GATEKEEPER TYPE 3 SUBSCRIBER AGREEMENT

_____ (‘**Organisation’s Representative**’) of
Insert name of person signing this Agreement

_____ABN: _____ (‘**Organisation**’)
Insert Organisation’s Name

hereby authorises the Organisation’s Authorised Officers appointed for the purpose of issuing ABN-DSCs to act as Authorised Officers in respect of Type 3 Gatekeeper Certificates on behalf of the Organisation on the terms and conditions of this Agreement.

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 to provide certain Gatekeeper services to, or for the purposes of, Government Agencies.

1.2 The Organisation wishes to authorise Authorised Officers appointed for the purpose of issuing ABN-DSCs to also be able to request the Issuance and Revocation of Type 3 Certificates (“**Certificate**”) which will be installed on a Device and identify the relevant application, device, process or service owned, operated or controlled by the Organisation.

1.3 VeriSign’s Public Gatekeeper Certification Services, and the use of the Certificates, are governed by the VeriSign Type 3 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 Type 3 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 Type 3 CP.

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

2. Interpretation

Expressions used in this Agreement have the same meanings as they have under the VeriSign Gatekeeper CPS and the VeriSign Type 3 CP.

3. Obligations

3.1 This Agreement will become effective on the date a completed copy of this Agreement is signed by the Organisation’s representative at which point each Authorised Officer and the Organisation become a Subscriber for the purposes of the VeriSign Type 3 CP.

3.2 By signing this Agreement the Organisation:

(a) agrees that on the instructions of an Authorised Officer (which may be communicated by means of an email digitally signed with an Authorised Officer’s Private Key) the VeriSign CA may:

(i) Issue Certificates for use by Devices identifying the Organisation and the nominated application, device, process or service;

(ii) Revoke Certificates; and

(iii) perform such other actions as are specified in the VeriSign Type 3 CP;

(b) agrees that the VeriSign CA and the Relevant RA may treat the instructions of an Authorised Officer as the Organisation's instructions in accordance with the VeriSign Type 3 CP;

(c) agrees to the terms of the VeriSign Type 3 CP; and

(d) agrees to take responsibility to ensure that each Authorised Officer complies with the terms of the VeriSign Type 3 CP, including, without limitation, the following sections which are attached:

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 for and on behalf of Organisation
by an officer having the authority to bind the business entity

……..
Signature

…….
Print Name

……..
Title

…….
Date

Once completed please mail to:
Gatekeeper Validations Department
VeriSign Australia Pty Ltd
PO Box 3092 South Melbourne 3205

*2.1.3 Subscriber Obligations**

THE ORGANISATION ACKNOWLEDGES THAT IT, AND NOT VERISIGN, IS EXCLUSIVELY RESPONSIBLE FOR PROTECTING ITS PRIVATE KEY(S) FROM COMPROMISE, LOSS, DISCLOSURE, MODIFICATION, OR UNAUTHORIZED USE.

1. The obligations of a Subscriber are imposed on the Organisation and the Authorised Officer who acts on behalf of the Organisation as set out in this **Section 2.1.3**.

2. Organisations must through an Authorised Officer:

   (a) ensure that only appropriately authorised people perform any of the functions specified in **section 3.1.11.2**;

   (b) ensure that Private Key(s) are generated using a Trustworthy System;

   (c) ensure that anyone performing any of the functions specified in **section 3.1.11.2** comply with their obligations under this CP and the CPS;

   (d) provide measures to avoid Compromise. loss, disclosure, modification or unauthorised use of Private Keys;

   (e) immediately notify the VeriSign CA when the Organisation becomes aware that a Private Key has been Compromised, or there is a substantial risk of Compromise;

   (f) ensure that all information provided to the VeriSign CA or 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;

   (g) immediately notify the VeriSign CA or the Relevant RA if:

      (i) there is any other change to the Registration Information, or any other information provided to the Relevant RA in relation to Issuance and use of their Certificates.

      (ii) the Device on which the Certificate is installed is sold, decommissioned, destroyed or lost;

      (iii) the application, Device, process or service identified by the Certificate ceases to be under the control of the Organisation; or

      (iv) the Organisation ceases to belong to the Community of Interest;

   (h) if requested by the Relevant RA, provide complete and accurate Registration Information or anything else relating to Issuance or use of the Keys and Certificates;

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

   (j) 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

   (k) where they generate Key Pairs, comply with **section 6.**

3. The Organisation agrees not to copy the Certificate (except for the purposes of backup and Escrow as permitted under this Certificate Policy) or to use the Certificate on more than one Device.

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 Expired or been Revoked 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 Device 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 Revocat ion 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 Subscriber 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 Subscriber;

(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.

THE USE OF CERTIFICATES DOES NOT NECESSARILY CONVEY EVIDENCE OF **AUTHORITY** ON THE PART OF ANY USER TO ACT ON BEHALF OF ANY PERSON OR TO UNDERTAKE ANY PARTICULAR ACT. RELYING PARTIES SEEKING TO VALIDATE DIGITALLY SIGNED MESSAGES ARE SOLELY RESPONSIBLE FOR EXERCISING DUEDILIGENCE AND REASO NABLE 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 http://www.verisign.com.au/gatekeeper.

4. The final decision concerning whether or not to rely on a verified Digital Signature is exclusively that of the Relying Party.

2.1.5 Repository Obligations

An entity operating a repository must ensure timely publication of Certificates and Revocation information as required by this CP.

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.

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 Authorised Legal Evaluators or approved 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 Accredited 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 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-

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

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 including 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**

2.2.5.1 Organisation

1. The Organisation is responsible and therefore liable for any acts of Authorised Officers or those to whom obligations have been delegated in relation to the CPS and this CP, and in particular in relation to the use of Keys and Certificates Issued under this CP.

2. The Organisation:

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

   (b) warrants to all Relying Parties that during the Operational Period of the Certificate, and until notified otherwise by the Organisation that:

      (i) no unauthorised person has ever had access to the Certificate'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 Organisation, or authorised by the Organisation or the Authorised Officer to the VeriSign CA or to the Relevant RA, are true;

      (v) all information contained in the Certificate is to the Organisation's and the Authorised Officer's knowledge true and complete;

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

      (vii) the Organisation will not allow the Private Key Corresponding to any Public Key listed in the Certificate to be used 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 Organisation encrypts the hash of a document with the Private Key, in circumstances where the Certificate has not been Suspended or Revoked, others may act on that as if the Organisation had signed the document with the Organisation'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 Organisation's or the Authorised Officer's negligence or wilful misconduct;

(ii) any falsehood or misrepresentation of fact by the Organisation or the Authorised Officer (or any person acting on the Organisation's instructions);

(iii) the Organisation's or the Authorised Officer'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 Certificate; or

(iv) any failure by the Organisation or the Authorised Officer to protect the 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 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.

(d) indemnifies the VeriSign CA and the Relevant RA for any loss, damage and expense of any kind, arising out of or in connection with the manner and extent of the use or publication of the Organisation's Certificate except to the extent that:

(i) the use or publication of that Certificate was caused by the VeriSign CA or the Relevant RA using or publishing the Certificate other than as allowed by this CP; or

(ii) the Organisation's Private Key or Certificate has been Compromised by VeriSign's or the Relevant RA's wilfully wrongful, fraudulent or negligent conduct.

2.2.5.2 Key Holder Liability

No stipulation.

2.2.5.3 Authorised Officer Liability

Organisations are responsible and liable for the use made by Authorised Officers of Certificates and Keys and the instructions issued to the VeriSign CA and PKI Entities by the Authorised Officer. Organis ations may make their own arrangements with Authorised Officers concerning the policies and procedures for use of the Certificates and Keys and providing Issuing and Revocation instructions to the VeriSign RA and PKI Entities, and liability provisions.

2.2.6 Relying Party Liability

No stipulation.

2.3 Financial responsibility

2.3.1 Indemnification of Relying Parties

No stipulation.

2.3.2 Fiduciary relationships

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

2.3.3 Administrative processes

VeriSign's financial viability was examined before it was granted endorsement under the Endorsed Supplier Arrangements.

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.

2.4.2.3 Notice*

1. Notices to Subscribers must be sent to the physical, postal, facsimile or email address of the Subscriber, which is included in its Registration Information, or to another address which the Subscriber has specified to the sender.

2. Notices to a PKI Service Provider must be sent to the physical, postal, facsimile or e-mail address of that entity set out on the VeriSign Website, or to another address which the entity has specified to the sender.

3. A notice to any entity in relation to this CP must be signed by the sending entity. If the notice is sent electronically it must be digitally signed.

4. A notice sent is taken to be received:

   (a) if it is hand-delivered to a physical address - at the time of delivery whether or not any person is there to receive it;

   (b) if it is posted by prepaid post - at 5pm on the third day after it is posted even if the notice is returned to the sender;

   (c) if it is transmitted by facsimile - when the sending machine produces a report showing the transmission was successful; and

   (d) if it is sent by e-mail - when it enters a system under the control of the addressee.

5. If, under the previous paragraph, a notice would be taken to be received outside normal business hours at the addressee's place of business, the parties agree in these circumstances that it is actually taken to be received at 9 am on the next business day at that place.

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 Type 3 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.