Suite 2.01
40 Cameron Ave
BELCONNEN
ACT 2617

5 March 2024

Ms Amelia Robards
a/Operations Manager,
Certificate and Directory Management Centre
CDMC | DDIS | ETOB | ICTOD | JCG

Dear Ms Robards,

Ref: Microsoft Root Certificate Program Attestation Letter

1. In accordance with the Microsoft Government Certification Authority Agreement between Microsoft Corporation and the Commonwealth of Australia Ionize have undertaken the annual audit of the Defence Public Key Infrastructure (PKI) as an Equivalent WebTrust audit for the following Certificate Authority:

Auditor	Ionize Pty Ltd
CA Owner	Department of Defence Australia
CA Name	Australian Defence Public Root CA
Subject Name	CN=Australian Defence Public Root CA,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
SHA1 thumbprint	A9CAFE9DFD67F4145AD397D0E2F3050D198DE6EE
SHA2 thumbprint	209E956AF04DF3996507C887D356230D6EB49FDBDD2D8A058FF50B8F80F690AA
Audit Start	AuditPeriodStart=2023-03-01
Audit End	AuditPeriodEnd=2024-02-29
Audit	Standard Audit Type BR Audit Type
Australian Defence Public Root CA hierarchy	Australian Department of Defence Public Identity Certificate Authority Australian Department of Defence Public Identity CA G2 Australian Department of Defence Public Device Certificate Authority

2. As an independent third party, Ionize undertook this Equivalent WebTrust audit utilising the requirements of the Commonwealth of Australia Gatekeeper PKI Framework Compliance Audit Program[1], as overseen by the Department of Finance. This audit period was of 1 March 2023 to 29 February 2024 by Lee Mansfield (IRAP #1043) a registered Information Security Registered Assessor Program[2] participant for the following Certificate Authorities (CAs):

Root Certificate Authorities

[1] https://www.dta.gov.au/our-projects/digital-identity/join-identity-federation/accreditation-and-onboarding/gatekeeper-public-key-infrastructure-framework
[2] https://www.cyber.gov.au/programs/irap

- Australian Department of Defence Public Root CA

Subordinate Certificate Authorities

- Australian Department of Defence Public Identity Certificate Authority
- Australian Department of Defence Public Device Certificate Authority

3. The Department of Defence is solely responsible for the management and issuance of all certificates under the Defence Root CA. As a condition of Gatekeeper accreditation, the Department of Defence Certificate and Directory Management Centre (CDMC) must undertake Gatekeeper PKI Framework annual compliance audits with a failure to conduct an annual Gatekeeper compliance audit represents a breach of the Gatekeeper Head Agreement (GHA)/ Memorandum of Agreement (MOA) and may result in termination of accreditation.

4. In addition to the annual Gatekeeper Audit, additional comparison assessment was undertaken against the WebTrust Principles and Criteria for Certification Authorities Version 2.2.2 and the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.7.

5. A total of 107 Gatekeeper Compliance Audit Program controls were assessed as part of this 2024 Gatekeeper IRAP assessment, with the controls segmented into the categories of : Gatekeeper Approved Documents, Personnel Security, Physical and Environmental security, Media and ICT Equipment Management, Access Control Management, Operations Security, CA Subscriber Key Lifecycle Management, Subscriber Key Lifecycle Management, Incident Management, Business Continuity Management, and Outsourced Arrangements.

6. Of these requirement areas, the Defence PKI was deemed compliant with all Gatekeeper Compliance Audit Program controls that were applicable.

7. As this Gatekeeper assessment is an IRAP assessment, it is a requirement of the IRAP assessment process that all changes to the Australian Government Information Security Manual (ISM) be incorporated into the assessment. Where applicable within the existing Gatekeeper Controls, the Control criteria has been updated to reflect the latest specification of a control within the ISM. With multiple iterations of the ISM since the Gatekeeper framework was released, any new controls have been included in this assessment.

8. The result of the Defence PKI Gatekeeper Audit was the recommendation to the Department of Finance by the Authorised Auditor who conducted the audit, that the Defence PKI that provides both Certificate and Registration Authority services for PKI use within the Australian Defence Force (ADF) should retain its Gatekeeper accreditation.

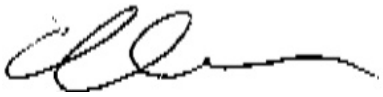
9. The second assessment undertook a comparison of the Defence PKI environment against the international WebTrust Principles and Criteria for Certification Authorities Version 2.2.2 standard, which has been specified for audit periods commencing after June 1, 2021. While this assessment is only a comparison and not a formal or endorsed WebTrust audit, the assessor did find through the assessment process, sufficient comparison to have a high level of confidence that the Certificate and Directory Management Centre was compliant to the WebTrust 2.2.2 standard.

10. The third assessment undertook a comparison of the Defence PKI environment against WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Version 2.7 standard, which has been specified for audit periods commencing after April 1, 2023. While this assessment is only a comparison and not a formal or endorsed WebTrust audit, the assessor did find through the assessment process, sufficient comparison to have a high level of confidence

that the Certificate and Directory Management Centre was compliant to the WebTrust SSL Baseline with Network Version 2.7 standard.

11. The CDMC as a leading PKI facility in the Gatekeeper program, is congratulated on the completion of another successful IRAP Gatekeeper assessment process and their day-to-day operation of the Defence PKI environment.

Warmest Regards,





Andrew Muller | Managing Director.

Date: 5 March 2024

Lee Mansfield | IRAP Assessor.

Date: 5 March 2024