

INDEPENDENT ACCOUNTANT'S REPORT

To the management of Microsoft Public Key Infrastructure Services ("MS PKI Services"):

Scope

We have examined MS PKI Services management's [assertion](#) that for its Certification Authority ("CA") operations in the United States of America, and in Ireland, for 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, 2024 to April 30, 2025, based on the [WebTrust Principles and Criteria for Certification Authorities - SSL Baseline, v2.8](#).

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. in [Attachment A](#), and are considered to be in scope of our examination.

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 - SSL Baseline, v2.8.

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 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 has not yet been resolved.
3	Subject Key Identifiers in some subscriber certificated do not comply	As publicly disclosed in Bugzilla 1944436 , there were multiple non-expired subscriber certificated issued with the same subjectKeyIdentifier value that did not comply with RFC 5280. The Bugzilla ticket was closed as RESOLVED on April 2, 2025.

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 SSL Baseline Requirements 4.9.1.1 due to the technical limitations of creating large CRLs that would negatively impact client-side validation of certificates.	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;

Observation	Relevant WebTrust Criteria
This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline – Version 2.8 to not be met for Principle 2 - Criteria 5.2.	• processes Certificate Problem Reports or revocation requests and revocation status information within the timelines in SSL 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 16, 2025

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
Intermediate CA Certificates
21. Microsoft ECC TLS Issuing AOC CA 01 22. Microsoft ECC TLS Issuing AOC CA 02 23. Microsoft ECC TLS Issuing EOC CA 01 24. Microsoft ECC TLS Issuing EOC CA 02 25. Microsoft RSA TLS Issuing AOC CA 01 26. Microsoft RSA TLS Issuing AOC CA 02 27. Microsoft RSA TLS Issuing EOC CA 01 28. Microsoft RSA TLS Issuing EOC CA 02

CA IDENTIFYING INFORMATION

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
1	1	C=US O=Microsoft Corporation CN=Microsoft ECC Root Certificate Authority 2017	N/AC=US O=Microsoft Corporation CN=Microsoft ECC Root Certificate Authority 2017	66F23DAF87DE8BB14AEA0C573101C2EC	RSA	sha384ECDSA	12/18/2019 23:06	7/18/2042 23:16	N/A		C8CB997270520CF8E68EB20457292ACF4210ED35	358DF39D764AF9E1B766E9C972DF352EE15C FAC227AF6AD1D70E8EA46EDCBA02
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	RSA	sha384ECDSA	7/26/2017s 22:22	7/26/2042 22:31	N/A		C8CB997270520CF8E68EB20457292ACF4210ED35	FEA1884AB3AEA6D0DBEDBE4B9CD9FEC8655 116300A86A856488FC488BB4B44D2
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		09CB597F86B2708F1AC339E3C0D9E98FBB4DB223	C741F70F4B2A8D88BF2E71C14122EF53EF10 EBA0CFA5E64CFA20F418853073E0
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		09CB597F86B2708F1AC339E3C0D9E98FBB4DB223	ECDD47B5ACBFA328211E1BFF54ADEAC95E6 991E3C1D50E27B527E903208040A1
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	6a170583db584151e1c454eca2a64c5d8e4 84a5bd1156e720b4458654ee9e5
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		de918648b7a1315931f14b5f07a9dc8879daa876	DDCD1E8A20638DAFAFF7201B81D56452ACD 2C759F1686BDC38F73DD15732BDC2
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	RSA	sha384RSA	4/10/2025 20:52	4/10/2040 20:58	N/A		6fab7edaff974372ec3b6777de82613588474285	87755cfe88bdb0d1099dcded3eae114ba976e 664b3248ee3dc649e357f17e8a7
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	RSA	sha384RSA	5/21/2025 00:00	6/19/2029 23:59	N/A		6fab7edaff974372ec3b6777de82613588474285	61799E3594F6FA6C9F619031E4A3C9F643FD A38C083704A5075E5709A21B1AB7
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	RSA	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)	AAFD300DD7A2D5EF8A7A7731AA66A6C26C11B86 F	949D6B48761CA134AD3E7A8571186F580EE8 87F2C6B56885140F4157F98D68DD
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	RSA	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)	AAFD300DD7A2D5EF8A7A7731AA66A6C26C11B86 F	2CAEFB855E70DF5A8985FE98C10DD56A40C 3DEDA83DA1530A29682015C5B7C66
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	RSA	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	9C64A9A4E3990E98FCE8317B2D4C1C07FFE 6E032DA8BB6D60A696E2FF038F1F
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	330000001B498D6736ED5612C200000000001B	RSA	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	4EC439672A44301A66E27947CC3B5897F13 2B667F712CC1A37018A3CC85816A
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	RSA	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	003F71DC4820216575FC5AACFE3B1AEB76F7 2AEA58B8E8CFEFC80B9F517AA4612
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	RSA	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	624D5576A652B2130768FE84B965EEFFFD9 1603D25CD5F7155A7DC2789DAC38
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	RSA	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	2975BAB51D00D862D0E16EEDEF8306A759C 65CD4B9F00DAF50ECDFCB4EC396E4
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	330000001D0913C309DA3F05A600000000001D	RSA	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	151A3E5969C661E6B637A8272B174CFD9538 7AACE78D57C3BD23F0CB3008186A
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	RSA	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	2EC9A5BA68B60F81E5F8662F7645743CCE1E DCE06AF686C775431F7BBB69ABD4
9	2	C = US O = Microsoft Corporation CN = Microsoft Azure ECC TLS Issuing CA 03	CN = DigiCert Global Root G3 OU = www.digicert.com O = DigiCert Inc C = US	01529ee8368f0b5d72ba433e2d8ea62d	RSA	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	BBD27139C5302C63D903F570F173AD4DC06 C974B9EBE292C90FFCAB85D6FA54E
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	33000000322164AEDAB61F509D0000000000032	RSA	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	4D0F5DA23B099209B048E1871B4BB1C4B4E 812E3FA0249BB8D19E00FFA9E918C
10	2	C=US O=Microsoft Corporation CN=Microsoft Azure ECC TLS Issuing CA 04	CN = DigiCert Global Root G3 OU = www.digicert.com O = DigiCert Inc C = US	02393d48d702425a7cb41c000b0ed7ca	RSA	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	7A3AE4F12920D5A8129BE1183FBEC4370EF1 0B8B3AD41EAE4A58D5385AA94D33
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	3300000034C732435DB22A0A2B0000000000034	RSA	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	BD3816423535DE993FA44A02F5562470C0CF B0D3B00532E3526A4A3AEC87522F
11	2	C=US O=Microsoft Corporation CN=Microsoft Azure ECC TLS Issuing CA 07	CN = DigiCert Global Root G3 OU = www.digicert.com O = DigiCert Inc C = US	0f1f157582cdc33734bdc5fcd941a33	RSA	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	8E23414A42E74886F7C72A861BA2DDDA017 5ED829223D894C5D272651FC0C189
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	3300000031526979844798BBB8000000000031	RSA	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	2C99B917B7A068578F7EFB4FB8E60B9CB5A0 E73BF300E0E1DC112E5654C5AE52
12	2	C=US O=Microsoft Corporation CN=Microsoft Azure ECC TLS Issuing CA 08	CN = DigiCert Global Root G3 OU = www.digicert.com O = DigiCert Inc C = US	0ef2e5d83681520255e92c608fbc2ff4	RSA	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	89AADE767B7BA43F8DDE8E9E74A2FCBBEA4 0D57155F7E1F2259C88835601FAED
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)	FE09714055051044D8A48175B89E1AE9A40688C8	3D3F4B440F933FFD269565EDA9E20E8DF863 C9CBE3651D3B476C5B4FAF5CE28

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	2	C=US O=Microsoft Corporation CN=Microsoft Azure RSA TLS Issuing CA 03	CN = DigiCert Global Root G2 OU = www.digicert.com O = DigiCert Inc C = US	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	9D1BC5D2DD75BF88B64F35E7F919E2546C225 BE888C1A8CBE82C0E9579234A7ED
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)	3B70D153E976259D60A8CA660FC69BAEF654166A	FD39FFC48F148354262162A2F55DD46DC256 4CFC1499309AD53F09C10981DCCA
14	2	C=US O=Microsoft Corporation CN=Microsoft Azure RSA TLS Issuing CA 04	CN = DigiCert Global Root G2 OU = www.digicert.com O = DigiCert Inc C = US	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)	3b70d153e976259d60a8ca660fc69baef654166a	33F9731BE910A66DC6ACD07D9D9CA212EE8 D0A9A5C78C8BF3E89BB74DF8FB936
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	330000003BF980B0C83783431700000000003B	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)	CE15163BEA02A3A66BDAD92BFDE58C52BE7A50A 8	F8B7926A451BADF516BE518614A77E6E325E 29819908796D807F59320F918EE2
15	2	C=US O=Microsoft Corporation CN=Microsoft Azure RSA TLS Issuing CA 07	CN = DigiCert Global Root G2 OU = www.digicert.com O = DigiCert Inc C = US	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	724247794951C93F3E41711617E95CE14326 3E3196C345A1DA78F6639749EC03
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	330000003A5DC2FFC321C16D9B00000000003A	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)	F67E2FBD80A34AB2705EBDF9A1FD8EDCA618007	CFDD061FCD4CFF3B8B9E133264CA7FDE45CA 49B70CFAA977AEODC422B4330A8C1
16	2	C=US O=Microsoft Corporation CN=Microsoft Azure RSA TLS Issuing CA 08	CN = DigiCert Global Root G2 OU = www.digicert.com O = DigiCert Inc C = US	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)	f67e2fbd80a34ab2705ebdf9a1fd8edca618007	511C1C41CB7EB2A10078C32C82F17925BA78 6DE46C633921D038F7409E15A5EA
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)	0F205DD7A15795D892CF2BD0C7C27704CE728076	24C7299864E0A2A6964F551C0E8DF2461532 FA8C48E4DBB86080716691F190E5
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	330000001DBE9496F3DB8B8DE700000000001D	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)	0F205DD7A15795D892CF2BD0C7C27704CE728076	0437AB2EC2C2B4890296C135034B21DB1464 34B8317EE703AA8AA943C5EA51AE
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	15A98761EBE011554DA3A46D206B0812CB2 EB69AE87AAA11A6DD4CB84ED5142A
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	D39CE39FF6F449D4F3391EE2004D705EC22F 99CFFCA40A88F85DB26454ADDBD1
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	D6831BA43607F5AC19778D627531562AF551 45F191CAB5EFAFA0E0005442B302
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	AB3203B3EA2017D509726A1D82293EFFCB8 C42CEB52C9AF1C0EE96B5C02BCBA
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	48FF8B494668C752304B48BF8E18758987DE F6582E5F09B921F4B60B83D6A8DD
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	3300000020A2F1491A37FBD31F0000000000020	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	7DF4D3EF45798F8C4384FC702BA52A44CE7B D6298B141628D4ABABC7678F6467
21	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	RSA	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)	315B89CE511B7CD1AA03C0EBED365DC29DD389E 1	5C6481731A8138DEA7D11C9AE8622891F945 EBA46825E7ABFE4754F0A6011AF8
22	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	RSA	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)	DEDCD76C239943EAAECDC8B71D185880364B8DF 4	808CA1ABBF2FF1A9AC71887DDA71FF6FCA 6C3B5224827F547515A4D9F7AF209
23	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	330000002A2D006485FDACBFEB000000000002A	RSA	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	2769381532D96183ED39BDC4E323F3C520FB E6ACF3BDA30222239DDFC44C8380
24	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	RSA	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	659C0F902D6059FBD1FCA528839F20604B80 C74364E58F9D48A2291F813ED82D
25	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	330000002FFAF06F6697E2469C000000000002F	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)	EB4C317C3D3F32B883D7C5DB7BDAE478DA9C145 7	481E582A206A7D7040CCDA17CF25D349785 A2AB94ED7552AB254DCD388032EC0
26	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	3300000030C756CC88F5C1E7EB0000000000030	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	D77C45C1587731C4632C19D6F3C9FE832626 615C879EA053664A4826EB2293EC
27	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	33000000310C4914B18C8F339A0000000000031	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	5EA3857EACD4C7CA5ACBCA9C4627E26F307 2038D191A29D4C3F9464B2E5F00C6
28	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	330000003244AD7521341496A90000000000032	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	4D558C4ABE87D37FAB5E7573ACCE83133E3 6212C864E003FBCB30B5FC248B011

ATTACHMENT B

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

CP Name	Version	Date
Microsoft PKI Services Certificate Policy	3.1.9	April 21, 2025
Microsoft PKI Services Certificate Policy	3.1.8	July 21, 2024
Microsoft PKI Services Certificate Policy	3.1.7	July 27, 2023

CPS Name	Version	Date
Microsoft PKI Services Public TLS Certification Practice Statement	3.3.1	April 29, 2025
Microsoft PKI Services Public TLS Certification Practice Statement	3.3.0	April 21, 2025
Microsoft PKI Services Certification Practice Statement	3.2.4	July 21, 2024
Microsoft PKI Services Certification Practice Statement	3.2.3	July 27, 2023

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 SSL 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 caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline – Version 2.8 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 SSL 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 the United States of America, and in Ireland, 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, 2024 to April 30, 2025, based on the [WebTrust Principles and Criteria for Certification Authorities - SSL Baseline, v2.8](#).

Microsoft Public Key Infrastructure Services
July 16, 2025

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
Intermediate CA Certificates
21. Microsoft ECC TLS Issuing AOC CA 01 22. Microsoft ECC TLS Issuing AOC CA 02 23. Microsoft ECC TLS Issuing EOC CA 01 24. Microsoft ECC TLS Issuing EOC CA 02 25. Microsoft RSA TLS Issuing AOC CA 01 26. Microsoft RSA TLS Issuing AOC CA 02 27. Microsoft RSA TLS Issuing EOC CA 01 28. Microsoft RSA TLS Issuing EOC CA 02

ATTACHMENT B

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

CP Name	Version	Date
Microsoft PKI Services Certificate Policy	3.1.9	April 21, 2025
Microsoft PKI Services Certificate Policy	3.1.8	July 21, 2024
Microsoft PKI Services Certificate Policy	3.1.7	July 27, 2023

CPS Name	Version	Date
Microsoft PKI Services Public TLS Certification Practice Statement	3.3.1	April 29, 2025
Microsoft PKI Services Public TLS Certification Practice Statement	3.3.0	April 21, 2025
Microsoft PKI Services Certification Practice Statement	3.2.4	July 21, 2024
Microsoft PKI Services Certification Practice Statement	3.2.3	July 27, 2023