Australian Government

Digital Transformation Office

Identity and Access Management Glossary

Version 2.0 December 2015

Digital Transformation Office

Licence

Use of the Coat of Arms

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

Contact us

Enquiries or comments regarding this document are welcome at:

Assurance Framework Competent Authority
C/O Director, Trusted Digital Identity Team
Digital Transformation Office
Email: authentication@dto.gov.au

Contents

1. Guide Management

1.1 Change Log

This is the first published edition of the Identity and Access Management Glossary (IAM Glossary). This release replaces the 2009 version of the Gatekeeper Glossary and contains all definitions, acronyms and related terms associated with the National e-Authentication Framework (NeAF) and the Third Party Identity Services Assurances Framework (Assurance Framework).

1.2 Review Date

This document will be reviewed regularly and updated in line with changes to the ISM, PSPF and relevant government policies.

1.3 Advice on this Guide

Advice on the IAM Glossary or suggestions for amendment can be forwarded to:

Assurance Framework Competent Authority
C/O Director, Trusted Digital Identity Team
Digital Transformation Office
Email: authentication@dto.gov.au

1.4 Document Structure

This document is structured in the following manner:

- Section 2 lists authentication related acronyms.
- Section 3 defines authentication related terms.

2. Acronyms

Term	Definition
3DES	Triple Data Encryption Standard
AACA	ASD Approved Cryptographic Algorithm
AACP	ASD Approved Cryptographic Protocol
ABN	Australian Business Number
ABR	Australian Business Register
ACDC	Australian Commercial Disputes Centre
ACE	ASD Cryptographic Evaluation
AES	Advanced Encryption Standard
AGSVA	Australian Government Security Vetting Agency
ALGA	Australian Local Government Association
APC	Approved Privacy Code
API	Application Programming Interface
APP	Australian Privacy Principles
ASD	Australian Signals Directorate
ASIC	Australian Securities and Investments Commission
ASIO	Australian Security Intelligence Organisation
B2B	Business to Business
B2I	Business to Individual
B2G	Business to Government
CA	Certification Authority
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CISO	Chief Information Security Officer
CKMP	Cryptographic Key Management Plan

Term	Definition
CMP	Certificate Management Protocol
COI	Community of Interest
CP	Certificate Policy
CPS	Certification Practice Statement
C-R	Challenge-response
CRL	Certificate Revocation List
CSP	Credential Service Provider
CSR	Certificate Signing Request
DH	Diffie-Hellman
DLM	Dissemination Limiting Marker
DRBCP	Disaster Recovery and Business Continuity Plan
DSA	Digital Signature Algorithm
DTO	Digital Transformation Office
DVS	Document Verification Service
EAL	Evaluated Assurance Level
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EOI	Evidence of Identity
EOR	Evidence of Relationship
EPL	Evaluated Products List
ETSI	European Telecommunication Standards Institute
G2G	Government to Government
GAC	Gatekeeper Accreditation Certificate
GCA	Gatekeeper Competent Authority

Term	Definition
GCAP	Gatekeeper Compliance Audit Program
HSM	Hardware Security Module
ICT	Information and Communication Technologies
IdP	Identity Provider
IP	Internet Protocol
IPPs	Information Privacy Principles
IRAP	Information Security Registered Assessors Program
IRP	Incident Response Plan
I2I	Individual to Individual
I2G	Individual to Government
ISD	Information Security Documents
ISM	Australian Government Information Security Manual
ISO/IEC	International Organisation for standardization / International Electro-technical Commission
ISP	Information Security Policy
IT	Information Technology
ITSA	Information Technology Security Adviser
ITSM	Information Technology Security Manager
ITSO	Information Technology Security Officer
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
IVR	Interactive Voice Response
LOA	Level of Assurance
MOA	Gatekeeper Memorandum of Agreement / Head Agreement
NeAF	National e-Authentication Framework
NIAP	National Information Assurance Partnership

Term	Definition
NIPG	National Identity Proofing Guidelines
NIST	National Institute of Standards and Technology
NLZ	No Lone Zone
NPE	Non-person Entity
OAIC	Office of the Australian Information Commissioner
OASIS	Organisation for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OTP	One-Time Password
PAA	Policy Approval Authority
PAD	Personal Authentication Device
PESP	Physical and Environmental Security Plan
PIA	Privacy Impact Assessment
PII	Personal Identifiable Information
PIN	Personal Identification Number
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
PKT	Public Key Technology
PMA	Policy Management Authority
PoI	Proof of Identity
PoT	Position of Trust
PP	Protection Profile
PSP	Personnel Security Plan
PSPF	Australian Government Protective Security Policy Framework

Term	Definition
PSRR	Protective Security Risk Review
RA	Registration Authority
RCA	Root Certification Authority
RFC	Request for Comment
RFT	Request for Tender
RP	Relying Party
RSA	Rivest-Shamir-Adleman
RSS	Rich Site Summary
SAML	Security Assertion Mark-up Language
SBR	Standard Business Reporting
SDLC	System Development Lifecycle
SHA	Secure Hashing Algorithm
SMS	Short Message Service
SOA	Service Orientated Architecture
SOP	Standard Operating Procedure
SOW	Statement of Work
SRMP	Security Risk Management Plan
SSP	System Security Plan
Top 4	Top 4 Strategies to Mitigate Cyber Intrusions
TPISAF	Third Party Identity Services Assurance Framework
VA	Validation Authority
VSP	Verification Service Provider
WebTrust	WebTrust Program for Certification Authorities

3. Glossary of Terms

Term	Definition
Accreditation	The procedure by which an authoritative body gives independent attestation conveying formal demonstration of a Service Provider's competence to provide services of the kind specified in an assurance framework.
Accreditation Process	The process for obtaining Gatekeeper Accreditation as set out at https://www.dto.gov.au/
Accreditation Policies and Criteria	The policies and criteria to be met by Service Providers as set out at https://www.dto.gov.au/
Agency	Includes all Australian Government non-corporate Commonwealth entities, corporate Commonwealth entities or companies under the *Public Governance Performance and Accountability Act 2013* or other bodies established in relation to public purposes.
Applicant	An individual or an Organisation (represented by an individual) who has lodged an application with a Service Provider for the issuance of a Digital Certificate.
Approved Documents	The documents that describe the operations of the Applicant and have been: Evaluated by Authorised Evaluator/s against the Gatekeeper Criteria and Policies as part of the Gatekeeper Accreditation Process; and subsequently Approved by the Gatekeeper Competent Authority in the course of granting Gatekeeper Accreditation to the Applicant.
Archive	Store records and associated journals for a given period of time for security, backup, or auditing purpose.
Assertion	The attribute that the relying party wishes to authenticate. These can include: entity, identity, value, role or delegation.
Asset	Anything of value such as ICT equipment, software, personnel, information and physical assets.
Assurance Level	A level of confidence in a claim, assertion, credential or service. The four levels of assurance recognised in Government policies are: Level 1 – No or little confidence Level 2 – Some confidence Level 3 – High confidence Level 4 – Very high confidence

Term	Definition
Asymmetric Encryption	See Public Key Cryptography
Attribute	A property or characteristic of an object that can be distinguished quantitatively or qualitatively by human or automated means.
AUSkey	A credential that identifies an Individual interacting with digital government services on behalf of a Business Entity.
Australia	As per Part V, Section 17(a) of the *Acts Interpretation Act 1901 (Cth)* Australia means the Commonwealth of Australia and, when used in a geographical sense, includes the Territory of Christmas Island and the Territory of Cocos (Keeling) Islands, but does not include any other external Territory.
Australian Business Number (ABN)	The Australian Business Number is a single identifier for dealings with the Australian Taxation Office (ATO) and for future dealings with other government departments and Agencies.
Australian Business Register (ABR)	The Australian Business Register (ABR) contains all the publicly available information provided by businesses when they register for an Australian Business Number (ABN). The Australian Business Register was established under s.24 of *A New Tax System (Australian Business Number) Act 1999*.
Australian Government Information Security Manual (ISM)	The Australian Signals Directorate's document suite that details controls, principles and rationale for information security on ICT systems. The ISM is designed to assist Australian government agencies in applying a risk-based approach to protecting information and ICT systems. The ISM includes a set of controls that, when implemented will help agencies meet their compliance requirements for mitigating security risks to their information and systems.
Australian Government Protective Security Policy Framework (PSPF)	The Australian Government's protective security requirements for the protection of its people, information and assets. The PSPF defines a series of mandatory requirements with which Commonwealth agencies and bodies must demonstrate their compliance. These requirements cover personnel security, information security and physical security.
Australian Privacy Principles (APP)	Contained in Schedule 1 of the *Privacy Act 1988* (Cth), the APPs regulate the handling of personal information by Australian Government agencies and some private sector organisations.
Australian Securities and Investment Commission (ASIC)	The ASIC is an independent Commonwealth government body that acts as Australia's corporate regulator.
Australian Signals Directorate (ASD)	Australia's national authority for signals intelligence and information security. Part of its role is to assess and provide information security products for the Australian government. It is a central source of information on authentication products and technologies. More information available at www.asd.gov.au

Term	Definition
Authentication	The process of establishing that an Individual, Organisation or NPE is who or what they claim to be.
Authentication Factor	A piece of information and/or process used to authenticate or verify the identity of an entity. Authentication factors are divided into four 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); or • Something an entity typically does (behaviour pattern).
Authorised Auditor	Refers solely to an individual who is listed on the Australian Signals Directorate Information Security Registered Assessors Program website
Authorised Evaluator	A person or an Organisation (including an employee of that Organisation) authorised in writing by the Gatekeeper Competent Authority to evaluate the Service Provider's compliance against the Gatekeeper Criteria and Policies.
Authorised Representative	A person empowered to exercise functions in the best interests of, or on behalf of an individual or Organisation.
Authoriser	A member of a class of persons with a clear capacity to commit an Organisation and to appoint a Certificate Manager. Persons who are members of this class include (but are not limited to): • Chief Executive Officer • Company Director • Trustee • Partner; or • Company Owner.
Availability	The assurance that systems are accessible and useable by authorised entities when required.
Binding	The process of linking a credential to an identity in an assured manner. With respect to EOI it is the process of establishing a linkage between an individual or entity and their claimed or documented identity in an assured manner.
Biometric	Measurable physical characteristics used to identify or verify the claimed identity of an individual.
Business Day	Any day other than a Saturday, Sunday or public holiday (including public service holidays).
Business Entity	An entity entitled to have an ABN within the meaning of s8 of *A New Tax System (Australian Business Number) Act 1999*.

Term	Definition
Business to Business (B2B)	Digital communication between Business Entities.
Business to Government (B2G)	Digital communication between Business Entities and government.
Business to Individual (B2I)	Digital communication between Business Entities and Individuals.
Certificate	An electronic document signed by the Certification Authority which: • Identifies either a Key Holder and/or the business entity that he/she represents; 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.
Certificate Directory	The published directory listing Digital Certificates currently in use which has not reached their Certificate Life.
Certificate Distribution	Means the secure delivery by either the CA or RA of a signed Digital Certificate to the Subscriber. This process may also include the secure provision of Private Keys to the Subscriber.
Certificate Holder	See Subscriber
Certificate Information	Information needed to generate a Digital Certificate as required by the Certificate Profile.
Certificate Life	The maximum duration for which a Digital Certificate can remain valid which under Gatekeeper is derived from the strength of the cryptographic algorithm that is used to generate the Digital Certificate's Keys.
Certificate Manager	A Certificate Manager is an individual authorised by an Organisation (through its Authoriser) to perform certain functions in the application and management of that Organisation's Business Certificates. An Organisation may have more than one Certificate Manager.
Certificate Policy (CP)	RFC3647 defines a Certificate Policy as "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".
Certificate Production	Means the process under which a CA generates and signs a Digital Certificates for end users, binding their identities to their Public Keys. Key Generation, may but, is not necessarily a part of the process of Certificate Production.
Certificate Profile	The specification of the fields to be included in a Digital Certificate and the contents of each. See Annex B of the Gatekeeper Framework for further information.

Term	Definition
Certificate Renewal	The process whereby a Digital Certificate is re-issued to the Key Holder prior to its expiry.
Certificate Revocation List (CRL)	The published directory which lists revoked Digital Certificates. The CRL may form part of the Certificate Directory or may be published separately.
Certificate Signing Request (CSR)	A message sent from an Applicant to a Certification Authority in order to apply for a digital certificate.
Certification Authority (CA)	A Service Provider that digitally signs X.509 v3 Digital Certificates using its Private Key.
Certification Path	An ordered sequence of digital certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.
Certification Practice Statement (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 of Accreditation	See Gatekeeper Accreditation Certificate
Certificate Validation Service	See Validation Authority
Chain of Trust	A process of validating each component of a hierarchy from the bottom up.
Chief Information Security Officer (CISO)	A senior executive who is responsible for coordinating communication between security and business functions as well as overseeing the application of controls and security risk management processes.
Ciphertext	Is the process of applying an encryption scheme to data which transforms the data into an unreadable mix of characters. Apply the reverse process transforms the ciphertext back into readable data, or plaintext.
Claimed identity	A declaration by an entity of the ownership of a set of attributes.
Classified information	Information that needs increased security to protect its confidentiality.

Term	Definition
Client	Is a generic term used in the Gatekeeper PKI Framework to denote a range of individuals or entities that may have dealings with an Agency or Organisation and includes customer, clients, members, associates and employees.
Cloud Service Provider	A company that provides cloud-based platform, infrastructure, application, or storage services to other organisations and/or individuals, usually for a fee
Commencement Date	The date on which the Applicant for Gatekeeper Accreditation and the Digital Transformation Office on behalf of the Commonwealth, execute the Gatekeeper Head Agreement.
Common Criteria	Is an international standard for computer security certification which is based on ISO/IEC 15408.
Commonwealth	The Commonwealth of Australia and including its employees and agents (persons or businesses formally authorised to act on the Commonwealth's behalf).
Commonwealth Agency	An Agency established by the Commonwealth or in which the Commonwealth has a controlling interest.
Commonwealth Record	See *Archives Act 1983 (Cth)*.
Community of Interest (COI)	A defined population of users (i.e. Subscribers and Relying Parties) that agree to operate to an agreed set of rules.
Compliance Audit	An engagement with an Authorised Auditor who conducts an independent audit to determine whether or not a Service Provider remains compliant with an accreditation regime.
Compromise	A violation (or suspected violation) of a system (includes a CA's or Subscriber's Private Keys) such that unauthorised disclosure of sensitive information may have occurred.
Confidential Information	The information described at Item 4 of Schedule 1 of the Gatekeeper Head Agreement, or other specific information agreed between the Service Provider and the Digital Transformation Office to be Confidential Information.
Confidentiality	The obligation of a recipient/holder of information to not disclose it to other parties.
Contract	A contract between the Service Provider and a Commonwealth Agency setting out the terms and conditions of the agreement, the rights and obligations or responsibilities of each party in relation to the provision of Services, but which does not include a Subscriber Agreement.

Term	Definition
Core Obligations Policy	Policy that specifies the core obligations of the participants in Gatekeeper PKI deployments. The obligations are in accordance with the participant's particular roles within a PKI deployment in relation to the application, generation, issuance and on-going management of Keys and Digital Certificates.
Correspond	A Public Key and a Private Key Correspond if they belong to the same Key Pair. A Private Key Corresponds to a Digital Certificate if it Corresponds to the subject Public Key specified in the Digital Certificate.
Credential	The "technology" used by a user for authentication (e.g. user-id+password, shared information, smartcard.
Credential Management	The "lifecycle" approach associated with a credential including creation, initialisation, personalisation, issue, maintenance, cancellation, verification and event logging.
Credentialing Organisation / (Credential Service Provider)	A trusted Organisation that issues authenticated or validated Credentials. Examples of Credentialing Organisation include medical, legal, auditing and technical (engineering) and professional associations and other such bodies.
Cross Certificate	A cross certificate enables Subscribers 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 CAs in each PKI deployment, which defines the responsibilities of each party.
Cryptographic algorithm	An algorithm used to perform cryptographic functions such as encryption, integrity, authentication, digital signatures or key establishment.
Cryptographic Key Management Plan (CKMP)	A plan that describes how cryptographic services are security deployed. It documents critical key management controls to protect keys and associated material during their life cycle, along with other controls to provide confidentiality, integrity and availability of keys.
Cyber Security Event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.
Cyber Security Incident	A single or series of unwanted or unexpected Cyber Security Events or activities that may threaten and/or compromise the confidentiality integrity or availability of business operations, systems or the information stored, processed or communicated by it
Data integrity	The accuracy and consistency of data over time, regardless if it is at rest or transmitted between entities.
Data spill	The accidental or deliberate exposure of classified, sensitive or official information into an uncontrolled or unauthorised environment or to persons without a need-to-know.

Term	Definition
Data Vault	A data vault is a third-party secure storage capability that individuals can use to store sensitive information. It is often, but not always, associated with a digital mailbox.
Device	Computer equipment onto which a Device Certificate may be installed.
Digital Certificate	See Certificate
Digital credential	A Digital Certificate with verified credentials of an individual or Organisation.
Digital Mailbox	A digital mailbox is a third-party provided email account that individuals can use to receive electronic communications (e.g. from businesses and government). Mailboxes may have additional storage capacity where individuals can choose to store important information – these are often referred to as data vaults.
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.
Digital Transformation Office	The Australian Government Agency responsible for the administration of the Gatekeeper accreditation program.
Disaster Recovery and Business Continuity Plan (DRBCP)	An Approved Document which describes how in the event of a system crash or failure: • Services will be restored and/or • Alternative temporary processes will be engaged to maintain or preserve services. • In particular, the document describes restoration priorities to ensure the continuity of government business reliant on the operation of the Service Provider.
Distinguished Name	A unique identifier assigned to each Key Holder, having the structure required by the Certificate Profile.
Document Verification Service (DVS)	An Australian Government initiative to improve identity security, combat identity crime and protect the identities of Australians from being used for illegal purposes.
Dual Key Pair	An Authentication Key Pair and Confidentiality Key Pair. Each Key Pair consists of a Private Key and a Public Key.
e-Authentication	The process that delivers a level of assurance of an assertion made by one party to another in an electronic environment.
Encryption	The process of transforming data into an unintelligible form to enable secure transmission.

Term	Definition
Enrolment	The act of binding an e-Authentication credential to a known instance of a user within an IT resource context (e.g. network, website, application system) in order to enable access by the user.
Entity	The person or “subject” (e.g. corporations, trusts, superannuation funds, incorporated associations) associated with a digital identity. An entity may have multiple digital identities.
Evaluated Assurance Level (EAL)	Common Criteria Evaluation Assurance Levels are 'standards' against which an evaluation is carried out. They define several degrees of rigour for the testing and the levels of assurance that each confers. They also define the formal requirements needed for a product to meet each assurance level.
End Entity	An entity that uses Keys and Certificates for creating or verifying Digital Signatures or for confidentiality. End Entities are Key Holders, Organisations or Relying Parties.
European Telecommunications Standards Institute (ETSI)	The European Telecommunications Standards Institute, officially recognised by the European Union as a European Standards Organisation producing globally- applicable standards for Information and Communications Technologies (ICT).
Evaluated Product	A hardware or software product which is on the Evaluated Product List.
Evaluated Product List (EPL)	The Evaluated Product List is a list of ICT security products certified against internationally recognised common criteria produced to assist in the selection of products that will provide an appropriate level of information security. The list, maintained by ASD, is published at http://www.asd.gov.au/infosec/epl/index.php
Evidence of Identity (EOI)	Evidence (e.g. in the form of documents) issued to substantiate the identity of the presenting party, usually produced at the time of Registration (i.e. when authentication credentials are issued).
Force Majeure	A circumstance beyond the reasonable control of a PKI Entity which results in the entity being unable to observe or perform on time one or more of its obligations, such circumstances including but not limited to: • Acts of Nature, lightning strikes, earthquakes, floods, storms, explosions, fires and any natural disaster; • Acts of war, acts of public enemies, terrorism, riots, civil commotion, malicious damage, sabotage and revolution; and • Strikes (other than by the PKI Entity’s personnel).
Gatekeeper Accreditation	Means formal recognition of a Service Provider granted by the Gatekeeper Competent Authority which signifies that the Service Provider is competent to carry out the operations described in the Approved Documents.

Term	Definition
Gatekeeper Accreditation Certificate (GAC)	The GAC is a certificate issued by the Gatekeeper Competent Authority to Accredited Service Providers.
Gatekeeper Accredited CA	An Applicant that has been accredited by the Gatekeeper Competent Authority after a successful evaluation in accordance with the Gatekeeper CA Accreditation Requirements.
Gatekeeper Accredited RA	An Applicant that has been accredited by the Gatekeeper Competent Authority after a successful evaluation in accordance with the Gatekeeper RA Accreditation Requirements.
Gatekeeper Accredited VA	An Applicant that has been accredited by the Gatekeeper Competent Authority after a successful evaluation in accordance with the Gatekeeper VA Accreditation Requirements.
Gatekeeper Accreditation Disclaimer	The Gatekeeper Accreditation Disclaimer defines the responsibilities and liability provisions of the Gatekeeper Competent Authority when granting accreditation to Service Providers.
Gatekeeper Accreditation Process	See Accreditation Process.
Gatekeeper Applicant	An Organisation/Agency that has applied for Gatekeeper accreditation.
Gatekeeper Approved Documents	See Approved Documents
Gatekeeper Audit Report	A report issued by an Authorised Auditor to the Gatekeeper Competent Authority at the completion of a Gatekeeper compliance audit. The report includes work conducted, any adverse issues identified, areas of non-compliance and recommendations to remediate any issues or non-compliances.
Gatekeeper Competent Authority (GCA)	The entity which approves the Applicant's application for Gatekeeper Accreditation (including the Approved Documents and any changes to them) as meeting the criteria for Gatekeeper Accreditation or Recognition. The Competent Authority for the Gatekeeper PKI is the Chief Executive Officer, Digital Transformation Office
Gatekeeper Compliance Audit Program (GCAP)	An external compliance audit conducted by an Authorised Auditor on an annual basis to ensure that the Service Provider is operating in accordance with its Approved Documents and continues to adhere to Gatekeeper Policies and Criteria.
Gatekeeper Memorandum of Agreement (MOA) / Gatekeeper Head Agreement	A deed of agreement/Head Agreement, including all schedules to the agreement, between an Agency in its capacity as a Service Provider and the Digital Transformation Office on behalf of the Commonwealth.

Term	Definition
Gatekeeper Identity Proofing Policy	The minimum identity verification activities to be performed by a RA to defined LOAs. The Gatekeeper Identity Proofing Policy is consistent with the National Identity Proofing Guidelines.
Gatekeeper Legal Evaluation Panel	The Gatekeeper Legal Evaluation Panel evaluate the legal documents for Gatekeeper Applicants applying for Gatekeeper Accreditation and Service Providers amending previously approved legal documents as part of their documentation suite.
Gatekeeper Mandatory Security Requirements	Protective security requirements derived from the PSPF that Gatekeeper Applicants are required to demonstrate their compliance with.
Gatekeeper Policies and Criteria	Means the Policies and Criteria at https://www.dto.gov.au/ that are applied in the Accreditation Process and in the on-going management of the Gatekeeper Head Agreement and other arrangements that may be entered into by the Digital Transformation Office in relation to the Gatekeeper Framework.
Gatekeeper website	The website at https://www.dto.gov.au/
Government to Government (G2G)	Digital communication between Agencies.
Government to Individual (G2I)	Digital communication between Government and individuals.
Identification	A claim or statement of identity (of an individual or business).
Identity	A set of attributes representative of an entity, particularly within an information and communication technologies (ICT) context which can be grouped into a Core Identity and Persona (s). An entity may be represented as “themselves” or as a representative, role, delegate etc.
Identity Proofing	The process by which sufficient information is captured and verified to identify an entity to a specified or understood level of assurance.
Identity Provider (IdP)	The owner of a system that creates, maintains, and manages identity information for entities and provides authentication services to one or more relying parties. An identity Provider may fulfil part or all of the duties of a Credential Service Provider, Registration Authority and/or Trust Broker if these duties are appropriately separated.
Incident Response Plan (IRP)	A plan for responding to cyber security incidents.
Individual	Relates to a person who intends to transact or is transacting securely online with government agencies in his/her capacity as a single human being as distinct from a group.
Individual to Government (I2G)	Digital communication between an Individual and Government.

Term	Definition
Individual to Individual (I2I)	Digital communication between individuals.
Information	Documents and papers; electronic data; the software or systems and networks on which the information is stored, processed or communicated, intellectual information acquired by individuals and physical items from which information regarding design, components or use could be derived.
Information Risk Assessor Program (IRAP Assessor)	Suitably qualified individuals accredited to provide ICT assessment services to government.
Information Security Documents (ISD)	A core suite of Information Security documentation that addresses all elements of organisations protective security arrangements.
Information Security Policy (ISP)	A high-level document that describes how an agency protects its systems. The ISP is normally developed to cover all systems and can exist as a single document or as a set of related documents.
Information Technology Security Adviser (ITSA)	The ITSM who has responsibility for information technology security management across the agency is designated as the ITSA. This title reflects the responsibility this person has as the first point of contact for the CISO and external agencies on any information technology security management issues.
Information Technology Security Manager (ITSM)	ITSMs are executives that coordinate the strategic directions provided by the CISO and the technical efforts of ITSOs. The main area of responsibility of ITSMs is that of the day-to-day management of information security within an agency.
Information Technology Security Officer (ITSO)	ITSOs implement technical solutions under the guidance of an ITSM to ensure that the strategic direction for information security within the agency set by the CISO is achieved.
ITU-T X.500	Information technology – Open Systems Interconnect – The Directory: Overview of concepts, models and services
Key	A Key is a string of characters used with a cryptographic algorithm to encrypt and decrypt.
Key Archive	The process of storing keys in a secure repository with the ability for them to be recovered at a later time if the key is lost
Key Escrow	The process of entrusting a Private Key to a third party (an Escrow Agent such as an Organisation or government) and providing another third party with a legal right to obtain the Key from the Escrow Agent in certain circumstances.
Key Generation	The process where the Subscribers Private Keys are created.
Key Holder	See Subscriber.

Term	Definition
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.
Key Recovery	The process of recovering a key from a secure repository.
Key Usage	The Key Usage extension defines the purpose (eg., encryption, signature etc) of the Key contained in the Digital Certificate.
Level of Assurance (LoA)	See Assurance Level.
MUST	An accreditation convention which indicates a mandatory requirement of an accreditation framework to be met by a Service Provider in order to satisfy a control or control test.
MUST NOT	An accreditation convention which indicates an event or activity that if practiced, exercised or implemented will breach an accreditation requirement.
National Identity Proofing Guidelines (NIPG)	Guidelines produced by the Attorney General's Department for identity verification within government Agencies.
National e-Authentication Framework (NeAF)	The Framework that covers the rules to be applied by Agencies to the authentication of external (i.e. non-Commonwealth Government) entities when dealing with them online. The Framework provides a risk management approach to authentication that aligns business needs and processes with appropriate authentication solutions and technologies.
No Lone Zone (NLZ)	An area in which personnel are not permitted to be left alone such that all actions are witnessed by at least one other person.
Non compliance	The failing of a control to meet an accreditation requirement.
Non-repudiation	Evidence, verifiable by a third party that a Transaction has been sent/authorised by the purported sender.
Novation	The substitution of a new contract for an old one. The new agreement extinguishes the rights and obligations that were in effect under the old agreement.
Online Certificate Status Protocol (OCSP)	A Online Certificate Status Protocol specifies a mechanism used to determine the status of digital certificates, in lieu of using Certificate Revocation Lists (CRLs)

Term	Definition
Object Identifier (OID)	An OID is a string of decimal numbers that uniquely identifies an object. These objects are typically an object class or an attribute. It serves to name almost every object type in X.509 Certificates, such as components of Distinguished Names and Certificate Policies.
One-time password (OTP)	A password that is changed each time it is required.
Operations Manual	An Approved Document that describes the daily management and operational practices of a Service Provider.
Organisation	Relates to an entity that has authorised one or more of its employees to hold and use Keys and Certificates on its behalf. An Organisation may or may not be a Business Entity.
Personal Information Identifiable (PII)	Information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about a natural person whose identity is apparent, or can reasonably be ascertained, from the information or opinion.
Personnel security clearance	See Security Clearance.
Physical and Environmental Security Plan (PESP)	A Physical & Environmental Security Plan documents measures to counter identified risks to a Service Providers functions, information, people and physical assets at a designated site.
Privacy Impact Assessment (PIA)	A PIA is an assessment tool that "tells the story" of a project from a privacy perspective. A PIA describes how personal information flows in a project, analyses the possible privacy impacts on individuals' privacy, identifies and recommends options for managing, minimising or eradicating these impacts.
Policies	All Gatekeeper policies, practices and procedures relevant to Gatekeeper Accreditation, including the policies referred to under Gatekeeper at https://www.dto.gov.au/
Position of Trust (PoT)	A role of authority within an Organisation usually involving duties that require a higher level of assurance than that provided by normal agency employment screening. In some organisations additional screening may be required. Those in a position of trust have the ability to access especially sensitive information. Positions of trust can include, but are not limited to, ITSAs, administrators or privileged users.
Prior audit work	Refers to the work of an alternative audit program successfully completed in defined period which may be used to meet compliance audit requirements.

Term	Definition
Privileged user	A user who can alter or circumvent system security protections. This can also apply to users who could have only limited privileges, such as software developers, who can still bypass security precautions. A privileged user can have the capability to modify system configurations, account privileges, audit logs, data files or applications.
Private Key	The Private Key in asymmetric Key Pair that must be kept secret to ensure confidentiality, integrity, authenticity and non-repudiation, as the case may be.
Protection Profile	A Protection Profile is a document that stipulates the security functionality that must be included in a Common Criteria evaluation.
Protective Security Risk Review (PSRR)	A comprehensive review of security threats and the development of recommended protective security measures, using risk-based methodology.
Public Key	The Key in an asymmetric Key Pair which may be made public.
Public key certificate	See Certificate
Public Key Cryptography (PKC)	Refers to a class of cryptographic algorithms which require two separate keys, one which is public and one which is private. Although different, the keys are mathematically linked and enable one key to perform the opposite functions of the other. The public key is used to encrypt data and verify a digital signature whereas the private key is used to decrypt data and generate a digital signature.
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.
Public Key Technology (PKT)	Public Key Technology is the hardware and software used for encryption, signing, verification as well as the software for managing Digital Certificates.
Registration	The processes associated with the initial creation of an electronic identity for a user. Registration usually encompasses EOI or EOR processes.
Registration Authority (RA)	A Service Provider that: • Is responsible for the registration of applicants for Digital Certificates by checking Evidence of Identity documentation submitted by the applicant for its compliance with Gatekeeper Identity Proofing Policy; • Is responsible for the provision of completed and authorised application form including copies of the submitted EOI documents to the relevant CA; and • May be responsible for the secure distribution of signed Digital Certificates to Subscribers.

Term	Definition
Relying Party (RP)	A recipient of a Certificate who acts in reliance on that Certificate and/or Digital Signatures verified using that Certificate.
Relying Party Agreement	An agreement between a CA (and if applicable, the relevant Gatekeeper Accredited RA) and a Relying Party which sets out the respective rights, obligations and liabilities of those parties in respect of the verification of Digital Signatures and the use of Certificates for verification purposes, and which legally binds those parties to the relevant CP and CPS.
Renew	The process of obtaining a new Certificate of the same category and type for the same subject once an existing Certificate has expired.
Repository	A database of information (e.g. Certificate status, evaluated documents) which is made accessible to users including the Relying Parties.
Repudiation	Repudiation is the denial or attempted denial of involvement by a party in all or part of an electronic Transaction.
Revoke	To terminate a Certificate prior to the end of its operational period.
Risk	The chance of something happening that will affect objectives – it is measured in terms of event likelihood and consequence.
Risk acceptance	An informed decision to accept risk.
Risk analysis	The systematic process to understand the nature, and deduce the level of risk.
Risk appetite	Statements that communicate the expectations of an organisations senior management about the organisations risk tolerance. These criteria help an organisation identify the risk and prepare appropriate treatments, and provide a benchmark against which the success of mitigations can be measured.
Risk management	The process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.
Risk mitigation	Actions taken to lessen the likelihood, negative consequences, or both, associated with a risk
Risk rating	A rating that indicates how significant each identified potential risk is to an organisation. The risk rating may be expressed qualitatively or quantitatively.
Residual risk	The remaining levels of risk after risk treatments have been implemented.
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

Term	Definition
RFC 5019	The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments
RFC 5280	Internet X.509 Public Key Infrastructure and Certificate Revocation List (CRL) Profile
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
Root CA (RCA)	A Certification Authority that is the top most Certification Authority in a trust hierarchy, and is directly trusted by an End Entity.
Security Clearance	A documented determination by an authorised betting agency that an employee is suitable to access security classified information (on a need-to-know basis) relative to the level of clearance granted. A Security Clearance provides assurance that personnel can be trusted with access to sensitive or classified information that is processed, stored or communicated by a system.
Security Risk Management Plan (SRMP)	A plan that identifies security risks and appropriate risk treatments.
Self-signed certificate	A Certificate for which the issuer (signer) is the same as the subject – the entity whose Public Key is being authenticated by the Certificate.
Service Provider	An accredited entity.
Services	Services provided by a Service Provider as applicable to the type of Accreditation granted under the Gatekeeper Head Agreement or Memorandum of Agreement.
SHOULD	An accreditation convention which indicates something that is not a mandatory but is recommended which either supports a mandatory obligation or is considered best practice.
Signature	A distinctive mark, or characteristic, indicating identity.
Signer	A person who affixes the Digital Signature to his or her information to enable a third party to confirm that the information was sent by that person.
Smartcard	A hardware device that incorporates one or more integrated circuit chips to implement cryptographic functions and that possesses some inherent resistance to tampering.
Standard Operating Procedures (SoP)	Standard Operating Procedures are detailed written instructions to achieve uniformity of the performance of a specific function.

Term	Definition
Subject Distinguished Name	A field in a Digital Certificate that identifies the person or entity to whom the Certificate is issued. The Subject Distinguished Name is an unambiguous name that can uniquely identity either the equipment or device that holds a Private Key or the individual Key Holder.
Subordinate Entity	A RA and any other entity which is subordinate to the CA and which performs functions or provides services necessary for issue and use of Keys and Certificates, or for reliance on Digital signatures. A Subordinate Entity does not include the CA itself or an End Entity.
Subscriber	The entity that applies for, is issued with and uses and e-Authentication credential. In the context of PKI a Subscriber is an individual, or the person who acts on behalf of the Organisation that is in possession of or has control of the Private Key and who uses that Key to digitally sign/receive messages.
System Security Plan (SSP)	A plan documenting the security controls and procedures for a system.
Threat	A circumstance or event with the potential to cause harm, including the destruction, unauthorised disclosure, or modification of data and/or denial of service. Threats arise from human actions and natural events.
Third Party Identity Services Assurance Framework (TPISAF)	The whole-of-government suite of policies, standards and procedures that govern the use of identity related services provided to government from the commercial provider market. These services include personal data vaults, digital mailboxes, and verification and authentication services.
Time Stamp	A record that indicates (at least) the correct date and time of an action (expressly or implicitly) and the identity of the person or device that created the notation.
Token	A hardware security device containing a user's Private Key(s), and Public Key Certificate.
Top 4 Strategies to Mitigate Cyber Intrusions (Top 4)	A collection of the most effective security controls an Organisation can implement which is based on ASD's visibility of the current cyber threat environment. The Top 4 Strategies include: • Application whitelisting, • Patching applications, • Patching operating systems, and • Minimising administrative privileges.
Trust Broker	The owner of a system that creates and maintains trustful relations between two or more entities that have low levels of trust.

Term	Definition
Trusted Digital Identity	A re-usable set of core attributes (expressed digitally).
Trusted Person	A person who serves in a Trusted Position and is qualified to serve in it.
Trusted Persons Register	A register of all trusted personnel in trusted positions, including system administrators, database administrators, privileged users, positions of trust..
Trusted Position	A role within a RA/CA that includes access to or control over cryptographic operations that may materially affect the issuance, use, suspension, or revocation of Certificates, including operations that restrict access to a Repository.
Trusted Root CA	See Root CA
Validation	The process of establishing the validity of a credential presented as part of an authentication process (for example the validity of a digital certificate may be validated using techniques such as revocation status checking and certificate path validation).
Validation Authority (VA)	A special form of PKI entity which can be used to check the validity and currency of digital certificates. A VA is typically used when the certificate generation and certificate status services are separated between Service Providers.
Valid Certificate	A Certificate issued by a CA and accepted by the Subscriber listed in it that has not been revoked or suspended and remains operational.
VANguard	Is a whole-of-government program that delivers authentication services to B2B and B2G digital transactions. In the context of Gatekeeper, VANguard is a certificate status service used by AUSkey.
Verification	Verification is a process whereby information is checked for accuracy and authenticity, usually with an authoritative source that personal information (e.g. name, date of birth) submitted by an individual is true and correct. The process of checking information by comparing the provided information with previously corroborated information
Verification Service Provider (VSP)	In the context of the Third Party Identity Services Assurance Framework a Verification Service Provider verifies the authenticity of documentation or personal information submitted by an Individual to establish a degree of confidence that the individual is who they say they are.
Verify	To determine or test the accuracy of EOI documentation submitted by an applicant in accordance with procedures set forth in the RA's Approved Documents, the relevant CP and CPS and the service agreement between the RA and CA.

Term	Definition
WebTrust Program for Certification Authorities (WebTrust)	WebTrust is an assurance service jointly developed by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants. It relies on a series of principles and criteria designed to promote confidence and trust between consumers and organisations conducting business on the Internet.
X.509 and X.509 v3	The ITU-T standard for Public Key Infrastructure. It is part of wider group protocols from the ITU-T X.500 Directory Services Standards.