

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 at locations enumerated in [Attachment B](#), 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, 2025 to April 30, 2026 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.

While the MS PKI Services management's [assertion](#) enumerates matters disclosed publicly on Mozilla's Bugzilla reporting system throughout the period May 1, 2025 to April 30, 2026, we noted that those matters were not relevant to the CAs enumerated in [Attachment A](#) and applicable to the [WebTrust Principles and Criteria for Certification Authorities – Network Security, v1.7](#).

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.

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.

A handwritten signature in black ink that reads "Deloitte & Touche LLP". The script is cursive and fluid, with the letters connected. The "D" is large and loops around, and the "LLP" is written in a slightly more upright but still cursive style.

Deloitte & Touche LLP
July 28, 2026

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
7.	Microsoft ID Verified CS AOC CA 03
8.	Microsoft ID Verified CS AOC CA 04
9.	Microsoft ID Verified CS EOC CA 03
10.	Microsoft ID Verified CS EOC CA 04
Timestamp Authority CA	
11.	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	C87ED26A852A18CA1998040727CF50104F68A8A2	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	3D29798CC5D3F0644A7E0DC9CB1CADE523EA5EC83B335109B605BFEEA7D5F5C1	
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	330000000496504BD2DBEEC88000000000004	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	33000000064A1AFACF05616A74000000000006	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	3300000005FB7A5C321361DF5D0000000000005	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 ID Verified CS AOC CA 03	C=US O=Microsoft Corporation CN=Microsoft ID Verified Code Signing PCA 2021	33000000180DEB9155A98A0098000000000018	RSA	sha384RSA	3/26/2026 18:11	3/26/2031 18:11	N/A	a4430c7f7f65aa585e73e8d280f0c17a2456970c6	ACAA07D57D4274B290D86C156AA0D6C5633E3CD92D43751E6A0F797C5B2DFF4D	
8	1	C=US O=Microsoft Corporation CN=Microsoft ID Verified CS AOC CA 04	C=US O=Microsoft Corporation CN=Microsoft ID Verified Code Signing PCA 2021	330000001631928D9202657B9A00000000000016	RSA	sha384RSA	3/26/2026 18:11	3/26/2031 18:11	N/A	6b2541defb6b7cfd18800a2d7f8f765daa733db8	15CEF5F63CA6D1F022B293E92C61C0059C49BB92EECD8CDE3A125D3C6356D94F	
9	1	C=US O=Microsoft Corporation CN=Microsoft ID Verified CS EOC CA 03	C=US O=Microsoft Corporation CN=Microsoft ID Verified Code Signing PCA 2021	3300000015053E6E198E9329D90000000000015	RSA	sha384RSA	3/26/2026 18:11	3/26/2031 18:11	N/A	6b5ea534c305c5624a215a8eab736062d4ac6385	BFF5C1A54B421E0CC12372F221FA56E6F1B0305A9C071A2AF1BF45893D2A4623	
10	1	C=US O=Microsoft Corporation CN=Microsoft ID Verified CS EOC CA 04	C=US O=Microsoft Corporation CN=Microsoft ID Verified Code Signing PCA 2021	33000000172745090B8B87AFC60000000000017	RSA	sha384RSA	3/26/2026 18:11	3/26/2031 18:11	N/A	9af15477750c87163746a0acde79f9f47fc178e9	BC309555FA42C56388EEBF87117695C6BAE89E4BA19C03CB721979A563A60929	
11	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	3300000005E5CF0FF662EC9870000000000005	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	36E731CFA9BFD69DAFB643809F6DEC500902F7197DAEAD86EA0159A2268A2B8	

ATTACHMENT B

LIST OF MS PKI SERVICES' LOCATIONS IN-SCOPE

#	Location Name	Location Type	Location	In-Scope for Physical and Environmental Control Testing
1	Corporate headquarters and office spaces	Main office	United States of America	No
2	Online CA hosting 1	Datacenter 1	United States of America	Yes
3	Online CA hosting 2	Datacenter 2	Ireland	Yes
4	Offline CA hosting 1	Primary offline CA facility	United States of America	Yes
5	Offline CA hosting 2	Disaster recovery / secondary offline CA facility	United States of America	Yes
6	Secure storage 1	Secure storage for online CAs and offline CAs	United States of America	Yes
7	Secure storage 2	Cold storage for online and offline CAs	United States of America	Yes
8	Secure storage 3	Disaster recovery / secondary storage for offline CAs	United States of America	Yes
9	Secure storage 4	Third-party cold storage for offline CAs	United States of America	Yes
10	Secure storage 5	Secure storage for online CAs and offline CAs	Ireland	Yes

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 locations enumerated in [Attachment B](#), 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, 2025 to April 30, 2026 based on the [WebTrust Principles and Criteria for Certification Authorities – Network Security, v1.7](#).

MS PKI Services has disclosed the following matters publicly on Mozilla's Bugzilla reporting system.

Sr.	Bugzilla ID	Bugzilla Title	Created On	Resolved On	Status
1	1962829	Microsoft PKI Services: Policy document bug	April 28, 2025	April 25, 2026	Resolved
2	1962830	Microsoft PKI Services: Subscriber certificate change made that was not compliant with CPS	April 28, 2025	June 20, 2025	Resolved
3	1965612	Microsoft PKI Services: Failure to Revoke in 5 Days for 1962829	May 9, 2025	May 4, 2026	Resolved
4	1970968	Microsoft PKI Services: Incorrect Revocation Reason Code	June 6, 2025	July 8, 2025	Resolved
5	1974592	Microsoft PKI Services: Pre-Sign Linting Validation did not occur in ICA creation	June 28, 2025	August 30, 2025	Resolved
6	1979475	Microsoft PKI Services: End Entity Certificate Mis-issuance against CPS (BasicConstraints)	July 28, 2025	January 20, 2026	Resolved
7	1990801	Microsoft: improper disclosure of CRL	September 26, 2025	November 3, 2025	Resolved
8	1999850	Microsoft PKI Services: OSCP Non-Compliance	November 13, 2025	July 1, 2026	Resolved
9	2007221	Microsoft PKI Services: Improper Disclosure of CRL	December 19, 2025	March 2, 2026	Resolved
10	2008847	Microsoft PKI Services: Sample Site Certificates expired	January 7, 2026	February 16, 2026	Resolved
11	2009539	Microsoft PKI Services: Improper Disclosure of CRLs – IDP – Existing CAs	January 10, 2026	February 16, 2026	Resolved
12	2009541	Microsoft PKI Services: Failure to report within 72 hrs - Sample Site Certs Expired	January 10, 2026	February 11, 2026	Resolved
13	2009542	Microsoft PKI Services: Improper Disclosure of CRLs – IDP – New CAs	January 10, 2026	February 16, 2026	Resolved
14	2009543	Microsoft PKI Services: Improper Disclosure of CRLs – Does Not Match CA Subject	January 10, 2026	February 9, 2026	Resolved
15	2009545	Microsoft PKI Services: Improper Disclosure of CRLs – Protocol Scheme	January 10, 2026	February 11, 2026	Resolved

Sr.	Bugzilla ID	Bugzilla Title	Created On	Resolved On	Status
16	<u>2021175</u>	Microsoft PKI Services: Failure to update action item status within 3 days	March 5, 2026	April 3, 2026	Resolved
17	<u>2026452</u>	Microsoft PKI Services: Failure to publish Full Incident Report for Bugzilla 2021175 within 14 days	March 26, 2026	April 22, 2026	Resolved
18	<u>2026453</u>	Microsoft PKI Services: Failure to report Bugzilla 2026452 within 72 hrs	March 26, 2026	April 22, 2026	Resolved
19	<u>2034251</u>	Microsoft PKI Services: Failure to Update Full Incident Report within 14 days of discovering new root cause	April 23, 2026	May 13, 2026	Resolved

Microsoft Public Key Infrastructure Services
July 28, 2026

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
7.	Microsoft ID Verified CS AOC CA 03
8.	Microsoft ID Verified CS AOC CA 04
9.	Microsoft ID Verified CS EOC CA 03
10.	Microsoft ID Verified CS EOC CA 04
Timestamp Authority CA	
11.	Microsoft Public RSA Timestamping CA 2020

ATTACHMENT B

LIST OF MS PKI SERVICES' LOCATIONS IN-SCOPE

#	Location Name	Location Type	Location	In-Scope for Physical and Environmental Control Testing
1	Corporate headquarters and office spaces	Main office	United States of America	No
2	Online CA hosting 1	Datacenter 1	United States of America	Yes
3	Online CA hosting 2	Datacenter 2	Ireland	Yes
4	Offline CA hosting 1	Primary offline CA facility	United States of America	Yes
5	Offline CA hosting 2	Disaster recovery / secondary offline CA facility	United States of America	Yes
6	Secure storage 1	Secure storage for online CAs and offline CAs	United States of America	Yes
7	Secure storage 2	Cold storage for online and offline CAs	United States of America	Yes
8	Secure storage 3	Disaster recovery / secondary storage for offline CAs	United States of America	Yes
9	Secure storage 4	Third-party cold storage for offline CAs	United States of America	Yes
10	Secure storage 5	Secure storage for online CAs and offline CAs	Ireland	Yes