VANguard Relying Party PKI Disclosure Statement (PDS)

Notice to Relying Parties

This PKI Disclosure Statement (PDS) applies to VANguard relying party certificates.

VANguard is an Australian Commonwealth program intended to provide authentication and time stamping services to facilitate online business activities. It is administered by the Australian Department of Industry, Innovation and Science (the Department).

Before trusting a certificate issued in association with this PDS identified by the object identifier (OID) **1.2.36.1.1001.30.8.1** you must have read and understood the provisions of this document.

Use constitutes acceptance.

The conditions applicable to each type of VANguard certificate will vary.

In each VANguard certificate, the certificate policies extension will be used to clearly indicate the OID under which the certificate has been issued and the purposes for which the certificate may be used. It will contain the Certification Practice Statement (CPS) URL where this PDS and the CPS are published, and a text field with the following disclaimer:

'*This certificate is subject to the usage constraints and limitations of liability contained in the PDS and Service Level Agreement. Reliance not expressly permitted in those documents is not supported.'*

Certification Authority (CA) Contact Information

Use the 'Contact Us' link on the VANguard website if you have any questions in relation to this PDS: http://www.vanguard.business.gov.au

For information regarding Certification Authority (CA) functions including support contact details and support hours, refer to the applicable Service Level Agreement (SLA).

Certificate Type, Validity, and Uses

The Department issues numerous certificates under this PDS to different relying parties on request, for example, State and Federal agencies and local councils, and other organisations, subject to the signing of a Memorandum of Understanding (MOU) and an SLA between the relying party and the Department.

VANguard relying party certificates may be used:

- to authenticate the relying party to VANguard so that they can access VANguard services
- to protect the security of communications between the relying party and VANguard
- for communications outside the VANguard system
- by VANguard to identify which relying party it was that submitted a transaction request.

VANguard relying party certificates are valid for four years, with reissue recommended every 36 to 42 months.

Relying party certificates must be validated using X.509 v3 certificate processing rules.

Certificate Issuing, Renewal, and Revocation

The Department provides a Roaming Registration Authority (RRA) to register relying parties onsite through an in-person visit by the VANguard RRA.

The RRA will validate Evidence of Identity (EOI), and issue the relying party with the VANguard trust point certificates.

As certificates near their end of life, the relying parties will generate new keys, and VANguard will issue new certificates. The new certificates will be valid and can be used immediately.

Privacy

Relying party certificates will contain the relying party name and Australian Business Number (ABN).

Relying party certificates subject to this PDS contain no personal information.

All VANguard certificate policies and practices require strict adherence to the *Privacy Act 1988 (Cth)* including, as appropriate, the Information Privacy Principles and the National Privacy Principles.

Audit

VANguard may be subject to audit by the Privacy Commissioner and the Commonwealth or State Auditor-General(s).

VANguard's Gatekeeper accredited certificate provider is accountable to the Gatekeeper Competent Authority for their compliance with relevant standards and the Gatekeeper regime overall.

Trust Marks

The provider of certificate services to VANguard must be Gatekeeper accredited.

The VANguard MPKI has been designed to reflect best practice and the following standards:

- ASD, *Australian Government Information Security Manual (ISM)*
- Commonwealth of Australia, *Protective Security Policy Framework* (PSPF)
- OASIS, *WS-Trust 1.3 - Security Token Service (STS) framework*, March 2007
- IETF*, RFC 5750 – Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling*, January 2010
- IETF, *RFC 6818 – Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,* January 2013
- IETF, *RFC 5652 – Cryptographic Message Syntax (CMS)*, September 2009
- IETF, *RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, November 2003
- IETF, *RFC* 5816 - *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)* ESSCertIDv2, April 2010

Reliance Limits

Relying Parties may be organisations who elect to use VANguard certificates in non-VANguard communications.

The VANguard business model does not provide for certificates with different levels of suitability for use up to pre-determined financial limits.

VANguard does not accept any liability in relation to the operations of the VANguard MPKI.

Relying Parties are advised that before using VANguard relying party certificates to engage in communications they should conduct their own individual risk assessment. Factors to consider are EOI processes in use, and any approvals that may have been granted by the Gatekeeper Competent Authority.

In particular, relying parties are advised that it may be prudent to use the telephone or another out-of-band channel to confirm that the certificate in question is suitable for use by a particular application.

Warranties, Liability and Indemnities

The Department will operate the VANguard MPKI:

- in accordance with applicable law
- with reasonable skill, diligence, and care
- in accordance with applicable industry standards and practice
- in accordance with the the requirements of this PDS and the associated CP and CPS.

No other warranties, express or implied, are given by the Department, or by any other entity who may be involved in the issuing or managing of certificates for the VANguard MPKI ('Service Providers'). All statutory warranties are excluded, to the extent permitted by law.

The Department accepts no liability under this PDS for or in connection with the VANguard MPKI and, without limitation, is not liable for the relying party's use of digital certificates issued under the VANguard MPKI, or otherwise in connection with those certificates.

This exclusion of liability:

- applies only to the extent permitted by law; and
- applies whether the liability arises in contract, tort (including negligence) or otherwise.

Unless otherwise set forth in contract, any organisation who relies on or makes use of a VANguard relying party certificate continually indemnifies the Department against all loss, liability, and expense caused by the use or publication of a certificate that arises from:

- use for illegal or improper purposes
- use for any purpose not explicitly permitted under this PDS
- a false or misleading statement of fact by any party other than VANguard
- any omission by the relying party to disclose a material fact if that omission was negligent or intended to deceive
- any failure on the part of the relying party to inform themselves of the terms and conditions of this document.

Applicable Law and Dispute Resolution

The law of the Australian Capital Territory (ACT) shall govern the interpretation and enforcement of this PDS, the SLA, the CPS, and any other associated agreements.

Disputes between parties to an SLA shall be resolved according the applicable provisions of that agreement. All disputes may be resolved through mediation or other form of alternative dispute resolution if both parties so choose; however, nothing in this clause affects either party's rights or its ability to commence legal proceedings.

Relying Party Obligations

As subscribers to VANguard, relying parties must:

- enter into and comply with the MOU and SLA
- protect their VANguard keys and certificates from compromise
- immediately notify the Department if they suspect their keys and certificates have, or may have been, compromised
- accept sole responsibility for the contents of any transmission, message, or other document signed with their keys and certificates
- destroy all copies of the key(s) on request
- use their keys and certificates at their sole risk
- provide accurate and complete information to the Department when applying for keys and certificates, and at all other times
- promptly notify the Department in the event that any part of that information changes

- use VANguard keys and certificates for the purposes authorised, and not for any other purpose including any unlawful or improper purpose
- conduct their own independent risk assessment when using VANguard certificates in non-VANguard applications.

Relying Party Obligations

Unless notified by VANguard in writing, relying parties that rely on VANguard certificates must check the certificate chain up to the issuing OCA and check the applicable CRL.

A relying party must promptly notify VANguard in the event that it suspects that there has been a compromise of the relevant VANguard trust point certificates.

Refund Policy

No refunds apply as VANguard does not charge fees to for either VANguard services or VANguard certificates.

Agreements, Certification Practice Statement (CPS)

A document hierarchy applies: the provisions of the applicable SLA or other relevant contract override the provisions of this PDS.

The provisions of this PDS override any applicable CPS.