

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 the United States of America, and in Ireland for its CAs as enumerated in [Attachment A](#), Microsoft DSR has:

- disclosed its TLS certificate lifecycle management business practices in its applicable version of Certificate Policy/Certification Practice Statement ("CP/CPS") as enumerated on [Attachment B](#), including its commitment to provide TLS certificates in conformity with the CA/Browser Forum Requirements on the Microsoft DSR [website](#), and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and TLS certificates it manages is established and protected throughout their lifecycles; and
 - TLS subscriber information is properly authenticated (for the registration activities performed by Microsoft DSR)
- maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data is restricted to authorized individuals;
 - the continuity of key and certificate management operations is maintained; and
 - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

throughout the period July 1, 2024 to November 8, 2024, based on the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, v2.8](#).

The CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted TLS Server Certificates require the CA to operate controls to adhere to the Network and Certificate System Security Requirements. The WebTrust Principles and Criteria for Certification Authorities - Network Security address this requirement and are reported on under separate cover.

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 – SSL Baseline with Network Security, v2.8.

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 examination 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.

Non-occurrences of controls

During the period of July 1, 2024 to November 8, 2024, there were no occurrences of controls related to the following criteria:

- 2.1 – Key Generation Ceremonies
- 2.4 – Verification Practices
- 2.5 – Certificate Review and Stat Checking

Therefore, no tests of the effectiveness of those controls related to those criteria were performed for the period July 1, 2024 to November 8, 2024.

Emphasis of matter

The period end date of November 8, 2024 is due to the decommissioning of Microsoft DSR's Certification Authority ("CA") operations in the United States of America and in Ireland.

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 services 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 – TLS Baseline 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
February 3, 2025

ATTACHMENT A

LIST OF IN SCOPE CAs

DV TLS 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	04EEEE8E50B4775B3C24797262917EE50002EC4C75B56CDF3EE1C18CFA5BA52
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	FF2F7FE106F438F32DED258D98C2FE0EF66CF6CFA	05E4005DB0C382F3BD66B47729E9011577601BF6F7B287E9A52CED710D258346

ATTACHMENT B

LIST OF MICROSOFT DSR'S CERTIFICATION PRACTICE STATEMENTS

CP/CPS Name	Version	Date
Microsoft DSR Certificate Policy/ Certification Practice Statement	2.14	March 15, 2024

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 TLS CA services.

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

- disclosed its TLS certificate lifecycle management business practices in its applicable version of Certificate Policy/Certification Practice Statements ("CP/CPS") as enumerated on [Attachment B](#), including its commitment to provide TLS certificates in conformity with the CA/Browser Forum Requirements on the Microsoft DSR [website](#), and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and TLS certificates it manages is established and protected throughout their lifecycles; and
 - TLS subscriber information is properly authenticated (for the registration activities performed by Microsoft DSR)
- maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data is restricted to authorized individuals;
 - the continuity of key and certificate management operations is maintained; and
 - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

throughout the period July 1, 2024 to November 8, 2024, based on the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, v2.8](#).

Microsoft Corporation Digital Security & Resilience ("Microsoft DSR")
February 3, 2025

ATTACHMENT A

LIST OF IN SCOPE CAs

DV TLS Issuing CAs

- | |
|---|
| <ol style="list-style-type: none">1. Microsoft RSA TLS CA 012. Microsoft RSA TLS CA 02 |
|---|

ATTACHMENT B

LIST OF MICROSOFT DSR'S CERTIFICATION PRACTICE STATEMENTS

CP/CPS Name	Version	Date
Microsoft DSR Certificate Policy/ Certification Practice Statement	2.14	March 15, 2024