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 Public Key Infrastructure Services ("MS PKI Services"):

Scope

We have examined MS PKI Services management's assertion that for its Certification Authority ("CA") operations in the United States of America, and in Ireland, for CAs as enumerated in Attachment A, MS PKI Services 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 May 1, 2024 to April 30, 2025 based on the WebTrust Principles and Criteria for Certification Authorities – Network Security, v1.7.

There are other CA hierarchies and PKI operations across Microsoft that are not managed by MS PKI services. These CA hierarchies and PKI operations are not in the scope of this examination, and this opinion does not extend to these services.

Certification authority's responsibilities

MS PKI Services' 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, v1.7.

Practitioner's responsibilities

Our responsibility is to express an opinion, 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 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.

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 MS PKI Services 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.

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 unauthorised 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.

Emphasis of matters

Without modifying our opinion, we noted the following other matters during our procedures:

	Matter topic	Matter description
1	**Vulnerability Management Exception Tracking**	As publicly disclosed in Bugzilla 1906028, the auditors issued a qualified opinion for the audit period ended March 31, 2024, citing deficiencies in the documentation of vulnerability mitigation plans and timelines within the Microsoft PKI Services Vulnerability Management process. As of August 6, 2024, the CA remediated the observation noted by implementing controls to provide reasonable assurance that it performs the vulnerability correction process within ninety-six (96) hours of the discovery of a critical vulnerability not previously addressed by the CA's vulnerability correction process. For the period from August 7, 2024, to April 30, 2025, the CA maintained sufficient controls to provide reasonable assurance that the Network and Certificate System Security Requirements for Principle 4 Criterion 4.6 as set forth by the CA/Browser Forum were achieved. The Bugzilla ticket was RESOLVED on August 15, 2024. We examined that MS PKI Services maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements for Principle 4 Criterion 4.6 as set forth by the CA/Browser Forum throughout the period May 1, 2024 to October 31, 2024 based on the WebTrust Principles and Criteria for Certification Authorities – Network Security, v1.7, and provided an independent accountant's report with our opinion on February 12, 2025.

Opinion

In our opinion MS PKI Services' assertion, as referred to above, is fairly stated, in all material respects.

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

Use of the WebTrust seal

MS PKI Services' 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
July 16, 2025

ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs
1. Microsoft Identity Verification Root Certificate Authority 2020
Intermediate CAs
2. Microsoft ID Verified Code Signing PCA 2021 3. Microsoft ID Verified CS AOC CA 01 4. Microsoft ID Verified CS AOC CA 02 5. Microsoft ID Verified CS EOC CA 01 6. Microsoft ID Verified CS EOC CA 02
Timestamp Authority CA
7. Microsoft Public RSA Timestamping CA 2020

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	C=US O=Microsoft Corporation CN=Microsoft Identity Verification Root Certificate Authority 2020	C=US O=Microsoft Corporation CN=Microsoft Identity Verification Root Certificate Authority 2020	5498D2D1D45B1995481379C811C08799	RSA	sha384RSA	4/16/2020 18:36	4/16/2045 18:44	N/A		C87ED26A852A1BCA1998040727CF50104F68A8A2	5367F20C7ADE0E2BCA790915056D086B720C33C1FA2A2661ACF787E3292E1270
2	1	C=US O=Microsoft Corporation CN=Microsoft ID Verified Code Signing PCA 2021	C=US O=Microsoft Corporation CN=Microsoft Identity Verification Root Certificate Authority 2020	330000000787A334A37BA58E1C000000000007	RSA	sha384RSA	4/1/2021 20:05	4/1/2036 20:15	N/A		d94129b00f0f636cef69d7f5cd299ea4486a30e6	3D29798CC5D3F0644A7E0DC9CB1CADE523EA5EC83B335109B605BFEAA7D5F5C1
3	1	C=US O=Microsoft Corporation CN=Microsoft ID Verified CS AOC CA 01	C=US O=Microsoft Corporation CN=Microsoft ID Verified Code Signing PCA 2021	3300000007378C5BA1D95B8CD4000000000007	RSA	sha384RSA	4/13/2021 17:31	4/13/2026 17:31	N/A		e883c433d7dc9f0c9c769a0aa6d4df87a65e58ee	7EE1F718CAE6B4D25D10115A367D84B7704E06BD6F8B498825FD42C852574BE9
4	1	C=US O=Microsoft Corporation CN=Microsoft ID Verified CS AOC CA 02	C=US O=Microsoft Corporation CN=Microsoft ID Verified Code Signing PCA 2021	330000000496504BD2DBEECB88000000000004	RSA	sha384RSA	4/13/2021 17:31	4/13/2026 17:31	N/A		244599a177902a7cc3ca83b06e6416842af82c67	E82D27596C5DDF9F11E8B6981F5D018211BF2580F0619E5954BAD400175F38D0
5	1	C=US O=Microsoft Corporation CN=Microsoft ID Verified CS EOC CA 01	C=US O=Microsoft Corporation CN=Microsoft ID Verified Code Signing PCA 2021	330000000064A1AFACF05616A74000000000006	RSA	sha384RSA	4/13/2021 17:31	4/13/2026 17:31	N/A		769c367413d1907d615fb302eb80f4994ba53e85	2FAA1C92228D5A05E07BAECFAA365F90A9B2F2DD846B014AE95880BAC3A976BB
6	1	C=US O=Microsoft Corporation CN=Microsoft ID Verified CS EOC CA 02	C=US O=Microsoft Corporation CN=Microsoft ID Verified Code Signing PCA 2021	3300000005FB7A5C321361DF5D000000000005	RSA	sha384RSA	4/13/2021 17:31	4/13/2026 17:31	N/A		659f51ce85687f2f8a4588aadda731bb1e0d005e	B96CCAB201048A0AC2BA07AEA08D6DBEEA1688F55380A369B14A7BE11AEF828D
7	1	C=US O=Microsoft Corporation CN=Microsoft Public RSA Timestamping CA 2020	C=US O=Microsoft Corporation CN=Microsoft Identity Verification Root Certificate Authority 2020	3300000005E5CF0FFF662EC987000000000005	RSA	sha384RSA	11/19/2020 20:32	11/19/2035 20:42	N/A	Time Stamping (1.3.6.1.5.5.7.3.8)	6B69283A352F486340CF7BD8AF49E93ED93DDB21	36E731CFA9BFD69DAFB643809F6DEC500902F7197DAEAAD86EA0159A2268A2B8

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

MICROSOFT PUBLIC KEY INFRASTRUCTURE SERVICES MANAGEMENT'S ASSERTION

Microsoft Public Key Infrastructure Services ("MS PKI Services") operates the Certification Authority ("CA") services as enumerated in Attachment A.

The management of MS PKI Services 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 MS PKI Services' CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

MS PKI Services management has assessed its controls over its CA services. Based on that assessment, in providing its Certification Authority (CA) services at United States of America and Ireland, MS PKI Services 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 May 1, 2024 to April 30, 2025 based on the WebTrust Principles and Criteria for Certification Authorities – Network Security, v1.7.

Microsoft Public Key Infrastructure Services
July 16, 2025

ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs
1. Microsoft Identity Verification Root Certificate Authority 2020
Intermediate CAs
2. Microsoft ID Verified Code Signing PCA 2021 3. Microsoft ID Verified CS AOC CA 01 4. Microsoft ID Verified CS AOC CA 02 5. Microsoft ID Verified CS EOC CA 01 6. Microsoft ID Verified CS EOC CA 02
Timestamp Authority CA
7. Microsoft Public RSA Timestamping CA 2020