

**Department of Human Services**

**Public Key Infrastructure (PKI) Glossary**

**February 2018**



**Version History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Status** | **Date of Issue** | **Comments** |
| 1.0 | Final | June 2013 | Initial version reflecting definitions from Australian Government Information Management Office Gatekeeper PKI Framework Glossary (the Gatekeeper PKI Glossary) 2012 |
| 2.0 | Final | 5 December 2016 | Revised version reflecting changes in the Gatekeeper PKI Framework version 3.1 |
| 3.0 | Final | 05 February 2018 | Revised version reflecting changes in the Gatekeeper PKI Framework version 3.1 |

**Table of Contents**

**PKI GLOSSARY.............................................................................................................................4**

1.1 Purpose statement....................................................................................................................4

1.2 Definitions .................................................................................................................................5

**1 PKI GLOSSARY**

**1.1 Purpose statement**

The Department of Human Services (Human Services) PKI Glossary (the glossary) defines words and terms for the purposes of the:

1. Human Services Root Certification Authority (Human Services RCA) Certificate Practice Statement
2. Human Services Root Certification Authority Certificate Policy
3. Human Services Organisation Certification Authority (Human Services OCA) Certification Practice Statement
4. Subscriber Certificate Policies (CP), and
5. *Department of Human Services PKI Certificates*.

Where words or terms are defined in the glossary, other grammatical forms of that word or term have a corresponding meaning. For example, “authenticate” has a meaning corresponding to the defined word “authentication”.

**1.2 Definitions**

**Note**: Some terms have been adopted from the Digital Transformation Agency Identity and Access Management Glossary. See:

[https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf)

|  |  |
| --- | --- |
| **Term or acronym** | **Explanatory notes** |
| Access | Obtaining knowledge or possession of classified material, or access to a designated secure area. |
| Access control | The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner. |
| ACSI | Australian Communications - Electronic Security Instructions. |
| Agency | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Applicant | (a) The individual or entity (represented by an individual) that applies for PKI keys and certificates in accordance with the applicable certificate policy, and/or  (b) A third party entity who wishes to become an accredited Human Services OCA subordinate to the Human Services RCA within the health sector PKI hierarchy. |
| Application | An application (paper or electronic) by an applicant for PKI keys and certificates. |
| Archiving | The storage of information and data to meet requirements of the *Archives Act 1983* or other requirements. |
| Asset | Anything that has value to an organisation. |
| Audit report | A report prepared by an auditor detailing the results of the gatekeeper compliance audit. |
| Australian Government materials | Section 9.5 of the Human Services RCA CP identifies the documents in which intellectual property rights are owned by Human Services on behalf of the Australian Government. |
| Australian Government Protective Security Policy Framework (PSPF) | The framework issued by the Attorney-General’s Department is the principal means for distributing Australian Government protective security policies, principles, standards and procedures to be followed by all government agencies for the protection of official information and resources. |
| Australian Government Security Vetting Agency (AGSVA) | Part of the Defence Security Authority in the Department of Defence. It conducts security vetting for all Australian Government agencies (apart from exempt agencies). Clearances granted by AGSVA have whole-of-government effect. |
| Australian Security Intelligence Organisation (ASIO) | Australia’s security service. Its functions are set out in the *Australian Security Intelligence Organisation Act 1979*. Its main role is to gather information and produce intelligence to enable it to provide government with information about activities or situations that might endanger Australia’s national security. |
| Australian Federal Police (AFP) | AFP enforces federal criminal law and protects Commonwealth and national interests from crime in Australia and overseas. |
| Australian Signals Directorate (ASD) | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Authentication | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Authentication key pair | Used for authentication and integrity. |
| Authorised auditor | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Authorised evaluator | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Authorised third party | A person or entity authorised to act on behalf of a subscriber (practice or entity) to bind that practice or entity and who are able to request revocation or reinstatement of a certificate. Authorised third parties include, but are not limited to:   1. an administrator appointed to administer an entity’s affairs 2. a court with jurisdiction within an entity’s area of operations 3. a third party with an appropriate Power of Attorney, or   the person notified by the practice or entity as having authority to bind the practice or entity. |
| Authoriser | Is an individual who has legal authority to act on behalf of the site/organisation. An Authoriser must authorise any new Certificate Manager to act on the site/organisation’s behalf. |
| B-Class safe | A security container manufactured to ASIO approved specifications. |
| Business day | 8:30 am to 5:00 pm local time. Monday to Friday inclusive, excluding public holidays. |
| Business Development Officer (BDO) | Human Services officer whose primary task is to assist subscribers with e-Business. They visit medical practices, pharmacies and other healthcare providers. |
| Card reader | An electronic device which allows a computer or laptop to access information within a smart card. |
| C-Class safe | A security container manufactured to ASIO approved specifications. |
| Certificate (also known as the PKI certificate) | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Certificate controllers | Human Services staff responsible for certificate management. All certificate controllers are duly authorised representatives of Human Services. |
| Certificate information | The information needed to complete a certificate application as required by the certificate profile. |
| Certificate Manager | Is responsible for managing the Certificate such as revoking, reissuing and renewing. The Certificate Manager is the primary contact for correspondence relating to the Certificate and its uses. |
| Certificate policy (CP) | The document sets out the policies applicable to the issue and use of a PKI certificate.  Certificate policies covered by this glossary are located at <https://www.humanservices.gov.au/organisations/health-professionals/enablers/public-key-infrastructure-pki-policy-documents>  *Refer to the definition found in the Identity and Access Management Glossary.*  <https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf> |
| Certificate profile | The specification of the fields to be included in a certificate and the contents of each field, as set out in the relevant certificate profile within the certificate policy. |
| Certificate Revocation List (CRL) | A signed, time-stamped list of serial numbers for Public Key Certificates of subscribers that have been revoked prior to their scheduled expiry. |
| Certification Authority (CA) | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf)  Also see Human Services OCA. |
| Certification Practice Statement (CPS) | A statement of the practices that a Certification Authority employs in issuing certificates.  The Human Services RCA CPS and the Human Services OCA CPS are located at  <https://www.humanservices.gov.au/organisations/health-professionals/enablers/public-key-infrastructure-pki-policy-documents> |
| Classified material | Official information which, for reasons of security, requires protection to prevent it being acquired by people, organisations or governments not authorised to receive it. Classified material may be either ‘national security’ or ‘non-national security’ material. |
| Client | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Client Organisation Certificate Authority (OCA) | An Organisation Certification Authority under the operational control of an organisation (which may be the same or hosted for another organisation), and which is also part of the health sector PKI and the Client OCA Certificate being signed by the Human Services RCA. |
| Commonwealth (Cth) | The Commonwealth of Australia including its employees and agents (persons or businesses formally authorised to act on the Commonwealth’s behalf). |
| Community of Interest (CoI) | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Compliance audit | An audit of operations undertaken by an authorised auditor to check that processes and procedures are in accordance with gatekeeper approved documents. |
| Compromise | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Compromised user | A subscriber who has had several instances of certificate revocation (assessed on a case–by-case basis) and is recorded as such by the CA. |
| Confidential information | Sections 9.3 and 9.4 of the Human Services RCA CPS provide reference to where confidential and personal information which is protected from disclosure under the health sector PKI can be identified. |
| Confidentiality | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Confidentiality key pair | Used to protect the confidentiality of an electronic message (e.g. by cryptography). |
| Cryptography | The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use. |
| Digital Transformation Agency (DTA) | The Australian Government Agency responsible for the administration of the Gatekeeper accreditation program. |
| Department of Human Services (Human Services) | The Australian Government department which is responsible for the development of service delivery policy and provides access to social, health and other payments and services. Medicare Australia, Centrelink, child support and CRS Australia were integrated into the department on 1 July 2011. |
| Decrypt | The practice of recovering an encrypted message by reverting from cipher text to plain language. |
| Digital certificate | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Digital signature | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Disaster Recovery and Business Continuity Plan | A Human Services RCA document which outlines the internal processes to be followed in the event of an incident effecting availability of the PKI service. |
| Distinguished name | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Document | Anything on which information is recorded by any means, including words, symbols, images or electro-magnetic impressions. |
| Electronic Business (e-Business) | Performing business online (i.e. electronically). |
| e-Business Service Centre (eBSC) | Provides tier 1 telephone-based support for PKI-related issues. |
| Encrypt | Practice of converting plain language to cipher text. |
| End entity | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Evidence of Identity (EOI) | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Electronic procurement (eProcurement) | A self-service solution for requisitioning and ordering goods and services online. |
| Evaluated Products List (EPL) | A list of hardware and software products which are considered to provide an adequate level of information security. In Australia, the EPL is maintained by the Defence Signals Directory.  See: <https://www.asd.gov.au/> |
| Expire | Refers to the end of a PKI certificate’s validity period. |
| Facility Security Officer (FSO) | Examines system records and event logs to ensure that Human Services staff act within their responsibilities and within the stated security policy. |
| Forensic plan | A plan documenting the approach to security incidents and ensuring evidence relating to such incidents is appropriate. |
| Gatekeeper accreditation/  Gatekeeper accredited | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Gatekeeper approved documents | *Refer to the definition of Approved Documents found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Gatekeeper Competent Authority (GCA) | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Gatekeeper Compliance Audit Program (GCAP) | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Gatekeeper Memorandum of Agreement (MOA) | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Gatekeeper Public Key Infrastructure (PKI) Framework | The Gatekeeper PKI Framework governs the use of digital keys and certificates by the Australian Government to assure the identity of subscribers to authentication services.  *See:* <https://www.dta.gov.au/files/authentication-framework/Gatekeeper-PKI-Framework-v3_1.pdf> |
| Health Network Public Key Infrastructure (PKI) | The Australian Government Department of Human Services (Human Services) owns and operates the Health Network Public Key Infrastructure (Health Network PKI) to:   * facilitate the authentication of confidential communications for a number of online programmes, and * enable access to Digital Health infrastructure and services. |
| Healthcare entity | Includes the body (which may or may not be a legal entity such as a health service established by legislation, a corporation or a registered business) responsible for the provision of healthcare services. |
| Healthcare Identifiers Service | The Certificate Policy (CP) for individual certificates provided by Human Services as service operator of the Healthcare Identifiers Service (HI Service) to individuals who are assigned healthcare provider individual roles by an authorised data source, and who are known in the HI Service and registered by Human Services in accordance with its role as the service operator of the HI service. |
| Healthcare individual | Refers to any individual who is involved in healthcare services. |
| Healthcare Public Directory | The publicly accessible directory that lists unexpired, suspended, revoked and expired certificates.  The directory acts as a ‘White Pages’ and can be searched on key words to find an entity’s certificate.  The Healthcare Public Directory contains a link to the NASH Directory.  References in the Medicare RCA CP, Medicare RCA CPS and Medicare OCA CPS to Healthcare Public Directory are deemed to mean or include, as applicable, NASH Directory in so far as those references concern or relate to:   1. the listing, publishing or storing of NASH certificates or related public keys 2. the availability of the directory, or 3. the publication of the directory. |
| Healthcare X.500 Directory | See Healthcare Public Directory. |
| Health Professional Card | The former name for a smart card. |
| Health sector | Interpreted broadly and includes, but is not restricted to the following groups:  (a) healthcare practitioners (e.g. Individual Healthcare Providers) who are duly qualified, registered, recognised or trusted as delivering services in the areas of:   1. primary and acute healthcare (doctors, specialists, pharmacists, pathologists, nurses, etc.) 2. allied healthcare (physiotherapists, chiropractors, osteopaths, podiatrists, prosthodontists, dentists, etc.) 3. alternative healthcare (homeopaths, naturopaths, herbalists, etc.)   (b) healthcare entities and organisations (e.g. Healthcare Provider Organisations)  (c) associated staff of the above groups (practice staff and staff in representative groups), and  (d) Australian, State, Territory and/or local government organisations, entities and their representatives. |
| Health sector PKI | Use of PKI within the health sector. |
| Human Services health sector Public Key Infrastructure | The health sector public key infrastructure under which keys and certificates are issued. |
| Human Services materials | Section 9.5 of the Human Services RCA CP identifies documents and materials in which ownership of the intellectual property rights are vested in Human Services on behalf of the Australian Government. |
| Human Services Relationship Organisation (RO) | The Relationship Organisation (Human Services RO) in the health sector PKI. It comprises communities of interest that have established relationships with clients considered adequate for the issuance of digital certificates. |
| Human Services Certificates Communities of Interest (CoI) Certificate Policy (CP)  (Formerly Medicare Australia Certificates CoI CP) | The certificate policy applicable for the issuing of certificates under the Human Services OCA. |
| Human Services Organisation Certification Authority (Human Services OCA) | Is immediately subordinate to the Human Services RCA in the health sector PKI hierarchy. The primary purpose of the OCA is to generate certificates and to perform other certificate management services in response to requests from authorised personnel. These are detailed in the Certificate Practice Statements (CPS).  The Human Services OCA is owned by Human Services. |
| Human Services Organisation Certification Authority Certification Practice Statement (Human Services OCA CPS) | Sets out the processes and procedures for issuance and management of certificates issued by the Human Services OCA. |
| Human Services Root Certification Authority (Human Services RCA) | The Human Services RCA issues and signs two types of Certification Authority certificates.   * it signs itself to create the trust anchor (self-signed certificates) for the health sector PKI operated by Human Services, and * it signs certificates for all Organisation Certification Authorities (OCAs) within the health sector PKI hierarchy, to signify those OCAs as being members of the health sector PKI.   Both functions are covered by the Human Services RCA CP.  A reference to the Human Services RCA includes, where applicable, a reference to its staff.  The Human Services RCA is owned by Human Services. |
| Human Services Root Certification Authority Certificate Policy (Human Services RCA CP) | The CP for the Human Services RCA, which is at the top of the health sector PKI hierarchy operated by Human Services. |
| Human Services Root Certification Authority (Human Services RCA) Certification Practice Statement | Covers the common practices and procedures that apply to the entire health sector PKI hierarchies operated by the Human Services Relationship Organisation (RO).  These common elements include:   * the use of evaluated products for any of the security-critical cryptographic operations * the separation of registration and certification operations * the application of tiered security * the employment of trustworthy staff * the application of rigorous change control processes, and * the institution of a continuous cycle of internal and external audits.   Relates to:   * the self-signed Human Services RCA authentication and confidentiality certificates which the Human Services RCA issues to itself, and * the authentication and confidentiality certificates signed by the Human Services RCA and issued to OCAs (e.g. the Human Services OCA). |
| Incident | An activity which:   * causes damage, or is intended to cause damage, to PKI information assets * prevents, or is intended to prevent, a CA from carrying out its designed function * indicates someone has attempted an unauthorised access * indicates that someone has had opportunity to attempt an unauthorised access * indicates that a staff member has been the target of a social engineering attack, gains, or attempts to gain, unauthorised access to sensitive material, or * results in the unauthorised disclosure of sensitive data. |
| Incident Investigation Officer (IIO) | The individual responsible for the management of an incident until incident closure. |
| Incident Response Plan | Response procedures to deal with incidents arising from threats and risks that are specific to the CA systems. |
| Incident Response Team (IRT) | Registration Authority staff established for the specific purpose of investigating an incident. The IRT has authority to seek relevant expertise from other appropriate organisations (e.g. AFP) to address the specific needs of the incident. |
| Individual certificates | A PKI certificate issued under the Human Services Community of Interest (Col) Certificate Policy (CP) for Healthcare Individual Certificates issued to a healthcare individual who is registered with, or known to, Human Services through application and/or relationship. The certificates are provided on a Secure Token to Subscribers. |
| Information Privacy Principles (IPPs) | The principles set out at section 14 of the *Privacy Act 1998* (Cth).  See: <https://www.oaic.gov.au/privacy-law/privacy-archive/privacy-resources-archive/information-privacy-principles> |
| Intellectual property rights (IPR) | Intellectual property rights means:   1. all copyright and neighbouring rights (including moral rights), trade mark, trade secret, service mark, design, drawing, patent, know-how, secret process, business or domain name, or other similar proprietary right and all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields; and 2. any rights to the registration of those rights, whether created, formed or arising, before or after the date of the agreement in Australia or elsewhere. |
| Key | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Key holder | Individual registered as the owner of the PKI certificate |
| Key Pair | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Known customer model | Entities known to Human Services that have previously undertaken an appropriate EOI process or who have had information sourced from authorised trusted data sources. |
| Moral rights | Rights of integrity of authorship, rights of attribution of authorship, rights not to have authorship falsely attributed and rights of a similar nature conferred by statute, that exist, or may come to exist, anywhere in the world. |
| NASH | National Authentication Service for Health. |
| NASH Directory | The directory that lists unexpired NASH certificates.  The directory acts as a ‘White Pages’ and can be searched on key words to find an entity’s certificate.  See Healthcare Public Directory. |
| National Privacy Principles (NPPs) | Privacy principles set out in the *Privacy Act 1988* (Cth) which came into effect for private sector organisations on 21 December 2001.  See: <https://www.oaic.gov.au/privacy-law/privacy-archive/privacy-resources-archive/national-privacy-principles> |
| Non-repudiation | The concept of ensuring that a party in a dispute cannot repudiate, or refute the validity of a statement. |
| Notice | Any consent, information, application, request or any other communication provided under, or in connection with, the relevant certificate policy. |
| OCA Certification Practice Statement (OCA CPS) | The CPS governing the operations of the OCA. |
| Object identifier (OID) | The name of an object that is used to identify fields in certificates. This object name is a value of ASN.1 type OBJECT IDENTIFIER. An object identifier value is a globally unique ordered list of integers. Each integer in the list is an “*object identifier component*”, and there must be at least two components to form a valid object identifier. |
| Operations manual | RCA/OCA document which provides information relating to the operations of the RCA/OCA and is intended for use by staff charged with the management and operation of the RCA/OCA. Not publicly available. |
| Organisation Certification Authorities (OCAs) | Are immediately subordinate to the Human Services RCA in the health sector PKI hierarchy. The primary purpose of a subordinate OCA (e.g. the Human Services OCA) is to provide certificates and certificate management services to relying parties and subscribers who are members of a CoI which is subordinate to the OCA in the health sector PKI. |
| Party | Party or parties refers to any, or all, of:   * Human Services OCA * the subscriber * the relying party |
| Passphrase | A string of characters to enable access to a system or private key. |
| Personal Identification Number (PIN) | An access control mechanism used during key transport to import or use private keys. |
| Personal information | Has the meaning given in the *Privacy Act 1988* (Cth), which is: “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 an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion”.  In relation to health sector PKI, personal information may include information or an opinion about an individual obtained in connection with any dealings with Human Services. |
| PKI entity | Any entity participating in health sector PKI, including the RCA, the OCA and subscribers. |
| PKI service provider | Any PKI entity which has roles, functions and obligations or rights under a Certificate Policy. PKI service providers include the RCA, the OCA and the RA. |
| Policy Management Authority (PMA) | Reviews all Human Services PKI policies and documents and is the approving authority for PKI policies. |
| Policy qualifier | Text incorporated into each certificate which defines the scope of use of that certificate. The policy qualifier for each certificate is set out in the applicable CP. |
| Pre-cut card | A card containing a certificate chip which is pushed out of the card and inserted into the USB token. |
| Private Confidentiality key | The key used to decipher or decode the contents of a message which has been encrypted for confidentiality. |
| Private key | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Privacy Policy | A document which describes policies dealing with the collection, storage, access, use and disclosure of personal information. |
| Protected | The classification applied to sensitive material requiring a reasonable degree of protection (i.e. the middle sensitive material classification). |
| Protective security plan | The plan that identifies the security mechanisms for the PKI. It sets out the responsibility for establishing and maintaining safeguards and strategies that will enable the appropriate levels of service and data confidentiality, integrity and availability to be provided. Not publicly available. |
| Public key | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Public Key Infrastructure (PKI) | An electronic trust framework adopted by the Australian Government to provide authentication and confidentiality for online transactions through the use of keys and certificates.  PKI enables the transfer of sensitive claims, payments and medical information across the internet, without compromising the individual’s right to privacy for the health sector. |
| Record | A document. |
| Registration | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Registration Authority (RA) | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Registration Authority (KeyGen) Subsystem | The component of the RA system that generates the PKI keys during the registration process. |
| Registration Authority Operator (RAO) | The CA/RA staff responsible for processing EOI checks and certificate requests. |
| Registration Authority Operations Manager (RAOM) | The CA/RA individual who is responsible for the daily operations of the CA/RA. |
| Re-key | The process that subscribers must undertake to replace a certificate that is due to expire. |
| Registration Organisation Units (ROUs) | Units within the Human Services RO. There is usually one ROU for each Community of Interest (CoI) in the health sector PKI operated by Human Services. The ROU has responsibilities in the CoI in managing the subscribers in that CoI. |
| Registration Organisation Unit Operators (ROUOs) | Staff within the Human Services CoI, but not certificate controllers. ROUOs operate in accordance with the processes and procedures set out in the Human Services OCA CPS and relevant CPs. |
| Relying party (RP) | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Relying Party Agreement | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Repudiation | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Resource | Staff, property or information belonging to, or in the care of, an agency. |
| Revoke | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Risk | The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets. |
| Risk level | The level of risk, based on the Australian Standard for Risk Management (AS/NZS 31000), that is associated with a particular threat. |
| Risk tolerance | A subjective assessment of the maximum level of risk of the occurrence of a particular threat that the business is prepared to tolerate. |
| Sanitation | The process of erasing the information from the media or equipment. It doesn’t change the classification of the media or equipment. |
| Secure token | Known as a smart card or USB token. Formerly known as the Health Professional Card, PKI Key, Secure token or ikey |
| Security configuration baseline | Refers to configuration baseline parameters that perform a security enforcing function. The security configuration baseline is a subset of the configuration baseline. |
| Self-signed certificate | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Server | A computer that can send commands and receive responses along with data contents. |
| Service Level Agreement (SLA) | Agencies and organisations are encouraged to establish Service Level Agreements (SLAs) with the Certification Authority/ies they utilise. |
| Site certificate | A PKI certificate issued under the Human Services Site Certificate for Community of Interest (CoI) Site Certificate Policy (CP). Site certificates are issued in the form of a compact disc (CD) and are generally used by practices or locations (pharmacies, aged care facilities etc.) for authentication of electronic transactions. |
| Smart card | A card, about the size of a credit card, that contains a microprocessor and is capable of storing cryptographic information (such as keys and certificates) and performing cryptographic operations. A smart card is one way Human Services issues a PKI certificate. |
| Software vendor | An entity that supplies a software product to the subscribers. Human Services-supplied PKI certificates are used for conducting transactions through these software products. The vendors are represented through the ‘Medical Software Industry Association’ which meets on a periodic basis with Human Services. |
| Staff | Includes officers, agents, sub-agents, employees and sub-contractors. |
| Subscriber | An entity or healthcare individual who holds a Human Services PKI certificate. |
| Subscriber agreement | PKI Terms and Conditions of Use. |
| System administrator | The individual who maintains the hardware and software infrastructure. |
| Threat | *Refer to the definition found in the Identity and Access Management Glossary.*  See:  [https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf](%20https://www.dta.gov.au/files/authentication-framework/Identity-and-Access-Management-Glossary-V2.pdf) |
| Token | Media capable of storing the private key of a subscriber. Secure tokens now referred to as USB tokens and smart cards. |
| USB token | Is either:   * a device containing a microprocessor which is capable of storing cryptographic information (such as keys and certificates) and performing cryptographic operations; or * A USB card reader that can house a pre-cut card |
| Vetting | The process of acquiring information to assess a person's suitability for access to classified and/or sensitive material or to a designated secure area. |