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 TLS certificate lifecycle management business practices in its applicable version of Certificate Policies and Certification Practice Statements as enumerated on Attachment B, including its commitment to provide TLS certificates in conformity with the CA/Browser Forum Requirements on the MS PKI Services website, and provided such services in accordance with its disclosed practices.
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and TLS certificates it manages is established and protected throughout their lifecycles; and
  - TLS subscriber information is properly authenticated (for the registration activities performed by MS PKI Services)
- 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 - TLS Baseline, v2.9.

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 those services.

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

Certification authority's responsibilities

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 - TLS Baseline, v2.9.

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*. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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	**Subscriber certificate template change made that was not compliant with CPS**	As publicly disclosed in Bugzilla 1962830, certificate template change was made to a property that did not comply with the active CPS, and as such subscriber certificates that did not comply with the CPS were issued. The Bugzilla ticket was closed as RESOLVED on June 20, 2025.
2	**Typo in policy document**	As publicly disclosed in Bugzilla 1962829, CPS Version 3.2.4 included a copy and paste typo by incorrectly stating that keyEncipherment is not present in Subscriber certificates, which did not align with how MS PKI Services has been operating. The Bugzilla ticket was closed as RESOLVED on April 25, 2026.
3	**Certificate revocation reason code selection error**	As publicly disclosed in Bugzilla 1970968, Microsoft PKI Services selected the incorrect revocation reason code while revoking a batch of 25,000 certificates, intending to mark them as superseded but inadvertently marking them as affiliationChanged. The Bugzilla ticket was closed as RESOLVED on July 8, 2025.
4	**Intermediate CA issuance without required pre-sign linting**	As publicly disclosed in Bugzilla 1974592, Microsoft PKI Services issued five intermediate certificate authorities for public TLS use without required pre-sign linting validation, and no subscriber certificates were issued from the impacted ICAs. The Bugzilla ticket was closed as RESOLVED on August 28, 2025.
5	**Public TLS end entity certificate CPS compliance issue**	As publicly disclosed in Bugzilla 1979475, Microsoft PKI Services identified a compliance issue involving the issuance of Public TLS end entity certificates that did not conform with Microsoft CPS, including 784 certificates issued without the Basic Constraint extension. The Bugzilla ticket was closed as RESOLVED on January 20, 2026.
6	**Expired certificates on Microsoft sample site**	As disclosed in Bugzilla 2008847, Microsoft PKI Services identified that Sample Sites for two Root Certificates contained expired "valid" certificate samples and expired "revoked" certificate samples, resulting in noncompliance with Section 2.2 of the Baseline Requirements. The Bugzilla ticket was closed as RESOLVED on February 16, 2026.
7	**CCADB partitioned CRL metadata formatting issue**	As publicly disclosed Bugzilla 1990801, Microsoft PKI Services added twelve new CAs to CCADB, and one partitioned CRL metadata field for the Microsoft TLS G2 ECC CA OCSP 06 CA was incorrectly formatted because the CRL string was missing the required JSON array brackets.

	Matter topic	Matter description
		The Bugzilla ticket was closed as RESOLVED on November 3, 2025.
8	**Microsoft improper disclosure of partitioned CRL URLs**	As publicly disclosed Bugzilla 2007221, in September, Bugzilla 1990801 was opened after Microsoft identified that the JSON Array of Partitioned CRL URLs for one of the newly created CAs was incorrectly formatted, resulting in a Section 6.2 CCADB Policy violation. Microsoft initially disclosed the full CRL URL for the 12 affected CAs, but later determined that the JSON Array of Partitioned CRL URLs must be disclosed in CCADB for all twelve CAs. The Bugzilla ticket was closed as RESOLVED on March 2, 2026.
9	**Microsoft improper Disclosure of CRLs – IDP – Existing CAs**	As disclosed in Bugzilla 2009539, Microsoft PKI Services identified syntax issues with CRL URLs posted in CCADB for existing CAs transitioning from full CRLs to partitioned CRLs, which triggered a CRL Watch alert that the Issuing Distribution Point did not contain the expected URL. Microsoft reported the issue as a potential Section 6.2 CCADB Policy compliance matter, updated CCADB for the affected CA on June 8, 2026 to resolve the alert, and expects similar issues may arise as the remaining existing CAs are transitioned to partitioned CRLs. The Bugzilla ticket was closed as RESOLVED on February 16, 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 - TLS Baseline, v2.9.

Basis for qualified opinion

During our examination, we noted the following which caused a qualification of our opinion:

	Observation	Relevant WebTrust Criteria
1	As publicly disclosed in Bugzilla 1965612, 100,322,979 subscriber certificates were not issued in accordance with the active CPS v3.2.4, which misstated that keyEncipherment is not present in Subscriber certificates. The CA was unable to revoke impacted certificates within 5 days as required by the TLS Baseline Requirements 4.9.1.1 due to the technical limitations of creating large CRLs that would negatively impact client-side validation of certificates. This Bugzilla was RESOLVED on May 4, 2026. This caused WebTrust Principles and Criteria for Certification Authorities – TLS Baseline – Version 2.9 to not be met for Principle 2 - Criteria 5.2.	**P2-5.2:** The CA maintains controls to provide reasonable assurance that it: • has the capability to accept and acknowledge Certificate Problem Reports on a 24/7 basis; • identifies high-priority Certificate Problem Reports; • begins an investigation of Certificate Problem Reports within 24 hours and provides a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report; • decides whether revocation or other appropriate action is warranted; • **processes Certificate Problem Reports or revocation requests and revocation status information within the timelines in TLS Baseline Requirements 4.9.1.1; and** • where appropriate, forwards such complaints to law enforcement.

Qualified opinion

In our opinion, except for the matters described in the Basis for qualified opinion section of our report, MS PKI Services' assertion, as referred to above, is fairly stated, in all material respects.

Use of the Qualified Mark

MS PKI Services' use of the WebTrust for Certification Authorities Qualified Mark 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.

This report does not include any representation as to the quality of MS PKI 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.

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	949D6B4B761CA134AD3E7A85711186F580EE887F2C6B568B5140F4157F98D68DD
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	33000000007737DEB49D007DC64000000000007	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 TLS CA services.

MS PKI Service management has assessed its disclosures of its certificate practices and controls over TLS CA services. During our assessment, we noted the following observations which caused the relevant criteria to not be met:

	Observation	Relevant WebTrust Criteria
1	As publicly disclosed in Bugzilla 1965612, 100,322,979 subscriber certificates were not issued in accordance with the active CPS v3.2.4, which misstated that keyEncipherment is not present in Subscriber certificates. The CA was unable to revoke impacted certificates within 5 days as required by the TLS Baseline Requirements 4.9.1.1 due to the technical limitations of creating large CRLs that would negatively impact client-side validation of certificates. This Bugzilla was RESOLVED on May 4, 2026. This caused WebTrust Principles and Criteria for Certification Authorities – TLS Baseline – Version 2.9 to not be met for Principle 2 - Criteria 5.2.	**P2-5.2:** The CA maintains controls to provide reasonable assurance that it: • has the capability to accept and acknowledge Certificate Problem Reports on a 24/7 basis; • identifies high-priority Certificate Problem Reports; • begins an investigation of Certificate Problem Reports within 24 hours and provides a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report; • decides whether revocation or other appropriate action is warranted; • **processes Certificate Problem Reports or revocation requests and revocation status information within the timelines in TLS Baseline Requirements 4.9.1.1; and** • where appropriate, forwards such complaints to law enforcement.

Based on that assessment, in MS PKI Services management's opinion, except for the matters described in the preceding table, in providing its TLS Certification Authority (CA) services at locations enumerated in Attachment C, MS PKI Services has:

- disclosed its TLS certificate lifecycle management business practices in its applicable version of Certificate Policies and Certification Practice Statements as enumerated on Attachment B, including its commitment to provide TLS certificates in conformity with the CA/Browser Forum Requirements on the MS PKI Services website, and provided such services in accordance with its disclosed practices.
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and TLS certificates it manages is established and protected throughout their lifecycles; and
  - TLS subscriber information is properly authenticated (for the registration activities performed by MS PKI Services)
- 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 - TLS Baseline, v2.9.

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

Sr.	Bugzilla ID	Bugzilla Title	Created On	Resolved On	Status
4	1970968	Microsoft PKI Services: Incorrect Revocation Reason Code	June 6, 2025	July 8, 2025	Resolved
5	1974592	Microsoft PKI Services: Pre-Sign Linting Validation did not occur in ICA creation	June 28, 2025	August 30, 2025	Resolved
6	1979475	Microsoft PKI Services: End Entity Certificate Mis-issuance against CPS (BasicConstraints)	July 28, 2025	January 20, 2026	Resolved
7	1990801	Microsoft: improper disclosure of CRL	September 26, 2025	November 3, 2025	Resolved
8	1999850	Microsoft PKI Services: 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