



Australian Government

Medicare Australia

PO 01

**SecureNet-HeSA Gatekeeper Health PKI –
Subscriber (Healthcare Individual)
Certificate Policy 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 Medicare Australia Personnel, 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

Glossary:

Definitions are provided in the *Health PKI Glossary version 3*, which is available at the RA's Website.

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	Introduction	6
1.1	Overview.....	6
1.1.1	Overview of SecureNet-HeSA Gatekeeper Health Public Key Infrastructure (Health PKI)	6
1.1.2	Key Documents	7
1.1.2.1	Policy Documents.....	7
1.1.2.2	Subscriber Agreement	7
1.1.2.3	Priority of Documents	7
1.1.2.4	Glossary	8
1.1.3	Certificates issued under this Document.....	8
1.1.3.1	Certificate types	8
1.1.3.2	Policy Qualifier.....	8
1.2	Identification	8
1.2.1	X.500 Object Identifier hierarchy	8
1.2.2	Standards.....	8
1.3	Community and Applicability	9
1.3.1	Certification Authorities	9
1.3.1.1	RCA	9
1.3.1.2	OCA	9
1.3.2	Registration Authority	9
1.3.3	End Entities	9
1.3.4	Applicability	9
1.3.5	Policy authorities	10
1.4	Contact Details	10
1.4.1	Specification administration organisation.....	10
1.4.2	Contact person.....	10
1.4.3	Person determining CPS suitability for the policy	10
2	General Provisions.....	11
2.1	Obligations	11
2.1.1	CA obligations	11
2.1.1.1	RCA obligations	11
2.1.1.2	OCA obligations	12
2.1.2	RA obligations	13
2.1.3	Subscriber obligations	14
2.1.3.1	Accuracy of information	14
2.1.3.2	Purposes for which Individual Keys and Certificates may be used	14
2.1.3.3	Effect of digital signatures with Individual Keys and Certificates.....	14
2.1.3.4	Protection of Individual Keys and Certificates	14
2.1.3.5	Other Subscriber obligations.....	15
2.1.4	Relying Party obligations.....	15
2.1.5	Repository obligations	15
2.2	Liability.....	15
2.2.1	CA liability	16
2.2.1.1	RCA liability	16
2.2.1.2	OCA liability	16
2.2.2	RA liability	16
2.2.3	Subscriber liability	17
2.2.4	Relying Party liability.....	17
2.2.5	Commonwealth liability	17
2.2.6	Limited Warranties.....	17
2.2.7	Contribution.....	18
2.2.8	Duty to Mitigate.....	18
2.2.9	Indemnity from Subscriber	18
2.2.10	Indemnity from Relying Party	18
2.3	Financial responsibility	18
2.3.1	Indemnification by Relying Parties.....	18

2.3.2	Fiduciary relationships	18
2.4	Interpretation and Enforcement	19
2.4.1	Governing Law	19
2.4.1.1	The Individual CP and Subscriber Agreement	19
2.4.1.2	Applicable contract structure	19
2.4.2	Severability, survival, merger, Notice	19
2.4.2.1	Severability	19
2.4.2.2	Survival (Continuing obligations)	19
2.4.2.3	Notice	20
2.4.2.4	Assignment and novation	21
2.4.3	Dispute resolution procedures	21
2.4.3.1	Disputes relating to Individual CPs	21
2.4.3.2	Disputes relating to other contractual relationships	22
2.5	Fees	22
2.5.1	Certificate issuance or Re-key fees	22
2.5.2	Certificate access fees	22
2.5.3	Revocation or status information access fees	22
2.5.4	Fees for other services such as policy information	23
2.5.5	Refund policy	23
2.6	Publication and Repository	23
2.6.1	Publication of information	23
2.6.2	Frequency of publication	23
2.6.3	Access Controls	23
2.6.4	Repositories	23
2.7	Compliance Audit	24
2.8	Confidentiality	24
2.8.1	Types of information to be kept Confidential	24
2.8.1.1	Information disclosed by Applicants	24
2.8.1.2	Personal information	24
2.8.1.3	Confidential Information	25
2.8.1.4	Other Protected Information	26
2.8.2	Types of information not considered Confidential	26
2.8.2.1	Certificate Information	26
2.8.3	Disclosure of Certificate Revocation/Suspension information	26
2.8.4	Release to law enforcement officials	26
2.8.5	Release as part of civil discovery	26
2.8.6	Disclosure upon owner's request	27
2.8.7	Other information release circumstances	27
2.9	Intellectual Property Rights	27
2.9.1	RCA / OCA Materials	27
2.9.2	RA Materials	27
2.9.3	Healthcare Public Directory	28
2.9.4	Subscriber's IPR	28
3	Identification and Authentication	29
3.1	Initial Registration	29
3.1.1	The process	29
3.1.2	Types of names	30
3.1.3	Need for names to be meaningful	31
3.1.4	Rules for interpreting various name forms	31
3.1.5	Uniqueness of names	31
3.1.6	Name claim dispute resolution procedure	31
3.1.7	Recognition, authentication and role of trademarks	31
3.1.8	Method to prove possession of Private Key	31
3.1.9	Authentication of organisation identity	31
3.1.10	Authentication of individual identity	32
3.2	Routine Re-key	32
3.2.1	Defining Re-key	32
3.2.2	Subscriber initiation of Re-key	32
3.2.3	RA initiated Re-key	33
3.2.4	Information changes during the Re-key process	33
3.2.5	Token and PIC distribution during the Re-key process	33
3.3	Re-key after Revocation	33
3.4	Revocation request	34
4	Operational Requirements	35
4.1	Certificate Application	35

4.2	Certificate Issuance	35
4.3	Certificate acceptance	35
4.4	Certificate Suspension and Revocation.....	36
4.4.1	Circumstances for Revocation	36
4.4.2	Who can request Revocation	37
4.4.3	Procedure for Revocation requests	37
4.4.3.1	RA processing.....	37
4.4.3.2	OCA processing	37
4.4.3.3	Subscriber responsibilities	37
4.4.4	Revocation request grace period	37
4.4.5	Circumstances for Suspension	38
4.4.6	Who can request Suspension	38
4.4.7	Procedure for Suspension requests	38
4.4.8	Limits on Suspension period	38
4.4.9	CRL issuance frequency	38
4.4.10	CRL checking requirements	38
4.4.11	Online revocation/status checking availability.....	38
4.4.12	Online Revocation checking requirements	38
4.4.13	Other forms of Revocation advertisements available.....	38
4.4.14	Checking requirements for other forms of revocation advertisements	38
4.4.15	Special requirements regarding Key Compromise.....	39
4.5	Security Audit procedures	39
4.6	Records Archival.....	39
4.7	Key changeover	39
4.8	Compromise and disaster recovery.....	39
4.9	CA or RA termination	40
5	Physical, procedural, and Personnel security controls.....	41
6	Technical Security Controls.....	42
7	Certificate and CRL Profiles.....	44
7.1	Certificate Profile.....	44
8	Specification Administration.....	45
8.1	Specification change procedures	45
8.2	Publication and notification policies	45
8.2.1	Initial publication.....	45
8.2.2	Change	45
8.2.3	Actual publication	46
8.3	Approved Document approval procedures	46

1 Introduction

1.1 Overview

1.1.1 Overview of SecureNet-HeSA Gatekeeper Health Public Key Infrastructure (Health PKI)

1. The SecureNet-HeSA Gatekeeper Health Public Key Infrastructure (Health PKI) facilitates electronic connectivity within the Australian Health Sector. The Registration Authority's Website (www.hesa.gov.au) provides additional information about Health PKI.
2. In general, a PKI consists of a hierarchy of trusted elements and End Entities. In Health PKI the hierarchy of trusted elements comprises:
 - a) the Root Certification Authority (RCA);
 - b) the Organisation Certification Authority (OCA); and
 - c) the Registration Authority (RA).
3. The RA is the Medicare Australia Extended Services Registration Authority which delivers RA services.
4. 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.
5. End Entities are Subscribers and Relying Parties. For information about the roles played by these entities, please refer to clause 1.3 of this CP.
6. The RCA / OCA and RA in Health PKI (refer to clause 1.3 of this CP) are Gatekeeper Accredited. The Department of Finance (Finance) is the agency responsible for the administration of the Gatekeeper Accreditation. The criteria for Gatekeeper Accreditation is found at www.gatekeeper.gov.au
7. Healthcare Individual Keys and Certificates (Individual Keys and Certificates) enable secure electronic communications in the health environment, between Subscribers in Health PKI. Individual Keys and Certificates also allow for electronic signing to verify identity. For information on Certificate scope, refer to clauses 1.3.3 and 1.3.4 of this CP.
8. Under Health PKI, the following Key Pairs are issued:
 - a) an Authentication Key Pair, which includes Public and Private Keys; and
 - b) a Confidentiality Key Pair, which includes Public and Private Keys.
9. The Authentication Key Pair is used for Authentication and integrity. The Subscriber uses their Private Authentication Key to

digitally sign an electronic message that they have created. The Relying Party then uses the Subscriber's Public Authentication Key to verify the Digital Signature of the Subscriber when the message is received.

10. The Confidentiality Key Pair is used to protect the Confidentiality of an electronic message. The Subscriber uses the Recipient's Public Confidentiality Key to Encrypt the message before sending. The Recipient then uses their Private Confidentiality Key to Decrypt the message once received.
11. Individual Certificates are Gatekeeper Type 1 Grade 2 Certificates. For further information about Gatekeeper, see www.gatekeeper.gov.au

1.1.2 Key Documents

1.1.2.1 Policy Documents

1. Key policy Documents for Health PKI are the Certification Practice Statement Documents, the Certificate Policy Documents and Subscriber Agreement Documents. These Documents can be accessed via the RA's Website.
2. This Individual CP outlines the policies that sit behind the Individual Certificates issued under Health PKI, and provides obligation and liability information. A separate CP contains information for Location Certificates issued by the OCA under Health PKI.
3. The PO 02 SecureNet-HeSA Gatekeeper Health PKI – Health Organisation Certification Authority Certification Practice Statement version 3 (OCA CPS) describes the practices of the OCA and the RA relevant to Health PKI.

1.1.2.2 Subscriber Agreement

1. An Applicant is required to enter into an Individual Agreement (*CO 01 SecureNet-HeSA Gatekeeper Health PKI - Healthcare Subscriber (Individual Agreement) version 3*). Once the RA issues an Applicant with Individual Keys and Certificates, the Applicant becomes the Subscriber.
2. The Individual Agreement forms a contract between the Subscriber, the RA and the OCA in relation to the possession and use of the Individual Keys and Certificates. This contract comes into effect for all Parties when:
 - a) the Applicant signs the Individual Agreement;
 - b) the RA requests the OCA to generate, sign and issue the Applicant's Certificates; and
 - c) the OCA generates, signs and issues the Applicant's Certificates.

1.1.2.3 Priority of Documents

1. If there is any conflict between provisions in key policy Documents, the following order of precedence applies:

- a) this CP; then
- b) the Individual Agreement; then
- c) the OCA CPS (PO 02 SecureNet-HeSA Gatekeeper Health PKI – Health Organisation Certification Authority Certificate Practice Statement version 3); then
- d) the RCA-issued CP (PO 01 SecureNet Gatekeeper Root Certification Authority issued Certificate Policy version 1).

1.1.2.4 Glossary

- 1. Key policy Documents should be read in conjunction with the *Health PKI Glossary version 3* (the Glossary) which contains definitions (either words or terms). Definitions used throughout this CP commence with capital letters. The Glossary is located at the RA's Website.

1.1.3 Certificates issued under this Document

1.1.3.1 Certificate types

- 1. This CP applies to Healthcare Individual Keys and Certificates (Individual Keys and Certificates). Refer to clauses 1.3.3 and 2 of this CP for further information.

1.1.3.2 Policy Qualifier

- 1. The text of the Policy Qualifier in all Individual Certificates is:
Certificates issued under a Health PKI Individual Certificate Policy (CP) must only be relied on by Individual and/or Location Subscribers for secure online Health-related messages and not for purposes other than those permitted by that CP.

1.2 Identification

1.2.1 X.500 Object Identifier hierarchy

- 1. Specified elements under Health PKI have been assigned an X.500 Object Identifier (OID). The authority for issuing OIDs is the SecureNet Policy Management Authority (SecureNet PMA).
- 2. The relevant OID for this Individual CP is:

SecureNet-HeSA Gatekeeper Health PKI Healthcare Individual CP	1.2.36.73665175.1.0.101.2
---	---------------------------

1.2.2 Standards

- 1. This Document is based on RFC 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, IETF PKIX RFC2527, by S. Chokhani and W. Ford, March 1999.
- 2. However, in some instances, that guideline does not provide adequate definition. In such cases, this Document will differ from the guideline insofar as is necessary for clarity only.

1.3 Community and Applicability

1.3.1 Certification Authorities

1.3.1.1 RCA

1. Cybertrust Australia Pty Ltd operates the RCA in Health PKI.
2. The RCA issues the Certificates that bind itself and the OCA to its Public Keys and is the highest point of trust in Health PKI. See the RCA-Issued CP and the RCA Certificate Practice Statement on the RCA's Website at www.certificates-australia.com.au for contact details and further information about functions.

1.3.1.2 OCA

1. Cybertrust Australia Pty Ltd operates the OCA in Health PKI.
2. The OCA generates, signs and issues the Certificates that bind the Registration Authority to its Public Keys, and do the same for Subscribers in response to Certificate requests that come from the RA. See the OCA Website at www.cybertrust.com for contact details.

1.3.2 Registration Authority

1. Medicare Australia is the RA that provides Registration services to the OCA in Health PKI. The RA is a Gatekeeper Extended Services RA, and as such conducts Evidence of Identity (EOI) checks, requests the OCA to generate Certificates and undertakes a range of other functions associated with the management of Keys and Certificates for Health PKI. For further details on the role and obligations of the RA, refer to clauses 2, 3 and 4 of this CP.

1.3.3 End Entities

1. For the purposes of this CP, an End Entity is:
 - a) a Subscriber; or
 - b) a Relying Party.
2. To be eligible for Individual Keys and Certificates, the Subscriber must be an individual person, of at least 18 years of age, and an active participant in the healthcare community.

1.3.4 Applicability

1. Individual Keys and Certificates should only be used for secure online Health-related messages:
 - a) in any transactions with Medicare Australia; or
 - b) any non-financial transactions between Subscribers within the Health Sector; or
 - c) in financial transactions between Subscribers within the Health Sector where the transaction value is up to \$10,000 in value.
2. Individual Keys and Certificates should not be used:

- a) for any illegal purpose; or
 - b) in a way which infringes any third person's rights (including Intellectual Property Rights).
3. Individual Keys and Certificates should not be used to send information which has a security classification greater than Highly Protected.
 4. Each Certificate has a life of two years, assuming no Certificate Revocation is necessary during this time. The Expiry date will be calculated as the second anniversary of the date on which the Certificates were generated, signed and issued by the OCA.

1.3.5 Policy authorities

1. Three policy approval authorities are relevant to this CP and related CPS Documents:
 - a) the Competent Authority;
 - b) the SecureNet Policy Management Authority (SecureNet PMA); and
 - c) the Medicare Australia Policy Management Authority (Medicare Australia PMA).
2. For further information refer to clause 8 of this Document.

1.4 Contact Details

1.4.1 Specification administration organisation

1. This CP is administered by the Medicare Australia PMA and approved by the SecureNet PMA and the Competent Authority. For further information refer to clause 8 of this CP.

1.4.2 Contact person

1. Enquiries or other communications about this Document should be addressed to the following address:

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

1.4.3 Person determining CPS suitability for the policy

1. Three entities are involved in determining the suitability of the OCA CPS for this CP:
 - a) the Health PMA;
 - b) the SecureNet PMA; and
 - c) the Competent Authority.
2. For further information refer to clause 8 of this CP.

2 General Provisions

2.1 Obligations

2.1.1 CA obligations

2.1.1.1 RCA obligations

1. The RCA must:
 - a) comply with all Gatekeeper Approved Documents, policies, criteria and procedures;
 - b) comply with applicable law;
 - c) maintain the Health PKI CPS, the OCA CPS and the RCA-Issued CP;
 - d) comply with, and ensure that its employees and contractors comply with, the conditions and obligations set out in the relevant CPs and the practices set out in the Health PKI CPS;
 - e) advise the OCA of its obligations under the RCA-Issued CP, the Health PKI CPS and the OCA CPS and make accessible a copy of these Documents to the OCA;
 - f) generate and issue Certificates to the OCA only on receipt of properly formatted and verified Certificate requests;
 - g) ensure, at the time the OCA Certificate is issued to the OCA, that:
 - i) the Certificate Information in the OCA Certificates accurately reflects information provided to it by or on behalf of the OCA;
 - ii) the OCA Certificate contains all the elements required by the relevant Certificate Profile; and
 - iii) the OCA is in possession or control of the Private Key corresponding to the Public Key included in the OCA Certificate;
 - h) issue Certificates that are factually accurate, as far as the RCA is reasonably aware from information known to it at the time of issue, and are free from data entry errors;
 - i) establish the SecureNet X.500 Directory to hold information pertaining to all Certificates issued under the RCA-Issued CP;
 - j) receive Suspension and Revocation requests in respect of the OCA Certificates and take appropriate action;
 - k) make reasonable enquiries in accordance with the arrangements agreed with the OCA to determine the validity of Compromises and suspected Compromises of Private Keys at any subordinate level the RCA deems warranted in its chain of trust;
 - l) promptly notify the OCA in the event that the RCA initiates Revocation of the OCA Certificate(s);

- m) if appropriate, issue a new OCA Certificate to the OCA if its Keys have been Compromised, or are suspected to have been Compromised, after receiving a properly formatted and verified request from the OCA for a new OCA Certificate;
- n) conduct compliance audits of the OCA;
- o) facilitate the conduct of regular audits by Finance-authorized external auditors to maintain Gatekeeper Accreditation status;
- p) when the RCA generates Key Pairs, ensure that each Key Pair can work as an operable pair of Cryptographic Keys;
- q) Revoke the OCA Certificate(s) as required by, and in accordance with, the RCA-Issued CP; and
- r) register the Revocation of the OCA Certificate(s) so that this information is readily available to a Relying Party.

2.1.1.2 OCA obligations

1. The OCA must:

- a) comply with all Gatekeeper Approved Documents, policies, criteria and procedures;
- b) comply with applicable law;
- c) comply with, and ensure that its employees and contractors comply with, the conditions and obligations set out in this CP and the practices set out in the OCA CPS;
- d) generate, sign and issue Individual Certificates in accordance with this CP on receipt of a digitally signed Individual Certificate request from the RA;
- e) ensure that, at the time Certificates are signed and returned to the RA:
 - i) the Certificates accurately reflect the information provided to the OCA by the RA; and
 - ii) the Certificates contain all of the elements required by the Certificate Profile;
- f) do all that is required to create and accurately maintain the Healthcare Public Directory (including by Registering Suspensions and Revocations);
- g) ensure that the Healthcare Public Directory is capable of being publicly searched at least by reference to the Distinguished Name, organisation or email address of a Subscriber with a sub-search possible on State or Territory;
- h) Suspend, Reinstate or Revoke Individual Certificates on receipt of a request to do so from the RA and post details of the Suspension, Reinstatement or Revocation of the Individual Certificate on the Healthcare Public Directory;
- i) if it suspects that Individual Certificates have been Compromised, inform the RA immediately of the suspected

- Compromise so that the RA can initiate a formal Suspension or Revocation request;
- j) publish and make accessible to the public Documents issued by OCA; and
- k) conduct and participate in regular audits.

2.1.2 RA obligations

1. The RA must:
 - a) comply with all Gatekeeper Approved Documents, policies, criteria and procedures;
 - b) comply with applicable law;
 - c) comply with, and ensure that its employees and contractors comply with, the conditions and obligations set out in this CP and the practices set out in the OCA CPS;
 - d) generate Individual Keys and Individual Certificate requests in accordance with this CP and the OCA CPS;
 - e) ensure all Key Pairs it generates are capable of working as an operable pair of Cryptographic Keys;
 - f) ensure the Certificate Information in all Individual Certificate Requests accurately reflects that provided to it by or on behalf of Applicants;
 - g) ensure copies of all Documents are accessible as provided for in this CP;
 - h) Register Applicants by:
 - i) ensuring that the Applicant completes and signs the relevant Subscriber Agreement;
 - ii) ensuring that the Evidence of Identity (EOI) processes for the Individual Keys and Certificates requested are complied with; and
 - iii) proposing and approving Distinguished Names for Subscribers;
 - i) distribute Individual Keys and Certificates to the Subscriber, ensuring that:
 - i) the Subscriber is provided with the Private Key corresponding to the Public Authentication Key given or identified in the Individual Certificates;
 - ii) the Subscriber's Private Authentication Key and the associated Personal Identification Code (PIC) are, to the maximum extent possible, protected from interception by third parties prior to the date of deemed possession of the Private Key by the Subscriber (refer to clause 3.1.8 of this CP); and
 - iii) the Subscriber's Private Authentication Key is not Compromised while under the RA's control;

- j) arrange for the Suspension, Reinstatement, Replacement or Revocation of the Individual Certificates, acting on advice from appropriate Parties, in accordance with this CP;
- k) implement this CP to promote the integrity of Health PKI as set out in this CP;
- l) conduct regular internal security audits of the RA; and
- m) assist an Authorised Auditor to conduct audits required by Gatekeeper.

2.1.3 Subscriber obligations

2.1.3.1 Accuracy of information

1. The Subscriber must ensure that all information he/she provides to the RA in connection with this Individual CP is true, accurate and complete at all times.
2. The Subscriber must promptly notify the RA if any information provided by him/her under the Individual CP is inaccurate or changes.
3. When the Subscriber receives the Individual Certificates, he/she must promptly check the accuracy of the information set out in them.

2.1.3.2 Purposes for which Individual Keys and Certificates may be used

1. Refer to clause 1.3.4 of this CP.

2.1.3.3 Effect of digital signatures with Individual Keys and Certificates

1. Use of Individual Keys and Certificates to digitally sign a message is intended to have the same legal effect as signing the same message on paper.
2. The Subscriber acknowledges that he/she may be bound to the legal effect of any transaction through the use of his/her Individual Keys and Certificates.

2.1.3.4 Protection of Individual Keys and Certificates

1. The Subscriber will be deemed to be in possession of the Individual Private Keys when:
 - a) the RA has mailed the Individual Keys and Certificates to the Subscriber;
 - b) the Subscriber has confirmed receipt of the Individual Keys and Certificates by return fax to the RA; and
 - c) the Subscriber has retrieved the related PIC (for activating the Individual Keys and Certificates) from the RA.
2. The Subscriber must take all reasonable steps to protect the safety and integrity of his/her Individual Keys and Certificates from the date of deemed possession.

3. The Subscriber must not disclose to any other person, write down or keep near the Token containing the Individual Keys and Certificates, the PIC, Passphrase or the Secret Identifier that he/she provided to the RA during the Application process.
4. If the Subscriber suspects or becomes aware that his/her Individual Private Authentication Key has been Compromised, he/she must:
 - a) immediately stop using the Individual Keys and Certificates; and;
 - b) immediately notify the RA; and
 - c) make reasonable attempts to notify any Relying Parties.

2.1.3.5 Other Subscriber obligations

1. The Subscriber is responsible for ensuring that messages sent using the Individual Private Key are sent to a currently listed Relying Party (for example by checking the Healthcare Public Directory);
2. The Subscriber is responsible for ensuring that, except for the purposes of Decryption, the Individual Keys and Certificates are not used if they are listed on the Healthcare Public Directory as being Suspended, Revoked or Expired.
3. If Certificate issuance or Re-key fees are payable by a Subscriber, he/she must pay those fees according to any fee schedule provided by the RA.
4. The Subscriber must only use the Healthcare Public Directory in accordance with this CP.
5. The Subscriber is responsible for keeping himself/herself informed of any Notices issued by the RA and OCA by reading any Notices distributed as outlined in this CP.

2.1.4 Relying Party obligations

1. Before relying on an Individual Certificate, the Relying Party is responsible for ensuring that the Certificate in question is valid and has not expired, or been Suspended or Revoked.
2. If an Individual Certificate has been used for a transaction that is outside the purpose specified in the Individual CP, the Relying Party relies on that Certificate entirely at his/her own Risk.

2.1.5 Repository obligations

1. The Repository obligations are performed by the OCA maintaining the Healthcare Public Directory.

2.2 Liability

The liability regime that applies to the activities conducted under this CP, or any other Approved Documents, is not subject to evaluation by the Authorised Legal Evaluator from the Gatekeeper Legal Panel or approval by the Competent Authority.

2.2.1 CA liability

2.2.1.1 RCA liability

1. The RCA is only liable under the CP for the Loss an entity or legal or natural person suffers if:
 - a) the RCA issued a Certificate under the RCA-issued CP;
 - b) the RCA breached clauses 2.1.1.1 (g), (p), (q) or (r) of this CP in respect of that Certificate; and
 - c) the entity or person reasonably relied on that Certificate and as a result, suffered the Loss.
2. If the RCA acted negligently when it breached the relevant clause or clauses.
3. Except as otherwise required by law, the total liability of the RCA to a person or entity in respect of any claim by that person or entity which arises under or in connection with this CP or the transactions contemplated by this CP will not exceed AUD\$1,000 in relation to any one claim.
4. The RCA is not liable under or in connection with this CP for Loss suffered by an entity or person which arises from reliance on a Certificate in circumstances that are outside the limitations placed on the Certificate in this CP, the RCA-issued CP, or any applicable Subscriber or Relying Party Agreement.
5. In no event shall the RCA be liable under or in connection with this CP for any loss of profit, loss of data or indirect or consequential loss incurred or suffered by any person or entity, whether or not the RCA was or should have been aware of the possibility of such loss.

2.2.1.2 OCA liability

1. The OCA is only liable under the CP for the Loss where an entity or legal or natural person suffers if:
 - a) the OCA issued a Certificate under this CP;
 - b) the OCA breached its obligations under this CP in respect of that Certificate; and
 - c) the entity or person reasonably relied on that Certificate and as a result, suffered the Loss,
2. if the OCA acted negligently when it breached the relevant clause or clauses.
3. The OCA is not liable for any failure by the RA to perform its obligations under the Individual CP.

2.2.2 RA liability

1. The RA (including its officers, employees and contractors) is not liable under the CP in any way whatsoever, for any Loss whether or not reasonably foreseeable, arising in connection with the Individual CP other than Loss directly arising from its failure to properly perform its obligations under the Individual CP.

2. The RA is not liable for any failure by the RCA / OCA to perform its obligations under the Individual CP.

2.2.3 Subscriber liability

1. The Subscriber agrees to be fully responsible for the use, security and integrity of his/her Individual Keys and Certificates, from the time he/she is deemed to be in possession of them.
2. The Subscriber may be liable for any Loss that he/she or any other person may suffer arising from his/her use of Individual Keys and Certificates, or any act or omission that he/she commits in breach of the Individual CP and Subscriber Agreement.

2.2.4 Relying Party liability

1. The Relying Party may be liable for any Loss that he/she or any other person suffers arising from his/her use of Individual Keys and Certificates, or any act or omission that he/she commits in breach of the Individual CP and Subscriber Agreement.

2.2.5 Commonwealth liability

1. Notwithstanding any other provision of this CP and whether Keys or Certificates are used in a transaction with an Agency or not:
 - a) the Commonwealth makes no representations or warranties in relation to:
 - i) the activities or performance of any of the PKI Entities which are carried out under, or in relation to Health PKI; or
 - ii) the services or products of the RCA / OCA or the RA; and
 - b) the Commonwealth is not liable in any way whatsoever, for any Loss whether or not reasonably foreseeable, arising in connection with:
 - i) an entity described in the Individual CP or the Location CP carrying out, or omitting to carry out, any activity described in, or contemplated by, the Approved Documents;
 - ii) the Commonwealth carrying out, or omitting to carry out, any activity related to the Gatekeeper Accreditation process; or
 - iii) a negligent act or omission of the RCA / OCA or the RA.

2.2.6 Limited Warranties

1. The RCA / OCA and the RA disclaim all warranties, express or implied. If any warranties or conditions are implied by legislation, then the liability of each of the RCA / OCA and the RA (and of any of their officers, employees and contractors), for any breach of the condition or warranty is limited to:
 - a) re-performing the services to which the warranty applied; or

- b) paying the cost of re-performing those services.

2.2.7 Contribution

- 1. The liability of a Party (the Party at fault) for Loss sustained by any other Party will be reduced proportionately to the extent that such Loss has been caused or contributed to by another Party's negligence or failure to comply with its obligations and responsibilities under the Individual CP.

2.2.8 Duty to Mitigate

- 1. For the reader's information only, each Party is under a duty to mitigate any damages or Loss that he/she may suffer or incur as a result of any breach of the Individual CP by another Party.

2.2.9 Indemnity from Subscriber

- 1. The Subscriber indemnifies each of the RCA / OCA and the RA (and their respective officers, employees and contractors), for any Loss suffered by any of these organisations or persons arising from:
 - a) any negligence or breach of the Subscriber Agreement by him/her; or
 - b) his/her reliance on an Individual Certificate or Location Certificate in a transaction that is outside the purpose specified in the Individual or Location CP (respectively).

2.2.10 Indemnity from Relying Party

- 1. The Relying Party indemnifies each of the RCA / OCA and the RA (and their respective officers, employees and contractors), for any Loss suffered by any of these organisations or persons arising from:
 - a) any negligence or breach of the Subscriber Agreement by him/her; or
 - b) his/her reliance on an Individual Certificate or Location Certificate in a transaction that is outside the purpose specified in the Individual or Location CP (respectively).

2.3 Financial responsibility

2.3.1 Indemnification by Relying Parties

- 1. Refer to clause 2.2.10 of this CP.

2.3.2 Fiduciary relationships

- 1. Nothing in this CP, or the issuing of Key Pairs and Certificates under it, establishes a fiduciary relationship between a PKI Service Provider and an End Entity.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

2.4.1.1 The Individual CP and Subscriber Agreement

1. The Individual CP and Subscriber Agreement are governed by, and are to be construed in accordance with, the laws from time to time in force in the Australian Capital Territory. The Parties agree to submit to the courts having jurisdiction in the Australian Capital Territory.
2. In conducting the activities under the Individual CP, all Parties agree to abide by the provisions of any relevant legislation, and the requirements of any Commonwealth, State, Territory or local body.
3. Clauses that relate to Intellectual Property Rights, safety, integrity, accuracy of information, Confidentiality, privacy, liability and indemnity will survive the Expiration or termination (for whatever reason) of the Individual CP and Subscriber Agreement.

2.4.1.2 Applicable contract structure

1. For the reader's information only, additional contracts and agreements relevant to this CP include:
 - a) the Gatekeeper Head Agreement (Certification Authority) which establishes a contractual relationship between the Commonwealth of Australia, represented by Finance, and the OCA for the provision of CA services to, and for the purposes of, Commonwealth Agencies;
 - b) the Gatekeeper MOA (Registration Authority) which establishes the relationship between the Commonwealth of Australia, represented by Finance, and the RA for the provision of RA services to, and for the purposes of, Commonwealth Agencies;
 - c) the Healthcare Individual Agreement which establishes a contractual relationship between the RCA / OCA, the RA and a Subscriber and/or Relying Party; and
 - d) the contractual arrangements between the RCA / OCA and the RA.

2.4.2 Severability, survival, merger, Notice

2.4.2.1 Severability

1. Any reading down or severance of a particular provision in this CP or the Subscriber Agreement does not affect the other provisions of that Agreement.

2.4.2.2 Survival (Continuing obligations)

1. Clauses which relate to:
 - a) Intellectual Property Rights, safety, integrity, accuracy of information, Confidentiality, privacy, liability, indemnity, security and consequences of termination; and

b) any other clause that by its nature is of continuing operation, will survive the Expiration or termination (for whatever reason) of this CP.

2.4.2.3 Notice

1. For the purpose of this clause, a Notice includes a consent, information, Application, request or any other communication provided under or in connection with this CP.
2. A Notice to a Party under this CP is only given or made if it is in writing and distributed in one of the following ways:
 - a) delivered or posted to that Party at its postal address;
 - b) emailed to that Party at its email address;
 - c) faxed to that Party at its fax number; and/or
 - d) posted on the RA's or OCA's Websites in accordance with this clause.
3. A Notice can only be provided by email where:
 - a) the Sender and Recipient are holders of current Individual and/or Location Certificates which have not been Suspended or Revoked; and
 - b) the Sender digitally signs the message using his/her Private Authentication Key.
4. A Notice will be issued and posted to the respective Websites when any of the following events occurs:
 - a) a new CP is approved;
 - b) there is a change or alteration to an existing CP; and/or
 - c) any other event which the RA or the OCA deem appropriate.
5. The content of Notices issued under this clause will be approved through the governance arrangements described in clause 8 of this CP, prior to publication on relevant Websites.
6. If a Party gives the other Parties three Business Days Notice of a change of its postal address, fax number or email address a Notice is only given or made by that other Party if it is delivered, posted or faxed to the latest postal or email address or fax number.
7. A Notice is to be treated as given or made as follows:
 - a) if it is delivered, when it is left at the relevant address;
 - b) if it is sent by post, three Business Days after it is posted (seven days if posted to or from a place outside Australia);
 - c) if it is sent by fax, as soon as the sender receives from the sender's fax machine a report of an error free transmission to the correct fax number;
 - d) if it is sent by email, as soon as the Recipient's host machine receives the Notice and the Digital Signature has been verified and authenticated; and/or

- e) if it is posted on the OCA or RA Websites, five Business Days after it is posted.
8. If a Notice is delivered, or an error free transmission report in relation to it is received, on a day that is not a Business Day, or if on a Business Day, after 5pm on that day in the place of the Party to whom it is sent, it is to be treated as having been given or made at the beginning of the next Business Day.

2.4.2.4 Assignment and novation

1. The RCA / OCA may not assign its rights or novate its obligations under this CP, except to a Gatekeeper Accredited entity and with the prior written consent of the Gatekeeper Competent Authority and the RA. The Gatekeeper Competent Authority and the RA may withhold consent at their discretion, although consent will not be unreasonably withheld.
2. The RA may not assign its rights or novate its obligations under this CP except to a Gatekeeper Accredited entity and with the prior written consent of the Gatekeeper Competent Authority and the RCA / OCA. The Gatekeeper Competent Authority and the RCA / OCA may withhold consent at their discretion, although consent will not be unreasonably withheld.

2.4.3 Dispute resolution procedures

2.4.3.1 Disputes relating to Individual CPs

1. Disputes arising out of this CP shall be resolved using the following processes:
 - a) The Parties shall use their best endeavours to resolve any problem that arises by negotiating with each other.
 - b) No Party shall resort to court proceedings (except for proceedings necessary to seek an urgent interim relief) in respect of a dispute arising out of or in connection with this CP until the process outlined in this clause 2.4.3.1 has been exhausted.
 - c) If a problem arises (including a breach or an alleged breach) which is not resolved at the operational level, or is sufficiently serious that it cannot be resolved at the operational level, the Party with the problem shall notify the other Party, and the management representatives of each of the Parties shall endeavour to agree on a resolution.
 - d) Should the management representatives of each of the Parties fail to reach a solution to the dispute within 5 Business Days from the date Notice of the problem was first given, the Parties may seek to settle the matter by referring the issue for mediation administered by the Australian Commercial Disputes Centre (ACDC).
 - e) The mediation is to be conducted in accordance with the latest version of the ACDC Mediation Guidelines to the extent that such guidelines are not inconsistent with any other provisions of this CP unless the mediation is administered by

an organisation other than the ACDC, in which case the mediation is to be conducted in accordance with the current guidelines of that organisation, to the extent that such guidelines are not inconsistent with any other provision of this CP.

- f) In the event that the dispute has not been settled within twenty eight (28) Business Days or other such period as agreed to in writing between the Parties hereto after the appointment of the mediator the dispute may be submitted to arbitration administered by ACDC and in accordance with their current arbitration guidelines.
- g) The arbitrator shall not be the same person as the mediator.
- h) The Parties will promptly furnish to the arbitrator (imposing appropriate obligations of confidence) all information reasonably requested by the arbitrator relating to the dispute.
- i) If either Party breaches any provision of this clause 2.4.3.1 in relation to a dispute, the other Party need not comply with that provision in relation to that same dispute.
- j) Unless prevented by the nature of the dispute, the Parties shall continue to perform in accordance with this CP while attempts are made to resolve the dispute.
- k) The Parties will share equally the fees and expenses of the mediator or the arbitrator, as the case may be.

2.4.3.2 Disputes relating to other contractual relationships

- 1. Disputes relating to any contractual relationship referred to in or related to this CP, other than disputes relating to a CP, must be resolved in accordance with the contract governing that relationship.

2.5 Fees

2.5.1 Certificate issuance or Re-key fees

- 1. Fees may be payable by Subscribers for the issue or Re-key of Certificates. Where fees are payable, the RA must provide an up to date fee schedule to all Subscribers via its Website.

2.5.2 Certificate access fees

- 1. Fees may be payable for Certificate access. Where this applies, the RA will provide an up-to-date fee schedule via its Website.

2.5.3 Revocation or status information access fees

- 1. Fees may be payable by Subscribers for Revocation and/or Reinstatement of Certificates. Where fees are payable, the RA must provide an up to date fee schedule to all Subscribers via its Website.
- 2. No fee is levied for accessing status information via the Healthcare Public Directory.

2.5.4 Fees for other services such as policy information

1. No fee is levied for access to this CP or any relevant CPS via the Internet.

2.5.5 Refund policy

1. A refund policy may apply to nominated fees. Any RA refund policy will be published on the RA's Website.

2.6 Publication and Repository

2.6.1 Publication of information

1. This CP and the related CPS are published electronically in PDF format on the RA's Website.
2. Notices to Subscribers about RA services may also be published on the RA's Website. Refer to clause 2.4.2.3 of this CP for more detailed information about Notice types and publication channels.

2.6.2 Frequency of publication

1. Publication frequency is as follows:
 - a) newly Gatekeeper Approved versions of this CP are published promptly;
 - b) relevant Certificate Information is published on the Healthcare X.500 Directory (referred to from this point as the Healthcare Public Directory) promptly following generation, signing and issue; and
 - c) the CRL in the Healthcare Public Directory is updated each time Certificates issued under this CP are Revoked.

2.6.3 Access Controls

1. There are no Access Controls on reading this CP or the related CPS on the RA's Website.
2. Access to Certificate Information (including CRLs) can be obtained by searching on name, email and organisation, with a sub-search possible on State or Territory.
3. Access Controls are used to restrict the ability to write to, or modify, these items to Authorised Personnel.

2.6.4 Repositories

1. The repository for all Public Key Certificates issued under this CP is the Healthcare Public Directory.
2. The Healthcare Public Directory provides information about Active, Suspended, Revoked and Expired Individual and Location Certificates issued under the respective CPs.
3. The Healthcare Public Directory shall:
 - a) not publish reasons why a Certificate has been Suspended or Revoked; and

- b) only publish information already contained in the Certificate, unless the Subscriber agrees to publish such information, or the information is in the public domain.
- 4. The Healthcare Public Directory can be accessed from the OCA and RA Websites.
- 5. The Healthcare Public Directory will be available 7 days a week, 24 hours a day.
- 6. Changes in the status of Certificates issued under this CP, including Revocation, Suspension and Expiry of Certificates will be published in the Healthcare Public Directory by the OCA.

2.7 Compliance Audit

- 1. Clause 2.7 is designed to address issues associated with compliance audits, for example:
 - a) frequency of entity compliance audit;
 - b) identity/qualifications of auditor;
 - c) auditor's relationship to audited Party;
 - d) topics covered by audit;
 - e) actions taken as a result of deficiency; and
 - f) communication of results.
- 2. Refer to clause 2.7 of the OCA CPS for detail.

2.8 Confidentiality

2.8.1 Types of information to be kept Confidential

2.8.1.1 Information disclosed by Applicants

- 1. The RA requires that an Applicant disclose Registration Information.

2.8.1.2 Personal information

- 1. The RA and the OCA must comply with their obligations under the Privacy Act 1988 (Cth), including:
 - a) any approved privacy code which applies to them under that Act; or
 - b) if no code applies - the National Privacy Principles.
- 2. Paragraph 1 does not apply:
 - a) where:
 - i) the RA or OCA is providing PKI services to a Commonwealth Agency, or to a contracted service provider to a Commonwealth Agency; and
 - ii) the obligations of the RA or OCA in the contract under which those services are provided are inconsistent with the requirements of the approved privacy code or the National Privacy Principles (as applicable); or

- b) where the RA or OCA is providing PKI services to a State or Territory authority.
3. In relation to Personal Information collected in the course of providing PKI services to a Commonwealth Agency, or to a contracted service provider to a Commonwealth Agency:
- a) the RA and the OCA must comply with the Information Privacy Principles contained in the Privacy Act in relation to that information as if they were Agencies; and
 - b) any subcontract entered into for the purpose of performing those PKI services must ensure that the subcontractor has the same awareness and obligations as the RA or OCA have under this clause 2.8.1.1, including this requirement in relation to subcontracts.
4. In relation to Personal Information collected in the course of providing PKI services to a State or Territory authority, the RA and the OCA must comply with their privacy obligations under:
- a) any applicable State or Territory laws; and
 - b) the contract under which the PKI services are provided.
5. In this clause 2.8.1.2, the expressions:
- a) Agency;
 - b) contracted service provider;
 - c) State or Territory authority,
6. have the same meaning as in the Privacy Act.

2.8.1.3 Confidential Information

1. For the purpose of this CP and any related CPS, Confidential Information means information that is by its nature Confidential and which:
- a) is marked Confidential;
 - b) is known by a Party to be Confidential; or
 - c) a Party ought to know was Confidential;
- but does not include information that:
- d) is or becomes public knowledge other than by breach of this CP or by any unlawful means; or
 - e) is in the possession of the Party without restriction in relation to disclosure before the date of receipt from the other Party or parties as the case may be; or
 - f) is legally required to be disclosed; or
 - g) has been independently developed or acquired by the Party.
2. Each Party must protect Confidential Information it holds against unauthorised disclosure.
3. Examples of Confidential Information include:

- a) Registration Information other than Certificate Information (and not including Personal Information which is protected under clause 2.8.1.1 of this CP); and
- b) RA Gatekeeper Approved Documents which do not reside in the public domain.

2.8.1.4 Other Protected Information

1. Certain information provided to the RA and OCA will be protected under specific legislation, or guidelines applicable to the RA and OCA or their officers, employees and agents. In relation to such information, the RA and OCA will protect that information in accordance with that legislation or those guidelines.

2.8.2 Types of information not considered Confidential

2.8.2.1 Certificate Information

1. Certificate Information is not considered to be Confidential Information and is displayed against the relevant Certificate on the Healthcare Public Directory.

2.8.3 Disclosure of Certificate Revocation/Suspension information

1. The Healthcare Public Directory provides information indicating the fact of Revocation and Suspension but not the reason/s behind this.

2.8.4 Release to law enforcement officials

1. No Document or Record held by any entity in Health PKI will be released to law enforcement agencies or officials except where:
 - a) a properly constituted warrant is produced or the information is otherwise legally required to be disclosed; and
 - b) the law enforcement official is properly identified.
2. For further information refer to the RA's Privacy Policy on its Website.

2.8.5 Release as part of civil discovery

1. No Document or Record held by any entity in Health PKI will be released to any person except where:
 - a) a properly constituted instrument that has emanated from a court having jurisdiction or an authority having legal jurisdiction (e.g. the Australian Securities and Investment Commission) requiring production of the information is produced; and
 - b) the person requiring production is a person Authorised to do so.
2. For further information refer to the RA's Privacy Policy on its Website.

2.8.6 Disclosure upon owner's request

1. The subject (owner) of Registration Information may Authorise release of that information to any other person. A person will not have Access to any other person's Registration Information without formal Authorisation being given by the person to whom the Registration Information pertains.
2. Formal Authorisation may take two forms:
 - a) a properly constituted electronic request providing that the request is digitally signed by a Private Key associated with a valid Certificate issued under a SecureNet PMA-approved CP; or
 - b) by application in writing.
3. For further information refer to the RA's Privacy Policy on its Website.

2.8.7 Other information release circumstances

1. No other release of information is permitted unless required by law.
2. For further information refer to the RA's Privacy Policy on its Website.

2.9 Intellectual Property Rights

2.9.1 RCA / OCA Materials

1. The following are the SecureNet Materials:
 - a) RCA-issued CP; and
 - b) Health PKI CPS.
2. Intellectual Property Rights (IPR) in the SecureNet Materials and any modifications and enhancements made to RCA / OCA Materials remain the property of the RCA / OCA, operating in the name of SecureNet.
3. The RCA / OCA grant perpetual, non-exclusive, world-wide and royalty free licenses:
 - a) to the RA to use, reproduce and communicate to the public the RCA / OCA Materials; and
 - b) the RA, the further right to sublicense the use and reproduction of RCA / OCA Materials to relevant participants in Health PKI;
4. for the purpose of ensuring that the RA can perform its roles under Health PKI.

2.9.2 RA Materials

1. The following are the RA Materials:
 - a) this Individual CP;

- b) the Location CP;
 - c) the OCA CPS;
 - d) the Healthcare Public Directory;
 - e) any other data or database created by the RA or its subcontractors for the purposes of Health PKI;
 - f) Subscriber Agreements;
 - g) Subscriber Certificates;
 - h) Individual and Location Keys; and
 - i) other Documents owned by the Commonwealth and published on the RA's Website for the purposes of Health PKI (but not including RCA / OCA Materials),
2. IPR in the RA Materials and any modifications or enhancements made to RA Materials remain, or are from the date of creation, the property of the RA.
 3. The RCA / OCA, the RA, Subscribers and Relying Parties must ensure that RA Materials are, to the extent practicable, signified as the property of the RA and that RA Materials remain at all times free of any lien, charge or other encumbrance of a third party.
 4. The RA grants to the Individual Subscribers and Relying Parties a revocable, royalty-free, non-exclusive, non-transferable license for the currency of an Individual Subscribers Certificate, to view and use (including downloading and printing) RA Materials and RCA / OCA Materials for the sole purpose of:
 - a) participating in Health PKI; or
 - b) understanding their rights and obligations under Health PKI, including obtaining legal or other advice as necessary.

2.9.3 Healthcare Public Directory

1. The RCA / OCA (as creator and maintainer of the Healthcare Public Directory) assign, from the date of creation, all IPR in the Healthcare Public Directory and all modifications to the Healthcare Public Directory to the RA.
2. The RA grants to the RCA / OCA a revocable, royalty-free, non-exclusive, non-transferable licence to use and modify the Healthcare Public Directory for the sole purpose of allowing the RCA / OCA to perform their obligations under Health PKI.

2.9.4 Subscriber's IPR

1. Each Subscriber grants to the RCA / OCA, the RA and the other Subscribers and Relying Parties a non-exclusive and royalty free license to use any IPR that a Subscriber may own in a Distinguished Name for the sole purpose of allowing those entities to participate in the PKI and discharge their obligations under this CP.

3 Identification and Authentication

3.1 Initial Registration

3.1.1 The process

1. The Registration process to obtain Individual Keys and Certificates requires the Applicant to complete the following steps:
 - a) The Applicant must complete and submit an Application online¹;
 - b) The Applicant must provide information and evidence to confirm his/her personal identity that will accrue a total value of at least 100 points as shown in the Table 1 below². All Documents provided to the RA to confirm personal identity must be copies of originals and certified as true copies by one of the Acceptable Referees listed on the Acceptable Referee Identification Form (ARIF). For more information refer to clause 3.1.9 of this CP.

Medicare Australia-known Applicants		
Document category	Document type	Point value
One Primary Identification Document (mandatory)	▪ Birth Certificate	70
	▪ citizenship certificate	70
	▪ current passport	70
	▪ expired passport (not cancelled and not expired for longer than two years from date of Application)	70
	▪ other documentation having same characteristics as a passport	70
Medicare Australia-known information	▪ Provider number; and ▪ Full name; and ▪ Business address as known by Medicare Australia.	40
All other Applicants		
One Primary Identification Document (mandatory)	▪ As for Medicare Australia-known Applicants	70

¹ In exceptional circumstances, Individual Applicants may be permitted to submit a paper-based Application using the Identification Reference Form (IRF). Advice should be sought from the RA.

² The Gatekeeper policy requirement for at least 100 points is derived from the identification requirements for a signatory to an account under the Financial Transactions Report Act 1988 (Cth). To ensure consistency with Gatekeeper policy, the RA will in time require photographic evidence in order to provide stronger applicant verification.

Medicare Australia-known Applicants		
Document category	Document type	Point value
One or more Secondary Identification Documents	▪ Current Australian drivers licence	40
	▪ Identification Card issued to a Commonwealth or State / Territory government employee, contractor or other Personnel	40
	▪ Document provided by current employer on employer letterhead and dated within the last three months	35
	▪ If self-employed, relevant documentation from their Registered Tax Agent / Accountant	35
	▪ Land Titles Office records	35
	▪ Rating authority	25
	▪ Reference to the latest Telstra telephone directory, and telephone contact with the signatory on this number	25
	▪ Credit card tax invoice	25
	▪ Council rates notice	25
	▪ Records of public utility	25
	▪ Record held under law	25

Table 1: EOI Documentation for individuals

- c) The Applicant must provide information and evidence to Medicare Australia to confirm his/her identity, the nature of which will vary depending on whether the Applicant has Medicare Australia-known status or not, as shown in the Table 2.

Medicare Australia-known Applicants
Telephone and fax numbers; and Email; and Secret Identifier.
All other Applicants
Full name; Business address; Telephone and fax numbers; Email; and Secret Identifier.

- d) The Applicant must complete and submit a signed Individual Agreement.

3.1.2 Types of names

1. A Distinguished Name is generated for each Subscriber.
2. Information that forms part of an Individual Subscriber's Distinguished Name is:

- a) Country;
- b) Organisation;
- c) State; and
- d) Common name.

3.1.3 Need for names to be meaningful

1. Distinguished Names generated in accordance with clause 3.1.2 of this CP are assumed to be meaningful.

3.1.4 Rules for interpreting various name forms

1. Distinguished Names shall include each of the elements specified in X.509.

3.1.5 Uniqueness of names

1. Each Distinguished Name assigned to a Subscriber under this CP shall be unique.

3.1.6 Name claim dispute resolution procedure

1. The RA shall resolve any name claim disputes brought to its attention, in consultation with the OCA.

3.1.7 Recognition, authentication and role of trademarks

1. Refer to clause 2 of this CP.

3.1.8 Method to prove possession of Private Key

1. A Subscriber will be deemed to be in possession of the Individual Private Keys when:
 - a) the RA has mailed the Individual Keys and Certificates to the address nominated during the application process;
 - b) the Subscriber has confirmed receipt of the Individual Keys and Certificates by fax to the RA; and
 - c) the Subscriber has retrieved the related Personal Identification Code (PIC) (for activating the Individual Keys and Certificates) from the RA.
2. The signature on the fax that confirms receipt of the Token must be that of the Subscriber and will be verified against the signature on the Subscriber Agreement. Additional procedures may be used to confirm Token receipt, for example telephone calls.
3. Should the RA be aware of any doubt that exists about the right to possession of the Keys, the RA will take action to prevent the Keys or PIC being delivered, or arrange Suspension or Revocation of the Certificates.

3.1.9 Authentication of organisation identity

1. Not applicable to Individual Keys and Certificates.

3.1.10 Authentication of individual identity

1. The RA will verify Evidence of Identity (EOI) for all Individual Applicants in accordance with the 100-point check recommended by the Financial Transactions Reports Act 1988 (Cth).
2. Individual Applicants are required to provide appropriate information and documentation to meet the requirements of the 100-point check (refer to clause 3.1 of this CP). All Documents submitted must be certified copies of originals, with certification provided by Acceptable Referees using the ARIF.
3. One Primary Identification Document must be provided as a mandatory part of the EOI process, which will give them 70 of the 100 points required.
4. Individuals who have an established a current claims/payments history with Medicare Australia³, and are able to correctly answer questions relating to their Provider file record, will be considered 'Medicare Australia-known'. Medicare Australia-known Applicants will be eligible for a further 40 points based on this relationship.
5. All other individuals will need to provide one or more Secondary Identification Documents to accrue the full 100 points required.
6. The RA may at its discretion require an Applicant to attend a personal interview for the purposes of identity verification.

3.2 Routine Re-key

3.2.1 Defining Re-key

1. Re-keying is the process that Subscribers must undertake to replace a Certificate that is due to Expire. The Re-keying process arranges for the generation, signing, issuance and distribution of replacement Certificates before the Expiry of the current Certificates.

3.2.2 Subscriber initiation of Re-key

1. Re-keying is the process that Subscribers must undertake to replace a Certificate that is due to Expire. The Re-keying process arranges for the generation, signing, issue and distribution of replacement Certificates before the Expiry of the current Certificates.
2. Responsibility for the Re-key lies with the Subscriber. Accordingly, a Subscriber may request Certificate Re-key using the Revocation / Suspension / Reinstatement / Re-key Request form, available from the RA's Website, provided that:
 - a) the request is made prior to the Expiry of the current Certificates;
 - b) there is no change in Certificate Information as contained in the Registration Records;

³ Registered at least 12 months and claims activity in the last quarter required.

- c) the current Certificates have not been Revoked or Suspended; and
- d) the Subscriber is not listed as a Compromised User by the RA.

3.2.3 RA initiated Re-key

1. The RA may also commence an automated Re-key reminder process by secure email before the Certificate Expiry date.
2. In this scenario, the RA will automatically generate a Re-key Reference Number for each Certificate that is due for Expiry and for which a Re-key Notice is being generated.

3.2.4 Information changes during the Re-key process

1. If during the Re-keying process the Subscriber wishes to change information recorded by the RA against their Certificates, the Subscriber will generally be required to complete components of the Registration process again. Subscribers should seek advice from the RA on which components of the Registration process will need to be completed.

3.2.5 Token and PIC distribution during the Re-key process

1. If the Subscriber advises the RA that Re-keying is required, and the Re-key advice does not constitute a new Registration, the RA will wait until approximately two weeks prior to the Certificate Expiry date, then commence the Token and PIC generation and distribution process.
2. Subscribers choosing to Re-key will have their new Token delivered to them by standard mail.
3. These Subscribers will be given a choice of PIC delivery mechanisms: secure email or telephone.
4. PICs to be retrieved by secure email will be Encrypted and distributed to the Subscriber via their current Certificates. Subscribers will use their current Certificates to Decrypt and Access the PIC.
5. PICs to be retrieved by telephone will be Encrypted and distributed to the RA's eBusiness Service Centre to await telephone retrieval by the Subscriber. Subscribers will be required to accurately quote their Secret Identifier and RA-generated Re-key Reference Number. With accurate quoting, Subscribers will be in order to receive their PIC by telephone, provided with instructions on loading the new Certificates into software applications and advised to change the PIC to a new Passphrase immediately. Subscribers who do not accurately quote their Secret Identifier and RA-generated Re-key Reference Number will have the PIC sent to them by standard post.

3.3 Re-key after Revocation

1. Re-key after Revocation of an Individual Certificate has occurred will be permitted in situations where identity is not put into

question. Subscribers should seek advice from the RA on which components of the Registration process will need to be completed.

3.4 Revocation request

1. The RA will validate the Revocation request and will process it according to the Revocation request procedure as outlined in clause 4.4.3 of this CP.
2. A request to Revoke Individual Certificates may be made electronically and signed with the Subscriber's Private Authentication Key issued under this CP. Alternatively, the request can be submitted using the Revocation / Suspension / Reinstatement / Re-key request form, available from the RA's Website.

4 Operational Requirements

4.1 Certificate Application

1. An Applicant must successfully complete the initial Registration process (refer to clause 3.1 of this CP).
2. The RA will conduct the Registration process in accordance with this CP.
3. After successful completion of the Registration process, the RA will request the OCA to generate, sign and issue Individual Certificates.

4.2 Certificate Issuance

1. The OCA will generate, sign and issue Individual Certificates on receipt of an Authenticated request from the RA. The OCA will then forward the Individual Certificates to the RA for distribution to the Subscriber.
2. The RA will incorporate the Individual Keys and Certificates into a Secure Token and then distribute to the Subscriber. The Token containing the Individual Keys and Certificates is not usable until activated with a Personal Identification Code (PIC).
3. The Secure Token will be distributed to the Subscriber by standard post, to the address recorded for the Subscriber during the Application process. A confirmation receipt will be included in the package sent to the Subscriber.
4. To confirm receipt of the Token package, the Subscriber will be required to sign the confirmation receipt and send by fax back to the RA. The RA will compare the signature on the confirmation receipt against that originally provided on the Subscriber Agreement. If the signatures are confirmed as being made by the same person, the RA will forward the associated PIC to the RA's eBusiness Service Centre, for telephone retrieval by the Subscriber. Normally this will be within two business hours of receipt of fax.

4.3 Certificate acceptance

1. In order to activate the Token containing the Individual Keys and Certificates, the Subscriber is required to telephone the RA's eBusiness Service Centre and successfully quote the RA-generated Application Reference Number and the Secret Identifier provided by them during the Application process.
2. Subscribers who are able to successfully quote their RA-generated Application Reference Number and Secret Identifier will receive their PIC by telephone, together with instructions on how to activate the Token containing their Individual Keys and Certificates.
3. Subscribers who are not able to successfully quote their RA-generated Application Reference Number and Secret Identifier will

have their PIC sent to them by standard post, to the address recorded for them during the Application process.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for Revocation

1. Prompt validation and actioning of an Individual Certificate Suspension or Revocation request is essential to maintain the integrity of Health PKI.
2. Individual Authentication Certificates and Individual Confidentiality Certificates will be Suspended or Revoked simultaneously.
3. Certificates will be Revoked where:
 - a) the Subscriber's Private Key is Compromised;
 - b) the media holding a Private Key is Compromised;
 - c) the Subscriber leaves the Health Sector;
 - d) the Subscriber's Keys or Certificates are no longer required by the Subscriber for secure online Health-related messages;
 - e) the Subscriber changes any information that necessitates a change in Distinguished Name;
 - f) the RA suspects the use of the Keys or Certificates has been Compromised; or
 - g) Certificate Information is inaccurate, for whatever reason.
4. Certificates will be Revoked if any of the circumstances for Revocation (above) are reported as suspected but unconfirmed, and the circumstances may be investigated during the grace period (refer to clause 4.4.4 of this CP).
5. Certificates may be Revoked if the RCA / OCA or the RA cease to operate.
6. The OCA may make reasonable enquiries in accordance with arrangements agreed with the RA and the Subscriber to determine the validity of Compromises and suspected Compromises of Individual Private Keys.
7. If a properly formatted request to Revoke Certificates is received by the RA and Authenticated, and has been made in accordance with the provisions of this CP, the RA will Revoke the Certificates immediately.
8. In situations where Revocation has been initiated for reasons relating to identity, a full Registration process will normally be required to re-confirm identity.
9. In situations where Revocation has been initiated for reasons that do not relate to identity, components of the Registration process will need to be repeated. Subscribers should seek advice from the RA on which components of the Registration process will need to be repeated.

4.4.2 Who can request Revocation

1. Certificate Revocation can be initiated by:
 - a) the OCA;
 - b) the RA;
 - c) the Subscriber; or
 - d) an Authorised Third Party.
2. The same Parties can request Certificate Reinstatement.

4.4.3 Procedure for Revocation requests

4.4.3.1 RA processing

1. Revocation requests by Subscribers and Authorised Third Parties are to be submitted to the RA using the relevant form, found on the RA's Website. The following procedure applies to Revocation requests.
2. When processing a request, the RA will:
 - a) Authenticate the request;
 - b) ensure the relevant Certificates and Public Keys are current;
 - c) prioritise the request according to the target processing times specified in clause 4.4.9 of this CP, including consideration of Suspension of the Certificate;
 - d) if applicable, add the Subscriber to its list of Compromised Users; and
 - e) send an Authenticated request to the OCA.

4.4.3.2 OCA processing

1. To process a request, the OCA will:
 - a) Authenticate the request from the RA;
 - b) add the Revoked Certificates to the CRL;
 - c) issue a Notice containing the Certificate details and the date and time of the Revocation to the RA and the Subscriber; and
 - d) list the Revoked Certificates in the Healthcare Public Directory.

4.4.3.3 Subscriber responsibilities

1. A Subscriber with Revoked Certificates is to continue to safeguard the Private Keys associated with the Revoked Certificates and take action as requested by the RA.

4.4.4 Revocation request grace period

1. Revocation requests will have a grace period – otherwise known as a Suspension - of two Business Days. Certificate Revocations will be able to be reversed within this period if it can be demonstrated that no Certificate Compromise has in fact occurred.

4.4.5 Circumstances for Suspension

1. Where any of the circumstances for Revocation (refer to clause 4.4 of this CP) are suspected but unconfirmed, Certificates may be Suspended while the circumstances are being investigated. Suspension during the grace period applies to all Certificate Revocations.

4.4.6 Who can request Suspension

1. As for Revocation (refer to clause 4.4.2 of this CP).

4.4.7 Procedure for Suspension requests

1. As for Revocation (refer to clause 4.4.3 of this CP), but with 'Suspension' substituted for 'Revocation'.

4.4.8 Limits on Suspension period

1. Refer to clause 4.4.4 of this CP.

4.4.9 CRL issuance frequency

1. The CRL in the Healthcare Public Directory is updated each hour. Certificates that are Suspended or Revoked prior to the issuance of the CRL will be reflected in the current CRL.

4.4.10 CRL checking requirements

1. Subscribers and Relying Parties should exercise reasonable care before undertaking transactions, for example by checking the validity and currency of a Certificate on the Healthcare Public Directory.

4.4.11 Online revocation/status checking availability

1. The OCA provides an online mechanism for downloading the CRL from the Healthcare Public Directory to verify the status of Certificates issued under this CP. The Healthcare Public Directory can be Accessed from the OCA and RA Websites.

4.4.12 Online Revocation checking requirements

1. Refer to Section 4.4.10 of this CP.

4.4.13 Other forms of Revocation advertisements available

1. Where RCA or OCA Keys and Certificates have been Compromised or Revoked, advertisements may be placed in the national press.

4.4.14 Checking requirements for other forms of revocation advertisements

1. Not applicable.

4.4.15 Special requirements regarding Key Compromise

1. Except for the purposes of Decryption, Keys and/or Certificates that are suspected of, or are known to be Compromised or Expired, should not be used.

4.5 Security Audit procedures

1. Clause 4.5 is designed to address issues associated with Records and Archives of information, for example:
 - a) types of event recorded;
 - b) frequency of processing log;
 - c) retention period for audit log;
 - d) protection of audit log;
 - e) audit log backup procedures;
 - f) audit collection system (internal versus external);
 - g) notification to event-causing subject; and
 - h) vulnerability assessments.
2. Refer to clause 4.5 of the OCA CPS for detail.

4.6 Records Archival

1. Clause 4.6 is designed to address issues associated with Archives of relevant Records, for example:
 - a) types of event recorded;
 - b) retention period for Archive;
 - c) protection of Archive;
 - d) Archive backup procedures;
 - e) requirements for time-stamping of Records;
 - f) Archive collection system (internal or external); and
 - g) procedures to obtain and verify Archive information.
2. Refer to clause 4.6 of the OCA CPS for detail.

4.7 Key changeover

1. The RCA / OCA and RA Key changeovers will be affected in such a manner as to cause minimal disruption to Subscribers.
2. Refer to clause 4.7 of the OCA CPS for detail.

4.8 Compromise and disaster recovery

1. Clause 4.8 is designed to address issues associated with compromise and disaster recovery, for example:
 - a) computing resources, software, and/or data are corrupted;
 - b) entity Public Key is Revoked;
 - c) entity Private Key is Compromised; and

- d) secure facility after a natural or other type of disaster.
- 2. Please refer to clause 4.8 of the OCA CPS for detail.

4.9 CA or RA termination

- 1. This clause 4.9 applies if the RCA / OCA or the RA become aware that they intend to (or are likely to) cease providing services which are necessary for the continuance of Health PKI.
- 2. Please refer to clause 4.9 of the OCA CPS for detail.

5 Physical, procedural, and Personnel security controls

1. This clause 5 is designed to address issues associated with the controls that the RA and OCA have in place to ensure physical, procedural and Personnel security, for example:
 - a) Physical controls:
 - i) site location and construction;
 - ii) physical Access;
 - iii) power and air conditioning;
 - iv) water exposures;
 - v) fire prevention and protection;
 - vi) media storage;
 - vii) waste disposal; and
 - viii) off-site back-up;
 - b) Procedural controls:
 - i) trusted roles;
 - ii) number of persons required per task; and
 - iii) identification and Authentication for each role;
 - c) Personnel controls:
 - i) background, qualifications, experience and clearance requirements;
 - ii) background check procedures;
 - iii) training requirements;
 - iv) retraining frequency and requirements;
 - v) job rotation frequency and sequence;
 - vi) sanctions for unauthorised actions;
 - vii) contracting Personnel requirements; and
 - viii) documentation supplied to Personnel.
2. For further information, refer to clause 5 of the OCA CPS.

6 Technical Security Controls

1. This clause 6 is designed to address issues associated with the controls that the RA and OCA have in place to ensure technical security, for example:
 - a) Key Pair generation and installation:
 - i) Key Pair generation;
 - ii) Private Key delivery to Entity;
 - iii) Public Key delivery to Certificate issuer;
 - iv) CA Public Key delivery to users;
 - v) Key sizes;
 - vi) Public parameters generation;
 - vii) Hardware / software Key generation; and
 - viii) Key usage purposes;
 - b) Private Key protection:
 - i) Standards for Cryptographic module;
 - ii) Private Key multi-person control;
 - iii) Private Key escrow;
 - iv) Private Key backup
 - v) Private Key Archival;
 - vi) Private Key entry into Cryptographic module;
 - vii) Method of activating Private Key;
 - viii) Method of deactivating Private Key; and
 - ix) Method of destroying Private Key;
 - c) Other aspects of Key Pair management:
 - i) Public Key Archival; and
 - ii) Usage periods for the Public Keys and Private Keys;
 - d) Activation data:
 - i) Activation data generation and installation;
 - ii) Activation data protection; and
 - iii) Other aspects of activation data;
 - e) Computer security controls:
 - i) Specific computer security technical requirements; and
 - ii) Computer security rating;
 - f) Life cycle technical controls:
 - i) System development controls;
 - ii) Security management controls; and
 - iii) Life cycle security ratings;

- g) Network security controls; and
 - h) Cryptographic module engineering controls.
2. For further information, refer to clause 6 of the OCA CPS.

7 Certificate and CRL Profiles

7.1 Certificate Profile

1. Clause 7.1 is designed to explain the technical make-up of Certificates, for example:
 - a) Certificate Profiles;
 - b) CRL Profiles:
 - i) Version numbers; and
 - ii) CRL and CRL entry extensions.
2. For this information, refer to clause 7 of the OCA CPS.

8 Specification Administration

8.1 Specification change procedures

1. The Competent Authority defines high level criteria against which CAs and RAs are evaluated. When successfully evaluated, CAs and RAs are Gatekeeper Accredited by the Competent Authority. Further information regarding Gatekeeper can be found at www.gatekeeper.gov.au
2. The RCA / OCA operates the SecureNet PMA which is responsible for setting Certificate policy for the overall SecureNet-HeSA Gatekeeper Health PKI Hierarchy. The SecureNet PMA also gives internal approval to CPs within Health PKI Hierarchy. The SecureNet PMA's e-mail address is info_APAC@cybertrust.com.
3. The Health PMA is responsible for setting Certificate Policy in the context of Health PKI. Its functions include:
 - a) providing internal approval to new policy and policy changes for Health PKI;
 - b) submitting new or changed policies to the SecureNet PMA for internal approval prior to submission to the Competent Authority; and
 - c) overseeing and managing compliance with Gatekeeper Accreditation.
4. The Health PMA comprises at least two members, one nominated by the RCA / OCA and one by the RA, as well as any other representatives agreed to between the RCA / OCA and the RA. The Health PMA is managed by the RA. The RA's e-mail address is registration@hesa.gov.au

8.2 Publication and notification policies

8.2.1 Initial publication

1. This CP and related CPS Documents have been subject to formal endorsement by the SecureNet PMA and approval by the Competent Authority.
2. This CP and its accompanying OID and related CPS Documents can be accessed via the RCA/ OCA and RA Websites.

8.2.2 Change

1. Changes to this CP and related CPS Documents must be approved by the Competent Authority.
2. Two forms of policy change are possible:
 - a) issue of a new CP or CPS; and
 - b) change or amendment of the existing CP or CPS.
3. Where a change to the CP is required, the OID of the policy will stay the same, however a new version number will be allocated by the SecureNet PMA on its endorsement of the amended CP.

4. Following approval by the Competent Authority, the Health PMA will facilitate publication of the new or amended CP or CPS.
5. Any changes to this CP or related CPS Documents must be made in accordance with Gatekeeper requirements.

8.2.3 Actual publication

1. The new or updated CP or related CPS Documents will be accessible via the RCA / OCA and RA Websites.
2. Subscribers will be advised of changes to the CP or related CPS via the OCA's and RA's Websites in accordance with clause 2.4.2.3 of this CP. Continued use of the amended CP or CPS beyond the specified date of effect will constitute acceptance of the amended CP or CPS.

8.3 Approved Document approval procedures

1. New or updated versions of this CP or the related CPS must be endorsed by the PMAs and approved by the Competent Authority to maintain Gatekeeper Accreditation status.