

INDEPENDENT ACCOUNTANT'S REPORT

To the management of Microsoft Corporation Digital Security & Resilience ("Microsoft DSR"):

Scope

We have examined Microsoft DSR management's [assertion](#) that for its Certification Authority ("CA") operations in United States of America, and in Ireland for its CAs as enumerated in [Attachment A](#), Microsoft DSR has:

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

throughout the period July 1, 2023 to June 30, 2024, based on the [WebTrust Principles and Criteria for Certification Authorities – Network Security, v1.0](#).

Certification authority's responsibilities

Microsoft DSR's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – Network Security, v1.0.

Practitioner's responsibilities

Our responsibility is to express an opinion on Microsoft DSR management's assertion based on our examination. Our examination was conducted in accordance with AT-C Section 205, *Assertion-Based Examination Engagements*, established by the American Institute of Certified Public Accountants, and International Standard on Assurance Engagements ("ISAE") 3000, *Assurance Engagements Other Than Audits or Reviews Of Historical Financial Information*. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

The relative effectiveness and significance of specific controls at Microsoft DSR and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls and other factors present at individual subscriber and relying party locations. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

Our independence and quality control

We are required to be independent and to meet other ethical responsibilities in accordance with the Code of Professional Conduct established by the American Institute of Certified Public Accountants ("AICPA") and Code of Ethics for Professional Accountants (including International Independence Standards) issued by the International Ethics Standards Board of Accountants' ("IESBA"). We have complied with those requirements. We applied the Statements on Quality Control Standards established by the AICPA and the International Standards on Quality Management issued by the International Auditing and Assurance Standards Board ("IAASB") and, accordingly, maintain a comprehensive system of quality control.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at Microsoft DSR and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Practitioner's opinion

In our opinion management's assertion, as referred to above, is fairly stated, in all material respects.

This report does not include any representation as to the quality of Microsoft DSR other than its CA operations in the United States of America, and in Ireland, nor the suitability of any of Microsoft DSR services for any customer's intended purpose.

Use of the WebTrust seal

Microsoft DSR's use of the WebTrust for Certification Authorities – Network Security Seal constitutes a symbolic representation of the contents of this report, and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

Deloitte & Touche LLP

Deloitte & Touche LLP
September 03, 2024

ATTACHMENT A

LIST OF IN SCOPE CAs

DV SSL Issuing CAs
1. Microsoft RSA TLS CA 01
2. Microsoft RSA TLS CA 02

CA IDENTIFYING INFORMATION

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
1	1	CN = Microsoft RSA TLS CA 01 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	C = IE, O = Baltimore, OU = CyberTrust, CN = Baltimore CyberTrust Root	0F14965F202069994FD5C7AC788941E2	RSA	SHA-256	Jul 21 23:00:00 2020 GMT	Oct 8 07:00:00 2024 GMT		TLS Web Server Authentication, TLS Web Client Authentication	B5760C3011CEC792424D4CC75C2CC8A90CE80B64	04EEEE8E50B4775B3C24797262917EE50002EC4C75B56CDF3EE1C18CFCAS8A52
2	1	CN = Microsoft RSA TLS CA 02 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	C = IE, O = Baltimore, OU = CyberTrust, CN = Baltimore CyberTrust Root	0FA74722C53D88C80F589EFB1F9D4A3A	RSA	SHA-256	Jul 21 23:00:00 2020 GMT	Oct 8 07:00:00 2024 GMT		TLS Web Server Authentication, TLS Web Client Authentication	FF2F7FE106F438F32DED258D98C2FE0EF66CFCFA	05E4005DB0C382F3BD66B47729E90115776018F6F7B287E9A52CED710D258346

MICROSOFT DSR MANAGEMENT'S ASSERTION

Microsoft Corporation Digital Security & Resilience ("Microsoft DSR") operates the Certification Authority ("CA") services as enumerated in [Attachment A](#), and provides CA services.

The management of Microsoft DSR is responsible for establishing and maintaining effective controls over its CA operations, including its network and certificate security system controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to Microsoft DSR's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Microsoft DSR management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in providing its SSL CA services in United States of America, and in Ireland, Microsoft DSR has:

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

throughout the period July 1, 2023 to June 30, 2024, based on the [WebTrust Principles and Criteria for Certification Authorities – Network Security, v1.0](#).

Microsoft Corporation Digital Security & Resilience ("Microsoft DSR")
September 03, 2024

ATTACHMENT A

LIST OF IN SCOPE CAs

DV SSL Issuing CAs
1. Microsoft RSA TLS CA 01 2. Microsoft RSA TLS CA 02