttr] [PDF], OASIS, Cantor S (ed).
93. OASIS Security Services Technical Committee (2019) *SAML V2.0 Metadata Interoperability Profile Version 1.0* [SAML2MDIOP] [PDF], OASIS, Cantor S (ed).
94. OASIS Security Services Technical Committee (2011), *Metadata Profile for Algorithm Support Version 1.0* [SAML2MetaAlgSup] [PDF], OASIS, Cantor S (ed).
95. OASIS Security Services (2005) https://docs.oasis-open.org/security/saml/v2.0/saml-schema-metadata-2.0.xsd [saml-schema-metadata-2.0].
96. OASIS Security Services Technical Committee (2012) *SAML Version 2.0 Errata 05* [SAML2Errata] [PSF], OASIS, Cantor S (ed).
97. OASIS Security Services Technical Committee (2012) *SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0* [MetaUI], OASIS, Cantor S (ed).
98. Office of the Australian Information Commissioner (OAIC) (2020) *Guide to undertaking privacy impacts assessments,* Australian Government OAIC.
99. Office of the Australian Information Commissioner (OAIC) (2014) *Guide to developing an APP privacy policy,* Australian Government OAIC.
100. Office of the Australian Information Commissioner (OAIC) (2016) *Guide to developing a data breach response plan,* Australian Government OAIC.
101. Office of the Chief Information Officer (2010) Electronic Credential and Authentication Standard, Ministry of Citizens' Services, Province of British Columbia, Canada.

102. Office of the Victorian Information Commissioner (2019) *Victorian Protective Data Security Framework Business Impact Levels,* [PDF], *OVIC.*
103. Open Banking Limited (2018) *Open Banking Customer Experience Guidelines*, openbanking.org.uk.
104. *Privacy Act 1988* (Cth)
105. *Proceeds of Crime Act 2002* (Cth)
106. *Proceeds of Crime Regulations 2002* (Cth)
107. *Public Governance, Performance and Accountability Act 2013* (Cth)
108. *Public Governance, Performance and Accountability Rule 2014* (Cth)
109. *Public Service Act 1999* (Cth)
110. Queensland Government (n.d.) *Business Continuity Planning template,* Department of Employment, Small Business and Training, Queensland Government.
111. Resnick P (ed) (2008) *Internet Message Format [RFC 5322],* Network Working Group.
112. Richer J (ed) (2015) *OAuth 2.0 Token Introspection [RFC 7662]*, Internet Engineering Task Force.
113. Stanton B, Theofanos M and Wolfson C (2008) *Usability and Biometrics: Ensuring Successful Biometric Systems,* Government of the United States NIST.
114. Telecommunication Standardisation Sector of ITU (ITU-T) (2010) *Recommendation X.1252 (04/2010): Baseline identity management terms and definitions,* International Telecommunications Union Publications.
115. Telecommunication Standardisation Sector of ITU (ITU-T) (2012) *Recommendation X.1254 (09/2020): Entity authentication assurance framework,* International Telecommunications Union Publications.
116. United Kingdom Cabinet Office (2012) *Good Practice Guide - Requirements for secure delivery of online public services (GPG 43)*, United Kingdom Cabinet Office, Gov.UK.
117. United Kingdom Cabinet Office (2014) *Good Practice Guide – Identity proofing and verification of an individual (GPG 45)*, United Kingdom Cabinet Office, Gov.UK. https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual
118. United Nations Commission on International Trade Law (UNCITRAL) (2018) *Legal Issues Related to Identity Management and Trust Services*, United Nations General Assembly.
119. Young I (2018) *Metadata Query Protocol draft-young-md-query-08* [SAML-MDQ], Network Working Group.