



Australian Government

Medicare Australia

Health PKI Glossary v3.0

This work is copyright. You may download, display, print and re produce this material in unaltered form only (retaining this notice) for your personal, non-commercial use or use within your organisation. Apart from any use as permitted under the Copyright Act 1968, all other rights are reserved. Requests and enquiries concerning reproduction and rights should be addressed to The Manager, Media, Communications and Government Relations Branch, Medicare Australia National Office, PO Box 1001 Tuggeranong DC ACT 2901 or posted at www.medicareaustralia.gov.au.

Copyright © Commonwealth of Australia 2005.

The information contained in this Document is intended for the Medicare Australia Personnel charged with the management and operation of Medicare Australia Extended Services Registration Authority, those persons named as Recipients, and Subscribers and Relying Parties using Certificates within the SecureNet-HeSA Gatekeeper Health Public Key Infrastructure (Health PKI).

Contact:

Mailing address:

Registration Authority Manager
Medicare Australia
Locked Bag 6666
Tuggeranong DC ACT 2901
AUSTRALIA

This Document has been Authorised by the Medicare Australia Policy Management Authority (Medicare Australia PMA):

_____ Date: _____

General Manager or nominee, Information Technology and Services Division, Medicare Australia Representative.

Table of Contents

1	HEALTH PKI GLOSSARY	4
1.1	Purpose statement	4
1.2	Definitions	6

1 HEALTH PKI GLOSSARY

1.1 Purpose statement

1. The *Health PKI Glossary version 3* (the Glossary) defines words and terms for the purposes of the following public Gatekeeper Accredited Documents:
 - (a) *PO 01 - SecureNet-HeSA Gatekeeper Health PKI – Subscriber (Healthcare Individual) Certificate Policy version 3* (Individual CP);
 - (b) *CO 01 - SecureNet-HeSA Gatekeeper Health PKI - Subscriber (Healthcare Individual) Agreement version 3* (Individual Agreement);
 - (c) *PO 01 - SecureNet-HeSA Gatekeeper Health PKI - Subscriber (Healthcare Location) Certificate Policy version 3* (Location CP);
 - (d) *CO 01 - SecureNet-HeSA Gatekeeper Health PKI - Subscriber (Healthcare Location) Agreement version 3* (Location Agreement);
 - (e) *PO 02 - SecureNet-HeSA Gatekeeper Health PKI OCA Certification Practice Statement version 3* (OCA CPS); and
 - (f) *SecureNet-HeSA Gatekeeper Health PKI Registration Authority Privacy Policy version 3* (RA Privacy Policy).
2. The Glossary also defines words and terms for the purposes of the following non-public Gatekeeper Accredited Documents that exist to ensure the security of Medicare Australia Extended Services Registration Authority (RA) infrastructure.
 - (a) *AD 02 - SecureNet-HeSA Gatekeeper Health PKI - Registration Authority Operations Manual version 3*;
 - (b) *PO 03 - SecureNet-HeSA Gatekeeper Health PKI - Registration Authority Concept of Operations version 3*;
 - (c) *SE 01 - SecureNet-HeSA Gatekeeper Health PKI - Registration Authority Security Policy*;
 - (d) *SE 02 - SecureNet-HeSA Gatekeeper Health PKI - Registration Authority Protective Security Risk Review version 3*;
 - (e) *SE 03 - SecureNet-HeSA Gatekeeper Health PKI - Registration Authority Disaster Recovery Plan and Business Continuity Plan version 3*;
 - (f) *SE 04 - SecureNet-HeSA Gatekeeper Health PKI - Registration Authority Protective Security Plan version 3*; and
 - (g) *SE 06 - SecureNet-HeSA Gatekeeper Health PKI - Registration Authority Key Management Plan version 3*.
3. Where a words or term is 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".
4. Words and terms used in the *PO 01 SecureNet Gatekeeper Root Certification Authority issued Certificate Policy version 1* (RCA-issued CP) and the *Root Certification Authority Certification Practice Statement version 3* (RCA CPS) are defined in the *SecureNet AD 01D Glossary of Terms*

version 1. The *SecureNet AD 01D Glossary of Terms version 1* is located at the RCA Website: www.certificates-australia.com.au.

5. **The RCA and the OCA are operated by Cybertrust Australia Pty Ltd using the name SecureNet. All references to the SecureNet entity throughout this document refer to the Cybertrust Australia Pty Ltd entity, operating the RCA and/or the OCA in the name of SecureNet.**

1.2 Definitions

Term or Acronym	Explanatory notes
Acceptable Referee	Persons approved to support the Evidence of Identity process for Certificate Applicants. Acceptable Referees are responsible for sighting original Primary and Secondary Documents for Applicants and certifying that copies submitted to the RA are true copies of originals. The list of Acceptable Referees is detailed on the Healthcare Identification Reference Form (for paper-based Applications) and Acceptable Referee Identification Form (for online Applications).
Acceptable Referee Identification Form (ARIF)	RA form used during the Evidence of Identity (EOI) process for web-based Applications.
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.
Advanced Registration Module (ARM)	UniCERT software that supports the functions of the Registration Authority.
Agency	(a) a Department of State, or a Department of the Parliament, of the Commonwealth, a State or a Territory; (b) a body corporate or an unincorporated body established or constituted for a public purpose by Commonwealth, State or Territory legislation, or an instrument made under that legislation (including a local authority); (c) a body established by the Governor General, a State Governor, or by a Minister of State of the Commonwealth, a State or Territory; or (d) an incorporated company over which the Commonwealth, a State or a Territory exercises control.
Agency Head	The head of a Department of State or a Department of the Public Service or the Chief Executive Officer of any other authority or agency of the Australian Government, including the Chief of the Defence Force, and the Chief of Staff for the Navy, Army and Air-Force.
Applicant	The End Entity that applies for PKI Keys and Certificates in accordance with the applicable Certificate Policy.
Application	A submission, whether electronic or paper-based, made by an Applicant, for Registration for Location or Individual Certificates.
Application Reference Number	A number generated by the RA for each Application successfully submitted by an Applicant. Applicants are required to quote this number as well as their Secret Identifier in order to be given their Personal Identification Code by telephone.
Archiving	The storage of information and data to meet requirements of the Archives Act 1983 or other requirements, and to enable disaster recovery to occur.
Asset*	Anything that has value to an organisation.
Audit Report	A report prepared by an auditor detailing the results of the compliance audit.

Term or Acronym	Explanatory notes
Australian Federal Police (AFP)	AFP enforces Commonwealth criminal law, and protects Commonwealth and national interests from crime in Australia and overseas.
Australian Government Information Management Office (AGIMO)	A business group within the Department of Finance and Administration.
Australian Government Solicitor (AGS)	The AGS is a Commonwealth authority within the Attorney-General's portfolio that provides legal and related services primarily to Commonwealth departments and agencies.
Australian Security Intelligence Organisation (ASIO)	ASIO is 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 that will enable it to warn the government about activities or situations that might endanger Australia's national security.
Australian Security Vetting Service (ASVS)	The ASVS is a business unit of the Protective Security Coordination Centre of the Commonwealth Attorney-General's Department. The ASVS conducts initial security clearances and undertakes security clearance reviews and upgrades.
Authentication*	The provision of assurance of the claimed identity of an entity.
Authentication Key Pair	The Authentication Key Pair is used for Authentication and integrity.
Authorised	Authorised by the Agency Head or his/her delegate.
Authorised Auditor	A person or organisation (including an employee of that organisation) authorised in writing by the Gatekeeper Competent Authority, to audit a Certification Authority's or Registration Authority's ongoing compliance with the Approved Documents, criteria and policies.
Authorised Evaluator	A person or organisation (including an employee of that organisation) authorised in writing by the Gatekeeper Competent Authority, to evaluate a Certification Authority's or Registration Authority's compliance against the criteria and with the accreditation process.
Authorised Third Party	A person or entity empowered to act on behalf of a Subscriber to request Revocation or Reinstatement of a Certificate. Authorised third parties include, but are not limited to: (a) an administrator appointed to administer an entity's affairs; (b) a court with jurisdiction within an entity's area of operations; or (c) a third party with an appropriate Power of Attorney.
Authorised User	Relates to a Location Certificate Policy and means any person (including the person who is the HSE Representative) who: (a) is employed or otherwise engaged by the HSE at the Healthcare Location; and (b) is authorised by the Duly Authorised Officer to use the Location Keys and Location Certificates (and associated Passphrases, if any) to send and receive Health-related messages at the Healthcare Location.
B-Class safe	A Security Construction and Equipment Committee (SCEC) endorsed security container manufactured to ASIO-approved specifications.

Term or Acronym	Explanatory notes
Business Day	A Business Day is defined as 8:30am to 5:30pm local time (including daylight saving time where applicable) Monday to Friday inclusive, but excluding Public Holidays at the relevant location. For the purpose of a transaction involving Medicare Australia, the relevant location is the ACT.
C-Class safe	A Security Construction and Equipment Committee (SCEC) endorsed security container manufactured to ASIO-approved specifications.
Certificate ¹	<p>A set of information which at least:</p> <ul style="list-style-type: none"> (a) identifies the Certification Authority issuing the Certificate; (b) unambiguously names or identifies its owner; (c) contains the owner's Public Key; and (d) is digitally signed by the Certification Authority issuing it. <p>A Certificate is intended to bind the named Subscriber to the Private Key, which is mathematically linked to the Public Key specified in the Certificate.</p> <p>In Health PKI, Certificates are generated, signed and issued by the OCA and distributed by the RA.</p>
Certificate Information	The information needed to complete a Certificate as required by the Certificate Profile.
Certificate Policy (CP)	<p>The Document which sets out the policies applicable to the issue and use of a Certificate.</p> <p>The CPs applicable to Health PKI set out, among other things:</p> <ul style="list-style-type: none"> (a) the conditions under which the Key Pairs are generated by the RA, and the RA's functions, obligations and responsibilities; (b) the conditions under which Certificate Requests are generated by the RA, Certificates are signed and issued by the OCA, and distributed by the RA, as well as the OCA's functions, obligations and responsibilities; (c) the roles, obligations and responsibilities of the Subscriber and Relying Party; and (d) the liabilities of each of the entities referred to in the relevant CP. <p>Both Certificate Policies covered by this Glossary are located at the RA Website: www.hesa.gov.au.</p>
Certificate Profile	The specification of the fields to be included in a Certificate and the contents of each, as set out in Section 7.1 of the relevant Certificate Policy.
Certificate Revocation List (CRL)	A signed, time-stamped list of serial numbers of the Public Key Certificates of Subscribers (other than Certification Authority's) that have been Revoked prior to their scheduled Expiry.
Certification Authority (CA)	In Health PKI, the CA is an authority trusted to allocate a Distinguished Name to a Certificate Subscriber, and attest to the correctness of information concerning that user by signing the Digital Certificate for that Subscriber.

¹ Definition from SAA MP75 (Standards Australia).

Term or Acronym	Explanatory notes
Certification Practice Statement (CPS)	<p>Generally, a statement of the practices that a Certification Authority employs in issuing Certificates. In Health PKI, the CPS addresses the practices of the RA relevant to this process.</p> <p>The OCA CPS is located at the RA Website: www.hesa.gov.au</p>
Classified Material	<p>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.</p>
Client OCA	<p>A Gatekeeper Accredited Organisation Certification Authority that acts on behalf of an organisation and is under the operational control of an organisation, and which is part of the Health PKI i.e. it has submitted its Public Keys to the RCA and had them certified by the RCA. In Health PKI, this is the OCA.</p>
Commonwealth	<p>The Commonwealth of Australia, including the Competent Authority, that is subject to the <i>Financial Management and Accountability Act 1997</i> or the <i>Commonwealth Authorities and Companies Act 1997</i>, and includes their employees, servants and agents.</p> <p>For the purposes of Health PKI, the Commonwealth is represented by the CEO of Medicare Australia and by the Department of Finance and Administration.</p>
Commonwealth Protective Security Manual (CPSM)	<p>The Manual issued by the Attorney-General's Department, which is the principal means for disseminating Commonwealth protective security policies, principles, standards and procedures to be followed by all Commonwealth agencies for the protection of official information and resources.</p>
Competent Authority	<p>The entity which approves the Certification Authority's and Registration Authority's infrastructure and practices (including the Approved Documents and any changes to them) as meeting the criteria for Gatekeeper Accreditation. The Competent Authority for Health PKI is the Australian Government Chief Information Officer (AGCIO), AGIMO.</p>
Compliance Audit	<p>An audit of operations undertaken by an authorised evaluator to check that processes and procedures are in accordance with Gatekeeper Approved Documents.</p>
Compromise	<p>Any circumstance in which a Certificate should not be relied upon, including loss or theft of a Private Key.</p>
Compromised User	<p>A Subscriber who has had several instances of Certificate Revocation (assessed on a case by case basis) and is recorded as such by the RA.</p>
Concept of Operations (RA)	<p>A high level description of the process or procedures under which the RA system operates, and includes a description of inputs, processing and outputs.</p>
Confidential Information	<p>Each Certificate Policy (CP) defines (in Section 2.8.1) the information which is protected from disclosure under that CP.</p>
Confidentiality*	<p>The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.</p>
Confidentiality Key Pair	<p>The Confidentiality Key Pair is used to protect the Confidentiality of an electronic message.</p>

Term or Acronym	Explanatory notes
Configuration Control Board (CCB)	The Registration Authority committee responsible for controlling any changes to the RA's architecture.
CP	See Certificate Policy.
CPS	See Certificate Practice Statement.
CRL	See Certificate Revocation List.
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.
Cybertrust Australia Pty Ltd	Cybertrust Australia Pty Ltd, ABN 74073665175. References to SecureNet are references to the Cybertrust Australia Pty Ltd legal entity.
DAO	See Duly Authorised Officer.
Decrypt	The practice of recovering an encrypted message by reverting from cipher text to plain language.
Defence Signals Directorate (DSD)	The Commonwealth authority in matters pertaining to communications and computer security. It is located within the Department of Defence. Website www.dsd.gov.au
Department of Finance and Administration (Finance)	The Agency responsible for the administration of the Gatekeeper strategy and accreditation program.
Digital Signature*	A mathematical construct that creates a unique and unforgeable identifier of the owner of the Distinguished Name.
Disaster Recovery and Business Continuity Plan for Medicare Australia Registration Authority	RA Document which outlines the internal processes to be followed in the event of a security incident, or the RA system and/or Medicare Australia databases being unavailable, or in the event of a major catastrophe affecting RA operations. Not publicly available.
Distinguished Name	A unique identifier assigned to each Certificate Applicant, having the structure required by the Certificate Profile.
Document	Anything on which information is recorded by any means, including words, symbols, images or electro-magnetic impressions.
Duly Authorised Officer (DAO)	Is applicable to Location Certificates, and means a person that the Health Sector Entity (HSE) authorises to act on its behalf in relation to: (a) applying for Location Keys and Certificates; (b) appointing Authorised Users; and (c) managing Location Keys and Certificates. Where the HSE is an individual the DAO may be that person himself/herself.
eBusiness Service Centre	The Centre within the RA (Medicare Australia) which provides telephone-based support for PKI-related issues.
Encrypt	Practice of converting plain language to cipher text.
End Entity	Either a Relying Party or a Subscriber.
Endorsed Supplier	An entity that is pre-qualified under the Endorsed Supplier Arrangement (ESA), which provides pre-qualification for suppliers in the Information Technology, Major Office Machine, Commercial Office Furniture and Auctioneering industries to sell into the government market place.

Term or Acronym	Explanatory notes
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. The Australian EPL is published at www.dsd.gov.au
Evidence Of Identity (EOI)	The process implemented to determine the identity of a person or entity using Documents or other information identifying the person and/or entity.
Expire	In Health PKI, refers to the end of a Certificate's two year lifetime.
Extended Services Registration Authority	See Registration Authority.
Facility Security Officer (FSO)	The FSO examines system records and event logs to ensure that RA Personnel have acted within their responsibilities and within the stated security policy.
Finance	See Department of Finance and Administration.
Forensic Plan	A plan documenting the RA's approach to maintaining security incidents and ensuring that evidence pertaining to such incidents is admissible in a court of law.
Gatekeeper	Gatekeeper is the Commonwealth strategy for the use of Public Key Infrastructure (PKI) and a key enabler for the delivery of the Commonwealth's Government Online agenda.
Gatekeeper Accreditation	Formal recognition of a Public Key Infrastructure Service Provider granted by the Gatekeeper Competent Authority against the Gatekeeper Certification Authority Accreditation criteria or the Registration Authority Accreditation criteria, as applicable. These criteria may be found at: www.gatekeeper.gov.au . Gatekeeper Accreditation may be granted to a PKI Service Provider of the kind set out below: (a) Core Registration Authority; (b) Registration Authority Extended Services (Full Accreditation); or (c) Certification Authority (Full Accreditation).
Gatekeeper Approved Documents	Refers to Documents that have been considered and approved by Gatekeeper during the Accreditation process.
Gatekeeper Compliance Audit Program	Annual compliance audit undertaken by the RA to ensure consistency with Gatekeeper Approved Documents, as required by the Gatekeeper Accreditation MOA (Registration Authority) with Finance.
Gatekeeper Head Agreement (Certification Authority)	The Head Agreement in force between the Commonwealth of Australia (Finance) and a Certificate Authority (CA) (in Health PKI this is Cybertrust Australia Pty Ltd) which recognises the CA's Gatekeeper Accreditation and sets up the legal framework for the maintenance of that accreditation.
Gatekeeper Memorandum of Agreement (MOA) (Registration Authority)	The MOA in force between the Department of Finance and Administration and Medicare Australia that recognises the RA's Gatekeeper Accreditation and sets up the legal framework for the maintenance of that accreditation.
Gatekeeper Policy Committee (GPC)	Provides a forum for discussion and development of policy and administrative changes to the Gatekeeper accreditation and recognition programs. The GPC reports to the Gatekeeper Competent Authority.

Term or Acronym	Explanatory notes
Health eSignature Authority (HeSA)	The name previously given to the section within Medicare Australia is charged with the management and operation of Medicare Australia Extended Services Registration Authority (RA or ESRA) in the Health PKI Hierarchy. RA's Website: www.hesa.gov.au .
Health Sector	The term Health Sector is interpreted broadly and includes, but is not restricted to the following groups: (a) healthcare practitioners (doctors, specialists, pharmacists, pathologists, nurses, etc); (b) allied health practitioners (such as physiotherapists, chiropractors, osteopaths, podiatrists, prosthodontists, dentists etc); (c) alternative care practitioners (such as homeopaths, naturopaths, herbalists, etc); (d) associated staff of the above groups (such as practice staff and staff in representative groups); and (e) Commonwealth, State, Territory and/or local government representatives involved with health sector initiatives.
Health Sector Entity (HSE)	An entity which provides healthcare or conducts related activities within the Health Sector in Australia at a Location, which entity may be a natural person or a business entity (eg company, partnership, association etc).
Healthcare Individual	An individual providing healthcare or conducting related activities within the Health Sector in Australia.
Healthcare Individual Agreement	Agreement that establishes a contractual relationship between the RCA / OCA and the RA and the Individual for the provision of certification and Registration services, and specifies the obligations and responsibilities of all Parties to that Agreement.
Healthcare Location	A place, building or premises (permanent, temporary, mobile or fixed) where a HSE is involved in healthcare activities and associated services.
Healthcare Location Agreement	Agreement that establishes a contractual relationship between the RCA / OCA and the RA and the HSE for the provision of certification and Registration services, and specifies the obligations and responsibilities of all Parties to that Agreement.
Healthcare Public Directory	The publicly accessible directory that lists unexpired, Suspended, Revoked and Expired Location and Individual Certificates.
Healthcare x.500 Directory	See Healthcare Public Directory.
Health-related messages	Messages between Subscribers in the Health Sector in relation to the provision of healthcare or related activities.
HeSA	See Health eSignature Authority.
HeSA Application Manager (HAM)	The Registration Authority hardware and software which is dedicated to managing the flow of Individual and Location Application requests.
Highly Protected	The highest level of non-national security classification.
HSE	Health Sector Entity
HSE Representative	The person nominated by the HSE to sign the Location Agreement and to certify that the DAO is authorised to act on behalf of the HSE.

Term or Acronym	Explanatory notes
Identification Reference Form (IRF)	RA form used during the Evidence of Identity (EOI) process for paper-based Applications.
Identity	The most apparent identity of a user, which can either be the real name of that user or a pseudonym, confirmed through a range of Gatekeeper Approved processes.
Incident	An activity which: <ul style="list-style-type: none"> (a) causes damage or is intended to cause damage to RA information assets; (b) prevents or is intended to prevent the RA from carrying out its designed function; (c) indicates someone has attempted an unauthorised access; indicates that someone has had opportunity to attempt an unauthorised access; (d) indicates that a member of RA staff has been the target of a so-called social engineering attack; (e) gains, or attempts to gain, unauthorised access to sensitive material; or (f) results in the unauthorised disclosure of sensitive data.
Incident Investigation Officer (IIO)	The RA individual responsible for the management of an Incident until the Incident closure or until he/she is formally relieved by someone in higher authority.
Incident Response Plan	Response procedures to deal with incidents arising from threats and risks that are specific to the RA systems.
Incident Response Team (IRT)	Team of RA Personnel established for the specific purpose of investigating an Incident. The IRT has authority to seek relevant expertise from other appropriate organisations (eg. AFP) to address the specific needs of the Incident.
In-Confidence	The classification given to material and resources, other than national security classified information or Cabinet Documents, which require a limited degree of protection (i.e. the lowest level of non national security classification).
Individual Certificate	A Certificate issued to a Healthcare Individual, in accordance with the Individual CP (see also Certificate).
Individual Keys	The Key Pairs assigned to a Healthcare Individual. The Public Key is specified in the corresponding Individual Certificate.
Information Privacy Principles (IPPs)	The principles set out at section 14 of the <i>Privacy Act 1998</i> (Cwth).
Intellectual Property Rights (IPR)	Intellectual Property Rights means: <ul style="list-style-type: none"> (a) 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 (b) 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.
IPPs	See Information Privacy Principles.
Key*	A sequence of symbols that controls the operation of a cryptographic transformation (eg. encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification).

Term or Acronym	Explanatory notes
Key Management Plan (RA)	RA Document which describes the Key management procedures for the RA. Not publicly available.
Key Pair	Expression used to describe the Public and Private Keys of Public Key Infrastructure. A matching Private Key and Public Key which are mathematically linked such that either one will decrypt ciphertext produced with the other and verification of the Digital Signature.
Location Certificate	A Certificate issued to a Health Sector Entity in respect of a Healthcare Location, in accordance with the Location CP (see also Certificate)
Location Keys	The Key Pair assigned to a Health Sector Entity in respect of a Healthcare Location. The Public Key is specified in the corresponding Location Certificate.
Location Keys and Certificates	Abbreviation for Healthcare Location Keys and Healthcare Location Certificates.
Loss	<p>All losses, liabilities, damages, fines, costs, interest, fees and expenses (including reasonable legal costs and expenses of a solicitor/own client basis and disbursements and costs of investigation, litigation, settlement, judgment interest and penalties and the value of internal management and staff time) whether present or future or unascertained, actual or contingent, and includes in respect of that loss:</p> <p>(a) the cost of taking reasonable, preventative,</p> <p>(b) protective remedial or mitigatory action; and</p> <p>(c) the cost of obtaining any replacement services to rectify, remedy or mitigate the damage caused by the relevant event.</p>
Media/Equipment Removal Form	RA form that must be completed by RA Personnel wanting to remove RA media / equipment from the premises. All requests must be approved and signed by the RAOM.
Medicare Australia	<p>Medicare Australia is a statutory agency established by the <i>Medicare Australia Act 1973</i>. Medicare Australia is within the Department of Human Services under the Minister for Human Services.</p> <p>Website: www.medicareaustralia.gov.au</p> <p>Medicare Australia is the Gatekeeper Accredited Extended Services Registration Authority (RA) in the Health PKI Hierarchy. It is a trusted element of that Hierarchy, and is a separate legal entity to Cybertrust Australia Pty Ltd (which operates the RCA and the OCA using the name SecureNet).</p> <p>There is a section within Medicare Australia that is charged with the management and operation of Medicare Australia Extended Services Registration Authority (RA) in the Health PKI Hierarchy.</p> <p>RA's Website: www.hesa.gov.au.</p>
Medicare Australia - known	Applicants who are individual people and have an established claims/payments history with Medicare Australia (and previously with the Health Insurance Commission). History must be for a minimum period of 12 months, and include recent business transactions.

Term or Acronym	Explanatory notes
Moral Rights	Moral Rights means 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.
National Privacy Principles (NPPs)	Additional privacy principles in the <i>Privacy Act 1988</i> (Cth) which came into effect for private sector organisations on 21 December 2001.
Non-Repudiation	Refers to the relative difficulty of one of the entities involved in a communication trying to deny having participated in all or part of the communication.
Notice	A Notice is any consent, information, application, request or any other communication provided under or in connection with the relevant Certificate Policy.
NPPs	See National Privacy Principles.
Object Identifier (OID)	The name of an object and 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 " <i>object identifier component</i> ", and there must be at least two components to form a valid object identifier.
OCA	Organisation Certification Authority.
OCA Certification Practice Statement (OCA CPS)	The CPS governing the operations of the OCA.
OCA Website	OCA operational documentation can be found at the OCA's Website: www.certificates-australia.com.au
Operations Manual (RA)	RA Document which provides information relating to the operations of the RA and is intended for use by Personnel charged with the management and operation of the RA. Not publicly available.
Operations Room	Secured area for RA Personnel involved with administrative aspects of Certificate Registrations and related services.
Oracle database	RA database that contains all the transactions associated with Certificate profiles, key generation and signing (registration), revocation, suspension and re-key requests.
Organisation Certification Authority	<p>The Organisation Certification Authority (OCA) operated by Cybertrust Australia Pty Ltd and issuing Certificates in the name of SecureNet, which generates, signs and issues Certificates and returns them to the RA for distribution to Subscribers. The OCA is Gatekeeper Accredited and is a trusted internal element in Health PKI. A reference to the OCA includes, where applicable, a reference to its Personnel.</p> <p>OCA operational documentation can be found at the OCA's Website: www.certificates-australia.com.au</p>
Out-of-bounds Check	That activity which is concerned primarily with verification of the personal and other details provided by an Applicant during the Registration process.
Party	For the Location Certificate means the OCA (operated by Cybertrust Australia Pty Ltd, issuing Certificates in the name of SecureNet), the RA (Medicare Australia) and the Health Sector Entity (HSE).

Term or Acronym	Explanatory notes
	For the Individual Certificate means the OCA (operated by Cybertrust Australia Pty Ltd, issuing Certificates in the name of SecureNet), the RA (Medicare Australia) and the Individual.
Passphrase	A string of characters to enable access to a system.
Personal Identification Code (PIC)	An Access Control mechanism used during Key transport to import Location or Individual Private Keys into a software application being used by the Location or Individual.
Personal Information	Has the meaning given in the <i>Privacy Act 1988</i> (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 PKI, Personal Information may include information or an opinion about an individual obtained in connection with any dealings with the RA or the OCA.
Personnel	'Personnel' includes officers, agents, sub-agents, employees and sub-contractors of either a CA or the RA.
PKI Entity	Any Entity participating in Health PKI, including the RCA, the OCA, the RA and Subscribers.
PKI Service Provider	Any PKI entity which has roles, functions and obligations or rights under an Individual or Location Certificate Policy, other than an End Entity. PKI Service Providers include the RCA, the OCA and the RA.
Policy Management Authority (PMA)	The authority which oversees and manages compliance by a Certification Authority and/or Registration Authority with its Certificate Policy/ies and other Approved Documents.
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 section 1.1.3.2 of the applicable CP.
Primary Identification Document	A document which has a value of 70 EOI points as defined in the <i>Financial Transaction Report Act 1988</i> .
Privacy Policy	A Document which describes policies dealing with the collection, storage, access, use and disclosure of Personal Information. The Medicare Australia Registration Authority Privacy Policy is published on the RA's Website.
Private Authentication Key	The Private Key used to digitally sign a message.
Private Confidentiality Key	The Private Key used to decipher or decode the contents of a message which has been Encrypted for Confidentiality.
Private Key*	That Key of an entity's asymmetric Key Pair which should only be used by that entity, and should not be disclosed to any other person.
Protected	The classification applied to sensitive material requiring a reasonable degree of protection (i.e. the middle sensitive material classification).
Protective Security Plan (RA)	The plan that identifies the security mechanisms for the RA infrastructure. 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 to RA. Not publicly available.

Term or Acronym	Explanatory notes
Protective Security Risk Review (RA)	The Document that details the annual evaluation of threats and risks to the RA's business operations. Not publicly available.
PSM	See Commonwealth Protective Security Manual
Public Authentication Key	The Public Key used to verify a Digital Signature.
Public Confidentiality Key	The Public Key used to encipher or encode the contents of a message for Confidentiality.
Public Key	That Key of an entity's asymmetric Key Pair which can be made public.
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 digital Keys and Certificates. For the Health Sector, PKI enables the transfer of sensitive medical information across the Internet, without Compromising the individual's right to privacy.
RA	See Registration Authority.
RA Electronic Registration Subsystem	The system which provides Applicants with the ability to use the Internet browser of their choice to lodge an Application for Individual and Location Certificates electronically through the RA's Website.
RA Key Register	RA register which lists Personnel who are formal custodians of the following Keys: (a) Medicare Australia Registration Authority Private Key; (b) HeSA ARM Private Key; and (c) HeSA RAO Private Key. The Key Register is stored securely in the RA Operations Room.
RA Materials	Means the documents specified in clause 2.9.2 of the Health PKI Individual CP and the Location CP in which Intellectual Property Rights are owned by the RA, Medicare Australia (Commonwealth represented by the CEO of Medicare Australia).
RA Re-key Request Subsystem	The system that provides existing Subscribers with the ability to submit a Re-key request through the RA's Web Server by using an Internet Browser of their choice.
RA System Administrator	The RA System Administrator is responsible for maintaining the technical components of the RA system.
RA Visitor's Log	Record of visitors to the RA Operations Room, all of whom must be escorted at all times, for purposes of auditing.
RA Website	The RA Website can be found at www.hesa.gov.au
RAO	Registration Authority Operator.
RAOM	Registration Authority Operations Manager.
RCA	Root Certification Authority.
RCA / OCA Materials	Means the documents specified in s 2.9.1 of the Individual CP and the Location CP in which Intellectual Property Rights are owned by the RCA / OCA (Cybertrust Australia Pty Ltd).
Recipient*	The entity that gets (receives or fetches) a message.
Record	A Record is a Document.
Redundancy mode	Any instance of system failure which can be resolved within the scope of the Redundancy Recovery mode: no loss of data; approximately one hour's loss of functionality; and in the worst case, a reduction in ability to provide a high throughput of Registrations.

Term or Acronym	Explanatory notes
Registration	The process of establishing the identity of an individual and documentation of proof to a prescribed level of confidence, which results in a Subscriber being provided with Keys and Certificates.
Registration Authority (RA)	<p>The entity which carries out a number of functions on behalf of a Certification Authority (CA), including establishing the identity of an Applicant for Keys and Certificates and requesting generation of Certificates from the CA.</p> <p>For Health PKI, the Registration Authority is Medicare Australia. Medicare Australia is Gatekeeper Accredited as an Extended Services Registration Authority.</p> <p>There is a section within Medicare Australia that is charged with the management and operation of Medicare Australia Extended Services Registration Authority (RA) in the Health PKI Hierarchy.</p>
Registration Authority (KeyGen) Subsystem	The component of the RA system that generates the PKI Keys during the Registration process.
Registration Authority Manager (RAM)	The RA individual who is responsible for overseeing the management of the RA.
Registration Authority Operations Manager (RAOM)	The RA individual who is responsible for the daily operations of the RA.
Registration Authority Operator (RAO)	The RA Personnel responsible for processing Evidence of Identity checks and Certificate requests.
Registration Information	Information that an Applicant is required to disclose for the purpose of obtaining Keys and Certificates. Registration Information may include information which is Personal Information or Confidential Information.
Re-Image / Restore mode	Any instance of system failure which can be resolved within the scope of the Re-Image / Restore Recovery mode: at worst one day's loss of data and approximately one day's loss of functionality. During this mode business continuity activities will be employed to provide for continued support of Revocation / Suspension activities.
Reinstatement	The process of moving from suspended Certificate status to active status.
Re-key	The process that Subscribers must undertake to replace a Certificate that is due to expire.
Re-key Reference Number	A number generated by the RA for each Certificate that is due to expire. Subscribers receive this number when receiving Re-key reminder Notices, and are required to quote this number and their Secret Identifier in order to be given the Personal Identification Code for their new Certificates by telephone.
Relying Party	<p>A person or entity which relies on a Certificate for Authentication, Non-Repudiation or Confidentiality.</p> <p>In Health PKI, a Relying Party must also be a Subscriber. (Note: an Individual Subscriber can rely on a message signed by a Location Subscriber and vice versa.)</p>
Repudiation*	Denial by one of the entities involved in a communication of having participated in all or part of the communication.

Term or Acronym	Explanatory notes
Resource	Personnel, property or information belonging to, or in the care of, an Agency.
Restart mode	Any instance of system failure which can be resolved within the scope of the Restart Recovery mode: at worst one week's loss of data and approximately one week's loss of functionality. During this mode, business continuity activities will be employed to provide for continued support of Revocation / Suspension activities.
Revoke	The process undertaken by the OCA, generally in response to a request by the RA, to invalidate a Certificate. A Subscriber may request Revocation through the RA.
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 4360), 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.
Root Certification Authority (RCA)	The CA which is the highest trusted element in Health PKI. Cybertrust Australia Pty Ltd, in its capacity as owner and operator of the RCA which issues Certificates in the name of SecureNet.
Root Certification Authority-issued Certificate Policy (RCA-issued CP)	The CP governing the issue of Certificates by the RCA to its Client Organisation Certification Authorities, including the OCA.
Sanitation	The process of erasing the information from the media or equipment. It does not of itself change the classification of the media or equipment.
Secondary Identification Document	Documents, other than Primary Identification Documents, that provide Evidence of Identity (EOI). The value of EOI points for Secondary Identification Documents depends on the type of document and is specified in the <i>Financial Transactions Report Act 1988</i> .
Secret Identifier	The secret word or phrase nominated by an Applicant or Subscriber for use in the context of telephone enquiries with the RA and telephone receipt of the Personal Identification Code.
Secure Operations Room	Secured area within the RA Operations Room for RA Personnel involved with security-related aspects of Certificate Registrations and related services.
SecureNet	The entity SecureNet Limited, now known as Cybertrust Australia Pty Ltd.
SecureNet Trust Centre	The SecureNet secure physical facility, owned by Cybertrust Australia Pty Ltd, and rated to Highly Protected or above, and staffed by security-cleared personnel, which hosts PKI applications and systems including the SecureNet Root Certification Authority and Client OCA.

Term or Acronym	Explanatory notes
SecureNet-HeSA Gatekeeper Health Public Key Infrastructure (Health PKI)	Cybertrust Australia Pty Ltd, in its capacity as owner and operator of the RCA which issues Certificates in the name of SecureNet.
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.
Security Policy for Medicare Australia Registration Authority	RA Document which identifies the security objectives for the RA. Not publicly available.
Security-in-Confidence	One of the X-IN-CONFIDENCE markings, which is used when the compromise of the information could cause limited damage to the Commonwealth, the Government, commercial entities or members of the public.
Standards Australia	An Australian organisation whose mission is to develop and promote the use of standards. Website: www.standards.com.au
Subscriber	For a Healthcare Location Certificate Policy (Location CP) a Subscriber is a Health Sector Entity (acting through a Health Sector Entity Representative and Duly Authorised Officer) where: (a) the Health Sector Entity Representative has signed the Healthcare Location Agreement on behalf of the HSE; and (b) the HSE has been deemed to be in possession of Location Keys and Certificates pursuant to the Location CP.
	For a Healthcare Individual Certificate Policy (Individual CP) a Subscriber is an Individual who: (a) has signed the Healthcare Individual Agreement; and (b) has been issued with and is deemed to be in possession of Individual Keys and Certificates pursuant to the Individual CP.
Subscriber Agreement	Agreement that establishes a contractual relationship between the RCA / OCA and the RA and either the Individual or the HSE for the provision of certification and Registration services, and specifies the obligations and responsibilities of all Parties to that Agreement. (see also Healthcare Individual Agreement and Healthcare Location Agreement)
Suspended	A reversible state of Revocation which allows a Certificate to be unrevoked, if it can be demonstrated that no Certificate Compromise has occurred. During the period of Suspension (maximum of two days), the Certificate is included in the CRL with a Revocation reason of 'Suspended'.
System Access Request Form	The form that RA Personnel are required to sign, acknowledging their responsibilities prior to being issued with a logon and user request for the RA systems.
System Administrator	The RA individual who maintains the RA's hardware and software infrastructure.
Threat*	(a) A potential event that could adversely affect the status of a Resource, such as through loss, damage, destruction, reduced capacity, compromise, etc. (b) A potential violation of security. (c) A potential cause of an unwanted incident which may result in harm to a system or organisation.

Term or Acronym	Explanatory notes
Token	Media capable of storing the Private Key of a Subscriber. Tokens include secure tokens and other devices such as smart cards.
User	An authorised entity that uses a Certificate, including an organisation, individual or Relying Party, but not including the CA issuing the certificate.
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.
Website	Refer to OCA Website and/or RA Website

NOTE: Terms or acronyms marked (*) have been adopted from ISO draft (subject to change)
 Glossary of IT security terminology prepared by JTC1 SC 27 at:
<http://www.din.de/ni/sc27/doc6.html>