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 at locations enumerated in Attachment C, for its CAs as enumerated in Attachment A, MS PKI Services has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of its Certificate Policies and Certification Practice Statements as enumerated in Attachment B
- maintained effective controls to provide reasonable assurance that
  - MS PKI Services' Certification Practice Statements are consistent with its Certificate Policies; and
  - MS PKI Services provides its services in accordance with its Certificate Policies and Certification Practice Statements
- 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 MS PKI Services); and
  - subordinate CA certificate requests are accurate, authenticated, and approved
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorised individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity.

throughout the period May 1, 2025 to April 30, 2026 based on the WebTrust Principles and Criteria for Certification Authorities, v2.2.2.

MS PKI Services does not escrow its CA keys, does not provide subscriber key generation services, subscriber key storage and recovery services, or integrated circuit card lifecycle management for subscribers, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.

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, v2.2.2.

Practitioner's responsibilities

Our responsibility is to express an opinion on MS PKI Services 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.

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	**OCSP response formatting and infrastructure rollback issue**	As publicly disclosed in Bugzilla 1999850, Microsoft PKI Services identified an issue in its new OCSP infrastructure where responses included fractional seconds in the 'thisUpdate', 'nextUpdate', and 'producedAt' fields, causing TLS handshake failures for some relying parties and creating inconsistency with RFC 5280. As a result, OCSP traffic was moved back to the legacy responder infrastructure while Microsoft works to remediate the issue and resume migration to the new environment. The Bugzilla ticket was closed as RESOLVED on July 1, 2026.

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 have only noted those matters relevant to the CAs enumerated in Attachment A and applicable to the WebTrust Principles and Criteria for Certification Authorities, v2.2.2.

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 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 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 28, 2026

ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs
1. Microsoft ECC Root Certificate Authority 2017
2. Microsoft RSA Root Certificate Authority 2017
3. Microsoft TLS RSA Root G2
4. Microsoft TLS ECC Root G2
Cross-signed CA Certificates
3. Microsoft TLS RSA Root G2
4. Microsoft TLS ECC Root G2
5. Microsoft Azure ECC TLS Issuing CA 01
6. Microsoft Azure ECC TLS Issuing CA 02
7. Microsoft Azure ECC TLS Issuing CA 05
8. Microsoft Azure ECC TLS Issuing CA 06
9. Microsoft Azure ECC TLS Issuing CA 03
10. Microsoft Azure ECC TLS Issuing CA 04
11. Microsoft Azure ECC TLS Issuing CA 07
12. Microsoft Azure ECC TLS Issuing CA 08
13. Microsoft Azure RSA TLS Issuing CA 03
14. Microsoft Azure RSA TLS Issuing CA 04
15. Microsoft Azure RSA TLS Issuing CA 07
16. Microsoft Azure RSA TLS Issuing CA 08
17. Microsoft Azure TLS Issuing CA 01
18. Microsoft Azure TLS Issuing CA 02
19. Microsoft Azure TLS Issuing CA 05
20. Microsoft Azure TLS Issuing CA 06
21. Microsoft TLS G1 ECC CA 01
22. Microsoft TLS G1 ECC CA 02
23. Microsoft TLS G1 RSA CA 01
24. Microsoft TLS G1 RSA CA 02
25. Microsoft TLS G1 RSA CA 03
26. Microsoft TLS G1 RSA CA 04
Intermediate CA Certificates
27. Microsoft ECC TLS Issuing AOC CA 01
28. Microsoft ECC TLS Issuing AOC CA 02
29. Microsoft ECC TLS Issuing EOC CA 01
30. Microsoft ECC TLS Issuing EOC CA 02
31. Microsoft RSA TLS Issuing AOC CA 01
32. Microsoft RSA TLS Issuing AOC CA 02
33. Microsoft RSA TLS Issuing EOC CA 01
34. Microsoft RSA TLS Issuing EOC CA 02
35. Microsoft TLS G2 RSA CA OCSP 02
36. Microsoft TLS G2 RSA CA OCSP 04
37. Microsoft TLS G2 RSA CA OCSP 06
38. Microsoft TLS G2 RSA CA OCSP 08
39. Microsoft TLS G2 RSA CA OCSP 10
40. Microsoft TLS G2 RSA CA OCSP 12
41. Microsoft TLS G2 RSA CA OCSP 14
42. Microsoft TLS G2 RSA CA OCSP 16
43. Microsoft TLS G2 ECC CA OCSP 02
44. Microsoft TLS G2 ECC CA OCSP 04
45. Microsoft TLS G2 ECC CA OCSP 06
46. Microsoft TLS G2 ECC CA OCSP 08

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 ECC Root Certificate Authority 2017	C=US O=Microsoft Corporation CN=Microsoft ECC Root Certificate Authority 2017	66F23DAF87DE8BB14AEA0C573101C2EC	ECC	sha384ECDSA	12/18/2019 23:06	7/18/2042 23:16	N/A		C8CB997270520CF8E6BEB20457292ACF4210ED35	358DF39D764AF9E1B766E9C972DF352EE15CFAC227AF6AD1D70E8E4A6EDCBA02
1	2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Root Certificate Authority 2017	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Root Certificate Authority 2017	71767E8D58E4FC9649C63EFBCF3ABDA7	ECC	sha384ECDSA	7/26/2017s 22:22	7/26/2042 22:31	N/A		C8CB997270520CF8E6BEB20457292ACF4210ED35	FEA1884AB3AEA6D0DBEDBE4B9CD9FEC8655116300A86A856488FC488BB4B44D2
2	1	C=US O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	C=US O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	1ED397095FD8B4B347701EAABE7F45B3	RSA	sha384RSA	12/18/2019 22:51	7/18/2042 23:00	N/A		09CB597F86B2708F1AC339E3C0D9E9BFBB4DB223	C741F70F4B2A8D88BF2E71C14122EF53EF10EBA0CFA5E64CFA20F418853073E0
2	2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	29C87039F4DBFDB94DBCDA6CA792836B	RSA	sha384RSA	7/26/2017 22:07	7/26/2042 22:15	N/A		09CB597F86B2708F1AC339E3C0D9E9BFBB4DB223	ECDD47B5ACBFA328211E1BFF54ADEAC95E6991E3C1D50E27B527E903208040A1
3	1	C=US, O=Microsoft Corporation, CN=Microsoft TLS RSA Root G2	C=US, O=Microsoft Corporation, CN=Microsoft TLS RSA Root G2	6486E3B269180FBF4040392E2E534B9B	RSA	sha384RSA	4/10/2025 18:36	4/10/2040 18:43	N/A		DE918648B7A1315931F14B5F07A9DC8879DAA876	6A170583DB584151E1C454EECA2A64CC5D8E484A5BD1156E720B44586546EE9E5
3	2	C=US, O=Microsoft Corporation, CN=Microsoft TLS RSA Root G2	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root G2	0B0C6B2C466917B04773C647D4AFC0C8	RSA	sha384RSA	5/21/2025 00:00	6/19/2029 23:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	DE918648B7A1315931F14B5F07A9DC8879DAA876	DDCD1E8A20638D4AAFF7201BB1D56452ACD2C759F1686BDC38F73DD15732BDC2
4	1	C=US, O=Microsoft Corporation, CN=Microsoft TLS ECC Root G2	C=US, O=Microsoft Corporation, CN=Microsoft TLS ECC Root G2	72E2022BC5B2C1B04D25056E62E27679	ECC	sha384ECDSA	4/10/2025 20:52	4/10/2040 20:58	N/A		6FAB7EDAFF974372EC3B6777DE82613588474285	87755CFE88BDB0D1099DCDED3EAE114BA976E664B3248EE3DC649E357F17E8A7
4	2	C=US, O=Microsoft Corporation, CN=Microsoft TLS ECC Root G2	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root G3	08D3C6D001F26CB5A23F0C7D6A73FFB6	ECC	sha384ECDSA	5/21/2025 00:00	6/19/2029 23:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	6FAB7EDAFF974372EC3B6777DE82613588474285	61799E3594F6FA6C9F619031E4A3C9F643FDA38C083704A5075E5709A21B1AB7
5	1	C=US O=Microsoft Corporation CN=Microsoft Azure ECC TLS Issuing CA 01	C=US O=DigiCert Inc OU=www.digicert.com CN=DigiCert Global Root G3	09DC42A5F574FF3A389EE06D5D4DE440	ECC	sha384ECDSA	8/12/2020 0:00	6/27/2024 23:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	AAFD300DD7A2D5EF8A7A7731AA66A6C26C11BB6F	949D6B4B761CA134AD3E7A8571186F580EE887F2C6B568B5140F4157F98D68DD
5	2	C=US O=Microsoft Corporation CN=Microsoft Azure ECC TLS Issuing CA 01	C=US O=Microsoft Corporation CN=Microsoft ECC Root Certificate Authority 2017	330000001AA9564F44321C54B900000000001A	ECC	sha384ECDSA	1/17/2020 20:28	6/27/2024 20:28	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	AAFD300DD7A2D5EF8A7A7731AA66A6C26C11BB6F	2CAEFBB55E70DF5A8985FE9BC10DD56A40C3DEDAB3DA1530A29682015C5B7C66
6	1	C=US O=Microsoft Corporation CN=Microsoft Azure ECC TLS Issuing CA 02	C=US O=DigiCert Inc OU=www.digicert.com CN=DigiCert Global Root G3	0E8DBE5EA610E6CBB569C736F6D7004B	ECC	sha384ECDSA	8/12/2020 0:00	6/27/2024 23:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	9DE50E7737479E0933D990BE2A09C2127F4ED2A3	9C64A9A43E990E98FBCE8317B2D4C1C07FFE6E032DA8BB6D60A696E2FF038F1F
6	2	C=US O=Microsoft Corporation CN=Microsoft Azure ECC TLS Issuing CA 02	C=US O=Microsoft Corporation CN=Microsoft ECC Root Certificate Authority 2017	330000001B498D6736ED5612C2000000000001B	ECC	sha384ECDSA	1/17/2020 20:28	6/27/2024 20:28	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	9DE50E7737479E0933D990BE2A09C2127F4ED2A3	4EC439672A443401A66E27947CC3B5897F132B667F712CC1A37018A3CC85B16A
7	1	C=US O=Microsoft Corporation CN=Microsoft Azure ECC TLS Issuing CA 05	C=US O=DigiCert Inc OU=www.digicert.com CN=DigiCert Global Root G3	0CE59C30FD7A83532E2D0146B332F965	ECC	sha384ECDSA	8/12/2020 0:00	6/27/2024 23:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	55DFEE1E27ACF29E2B9E8039357956473ACEB310	003F71DC4820216575FC5AACFE3B1AEB76F72AEA5B8E8FCEFC80B9F517A4A612
7	2	C=US O=Microsoft Corporation CN=Microsoft Azure ECC TLS Issuing CA 05	C=US O=Microsoft Corporation CN=Microsoft ECC Root Certificate Authority 2017	330000001CC0D2A3CD78CF2C1000000000001C	ECC	sha384ECDSA	1/17/2020 20:28	6/27/2024 20:28	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	55DFEE1E27ACF29E2B9E8039357956473ACEB310	624D5576A652B2130768BFE84B965EEFFFD91603D25CD5F7155A7DC2789DAC38
8	1	C=US O=Microsoft Corporation CN=Microsoft Azure ECC TLS Issuing CA 06	C=US O=DigiCert Inc OU=www.digicert.com CN=DigiCert Global Root G3	066E79CD7624C63130C77ABEB6A8BB94	ECC	sha384ECDSA	8/12/2020 0:00	6/27/2024 23:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	1FCEC79D64535FB6FC9507AE95263351C127D926	2975BAB51D00D862D0E16EEDEF8306A759C65CD4B9F00DAF50ECDFCB4EC396E4
8	2	C=US O=Microsoft Corporation CN=Microsoft Azure ECC TLS Issuing CA 06	C=US O=Microsoft Corporation CN=Microsoft ECC Root Certificate Authority 2017	330000001D0913C309DA3F05A6000000000001D	ECC	sha384ECDSA	1/17/2020 20:28	6/27/2024 20:28	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	1FCEC79D64535FB6FC9507AE95263351C127D926	151A3E5969C6616EB637A8722B174CFD95387AACE78D57C3BD23F0CB3008186A
9	1	C=US O=Microsoft Corporation CN=Microsoft Azure ECC TLS Issuing CA 03	C=US O=Microsoft Corporation CN=Microsoft ECC Root Certificate Authority 2017	330000003322A2579B5E698BCC000000000033	ECC	sha384ECDSA	5/25/2023 23:47	5/25/2028 23:47	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	72E096A151EA300C58B5F519AB9A7CCD9755102E	2EC9A5BA68B60F81E5F8662F7645743CCE1EDCE06AF686C775431F7BBB69ABD4
9	2	C = US O = Microsoft Corporation CN = Microsoft Azure ECC TLS Issuing CA 03	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G3	01529EE8368F0B5D72BA433E2D8EA62D	ECC	sha384ECDSA	6/7/2023 17:00	8/25/2026 16:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	72E096A151EA300C58B5F519AB9A7CCD9755102E	BBD27139C5302C63D903F570F173AD4DC06C974B9EBE292C90FFCCAB5D6FA54E
9	3	C = US O = Microsoft Corporation CN = Microsoft Azure ECC TLS Issuing CA 03	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G3	0E001F888F7EB98A8EFCFBAC8D22F173	ECC	sha384ECDSA	6/1/2023 00:00	8/25/2026 23:59	6/6/2023 17:02	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	72E096A151EA300C58B5F519AB9A7CCD9755102E	AF790CAFCD0E9AEADCB8D535612952B2D660DAE9AA0C709467AD1BB913C5E0B7
10	1	C=US O=Microsoft Corporation CN=Microsoft Azure ECC TLS Issuing CA 04	C=US O=Microsoft Corporation CN=Microsoft ECC Root Certificate Authority 2017	330000003221 64AEDAB61F509D000000000032	ECC	sha384ECDSA	5/25/2023 23:47	5/25/2028 23:47	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	35F1E7113268E6B2C8DA71E670F3E83CB80E071B	4D0F5DA23B099209B048E1871B4BB1C4B4E812E3FA0249BB8D19E0FFA9E91BC
10	2	C=US O=Microsoft Corporation CN=Microsoft Azure ECC TLS Issuing CA 04	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G3	02393D48D702425A7CB41C000B0ED7CA	ECC	sha384ECDSA	6/7/2023 17:00	8/25/2026 16:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	35F1E7113268E6B2C8DA71E670F3E83CB80E071B	7A3AE4F12920D5A8129BE1183FBEC4370EF10B8B3AD41EAE4A58D5385AA94D33
10	3	C=US O=Microsoft Corporation CN=Microsoft Azure ECC TLS Issuing CA 04	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G3	0A06BECD2AB134B6FEF42B867A138EB2	ECC	sha384ECDSA	6/1/2023 00:00	8/25/2026 23:59	6/6/2023 17:03	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	35F1E7113268E6B2C8DA71E670F3E83CB80E071B	FFE11B73AD27C296CD9BEFD0BC4EDE0AB8E2688ECE3A8847A1C85DEC9C530E07
11	1	C=US O=Microsoft Corporation CN=Microsoft Azure ECC TLS Issuing CA 07	C=US O=Microsoft Corporation CN=Microsoft ECC Root Certificate Authority 2017	3300000034C732435DB22A0A2B000000000034	ECC	sha384ECDSA	5/25/2023 23:48	5/25/2028 23:48	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	C35EAC4076C0064DE32B9499306073349829C651	BD3816423553ED993FA44A02F5562470C0CFB0D3B00532E3526A4A3AEC87522F
11	2	C=US O=Microsoft Corporation CN=Microsoft Azure ECC TLS Issuing CA 07	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G3	0F1F157582CDCD33734BDC5FCD941A33	ECC	sha384ECDSA	6/7/2023 17:00	8/25/2026 16:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	C35EAC4076C0064DE32B9499306073349829C651	BE23414A42E74886E7C72A861BA2DDDA0175ED829223D894C5D272651FC0C189
11	3	C=US O=Microsoft Corporation CN=Microsoft Azure ECC TLS Issuing CA 07	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G3	03A9AD57B415ED4F5027FC293FDF9948	ECC	sha384ECDSA	6/1/2023 00:00	8/25/2026 23:59	6/6/2023 17:04	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	C35EAC4076C0064DE32B9499306073349829C651	D59BEE8525BF9AEEFD44E8A61BDC519A558266B8BE09E6CF92C45C6E6E7316AE
12	1	C=US O=Microsoft Corporation CN=Microsoft Azure ECC TLS Issuing CA 08	C=US O=Microsoft Corporation CN=Microsoft ECC Root Certificate Authority 2017	330000003152697984479 8BBB8000000000031	ECC	sha384ECDSA	5/25/2023 23:47	5/25/2028 23:47	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	AD541D035471C62F5ED65B1858CE6E24C5D6A20A	2C99B917B7A068578F7EFB4FB8E60B9CB5A0E73BF300E0E1DC112E5654C5AE52
12	2	C=US O=Microsoft Corporation CN=Microsoft Azure ECC TLS Issuing CA 08	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G3	0EF2E5D83681520255E92C608FBC2FF4	ECC	sha384ECDSA	6/7/2023 17:00	8/25/2026 16:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	AD541D035471C62F5ED65B1858CE6E24C5D6A20A	89AADE767B7BA43F8DDE8E9E74A2FCBBEA40D57155F7E1F2259C88835601FAED
12	3	C=US O=Microsoft Corporation CN=Microsoft Azure ECC TLS Issuing CA 08	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G3	0E9AB506722B783463F10BBB17542230	ECC	sha384ECDSA	6/1/2023 00:00	8/25/2026 23:59	6/6/2023 17:02	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	AD541D035471C62F5ED65B1858CE6E24C5D6A20A	CDAE3E94571D2E9D439A06606E96B0A0EB38299EC01F1D5BB9A748C0C18CC2C3
13	1	C=US O=Microsoft Corporation CN=Microsoft Azure RSA TLS Issuing CA 03	C=US O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	330000003968EA517D8A7E30CE000000000039	RSA	sha384RSA	5/25/2023 23:49	5/25/2028 23:49	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	FE09714055051044D8A48175B89E1AE94A0688C8	3D3F4B440F933FFD269565EDA9E20E8DF863C9CBE3651D3B476C5B4F4AF5CE28
13	2	C=US O=Microsoft Corporation CN=Microsoft Azure RSA TLS Issuing CA 03	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2	05196526449A5E3D1A38748F5DCFEBCC	RSA	sha384RSA	6/7/2023 17:00	8/25/2026 16:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	FE09714055051044D8A48175B89E1AE94A0688C8	9D1BC5D2DD75BF8B64F35E7F919E2546C225BE888C1A8CBE82C0E9579234A7ED

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
13	3	C=US O=Microsoft Corporation CN=Microsoft Azure RSA TLS Issuing CA 03	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2	0D75EDB5BF815E355A7DDCE1870E760F	RSA	sha384RSA	6/1/2023 00:00	8/25/2026 23:59	6/6/2023 16:58	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	FE09714055051044D8A48175B89E1AE94A0688C8	35A2357D1C93E12ADF2109FE4087DC2DE25516E39D5D9F72E85F73C5C680DDC7
14	1	C=US O=Microsoft Corporation CN=Microsoft Azure RSA TLS Issuing CA 04	C=US O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	330000003CD7CB44EE579961D000000000003C	RSA	sha384RSA	5/25/2023 23:49	5/25/2028 23:49	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	3B70D153E976259D60A8CA660FC69BAE6F54166A	FD39FFC48F148354262162A2F55DD46DC2564CFC1499309AD53F09C10981DCCA
14	2	C=US O=Microsoft Corporation CN=Microsoft Azure RSA TLS Issuing CA 04	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2	09F96EC295555F24749EAF1E5DCED49D	RSA	sha384RSA	6/7/2023 17:00	8/25/2026 16:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	3B70D153E976259D60A8CA660FC69BAE6F54166A	33F9731BE910A66DC6ACD07D9D9CA212EE8D0A9A5C78C8BF3E89BB74DF8FB936
14	3	C=US O=Microsoft Corporation CN=Microsoft Azure RSA TLS Issuing CA 04	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2	0FF735DB59DE63193F0FA7079099C96A	RSA	sha384RSA	6/1/2023 00:00	8/25/2026 23:59	6/6/2023 16:59	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	3B70D153E976259D60A8CA660FC69BAE6F54166A	5C6D57933992E9D88B6C43C2666CD8E269439F510B30AA84E35A32832ECA240F
15	1	C=US O=Microsoft Corporation CN=Microsoft Azure RSA TLS Issuing CA 07	C=US O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	330000003BF980B0C837834317000000000003B	RSA	sha384RSA	5/25/2023 23:49	5/25/2028 23:49	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	CE15163BEA02A3A66BDAD92BFDE58C52BE7A50A8	FBB7926A451BADF516BE518614A77E6E325E29819908796D807F59320F918EE2
15	2	C=US O=Microsoft Corporation CN=Microsoft Azure RSA TLS Issuing CA 07	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2	0A43A9509B01352F899579EC7208BA50	RSA	sha384RSA	6/7/2023 17:00	8/25/2026 16:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	CE15163BEA02A3A66BDAD92BFDE58C52BE7A50A8	724247794951C93F3E41711617E95CE143263E3196C345A1DA78F6639749EC03
15	3	C=US O=Microsoft Corporation CN=Microsoft Azure RSA TLS Issuing CA 07	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2	0B9E5E59E54105FE2FF42DEE1C9F9938	RSA	sha384RSA	6/1/2023 00:00	8/25/2026 23:59	6/6/2023 17:00	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	CE15163BEA02A3A66BDAD92BFDE58C52BE7A50A8	54F020151A90182095D4F844448DF4911EA683E7F4283E3EB1FF50FF1D78FD2E
16	1	C=US O=Microsoft Corporation CN=Microsoft Azure RSA TLS Issuing CA 08	C=US O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	330000003A5DC2FFC321C16D9B000000000003A	RSA	sha384RSA	5/25/2023 23:49	5/25/2028 23:49	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	F67E2FBD80A34AB2705BEBDF9A1FD8EDCA618007	CFDD061FCD4CFF3BB9E133264CA7FDE45CA49B70CFAA977AE0DC422B4330A8C1
16	2	C=US O=Microsoft Corporation CN=Microsoft Azure RSA TLS Issuing CA 08	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2	0EFB7E547EDF0FF1069AEE57696D7BA0	RSA	sha384RSA	6/7/2023 17:00	8/25/2026 16:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	F67E2FBD80A34AB2705BEBDF9A1FD8EDCA618007	511C1C41CB7EB2A10078C32C82F17925BA786DE46C633921D038E7409E15A5EA
16	3	C=US O=Microsoft Corporation CN=Microsoft Azure RSA TLS Issuing CA 08	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2	0133380EA444E519D557DC516EDCB120	RSA	sha384RSA	6/1/2023 00:00	8/25/2026 23:59	6/6/2023 17:01	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	F67E2FBD80A34AB2705BEBDF9A1FD8EDCA618007	04E385FA49454BA99020DFAAA78A97C5B37E212763D03C648FB11F0999F9FD1F
17	1	C=US O=Microsoft Corporation CN=Microsoft Azure TLS Issuing CA 01	C=US O=DigiCert Inc OU=www.digicert.com CN=DigiCert Global Root G2	0AAFA6C5CA63C45141EA3BE1F7C75317	RSA	sha384RSA	7/29/2020 12:30	6/27/2024 23:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	0F205DD7A15795DB92CF2BD0C7C27704CE728076	24C7299864E0A2A6964F551C0E8DF2461532FA8C48E4DBBB6080716691F190E5
17	2	C=US O=Microsoft Corporation CN=Microsoft Azure TLS Issuing CA 01	C=US O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	330000001DBE9496F3DB8B8DE7000000000001D	RSA	sha384RSA	1/17/2020 20:22	6/27/2024 20:22	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	0F205DD7A15795DB92CF2BD0C7C27704CE728076	0437AB2EC2C2B4890296C135034B21DB146434B8317EE703AA8AA943C5EA51AE
18	1	C=US O=Microsoft Corporation CN=Microsoft Azure TLS Issuing CA 02	C=US O=DigiCert Inc OU=www.digicert.com CN=DigiCert Global Root G2	0C6AE97CCED599838690A00A9EA53214	RSA	sha384RSA	7/29/2020 12:30	6/27/2024 23:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	00AB91FC216226979AA8791B61419060A96267FD	15A98761EBE011554DA3A46D206B0812CB2EB69AE87AAA11A6DD4CB84ED5142A
18	2	C=US O=Microsoft Corporation CN=Microsoft Azure TLS Issuing CA 02	C=US O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	330000001EC6749F058517B4D000000000001E	RSA	sha384RSA	1/17/2020 20:22	6/27/2024 20:22	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	00AB91FC216226979AA8791B61419060A96267FD	D39CE39FF6F449D4F3391EE2004D705EC22F99CFFCA40A88F85DB26454ADDBD1
19	1	C=US O=Microsoft Corporation CN=Microsoft Azure TLS Issuing CA 05	C=US O=DigiCert Inc OU=www.digicert.com CN=DigiCert Global Root G2	0D7BEDE97D8209967A52631B8BDD18BD	RSA	sha384RSA	7/29/2020 12:30	6/27/2024 23:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	C7B29C7F1CE3B85AEFE9681AA85D94C126526A68	D6831BA43607F5AC19778D627531562AF55145F191CAB5EFAFA0E0005442B302
19	2	C=US O=Microsoft Corporation CN=Microsoft Azure TLS Issuing CA 05	C=US O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	330000001F9F1FA2043BC28DB900000000001F	RSA	sha384RSA	1/17/2020 20:22	6/27/2024 20:22	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	C7B29C7F1CE3B85AEFE9681AA85D94C126526A68	AB3203B3EA2017D509726A1D82293EFFCB8C42CEB52C9AF1C0EEE96B5C02BCBA
20	1	C=US O=Microsoft Corporation CN=Microsoft Azure TLS Issuing CA 06	C=US O=DigiCert Inc OU=www.digicert.com CN=DigiCert Global Root G2	02E79171FB8021E93FE2D983834C50C0	RSA	sha384RSA	7/29/2020 12:30	6/27/2024 23:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	D5C1673AC2A39DF477525B59123829E65568BBA5	48FF8B494668C752304B48BFE818758987DEF6582E5F09B921F4B60BB3D6A8DD
20	2	C=US O=Microsoft Corporation CN=Microsoft Azure TLS Issuing CA 06	C=US O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	3300000020A2F1491A37FBD31F000000000020	RSA	sha384RSA	1/17/2020 20:22	6/27/2024 20:22	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	D5C1673AC2A39DF477525B59123829E65568BBA5	7DF4D3EF45798F8C4384FC702BA52A44CE7BD6298B141628D4ABABC7678F6467
21	1	C=US O=Microsoft Corporation CN=Microsoft TLS G1 ECC CA 01	C=US O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	330000003D136DEBEF4C351D1200000000003D	ECC	sha384ECDSA	8/28/2025 9:50	8/28/2030 9:50	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	7CAAC9A9DDD1AFD8F4D24161572F4BF8D36E5D0E	2B5F1CA6E115D42112224720694D73BA50CA9B5C64E9DA2529B8F4AAF38DF384
21	2	C = US, O = Microsoft Corporation, CN = Microsoft TLS G1 ECC CA 01	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G3	0778A9033B5EC969FF4F5B6285952F54	ECC	sha384ECDSA	12/23/2025 00:00	6/15/2026 23:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	7CAAC9A9DDD1AFD8F4D24161572F4BF8D36E5D0E	CAF00842A72F9696E53C29F2C5E7A1B9D71A3E2F0C31D8B940694D59DCCEF643
21	3	C = US, O = Microsoft Corporation, CN = Microsoft TLS G1 ECC CA 01	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G3	0950BBDE2B07B8BFA44EB03D8174E5A8	ECC	sha384ECDSA	12/18/2025 00:00	6/15/2026 23:59	12/23/2025 18:19	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	D2D101768A55F51FE426B4F9E03734525FA7A585	E01233CBC292EF6D2476E1D22588510FE9F86BF65DFD8E6A9BF93B325FAA6E29
21	4	C = US, O = Microsoft Corporation, CN = Microsoft TLS G1 ECC CA 01	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G3	0C3D2F09209D76D81B29FCB3EEA66C06	ECC	sha384ECDSA	9/17/2025 00:00	4/15/2029 23:59	1/12/2026 18:29	Server Authentication (1.3.6.1.5.5.7.3.1)	7CAAC9A9DDD1AFD8F4D24161572F4BF8D36E5D0E	39C492D06ED1150D35FCEACF0DF28D0FB61BBA072A34AA4E824D6BE339A7EB23
22	1	C=US O=Microsoft Corporation CN=Microsoft TLS G1 ECC CA 02	C=US O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	330000003C7D4B4D2574A8855B000000000003C	ECC	sha384ECDSA	8/28/2025 9:50	8/28/2030 9:50	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	5B381B7EAC1CC5B335DC4D1A6612B3215FA54CC7	C8201D6406020821C00855E25CF826983BBD143F074935F440FB3BF980A2F90A
22	2	C = US, O = Microsoft Corporation, CN = Microsoft TLS G1 ECC CA 02	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G3	049A2554F88B66EF2B9838855FFBAF0A	ECC	sha384ECDSA	12/23/2025 00:00	6/15/2026 23:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	5B381B7EAC1CC5B335DC4D1A6612B3215FA54CC7	C772865E6F9E0A778B0E86444A21FB6547F7A05E169CCFC5BFEA05317E0F5F69
22	3	C = US, O = Microsoft Corporation, CN = Microsoft TLS G1 ECC CA 02	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G3	05022B8F0977569D822CB0B4B74D5555	ECC	sha384ECDSA	9/17/2025 00:00	4/15/2029 23:59	1/12/2026 18:30	Server Authentication (1.3.6.1.5.5.7.3.1)	5B381B7EAC1CC5B335DC4D1A6612B3215FA54CC7	3BFBAB94D8573CF5501E87273833172EE3B2184FFFFD9B95A3906FC4DD3ADA50
23	1	C=US O=Microsoft Corporation CN=Microsoft TLS G1 RSA CA 01	C=US O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	3300000044E807BA6918AB9AE4000000000044	RSA	sha384RSA	8/28/2025 9:51	8/28/2030 9:51	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	20BBF2198EA4C672B4AAC904416F559AA69F3D0F	79DBA0721F6DC1AD8EDC3DC27518702F970044188928BF7E8B42A04531424F73
23	2	C = US, O = Microsoft Corporation, CN = Microsoft TLS G1 RSA CA 01	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2	0756A78B1EBAD43408B905304D9CB97C	RSA	sha384RSA	12/23/2025 00:00	6/15/2026 23:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	20BBF2198EA4C672B4AAC904416F559AA69F3D0F	374CAAB4721816A4F3801300ED6CE5D64F1554F9178D940B4E7306BC93D2B72E
23	3	C = US, O = Microsoft Corporation, CN = Microsoft TLS G1 RSA CA 01	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2	01A66577E2755575D4EDDA5F06E741D1	RSA	sha384RSA	9/17/2025 00:00	4/15/2029 23:59	1/12/2026 18:31	Server Authentication (1.3.6.1.5.5.7.3.1)	20BBF2198EA4C672B4AAC904416F559AA69F3D0F	3ED3F8679802E0ABEEDB388A901DAF619B6F2B34F6926DCCFFF2139517351178
24	1	C=US O=Microsoft Corporation CN=Microsoft TLS G1 RSA CA 02	C=US O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	33000000453BFFDCDACA3EFD32000000000045	RSA	sha384RSA	8/28/2025 9:51	8/28/2030 9:51	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	C3D4063CD31A48109032358628D3948C712AD7AF	04396B0ED932A93150457013D839077784BFB143EA900B6A4990FCA139CBD4D1
24	2	C = US, O = Microsoft Corporation, CN = Microsoft TLS G1 RSA CA 02	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2	037004DBDB89FFA03F90816821A5991E	RSA	sha384RSA	12/23/2025 00:00	6/15/2026 23:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	C3D4063CD31A48109032358628D3948C712AD7AF	D3A843D4DC92EB5DF127E646C2F50EE803452747D8C9C6D4FDB9F7CB2060C5B7

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
24	3	C = US, O = Microsoft Corporation, CN = Microsoft TLS G1 RSA CA 02	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2	01A66577E2755575D4EDDA5F06E741D1	RSA	sha384RSA	9/17/2025 00:00	4/15/2029 23:59	1/12/2026 18:32	Server Authentication (1.3.6.1.5.5.7.3.1)	C3D4063CD31A48109032358628D3948C712AD7AF	64FE47E1256083CDAA1FE17AB2D3D965919FAD9CFE063A45A85F62487F88047E
25	1	C=US O=Microsoft Corporation CN=Microsoft TLS G1 RSA CA 03	C=US O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	33000000465C83326B083F339E000000000046	RSA	sha384RSA	8/28/2025 9:51	8/28/2030 9:51	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	BCCBC8BC0D5623C1E6AFCA87D56B7ACEC662CCEB	8797D4D4A3473CA1D86A279BED9639937B27C52F3CDA0B6009D695BC373BDEBB
25	2	C = US, O = Microsoft Corporation, CN = Microsoft TLS G1 RSA CA 03	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2	0FCAAF57DD2227BC2F0FFCDBECB45A53	RSA	sha384RSA	12/23/2025 00:00	6/15/2026 23:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	BCCBC8BC0D5623C1E6AFCA87D56B7ACEC662CCEB	6A9A2AF2D7FAACE5E2817E8398827A1406BEE711DDB718E7B559577AA4C12B5F
25	3	C = US, O = Microsoft Corporation, CN = Microsoft TLS G1 RSA CA 03	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2	0EAB72B62946450C62DE692C8265048A	RSA	sha384RSA	9/17/2025 00:00	4/15/2029 23:59	1/12/2026 18:33	Server Authentication (1.3.6.1.5.5.7.3.1)	BCCBC8BC0D5623C1E6AFCA87D56B7ACEC662CCEB	DED374DC72904DCCAFB7DCD8429D45A6AADAB8028FD7C70CB1A0BD53FE0CCC6E
26	1	C=US O=Microsoft Corporation CN=Microsoft TLS G1 RSA CA 04	C=US O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	33000000477A82567E021DB1150000000000047	RSA	sha384RSA	8/28/2025 9:51	8/28/2030 9:51	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	B5C26D72E38147DEC0DDA671E4557788A535DC9F	2765F456AA084CC2BA015C44D42EC783F2BF6E706C9132E8A6EFD3C800F32D93
26	2	C = US, O = Microsoft Corporation, CN = Microsoft TLS G1 RSA CA 04	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2	0A173E50576F5B7BDD10DFACFF0D7842	RSA	sha384RSA	12/23/2025 00:00	6/15/2026 23:59	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	B5C26D72E38147DEC0DDA671E4557788A535DC9F	41D989FF321395E82049C2E95ABCBD79C6CC207B62F9F18274BDE2C72F8341D6
26	3	C = US, O = Microsoft Corporation, CN = Microsoft TLS G1 RSA CA 04	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2	0C40B9C958224B341C912C34C5742135	RSA	sha384RSA	9/17/2025 00:00	4/15/2029 23:59	1/12/2026 18:33	Server Authentication (1.3.6.1.5.5.7.3.1)	B5C26D72E38147DEC0DDA671E4557788A535DC9F	6EC85CD93E5A7B4CAE58818CB0296A80B3B23AC8D7268E48882E53700F1544A8
27	1	C=US O=Microsoft Corporation CN=Microsoft ECC TLS Issuing AOC CA 01	C=US O=Microsoft Corporation CN=Microsoft ECC Root Certificate Authority 2017	33000000282BFD23E7D1ADD707000000000028	ECC	sha384ECDSA	6/24/2021 19:58	6/24/2021 19:58	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	315BB9CE511B7CD1AA03C0EBED365DC29DD389E1	5C64B1731A8138DEA7D11C9AE8622891F945EBA46825E7ABFE4754F0A6011AF8
28	1	C=US O=Microsoft Corporation CN=Microsoft ECC TLS Issuing AOC CA 02	C=US O=Microsoft Corporation CN=Microsoft ECC Root Certificate Authority 2017	33000000290F8A6222EF6A5695000000000029	ECC	sha384ECDSA	6/24/2021 19:58	6/24/2021 19:58	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	DEDCD76C239943EAACEDC8B71D185880364B8DF4	808CA1ABBFE2FF1A9AC71887DDA71FF6FCA6C3B5224827F547515A4D9F7AF209
29	1	C=US O=Microsoft Corporation CN=Microsoft ECC TLS Issuing EOC CA 01	C=US O=Microsoft Corporation CN=Microsoft ECC Root Certificate Authority 2017	330000002A2D006485FDACBFEB00000000002A	ECC	sha384ECDSA	6/24/2021 19:58	6/24/2021 19:58	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	BB1CEDD08871A9CAFBCD935F7179223578C69ACA	2769381532D96183ED39BDC4E323F3C520FBE6ACF3BDA30222239DDFC44C8380
30	1	C=US O=Microsoft Corporation CN=Microsoft ECC TLS Issuing EOC CA 02	C=US O=Microsoft Corporation CN=Microsoft ECC Root Certificate Authority 2017	330000002BE6902838672B6679000000000002B	ECC	sha384ECDSA	6/24/2021 19:58	6/24/2021 19:58	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	BFD832342BA1953BB4B5D4B9402D724A9C1A0086	659C0F902D6059FBD1FCA528839F20604B80C74364E58F9D48A2291F813ED82D
31	1	C=US O=Microsoft Corporation CN=Microsoft RSA TLS Issuing AOC CA 01	C=US O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	330000002FFAF06F6697E2469C00000000002F	RSA	sha384RSA	6/24/2021 20:57	6/24/2021 20:57	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	EB4C317C3D3F32B883D7C5DB7BDAE478DA9C1457	481E582A206A7D7040CCDA17CF25D349785A2AB94ED7552AB254DCD38B032EC0
32	1	C=US O=Microsoft Corporation CN=Microsoft RSA TLS Issuing AOC CA 02	C=US O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	3300000030C756CC88F5C1E7EB000000000030	RSA	sha384RSA	6/24/2021 20:57	6/24/2021 20:57	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	8A96C2810D578A42CE30F9B8C19D0C1E53A64FE5	D77C45C1587731C4632C19D6F3C9FE832626615C879EA053664A4B26EB2293EC
33	1	C=US O=Microsoft Corporation CN=Microsoft RSA TLS Issuing EOC CA 01	C=US O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	33000000310C4914B18C8F339A000000000031	RSA	sha384RSA	6/24/2021 20:57	6/24/2021 20:57	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	73087893F9D5A99CA3777E113474FF453271B783	5EA3857EACD4C7CA5ACBCA9C4627E26F3072038D191A29D4C3F9464B2E5F00C6
34	1	C=US O=Microsoft Corporation CN=Microsoft RSA TLS Issuing EOC CA 02	C=US O=Microsoft Corporation CN=Microsoft RSA Root Certificate Authority 2017	3300000032444D7521341496A9000000000032	RSA	sha384RSA	6/24/2021 20:57	6/24/2021 20:57	N/A	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)	C984963873A62E4B186A6D44D594A37D34A6C7F7	4D55BC4ABEB7D37FAB57E573ACCE83133E36212C864E003FBCB30B5FC248B011
35	1	C=US O=Microsoft Corporation CN=Microsoft TLS G2 RSA CA OCSP 02	C=US O=Microsoft Corporation CN=Microsoft TLS RSA Root G2	330000000C4964A16F44203B2200000000000C	RSA	Sha384RSA	8/1/2025 1:03	6/3/2029 1:03	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	B82F33A67C514F7F1F2DD5C8154238A4B20E8F2F	EA7A25255D111FC3CE4CB8FABE3ADF9C27BBE6DB203F955066BAB4C5A71F3D08
35	2	C=US O=Microsoft Corporation CN=Microsoft TLS G2 RSA CA OCSP 02	C=US O=Microsoft Corporation CN=Microsoft TLS RSA Root G2	33000000674997E55D8C5020D000000000006	RSA	Sha384RSA	6/26/2025 21:23	6/3/2029 21:23	7/2/2025 00:00	Server Authentication (1.3.6.1.5.5.7.3.1)	B82F33A67C514F7F1F2DD5C8154238A4B20E8F2F	E4F93B694981068A6E07ADD2AFE050464B82F9276B96BA3ECF59817DDB6E1085
36	1	C=US O=Microsoft Corporation CN=Microsoft TLS G2 RSA CA OCSP 04	C=US O=Microsoft Corporation CN=Microsoft TLS RSA Root G2	330000000B13E5667D4A9B5580000000000000B	RSA	Sha384RSA	8/1/2025 1:02	6/3/2029 1:02	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	540CBCEC18F77DF103E284BE34644467CF751F65	AC8EA9F2874FD368A3E778B1A0B165EE898DB9B9687C17EDCDC76908AB58C82C
36	2	C=US O=Microsoft Corporation CN=Microsoft TLS G2 RSA CA OCSP 04	C=US O=Microsoft Corporation CN=Microsoft TLS RSA Root G2	33000000050717B5EE99E2F4DF000000000005	RSA	Sha384RSA	6/26/2025 21:23	6/3/2029 21:23	7/2/2025 0:00	Server Authentication (1.3.6.1.5.5.7.3.1)	540CBCEC18F77DF103E284BE34644467CF751F65	870A6F0B649FA5781A27710F50FBE1C5027E7B7DE000BE9D20D02C6791B96AC8
37	1	C=US O=Microsoft Corporation CN=Microsoft TLS G2 RSA CA OCSP 06	C=US O=Microsoft Corporation CN=Microsoft TLS RSA Root G2	330000000DEF69CD2D722373560000000000D	RSA	Sha384RSA	8/1/2025 1:03	6/3/2029 1:03	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	0C5D6BCD4A34016034342401E03F500583EBA845	16B74B335C6F9801CFC499E39CC292F6D13C5191BE87126226403819DA4AD213
37	2	C=US O=Microsoft Corporation CN=Microsoft TLS G2 RSA CA OCSP 06	C=US O=Microsoft Corporation CN=Microsoft TLS RSA Root G2	33000000710F17E5773D03D87000000000007	RSA	Sha384RSA	6/26/2025 21:23	6/3/2029 21:23	7/2/2025 00:00	Server Authentication (1.3.6.1.5.5.7.3.1)	0C5D6BCD4A34016034342401E03F500583EBA845	016CB2A68F7B7D96311306DB9648FA798C2C40BE1574AD12891549C99F41082E
38	1	C=US O=Microsoft Corporation CN=Microsoft TLS G2 RSA CA OCSP 08	C=US O=Microsoft Corporation CN=Microsoft TLS RSA Root G2	3300000011F100A7EB05EBA100000000000011	RSA	Sha384RSA	8/14/2025 4:03	6/3/2029 4:03	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	0FB23280ED7F8A9C008438E6D8D7F6708577ED7A	885451307A4ABF298BB28ADD793EC7826629B057ECA79E6F51DC51F42CD64A2D
39	1	C=US O=Microsoft Corporation CN=Microsoft TLS G2 RSA CA OCSP 10	C=US O=Microsoft Corporation CN=Microsoft TLS RSA Root G2	330000000F33206537EE42AE4F000000000000F	RSA	Sha384RSA	8/1/2025 1:03	6/3/2029 1:03	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	D04C83D18E712E3D34B1FF9B792C8E74D4E27806	6EBFF927297A5B3AAF5EAE672252C36A5158473FA5BBF0E29508D5528358F83B
39	2	C=US O=Microsoft Corporation CN=Microsoft TLS G2 RSA CA OCSP 10	C=US O=Microsoft Corporation CN=Microsoft TLS RSA Root G2	33000000008710CE4EAF0BCC488000000000008	RSA	Sha384RSA	6/26/2025 21:23	6/3/2029 21:23	7/2/2025 00:00	Server Authentication (1.3.6.1.5.5.7.3.1)	D04C83D18E712E3D34B1FF9B792C8E74D4E27806	ECF249379A0C083CACE54EC906AE4550ECC634DA4A8262FEA7083ECB9E13FC39
40	1	C=US O=Microsoft Corporation CN=Microsoft TLS G2 RSA CA OCSP 12	C=US O=Microsoft Corporation CN=Microsoft TLS RSA Root G2	33000000107D59860FD64D72430000000000010	RSA	Sha384RSA	8/14/2025 4:03	6/3/2029 4:03	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	31A5A58943EFC7AC31153E487AE306C6E9EDBC2A	D9280DDA01FCDFE208955CC7FBEF27C3909C0A05D2C2E24E27DBB33C3BE5889C
41	1	C=US O=Microsoft Corporation CN=Microsoft TLS G2 RSA CA OCSP 14	C=US O=Microsoft Corporation CN=Microsoft TLS RSA Root G2	33000000127E739347E75BE1A1000000000012	RSA	Sha384RSA	8/14/2025 4:03	6/3/2029 4:03	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	5268F4FA1256E3F6D842AF300B40B83923F5F72B	B2ABE84672548695C111FF9A9D6D8D55EABABF2FC311D02ECF86A93CD7FCE361
42	1	C=US O=Microsoft Corporation CN=Microsoft TLS G2 RSA CA OCSP 16	C=US O=Microsoft Corporation CN=Microsoft TLS RSA Root G2	330000000E42938F25DC51A99B000000000000E	RSA	Sha384RSA	8/1/2025 1:03	6/3/2029 1:03	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	0639F056D1ED90C836A3A00F94FE6294A7E6FC37	38D895F5105BC2545822C17A2444F4B0EA3D298D2C15A38296AA7295A3D85CE9
42	2	C=US O=Microsoft Corporation CN=Microsoft TLS G2 RSA CA OCSP 16	C=US O=Microsoft Corporation CN=Microsoft TLS RSA Root G2	33000000092799CF18B020C53F000000000009	RSA	Sha384RSA	6/26/2026 21:23	6/3/2029 21:23	7/2/2025 00:00	Server Authentication (1.3.6.1.5.5.7.3.1)	0639F056D1ED90C836A3A00F94FE6294A7E6FC37	1D959F28A67BE6DCF5ED1E393AB92CEBE24DE22B4BF12BBC2C4F01C044AF9955
43	1	C=US O=Microsoft Corporation CN=Microsoft TLS G2 ECC CA OCSP 02	C=US O=Microsoft Corporation CN=Microsoft TLS ECC Root G2	33000000005516A21C89814CCF7000000000005	ECC	sha384ECDSA	8/1/2025 1:02	6/3/2029 1:02	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	E51FC46A0936E2AFE1646EBDFC6BE9EDC5D02A74	8A7B34C8E82EFB3B5B416671230729FAD2E26279383FB2993ED2920BD6E21241
44	1	C=US O=Microsoft Corporation CN=Microsoft TLS G2 ECC CA OCSP 04	C=US O=Microsoft Corporation CN=Microsoft TLS ECC Root G2	33000000008D690FFF489D9C4D7000000000008	ECC	sha384ECDSA	8/14/2025 4:03	6/3/2029 4:03	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	A449ADEE0230A5B8B36C37982AF03C4EE2ADB1B2	36A52BC5A51CA90DF18A1BAFF92982301582A54C2BBE4F8D618D96D2E830A501
45	1	C=US O=Microsoft Corporation CN=Microsoft TLS G2 ECC CA OCSP 06	C=US O=Microsoft Corporation CN=Microsoft TLS ECC Root G2	33000000066FA24C31C3956FAB000000000006	ECC	sha384ECDSA	8/1/2025 1:02	6/3/2029 1:02	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	389B2CE59C4F9DC21461EAE944108D70494BEA5B	27B122BC1DBE12C88B1ACBEBC33030BDBCCF4DE724EC8E82266513D0797C097A
46	1	C=US O=Microsoft Corporation CN=Microsoft TLS G2 ECC CA OCSP 08	C=US O=Microsoft Corporation CN=Microsoft TLS ECC Root G2	33000000077737DEB49D007DC64000000000007	ECC	sha384ECDSA	8/14/2025 4:03	6/3/2029 4:03	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	C3A5B3FC6CD19B84884FE69291F7BEF6E50AE205	C72C4B58522EE034B49A26EE822BC4D67C8D348756C5BB373B6A2D7B821A97B0

ATTACHMENT B

LIST OF MS PKI SERVICES' CERTIFICATE POLICIES AND CERTIFICATION PRACTICE STATEMENTS

CP Name	Version	Date
Microsoft PKI Services Certificate Policy	3.2.0	April 20, 2026
Microsoft PKI Services Certificate Policy	3.1.9	April 21, 2025

CPS Name	Version	Date
Microsoft PKI Services Public TLS Certification Practice Statement	3.3.6	April 13, 2026
Microsoft PKI Services Public TLS Certification Practice Statement	3.3.5	February 12, 2026
Microsoft PKI Services Public TLS Certification Practice Statement	3.3.4	December 1, 2025
Microsoft PKI Services Public TLS Certification Practice Statement	3.3.3	September 16, 2025
Microsoft PKI Services Public TLS Certification Practice Statement	3.3.2	July 3, 2025
Microsoft PKI Services Public TLS Certification Practice Statement	3.3.1	April 29, 2025

ATTACHMENT C

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 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, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subordinate CA certification

The management of MS PKI Services 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, certificate lifecycle management controls, and subordinate CA 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 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 disclosures of its certificate practices and controls over its CA services. Based on that assessment, in MS PKI Services management's opinion, in providing its CA services at locations enumerated in Attachment C, MS PKI Services has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in the applicable versions of its Certificate Policies and Certification Practice Statements as enumerated in Attachment B
- maintained effective controls to provide reasonable assurance that
    - MS PKI Services' Certification Practice Statements are consistent with its Certificate Policies; and
    - MS PKI Services provides its services in accordance with its Certificate Policies and Certification Practice Statements
- 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 MS PKI Services); and
    - subordinate CA certificate requests are accurate, authenticated, and approved
- 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 May 1, 2025 to April 30, 2026 based on the WebTrust Principles and Criteria for Certification Authorities, v2.2.2, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certification Practice Statement Management
- Certificate Policy Management
- CP and CPS Consistency

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 Archival
- 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

Subordinate CA and Cross Certificate Lifecycle Management Controls

- Subordinate CA Certificate and Cross Certificate Lifecycle Management

MS PKI Services does not escrow its CA keys, does not provide subscriber key generation services, subscriber key storage and recovery services, or integrated circuit card lifecycle management for subscribers, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.

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

Sr.	Bugzilla ID	Bugzilla Title	Created On	Resolved On	Status
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: OCSP 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
16	2021175	Microsoft PKI Services: Failure to update action item status within 3 days	March 5, 2026	April 3, 2026	Resolved
17	2026452	Microsoft PKI Services: Failure to publish Full Incident Report for Bugzilla 2021175 within 14 days	March 26, 2026	April 22, 2026	Resolved
18	2026453	Microsoft PKI Services: Failure to report Bugzilla 2026452 within 72 hrs	March 26, 2026	April 22, 2026	Resolved
19	2034251	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 ECC Root Certificate Authority 2017
2. Microsoft RSA Root Certificate Authority 2017
3. Microsoft TLS RSA Root G2
4. Microsoft TLS ECC Root G2
Cross-signed CA Certificates
3. Microsoft TLS RSA Root G2
4. Microsoft TLS ECC Root G2
5. Microsoft Azure ECC TLS Issuing CA 01
6. Microsoft Azure ECC TLS Issuing CA 02
7. Microsoft Azure ECC TLS Issuing CA 05
8. Microsoft Azure ECC TLS Issuing CA 06
9. Microsoft Azure ECC TLS Issuing CA 03
10. Microsoft Azure ECC TLS Issuing CA 04
11. Microsoft Azure ECC TLS Issuing CA 07
12. Microsoft Azure ECC TLS Issuing CA 08
13. Microsoft Azure RSA TLS Issuing CA 03
14. Microsoft Azure RSA TLS Issuing CA 04
15. Microsoft Azure RSA TLS Issuing CA 07
16. Microsoft Azure RSA TLS Issuing CA 08
17. Microsoft Azure TLS Issuing CA 01
18. Microsoft Azure TLS Issuing CA 02
19. Microsoft Azure TLS Issuing CA 05
20. Microsoft Azure TLS Issuing CA 06
21. Microsoft TLS G1 ECC CA 01
22. Microsoft TLS G1 ECC CA 02
23. Microsoft TLS G1 RSA CA 01
24. Microsoft TLS G1 RSA CA 02
25. Microsoft TLS G1 RSA CA 03
26. Microsoft TLS G1 RSA CA 04
Intermediate CA Certificates
27. Microsoft ECC TLS Issuing AOC CA 01
28. Microsoft ECC TLS Issuing AOC CA 02
29. Microsoft ECC TLS Issuing EOC CA 01
30. Microsoft ECC TLS Issuing EOC CA 02
31. Microsoft RSA TLS Issuing AOC CA 01
32. Microsoft RSA TLS Issuing AOC CA 02
33. Microsoft RSA TLS Issuing EOC CA 01
34. Microsoft RSA TLS Issuing EOC CA 02
35. Microsoft TLS G2 RSA CA OCSP 02
36. Microsoft TLS G2 RSA CA OCSP 04
37. Microsoft TLS G2 RSA CA OCSP 06
38. Microsoft TLS G2 RSA CA OCSP 08
39. Microsoft TLS G2 RSA CA OCSP 10
40. Microsoft TLS G2 RSA CA OCSP 12
41. Microsoft TLS G2 RSA CA OCSP 14
42. Microsoft TLS G2 RSA CA OCSP 16
43. Microsoft TLS G2 ECC CA OCSP 02
44. Microsoft TLS G2 ECC CA OCSP 04
45. Microsoft TLS G2 ECC CA OCSP 06
46. Microsoft TLS G2 ECC CA OCSP 08

ATTACHMENT B

LIST OF MS PKI SERVICES' CERTIFICATE POLICIES AND CERTIFICATION PRACTICE STATEMENTS

CP Name	Version	Date
Microsoft PKI Services Certificate Policy	3.2.0	April 20, 2026
Microsoft PKI Services Certificate Policy	3.1.9	April 21, 2025

CPS Name	Version	Date
Microsoft PKI Services Public TLS Certification Practice Statement	3.3.6	April 13, 2026
Microsoft PKI Services Public TLS Certification Practice Statement	3.3.5	February 12, 2026
Microsoft PKI Services Public TLS Certification Practice Statement	3.3.4	December 1, 2025
Microsoft PKI Services Public TLS Certification Practice Statement	3.3.3	September 16, 2025
Microsoft PKI Services Public TLS Certification Practice Statement	3.3.2	July 3, 2025
Microsoft PKI Services Public TLS Certification Practice Statement	3.3.1	April 29, 2025

ATTACHMENT C

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

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 at locations enumerated in Attachment C, for its CAs as enumerated in Attachment A, MS PKI Services has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of its Certificate Policies and Certification Practice Statements as enumerated in Attachment B
- maintained effective controls to provide reasonable assurance that:
  - MS PKI Services' Certification Practice Statements are consistent with its Certificate Policies; and
  - MS PKI Services provides its services in accordance with its Certificate Policies and Certification Practice Statements
- 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 MS PKI Services); and
  - subordinate CA certificate requests are accurate, authenticated, and approved
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorised individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity.

throughout the period May 1, 2025 to April 30, 2026 based on the WebTrust Principles and Criteria for Certification Authorities, v2.2.2.

MS PKI Services does not escrow its CA keys, does not provide subscriber key generation services, subscriber key storage and recovery services, or integrated circuit card lifecycle management for subscribers, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.

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, v2.2.2.

Practitioner's responsibilities

Our responsibility is to express an opinion on MS PKI Services 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.

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	**OCSP response formatting and infrastructure rollback issue**	As publicly disclosed in Bugzilla 1999850, Microsoft PKI Services identified an issue in its new OCSP infrastructure where responses included fractional seconds in the 'thisUpdate', 'nextUpdate', and 'producedAt' fields, causing TLS handshake failures for some relying parties and creating inconsistency with RFC 5280. As a result, OCSP traffic was moved back to the legacy responder infrastructure while Microsoft works to remediate the issue and resume migration to the new environment. The Bugzilla ticket was closed as RESOLVED on July 1, 2026.

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 have only noted those matters relevant to the CAs enumerated in Attachment A and applicable to the WebTrust Principles and Criteria for Certification Authorities, v2.2.2.

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 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 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 28, 2026

ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs
1. Microsoft ECC Product Root Certificate Authority 2018
2. Microsoft ECC TS Root Certificate Authority 2018
3. Microsoft Root Certificate Authority 2010
4. Microsoft Root Certificate Authority 2011
5. Microsoft Root Certificate Authority 2014
6. Microsoft Time Stamp Root Certificate Authority 2014
Intermediate CA Certificates
7. Microsoft Azure Attestation PCA 2019
8. Microsoft Certificate List CA 2011
9. Microsoft Certificate List CA 2024
10. Microsoft Code Signing PCA 2010
11. Microsoft Code Signing PCA 2011
12. Microsoft Code Signing PCA 2024
13. Microsoft Content Distribution Secure Server CA 2.1
14. Microsoft Content Distribution Secure Server CA 2.2
15. Microsoft ECC Certificate List PCA 2018
16. Microsoft ECC Code Signing PCA 2018
17. Microsoft ECC Content Distribution Secure Server CA 2.1
18. Microsoft ECC Content Distribution Secure Server CA 2.2
19. Microsoft ECC Time Stamp PCA 2018
20. Microsoft ECC Update Secure Server CA 2.1
21. Microsoft ECC Update Secure Server CA 2.2
22. Microsoft ECC Update Signing CA 2.1
23. Microsoft ECC Update Signing CA 2.2
24. Microsoft ECC Update Signing CA 2.3
25. Microsoft MarketPlace PCA 2011
26. Microsoft Marketplace CA G 021
27. Microsoft Marketplace CA G 022
28. Microsoft Marketplace CA G 023
29. Microsoft Marketplace CA G 024
30. Microsoft Marketplace CA G 025
31. Microsoft Marketplace CA G 026
32. Microsoft Marketplace CA G 027
33. Microsoft Marketplace CA G 028
34. Microsoft Marketplace Production CA 2011
35. Microsoft Secure Server CA 2011
36. Microsoft Time Stamp CA 2015
37. Microsoft Time-Stamp PCA 2010
38. Microsoft Update Metadata Signing CA 3.1
39. Microsoft Update Secure Server CA 2.1
40. Microsoft Update Secure Server CA 2.2
41. Microsoft Update Secure Server CA 3.1
42. Microsoft Update Signing CA 2.1
43. Microsoft Update Signing CA 2.2
44. Microsoft Update Signing CA 2.3
45. Microsoft Update SIH Signing CA 3.1
46. Microsoft Update SLS Signing CA 3.1
47. Microsoft Update SLS Signing CA 3.2
48. Microsoft Windows Code Signing PCA 2024
49. Microsoft Windows Component Preproduction CA 2024
50. Microsoft Windows PCA 2010
51. Microsoft Windows Phone PCA 2011
52. Microsoft Windows Phone Production PCA 2012

53. Microsoft Windows Production PCA 2011
54. Microsoft Windows Third Party Component CA 2012
55. Microsoft Windows Third Party Component CA 2013
56. Microsoft Windows Third Party Component CA 2014
57. Microsoft Windows Third Party Component CA 2024
58. VS Package Repositories CA
59. Windows Azure StorSimple CA 2013
60. Windows Production PCA 2023
61. Windows UEFI CA 2023
62. Microsoft ECC Update SIH Signing CA 3.2
63. Microsoft ECC Update SIH Signing CA 3.1
64. Microsoft ECC Update Metadata Signing CA 3.1
65. Microsoft ECC Update Metadata Signing CA 3.2
66. Microsoft Update SLS Signing CA 3.3
67. Microsoft Update Metadata Signing CA 3.2
68. Microsoft Update Secure Server CA 3.2
69. Microsoft Update SIH Signing CA 3.2

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 S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	14982666DC7CCD8F4053677BB999EC85	ECC	sha384ECDSA	2/27/2018 20:42	2/27/2043 20:50	N/A	0	43EF7087B89DBFEC8819DCC6C46B750D75343308	CACA93B9D23D2B6FA76E8B8471931E0DF3EC6F63AF3CDBB936C41954A1872326
2	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC TS Root Certificate Authority 2018	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC TS Root Certificate Authority 2018	153875E1647ED1B047B4EFAF41128245	ECC	sha384ECDSA	2/27/2018 20:51	2/27/2043 21:00	N/A	0	E847C8429AB09DAE6F0B283B98158FE3B1E880B2	3FD4BE8BAAD2F26E1BDE06C7584BB720DD1A972D111F5A4999BC44B08FB4960D
2	2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC TS Root Certificate Authority 2018	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC TS Root Certificate Authority 2018	'330000001498434745943178490000000014	ECC	sha384ECDSA	9/28/2018 17:55	9/6/2035 17:55	N/A	Time Stamping (1.3.6.1.5.5.7.3.8)	E847C8429AB09DAE6F0B283B98158FE3B1E880B2	D4D27BC233F38B4414617E72871F54D40758AB988072D9FFEC31AEDA60ECC6D0
3	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	28CC3A25BFBA44AC449A9B586B4339AA	RSA	sha256RSA	6/23/2010 21:57	6/23/2035 22:04	N/A	0	D5F656CB8FE8A25C6268D13D94905BD7CE9A18C4	DF545BF919A2439C36983B54CDFC903DFA4F37D3996D8D84B4C31EEC6F3C163E
4	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	3F8BC8B5FC9FB29643B569D66C42E144	RSA	sha256RSA	3/22/2011 22:05	3/22/2036 22:13	N/A	0	722D3A02319043B914054EE1EAA7C731D1238934	847DF6A78497943F27FC72EB93F9A637320A02B561D0A91B09E87A7807ED7C61
5	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2014	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2014	5586A39A5F38DFB24A7B48D1B491FFF3	RSA	sha256RSA	10/22/2014 21:00	10/22/2039 21:01	N/A	0	11d6d4f06236a01ee769835aad7db41527b79945	B13DDACB6431E702356A0002730B933C65272F9180D53BCD4577F8D500680A42
6	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Time Stamp Root Certificate Authority 2014	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Time Stamp Root Certificate Authority 2014	2FD67A43229329045E953343EE27466	RSA	sha256RSA	10/22/2014 22:08	10/22/2039 22:15	N/A	0	CBD1F2CE48FD019FEA56AA57D17E9958F83FFFE0	65AF95F4BE86847344634282F941B2E605063EF0C8542F014CA088D182109E4F
6	2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Time Stamp Root Certificate Authority 2014	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Time Stamp Root Certificate Authority 2014	33000000112BF711003F3F012A000000000011	RSA	sha256RSA	11/8/2016 21:01	6/22/2035 21:01	N/A	Time Stamping (1.3.6.1.5.5.7.3.8)	CBD1F2CE48FD019FEA56AA57D17E9958F83FFFE0	A303E478DD3CBC0E47A290FD5B59AF5C017A95E4886EC354EC6DA8B9380EE399
7	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Azure Attestation PCA 2019	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	3300000037756C792A2979DF3D000000000037	RSA	sha256RSA	5/30/2019 22:48	5/30/2034 22:58	N/A	0	ad475e6ccfa9d55a75355dfa28a17578289f71ad	D8A4236A2BD59061D008139D2071EA7BEF642E1B959A0CE6626666B43BD2C095
8	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Certificate List CA 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	61116C92000000000007	RSA	sha256RSA	3/29/2011 18:58	3/29/2026 19:08	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Microsoft Trust List Signing (1.3.6.1.4.1.311.10.3.1), Root List Signer (1.3.6.1.4.1.311.10.3.9), Revoked List Signer (1.3.6.1.4.1.311.10.3.19)	41F021C7EDC487FA8375FF0A0CDC2DECA86AAB59	A53A400DF29EC7B8C8FCE7CFFFE47334F43B1642E604DD0307491737EBBC00CE
9	1	C=US O=Microsoft Corporation CN=Microsoft Certificate List CA 2024	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	330000001D30D6F149DCD42E1D000000000001D	RSA	sha384RSA	8/22/2024 20:32	6/23/2035 22:04	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Windows Update (1.3.6.1.4.1.311.76.6.1)	306e265901fa54f32fbffc613b2647f5a61a3ae2	56625EC7886445706FE74CCD2ABF69B7C9C9CCDE3C7354903AF1C8F0E30E9D1C
10	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Code Signing PCA 2010	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	610C524C000000000003	RSA	sha256RSA	7/6/2010 20:40	7/6/2025 20:50	N/A	0	E6FC5F7BBB220058E4724EB5F421742332E6EFAC	9AAD6C1A83A1B974BA574A995AF35B8CA772DA919270DB1605A8B81E1BBC896F
11	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Code Signing PCA 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	610E90D2000000000003	RSA	sha256RSA	7/8/2011 20:59	7/8/2026 21:09	N/A	0	486E64E55005D382AA17373722B56DA8CA750295	56DA8722AFD94066FFE1E4595473A4854892B843A0827D53FB7D8F4AEED1E18B
12	1	C=US O=Microsoft Corporation CN=Microsoft Code Signing PCA 2024	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	33000000393BB63719BF061D67000000000039	RSA	sha384RSA	8/8/2024 20:54	3/22/2036 22:13	N/A	0	E847C8429AB09DAE6F0B283B98158FE3B1E880B2	3DADFAF812DD1BBAEF45834CCBD188F3CD97139E2ED1ACA69C2DD63082142F8F
13	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Content Distribution Secure Server CA 2.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	3300000035D47483932E18187C000000000035	RSA	sha256RSA	12/7/2018 20:12	12/7/2033 20:22	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	DEAA37759FD493A715504C4578E761BA37027F4B	64EBAE10EF707ECF156B560A1C9236455A5E9F1C16F270996E41D5F0DFEDA561
14	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Content Distribution Secure Server CA 2.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	3300000036A26D4F583DFDC113000000000036	RSA	sha256RSA	12/7/2018 20:12	12/7/2033 20:22	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	84D6BFD9B25E9D87E3B2C0864CD39CC168B60E67	B90776868F9AA9F0048D2BBEC85908CD2735A36BACB5886AF5C3458303703471
15	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Certificate List PCA 2018	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	330000000037742B6E32092D50F000000000003	ECC	sha384ECDSA	3/1/2018 21:40	3/1/2033 21:50	N/A	0	7aa29b3c3676b7033c6ccf439e509c86758055ce	C307C2757F1026AA755DC7830E43C61BA30BFE178FB9F92B621B830B3DA21C83
16	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Code Signing PCA 2018	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	3300000002B2A4C58304AEE1E1000000000002	ECC	sha384ECDSA	3/1/2018 21:40	3/1/2033 21:50	N/A	0	862aaefa129e681f41ad660d486b1a707ff7c5c8	E673905E74CCA3307C5E2C7D1E78DCA1F6F2783A21F8B02B58472E304C680DB8
17	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Content Distribution Secure Server CA 2.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	33000000090 66CB601E4418E73000000000009	ECC	sha384ECDSA	12/7/2018 20:05	12/7/2033 20:15	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	455478B823ACADE42A8CBB014152B49C8E8191EE	E39F93F3B2B40FD3C41DE7DFA7D0B0CB6C4D8F97CBAB2BB81C178F4B5F3C7EED
18	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Content Distribution Secure Server CA 2.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	330000000ADB1A07295C828D77000000000000A	ECC	sha384ECDSA	12/7/2018 20:05	12/7/2033 20:15	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	D3C732531923973ECA3FFC83992F92CB3CD3D2C0	959D932A756F59612F2D757926D8AD3B11CB2684CA9203AE281F5CC26049BE94
19	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Time Stamp PCA 2018	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC TS Root Certificate Authority 2018	330000000278C1161CA7F6D350000000000002	ECC	sha384ECDSA	3/1/2018 21:48	3/1/2033 21:58	N/A	0	e8674bb61257af7710de403357646afc23e54881	5E72BC836123C6EA5DE54A3697DE416EE167C2AC62C7C89F61BEB89C735160A7

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
20	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Update Secure Server CA 2.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	3300000004A1F5B5883D3F0022000000000004	ECC	sha384ECDSA	9/28/2018 21:34	9/28/2033 21:44	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	1641B107C78BF3D2061490260ADBB12BC04462C3	21158AD4DCE10197239A87EBEB4D8D47E9E9BE716AD497A2E036774CAF5072CF
21	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Update Secure Server CA 2.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	33000000087B3662C012063EB4000000000008	ECC	sha384ECDSA	12/7/2018 20:05	12/7/2033 20:15	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	9dea50acb6663e22781d9640142b719e31c6d8c4	6345FD68446C011FD442A04A37E8407A51E548DE61A66856331 34EDD67292F1A
22	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Update Signing CA 2.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	33000000051A3AE66A9EE4F897000000000005	ECC	sha384ECDSA	9/28/2018 21:34	9/28/2033 21:44	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Unknown Key Usage (1.3.6.1.4.1.311.76.6.1)	D2465153A49F6324F2E8D2B2AB854C9E32FFD852	73DF319F3BF18FA9C9D0B38DAABA98038C4F867D3C9CE609737DFA682BDA1FFB
23	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Update Signing CA 2.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	3300000006DEA087FB82845B90000000000006	ECC	sha384ECDSA	9/28/2018 21:34	9/28/2033 21:44	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Unknown Key Usage (1.3.6.1.4.1.311.76.6.1)	0478de0ab9f5c19eaa7c890c02a50d9f7546a76f	3EBC65CCB963BAA55AFA2F0D24A20044C7D17D97208EA2B318778C505CB7C08F
24	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Update Signing CA 2.3	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	3300000007E8141B8B05B5FBA3000000000007	ECC	sha384ECDSA	9/28/2018 21:34	9/28/2033 21:44	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Unknown Key Usage (1.3.6.1.4.1.311.76.6.1)	9ac2f5ae2b21ef6c239eeddbeab84b4da520dc0d	C67E5F87209E33B857566DBF525FC0869EF8C715E5BA4A752DAE2A38DB16E14C
25	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	611244A2000000000002	RSA	sha256RSA	3/28/2011 21:09	3/28/2031 21:19	N/A	0	0F53CB3F166125FE60891DD3B97CE890ADB394D1	5A9D217E71180301A044E4CFBDE431FDF4C1CFC998B1B6343B5A10AA9E4CDE98
26	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=AOC CN=Microsoft Marketplace CA G 021	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	330000005C3AB23618FF8DF7B1000000000005C	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	5292df39da46425b8a6e6b1de33a43ac7ad5254b	2C9A040FCCAB13082EEBC3E2CE4023901EAF623D522F6D29C9B9788759A7C35D
27	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=AOC CN=Microsoft Marketplace CA G 022	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	33000000567DB266D0825D8B990000000000056	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	4782e488d37806f136d0d1f7818f1e1428240d4b	9F2C808A8705320E19FC4F34211C580667469B7033C40F239265249F792D6286
28	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=AOC CN=Microsoft Marketplace CA G 023	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	33000000570D7B1FC64FD44E7B000000000057	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	26dc3df5a3eb8950dbcb65c17db4b3a1238a5d97	DF0BCA1D35DDD79B1B7D7CFE769ADE9D2BCAA61766ED39CA1AD0DCCDF839C7F4
29	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=AOC CN=Microsoft Marketplace CA G 024	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	3300000053E45C4DC84039D4C0000000000053	RSA	sha256RSA	5/14/2019 18:51	5/14/2024 18:51	N/A	0	aa47be1b68e38ec4bac55ca1703ea61d9c2c1cf2	6466C53BCAA7631A2B932C6CA883CB7A6069AA15E0834D0F567E269EA56B4F33
29	2	C=US S=Washington L=Redmond O=Microsoft Corporation OU=AOC CN=Microsoft Marketplace CA G 024	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	3300000058E5873D5CF575E414000000000058	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	75151394260a61aec9fb8f914766a6bae680023d	14EC068F3D53E4B0FE038CBC416EBFE8E1CC728536EDEE9103EE69E729F7F3E4
30	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=EOC CN=Microsoft Marketplace CA G 025	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	33000000591BBEB16AF06B6A40000000000059	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	2bc8e3a408a6a0c5195c5bcc3ece5e70982f3d5c	F811DEA5AFCF25FBC3EEAB33918B83C3CE4A241B8445AC1123D65F8A84A32308
31	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=EOC CN=Microsoft Marketplace CA G 026	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	330000005B4E9A3269B8AD800D000000000005B	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	8e6f5ca466c1e11a8183c97d9ef5d246ed88216c	76B81CDC8C9C89EA598F3F7875F332FD9C0DE67B11743858569231 1706AF4E86
32	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=EOC CN=Microsoft Marketplace CA G 027	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	330000005A16D74E269F012BD400000000005A	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	3e7e0234a965526b487ad0d6806ec0df60e78b03	21EC00EA4D12FA20874663CF04DA6F63660CC1EBEB0E1D2C12F3D78CBBBCA9BA
33	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=EOC CN=Microsoft Marketplace CA G 028	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	33000000545A16CB93E5310AE8000000000054	RSA	sha256RSA	5/14/2019 18:51	5/14/2024 18:51	N/A	0	1280f52d7a2fe950e886076b5ef8a839b9f5785f	951D2F622C2B542C00F70E19833F15F880B113BD2D309B0643C0020DBD729A94
33	2	C=US S=Washington L=Redmond O=Microsoft Corporation OU=EOC CN=Microsoft Marketplace CA G 028	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	330000005D9F04EC95B702B46F00000000005D	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	1280f52d7a2fe950e886076b5ef8a839b9f5785f	12D43CDF626305E3A496CE63F27674FCB627AE4506A276E3EF3200BEEA129806
34	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Marketplace Production CA 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	3300000055C8066B38239729090000000000055	RSA	sha256RSA	9/9/2021 22:42	9/9/2030 22:52	N/A	0	74e66f4536729ab9b034c787052fd5eb61271c22	CA92943AB468CBB9604A97F909AE31C04577F5ADCBF7565F40C5837A072A5FE4
35	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Secure Server CA 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	613FB718000000000004	RSA	sha256RSA	10/18/2011 22:55	10/18/2026 23:05	N/A	0	3656896549CB5B9B2F3CAC4216504D91B933D791	83688F2AEF71386E0936C4B3013B07E8E0C796D8427716DD48B2A63D79509129
36	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Time Stamp CA 2015	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	3300000002F9FA0638351073C2000000000002	RSA	sha256RSA	3/25/2015 21:18	3/25/2030 21:28	N/A	0	212FBE3E2C5C9A59E5D5AD0BE971941D79515F84	857AEC60913116E2B61190B1E86FA001F27E8D165FAED492F829313E8212B666
37	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Time-Stamp PCA 2010	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	6109812A000000000002	RSA	sha256RSA	7/1/2010 21:36	7/1/2025 21:46	N/A	0	D5633A5C8A3190F3437B7C461BC533685A856D55	86EC118D1EE69670A46E2BE29C4B4208BE043E36600D4E1DD3F3D515CA119020
37	2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Time-Stamp PCA 2010	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	3300000015C5E76B9E029B4999000000000015	RSA	sha256RSA	9/30/2021 18:22	9/30/2030 18:32	N/A	Time Stamping (1.3.6.1.5.5.7.3.8)	D5633A5C8A3190F3437B7C461BC533685A856D55	EBEC1EDD9E140D9C105CC62B15A915C5443DDC514A35E5773C09AFB0274C7BA5
38	1	C=US O=Microsoft Corporation CN=Microsoft Update Metadata Signing CA 3.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000003E2DD309B9002F6FA9000000000003E	RSA	sha384RSA	3/13/2025 19:20	12/13/2035 19:30	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Unknown Key Usage (1.3.6.1.4.1.311.76.6.1)	ba9b5bc7b6ada704090c26a396d1a718894f903a	5CEF267491F3F59ED097124935155F51BD3756E32B7A432FE097EA170C5F339F
39	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Update Secure Server CA 2.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	330000000AB891A2C80A50A5DF000000000000A	RSA	sha256RSA	6/21/2012 17:33	6/21/2027 17:43	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	D2F23D8474861B5085AA5DE5A5079AF047D32E69	6139E2DF97DC93BF7E90A303F75B3968FD06C57316B45E94DCFF773707CF2754
40	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Update Secure Server CA 2.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000000B9AA76BB008015CF8000000000000B	RSA	sha256RSA	6/21/2012 19:22	6/21/2027 19:32	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	A4F291B745D77C968B35C8B6311AD4CAEFA5604C	C1BC7AC733DEC68A6A6AF944A5A2B4F79F492ABAACE213811F6EF681D7861B57

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
41	1	C=US O=Microsoft Corporation CN=Microsoft Update Secure Server CA 3.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000003B8123BBB6A0B4EB6B000000000003B	RSA	sha384RSA	3/13/2025 18:12	12/13/2035 18:22	N/A	0	34cf450d3a7fb272280e6056130e83607dea65c3	63E747F977AD8C8A0177004062E89AF20884610F4642EBD44589D2BEAC8E3EA2
42	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Update Signing CA 2.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	3300000007B1CC402755483F69000000000007	RSA	sha256RSA	6/19/2012 22:53	6/19/2027 23:03	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Unknown Key Usage (1.3.6.1.4.1.311.76.6.1)	AD94768F83AD0E03A3E83BB0D73468D4793A7DDC	882F36D6F0DABF4B017FC6E8EA6D4F0F2786300D7B8210C3AE5C793F95E1C0C9
43	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Update Signing CA 2.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000000859E394E054C7175D000000000008	RSA	sha256RSA	6/19/2012 22:53	6/19/2027 23:03	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Unknown Key Usage (1.3.6.1.4.1.311.76.6.1)	5D5D6BFB4B214A48BADA6752B96A3B8DC49155AD	24919D52EFB9ECBEC6C1D24CBC2E10D041B516B9410D6CEB75FF2F348BD0E5C8
44	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Update Signing CA 2.3	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000000D9528549AD55D42715000000000009	RSA	sha256RSA	6/19/2012 22:54	6/19/2027 23:04	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Unknown Key Usage (1.3.6.1.4.1.311.76.6.1)	D0F3FA5FF546F5CBB3D88FAE8F8CEC861CDF61C8	46B4D5B761CA7B14D4877C3B2D3F22DBF92BC34B694E971E942517DABEB4B06C
45	1	C=US O=Microsoft Corporation CN=Microsoft Update SIH Signing CA 3.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000003F207459BF58D59333000000000003F	RSA	sha384RSA	3/13/2025 19:36	12/13/2035 19:46	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Microsoft Trust List Signing (1.3.6.1.4.1.311.10.3.1), Root List Signer (1.3.6.1.4.1.311.10.3.9), Revoked List Signer (1.3.6.1.4.1.311.10.3.19)	b47e049719dfbf77f235edbb457d74d9818b0605	79475879DE5120750B09AD1D87DE80A93596130D8C5E7B3810A5CF707C3A3A19
46	1	C=US O=Microsoft Corporation CN=Microsoft Update SLS Signing CA 3.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000003C5595271D82CD0793000000000003C	RSA	sha384RSA	3/13/2025 18:37	12/13/2035 18:47	N/A	0	2ef850e59e729d830a2c2207b9049878e667b461	4A8FD639FD1F2A94F5F0710F3A2AA3C5E1E5D60AB2AB5618D24BA5A54B0F02B2
47	1	C=US O=Microsoft Corporation CN=Microsoft Update SLS Signing CA 3.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000003D86A3B33AD845F230000000000003D	RSA	sha384RSA	3/13/2025 19:04	12/13/2035 19:14	N/A	0	A92902398E16C49778CD90F99E4F9AE17C55AF53	B2625F512F768288485B2A7759B396BABE3D97199BDFD9D0E903DD06E3F9781C0
48	1	C=US O=Microsoft Corporation CN=Microsoft Windows Code Signing PCA 2024	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	330000001C489F81DFA1B0B777000000000001C	RSA	sha384RSA	8/8/2024 21:36	6/23/2035 22:04	N/A	0	1e82df0ed78cb3d70234830edaabad65b9afb8ec	3DADFAF812DD1BBAEF45834CCBD188F3CD97139E2ED1ACA69C2DD63082142F8F
49	1	C=US O=Microsoft Corporation CN=Microsoft Windows Component Preproduction CA 2024	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000003AE8F966B913AC7751000000000003A	RSA	sha384RSA	8/8/2024 22:07	3/22/2036 22:13	N/A	0	67223fe1b42ea930bfb409daedec03c0d0a44b48	B4065016A9886B3D56F94814A8BA391B50A28D3020C9054DE0AF9222C9FF3272
50	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Windows PCA 2010	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	610C6A19000000000004	RSA	sha256RSA	7/6/2010 20:40	7/6/2025 20:50	N/A	0	D14FA98A0708CEF4241898E500FFF3D6791D37BC	F01614A7A81BA477F0746CF2DE71B20DDDEC709E756C9EA57CB67F93F25BA9FD
51	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Windows Phone PCA 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	610B5C91000000000005	RSA	sha256RSA	2/28/2011 22:11	6/23/2035 22:04	N/A	0	FD399547DEEF1ACE48502070072F7EFE7E7468F5	AE378D79D44CC75CEE8BAE50DD8BCBF2D4FF7C598B62FE75C3CE234C4001AFD9
52	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Windows Phone Production PCA 2012	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	330000000BFCF98E584C1550BF000000000000B	RSA	sha256RSA	7/24/2012 22:23	7/24/2027 22:33	N/A	0	4498DF99096EB8D642212E9B9EDF266EC38E954B	E6A9B56A89AA3B191D23A6FB7FECB1F09DED4552A682FCF72B1D479C3B23C9BA
53	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Windows Phone Production PCA 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	61077656000000000008	RSA	sha256RSA	10/19/2011 18:41	10/19/2026 18:51	N/A	0	A92902398E16C49778CD90F99E4F9AE17C55AF53	E8E95F0733A55E8BAD7BE0A1413EE23C51FCEA64B3C8FA6A786935FDDCC71961
54	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Windows Third Party Component CA 2012	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	610BAAC1000000000009	RSA	sha256RSA	4/18/2012 23:48	4/18/2027 23:58	N/A	0	6171A787AFFF69D521764F52932800BE7912AB84	9D08973E4D108DA40A1A0B274180E17371134B4DD1621FA5C1F131B739B4B823
55	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Windows Third Party Component CA 2013	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	33000000149DFBC31F1F63C310000000000014	RSA	sha256RSA	5/1/2013 20:44	5/1/2028 20:54	N/A	0	7792047827B20B49077597EEE9EB5E265C094475	8EF01BB5E07987053659E039E5A72580C88C444BC1A31AB412CE81A4AD53044E
56	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Windows Third Party Component CA 2014	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000000D690D5D7893D076DF000000000000D	RSA	sha256RSA	10/15/2014 20:31	10/15/2029 20:41	N/A	0	C83A9CA74AC323F2257EB9DAAB29530E5400C3A1	A0F259A07039908EEB943E223FDF996E5E1E131D9AA6A602FF4672F7B9298AEE
57	1	C=US O=Microsoft Corporation CN=Microsoft Windows Third Party Component CA 2024	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	330000001B2DC28C2D7F55CC0B000000000001B	RSA	sha384RSA	8/8/2024 20:14	6/23/2035 22:04	N/A	0	1c649345e78c7ab68873cad7e9ad3c5052977b9e	86C83B2BBDCC9CD3C45F85AE11013B93F26BFE97D36B3695A863D163138CF48C
58	1	C=US O=Microsoft Corporation CN=VS Package Repositories CA	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	330000003876C4AEB839AAE393000000000038	RSA	sha384RSA	1/20/2022 19:46	3/22/2036 22:13	N/A	0	c101c3929cec3c609f99399a770838b5700383d5	AC415BBB3EE2E11B5EFD11808B8026B02736A82480C26AB7569FC19195344202
59	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Windows Azure StorSimple CA 2013	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000000C8CC7499215880C900000000000C	RSA	sha256RSA	10/15/2013 18:09	10/15/2028 18:19	N/A	0	c45e0e66efe4c73a33532a9c7e3986be1cc21f50	854B33F368F4D9BA80F4797D8E7150DC8754E7EF9E06ACBEC16F92C06E20DEBF
60	1	C=US O=Microsoft Corporation CN=Windows Production PCA 2023	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	3300000017 85BD56094BF8C821000000000017	RSA	sha384RSA	6/13/2023 18:34	6/13/2035 18:44	N/A	0	86ed0bae3f5a09d23d1e2119557f9f315322f800	4F771E28419476AF6791F116F65E963812EE85F841A8184E85F592BA3D51A4BF
61	1	C=US O=Microsoft Corporation CN=Windows UEFI CA 2023	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	330000001A888B9800562284C1000000000001A	RSA	sha256RSA	6/13/2023 18:58	6/13/2035 19:08	N/A	0	aefc5fbbbe055d8f8daa585473499417ab5a5272	076F1FEA90AC29155EBF77C17682F75F1FDD1BE196DA302DC8461E350A9AE330
62	1	C=US O=Microsoft Corporation CN=Microsoft ECC Update SIH Signing CA 3.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	330000000B51C891E4C25D195B000000000000B	ECC	sha384ECDSA	5/14/2025 18:31	5/14/2035 18:41	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Windows Update (1.3.6.1.4.1.311.76.6.1)	5647460ab47ea6dcfa68660af5d415e9f1ade3ec	4999A388B1EEB582C2EFC698B53832C8EFA4780F2E22F2D167F43CB561185D64
63	1	C=US O=Microsoft Corporation CN=Microsoft ECC Update SIH Signing CA 3.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	330000000CA807CE95DB1EAC4E000000000000C	ECC	sha384ECDSA	5/14/2025 19:21	5/14/2035 19:31	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Windows Update (1.3.6.1.4.1.311.76.6.1)	bce549c26e16ef08b5d2529f2d2c0dc082fb216b	1987938D55A9620A08EE0C07B183A33244A205D56E4A908AAE5107A21B477076
64	1	C=US O=Microsoft Corporation CN=Microsoft ECC Update Metadata Signing CA 3.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft	330000000D8DF141274A790FED000000000000D	ECC	sha384ECDSA	5/14/2025 19:50	5/14/2035 20:00	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Windows Update (1.3.6.1.4.1.311.76.6.1)	03158374881299fd1d93fba3a8a69061b5c58391	040465673A9CD31E2502966CA8F4A7E29C0C9740F1FB415A32984A29C2639A16

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
			ECC Product Root Certificate Authority 2018									
65	1	C=US O=Microsoft Corporation CN=Microsoft ECC Update Metadata Signing CA 3.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	330000000E47DE4BC44F2A7523000000000000E	ECC	sha384ECDSA	5/14/2025 20:17	5/14/2035 20:27	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Windows Update (1.3.6.1.4.1.311.76.6.1)	e41e6824aea275f3f1d60a8398501781e43c8eae	317B7AA4A5210C4E2687D1D6F8DFA389351D8B70CE6BC286C9601C8BA221366A
66	1	C=US O=Microsoft Corporation CN=Microsoft Update SLS Signing CA 3.3	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	33000000403A68CBD2FE3C5D17000000000040	RSA	sha384RSA	5/14/2025 20:44	12/14/2035 20:54	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Windows Update (1.3.6.1.4.1.311.76.6.1)	dab0c80606ce46b43efad276bc768c12c1be6925	A2FA09B8D81D1C5CE2425568B973FB05144DB97213B51A320B31D5EFBEC7D62D
67	1	C=US O=Microsoft Corporation CN=Microsoft Update Metadata Signing CA 3.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	33000000413B26B270125071BF000000000041	RSA	sha384RSA	5/14/2025 21:13	12/14/2035 21:23	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Windows Update (1.3.6.1.4.1.311.76.6.1)	dfb1fcf411c0982e5983342dc76307b909ea59c9	362AD926C3A4CCDF49E498779E7989F0FF766F759CEF8A679AEE9075000C568A
68	1	C=US O=Microsoft Corporation CN=Microsoft Update Secure Server CA 3.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	3300000042E9F495BE713B179E000000000042	RSA	sha384RSA	5/14/2025 21:36	12/14/2035 21:46	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	cdf81db6f42bce47a5b520c1b510a238ab55a073	3748B0AA073F4639BEC3DF60698CC38A4D5CD360D3346001943D32041356AABE
69	1	C=US O=Microsoft Corporation CN=Microsoft Update SIH Signing CA 3.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	33000000437FA0F1707E4C1F75000000000043	RSA	sha384RSA	5/14/2025 22:00	12/14/2035 22:10	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Windows Update (1.3.6.1.4.1.311.76.6.1)	b442d960df4706e8702a73bd419a61830a7c7d03	816FB2FBD75D47F0C33D0C7821C47AEFB5A61BB00B9B0B1E475ADC5F5961EDD0

ATTACHMENT B

LIST OF MS PKI SERVICES' CERTIFICATE POLICIES AND CERTIFICATION PRACTICE STATEMENTS

CP Name	Version	Date
Microsoft PKI Services Certificate Policy	3.2.0	April 20, 2026
Microsoft PKI Services Certificate Policy	3.1.9	April 21, 2025

CPS Name	Version	Date
Microsoft PKI Services Corporate Certification Practice Statement	3.2.0	April 20, 2026
Microsoft PKI Services Corporate Certification Practice Statement	3.1.9	April 21, 2025

ATTACHMENT C

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 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, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subordinate CA certification

The management of MS PKI Services 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, certificate lifecycle management controls, and subordinate CA 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 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 disclosures of its certificate practices and controls over its CA services. Based on that assessment, in MS PKI Services management's opinion, in providing its CA services at locations enumerated in Attachment C, MS PKI Services has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in the applicable versions of its Certificate Policies and Certification Practice Statements as enumerated in Attachment B
- maintained effective controls to provide reasonable assurance that
    - MS PKI Services' Certification Practice Statements are consistent with its Certificate Policies; and
    - MS PKI Services provides its services in accordance with its Certificate Policies and Certification Practice Statements
- 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 MS PKI Services); and
    - subordinate CA certificate requests are accurate, authenticated, and approved
- 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 May 1, 2025 to April 30, 2026 based on the WebTrust Principles and Criteria for Certification Authorities, v2.2.2, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certification Practice Statement Management
- Certificate Policy Management
- CP and CPS Consistency

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 Archival
- 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

Subordinate CA and Cross Certificate Lifecycle Management Controls

- Subordinate CA Certificate and Cross Certificate Lifecycle Management

MS PKI Services does not escrow its CA keys, does not provide subscriber key generation services, subscriber key storage and recovery services, or integrated circuit card lifecycle management for subscribers, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.

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

Sr.	Bugzilla ID	Bugzilla Title	Created On	Resolved On	Status
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: OCSP 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
16	2021175	Microsoft PKI Services: Failure to update action item status within 3 days	March 5, 2026	April 3, 2026	Resolved
17	2026452	Microsoft PKI Services: Failure to publish Full Incident Report for Bugzilla 2021175 within 14 days	March 26, 2026	April 22, 2026	Resolved
18	2026453	Microsoft PKI Services: Failure to report Bugzilla 2026452 within 72 hrs	March 26, 2026	April 22, 2026	Resolved
19	2034251	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 ECC Product Root Certificate Authority 2018
2. Microsoft ECC TS Root Certificate Authority 2018
3. Microsoft Root Certificate Authority 2010
4. Microsoft Root Certificate Authority 2011
5. Microsoft Root Certificate Authority 2014
6. Microsoft Time Stamp Root Certificate Authority 2014
Intermediate CA Certificates
7. Microsoft Azure Attestation PCA 2019
8. Microsoft Certificate List CA 2011
9. Microsoft Certificate List CA 2024
10. Microsoft Code Signing PCA 2010
11. Microsoft Code Signing PCA 2011
12. Microsoft Code Signing PCA 2024
13. Microsoft Content Distribution Secure Server CA 2.1
14. Microsoft Content Distribution Secure Server CA 2.2
15. Microsoft ECC Certificate List PCA 2018
16. Microsoft ECC Code Signing PCA 2018
17. Microsoft ECC Content Distribution Secure Server CA 2.1
18. Microsoft ECC Content Distribution Secure Server CA 2.2
19. Microsoft ECC Time Stamp PCA 2018
20. Microsoft ECC Update Secure Server CA 2.1
21. Microsoft ECC Update Secure Server CA 2.2
22. Microsoft ECC Update Signing CA 2.1
23. Microsoft ECC Update Signing CA 2.2
24. Microsoft ECC Update Signing CA 2.3
25. Microsoft MarketPlace PCA 2011
26. Microsoft Marketplace CA G 021
27. Microsoft Marketplace CA G 022
28. Microsoft Marketplace CA G 023
29. Microsoft Marketplace CA G 024
30. Microsoft Marketplace CA G 025
31. Microsoft Marketplace CA G 026
32. Microsoft Marketplace CA G 027
33. Microsoft Marketplace CA G 028
34. Microsoft Marketplace Production CA 2011
35. Microsoft Secure Server CA 2011
36. Microsoft Time Stamp CA 2015
37. Microsoft Time-Stamp PCA 2010
38. Microsoft Update Metadata Signing CA 3.1
39. Microsoft Update Secure Server CA 2.1
40. Microsoft Update Secure Server CA 2.2
41. Microsoft Update Secure Server CA 3.1
42. Microsoft Update Signing CA 2.1
43. Microsoft Update Signing CA 2.2
44. Microsoft Update Signing CA 2.3
45. Microsoft Update SIH Signing CA 3.1
46. Microsoft Update SLS Signing CA 3.1
47. Microsoft Update SLS Signing CA 3.2
48. Microsoft Windows Code Signing PCA 2024
49. Microsoft Windows Component Preproduction CA 2024
50. Microsoft Windows PCA 2010
51. Microsoft Windows Phone PCA 2011
52. Microsoft Windows Phone Production PCA 2012

53. Microsoft Windows Production PCA 2011
54. Microsoft Windows Third Party Component CA 2012
55. Microsoft Windows Third Party Component CA 2013
56. Microsoft Windows Third Party Component CA 2014
57. Microsoft Windows Third Party Component CA 2024
58. VS Package Repositories CA
59. Windows Azure StorSimple CA 2013
60. Windows Production PCA 2023
61. Windows UEFI CA 2023
62. Microsoft ECC Update SIH Signing CA 3.2
63. Microsoft ECC Update SIH Signing CA 3.1
64. Microsoft ECC Update Metadata Signing CA 3.1
65. Microsoft ECC Update Metadata Signing CA 3.2
66. Microsoft Update SLS Signing CA 3.3
67. Microsoft Update Metadata Signing CA 3.2
68. Microsoft Update Secure Server CA 3.2
69. Microsoft Update SIH Signing CA 3.2

ATTACHMENT B

LIST OF MS PKI SERVICES' CERTIFICATE POLICIES AND CERTIFICATION PRACTICE STATEMENTS

CP Name	Version	Date
Microsoft PKI Services Certificate Policy	3.2.0	April 20, 2026
Microsoft PKI Services Certificate Policy	3.1.9	April 21, 2025

CPS Name	Version	Date
Microsoft PKI Services Corporate Certification Practice Statement	3.2.0	April 20, 2026
Microsoft PKI Services Corporate Certification Practice Statement	3.1.9	April 21, 2025

ATTACHMENT C

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

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 at locations enumerated in Attachment C, for its CAs as enumerated in Attachment A, MS PKI Services has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of its Certificate Policies and Certification Practice Statements as enumerated in Attachment B
- maintained effective controls to provide reasonable assurance that
  - MS PKI Services' Certification Practice Statements are consistent with its Certificate Policies; and
  - MS PKI Services provides its services in accordance with its Certificate Policies and Certification Practice Statements
- 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 MS PKI Services); and
  - subordinate CA certificate requests are accurate, authenticated, and approved
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorised individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

throughout the period May 1, 2025 to April 30, 2026 based on the WebTrust Principles and Criteria for Certification Authorities, v2.2.2.

MS PKI Services does not escrow its CA keys, does not provide subscriber key generation services, subscriber key storage and recovery services, or integrated circuit card lifecycle management for subscribers, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.

Subscriber key-related services provided by Microsoft outside of the CA operations performed by MS PKI Services are out of scope. Additionally, 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, v2.2.2.

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, v2.2.2.

Practitioner's responsibilities

Our responsibility is to express an opinion on MS PKI Services 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.

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 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 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 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 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		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	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	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 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		a4430c7f765aa585e73e8d280f0c17a2456970c6	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	330000001631928D9202657B9A000000000016	RSA	sha384RSA	3/26/2026 18:11	3/26/2031 18:11	N/A		6b2541defb6b7cfd18800a2d7f8f765daa733db8	15CEF5F63CA6D1F022B293E92C61C0059C49BB92EECDBCDE3A125D3C6356D94F
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	3300000015053E6E198E9329D9000000000015	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	330000001727450908B8B87AFC6000000000017	RSA	sha384RSA	3/26/2026 18:11	3/26/2031 18:11	N/A		9af15477750c87163746a0acde79f9f47fc178e9	BC309555FA42C563B8EEBFB7117695C6BAE89E4BA19C03CB721979A563A60929
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	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

ATTACHMENT B

LIST OF MS PKI SERVICES' CERTIFICATE POLICIES AND CERTIFICATION PRACTICE STATEMENTS

CP Name	Version	Date
Microsoft PKI Services Certificate Policy	3.2.0	April 20, 2026
Microsoft PKI Services Certificate Policy	3.1.9	April 21, 2025

CPS Name	Version	Date
Microsoft PKI Services Third Party Certification Practice Statement	1.0.5	July 21, 2025
Microsoft PKI Services Third Party Certification Practice Statement	1.0.4	July 21, 2024

ATTACHMENT C

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 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, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subordinate CA certification

The management of MS PKI Services 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, certificate lifecycle management controls, and subordinate CA 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 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 disclosures of its certificate practices and controls over its CA services. Based on that assessment, in MS PKI Services management's opinion, in providing its CA services at locations enumerated in Attachment C, MS PKI Services has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in the applicable versions of its Certificate Policies and Certification Practice Statements as enumerated in Attachment B
- maintained effective controls to provide reasonable assurance that
    - MS PKI Services' Certification Practice Statements are consistent with its Certificate Policies; and
    - MS PKI Services provides its services in accordance with its Certificate Policies and Certification Practice Statements
- 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 MS PKI Services); and
    - subordinate CA certificate requests are accurate, authenticated, and approved
- 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 May 1, 2025 to April 30, 2026 based on the WebTrust Principles and Criteria for Certification Authorities, v2.2.2, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certification Practice Statement Management
- Certificate Policy Management
- CP and CPS Consistency

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 Archival
- 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

Subordinate CA and Cross Certificate Lifecycle Management Controls

- Subordinate CA Certificate and Cross Certificate Lifecycle Management

MS PKI Services does not escrow its CA keys, does not provide subscriber key generation services, subscriber key storage and recovery services, or integrated circuit card lifecycle management for subscribers, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.

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

Sr.	Bugzilla ID	Bugzilla Title	Created On	Resolved On	Status
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: OCSP 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
16	2021175	Microsoft PKI Services: Failure to update action item status within 3 days	March 5, 2026	April 3, 2026	Resolved
17	2026452	Microsoft PKI Services: Failure to publish Full Incident Report for Bugzilla 2021175 within 14 days	March 26, 2026	April 22, 2026	Resolved
18	2026453	Microsoft PKI Services: Failure to report Bugzilla 2026452 within 72 hrs	March 26, 2026	April 22, 2026	Resolved
19	2034251	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' CERTIFICATE POLICIES AND CERTIFICATION PRACTICE STATEMENTS

CP Name	Version	Date
Microsoft PKI Services Certificate Policy	3.2.0	April 20, 2026
Microsoft PKI Services Certificate Policy	3.1.9	April 21, 2025

CPS Name	Version	Date
Microsoft PKI Services Third Party Certification Practice Statement	1.0.5	July 21, 2025
Microsoft PKI Services Third Party Certification Practice Statement	1.0.4	July 21, 2024

ATTACHMENT C

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