Australian Government

Digital Identity

01 Glossary of Abbreviations and Terms

Trusted Digital Identity Framework

Release 4 October 2021, Version 1.4

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 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@dta.gov.au.

Document management

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

Change log

Version	Date	Author	Description of the changes
0.1	July 2019	SJP	Initial version (removed from the previously titled *TDIF* Overview and Glossary)
0.2	Sep 2019	SJP	Updated to incorporate feedback provided by key stakeholders during the first round of collaboration on *TDIF* Release 4
0.3	Dec 2019	SJP	Updated to incorporate feedback provided by key stakeholders during the second round of collaboration on *TDIF* Release 4
0.4	Mar 2019	AV, MC, SJP	Updated to incorporate feedback provided during the third round of consultation on *TDIF* Release 4
1.0	May 2020		Published version
1.1	Sept 2020	MC	Updated to incorporate IP3 changes in the Role Requirements document.
1.2	Feb 2021	JK	CRID0001 – Style edit, grammar changes, new defined terms added, abbreviations added. CRID0002 – minor definition changes, style update.
1.3	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	Oct 2021	JK	CRID0027 – Emergency changes to glossary

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

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

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

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

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

Term	Meaning
SAML	Security Assertion Mark-up Language
SF	Single Factor
SF OTP	Single Factor One Time Password
SHA	Secure Hashing Algorithm
SMS	Short Message Service
SoA	Statement of Applicability
SOP	Standard Operating Procedure
SP	Special Publication
SRMP	Security Risk Management Plan
SSO	*Single Sign On*
SSP	System Security Plan
TDIF	Trusted Digital Identity Framework
TLS	Transport Layer Security
TPISAF	Third Party Identity Services Assurance Framework
UitC	Use in the Community (document)
UNCITRAL	United Nations Commission on International Trade Law
URN	Uniform Resource Name
W3C	World Wide Web Consortium
WCAG	Web Content Accessibility Guidelines
XML	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 Authority. A senior executive designated within an *Applicant* or *Accredited Provider's* organisation responsible for managing aspects of its *Identity System*. Source: *TDIF*.

***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*. Source: *TDIF*. See also: *Applicant.*

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

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

Annual Assessment. Details the *Accredited Provider's Identity System* compliance against *TDIF* requirements. This includes areas of compliance and non-compliance against the *TDIF* and any suggested remediation actions. Source: *TDIF*.

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.

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). The *Internal System User* who is specifically involved with assessing *User Applications* and making a decision about the *Identity Claim*. Source: TDIF. See also: *Internal System User, Personnel*.

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). An entity that has been accredited in accordance with the TDIF as an attribute service provider and that verifies specific attributes relating to entitlements, qualifications or characteristics of an individual (for example, this Joe Bloggs is authorised to act on behalf of business XYZ in a particular capacity).

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 Identity Federation. An *Identity Federation* which is managed by the Australian Federal 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 (AACA). 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. *AACA*s 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. An encrypted communication channel that uses approved cryptography (*AACA* or *AACP)* where the client connection has authenticated to the server. Source: *TDIF*.

Authentication. A function for establishing the validity and assurance 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. See: *Authentication.*

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 one *Participant* to another *Participant* using a *Federation Protocol*. 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*

Binding (at enrolment). See: *Credential Binding*

Biometric Binding. The process, under the *TDIF*, of linking a biometric with a validated *Identity*, for instance by performing a biometric verification of the face recorded on the *Acquired Image* of the *User* with the face recorded on the relevant *Photo ID*. Source: *TDIF*. See also: *Biometric Verification, Biometric Matching.*

***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. (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 identification 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 verification. The process of performing a one-to-one biometric match of an individual against an *Identity* claim. 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 (CoI) (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 records[1]. 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

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

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*

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*. The *User* possesses the *Credential* and controls its use through one or other authentication protocols. A *Credential* may incorporate a password, cryptographic key or other form of secret. Source: *NIPG*.

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, ranked from lowest to highest based on the consequence of incorrectly determining that an *Individual* is who they claim they are. 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 *TDIF* Accredited Roles. *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 *Identity Service Provider*. 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 a cryptographic algorithm (*AACA*) 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 for dealing with impersonation attacks developed by a *Credential Service Provider*. Source: *TDIF*

Cyber Security Incident. An unwanted or unexpected cyber security event, or a series of such events, that have significant probability of compromising business operations. Examples include:

- Receiving suspicious or seemingly targeted emails with attachments or links.
- Any compromise or corruption of information.
- Unauthorised access or intrusion into an *Identity* service.
- Data spill.
- Intentional or accidental introduction of viruses to a network.
- Denial of service attacks.
- Suspicious or unauthorised network activity.

Source: *ISM*.

D

***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* (ecosystem deduplication). Source: *TDIF*.

Digital Certificate. See: *Certificate*

Digital Identity. An electronic representation of an *Entity* which enables that *Entity* to be sufficiently distinguished when interacting online. 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 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 Identity Federation* 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*.

Entity. Something that has separate and distinct existence and that can be identified in a context. Note: an entity can be a physical person, an organisation, an active or passive thing, a device, a software application, a service, etc. Source: *ITU-T* Rec X.1252.

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-scape 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*.

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: *OAIC*.

F

Face Verification Service (FVS). A national online system that compares a photo against the image used on *Identity* documents. The FVS can:

- Make access to government services more convenient for customers by avoiding the need to attend a shopfront.
- Help victims of *Identity* crime reclaim their *Identity* faster.
- Help prevent *Identity* theft by detecting fake or stolen documents.

Source: ID Match (Australian Government Department of Home Affairs).

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). If an error occurs while acquiring the biometric sample during a verification or identification attempt, it is known as a failure to acquire. The proportion of verification or identification attempts that fail for this reason is the failure to acquire rate (*FTA*). Source: *TDIF*.

***Failure to Enroll Rate (FTE)*:** If failure occurs during enrollment, it is known as a failure to enroll. The proportion of enrollment transactions that fail is known as the failure to enroll rate (*FTE*). Source: *TDIF*.

False Match Rate (FMR): An imposter match that is declared to be a match due to the match receiving a match score above the match threshold. The proportion of imposter matches that are falsely matched is known as the false match rate (*FMR*). Source: *TDIF*.

***False Non-match Rate (FNMR)*:** A genuine match that is declared to be a non-match due to the match receiving a match score below the match threshold. The proportion of genuine matches that are falsely non-matched is known as the false non-match rate (FNMR). Source: *TDIF*.

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.*

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.*

Fraud Control Plan. Documents the approach to controlling fraud at a strategic, operational and tactical level and includes details on how entities raise awareness and training that is available. Source: *AGD*

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*.

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 *TDIF Accredited Roles*. An *Identity Exchange* conveys, manages and coordinates the flow of *Identity Attributes* and *Assertions* between members of an *Identity Federation*. Source: *TDIF*.

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 fraud. The gaining of money, goods, services or other benefits or the avoidance of obligations using a fabricated, manipulated, stolen or otherwise fraudulently assumed *Identity*. Source: *NIPG*.

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 define and confirm their *Identity*. Source: *TDIF*.

Identity Proofing Level. An *IP* level describes the level of assurance or confidence in the *Identity Proofing* process ranked from lowest to highest based on the consequence of incorrectly identifying an *Individual*. 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* to select an *Identity Service Provider* from a list of *Identity Service Providers* that are integrated with the *Identity Exchange* when accessing a *Relying Party.* Source: *TDIF*

Identity Service Provider (IdP). One of the four *TDIF Accredited Roles*. An *Identity Service Provider* creates, maintains and manages *Identity* information of *Individuals* and offers identity-based services. Source: *TDIF*.

Identity system. 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.

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 Provider*s 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*.

***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*

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 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

Key Holder. See: *Individual*

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.*

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. A type of presentation attack detection that measures and analyses anatomical characteristics and involuntary or voluntary reactions. It is used to determine if a biometric sample captured from a living subject is present at the point of capture. Source ISO 30107. See also: *Presentation Attack Detection.*

Local Biometric Binding. Biometric binding performed by the *Assessing Officer* with the *User* in the physical presence of the *Applicant*. Source: *TDIF*.

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

M

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 visually verifying that the physically present *User's* likeness matches the corresponding image recorded in the *Individual's* 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. Commonly referred to as a password or, if numeric, a PIN, is a secret value chosen and memorised by the *User*. 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 *TDIF 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 (either something a person knows or something a person is). 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 (either something a person knows or something a person is). Source: *TDIF*.

Multi-factor One-Time Password (MF OTP). A trusted device that generates *OTPs* as part of an authentication activity. This includes hardware devices and 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, proving possession and control of the device. Source: *TDIF*.

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

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*.

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 – e.g. an SMS to send a PIN or one-time password. Source: *TDIF*.

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

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 includes sensitive information.
Source: Section 6 of the *Privacy Act 1988* (Cth)

Personnel. Any member of an *Applicant's* staff or contracted service providers staff used to service the *Applicant's* contracts, or other *Individuals* who provide services to the organisation or access the *Applicant's* information or assets as part of sharing initiatives. Source: *TDIF.* See also: *Assessing Officer, Internal System User.*

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.*

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 an *Identity System* that identifies the impact that the *Identity System* 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.

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 organisation or government agency that relies on verified *Attributes* or *Assertions* provided by *Identity Service Providers* and *Attribute Service Providers* through an *Identity Exchange* to enable the provision of a digital service. Source: *TDIF*.

Remote Manual Face Comparison. The process of *Manual Face Comparison* performed at another location utilising images or videos of the *User* which may be collected in real time. Source: *TDIF*. See also: *Manual Face Comparison.*

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

Requirements Traceability Matrix (RTM). Captures the output from requirements tracing, a process of documenting the links between the requirements and the test cases developed to verify and validate those requirements. Source: *AS NZS ISO/IEC IEEE* 29119.1-2015

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 overall process of risk identification, risk analysis and risk evaluation. A *risk assessment* should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders. It should use the best available information, supplemented by further enquiry as necessary. Source: ISO 31000:2018.

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*.

Security risk. Any event that could result in the compromise, loss of integrity or unavailability of information or resources, or deliberate harm to people. Measures in terms of its likelihood and consequences. 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*.

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. Authentication is accomplished by proving possession and control of the key. Source: *TDIF*.

Single-factor cryptographic (SF Crypto) (device). A cryptographic key stored in a trusted device that has been demonstrated to be tamper evident. Authentication is accomplished by proving possession and control of the key. 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 verifying that the *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 issuing body (or their representative, e.g. via an *Identity Matching Service*). *Source Verification* generally provides the most accurate, up to date information, however it may not be able to prove physical possession of an *Identity Document* (e.g. a licence number may be written down) and it may not have all the details of an original *Identity Document* (e.g. birth certificate information is often a summary of the original). **.** 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 - Annual Assessment. 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. An internal register of TDIF Accredited *Provider*s and decisions. 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 testing*.** A way of validating systems 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 Plan. A plan that details the testing of all applicable TDIF requirements. 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 an *Australian Signals Directorate Approved Cryptographic Algorithm* bound to a secure chip or appended to it (e.g. via *Public Key Technology*). *Technical Verification* is generally very accurate but is dependent of the issuer's revocation processes (e.g. a stolen passport yet to be revoked may still pass *Technical Verification*). Source: *TDIF*.

Trusted Computing Environment. Totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination responsible for enforcing a security policy. Source: NIST

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 interacts with an *Accredited Provider's Identity System* with the purpose of obtaining a service from a *Relying Party*. In the context of the *TDIF*, a *User* may share *Attributes, Assertions*, create a *Digital Identity* or use a *Credential*. 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*. Attributes that can be validated include contact attributes (e.g. SMS activation code being sent to a mobile phone number to confirm control of the associated phone number). Source: *TDIF*.

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 operator visually confirming, either electronically or in-person, that the *EoI* presented, with any security features, appears to be valid and unaltered, or making a facial comparison check. Generally, this is less secure than *Source Verification* or *Technical Verification* as it introduces the possibility of operator error; however, it also allows for a more detailed human evaluation of the *Individual*. 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.