Deloitte.

Deloitte Touche Tohmatsu
ABN 74 490 121 060

8 Brindabella Circuit
Brindabella Business Park ACT 2609
GPO Box 823
Canberra ACT 2601 Australia

Tel: +61 2 6263 7000
Fax: +61 6263 7004
www.deloitte.com.au

Jody Cloutier
Sr. Security Program Manager
Microsoft Crypto Ecosystem
Microsoft Corporation
One Microsoft Way, Redmond,
Washington 98052-6399 USA

27 July 2016

Ref: Microsoft Root Certificate Program Attestation Letter (Work Order No. CIOG487/15)

With respect to the Microsoft Government Certification Authority Agreement between Microsoft Corporation and the Commonwealth of Australia acting through and represented by the Department of Defence, Deloitte has undertaken the annual audit of the Defence PKI against the requirements of the Commonwealth of Australia Gatekeeper Public Key Infrastructure Framework Compliance Audit Program(https://www.dto.gov.au/files/authentication-framework/Gatekeeper-PKI-Framework-Compliance-Audit-Program-v2_1.pdf).

Under the Gatekeeper Public Key Infrastructure (PKI) Framework, in accordance with Clause 11 of the Gatekeeper Head Agreement/Memorandum of Agreement, the Department of Defence Certificate and Directory Management Centre must undertake annual compliance audits to retain Gatekeeper accreditation. Specifically the Digital Transformation Office requires that Authorised Auditors conduct an audit of Service Providers' compliance with the Framework. Failure to conduct an annual Gatekeeper compliance audit represents a breach of the Gatekeeper Head Agreement/ Memorandum of Agreement and may result in termination of accreditation.

This assessment was undertaken by Lee Mansfield (IRAP Assessor) on behalf of Deloitte as an Authorised Auditor and was conducted over the period January 2016 to April 2016. As part of the Gatekeeper IRAP assessment, the Certificate and Directory Management Centre was assessed against a total of two hundred and twenty eight (228) controls.

During the audit, Deloitte also undertook, as an adjunct to the annual Gatekeeper Accreditation Framework audit (which is the Australian government standard that ensures the integrity of an entity's identity in a consistent manner), an assessment of the Defence PKI against the WebTrust 2.0 standard. While this assessment was not a formal or endorsed WebTrust audit, the assessor did find sufficient comparison through the assessment process, to have a high level of confidence that the Defence PKI was primarily compliant to the WebTrust standard. It should be noted that Gatekeeper Compliance Audit Program, in Annex C and D, maps the controls listed between it and WebTrust and ETSI.

Whilst the audit identified some areas to be remediated, none of these were rated as Critical. As such, as a result of the audit, it is in the opinion of the assessor that the Defence PKI is still sufficiently compliant with the Gatekeeper Framework that the Australian Department of Defence should retain its Gatekeeper Accreditation.

The Certificate and Directory Management Centre has also undertaken to address the assessment reports recommendations and non-compliances through the 2016 Audit Remediation Plan, presented to the IRAP assessor after review of a draft assessment report. It is expected that the Certificate and Directory Management Centre shall further increase their compliance and mitigate their risks. The Certificate and Directory Management Centre should be congratulated on the day to day operation of the Defence PKI environment and the completion of a successful IRAP Gatekeeper assessment process.

Warmest Regards,

Matt O'Donnell

Partner

Date: 27th July 2016

Lee Mansfield

IRAP Assessor

Date: 27th July 2016