GATEKEEPER INDIVIDUAL SUBSCRIBER AGREEMENT

INSTRUCTIONS FOR USE

Before a Certificate will be issued to you you need to follow these steps:

1. Fill in your name and the grade of Certificate you wish to be issued with.
2. You need to read and sign the Agreement.
3. The original signed copy of this Agreement must be provided to the VeriSign RA or a Gatekeeper Accredited RA authorised by the VeriSign CA.

I, _____ ('**Applicant**') wish to be issued with

Insert your name

an individual Gatekeeper certificate of grade _____.

Certificate Type *Insert Grade*

1. Background

1.1 The Chief Executive Officer for the National Office for the Information Economy ("**NOIE**") has accredited VeriSign Australia Pty Ltd trading as eSign Gatekeeper Services ("**eSign**") to provide certain Gatekeeper services to, or for the purposes of, Government Agencies.

1.2 You wish to obtain a VeriSign Gatekeeper Certificate of the Certificate Type and Certificate Grade set out above.

1.3 VeriSign's Public Gatekeeper Certification Services, and the use of the Individual Certificate, are governed by the VeriSign Individual CP as amended from time to time, which is incorporated in its entirety into this Agreement. This Agreement contains some important matters dealt with in the VeriSign Individual CP. For full details of the obligations of the VeriSign CA, the VeriSign RA, Subscribers, Relying Parties, and all other PKI Entities, please refer to the VeriSign Individual CP.

1.4 All documents referred to in this Agreement are published in the Repository (https://www.verisign.com.au/repository/gatekeeper/) on the VeriSign Gatekeeper Website (http://www.verisign.com.au/gatekeeper/).

2. Interpretation

Expressions used in this Agreement have the same meanings as they have under the VeriSign Gatekeeper CPS and the VeriSign Individual CP.

3. Obligations

3.1 This Agreement will become effective on the date a completed copy of this Agreement is signed by you at which point you become a Subscriber for the purposes of the VeriSign Individual CP.

3.2 By signing this Agreement you:

(a) request that the VeriSign CA issues you with a Certificate identifying you in accordance with the VeriSign Individual CP;

(b) agree to the terms of the VeriSign Individual CP; and

(c) agree to comply with the terms of the VeriSign Individual CP, including, without limitation, the following sections :

section 2.1.3 (Subscriber Obligations)
section 2.1.4 (Relying Party Obligations)
section 2.1.4.1 (Validating Digital Signatures)
section 2.2 (Liability)
section 2.4.1 (Governing Law)

section 2.4.2.1 (Severability)
section 2.4.2.2 (Survival)
section 2.4.2.4 (Precedence)

SIGNED BY THE APPLICANT

……

Signature

……

Print Name

……

Date

2.1.3 Subscriber Obligations

1. Each Applicant must securely generate his or her own Private Keys, using a Trustworthy System, and take necessary precautions to prevent their Compromise, loss, disclosure, modification, or unauthorised use. Applicants must comply with **section 6** of this CP.

EACH CERTIFICATE APPLICANT AND EACH SUBSCRIBER ACKNOWLEDGES THAT THEY, AND NOT VERISIGN, ARE EXCLUSIVELY RESPONSIBLE FOR PROTECTING THEIR PRIVATE KEY(S) FROM COMPROMISE, LOSS, DISCLOSURE, MODIFICATION, OR UNAUTHORIZED USE.

2. An Applicant becomes a Subscriber when Certificates are Issued to and Accepted by them.

3. A Subscriber may not delegate his or her responsibilities for the generation, use, retention, or proper destruction of his or her Private Keys.

4. Subscribers must:

   (a) ensure that their Private Keys are not Compromised;

   (b) immediately notify the VeriSign CA if they become aware that their Private Key has been Compromised, or there is a substantial risk of Compromise;

   (c) ensure that all information provided to the Relevant RA in relation to Issue and use of their Key Pairs and Certificates is to the best of their knowledge, true and complete;

   (d) immediately notify the VeriSign CA or the Relevant RA if there is any change to their Registration Information, or any other information provided to the VeriSign CA or the Relevant RA in relation to Issue and use of their Keys and Certificates.

   (e) use Keys and Certificates only for the purposes for which they were Issued and within the usage and reliance limitations, as specified in this CP, the Certificate Profile and the Certificate;

   (f) check the details set out in a Certificate on receipt, and promptly notify the VeriSign CA if faulty or improper Registration or Certificate Issuance has occurred; and

   (g) if requested by the Relevant RA, provide complete and accurate information in relation to their Registration Information or anything else relating to issue or use of their Keys and Certificates.

2.1.4 Relying Party obligations

1. Before relying on a Certificate or a Digital Signature, Relying Parties must:

   (a) Validate the Certificate and Digital Signature (including by checking whether or not it has been Revoked, Expired or Suspended) in accordance with **section 2.1.4.1**; and

   (b) ascertain and comply with the purposes for which the Certificate was issued and any other limitations on reliance or use of the Certificate which are specified in the Certificate, the CPS or this CP.

2. If a Relying Party relies on a Digital Signature or Certificate in circumstances where it has not been Validated in accordance with **paragraph 2.1.4.1** it assumes all risks with regard to it (except those that would have arisen had the Relying Party Validated the Certificate) and is not entitled to any presumption that the Digital Signature is effective as the signature of the Subscriber or that the Certificate is valid.

3. Relying Parties must also comply with any other relevant obligations specified in this CP including those imposed on the entity when it is acting as a Subscriber.

2.1.4.1 Validating Digital Signatures*

1. Validation of a Digital Signature is undertaken to determine that:

   (a) the Digital Signature was created by the Private Key Corresponding to the Public Key listed in the Certificate of the person affixing their Digital Signature to the information (the '**Signer**'); and

   (b) that the associated information has not been altered since the Digital Signature was created.

2. Validation of a Digital Signature is performed by applications following this process:

   (a) **Establishing a Certificate Chain for the Certificate used to sign the information** – In the case of a Public Hierarchy this involves confirming that the CA who Issued the Certificate is a Subordinate CA of the VGR. In the case of a Private Hierarchy it involves confirming that the CA who issued the Certificate is trusted by the Relying Party;

(b) **Checking the Repository for Revocation of Certificates in this Chain** – The Relying Party must determine if any of the Certificates along the chain from the Signer to an acceptable root within the VeriSign Gatekeeper PKI have been Revoked, because a Revocation has the effect of prematurely terminating the Operational Period during which verifiable Digital Signatures can be created. This may be ascertained by querying the CRL or OCSP responder (if available) to determine whether any Certificates in the Certificate Chain have been Revoked;

(c) **Applying the hash function to the signed data** – Apply the same hash function as was originally applied by the Signer;

(d) **Decrypting the original hash** – Using the Public Key contained in the Certificate decrypt the original hash value; and

(e) **Compare the hash functions** – If the value created by step 2(c) is the same as the value recovered by step 2(d), then the information is Validated.

3. A PKI Entity agrees that a Digital Signature may be relied upon against the Signer if:

(a) it was created during the Operational Period of a valid Certificate (ie before the Certificate Expired or was Revoked);

(b) the Digital Certificate used for Signing has the digitalSignature Bit asserted in the Key Usage extension;

(c) such Digital Signature can be properly Validated by confirmation of its Certificate Chain;

(d) the Relying Party has no knowledge or notice of a breach of the requirements of the CPS or this CP by the Signer;

(e) the purpose for which it was relied on was within the purposes or limitations referred to in the Certificate or the relevant Certificate Policy;

(f) the Relying Party has no knowledge of a reason why the Digital Signature should not be relied upon in the circumstances; and

(g) the Relying Party has complied with all relevant requirements of this CP.

RELYING PARTIES SEEKING TO VALIDATE DIGITALLY SIGNED MESSAGES ARE SOLELY RESPONSIBLE FOR EXERCISING DUE DILIGENCE AND REASONABLE JUDGMENT BEFORE RELYING ON CERTIFICATES AND DIGITAL SIGNATURES. A CERTIFICATE IS NOT A GRANT FROM VERISIGN OF ANY RIGHTS OR PRIVILEGES, EXCEPT AS SPECIFICALLY PROVIDED IN THE CPS OR THIS CP.

YOU ARE HEREBY NOTIFIED OF THE POSSIBILITY OF THEFT OR OTHER FORM OF COMPROMISE OF A PRIVATE KEY CORRESPONDING TO A PUBLIC KEY CONTAINED IN A CERTIFICATE, WHICH MAY OR MAY NOT BE DETECTED, AND OF THE POSSIBILITY OF USE OF A STOLEN OR COMPROMISED KEY TO FORGE A DIGITAL SIGNATURE TO A DOCUMENT. FOR INFORMATION REGARDING PRIVATE KEY PROTECTION, SEE THE VERISIGN GATEKEEPER WEBSITE.

4. Additionally, the Relying Party should consider the Certificate Grade. The final decision concerning whether or not to rely on a verified Digital Signature is exclusively that of the Relying Party.

2.2 Liability[1]

2.2.1 Liability Generally*

1. The liability of an entity referred to in this CP for breach of a contract to which the entity is a party, or for any other common law or statutory cause of action, shall be determined under the relevant law in Australia that is recognised, and would be applied, by the High Court of Australia.

2. Where a PKI Entity is legally liable to compensate another party, the liability of the first mentioned PKI Entity will be reduced proportionally to the extent that any act or omission on the part of the other PKI Entity contributed to the relevant liability, loss, damage, cost or expense.

3. The PKI Entities acknowledge that one of the factors that affects their ability to limit their liability is the extent to which they effectively notify the PKI Entity suffering the loss or damage of any limits or limitations on which the entity intends to rely.

4. The provisions set out in this **section 2.2** survive the termination of the relevant contract.

[1] The sections of heading 2.2 have been significantly expanded from RFC2527.

5. Apart from **section 2.2.2**, the liability regime applicable to activities conducted under this CP by the VeriSign CA or the VeriSign RA is not evaluated by NOIE evaluators (Australian Government Solicitor) or accredited by the Competent Authority.

2.2.2 Liability of the Commonwealth*

1. The Competent Authority is only responsible for performing the accreditation process with due care, in adherence to published Gatekeeper Criteria and Policies. The Competent Authority is not liable for any errors and/or omissions in the final Approved Documents, which remain the responsibility of the accredited Certification or Registration Authority as the case may be.

2. Notwithstanding any other provisions of this CP:

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

      (i) the activities or performance of any of the PKI Service Providers which are carried out under, or in relation to, this CP; or

      (ii) if relevant, the services or products of a particular PKI Service Providers; and

   (b) the PKI Entities acknowledge and agree that except to the extent that a Commonwealth Agency is carrying out the role of a PKI Entity (in which case the liability of the Commonwealth will be determined in accordance with the provisions set out in this **section 2.2**), the Commonwealth is not liable in any manner whatsoever whether the Keys or Certificates are used in a transaction with an Agency or not, for any loss or damage caused to, or suffered by any person, including a PKI Entity as a result of:

      (i) an entity described in this 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;

      (iii) a negligent act or omission of the Commonwealth.

2.2.3 Force majeure*

1. A PKI Entity is not liable for any loss or damage arising from any delay or failure to perform its obligations described in the CPS or this CP if such delay is due to Force Majeure.

2. If a delay or failure by a PKI Service Provider to perform its obligations is due to Force Majeure, the performance of that entity's obligations is suspended.

3. If delay or failure by a PKI Service Provider to perform its obligations due to Force Majeure exceeds 30 days, the PKI Entity affected by the failure to perform the obligations may terminate the arrangement, agreement or contract it has with the non-performing PKI Service Provider on providing notice to that PKI Entity in accordance with this CP. If the arrangement, agreement or contract is terminated, then the non-performing PKI Service Provider shall refund any money (if any) paid by the terminating entity to the non-performing entity for services not provided by the non-performing PKI Service Provider.

2.2.4 VeriSign and Relevant RA Liability*

1. VeriSign and the Relevant RA exclude all warranties, conditions and obligations of any type from the relationship between VeriSign or the Relevant RA and any other PKI Entity (including without limitation as a result of operating the VeriSign CA or the VeriSign RA or the VGR) except:

   (a) to the extent otherwise provided in this CP; or

   (b) where a condition or warranty is implied into an agreement by a law, and that condition or warranty cannot be excluded.

2. In no event will VeriSign or the Relevant RA be liable for any indirect, special, incidental, or consequential damages or for any loss of profits or revenues, loss of data, loss of use, loss of goodwill, or other indirect, consequential, or punitive damages, whether or not reasonably foreseeable, arising from or in connection with the use, delivery, license, performance, or non-performance of Certificates, Digital Signatures, or any other transaction or services related to or offered or contemplated by the CPS or this CP, breach of contract or any express or implied warranty or indemnity under or in relation to any Certificates or the CPS or this CP or otherwise misrepresentation, negligence, strict liability or other tort, even if VeriSign or the Relevant RA has been advised of the possibility of such damages or should have been aware of such a possibility.

3. VeriSign's and the Relevant RA's aggregate liability to a non-VeriSign PKI Entity and any and all persons concerning a Certificate for the aggregate of all Digital Signatures and transactions related to that Certificate, shall be limited to AUD50,000.

4. In the event that VeriSign's or the Relevant RA's total liability exceeds the amount above, the available liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court of competent jurisdiction. In no event shall VeriSign or the Relevant RA be obligated to pay more than the aggregate liability cap for each Certificate, regardless of the method of apportionment among claimants to the amount of the liability cap.

5. In regard to section 2.2.4 VeriSign is also contracting as an agent for Australia Post. Subscribers and Relying Parties agree that they have not relied on any warranty or representation by Australia Post in entering the Subscriber Agreement or the Relying Party Agreement.

2.2.5 Subscriber Liability*

1. The Subscriber:

   (a) is solely responsible for the contents of any transmission, message or other document signed using the Subscriber's Private Key;

   (b) warrants to all Relying Parties that during the Operational Period of the Certificate :

      (i) no unauthorised person has ever had access to the Subscriber's Private Key;

      (ii) the Certificate will be used exclusively for appropriate and lawful purposes;

      (iii) at the time the Digital Signature is created, the Certificate has not Expired or been Suspended or Revoked;

      (iv) all representations made by the Subscriber or authorised by the Subscriber to the VeriSign CA or to the Relevant RA, are true;

      (v) all information contained in the Certificate is to the Subscriber's knowledge true;

      (vi) each Digital Signature created using the Private Key Corresponding to the Public Key listed in the Certificate is the Subscriber's Digital Signature;

      (vii) the Subscriber will not use the Private Key Corresponding to any Public Key listed in the Certificate for purposes of signing any Digital Certificate (or any other format of certified Public Key) or Certificate Revocation List, unless expressly agreed in writing with VeriSign, and

      (viii) when the Subscriber encrypts the hash of a document with the Subscriber's Private Key, in circumstances where the Subscriber's Certificate has not been Suspended or Revoked, others may act on that as if the Subscriber had signed the document with the Subscriber's usual signature in the normal way;

   (c) indemnifies the VeriSign CA and the Relevant RA for any loss, damage and expense of any kind, arising out of or in connection with:

      (i) the manner and extent of the use or publication of the Subscriber's Certificate except to the extent that the use or publication of the Key Holder's Certificate was caused by the VeriSign CA or the Relevant RA using or publishing the Key Holder's Certificate other than as allowed by this CP;

      (ii) the Subscriber's negligence or wilful misconduct;

      (iii) any falsehood or misrepresentation of fact by the Subscriber (or any person acting on the Subscriber's instructions);

      (iv) the Subscriber's failure to disclose a material fact, if the misrepresentation or omission was made negligently or with the intent to deceive the VeriSign CA or the Relevant RA or any person receiving or relying on the Subscriber's Certificate; or

      (v) any failure by the Subscriber to protect the Subscriber's Private Key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the Compromise, loss, disclosure, modification, or unauthorised use of the Subscriber's Private Key,

   except to the extent that the Subscriber's Private Key or Certificate has been Compromised by VeriSign's or the Relevant RA's wilfully wrongful, fraudulent or negligent conduct.

2.2.6 Relying Party Liability

No stipulation.

2.4 Interpretation and Enforcement

2.4.1 Governing law

1. This CP and the CPS are governed by, and are to be construed in accordance with, the laws from time to time in force in the Australian Capital Territory, Australia.

2. The PKI Entities agree to submit to the jurisdiction of the courts having jurisdiction within the Australian Capital Territory, Australia.

2.4.2 Severability, survival, merger, notice

*2.4.2.1 Severability**

Any reading down or severance of a particular provision does not affect the other provisions of this CP or the CPS.

*2.4.2.2 Survival**

Provisions described as having an ongoing operation survive the termination or expiration of the relevant contractual relationship between any PKI Entities.

*2.4.2.4 Precedence**

To the extent of any conflict between the following documents the first mentioned document shall govern:

(a) this CP;

(b) the CPS;

(c) the Individual Subscriber Agreement;

(d) another agreement between the parties as to the manner and provision of the services described herein;

(e) another Approved Document; and

(f) a document that is not an Approved Document.