



CO 01

SecureNet-HeSA Gatekeeper Health PKI –  
Subscriber (Healthcare Location) Agreement

PURPOSE OF DOCUMENT

By making an application and submitting this completed Agreement, the Health Sector Entity (HSE) is asking Medicare Australia, a Gatekeeper Accredited Extended Services Registration Authority (RA), to issue SecureNet-HeSA Gatekeeper Health PKI (or Health PKI) Healthcare Location Keys and Certificates.

This Agreement establishes a contractual relationship between the HSE (whether the Location is acting as a Subscriber or Relying Party), the Commonwealth of Australia as represented by the CEO of Medicare Australia (the Registration Authority or RA) and Cybertrust Australia Pty Ltd (which operates the Health Organisation Certification Authority or OCA, issuing certificates in the name of SecureNet) in relation to the possession and use of the Location Keys and Certificates Medicare Australia (as the RA) delivers RA services.

All references to SecureNet throughout this document refer to the Cybertrust Australia Pty Ltd entity, issuing certificates in the name of SecureNet.

You may wish to seek independent professional advice regarding this Agreement.

PARTIES TO THIS AGREEMENT

This Agreement is between:

1. Registration Authority (RA)

The Commonwealth of Australia  
as represented by the CEO of Medicare  
Australia  
ABN 75 174 030 967  
Locked Bag 6666  
Tuggeranong DC ACT 2901

2. Organisation Certification Authority (OCA)

Cybertrust Australia Pty Ltd  
ABN 74 073 665 175  
Locked Bag 32  
Pymont NSW 2009

3. The Health Sector Entity (HSE)

HSE details: Details of the HSE undertaking healthcare activities and associated services from the specified Healthcare Location (Location).

HSE legal name: .....

ABN: .....ACN (if a company):.....

HSE Representative name and position:

Name: ..... Position: .....

Details of the Location for which Location Keys and Certificates are being applied:

Name of Location (practice/trading name of HSE): .....

Street address of Location (Notices will be sent to this address. Location Keys and Certificates will also be sent to this address unless another address is specified by the HSE for this purpose): Suite:.....

Floor: ..... Building: .....

Street: .....

City/suburb: ..... State: ..... Postcode: .....

## 1 Interpretation

- 1.1 In this Agreement, capitalised terms have the same meaning as in the *Health PKI Glossary version 3*, available from the RA's Website ([www.hesa.gov.au](http://www.hesa.gov.au)).

## 2 Privacy

- 2.1 The HSE and Duly Authorised Officer (DAO) acknowledge that Personal Information is collected in respect of the DAO (and the HSE if the HSE is an individual (i.e. sole trader)). This information is used by the RA and OCA for the purpose of issuing and managing the Location Keys and Certificates. The RA and OCA will ensure their policies and practices comply with the Information Privacy Principles under the *Privacy Act 1988* (Cth) in respect of that information. The RA's full Privacy Policy can be found on its Website.
- 2.2 By applying for Location Keys and Certificates, the DAO (and the HSE if applicable) consents to:
- (a) the RA collecting, using and disclosing any Personal Information for the purposes of the Health PKI; and
  - (b) the Location Certificate details being published in the Healthcare Public Directory.

## 3 Terms and Conditions set out in Location and Individual Certificate Policies

- 3.1 The provisions of the *PO 01 SecureNet-HeSA Gatekeeper Health PKI – Subscriber (Healthcare Location) Certificate Policy version 3* (Location CP) apply to the HSE as a Subscriber as if those provisions were set out in this Agreement.
- 3.2 Parties to this Agreement should read the Location CP and the *PO 01 SecureNet-HeSA Gatekeeper Health PKI – Subscriber (Healthcare Individual) Certificate Policy version 3* (Individual CP), which are available from the RA's Website.
- 3.3 If the HSE relies on another Subscriber's Location Certificate or Healthcare Individual Certificate, the provisions of the Location CP or the Individual CP respectively apply to the HSE as a Relying Party as if those provisions were set out in this Agreement.
- 3.4 If there is any inconsistency between the terms of this Agreement and the terms of the applicable CP, the CP will prevail.

## 4 Period of Agreement

- 4.1 This Agreement will come into effect when the OCA generates, signs and issues the Location Certificates.
- 4.2 This Agreement terminates when the Location Certificates Expire and are not Re-keyed, or are Revoked.

## 5 Subscriber obligations

### *Introductory statement*

- 5.1 The obligations of a Subscriber are shared between the HSE, the DAO and any Authorised Users who act on behalf of the HSE.
- 5.2 The Parties recognise that the obligations imposed on the HSE, in its capacity as a Location Applicant, Subscriber and/or Relying Party, will be performed by the DAO and/or the Authorised Users on behalf of the HSE.
- 5.3 The HSE, whether acting in its capacity as a Location Applicant or Subscriber, is fully responsible for the actions of its DAO and any Authorised Users.

### *Appointment of DAO and Authorised Users*

- 5.4 The HSE is responsible for identifying an appropriate individual to act in the role of DAO.
- 5.5 The HSE will ensure an appropriate and sufficient infrastructure (both physical and procedural) is provided to ensure that the DAO and any Authorised Users are capable of meeting their obligations.
- 5.6 The HSE must ensure an appropriate level of confidence in the Authentication of the DAO and any Authorised Users, whether at the original point of employment or specifically for the Location Keys and Certificates.
- 5.7 The HSE is required to ensure that the DAO and any Authorised Users are aware of, understand and comply with their obligations as detailed in the Location CP.

### **Accuracy of information**

- 5.8 The HSE must ensure that all information it provides to the RA, through the DAO or otherwise, in connection with the Location CP is true, accurate and complete at all times.
- 5.9 The DAO must promptly notify the RA if any information provided by it in relation to the HSE under the Location CP is inaccurate or changes.
- 5.10 When the DAO receives the Location Certificates, he/she must promptly check the accuracy of the information set out in them.

### **Purposes for which Location Keys and Certificates may be used**

- 5.11 Location 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.
- 5.12 Location Keys and Certificates should be used for:
  - (a) Health-related messages where an individual signature IS NOT required; and
  - (b) for secure internal Location use.
- 5.13 Location 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).
- 5.14 Location Keys and Certificates should not be used to send information which has a security classification greater than Highly Protected.

### **Protection of Location Keys and Certificates:**

- 5.15 The HSE will be deemed to be in possession of the Location Private Keys when:
  - (a) the RA has mailed the Location Keys and Certificates to the address nominated during the application process;
  - (b) the DAO has confirmed receipt of the Location Keys and Certificates by return fax to the RA; and
  - (c) the DAO has retrieved the related Personal Identification Code (PIC) (for activating the Location Keys and Certificates) from the RA.
- 5.16 The HSE, the DAO and any Authorised Users must take all reasonable steps to protect the safety and integrity of the Location Keys and Certificates from the date of deemed possession.
- 5.17 The DAO must not disclose to anyone other than the Authorised Users, write down or keep near the Token containing the Location Keys and Certificates, the PIC, Passphrase or the Secret Identifier provided by him/her to the RA during the Application process.
- 5.18 If an Authorised User suspects or becomes aware that the Location Private Authentication Key has been Compromised, he/she must:
  - (a) immediately stop using (and take all reasonable steps to arrange for Authorised Users to stop using) the Location Keys and Certificates;
  - (b) immediately notify the RA; and
  - (c) make reasonable attempts to notify any Relying Parties.

### **Other Subscriber obligations**

- 5.19 The DAO and any Authorised Users are responsible for ensuring that messages sent using the Location Private Key are sent to a currently listed Relying Party (for example by checking the Healthcare Public Directory).
- 5.20 The DAO and any Authorised Users are responsible for ensuring that, except for the purposes of Decryption, the Location Keys and Certificates are not used if they are listed on the Healthcare Public Directory as being Suspended, Revoked or Expired.
- 5.21 If Certificate issuance or Re-key fees are payable by a Subscriber, the DAO must ensure those fees are paid according to any fee schedule provided by the RA.

- 5.22 The DAO and any Authorised Users must take reasonable care to ensure the Healthcare Public Directory is used in accordance with the Location CP.
- 5.23 The DAO is responsible for keeping himself/herself informed of any Notices issued by the RA and OCA by reading any Notices distributed as outlined in the Location CP, and informs Authorised Users as appropriate.

## **6 Relying Party obligations**

- 6.1 Before relying on a Location Certificate or 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.
- 6.2 If a Location Certificate or Individual Certificate has been used for a transaction that is outside the purpose specified in the Location CP or the Individual CP (respectively), the Relying Party relies on that Certificate entirely at its own risk.

## **7 RA obligations**

- 7.1 The RA's obligations are set out in the Individual CP, the Location CP and the PO 02 SecureNet-HeSA Gatekeeper Health PKI - Health Organisation Certification Authority Certification Practice Statement version 3 (OCA CPS). These include:
- (a) conducting EOI checks and Registering Applicants;
  - (b) generating Location Keys;
  - (c) securely distributing Location Keys and Certificates;
  - (d) arranging Certificate Revocation, Suspension and Reinstatement when required; and
  - (e) maintaining the integrity of Health PKI.

## **8 OCA obligations**

- 8.1 The OCA's obligations are set out in the Individual CP, the Location CP and the OCA CPS. These include:
- (a) generating, signing and issuing Location Certificates;
  - (b) Suspending, Revoking and Reinstating Certificates when required; and
  - (c) maintaining the Healthcare Public Directory.

## **9 Changes to the Agreement**

- 9.1 The RA or OCA may make changes to the Location CP, the Location Agreement and the OCA CPS in the way indicated in each of those Documents. The HSE will be alerted to changes by a Notice posted on the RA's Website.
- 9.2 By continuing to use the Location Keys and Certificates beyond the specified date of effect of the change, the HSE accepts the change.
- 9.3 If the HSE does not wish to accept the change, the DAO must advise the RA before the specified date of effect of the change.

## **10 Subscriber liability**

- 10.1 The HSE is liable in full for the acts and omissions of its DAO and any Authorised Users.
- 10.2 The HSE may be liable for any Loss that it, or any other person, may suffer arising from the use of its Location Keys and Certificates, or any act or omission that the HSE, the DAO and any Authorised Users commit in breach of the Location CP and this Agreement.

## **11 RA liability**

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

## **12 OCA liability**

- 12.1 The OCA is only liable under this Agreement for the Loss an entity or legal or natural person suffers if:

- (a) the OCA issued a Certificate under the Location CP;
  - (b) the OCA breached its obligations under the Location CP in respect of that Certificate; and
  - (c) the entity or person reasonably relied on that Certificate and as a result, suffered the Loss,
- 12.2 if the OCA acted negligently when it breached the relevant clause or clauses.

12.3 The OCA is not liable for any failure by the RA to perform its obligations under the Location CP.

### **13 Root Certification Authority (RCA) liability**

13.1 The RCA is only liable under this Agreement 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 clause 2.1.1.1 (g), (p), (q) or (r) of the Location CP in respect of that Certificate; and
- (c) the entity or person reasonably relied on that Certificate and as a result, suffered the Loss,

13.2 if the RCA acted negligently when it breached the relevant clause or clauses.

13.3 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 the Location CP or the transactions contemplated by the Location CP will not exceed AUD\$1,000 in relation to any one claim.

13.4 The RCA is not liable under or in connection with the Location 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 the Location CP, the RCA-issued CP, or any applicable Subscriber or Relying Party Agreement.

13.5 In no event shall the RCA be liable under or in connection with the Location 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.

### **14 Commonwealth liability**

14.1 Notwithstanding any other provision of the Location CP or this Agreement, and whether Keys or Certificates are used in a transaction with an Agency or not:

14.1.1 the Commonwealth makes no representations, and offers no warranties or conditions, express or implied, in relation to:

- (a) the activities or performance of any of the PKI Entities which are carried out under, or in relation to, the Location CP; or
- (b) if relevant, the services or products of a particular PKI Entity; and

14.1.2 the Commonwealth is not liable in any way whatsoever, for any Loss whether or not reasonably foreseeable, arising in connection with:

- (a) an entity described in the Location CP or the Individual CP carrying out, or omitting to carry out, any activity described in, or contemplated by, the Approved Documents;
- (b) the Commonwealth carrying out, or omitting to carry out, any activity related to the Gatekeeper Accreditation process; or
- (c) a negligent act or omission of the Commonwealth, the RA or the RCA / OCA.

### **15 Limited Warranties**

15.1 The RA and the RCA / OCA disclaim all warranties, express or implied. If any warranties or conditions are implied by legislation, then the liability of each of the RA and the RCA / OCA (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.

### **16 Contribution**

16.1 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 Location CP.

## **17 Indemnity from Subscriber and Relying Party**

- 17.1 Whether acting as a Subscriber or a Relying Party, the HSE indemnifies each of the RA, the RCA / OCA and the Commonwealth (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 this Agreement by the HSE, the DAO or an Authorised User; or
  - (b) the HSE's reliance on an Location Certificate or Individual Certificate in a transaction which is outside the purpose specified in the Location or Individual CPs (respectively).

## **18 General**

- 18.1 The Location CP and this 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.
- 18.2 In conducting the activities under the Location CP, all Parties agree to abide by the provisions of any relevant legislation, and the requirements of any Commonwealth, State, Territory or local body.
- 18.3 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 Location CP and this Agreement.

**Special note: Signature block overpage**

**Signed by the HSE Representative in his/her capacity as agent for the HSE<sup>1</sup>**

As an authorised representative of the HSE detailed on page 1 of this Agreement, I have the authority to sign on behalf of HSE and therefore bind it to this Agreement.

..... Signature of HSE Representative	..... Signature of witness
..... Name of HSE Representative	..... Name of witness [please print]
..... Date	..... Date
	..... ..... Address of witness [please print]
	..... Phone contact details of witness

---

<sup>1</sup> **SPECIAL NOTE REGARDING TRUSTS/PARTNERSHIPS THAT ARE NOT REGISTERED COMPANIES** (ie. have no Australian Company Number or ACN): HSE's in this situation may wish to have one or more members of the HSE sign this Agreement. Space is provided above for one member to sign. If other members wish to sign, please write the comparable signature block wording below/overpage with a witnessed signature/s. Trust/partnership members signing will need to include words comparable to "*As a member of the trust/partnership in question, I have the authority to sign on behalf of the trust/partnership and therefore bind the entity to this agreement*". Each member signing will need to provide personal identity documents to the RA. Please contact the RA if you have any questions regarding this matter.