Deloitte & Touche LLP
1015 2nd Ave, Suite 500
Seattle, WA 98104
Tel: +1 206 716 7000
Fax: +1 206 965 7000
www.deloitte.com

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 business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of its Certificate Policy/Certification Practice Statement ("CP/CPS") as enumerated in Attachment B
- maintained effective controls to provide reasonable assurance that
  - Microsoft DSR provides its services in accordance with its CP/CPS
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles; and
  - subscriber information is properly authenticated (for the registration activities performed by Microsoft DSR); and
- 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, 2023 to June 30, 2024 (the "Period") based on the WebTrust Principles and Criteria for Certification Authorities, v2.2.2.

Microsoft DSR does not escrow or archive its CA keys, does not provide subscriber key generation services, subscriber key storage and recovery services, or integrated circuit card lifecycle management for subscribers, does not provide certificate suspension services, and does not provide third-party subordinate CA certificate lifecycle management. Accordingly, our examinations did not extend to controls that would address those criteria.

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, v2.2.2.

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*. This standard requires that we plan and perform our 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.

Practitioner's opinion

In our opinion, Microsoft DSR 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 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	04EEEA8E50B4775B3C247972629 17EE50002EC4C75B56CDF3EE1C18CFCA5BA52
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	05E4005DB0C382F3BD66B47729E9011577601BF6F7B287E9A52CED710D258346

ATTACHMENT B

LIST OF MICROSOFT DSR CERTIFICATE POLICY/CERTIFICATION PRACTICE STATEMENTS

CP/CPS Name	Version	Date
Microsoft DSR Certificate Policy/ Certification Practice Statement	2.14	March 15, 2024
Microsoft DSR Certificate Policy/ Certification Practice Statement	2.13	August 21, 2023
Microsoft DSR Certificate Policy/ Certification Practice Statement	2.12	February 14, 2023

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

MICROSOFT DSR MANAGEMENT'S ASSERTION

Microsoft Corporation Digital Security & Resilience Public Key Infrastructure ("Microsoft DSR") operates the Certification Authority ("CA") services as enumerated in Attachment A, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation

The management of Microsoft DSR is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, and certificate lifecycle management 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 CA 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 Microsoft DSR management's opinion, in providing its CA services in the United States of America and in Ireland, Microsoft DSR has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in the applicable versions of its Certificate Policy/Certification Practice Statement ("CP/CPS") as enumerated in Attachment B

- maintained effective controls to provide reasonable assurance that
    - Microsoft DSR provides its services in accordance with its CP/CPS

- maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
    - 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, 2023 to June 30, 2024 based on the WebTrust Principles and Criteria for Certification Authorities, v2.2.2, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)

CA Business Practices Management

- Certification Practice Statement Management

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security

- Operations Management
- System Access Management
- System Development, Maintenance, and Change Management
- Disaster Recovery, Backups, and Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Transportation
- CA Key Migration

Subscriber Key Lifecycle Management Controls

- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Microsoft DSR does not escrow or archive its CA keys, does not provide subscriber key generation services, subscriber key storage and recovery services, or integrated circuit card lifecycle management for subscribers, does not provide certificate suspension services, and does not provide third-party subordinate CA certificate lifecycle management. Accordingly, our examinations did not extend to controls that would address those criteria.

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

ATTACHMENT B

LIST OF MICROSOFT DSR CERTIFICATE POLICY/CERTIFICATION PRACTICE STATEMENTS

CP/CPS Name	Version	Date
Microsoft DSR Certificate Policy/ Certification Practice Statement	2.14	March 15, 2024
Microsoft DSR Certificate Policy/ Certification Practice Statement	2.13	August 21, 2023
Microsoft DSR Certificate Policy/ Certification Practice Statement	2.12	February 14, 2023