

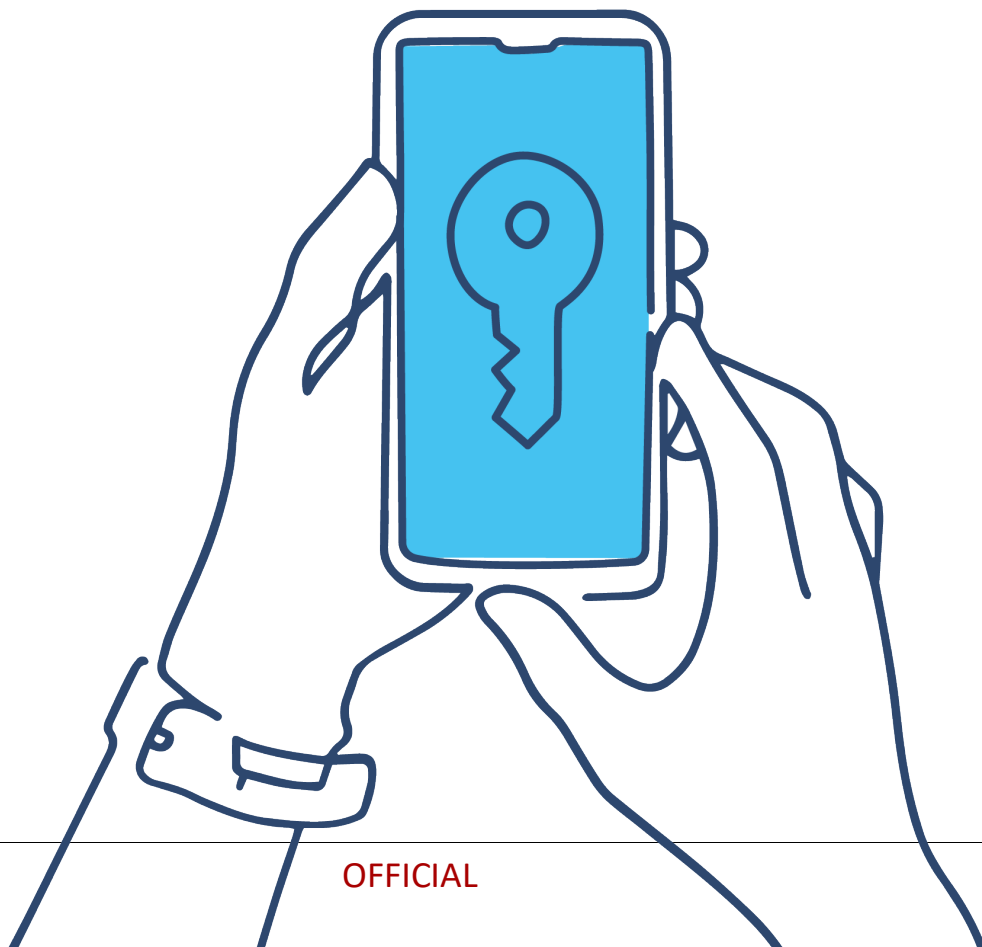


Digital Identity

01 Glossary of Abbreviations and Terms

Trusted Digital Identity Framework
Release 4.8 - Feb 2023

PUBLISHED VERSION



Digital Transformation Agency (DTA)

This work is copyright. Apart from any use as permitted under the Copyright Act 1968 and the rights explicitly granted below, all rights are reserved.

Licence



With the exception of the Commonwealth Coat of Arms and where otherwise noted, this product is provided under a Creative Commons Attribution 4.0 International Licence. (<http://creativecommons.org/licenses/by/4.0/legalcode>)

This licence lets you distribute, remix, tweak and build upon this work, even commercially, as long as you credit the *DTA* for the original creation. Except where otherwise noted, any reference to, reuse or distribution of part or all of this work must include the following attribution:

Trusted Digital Identity Framework (TDIF)™: 01 – Glossary of Abbreviations and Terms © Commonwealth of Australia (Digital Transformation Agency) 2023

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 this document.

TDIF requirements and references to *Applicants* are to be read as also meaning *Accredited Providers*, 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 the Director, Digital Identity Policy at digitalidentity@dtg.gov.au.

Document management

The *DTA* has reviewed and endorsed this document for release.

Change log

Document Version	Release Version	Date	Author	Description of the changes
0.1		July 2019	SJP	Initial version (removed from the previously titled <i>TDIF</i> Overview and Glossary)
0.2		Sep 2019	SJP	Updated to incorporate feedback provided by key stakeholders during the first round of collaboration on <i>TDIF</i> Release 4
0.3		Dec 2019	SJP	Updated to incorporate feedback provided by key stakeholders during the second round of collaboration on <i>TDIF</i> Release 4
0.4		Mar 2019	AV, MC, SJP	Updated to incorporate feedback provided during the third round of consultation on <i>TDIF</i> Release 4
1.0	4.0	May 2020		Published version
1.1	4.0	Sept 2020	MC	Updated to incorporate IP3 changes in the Role Requirements document.
1.2	4.2	Feb 2021	JK	CRID0001 – Style edit, grammar changes, new defined terms added, abbreviations added. CRID0002 – minor definition changes, style update.
1.3	4.4	June 2021	JK, SJP, AV, MS	CRID0003, CRID0009, CRID0018 – Style edit, new defined terms added to support other framework documentation changes, abbreviations added.
1.4	4.5	Oct 2021	JK	CRID0027 – Emergency changes to glossary
1.5	4.6	Mar 2022	JK, AV, SJP, MS, DN	Improvements to structure and clarity. Updates to reflect requirements changes.
NA	4.7	June 2022		No changes to document
NA	4.8	Feb 2023		No changes to document

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

01 Glossary of Abbreviations and Terms.....	i
Glossary of abbreviations	2
Glossary of terms	8
A	8
B	14
C	15
D	19
E	21
F.....	23
G, H, I	25
K, L	29
M.....	31
N	33
O	33
P, Q.....	35
R	38
S	40
T.....	42
U	45
V, W, X, Y, Z.....	46

Glossary of abbreviations

Term	Meaning
AACA	Australian Signals Directorate Approved Cryptographic Algorithm
AACP	Australian Signals Directorate Approved Cryptographic Protocol
ACSC	Australian Cyber Security Centre
ACR	Authentication Context Class Reference
ACS	Assertion Consumer Service
AFP	Australian Federal Police
AGD	Attorney General's Department
AGIMO	Australian Government Information Management Office
AGIS	Australian Government Investigation Standards
API	Application Programming Interface
APP	Australian Privacy Principles
AQF	Australian Qualifications Framework
ASD	Australian Signals Directorate
ASP	<i>Attribute Service Provider</i>
AS NZS	Australia and New Zealand Standards
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CDPP	Commonwealth Director of Public Prosecutions
CFCF	Commonwealth Fraud Control Framework
CISO	Chief Information Security Officer
CKMP	Cryptographic Key Management Plan

Term	Meaning
<i>CL</i>	Credential Level
<i>Col</i>	Commencement of Identity
<i>CP</i>	<i>Certificate Policies</i>
<i>CPS</i>	<i>Certification Practice Statements</i>
<i>CSCA</i>	Country Signing Certification Authority
<i>CSO</i>	Chief Security Officer
<i>CSP</i>	Credential Service Provider
<i>DFAT</i>	Department of Foreign Affairs and Trade
<i>DITRDC</i>	Department of Infrastructure, Transport, Regional Development and Communications
<i>DRBCP</i>	Disaster Recovery and Business Continuity Plan
<i>DTA</i>	Digital Transformation Agency
<i>DTD</i>	Document Type Definition
<i>DVS</i>	Document Verification Service
<i>EAP-TLS</i>	Extensible Authentication Protocol-Transport Layer Security
<i>EDI</i>	Evanescent Deterministic Identifier
<i>Eol</i>	Evidence of Identity
<i>FAR</i>	Failure to Acquire Rate
<i>FMR</i>	False Match Rate
<i>FSI</i>	Financial System Inquiry
<i>FNMR</i>	False Non-match Rate
<i>FTE</i>	Failure to Enrol Rate

Term	Meaning
<i>FVS</i>	Face Verification Service
<i>HTML</i>	Hyper Text Markup Language
<i>ICAO</i>	International Civil Aviation Organisation
<i>ICT</i>	Information and Communication Technologies
<i>ID</i>	Identity
<i>IdP</i>	<i>Identity Service Provider</i>
<i>IdX</i>	<i>Identity Exchange</i>
<i>IEC</i>	International Electro-technical Commission
<i>IEEE</i>	Institute of Electrical and Electronics Engineers
<i>IETF</i>	Internet Engineering Task Force
<i>IMEI</i>	International Mobile Equipment Identity
<i>IP</i>	Internet Protocol
<i>IP 1</i>	Identity Proofing Level 1
<i>IP 1 Plus</i>	Identity Proofing Level 1 Plus
<i>IP 2</i>	Identity Proofing Level 2
<i>IP 2 Plus</i>	Identity Proofing Level 2 Plus
<i>IP 3</i>	Identity Proofing Level 3
<i>IP 4</i>	Identity Proofing Level 4
<i>IRAP</i>	Information Security Registered Assessors Program
<i>IRP</i>	Incident Response Plan
<i>ISM</i>	Australian Government Information Security Manual
<i>ISO</i>	International Organisation for standardization

Term	Meaning
<i>ICT</i>	Information and Communications Technology
<i>ITU-T</i>	International Telecommunication Union – Telecommunication Standardization Sector
<i>JSON</i>	JavaScript Object Notation
<i>LOA</i>	Level of Assurance
<i>MDQ</i>	Metadata Query
<i>MF</i>	Multi-Factor
<i>MF OTP</i>	Multi Factor One Time Password
<i>MitM</i>	Man in the Middle (attack)
<i>MOU</i>	Memorandum of Understanding
<i>NAATI</i>	National Accreditation Authority for Translators and Interpreters
<i>NDES</i>	National Digital Economy Strategy
<i>NDLFRS</i>	National Driver Licence Facial Recognition Solution
<i>NeAF</i>	National eAuthentication Framework
<i>NIAP</i>	National Information Assurance Partnership
<i>NIPG</i>	National Identity Proofing Guidelines
<i>NIST</i>	National Institute of Standards and Technology
<i>NTIF</i>	National Trusted Identities Framework
<i>OA</i>	Oversight Authority
<i>OAIC</i>	Office of the Australian Information Commissioner
<i>OASIS</i>	Organisation for the Advancement of Structured Information Standards
<i>OECD</i>	Organisation for Economic Co-operation and Development

Term	Meaning
<i>OIDC</i>	OpenID Connect 1.0
<i>OIX</i>	Open Identity Exchange
<i>OP</i>	OpenID Connect Provider
<i>OR</i>	Operating Rules
<i>OTP</i>	One-Time Password
<i>OWASP</i>	Open Web Application Security Project
<i>PAD</i>	Presentation Attack Detection
<i>PIA</i>	Privacy Impact Assessment
<i>PII</i>	Personally Identifiable Information
<i>PIN</i>	<i>Personal</i> Identification Number
<i>PKI</i>	Public Key Infrastructure
<i>PKT</i>	Public Key Technology
<i>PMC</i>	Prime Minister and Cabinet
<i>PSPF</i>	Protective Security Policy Framework
<i>PSTN</i>	Public Switched Telephone Network
<i>RBDM</i>	Registries of Births, Deaths and Marriages
<i>RFC</i>	<i>Request for Comment</i>
<i>RFID</i>	Radio-frequency Identification
<i>RP</i>	Relying Party
<i>RSA</i>	Rivest-Shamir-Adleman
<i>RTA</i>	Road Traffic and Transport Authorities
<i>RTM</i>	<i>Requirements Traceability Matrix</i>

Term	Meaning
<i>SAML</i>	Security Assertion Mark-up Language
<i>SF</i>	Single Factor
<i>SF OTP</i>	Single Factor One Time Password
<i>SHA</i>	Secure Hashing Algorithm
<i>SMS</i>	Short Message Service
<i>SoA</i>	Statement of Applicability
<i>SOP</i>	Standard Operating Procedure
<i>SP</i>	Special Publication
<i>SRMP</i>	Security Risk Management Plan
<i>SSO</i>	<i>Single Sign On</i>
<i>SSP</i>	System Security Plan
<i>TDIF</i>	Trusted Digital Identity Framework
<i>TLS</i>	Transport Layer Security
<i>TPISAF</i>	Third Party Identity Services Assurance Framework
<i>UitC</i>	Use in the Community (document)
<i>UNCITRAL</i>	United Nations Commission on International Trade Law
<i>URN</i>	Uniform Resource Name
<i>W3C</i>	World Wide Web Consortium
<i>WCAG</i>	Web Content Accessibility Guidelines
<i>XML</i>	Extensible Markup Language

Glossary of terms

A wide variety of terms are used in the realm of identity management. While the definition of many of these terms are sourced from existing government policies and international standards, the definition of some terms has been modified to meet the needs of the *TDIF*. Where this occurs, the source is listed as *TDIF*.

A

Access control. The process of granting or denying requests for access to systems, applications and information. Can also refer to the process of granting or denying requests for access to facilities. Source: *ISM*.

Accessibility. Addresses discriminatory aspects related to equivalent user experience for people with disabilities. Web accessibility means that people with disabilities can equally perceive, understand, navigate, and interact with websites and tools. It also means that they can contribute equally without barriers. Source: *W3C*.

Accessibility Assessment. A *Functional Assessment* against the *W3C Web Content Accessibility Guidelines* (versions 2.0 and 2.1). Source: *TDIF*. See also: *Accessibility, Functional Assessments*.

Access token. A JSON Web Token or equivalent that acts as proof of authorisation to access a service. Source: *OpenID Connect Core 1.0*

Accountable Executive. A senior executive designated within an *Applicant* or *Accredited Provider's* organisation responsible for managing aspects of its *Identity System*. Source: *TDIF*.

Note 1 For a Commonwealth entity, the position of Accountable Executive may be held by the entity's accountable authority (within the meaning of the *Public Governance, Performance and Accountability Act 2013* or applicable state or territory legislation).

Note 2 Details of the entity's Accountable Executive are to be provided by the entity when applying for accreditation.

Accreditation. The act by an authoritative body of granting recognition. In the context of the *TDIF*, accreditation is awarded by the *DTA* to *Applicants* that demonstrate they meet all applicable *TDIF* requirements. Source: *TDIF*.

Accredited Participants. An organisation that is an *Accredited Provider* and is participating in the *Australian Government's Identity Federation*. See also: *Accredited Provider, Applicant*. Source: *TDIF*.

Accredited Provider. Organisations that have achieved *TDIF* accreditation. An *Accredited Provider* can be an *Attribute Service Provider, Identity Provider, Credential Service Provider* or *Identity Exchange Provider*. Source: *TDIF*. See also: *Applicant*.

Accredited Roles. The four accreditation classes supported under the *TDIF*, including *Attribute Service Providers, Credential Service Providers, Identity Exchange* and *Identity Service Providers*. Source: *TDIF*.

Acquired Image. An image of the *User's* face that is used as the sample for biometric matching. Source: *TDIF*.

Alternative Assessment Reports. Alternative reports or prior audit work on an *Applicant's Identity System* that may be used as a substitution for *Functional Assessments* or as evidence to meet the *TDIF* requirements. Source: *TDIF*

Annual Assessment. Details the *Accredited Provider's Identity System's* compliance against *TDIF* requirements as specified by *TDIF 07 Maintain Accreditation*. Source: *TDIF*.

APP entity. Has the same meaning as in the *Privacy Act 1988*.

Applicant. Organisations that undergo the *TDIF Accreditation Process* in the role of an *Attribute Service Provider, Credential Service Provider, Identity Service Provider, Identity Exchange* or a combination of these. Source: *TDIF*.

Applicant Capability. The product serviced by the *Applicant* and used by the *User* for the purposes of *Identity Proofing* and *Biometric Binding*. Source: *TDIF*.

Application. The *Identity Proofing* process which involves *Biometric Binding*. Source: *NIPG*.

Approved Cryptography. Either:

- Australian Signals Directorate Approved Cryptographic Algorithms (AACAs); or
- Australian Signals Directorate Approved Cryptographic Protocols (AACPs).

Assertion. A statement from a *TDIF Accredited Role* to a *Relying Party* that contains information about a *User*. *Assertions* may also contain verified *Attributes*. Source: *TDIF*.

Assessing Officer(s). A member of *Personnel* of an *Accredited Provider* who is trained and authorised by that provider to perform *Local Biometric Binding* and *Manual Face Comparison*. Source: *TDIF*

Assessment. An independent review and examination of validity, accuracy and reliability of information contained on a system to assess the adequacy of system controls and ensure compliance with established policies and procedures. In the context of conducting system accreditations, an audit (also known as a compliance assessment) is an examination and verification of an entity's systems and procedures, measured against predetermined standards. Source: *TDIF*.

Assessor. 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. Source: *TDIF*. See also: *Assessment*.

Assisted Digital. The support provided by an *Accredited Provider* to an *Individual* who can't use a digital service independently. This includes *Individuals* who are offline with no digital skills and those who are online but only have limited digital skills. Source: *TDIF*.

Assumed Self-asserted Attributes (for Identity Service Providers). Contact or *Identity Attributes* that are provided by an *Individual* and are generally not *verified* or *validated* by the *Identity Service Provider*. *Assumed Self-asserted Attributes* that an *Identity Service Provider* can collect are limited by *TDIF* requirements. Source: *TDIF*. See also: *Attributes*, *Assumed Self-asserted Attributes (for Attribute Service Providers)*

Assumed Self-asserted Attributes (for Attribute Service Providers). An *Attribute Class* of *Attributes* provided by an *Individual* that are generally not *verified* or *validated*. These *Attributes* can assist with service delivery, such as prefilling online forms. This *Attribute Class* can be used for 'Tell Us Once' services. Source: *TDIF*

Attacker. See: *Malicious Actor*

Attestation. Is information conveyed regarding a directly connected *Credential* or the endpoint involved in an authentication operation. Source: *NIST*

Attribute(s). An item of information or data associated with a subject. Examples of attributes include information such as name, address, date of birth, email address, mobile number, etc. Source: *UNCITRAL*.

Attribute Class. A categorisation of *Attributes* depending on the type of information they detail. Source: *ISM*.

Attribute Service Provider (ASP). One of the four *Accredited Roles*. An entity that has been accredited in accordance with the TDIF as an attribute service provider and that provides a service that verifies or manages specific attributes relating to entitlements, qualifications or characteristics of an *Individual*. Source: TDIF

Attribute Set: A collection of *Attributes* that aligns with the logical sets of *Attributes* that a *Relying Party* will typically ask for as a collection, and that a *User* will provide *Consent* for as a collection. Source: TDIF

Attribute Sharing Policies. Policies that describe the rules that must be applied when sharing *Attributes* with a *Relying Party*. Source: *TDIF*.

Attribute Verification Services. See *Identity Matching Service*.

Audit log. A chronological record of system activities including records of system access and operations performed. Source: *ISM*.

Audit trail. A chronological record that reconstructs the sequence of activities surrounding, or leading to, a specific operation, procedure or event. Source: *ISM*.

Australian Business Number (ABN). An ABN is a unique 11 digit number that identifies a business to the Australian Government and community. Source: *Business.gov.au*

Australian Government Agencies Privacy Code. A written code of practise which sets out specific requirements and key practical steps that agencies must take as part of complying with Australian Privacy Principle 1.2. Source: *OAIC*.

Australian Government Digital Identity System (the System). An *Identity Federation* which is managed by the Australian Government. Source: *DTA*

Australian Government Information Security Manual (ISM). A manual to assist Australian government agencies in applying a risk-based approach to protecting their information and systems. The *ISM* includes a set of information security controls that, when implemented, will help agencies meet their compliance requirements for mitigating security risks to their information and systems. Source: *ASD*.

Australian Government Investigation Standards (AGIS). Is a cornerstone of the Australian Government's fraud control policy and is the minimum standard for Australian Government agencies' conducting investigations relating to the programs and legislation they administer. Source: *AGD*.

Australian Government Protective Security Policy Framework (PSPF). Defines a series of core policies and mandatory requirements with which applicable Commonwealth agencies and bodies must demonstrate their compliance. These requirements cover protective security governance, personnel security, information security and physical security. Source: *AGD*.

Australian Privacy Principles (APP). Are the cornerstone of the privacy protection framework in the *Privacy Act 1988*. There are 13 *Australian Privacy Principles* and they govern standards, rights and obligations around:

- The collection, use and disclosure of personal information.
- An organisation or agency's governance and accountability.
- Integrity and correction of personal information.
- The rights of *Individuals* to access their personal information.

Source: *OAIC*.

Australian Signals Directorate Approved Cryptographic Algorithms (AACAs). Algorithms that have been extensively scrutinised by industry and academic communities in a practical and theoretical setting and have not been found to be susceptible to any feasible attacks. AACAs fall into three categories: asymmetric/public key algorithms, hashing algorithms and symmetric encryption algorithms. Source: *ISM*.

Australian Signals Directorate Approved Cryptographic Protocols (AACP).

Cryptographic equipment and software that has passed a formal evaluation. Source: *ISM*.

Authenticated Protected Channel. A communication channel that uses *Approved Cryptography* where the client connection has authenticated to the relevant server. Source: *TDIF*.

Authenticated Session. A persistent interaction between two participants in an *Identity System* which begins with an *Authentication Event* and ends with a *Session Termination Event*.

Authentication. A function for establishing the validity of a claimed *Identity* of a *User*, device or another entity in an information or communications system. Source: *OECD*.

Authentication Credential. See: *Credential*.

Authentication Event. The process of a *User* using their *Credentials* to prove that they are the valid user of a *Digital Identity*

Authentication Factor. A piece of information and/or process used to authenticate or verify the *identity* of an *entity*. *Authentication factors* are divided into three categories:

- Something an entity has (device signature, passport, hardware device containing a credential, private key)
- Something an entity knows (password, pin)
- Something an entity is (biometric characteristic).

Source: *TDIF*

Authentication Protocol. A defined sequence of messages between a *User* and a *Credential Service Provider* that demonstrates that the *User* has possession and control of one or more valid *Credentials* to establish their *identity*. Source: *TDIF*.

Authentication Request. A request for *Authentication* from:

- a *User* to an *Accredited Participant* or *Applicant*; or
- an *Accredited Participant* or *Applicant* to another *Entity*. Source: *TDIF*.

Authorised Representative. An *Individual* or *Entity* authorised to act on a *User's* behalf, in accordance with policies or procedures set out by an *Applicant* or *Accredited Provider*. Source: *TDIF*.

Authoritative Source. Repositories recognised by the *DTA* that confirm the veracity of *Attributes* and associated information. Source: *TDIF*. See also: *Identity Document Issuer*.

B

Behavioural Information Includes data on the services an *Individual* has accessed or tried to access, when the *Accredited Provider* was used by the *Individual*, the method of access to the *Accredited Provider* and when their *Identity* was verified. Source: *TDIF*.

Binding Objective. This is an objective of *Identity Proofing*, which provides confidence that the *Individual's Identity* claim is not only legitimate, but that the *Individual* currently claiming the *Identity* is its legitimate holder. Source: *DTA*

Biometric Binding. The process, under the *TDIF*, of linking an *Individual* with a claimed *Identity* by performing *Biometric Verification*. Source: *TDIF*. See also: *Biometric Verification*, *Biometric Matching*.

Biometric Capability. The components of an *Applicant's Identity System* that perform or support *Biometric Binding*, *Presentation Attack Detection*, *Biometric Matching* and/or *Manual Face Comparison* processes. Source: *TDIF*.

Biometric information. Information about any measurable biological or behavioural characteristics of a natural person that can be used to identify them or verify their *Identity*, such as face, fingerprints and voice. Biometric information includes biometric templates. (Under the *Privacy Act 1988*, *Biometric information* is considered sensitive information, which provides additional obligations on organisations.). Source: *NIPG*.

Biometric Matching: The process of automated recognition of a *User* utilising their distinctive biological or behavioural characteristics. Source: *TDIF*.

Biometric Sample. Data obtained by a biometric capture device such as a facial image, voice recording, or fingerprint image. Source: *TDIF*. See also: *Biometric Information*.

Biometric Template: A set of stored biometric features comparable directly to probe biometric features (numbers or labels extracted from biometric samples and used for comparison). Source: *ISO 2382-37*

Biometric Testing Entity. An independent, third-party entity appropriately qualified to carry out biometric testing for PAD and Matching Algorithms. Source: *TDIF*.

Biometric verification. The process of one-to-one comparison of an *Individual* against the image on their claimed *Photo ID* by performing either *Technical Biometric Matching*, *Source Biometric Matching* or *Manual Face Comparison* processes. Source: *TDIF*. See also: *Biometric Matching*.

C

Certificate (Digital Certificate). An electronic document signed by the *Certification Authority* which:

- Identifies either a *Key Holder* and/or the business entity that they represent; or a device or application owned, operated or controlled by the business entity
- Binds the *Key Holder* to a *Key Pair* by specifying the *Public Key* of that *Key Pair*
- Contains the information required by the *Certificate* profile.

Certification Authority. A *Credential Service Provider* that digitally signs X.509 v3 *Digital Certificates* using its *Private Key*. Source: *TDIF*

Certification Practice Statements (CPS). A statement of the practices that a Certification Authority employs in managing the Digital Certificates it issues (this includes the practices that a Registration Authority employs in conducting registration activities on behalf of that Certification Authority).

These statements will describe the PKI certification framework, mechanisms supporting the application, insurance, acceptance, usage, suspension/revocation and expiration of Digital Certificates signed by the CA, and the CA's legal obligations, limitations and miscellaneous provisions.

Certificate Policies. A named set of rules that indicates the applicability of a Certificate to a particular community and/or class of applications with common security requirements. Source: RFC3647

Certificate Revocation Lists (CRL). The published directory which lists revoked Digital Certificates. The CRL may form part of the Certificate Directory or may be published separately. Source: *TDIF*

Chief Security Officer (CSO). The person responsible, at a management level, for security in an organisation. Source: *TDIF*

Claimed Photo ID. The *Photo ID* document presented by the *Individual* for *Identity Proofing* as part of an *Identity Claim*. Source: *TDIF*. See also: *Identity Document*, *Photo ID*.

Commencement of Identity (Col) (document). The first registration of an *Individual* by a government agency in Australia and includes RBDM birth registrations and issuance of Home Affairs immigration documents and records¹. Source: *NIPG*.

Commonwealth Director of Public Prosecutions (CDPP). Is an independent prosecuting service and government agency within the portfolio of the Attorney-General of Australia as part of the Attorney-General's Department. Source: *AGD*

Commonwealth Fraud Control Framework (CFCF). The *Commonwealth Fraud Control Framework* outlines the Australian Government's requirements for fraud control. This includes a requirement that government entities have a comprehensive fraud control program that covers prevention, detection, investigation and reporting strategies. Source: *AGD*.

Compromised Credential. A *credential* that has been reported to the *CSP* or identified by the *CSP* that has been lost, stolen, damaged or duplicated without authorisation. Source: *TDIF*. See also: *Credential*, *Restricted Credential*

¹ In the context of the *TDIF* an Australian Passport is also considered a Col document.

Computed Attribute. An *Attribute* that is dynamically derived from the *Attributes* in an *Attribute Set* using an algorithm. For example, deriving an *Individual's* current age from their date of birth. Source: *TDIF*.

Consent. Means *Express Consent* or *Implied Consent*. The four key elements of *Consent* are:

- The *Individual* is adequately informed before giving *Consent*.
- The *Individual* gives *Consent* voluntarily.
- The *Consent* is current and specific.
- The *Individual* has the capacity to understand and communicate their *Consent*.

Source: OAIC.

Consumer History. The history of all a *User's* interactions with an *Identity Exchange*. Source: *TDIF*.

Control(s). Any process, policy, device, practice or other actions within the internal environment of an organisation which modifies the likelihood or consequences of a risk. Source: *ISO 31000*.

Credential. The technology used to authenticate a *User's Identity*. Source: *TDIF*.

Note: A *Credential* may incorporate a password, cryptographic key or other form of secret.

Credential Binding. The process of linking a *Credential* with a *Digital Identity*. Source: *TDIF*.

Credential Level (CL). The level of assurance or confidence in the authentication process. Source: *TDIF*.

Credential Level 1 (CL1). A basic authentication credential suitable for use at the IP1 proofing level. This allows single-factor authentication, e.g. password. Source: *TDIF*.

Credential Level 2 (CL2). A strong authentication credential suitable at the IP1, IP2 and IP3 proofing levels. This requires two-factor authentication, e.g. password with additional one-time password. Source: *TDIF*.

Credential Level 3 (CL3). A very strong authentication credential, suitable at the IP1, IP2, IP3 and IP4 levels. This requires two factor authentication and hardware verification. Source: *TDIF*.

Credential management. The ‘lifecycle’ approach associated with a *Credential* including creation, initialisation, personalisation, issue, maintenance, recovery, cancellation, verification and event logging. Source: *TDIF*.

Credential Service Provider (CSP). One of the four Accredited Roles. An entity that has been accredited in accordance with the TDIF as a *Credential Service Provider* and that provides a service that does either or both of the following:

- generates, binds, manages or distributes *Credentials* to *Individuals*;
- binds, manages or distributes *Credentials* generated by *Individuals*.

Source: *TDIF*.

Cross Certificate. A cross certificate enables *Individuals* and *Relying Parties* in one *PKI* deployment to trust *entities* in another *PKI* deployment. This trust relationship is usually supported by a cross certification agreement between *Certificate Authorities* in each *PKI* deployment, which defines the responsibilities of each party. Source: *TDIF*

Cryptographic Key (Key). A *Key* is a string of characters used with *Approved Cryptography* to encrypt and decrypt. Source: *TDIF*

Cryptographic Key Management Plan (CKMP). A *Cryptographic Key Management Plan* identifies the implementation, standards, procedures and methods for key management in *PKI* service providers and provides a good starting point for the protection of cryptographic systems, keys and digital certificates. Source: *Gatekeeper PKI Framework*.

Cryptographic Protocol. An agreed standard for secure communication between two or more entities to provide confidentiality, integrity, *authentication* and non-repudiation of information. Source: *ASD*.

CSP-Compromise Resistance. *Authentication protocols* that do not require the *Credential Service Provider* to persistently store secrets that could be used for *authentication*. Source: *TDIF*.

CSP-impersonation Resistance. *Authentication methods* implemented by a *Credential Service Provider* for preventing and addressing impersonation attacks. Source: *TDIF*.

Cyber Security Incident. One or more acts, events or circumstances that involve:

- unauthorised access to, modification of or interference with a system, service or network; or
- an unauthorised attempt to gain access to, modify or interfere with a system, service or network; or
- unauthorised impairment of the availability, reliability, security or operation of a system, service or network; or
- an unauthorised attempt to impair the availability, reliability, security or operation of a system, service or network.

Cyber Security Risk. In relation to an *Applicant or Accredited Provider*, means the risk that a cyber security incident in relation to the services for which it is accredited or its *Identity System*, will occur.

D

Data Breach. Loss or misuse of, unauthorised access to, or unauthorised modification or disclosure of, *Personal Information* held by an entity.

Data Breach Response Plan. Is a framework that sets out the roles and responsibilities involved in managing a data breach. It also describes the steps an entity will take if a data breach occurs. Source: *OAIC*

Deduplication. The process of determining whether two or more *Digital Identity* records relate to the same *Individual* or a different *Individual*, whether within a single *IdP (IdP deduplication)*, or across multiple *IdPs*, at the *Identity Exchange Provider*(ecosystem deduplication). Source: *TDIF*.

Digital Certificate. See: *Certificate*

Digital Identity. A distinct electronic representation of an *Individual* which enables that *Individual* to be sufficiently distinguished when interacting online with services. A *Digital Identity* may include *Attributes* and *Assertions* which are bound to a *Credential*. A *Digital Identity* can be used by *Individuals* to access online services. Source: *TDIF*.

Digital Identity Fraud Control Plan. A plan that meets the requirements specified in FRAUD-02-02-01a. Source: TDIF.

Digital Identity Fraud Controller. For an *Applicant*:

- the position of Digital Identity Fraud controller for the Applicant, having the duties and responsibilities specified in the Applicant's fraud control plan; or
- the person appointed as, or appointed to act in the position of, Digital Identity Fraud Controller for the Applicant as mentioned in FRAUD-02-01-01.

Digital Identity Fraud Incident. An act, event or circumstance that:

- occurs in connection with a service:
 - that an entity is accredited to provide; and
- results in any of the following being, or suspected of being compromised or rendered unreliable:
 - the *Digital Identity of an Individual*;
 - an attribute of an *Individual*;
 - a credential relating to an *Individual*;
 - a representation relating to an attribute of an *Individual* or a *Digital Identity of an Individual*.

Digital Identity Fraud Risk. Means the risk that a *Digital Identity Fraud Incident* will occur in relation to an entity. Source: TDIF

Digital Identity Information. Information that is:

- generated in an *Identity System*; or
- obtained from an *Identity System*; or
- collected for the purposes of an *Identity System*.

Digital Signature. An electronic signature created using a *Private Signing Key*. The cryptographic process allows the proof of the source (with non-repudiation) and the verification of the integrity of the data. Source: TDIF

Disaster Recovery and Business Continuity Plan (DRBCP). Helps minimise the disruption to the availability of information and systems after a security incident or

disaster by documenting the response procedures. Source: *Gatekeeper PKI Framework*.

Document Biometric Matching. The process of verifying that the *User's Acquired Image* biometrically matches the corresponding image recorded in the *User's Claimed Photo ID*. This process includes only *Claimed Photo ID* documents that are government issued with cryptographically signed *RFID* chips that store the image, such as an ePassport. Source: *TDIF*.

Document Verification Service (DVS). A national online system that checks whether the biographic information on an *Identity* document matches the original record. The result will simply be 'yes' or 'no'. The *DVS* does not check facial images. The *DVS* makes it harder for people to use fake *Identity* documents and both the public and private sectors use the *DVS*. Source: ID Match (Department of Home Affairs).

Double blind. Refers to a concept of *Australian Government's Digital Identity System* such that each *Participant* is blinded from each other. *Double blind* applies between:

- The *Relying Party* and the *Identity Service Provider*.
- The *Identity Service Provider* and the *Attribute Service Provider*.
- The *Relying Party* and the *Attribute Service Provider*, unless otherwise approved by the *Oversight Authority*.

Double blind does not apply between the *Credential Service Provider* and the *Identity Service Provider*. Source: *TDIF*.

E

Easy English. A style of writing that has been developed to provide understandable, concise information for people with low English literacy. *Individuals* with low English literacy can be described as people with a limited ability to read and write words. Source: Scope Vic.

End user. A *Person* that interacts with a *TDIF Provider's* service with the intention of obtaining a *Digital Identity*. Source: *TDIF*.

Enforcement Body. Has the same meaning as in the *Privacy Act 1988*.

Entity. Any of the following:

- an individual;
- a body corporate;
- a Commonwealth entity, or a Commonwealth company, within the meaning of the Public Governance, Performance and Accountability Act 2013;
- a person or body that is an agency within the meaning of the Freedom of Information Act 1982;
- a body specified, or the person holding an office specified, in Part I of Schedule 2 to the Freedom of Information Act 1982;
- a department or authority of a State;
- a department or authority of a Territory;
- a partnership;
- an unincorporated association;
- a trust.

Source: *TDIF*

Essential Eight. No single mitigation strategy is guaranteed to prevent cyber security incidents. Government agencies and organisations are recommended to implement essential eight mitigation strategies as a baseline. This baseline, known as the *Essential Eight*, makes it much harder for adversaries to compromise systems. Furthermore, implementing the *Essential Eight* pro-actively can be more cost-effective in terms of time, money and effort than having to respond to a large-scale cyber security incident. Source: *ASD*.

Evidence of Identity (Eoi) (document). Information that a person may present to support assertions or claims to a particular *Identity*. The types of evidence that, when combined, provide confidence that an *Individual* is who they say they are, and that the *Identity* is valid and not known to be fraudulent. This evidence may be provided in the form of *Identity* documents or other card-based credentials that contain key *Attributes* (such as name, date of birth, unique identifier) or provide information on an *Individual's* 'pattern of life' or 'community footprint'. Source: *NIPG*.

Exceptional Use Case. A situation where an *Individual* does not possess, and is unable to obtain, the information or evidence of identity required for the relevant proofing level, including as a result of the *Individual*:

- having their birth not registered;
- being homeless or displaced;

- being an undocumented arrival to Australia;
- living in remote areas;
- being a foreign national living in Australia (provided that individual is not also an Australian citizen), or an Australian citizen living in another country;
- *Individuals* who do not have any identity documents but need a *Digital Identity*, for example, foreign nationals living outside Australia who need to access Government systems or services;
- being transgender or intersex;
- being affected by natural disasters; or
- having limited access to evidence of identity.

Note Individuals with limited access to evidence of identity includes, for example, individuals who were raised in institutional or foster care, have limited participation in society; or are under the age of 18 and yet to obtain evidence of identity.

Express Consent. is given explicitly, either orally or in writing. This could include a handwritten signature, or oral statement, or use of an electronic medium or voice signature to signify agreement. Source: *OA/C*.

F

Fact of Death File. Is a compilation of death records from each of the data custodians. These files contain full name, date of birth and residential address details of all the people who have died in Australia. Data files are available on the Australian Coordinating Registry dating back to 1992. Source: Queensland Government.

Failure to Acquire Rate (FAR). The proportion of a specified set of biometric acquisition processes that fail. Source: *ISO 2382-37*

Note See ISO 2382-37 for further details of the meaning of this term.

Failure to Enroll Rate (FTE): Failure to create and store a biometric enrolment data record for an eligible biometric capture subject, in accordance with a biometric enrolment policy. Source: *ISO 2382-37*.

Note See ISO 2382-37 for further details of the meaning of this term.

False Match Rate (FMR):. The proportion of the completed biometric non-mated comparison trials that result in a false match. Source: *TDIF*.

Note See ISO 2382-37 for further details of the meaning of this term.

False Non-match Rate (FNMR): The proportion of the completed biometric mated comparison trials that result in a false non-match.. Source: *TDIF*.

Note See ISO 2382-37 for further details of the meaning of this term.

Family name. A person's last name or surname. The ordering of family name and given names varies among cultures. Some cultures do not recognise a 'family' name; In Australia the last name is usually adopted as the family name. Source: *NIPG*.

Federation Protocol. A defined sequence of messages between *Participants* in an *Identity Federation* that allow the conveyance of *Identity* and authentication information between *Participants*. Source: *NIST SP 800-63-3*

Federation Proxy. A component that acts as a logical *Relying Party* to a set of Identity Service Providers and a logical Identity Service Provider to a set of Relying Parties, bridging the two systems with a single component. These are sometimes referred to as "brokers". Source: *NIST SP 800-63-3*.

Financial System Inquiry (FSI). An inquiry commenced by a state or federal government charged with examining how the financial system operates. Source: *Financial System Inquiry Final Report November 2014*.

Forward Work Plan. A list of outstanding risks or recommendations that an *Applicant* has committed to mitigating or implementing respectively on future dates in order to satisfy the TDIF Requirements. Source: *TDIF*.

Fraud. Dishonestly obtaining a benefit, or causing a loss, by deception or other means. Source: *CFCF*.

Fraud Control Objective: This is an objective of *Identity Proofing*, which provides additional confidence that a fraudulent (either fictitious or stolen) *Identity* is not being used. These checks decrease the risk of a fraudulent *Identity* within the *Identity Federation*. Source: *DTA*.

Functional Assessments. Assessments of an *Applicant's Identity System* by an *Assessor* to establish conformance with various TDIF requirements. Functional Assessments cover the following:

- *Privacy Impact Assessment*

- *Privacy Assessment*
- *Security Assessment*
- *Accessibility Assessment*
- *Penetration Test*

Source: *TDIF*.

Functional Assessment Report. Documented outcomes of *Functional Assessments*. This report is completed by the *Applicant*. Source: *TDIF*.

G, H, I

Given name. Given names include combinations of first name/s, forename, Christian name/s, middle name/s and second name/s. Source: *NIPG*.

Handling requirements. An agreed standard for the storage and dissemination of information to ensure its protection. This can include electronic information, paper-based or media containing information. Source: *ISM*.

High Risk Project. A change to the services for which the entity is accredited or the entity's *Identity System* that is or is likely to have a significant impact on:

- the nature or scope of personal information collected, stored or processed by the entity; or
- the manner in which personal information is collected, stored or processed by the entity.

Identifier. One or more attributes that uniquely characterize an entity in a specific context. Source: *UNCITRAL*.

Identity (ID). (a) information about a specific *Individual* in the form of one or more attributes that allow the *Individual* to be sufficiently distinguished within a particular context; (b) a set of the *Attributes* about a *Person* that uniquely describes that *Person* within a given context. Source: *UNCITRAL*.

Identity attribute. See *Attribute*.

Identity Document. A physical document or non-documentary *Identity* data held in a repository accessible capable of being used as *Evidence of Identity* in Australia.

Source: *NIPG* (adapted by *DTA*).

Identity document issuer. An approved government or non-government entity that issues *Identity documents*, such as passports, driver licences or proof of age cards.

Source: *TDIF*. See also: *Authoritative Source*

Identity Exchange (IdX). One of the four *Accredited Roles*. An entity that has been accredited in accordance with the *TDIF* as an identity exchange and that provides a service that conveys, manages and coordinates the flow of data or other information between participants in an *Identity Federation*. Source: *TDIF*.

Identity Facility. See: part 2 of *Identity System*.

Identity federation. A group of *Participants* that work together to ensure identity-related information can be relied on by *Relying Parties* to make risk-based decisions. Synonyms: Multi-party *Identity System*, federated identity management system, identity ecosystem. Source: *TDIF*.

Identity management. A set of processes to manage the identification, authentication and authorization of individuals, legal entities, devices or other subjects in an online context. Source: *UNCITRAL*.

Identity Matching Service. A government service which compares personal information on *Identity* documents against existing government records, such as passports, driver licences and birth certificates. *Identity Matching Services* include the *DVS* and *FVS*. Source: *ID Match* (Australian Government Department of Home Affairs).

Identity Proofing (IP). Refers to the process of collecting, verifying, and validating sufficient *Attributes* (and supporting evidence) about a specific *Individual* to confirm their *Identity*. Source: *TDIF*.

Identity Proofing Level (IP Level). describes the level of assurance or confidence in the *Identity Proofing* process. Source: *TDIF*.

Identity Proofing Level 1 (IP 1) is used when no *Identity* verification is needed or when a very low level of confidence in the claimed *Identity* is needed. This level supports self-asserted *Identity* (I am who I say I am) or pseudonymous *Identity*. The

intended use of *Identity Proofing Level 1* is for services where the risks of not undertaking *Identity* verification will have a negligible consequence to the *Individual* or the service. For example, to pay a parking infringement or obtain a fishing licence.

Source: TDIF.

Identity Proofing Level 1 Plus (IP 1 Plus) is used when a low level of confidence in the claimed *Identity* is needed. This requires one *Identity Document* to verify someone's claim to an existing *Identity*. The intended use of *Identity Proofing Level 1 Plus* is for services where the risks of getting *Identity* verification wrong will have minor consequences to the *Individual* or the service. For example, the provision of loyalty cards. Source: TDIF.

Identity Proofing Level 2 (IP 2) is used when a low-medium level of confidence in the claimed *Identity* is needed. This requires two or more *Identity Documents* to verify someone's claim to an existing *Identity*. The intended use of *Identity Proofing Level 2* is for services where the risks of getting *Identity* verification wrong will have moderate consequences to the *Individual* or the service. For example, the provision of utility services. An *Identity Proofing Level 2 Identity* check is sometimes referred to as a "100-point check". Source: TDIF.

Identity Proofing Level 2 Plus (IP 2 Plus) is used when a medium level of confidence in the claimed *Identity* is needed. This requires two or more *Identity Documents* to verify someone's claim to an existing *Identity* and requires the *Binding Objective* to be met. The intended use of *Identity Proofing Level 2 Plus* is for services where the risks of getting *Identity* verification wrong will have moderate-high consequences to the *Individual* or the service. For example, undertaking large financial transactions. Source: TDIF.

Identity Proofing Level 3 (IP 3) is used when a high level of confidence in the claimed *Identity* is needed. This requires two or more *Identity Documents* to verify someone's claim to an existing *Identity* and requires the *Binding Objective* to be met. The intended use of *Identity Proofing Level 3* is for services where the risks of getting *Identity* verification wrong will have high consequences to the *Individual* or the service. For example, access to welfare and related government services. Source: TDIF.

Identity Proofing Level 4 (IP 4) is used when a very high level of confidence in the claimed *Identity* is needed. This requires four or more *Identity Documents* to verify someone's claim to an existing *Identity* and the *Individual* claiming the *Identity* must

attend an in-person interview as well as meet the requirements of *Identity Proofing Level 3*. The intended use of *Identity Proofing Level 4* is for services where the risks of getting *Identity* verification wrong will have a very high consequence to the *Individual* or the service. For example, the issuance of government-issued documents such as an Australian passport. Source: TDIF.

IdP Selection. The method or process of an *Identity Exchange* that allows an *Individual*, when obtaining a service from a *Relying Party*, to select an *Identity Service Provider* from a list of *Identity Service Providers* that are integrated with the *Identity Exchange*. Source: TDIF

Identity Service Provider (IdP). One of the four *Accredited Roles*. An entity that has been accredited in accordance with the TDIF as an identity service provider and that provides a service that generates, manages, maintains or verifies information relating to the identity of *Individuals*. Source: TDIF.

Identity system.

1. An online environment for *Identity* management transactions governed by a set of system rules (also referred to as a trust framework) where *Individuals*, organisations, services and devices can trust each other because authoritative sources establish and authenticate their identities. Source: UNCITRAL.
2. the facility through which an *Applicant* or *Accredited Provider* provides the services for which it is accredited. Source: TDIF²

IdP-CSP communications. Communications between an *Identity Service Provider* and a *Credential Service Provider*. Source: TDIF

IdP filtering. The process by which an *Identity Exchange* determines the available *Identity Service Providers* that can service an authentication request from a *Relying Party*. Source: TDIF.

IdP Link. This is a *Pairwise Identifier* that links the *Identity* for an authenticated user at an IdP with the *Digital Identity* brokered by an *Identity Exchange*. This identifier is generated by the *Identity Service Provider*. Source: TDIF.

² Where a requirement refers to an *Identity System*, the latter definition will be used.

ID Token. A JSON Web Token that contains claims about an *Authentication Event*. It may contain other claims. Used in the *OIDC Federation Protocol*. Source: *OpenID Connect Core 1.0*

Image Quality Profile. For a facial image, the static and dynamic characteristics of the subject and the processes used to acquire the image.

Note Examples of characteristics include the image background, resolution, size, brightness, the subject's pose and whether they have open eyes and/or mouth.

Implied Consent. *Implied Consent* arises when *Consent* may reasonably be inferred in the circumstances from the conduct of the *Individual* and the *APP entity*. Source: OAIC.

Incident Response Plan (IRP). A plan for responding to cyber security incidents. Source: ISM.

Individual. A natural person (i.e. human). Source: *Acts Interpretation Act 1901*.

Information Commissioner. means the person appointed under section 14 of the *Australian Information Commissioner Act 2010 (Cth)* as the Australian Information Commissioner. Source: *Australian Information Commissioner Act 2010 (Cth)*.

Information Security Manual (ISM). See *Australian Government Information Security Manual*.

Internal system user. An employee, secondee or third party authorised by the *Accredited Provider's* organisation or agency to access and perform functions on the *Identity* service. E.g. a system administrator. Source: *TDIF*. See also: *Assessing Officer, Personnel*.

Issuing Authority. See: *Identity Document Issuer*.

K, L

Key. See: *Cryptographic Key (key)*.

Key Holder. See: *Individual*

Key Pair. A pair of asymmetric *Cryptographic Keys* (e.g. one decrypts messages which have been encrypted using the other) consisting of a *Public Key* and a *Private Key*. Source: TDIF.

Known Customer. An *Individual* whose *Identity* has previously been verified by another trusted organisation or previously by the same organisation. Where the person already possesses recognised *Credentials* at the desired *Identity Proofing Level*, authentication of this *Credential* may be accepted as a substitute for all or part of the *Identity Proofing* process. Source: NIPG. See also: *End User*, *User*.

Knowledge Based Authentication. See: *Shared Secrets*.

Legitimacy Objective: This is an objective of *Identity Proofing*, which ensures that the *Identity* has been genuinely created as well as confirming that there is continuity in an *Individual's Identity Attributes* where there have been changes. Source: DTA.

Level A presentation attack species. Means a category of presentation attack instruments which:

- have an elapsed creation time equal to or less than one day;
- can be created or undertaken by a layperson;
- can be undertaken with standard equipment; and
- involves a source of biometric information which is easy to obtain.

Note An example of biometric information which is easy to obtain includes a photo from social media or voice recording.

Level B presentation attack species. Means a category of presentation attack instruments which:

- have an elapsed creation time equal to or less than seven days;
- can be created or undertaken by a person who has the required expertise to do so;
- can be undertaken with standard or specialised equipment; and
- involves a source of biometric information which is moderately difficult to obtain.

Note An example of biometric information which is moderately difficult to obtain includes a stolen fingerprint image or voice recording of a specific phrase.

Levels of Assurance. See: *Identity Proofing Level* and *Credential Level*

Linking document. A document which demonstrates the continuity of the claimed *Identity* where *Attributes*, such as name or date of birth, have changed. Source: *TDIF*.

Liveness detection. Measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, in order to determine if a biometric sample is being captured from a living subject present at the point of capture. Source: *ISO 30107-1*. See also: *Presentation Attack Detection*.

Local Biometric Binding. *Biometric Binding* of an *Individual* performed by, and in the physical presence of, an *Assessing Officer*. Source: *TDIF*.

Look-Up Secret. Is a physical or electronic record that stores a set of secrets shared between the *User* and the *Credential Service Provider*. Source: *NIST*.

M

Major Production Release. A new version of software forming part of an *Identity System* that:

- includes changes to the underlying architecture;
- results in new or enhanced features of the *Identity System*; or
- results in new or enhanced functionality of the *Identity System*. Source: *TDIF*.

Malicious Actor. An entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact – an organisation's security. Also referred to as an *attacker*. Source: *ASD*

Manual Face Comparison. The process of using *Visual Verification* to compare the likeness of a physically present user to the *User's Claimed Photo ID*. Source: *TDIF*. See also: *Local Biometric Binding*, *Remote Manual Face Comparison*

MAY. Means truly optional. This requirement has no impact on an *Applicant's* ability to achieve or maintain *TDIF* accreditation if it is implemented or ignored. Source: *TDIF*.

Memorandum of Understanding (MOU). A non-legally binding agreement between two or more parties which expresses the terms and intended common action of the parties. Source: *TDIF*.

Memorised secret. A secret value chosen and memorised by the *User*, such as a password or, if numeric, a PIN. Source: *TDIF*.

Metadata. See: *System Metadata*.

Multi-entity Identity Systems. Organisations that provide components of an *Identity System* that work together to perform the functions of one of the *Accredited Roles*. Source: *TDIF*

Multi-factor authentication. An authentication protocol that relies on more than one authentication factor for successful authentication. Source: *NeAF*.

Multi-factor cryptographic (MF Crypto) (device). A hardware device that performs cryptographic operations using one or more protected cryptographic keys and requires activation through a second authentication factor. Although cryptographic devices contain software, they differ from cryptographic software *Credentials* in that all embedded software on the hardware device is under the control of the *CSP* or issuer. Source: *TDIF*.

Multi-factor cryptographic (MF Crypto) (software). A cryptographic key stored on disk or some other "soft" media that requires activation through a second authentication factor. Source: *TDIF*.

Multi-factor One-Time Password (MF OTP). A device or software that generates *OTPs* that requires activation through a second authentication factor. Source: *TDIF*.

Note: This includes hardware devices and software-based *OTP* generators on devices such as mobile phones. The *OTP* is displayed on the device and input or transmitted by a person, proving possession and control of the device.

MUST. Means an absolute requirement of the *TDIF*. Failure to meet this requirement will impact the *Applicant's* ability to achieve and maintain *TDIF* accreditation. Source: *TDIF*.

MUST NOT. Means an absolute prohibition of the *TDIF*. Failure to prevent this prohibition from occurring will impact the *Applicant's* ability to achieve and maintain *TDIF* accreditation. Source: *TDIF*.

N

National e-Authentication Framework (NeAF). A risk-based approach applied to identify and authenticate *Individuals* to a desired level of assurance for online interactions. Source: *NeAF*.

National Identity Proofing Guidelines (NIPG). The Council of Australian Governments' national guidelines for *Identity Proofing*. The *TDIF Identity Proofing* requirements are broadly based on the *NIPG*. Source: *NIPG*.

National Relay Service. Is an Australian Government initiative that allows people who are deaf, hard of hearing and/or have speech impairment make and receive phone calls. Source: *DITRDC*

National Terrorism Threat Level. A scale of five levels that tells the public about the likelihood of an act of terrorism occurring in Australia. The levels are 'Not Expected', 'Possible', 'Probable', 'Expected' and 'Certain'. The *National Terrorism Threat Level* also provides an indicator to government agencies enabling them to respond appropriately with national threat preparedness and response planning. Source: Commonwealth Department of Home Affairs.

Need-to-know. The principle of restricting an *Individual's* access to only the information they require to fulfil the duties of their role. Source: *ISM*.

Non-person entity. An entity with a digital identity that acts in cyberspace but is not a human actor. This can include organisations, hardware devices, software applications and information artifacts. Source: *NIST*. See also: *Entity*.

Notification of Collection. A notice to a *Person* by an *Entity* that the *Entity* is collecting the *Personal Information* of the *Person*. Source: *Privacy Act 1988 (Cth)*

O

Officer. Has the meaning given in section 9 of the *Corporations Act 2001*.

OFFICIAL information. All information created, sent or received as part of the work of the Australian Government. This information is an official record and it provides

evidence of what an entity has done and why. *OFFICIAL information* can be collected, used, stored and transmitted in many forms including electronic, physical and verbal (e.g. conversations and presentations). The *PSPF* requires entities to implement operational controls to protect information holdings in proportion to their value, importance and sensitivity. All *OFFICIAL information* requires an appropriate degree of protection as information (and assets holding information) and subject to both intentional and accidental threats. The Australian Government Attorney General's Department recommends entities apply the minimum protections outlined in the *PSPF* for *OFFICIAL information* that is not assessed as being sensitive or security classified information. Source: *PSPF*.

One-Time Password (OTP). A password that is changed each time it is required. Source: *NeAF*.

One-to-many Matching. The process of comparing a *Biometric Sample* against a database of *Biometric Information* to find and return *Biometric Information* attributable to a single individual. Source: *TDIF*.

Online Biometric Binding. *Biometric Binding* performed remotely via the Internet. Source: *TDIF*.

Online Certificate Status Protocol. An *Online Certificate Status Protocol* specifies a mechanism used to determine the status of *Digital Certificates*, in lieu of using *Certificate Revocation Lists*. Source: *TDIF*. See also: *Certificate Revocation Lists*

OpenID Provider (OP). OAuth 2.0 Authorization Server that is capable of authenticating the *User* and providing claims to a *Relying Party* about the *Authentication Event* and the *User*. Source: *OpenID Connect Core 1.0 Specification*.

Operating Rules (OR). Sets out the legal framework for the operation of an *Identity Federation*, including key rights, obligations and liabilities of *Participants*. Source: *TDIF*.

Operation Objective: This is an objective of *Identity Proofing*, which provides additional confidence that an *Individual's Identity* is legitimate in that it is being used in the community (including online where appropriate). Requiring a pattern of use over a

period of time implies that the *Individual's Identity* has a history and reduces the risk that it is fraudulent. Source: *DTA*

Operations Manual: A manual describing the management of an *Applicant's* operations. For the contents of this manual see section 2.2 of the *TDIF: 05 Role Requirements*. Source: *TDIF*.

Out-of-band device. A physical device that uses an alternative channel for transmitting information Source: *TDIF*.

Note For example, an SMS to send a PIN or one-time password.

Oversight Authority (OA). The entity responsible for the administration and oversight of the *Australian Government's Identity Federation* in accordance with *MOUs* and the *TDIF*. Source: *TDIF*.

P, Q

Pairwise Identifier: Identifier that identifies a *User* at either the *Identity Exchange* or *Relying Party* which made an authentication request that cannot be correlated with another *Participant's Pairwise Identifier*. Source: *TDIF*

Participant. *Accredited Providers* and *Relying Parties* that operate in an *Identity Federation*. Source: *TDIF*

Passphrase. A sequence of words used for authentication. Source: *ISM*.

Password. A sequence of characters used for authentication. Source: *ISM*.

Penetration test. A *penetration test* is designed to exercise real-world targeted cyber intrusion scenarios to achieve a specific goal, such as compromising critical systems or information. Source: *ISM*.

Person. Expression used to denote generally (such as 'person', 'party', 'someone', 'anyone', 'no-one', 'one', 'another' and 'whoever'), include a body politic or corporate as well as an *Individual*. Source: *Acts Interpretation Act 1901*. See also: *Individual*.

Personal Information. Information or an opinion about an identified *Individual*, or an *Individual* who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.

Personal Information in the *TDIF* includes:

- an *attribute* of an *Individual*;
- a *restricted attribute* of an *Individual*; and
- *Biometric information* of an *Individual*.

Source: Section 6 of the *Privacy Act 1988* (Cth);

Personnel (of an entity).

- An officer or employee of the entity; or
- an individual who, under a labour hire or similar arrangement with the entity, performs work for the entity in relation to the services for which the entity is accredited.

Photo ID (document). Photographic Identification (Photo ID). An *Identity* document with *Attributes* and includes a facial image of the *Identity* document holder that are verifiable with an *Authoritative Source*. Source: *TDIF*. See also: *Claimed Photo ID*.

Presentation Attack (against a biometric system). Presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system. Source: ISO 30107. See also: *Presentation Attack Detection*.

Presentation Attack Detection (PAD). The automated detection of a presentation attack. Source: ISO 30107. See also: *Liveness Detection*, *Presentation Attack Detection*.

Presentation Attack Instrument (PAI). An object or biometric characteristic that is used in a *Presentation Attack*.

Presentation Attack Instrument Species (PAIS). A class of *Presentation Attack Instrument* created using a common production method and based on different biometric characteristics.

Privacy Assessment. A process used by an *Applicant* to demonstrate compliance with the *TDIF* privacy requirements, address all recommendations arising from a *Privacy Impact Assessment* and document results of the *Privacy Assessment* in a report. Source: *TDIF*.

Privacy Champion. Is a senior official within the agency who has the functions of:

- a. Promoting a culture of privacy within the agency that values and protects personal information.
- b. Providing leadership within the agency on broader strategic privacy issues.
- c. Reviewing and/or approving the agency's *Privacy Management Plan*, and documented reviews of the agency's progress against the *Privacy Management Plan*.
- d. Providing regular reports to the agency's executive, including about any privacy issues arising from the agency's handling of personal information.

Source: Privacy (Australian Government Agencies – Governance) *APP Code 2017*.

Privacy Impact Assessment (PIA). A systematic assessment of a project that identifies the impact that the project might have on the privacy of *Individuals*, and sets out recommendations for managing, minimising or eliminating that impact. Source: OAIC.

Privacy Management Plan. is a document that:

- a. Identifies specific, measurable privacy goals and targets.
- b. Sets out how an agency will meet its compliance obligations under APP 1.2.

Source: *Australian Government Agencies Privacy Code*.

Privacy Policy. Has the meaning given by APP 1.3. Source: *Privacy Act 1988*.

Privacy Officer. The first point of contact for privacy matters within an agency and is responsible for ensuring day-to-day operational privacy activities are undertaken.

Source: OAIC.

Private Key. The Private Key in an asymmetric *Key Pair* that must be kept secret to ensure confidentiality, integrity, authenticity and non-repudiation. Source: *TDIF*. See also: *Key Pair, Public Key, Key*.

Protective security documentation. The minimum set of documents that an *Applicant* develops as part of meeting its protective security obligations of *TDIF* accreditation. Source: *TDIF*.

Public Key. The *Key* in an asymmetric *Key Pair* which may be made public. Source: *TDIF*. See also: *Key Pair, Private Key, Key*.

Public Key Infrastructure (PKI). The combination of hardware, software, people, policies and procedures needed to create, manage, store and distribute keys and certificates based on public key cryptography. Source: Gatekeeper PKI Framework.

Public Key Technology (PKT). The hardware and software used for digital encryption, digital signing and digital verification of digital certificates. Source: Gatekeeper PKI Framework.

Qualifying Attestation Letter. A formal letter from the Applicant's *Accountable Executive* and addressed to the DTA attesting to the *Applicant's* compliance with all obligations under the TDIF. This letter is submitted to the DTA at the end of initial accreditation and an Applicant's Annual Assessment. Source: TDIF

R

Rate Limiting (throttling). A control to protect *credentials* against online guessing attacks by limited the number of consecutive failed *Authentication* attempts on a single *Digital Identity*. Source: TDIF

Registration Authority (RA). See: *Identity Service Provider*

Registries of Births, Deaths and Marriages (RBDM). Register a birth, apply for a certificate, change your name or search your family history. The registration of births, deaths and marriages, changes of name, changes of sex, adoptions and provision of certificates is the responsibility of the state and territory governments in Australia. Source: Australian Government.

Relying Party (RP). An entity that relies, or seeks to rely, on *Attribute* of an *Individual* that are provided by *Identity Service Providers* or *Attribute Service Providers* to:

- Provide a service to the *Individual*; or
- Enable the *Individual* to access a service.

Source: TDIF

Replay resistance. Protection against the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorised effect or gaining unauthorised access. Source: NIST

Requirements Traceability Matrix (RTM). A written record of the links between the *TDIF requirements* and evidence provided by the *Applicant* to verify and validate those requirements. Source: *TDIF*

Restricted Attributes. Attributes that are collected by an *Identity Service Provider* but cannot be shared unless permission is sought from the *DTA* to do so. Source: *TDIF*.

Restricted Credentials. A *credential* that the *CSP* identifies as having additional risk of false acceptance associated with its use and is therefore subject to additional requirements. Source: *NIST*.

Risk Assessment. The systematic, iterative and collaborative process of risk identification, risk analysis and risk evaluation. Source: *ISO 31000:2018*.

Note A risk assessment should use the best available information, supplemented by the views of stakeholders and further enquiry as necessary. See the guidelines outlined in *ISO 31000:2018* for recommended Risk assessment practise.

Risk management framework. A set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation. Source: *ISO 31000:2018*.

Risk tolerance. The levels of risk taking that are acceptable in order to achieve a specific objective or manage a category of risk. Source: *ISO 31000:2018*.

Road Traffic and Transport Authorities (RTA). State and territory governments have responsibility for roads and road transport within their jurisdiction. Their websites may include information about traffic and road conditions, road construction, road rules, and road safety, as well as vehicle registration and licensing. Source: Australian Government.

Root Certification Authority (Root CA). A Certification Authority that is the top most *Certification Authority* in a trust hierarchy. Source: *TDIF*

RP Link. This is a *Pairwise Identifier* that links the *Digital Identity* brokered by an *Identity Exchange* to the service record at a *Relying Party*. The *Identity Exchange* generates this identifier. Source: *TDIF*.

S

Security assessment. An activity undertaken to assess security controls for a system and its environment to determine if they have been implemented correctly and are operating as intended. Source: *ISM*.

Serious and complex fraud. Fraud which, due to its size or nature, is considered too complex for most entities to investigate. Source: *CFCF*.

Session. Allows an *Individual* to continue accessing the service across multiple subsequent interactions without requiring repeated authentication. Source: *TDIF*.

Session Termination Event. The event that brings an *Authenticated Session* to an end.

Note The session could terminate after a specific period, or on the occurrence of a specific event such as the user closing the browser or logging out of the account.

Shared Secret. A secret used in authentication that is known to the *User* and the *CSP*. Source: *TDIF*.

Sighting. The examination of a document by a trained *Assessing Officer* to confirm the authenticity of the *Identity* document. Source: *TDIF*. See also: *Manual Face Comparison*.

Single-factor authentication. An authentication protocol that relies on only one authentication factor for successful authentication. Source: *TDIF*.

Single-factor cryptographic (SF Crypto) (software). A cryptographic key stored in some form of 'soft' media. Source: *TDIF*.

Single-factor cryptographic (SF crypto) device. A hardware device that performs cryptographic operations using one or more protected cryptographic keys and is authenticated by proving possession and control of the key. Although cryptographic devices contain software, they differ from cryptographic software *Credentials* in that all embedded software on the hardware device is under the control of the CSP or issuer. Source: *TDIF*.

Single-factor One-Time Password (SF OTP) (device). A device that generates *OTPs*, including hardware devices (e.g. a dongle), *SMS* or software-based *OTP*

generators installed on devices such as mobile phones. The *OTP* is displayed on the device and input or transmitted by a person. Source: *TDIF*.

Single Logout. *Single Logout (SLO)* refers to the ability for a user to initiate a logout process for all *Relying Parties* that relied on a single logon session for the *User* at an *Identity Exchange*. Source: *TDIF*.

Single Sign-on. *Single Sign-on (SSO)* refers to the ability for a *User* to make use of their *Digital Identity* at multiple services in a short period of time, with only a single *User Authentication*. Source: *TDIF*.

Source Biometric Matching. The process of using a *Photo ID Authoritative Source* to verify that a *User's Acquired Image* biometrically matches the corresponding image recorded against that *Identity* from the *Photo ID Authoritative Source*. Source: *TDIF*. See also: *Source Verification*.

Source Verification. The act of verifying physical or electronic *EoI* directly with the *Identity Document Issuer* (or *Authoritative Source* for such document e.g. via an *Identity Matching Service*). Source: *TDIF*. See also: *Biometric Matching*

Statement of Applicability (SoA). The list of protective security controls implemented by an *Applicant* for their *Identity System*. The *Statement of Applicability* forms the basis of the *Applicant's* security assessment. Source: *TDIF*

Step-Up. A process where the level of assurance of an *Individual's Identity* is increased from one *Identity Proofing Level* to another, or an *Individual's Credential* is increased from one *Credential Level* to another. Source: *TDIF*.

Strategies to Mitigate Cyber Security Incidents. Is a document created by the Australian Signals Directorate's Australian Cyber Security Centre to help cyber security professionals in all organisations mitigate cyber security incidents caused by various cyber threats. Source: *ASD*

System Metadata. Data relating to a *User* and their interaction with an *identity system* that is generated by an *identity system*. Metadata does not include personal information. Source: *TDIF*.

System Security Plan (SSP). A document that describes a system and its associated security controls. Source: *ISM*.

T

TDIF: 01 – Glossary of Abbreviations and Terms. Includes a list of acronyms and a definition of key terms used in the *TDIF*. Source: *TDIF*.

TDIF: 02 – Overview. Provides a high-level overview of the *TDIF*. Source: *TDIF*.

TDIF: 03 – Accreditation Process. Sets out the process and requirements an *Applicant* is required to complete to achieve *TDIF* accreditation. Source: *TDIF*.

TDIF: 04 – Functional Requirements. Includes requirements applicable to the *Accredited Roles*, including fraud control, privacy, records management, protective security and user experience. 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 *Accessibility Assessment* against the *Web Content Accessibility Guidelines*. Source: *TDIF*.

TDIF 04A – Functional Guidance. Provides guidance to *Applicants* on meeting the requirements set out in *TDIF: 04 Functional Requirements*. Source: *TDIF*.

TDIF 05 – Role Requirements. Includes user terms and lifecycle management requirements applicable to the *Accredited Roles*. Source: *TDIF*.

TDIF 05A – Role Guidance. Provides guidance to *Applicants* on meeting requirements set out in *TDIF: 05 - Role Requirements*. Source: *TDIF*.

TDIF 06 – Federation Onboarding Requirements. 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 technical integration testing, operating obligations and the accreditation requirements for an *Identity Exchange*. Source: *TDIF*.

TDIF 06A – Federation Onboarding Guidance. Provides guidance to *Applicants* on meeting requirements set out in the *TDIF: 06 Federation Onboarding Requirements*. Source: *TDIF*.

TDIF 06B - OpenID Connect 1.0 Profile. Describes how OpenID Connect 1.0 is used within the *Australian Government's identity federation*. Source: *TDIF*.

TDIF 06C - SAML 2.0 Profile. Describes how SAML2.0 is used within the *Australian Government's identity federation*. Source: *TDIF*.

TDIF 06D – Attribute Profile. Describes the *Attributes* disclosed across the *Australian Government's identity federation* and how these are mapped in the OpenID Connect 1.0 Profile and SAML 2.0 Profile. Source: *TDIF*.

TDIF 07 - Maintain Accreditation. 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. Source: *TDIF*.

TDIF Accreditation Criteria. A *TDIF* requirement an organisation is required to meet. Source: *TDIF*. Source: *TDIF*.

TDIF Accreditation Process. The accreditation process which involves a combination of documentation requirements, third party evaluations and operational testing that *Applicants* must complete to the satisfaction of the *DTA* in order to achieve *TDIF* accreditation. Source: *TDIF*.

TDIF Accreditation Register. A register of *TDIF Accredited Providers*. Source: *TDIF*.

TDIF Application Letter. A formal application letter addressed to the *DTA* seeking *TDIF* accreditation. Source: *TDIF*.

TDIF Exemption Request. A formal request to the *DTA* seeking exemption against a *TDIF* requirement. Source: *TDIF*.

TDIF Reaccreditation. When an *Entity* that has already undergone *Accreditation* goes through *Accreditation* again. Source: *TDIF*.

Technical Biometric Matching. The use of an algorithm to determine that the *User's Acquired Image* biometrically matches a corresponding image read from a *Photo ID*

which has been *verified* using *Technical Verification*. Source: TDIF. See also: *Technical Verification*

Technical testing. A way of testing an *Identity System* through executing the user flows, user interactions and component interactions to ensure that the system has all the required functionality specified in the *TDIF*. Source: *TDIF*.

Technical Test Report. A report that demonstrates testing has been executed in accordance with the approved test plan. It outlines the status of all test cases (including the execution coverage and defects), test completion criteria (for criteria that has been met) and a risk assessment against criteria that have not been met. Source: *TDIF*.

Technical Verification. The act of verifying physical or electronic evidence using *Approved Cryptography* bound to a secure chip or appended to it (e.g. via *Public Key Technology*). Source: *TDIF*.

Trust Framework. A term used to define the scope and purpose of the *Identity System*. It 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*. Source: *OIX*.

Trusted Digital Identity Framework (TDIF). . The *Trusted Digital Identity Framework (TDIF)* is an accreditation framework for *Digital Identity* services. It sets out the requirements that *Applicants* need to meet to achieve *accreditation* including (but not limited to) privacy, fraud and security control, accessibility and usability, system testing, risk management, *Identity Proofing* and *Credential* management. The *TDIF* also includes guidance material and templates to support *Applicants* to meet *TDIF* requirements. Source: *TDIF*.

Trusted referee. A *trusted referee* is a person or organisation that holds a position of trust in the community and does not have a conflict of interest, such as an Aboriginal elder or reputable organisation that the person is a customer, employee or contractor of, and is known and listed by the enrolling agency to perform the function of a referee. The *Statutory Declarations Act 1959* provides a list of people who hold a position of trust in the community. Similar lists are also generally included in state and territory

legislation. *Trusted referees* may also include guardians or other people nominated to act on a person's behalf, whose identities have been verified. Source: *NIPG*.

U

Unique in context. The ability to distinguish *Digital Identities* from one another and that the right service is delivered to the right *Person*. Source: *TDIF*.

Uniqueness Objective. Confirms uniqueness of an *Identity*. To ensure that digital identities can be distinguished from one another and that the right service is delivered to the right person. Source: *DTA*.

Usability Test Plan. A Plan that outlines how usability testing will be conducted. Source: *TDIF*.

Use in the Community (UitC) (document). A government issued document, or a document issued by a reliable and independent source used to demonstrate the use of an *Individual's Identity* in the community over time. (e.g. a Medicare card). Source: *TDIF*.

User. An *Individual* who uses or interacts with an *Accredited Provider's Identity System* to:

- create or maintain a *Digital Identity*; or
- obtain a service from a *Relying Party*.

Source: *TDIF*. See also: *End User*.

User Agent String. Identifies the browser and operating system of an attempted system request. Source: *TDIF*

User Dashboard. A collective term for the feature that an *Identity Exchange* provides for a *User* to view their consumer history and manage their interactions with *Relying Parties*. Source: *TDIF*

User Researcher. An independent evaluator with expertise in understanding *User* behaviours, needs, and motivations through observation techniques, task analysis, and other feedback methodologies. Source: *DTA*.

V, W, X, Y, Z

Validation (in an *Identity Proofing* context). A check that an *Attribute* exists and is under the control of a *known Individual*. Source: *TDIF*.

Note For example an SMS activation code being sent to a mobile phone number to confirm control of the associated phone number.

Verification (in an *Identity Proofing* context). Confirmation, through *Technical Verification*, *Source Verification*, or *Visual Verification*, that an *Identity Attribute* exists and is legitimate. Source: *TDIF*. See also: *Technical Verification*, *Source Verification*, *Visual Verification*

Visual Verification. The act of a trained member of *Personnel* of an *Accredited Provider* visually confirming the physically presented *EoI* document appears to be valid and unaltered. Source: *ISM*. See also: *Local Biometric Binding*, *Sighting*.

Vulnerability assessment. A *Vulnerability Assessment* can consist of a documentation-based review of a system's design, an in-depth hands-on assessment or automated scanning with software tools. In each case, the goal is to identify as many security vulnerabilities as possible. Source: *ISM*.

Web Content Accessibility Guidelines (WCAG). Covers a wide range of recommendations for making Web content more accessible. Following these guidelines will make content accessible to a wider range of people with disabilities, including blindness and low vision, deafness and hearing loss, learning disabilities, cognitive limitations, limited movement, speech disabilities, photosensitivity and combinations of these. Source: W3C.