Deloitte.

Deloitte & Touche LLP
1015 2nd Ave, Suite 500
Seattle, WA 98104
Tel: +1 206 716 7000
Fax: +1 206 965 7000
www.deloitte.com

INDEPENDENT ACCOUNTANT'S REPORT

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

Scope

We have examined MS PKI Services management's assertion that for its Certification Authority ("CA") operations in the United States of America, and in Ireland, for its CAs as enumerated in Attachment A, MS PKI Services has:

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

throughout the period May 1, 2023 to April 30, 2024 based on the WebTrust Principles and Criteria for Certification Authorities, v2.2.2.

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

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

Certification authority's responsibilities

MS PKI Services' management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities, v2.2.2.

Practitioner's responsibilities

Our responsibility is to express an opinion on MS PKI Services management's assertion based on our examination. Our examination was conducted in accordance with AT-C Section 205, *Assertion-Based Examination Engagements*, established by the American Institute of Certified Public Accountants and International Standard on Assurance Engagements ("ISAE") 3000, *Assurance Engagements Other Than Audits Or Reviews Of Historical Financial Information*. This standard requires that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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.

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. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

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.

Other matters

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

	Matter topic	Matter description
1	**Access to High Security Zone was granted to non-trusted personnel**	As publicly disclosed in Bugzilla 1848279 and 1848280, a non-trusted role user was granted access to High Security Zone from August 2, 2023 until August 9, 2023. Both Bugzilla tickets were closed as RESOLVED on October 12, 2023.
2	**OCSP Responder does not know a Certificate**	As publicly disclosed in Bugzilla 1879552, 101 certificates were issued without being published to the OCSP responder. The Bugzilla ticket was closed as RESOLVED on March 29, 2024.
3	**CA Certificates not published in DER Encoded Format**	As publicly disclosed in Bugzilla 1884461, 8 certificates, which were published on July 7, 2023, pointed to a PEM encoded certificate, instead of a DER encoded certificate that was required by RFC 5280 Section 4.2.2.1. The Bugzilla ticket was closed as RESOLVED on April 5, 2024.
4	**CRL Publication Failures**	As publicly disclosed in Bugzilla 1842121, 24 CRLS were published with value of the nextUpdate field more than ten days beyond the value of the thisUpdate field, causing a delay of CRL publication. The Bugzilla ticket was closed as RESOLVED on September 29, 2023.

Practitioner's opinion

In our opinion, management's assertion, as referred to above, is fairly stated, in all material respects.

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

Use of the WebTrust seal

MS PKI Services' use of the WebTrust for Certification Authorities Seal constitutes a symbolic representation of the contents of this report, and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

Deloitte & Touche LLP

Deloitte & Touche LLP
July 05, 2024

ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs
1. Microsoft ECC Root Certificate Authority 2017
2. Microsoft RSA Root Certificate Authority 2017
Cross-signed CA Certificates
3. Microsoft Azure ECC TLS Issuing CA 01
4. Microsoft Azure ECC TLS Issuing CA 02
5. Microsoft Azure ECC TLS Issuing CA 05
6. Microsoft Azure ECC TLS Issuing CA 06
7. Microsoft Azure ECC TLS Issuing CA 03
8. Microsoft Azure ECC TLS Issuing CA 04
9. Microsoft Azure ECC TLS Issuing CA 07
10. Microsoft Azure ECC TLS Issuing CA 08
11. Microsoft Azure RSA TLS Issuing CA 03
12. Microsoft Azure RSA TLS Issuing CA 04
13. Microsoft Azure RSA TLS Issuing CA 07
14. Microsoft Azure RSA TLS Issuing CA 08
15. Microsoft Azure TLS Issuing CA 01
16. Microsoft Azure TLS Issuing CA 02
17. Microsoft Azure TLS Issuing CA 05
18. Microsoft Azure TLS Issuing CA 06
Intermediate CA Certificates
19. Microsoft ECC TLS Issuing AOC CA 01
20. Microsoft ECC TLS Issuing AOC CA 02
21. Microsoft ECC TLS Issuing EOC CA 01
22. Microsoft ECC TLS Issuing EOC CA 02
23. Microsoft RSA TLS Issuing AOC CA 01
24. Microsoft RSA TLS Issuing AOC CA 02
25. Microsoft RSA TLS Issuing EOC CA 01
26. 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		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	RSA	sha384ECDSA	7/26/2017 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 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)	AAFD300DD7A2D5EF8A7A7731AA66A6C26C11BB6F	949D6B4B761CA134AD3E7A8571186F580EE887F2C6B568B5140F4157F98D68DD
3	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)	AAFD300DD7A2D5EF8A7A7731AA66A6C26C11BB6F	2CAEFBB55E70DF5A8985FE9BC10DD56A40C3DEDAB3DA1530A29682015C5B7C66
4	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	9C64A9A43E990E98FBCE8317B2D4C1C07FFE6E032DA8BB6D60A696E2FF038F1F
4	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	4EC439672A443401A66E27947CC3B5897F132B667F712CC1A37018A3CC85B16A
5	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	003F71DC4820216575FC5AACFE3B1AEB76F72AEA5B8E8FCEFC80B9F517A4A612
5	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	330000001CC0D2A3CD78CF2C100000000001C	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	624D5576A652B2130768BFE84B965EEFFFD91603D25CD5F7155A7DC2789DAC38
6	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	2975BAB51D00D862D0E16EEDEF8306A759C65CD4B9F00DAF50ECDFCB4EC396E4
6	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	151A3E5969C6616EB637A8722B174CFD95387AACE78D57C3BD23F0CB3008186A
7	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	2EC9A5BA68B60F81E5F8662F7645743CCE1EDCE06AF686C775431F7BBB69ABD4
7	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	BBD27139C5302C63D903F570F173AD4DC06C974B9EBE292C90FFCCAB5D6FA54E
8	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	33000000322164AEDAB61F509D000000000032	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	4D0F5DA23B099209B048E1871B4BB1C4B4E812E3FA0249BB8D19E00FFA9E91BC
8	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	7A3AE4F12920D5A8129BE1183FBEC4370EF10B8B3AD41EAE4A58D5385AA94D33
9	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	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	BD3816423553ED993FA44A02F5562470C0CFB0D3B00532E3526A4A3AEC87522F
9	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	0f1f157582cdcd33734bdc5fcd941a33	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	BE23414A42E74886E7C72A861BA2DDDA0175ED829223D894C5D272651FC0C189
10	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	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	2C99B917B7A068578F7EFB4FB8E60B9CB5A0E73BF300E0E1DC112E5654C5AE52
10	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	89AADE767B7BA43F8DDE8E9E74A2FCBBEA40D57155F7E1F2259C88835601FAED
11	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
11	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	9D1BC5D2DD75BF8B64F35E7F919E2546C225BE888C1A8CBE82C0E9579234A7ED
12	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	330000003CD7CB44EE579961D00000000003C	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
12	2	C=US O=Microsoft Corporation CN=Microsoft Azure RSA TLS Issuing CA 04	CN = DigiCert Global Root G2 OU = www.digicert.com	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

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
			O = DigiCert Inc C = US									
13	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
13	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	724247794951C93F3E41711617E95CE143263E3196C345A1DA78F6639749EC03
14	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)	F67E2FBD80A34AB2705BEBDF9A1FD8EDCA618007	CFDD061FCD4CFF3BB9E133264CA7FDE45CA49B70CFAA977AE0DC422B4330A8C1
14	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)	f67e2fbd80a34ab2705bebdf9a1fd8edca618007	511C1C41CB7EB2A10078C32C82F17925BA786DE46C633921D038E7409E15A5EA
15	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
15	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)	0F205DD7A15795DB92CF2BD0C7C27704CE728076	0437AB2EC2C2B4890296C135034B21DB146434B8317EE703AA8AA943C5EA51AE
16	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
16	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
17	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
17	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
18	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
18	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
19	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)	315BB9CE511B7CD1AA03C0EBED365DC29DD389E1	5C64B1731A8138DEA7D11C9AE8622891F945EBA46825E7ABFE4754F0A6011AF8
20	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)	DEDCD76C239943EAACEDC8B71D185880364B8DF4	808CA1ABBFE2FF1A9AC71887DDA71FF6FCA6C3B5224827F547515A4D9F7AF209
21	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	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	2769381532D96183ED39BDC4E323F3C520FBE6ACF3BDA30222239DDFC44C8380
22	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	330000002BE6902838672B667900000000002B	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	659C0F902D6059FBD1FCA528839F20604B80C74364E58F9D48A2291F813ED82D
23	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
24	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
25	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
26	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

ATTACHMENT B

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

CP Name	Version	Date
Microsoft PKI Services Certificate Policy	3.1.7	July 27, 2023
Microsoft PKI Services Certificate Policy	3.1.6	February 22, 2023

CPS Name	Version	Date
Microsoft PKI Services Certification Practice Statement	3.2.3	July 27, 2023
Microsoft PKI Services Certification Practice Statement	3.2.2	February 22, 2023

Microsoft

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

MICROSOFT PUBLIC KEY INFRASTRUCTURE SERVICES MANAGEMENT'S ASSERTION

Microsoft Public Key Infrastructure Services ("MS PKI Services") operates the Certification Authority ("CA") services as enumerated in Attachment A, and provides the following CA services:

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

The management of MS PKI Services is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to MS PKI Services' CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

MS PKI Services management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in MS PKI Services management's opinion, in providing its CA services in the United States of America, and in Ireland, MS PKI Services has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in the applicable versions of its Certificate Policies and Certification Practice Statements as enumerated in Attachment B
- maintained effective controls to provide reasonable assurance that
    - MS PKI Services' Certification Practice Statements are consistent with its Certificate Policies; and
    - MS PKI Services provides its services in accordance with its Certificate Policies and Certification Practice Statements
- maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
    - subscriber information is properly authenticated (for the registration activities performed by MS PKI Services); and
    - subordinate CA certificate requests are accurate, authenticated, and approved
- maintained effective controls to provide reasonable assurance that:
    - logical and physical access to CA systems and data is restricted to authorized individuals;
    - the continuity of key and certificate management operations is maintained; and
    - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

throughout the period May 1, 2023 to April 30, 2024 based on the WebTrust Principles and Criteria for Certification Authorities, v2.2.2, including the following:

CA Business Practices Disclosure

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

CA Business Practices Management

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

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- System Development, Maintenance, and Change Management
- Disaster Recovery, Backups, and Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Transportation
- CA Key Migration

Subscriber Key Lifecycle Management Controls

- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA and Cross Certificate Lifecycle Management Controls

- Subordinate CA Certificate and Cross Certificate Lifecycle Management

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

Microsoft Public Key Infrastructure Services
July 05, 2024

ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs
1. Microsoft ECC Root Certificate Authority 2017 2. Microsoft RSA Root Certificate Authority 2017
Cross-signed CA Certificates
3. Microsoft Azure ECC TLS Issuing CA 01 4. Microsoft Azure ECC TLS Issuing CA 02 5. Microsoft Azure ECC TLS Issuing CA 05 6. Microsoft Azure ECC TLS Issuing CA 06 7. Microsoft Azure ECC TLS Issuing CA 03 8. Microsoft Azure ECC TLS Issuing CA 04 9. Microsoft Azure ECC TLS Issuing CA 07 10. Microsoft Azure ECC TLS Issuing CA 08 11. Microsoft Azure RSA TLS Issuing CA 03 12. Microsoft Azure RSA TLS Issuing CA 04 13. Microsoft Azure RSA TLS Issuing CA 07 14. Microsoft Azure RSA TLS Issuing CA 08 15. Microsoft Azure TLS Issuing CA 01 16. Microsoft Azure TLS Issuing CA 02 17. Microsoft Azure TLS Issuing CA 05 18. Microsoft Azure TLS Issuing CA 06
Intermediate CA Certificates
19. Microsoft ECC TLS Issuing AOC CA 01 20. Microsoft ECC TLS Issuing AOC CA 02 21. Microsoft ECC TLS Issuing EOC CA 01 22. Microsoft ECC TLS Issuing EOC CA 02 23. Microsoft RSA TLS Issuing AOC CA 01 24. Microsoft RSA TLS Issuing AOC CA 02 25. Microsoft RSA TLS Issuing EOC CA 01 26. 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	3.1.7	July 27, 2023
Microsoft PKI Services Certificate Policy	3.1.6	February 22, 2023

CPS Name	Version	Date
Microsoft PKI Services Certification Practice Statement	3.2.3	July 27, 2023
Microsoft PKI Services Certification Practice Statement	3.2.2	February 22, 2023

Deloitte & Touche LLP
1015 2nd Ave, Suite 500
Seattle, WA 98104
Tel: +1 206 716 7000
Fax: +1 206 965 7000
www.deloitte.com

INDEPENDENT ACCOUNTANT'S REPORT

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

Scope

We have examined MS PKI Services management's assertion that for its Certification Authority ("CA") operations in the United States of America, and in Ireland, for its CAs as enumerated in Attachment A, MS PKI Services has:

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

throughout the period May 1, 2023 to April 30, 2024 based on the WebTrust Principles and Criteria for Certification Authorities, v2.2.2.

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

Subscriber key-related services provided by Microsoft outside of the CA operations performed by MS PKI Services are out of scope. Additionally, there are other CA hierarchies and PKI operations across Microsoft that are not managed by MS PKI services. These CA hierarchies and PKI operations are not in the scope of this examination, and this opinion does not extend to these services.

Certification authority's responsibilities

MS PKI Services' management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities, v2.2.2.

Practitioner's responsibilities

Our responsibility is to express an opinion on MS PKI Services management's assertion based on our examination. Our examination was conducted in accordance with AT-C Section 205, *Assertion-Based Examination Engagements*, established by the American Institute of Certified Public Accountants, and International Standard on Assurance Engagements ("ISAE") 3000, *Assurance Engagements Other Than Audits Or Reviews Of Historical Financial Information*. This standard requires that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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.

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. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

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**.**

Other matters

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

	Matter topic	Matter description
1	**Access to High Security Zone was granted to non-trusted personnel**	As publicly disclosed in Bugzilla 1848279 and 1848280, a non-trusted role user was granted access to High Security Zone from August 2, 2023 until August 9, 2023. Both Bugzilla tickets were closed as RESOLVED on October 12, 2023.

Opinion

In our opinion management's assertion, as referred to above, is fairly stated, in all material respects.

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

Use of the WebTrust seal

MS PKI Services' use of the WebTrust for Certification Authorities Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

Deloitte & Touche LLP

Deloitte & Touche LLP
July 05, 2024

ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs
1. Microsoft Identity Verification Root Certificate Authority 2020
Intermediate CAs
2. Microsoft ID Verified Code Signing PCA 2021 3. Microsoft ID Verified CS AOC CA 01 4. Microsoft ID Verified CS AOC CA 02 5. Microsoft ID Verified CS EOC CA 01 6. Microsoft ID Verified CS EOC CA 02 7. Microsoft RSA Document Signing CA 2023
Timestamp Authority CA
8. Microsoft Public RSA Timestamping CA 2020

CA IDENTIFYING INFORMATION

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
1	1	C=US O=Microsoft Corporation CN=Microsoft Identity Verification Root Certificate Authority 2020	C=US O=Microsoft Corporation CN=Microsoft Identity Verification Root Certificate Authority 2020	5498D2D1D45B1995481379C811C08799	RSA	sha384RSA	4/16/2020 18:36	4/16/2045 18:44	N/A		C87ED26A852A1BCA1998040727CF50104F68A8A2	5367F20C7ADE0E2BCA790915056D086B720C33C1FA2A2661ACF787E3292E1270
2	1	C=US O=Microsoft Corporation CN=Microsoft ID Verified Code Signing PCA 2021	C=US O=Microsoft Corporation CN=Microsoft Identity Verification Root Certificate Authority 2020	330000000787A334A37BA58E1C000000000007	RSA	sha384RSA	4/1/2021 20:05	4/1/2036 20:15	N/A		d94129b00f0f636cef69d7f5cd299ea4486a30e6	3D29798CC5D3F0644A7E0DC9CB1CADE523EA5EC83B335109B605BFEAA7D5F5C1
3	1	C=US O=Microsoft Corporation CN=Microsoft ID Verified CS AOC CA 01	C=US O=Microsoft Corporation CN=Microsoft ID Verified Code Signing PCA 2021	3300000007378C5BA1D95B8CD4000000000007	RSA	sha384RSA	4/13/2021 17:31	4/13/2026 17:31	N/A		e883c433d7dc9f0c9c769a0aa6d4df87a65e58ee	7EE1F718CAE6B4D25D10115A367D84B7704E06BD6F8B498825FD42C852574BE9
4	1	C=US O=Microsoft Corporation CN=Microsoft ID Verified CS AOC CA 02	C=US O=Microsoft Corporation CN=Microsoft ID Verified Code Signing PCA 2021	330000000496504BD2DBEECB88000000000004	RSA	sha384RSA	4/13/2021 17:31	4/13/2026 17:31	N/A		244599a177902a7cc3ca83b06e6416842af82c67	E82D27596C5DDF9F11E8B6981F5D018211BF2580F0619E5954BAD400175F38D0
5	1	C=US O=Microsoft Corporation CN=Microsoft ID Verified CS EOC CA 01	C=US O=Microsoft Corporation CN=Microsoft ID Verified Code Signing PCA 2021	33000000064A1AFACF05616A74000000000006	RSA	sha384RSA	4/13/2021 17:31	4/13/2026 17:31	N/A		769c367413d1907d615fb302eb80f4994ba53e85	2FAA1C92228D5A05E07BAECFAA365F90A9B2F2DD846B014AE95880BAC3A976BB
6	1	C=US O=Microsoft Corporation CN=Microsoft ID Verified CS EOC CA 02	C=US O=Microsoft Corporation CN=Microsoft ID Verified Code Signing PCA 2021	3300000005FB7A5C321361DF5D000000000005	RSA	sha384RSA	4/13/2021 17:31	4/13/2026 17:31	N/A		659f51ce85687f2f8a4588aadda731bb1e0d005e	B96CCAB201048A0AC2BA07AEA08D6DBEEA1688F55380A369B14A7BE11AEF828D
7	1	C=US O=Microsoft Corporation CN=Microsoft RSA Document Signing CA 2023	C=US O=Microsoft Corporation CN=Microsoft Identity Verification Root Certificate Authority	330000000D7FC27C5865F33126000000000000D	RSA	sha384RSA	2/23/2023 22:46	2/23/2038 22:56	N/A		e005eb7a28bbb2d8701eefde69e9862c2c015f16	0E5A11A91688D904D2B7DAFC679545DE958B5C6BED175CF9F1F5FE0FCE2881D0
8	1	C=US O=Microsoft Corporation CN=Microsoft Public RSA Timestamping CA 2020	C=US O=Microsoft Corporation CN=Microsoft Identity Verification Root Certificate Authority 2020	3300000005E5CF0FFF662EC987000000000005	RSA	sha384RSA	11/19/2020 20:32	11/19/2035 20:42	N/A	Time Stamping (1.3.6.1.5.5.7.3.8)	6B69283A352F486340CF7BD8AF49E93ED93DDB21	36E731CFA9BFD69DAFB643809F6DEC500902F7197DAEAAD86EA0159A2268A2B8

ATTACHMENT B

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

CP Name	Version	Date
Microsoft PKI Services Certificate Policy	3.1.7	July 27, 2023
Microsoft PKI Services Certificate Policy	3.1.6	February 22, 2023

CPS Name	Version	Date
Microsoft PKI Services Third Party Certification Practice Statement	1.0.2	May 22, 2023
Microsoft PKI Services Third Party Certification Practice Statement	1.0.1	February 15, 2022

Microsoft

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

MICROSOFT PUBLIC KEY INFRASTRUCTURE SERVICES MANAGEMENT'S ASSERTION

Microsoft Public Key Infrastructure Services ("MS PKI Services") operates the Certification Authority ("CA") services as enumerated in Attachment A, and provides the following CA services:

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

The management of MS PKI Services is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to MS PKI Services' CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

MS PKI Services management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in MS PKI Services management's opinion, in providing its CA services in the United States of America, and in Ireland, MS PKI Services has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in the applicable versions of its Certificate Policies and Certification Practice Statements as enumerated in Attachment B
- maintained effective controls to provide reasonable assurance that
  - MS PKI Services' Certification Practice Statements are consistent with its Certificate Policies; and
  - MS PKI Services provides its services in accordance with its Certificate Policies and Certification Practice Statements
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by MS PKI Services); and
  - subordinate CA certificate requests are accurate, authenticated, and approved
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

throughout the period May 1, 2023 to April 30, 2024 based on the WebTrust Principles and Criteria for Certification Authorities, v2.2.2, including the following:

CA Business Practices Disclosure

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

CA Business Practices Management

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

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- System Development, Maintenance, and Change Management
- Disaster Recovery, Backups, and Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Transportation
- CA Key Migration

Subscriber Key Lifecycle Management Controls

- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA and Cross Certificate Lifecycle Management Controls

- Subordinate CA Certificate and Cross Certificate Lifecycle Management

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

Microsoft Public Key Infrastructure Services
July 05, 2024

ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs
1. Microsoft Identity Verification Root Certificate Authority 2020
Intermediate CAs
2. Microsoft ID Verified Code Signing PCA 2021 3. Microsoft ID Verified CS AOC CA 01 4. Microsoft ID Verified CS AOC CA 02 5. Microsoft ID Verified CS EOC CA 01 6. Microsoft ID Verified CS EOC CA 02 7. Microsoft RSA Document Signing CA 2023
Timestamp Authority CA
8. Microsoft Public RSA Timestamping CA 2020

ATTACHMENT B

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

CP Name	Version	Date
Microsoft PKI Services Certificate Policy	3.1.7	July 27, 2023
Microsoft PKI Services Certificate Policy	3.1.6	February 22, 2023

CPS Name	Version	Date
Microsoft PKI Services Third Party Certification Practice Statement	1.0.2	May 22, 2023
Microsoft PKI Services Third Party Certification Practice Statement	1.0.1	February 15, 2022

Deloitte.

Deloitte & Touche LLP
1015 2nd Ave, Suite 500
Seattle, WA 98104
Tel: +1 206 716 7000
Fax: +1 206 965 7000
www.deloitte.com

INDEPENDENT ACCOUNTANT'S REPORT

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

Scope

We have examined MS PKI Services management's assertion that for its Certification Authority ("CA") operations in the United States of America, and in Ireland, for its CAs as enumerated in Attachment A, MS PKI Services has:

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

throughout the period May 1, 2023 to April 30, 2024 based on the WebTrust Principles and Criteria for Certification Authorities, v2.2.2.

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

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

Certification authority's responsibilities

MS PKI Services' management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities, v2.2.2.

Practitioner's responsibilities

Our responsibility is to express an opinion on MS PKI Services management's assertion based on our examination. Our examination was conducted in accordance with AT-C Section 205, *Assertion-Based Examination Engagements*, established by the American Institute of Certified Public Accountants, and International Standard on Assurance Engagements ("ISAE") 3000, *Assurance Engagements Other Than Audits Or Reviews Of Historical Financial Information*. This standard requires that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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.

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. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

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.

Other matters

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

	Matter topic	Matter description
1	**Access to High Security Zone was granted to non-trusted personnel**	As publicly disclosed in Bugzilla 1848279 and 1848280, a non-trusted role user was granted access to High Security Zone from August 2, 2023 until August 9, 2023. Both Bugzilla tickets were closed as RESOLVED on October 12, 2023.

Opinion

In our opinion management's assertion, as referred to above, is fairly stated, in all material respects.

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

Use of the WebTrust seal

MS PKI Services' use of the WebTrust for Certification Authorities Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

Deloitte & Touche LLP

Deloitte & Touche LLP
July 05, 2024

ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs

1. Microsoft ECC Product Root Certificate Authority 2018
2. Microsoft ECC TS Root Certificate Authority 2018
3. Microsoft Root Certificate Authority 2010
4. Microsoft Root Certificate Authority 2011
5. Microsoft Root Certificate Authority 2014
6. Microsoft Time Stamp Root Certificate Authority 2014

Intermediate CA Certificates

7. Microsoft Azure Attestation PCA 2019
8. Microsoft Certificate List CA 2011
9. Microsoft Code Signing PCA 2010
10. Microsoft Code Signing PCA 2011
11. Microsoft Content Distribution Secure Server CA 2.1
12. Microsoft Content Distribution Secure Server CA 2.2
13. Microsoft ECC Certificate List PCA 2018
14. Microsoft ECC Code Signing PCA 2018
15. Microsoft ECC Content Distribution Secure Server CA 2.1
16. Microsoft ECC Content Distribution Secure Server CA 2.2
17. Microsoft ECC Time Stamp PCA 2018
18. Microsoft ECC Update Secure Server CA 2.1
19. Microsoft ECC Update Secure Server CA 2.2
20. Microsoft ECC Update Signing CA 2.1
21. Microsoft ECC Update Signing CA 2.2
22. Microsoft ECC Update Signing CA 2.3
23. Microsoft MarketPlace PCA 2011
24. Microsoft Marketplace CA G 021
25. Microsoft Marketplace CA G 022
26. Microsoft Marketplace CA G 023
27. Microsoft Marketplace CA G 024
28. Microsoft Marketplace CA G 025
29. Microsoft Marketplace CA G 026
30. Microsoft Marketplace CA G 027
31. Microsoft Marketplace CA G 028
32. Microsoft Marketplace Production CA 2011
33. Microsoft Secure Server CA 2011
34. Microsoft Time Stamp CA 2015
35. Microsoft Time-Stamp PCA 2010
36. Microsoft Update Secure Server CA 2.1
37. Microsoft Update Secure Server CA 2.2
38. Microsoft Update Signing CA 2.1
39. Microsoft Update Signing CA 2.2
40. Microsoft Update Signing CA 2.3
41. Microsoft Windows PCA 2010
42. Microsoft Windows Phone PCA 2011
43. Microsoft Windows Phone Production PCA 2012
44. Microsoft Windows Production PCA 2011
45. Microsoft Windows Third Party Component CA 2012
46. Microsoft Windows Third Party Component CA 2013
47. Microsoft Windows Third Party Component CA 2014
48. VS Package Repositories CA
49. Windows Azure StorSimple CA 2013
50. Windows Production PCA 2023
51. Windows UEFI CA 2023

CA IDENTIFYING INFORMATION

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
1	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	14982666DC7CCD8F4053677BB999EC85	ECC	sha384ECDSA	2/27/2018 20:42	2/27/2043 20:50	N/A	0	43EF7087B89DBFEC8819DCC6C46B750D75343308	CACA93B9D23D2B6FA76E8B8471931E0DF3EC6F63AF3CDBB936C41954A1872326
2	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC TS Root Certificate Authority 2018	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC TS Root Certificate Authority 2018	153875E1647ED1B047B4EFAF41128245	ECC	sha384ECDSA	2/27/2018 20:51	2/27/2043 21:00	N/A	0	E847C8429AB09DAE6F0B283B98158FE3B1E880B2	3FD4BE8BAAD2F26E1BDE06C7584BB720DD1A972D111F5A4999BC44B08FB4960D
2	2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC TS Root Certificate Authority 2018	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC TS Root Certificate Authority 2018	'330000001498434745943178490000000000014	ECC	sha384ECDSA	28/9/2018 17:55	9/6/2035 17:55	N/A	Time Stamping (1.3.6.1.5.5.7.3.8)	E847C8429AB09DAE6F0B283B98158FE3B1E880B2	D4D27BC233F38B4414617E72871F54D40758AB988072D9FFEC31AEDA60ECC6D0
3	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	28CC3A25BFBA44AC449A9B586B4339AA	RSA	sha256RSA	6/23/2010 21:57	6/23/2035 22:04	N/A	0	D5F656CB8FE8A25C6268D13D94905BD7CE9A18C4	DF545BF919A2439C36983B54CDFC903DFA4F37D3996D8D84B4C31EEC6F3C163E
4	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	3F8BC8B5FC9FB29643B569D66C42E144	RSA	sha256RSA	3/22/2011 22:05	3/22/2036 22:13	N/A	0	722D3A02319043B914054EE1EAA7C731D1238934	847DF6A78497943F27FC72EB93F9A637320A02B561D0A91B09E87A7807ED7C61
5	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2014	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2014	5586A39A5F38DFB24A7B48D1B491FFF3	RSA	sha256RSA	10/22/2014 21:00	10/22/2039 21:01	N/A	0	11d6d4f06236a01ee769835aad7db41527b79945	B13DDACB6431E702356A0002730B933C65272F9180D53BCD4577F8D500680A42
6	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Time Stamp Root Certificate Authority 2014	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Time Stamp Root Certificate Authority 2014	2FD67A432293329045E953343EE27466	RSA	sha256RSA	10/22/2014 22:08	10/22/2039 22:15	N/A	0	CBD1F2CE48FD019FEA56AA57D17E9958F83FFFE0	65AF95F4BE86847344634282F941B2E605063EF0C8542F014CA088D182109E4F
6	2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Time Stamp Root Certificate Authority 2014	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Time Stamp Root Certificate Authority 2014	33000000112BF711003F3F012A000000000011	RSA	sha256RSA	11/8/2016 21:01	22/6/2035 21:01	N/A	Time Stamping (1.3.6.1.5.5.7.3.8)	CBD1F2CE48FD019FEA56AA57D17E9958F83FFFE0	A303E478DD3CBC0E47A290FD5B59AF5C017A95E4886EC354EC6DA8B9380EE399
7	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Azure Attestation PCA 2019	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	3300000037756C792A2979DF3D000000000037	RSA	sha256RSA	5/30/2019 22:48	5/30/2034 22:58	N/A	0	ad475e6ccfa9d55a75355dfa28a17578289f71ad	D8A4236A2BD59061D008139D2071EA7BEF642E1B959A0CE6626666B43BD2C095
8	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Certificate List CA 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	61116C92000000000007	RSA	sha256RSA	3/29/2011 18:58	3/29/2026 19:08	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Microsoft Trust List Signing (1.3.6.1.4.1.311.10.3.1), Root List Signer (1.3.6.1.4.1.311.10.3.9), Revoked List Signer (1.3.6.1.4.1.311.10.3.19)	41F021C7EDC487FA8375FF0A0CDC2DECA86AAB59	A53A400DF29EC7B8C8FCE7CFFFE47334F43B1642E604DD0307491737EBBC00CE
9	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Code Signing PCA 2010	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	610C524C000000000003	RSA	sha256RSA	7/6/2010 20:40	7/6/2025 20:50	N/A	0	E6FC5F7BBB220058E4724EB5F421742332E6EFAC	9AAD6C1A83A1B974BA574A995AF35B8CA772DA919270DB1605A8B81E1BBC896F
10	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Code Signing PCA 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	610E90D2000000000003	RSA	sha256RSA	7/8/2011 20:59	7/8/2026 21:09	N/A	0	486E64E55005D382AA17373722B56DA8CA750295	56DA8722AFD94066FFE1E4595473A4854892B843A0827D53FB7D8F4AEED1E18B
11	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Content Distribution Secure Server CA 2.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	3300000035D47483932E18187C000000000035	RSA	sha256RSA	12/7/2018 20:12	12/7/2033 20:22	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	DEAA37759FD493A715504C4578E761BA37027F4B	64EBAE10EF707ECF156B560A1C9236455A5E9F1C16F270996E41D5F0DFEDA561
12	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Content Distribution Secure Server CA 2.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	3300000036A26D4F583DFDC113000000000036	RSA	sha256RSA	12/7/2018 20:12	12/7/2033 20:22	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	84D6BFD9B25E9D87E3B2C0864CD39CC168B60E67	B90776868F9AA9F0048D2BBEC85908CD2735A36BACB5886AF5C3458303703471
13	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Certificate List PCA 2018	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	33000000037742B6E32092D50F000000000003	ECC	sha384ECDSA	3/1/2018 21:40	3/1/2033 21:50	N/A	0	7aa29b3c3676b7033c6ccf439e509c86758055ce	C307C2757F1026AA755DC7830E43C61BA30BFE178FB9F92B621B830B3DA21C83
14	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Code Signing PCA 2018	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	3300000002B2A4C58304AEE1E1000000000002	ECC	sha384ECDSA	3/1/2018 21:40	3/1/2033 21:50	N/A	0	862aaefa129e681f41ad660d486b1a707ff7c5c8	E673905E74CCA3307C5E2C7D1E78DCA1F6F2783A21F8B02B58472E304C680DB8
15	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Content Distribution Secure Server CA 2.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	3300000009066CB601E4418E73000000000009	ECC	sha384ECDSA	12/7/2018 20:05	12/7/2033 20:15	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	455478B823ACADE42A8CBB014152B49C8E8191EE	E39F93F3B2B40FD3C41DE7DFA7D0B0CB6C4D8F97CBAB2BB81C178F4B5F3C7EED
16	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Content Distribution Secure Server CA 2.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	330000000ADB1A07295C828D770000000000000A	ECC	sha384ECDSA	12/7/2018 20:05	12/7/2033 20:15	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	D3C732531923973ECA3FFC83992F92CB3CD3D2C0	959D932A756F59612F2D757926D8AD3B11CB2684CA9203AE281F5CC26049BE94
17	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Time Stamp PCA 2018	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC TS Root Certificate Authority 2018	330000000278C1161CA7F6D350000000000002	ECC	sha384ECDSA	3/1/2018 21:48	3/1/2033 21:58	N/A	0	e8674bb61257af7710de403357646afc23e54881	5E72BC836123C6EA5DE54A3697DE416EE167C2AC62C7C89F61BEB89C735160A7
18	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Update Secure Server CA 2.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	3300000004A1F5B5883D3F0022000000000004	ECC	sha384ECDSA	9/28/2018 21:34	9/28/2033 21:44	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	1641B107C78BF3D2061490260ADBB12BC04462C3	21158AD4DCE10197239A87EBEB4D8D47E9E9BE716AD497A2E036774CAF5072CF
19	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Update Secure Server CA 2.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	33000000087B3662C012063EB4000000000008	ECC	sha384ECDSA	12/7/2018 20:05	12/7/2033 20:15	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	9dea50acb6663e22781d9640142b719e31c6d8c4	6345FD68446C011FD442A04A37E8407A51E548DE61A6685633134EDD67292F1A

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
20	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Update Signing CA 2.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	33000000051A3AE66A9EE4F897000000000005	ECC	sha384ECDSA	9/28/2018 21:34	9/28/2033 21:44	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Unknown Key Usage (1.3.6.1.4.1.311.76.6.1)	D2465153A49F6324F2E8D2B2AB854C9E32FFD852	73DF319F3BF18FA9C9D0B38DAABA98038C4F867D3C9CE609737DFA682BDA1FFB
21	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Update Signing CA 2.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	3300000006DEA087FB82845B90000000000006	ECC	sha384ECDSA	9/28/2018 21:34	9/28/2033 21:44	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Unknown Key Usage (1.3.6.1.4.1.311.76.6.1)	0478de0ab9f5c19eaa7c890c02a50d9f7546a76f	3EBC65CCB963BAA55AFA2F0D24A20044C7D17D97208EA2B318778C505CB7C08F
22	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Update Signing CA 2.3	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	3300000007E8141B8B05B5FBA3000000000007	ECC	sha384ECDSA	9/28/2018 21:34	9/28/2033 21:44	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Unknown Key Usage (1.3.6.1.4.1.311.76.6.1)	9ac2f5ae2b21ef6c239eeddbeab84b4da520dc0d	C67E5F87209E33B857566DBF525FC0869EF8C715E5BA4A752DAE2A38DB16E14C
23	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	611244A2000000000002	RSA	sha256RSA	3/28/2011 21:09	3/28/2031 21:19	N/A	0	0F53CB3F166125FE60891DD3B97CE890ADB394D1	5A9D217E71180301A044E4CFBDE431FDF4C1CFC998B1B6343B5A10AA9E4CDE98
24	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=AOC CN=Microsoft Marketplace CA G 021	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	330000005C3AB23618FF8DF7B100000000005C	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	5292df39da46425b8a6e6b1de33a43ac7ad5254b	2C9A040FCCAB13082EEBC3E2CE4023901EAF623D522F6D29C9B9788759A7C35D
25	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=AOC CN=Microsoft Marketplace CA G 022	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	33000000567DB266D0825D8B99000000000056	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	4782e488d37806f136d0d1f7818f1e1428240d4b	9F2C808A8705320E19FC4F34211C580667469B7033C40F239265249F792D6286
26	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=AOC CN=Microsoft Marketplace CA G 023	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	33000000570D7B1FC64FD44E7B000000000057	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	26dc3df5a3eb8950dbcb65c17db4b3a1238a5d97	DF0BCA1D35DDD79B1B7D7CFE769ADE9D2BCAA61766ED39CA1AD0DCCDF839C7F4
27	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=AOC CN=Microsoft Marketplace CA G 024	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	3300000053E45C4DC84039D4C0000000000053	RSA	sha256RSA	5/14/2019 18:51	5/14/2024 18:51	N/A	0	aa47be1b68e38ec4bac55ca1703ea61d9c2c1cf2	6466C53BCAA7631A2B932C6CA883CB7A6069AA15E0834D0F567E269EA56B4F33
27	2	C=US S=Washington L=Redmond O=Microsoft Corporation OU=AOC CN=Microsoft Marketplace CA G 024	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	3300000058E5873D5CF575E414000000000058	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	75151394260a61aec9fb8f914766a6bae680023d	14EC068F3D53E4B0FE038CBC416EBFE8E1CC728536EDEE9103EE69E729F7F3E4
28	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=EOC CN=Microsoft Marketplace CA G 025	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	33000000591BBEB16AF06B6A40000000000059	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	2bc8e3a408a6a0c5195c5bcc3ece5e70982f3d5c	F811DEA5AFCF25FBC3EEAB33918B83C3CE4A241B8445AC1123D65F8A84A32308
29	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=EOC CN=Microsoft Marketplace CA G 026	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	330000005B4E9A3269B8AD800D00000000005B	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	8e6f5ca466c1e11a8183c97d9ef5d246ed88216c	76B81CDC8C9C89EA598F3F7875F332FD9C0DE67B117438585692311706AF4E86
30	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=EOC CN=Microsoft Marketplace CA G 027	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	330000005A16D74E269F012BD400000000005A	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	3e7e0234a965526b487ad0d6806ec0df60e78b03	21EC00EA4D12FA20874663CF04DA6F63660CC1EBEB0E1D2C12F3D78CBBBCA9BA
31	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=EOC CN=Microsoft Marketplace CA G 028	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	33000000545A16CB93E5310AE8000000000054	RSA	sha256RSA	5/14/2019 18:51	5/14/2024 18:51	N/A	0	1280f52d7a2fe950e886076b5ef8a839b9f5785f	951D2F622C2B542C00F70E19833F15F880B113BD2D309B0643C0020DBD729A94
31	2	C=US S=Washington L=Redmond O=Microsoft Corporation OU=EOC CN=Microsoft Marketplace CA G 028	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	330000005D9F04EC95B702B46F00000000005D	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	1280f52d7a2fe950e886076b5ef8a839b9f5785f	12D43CDF626305E3A496CE63F27674FCB627AE4506A276E3EF3200BEEA129806
32	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Marketplace Production CA 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	3300000055C8066B38239729090000000000055	RSA	sha256RSA	9/9/2021 22:42	9/9/2030 22:52	N/A	0	74e66f4536729ab9b034c787052fd5eb61271c22	CA92943AB468CBB9604A97F909AE31C04577F5ADCBF7565F40C5837A072A5FE4
33	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Secure Server CA 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft MarketPlace PCA 2011	613FB718000000000004	RSA	sha256RSA	10/18/2011 22:55	10/18/2026 23:05	N/A	0	3656896549CB5B9B2F3CAC4216504D91B933D791	83688F2AEF71386E0936C4B3013B07E8E0C796D8427716DD48B2A63D79509129
34	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Time Stamp CA 2015	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	3300000002F9FA0638351073C2000000000002	RSA	sha256RSA	3/25/2015 21:18	3/25/2030 21:28	N/A	0	212FBE3E2C5C9A59E5D5AD0BE971941D79515F84	857AEC60913116E2B61190B1E86FA001F27E8D165FAED492F829313E8212B666
35	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Time-Stamp PCA 2010	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	6109812A000000000002	RSA	sha256RSA	7/1/2010 21:36	7/1/2025 21:46	N/A	0	D5633A5C8A3190F3437B7C461BC533685A856D55	86EC118D1EE69670A46E2BE29C4B4208BE043E36600D4E1DD3F3D515CA119020
35	2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Time-Stamp PCA 2010	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	3300000015C5E76B9E029B4999000000000015	RSA	sha256RSA	9/30/2021 18:22	9/30/2030 18:32	N/A	Time Stamping (1.3.6.1.5.5.7.3.8)	D5633A5C8A3190F3437B7C461BC533685A856D55	EBEC1EDD9E140D9C105CC62B15A915C5443DDC514A35E5773C09AFB0274C7BA5
36	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Update Secure Server CA 2.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	330000000AB891A2C80A50A5DF00000000000A	RSA	sha256RSA	6/21/2012 17:33	6/21/2027 17:43	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	D2F23D8474861B5085AA5DE5A5079AF047D32E69	6139E2DF97DC93BF7E90A303F75B3968FD06C57316B45E94DCFF773707CF2754
37	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Update Secure Server CA 2.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000000B9AA76BB008015CF800000000000B	RSA	sha256RSA	6/21/2012 19:22	6/21/2027 19:32	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	A4F291B745D77C968B35C8B6311AD4CAEFA5604C	C1BC7AC733DEC68A6A6AF944A5A2B4F79F492ABAACE213811F6EF681D7861B57
38	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Update Signing CA 2.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	3300000007B1CC402755483F69000000000007	RSA	sha256RSA	6/19/2012 22:53	6/19/2027 23:03	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Unknown Key Usage (1.3.6.1.4.1.311.76.6.1)	AD94768F83AD0E03A3E83BB0D73468D4793A7DDC	882F36D6F0DABF4B017FC6E8EA6D4F0F2786300D7B8210C3AE5C793F95E1C0C9
39	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Update Signing CA 2.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000000859E394E054C7175D000000000008	RSA	sha256RSA	6/19/2012 22:53	6/19/2027 23:03	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Unknown Key Usage (1.3.6.1.4.1.311.76.6.1)	5D5D6BFB4B214A48BADA6752B96A3B8DC49155AD	24919D52EFB9ECBEC6C1D24CBC2E10D041B516B9410D6CEB75FF2F348BD0E5C8
40	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Update Signing CA 2.3	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	3300000009528549AD55D42715000000000009	RSA	sha256RSA	6/19/2012 22:54	6/19/2027 23:04	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Unknown Key Usage (1.3.6.1.4.1.311.76.6.1)	D0F3FA5FF546F5CBB3D88FAE8F8CEC861CDF61C8	46B4D5B761CA7B14D4877C3B2D3F22DBF92BC34B694E971E942517DABEB4B06C

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
41	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Windows PCA 2010	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	610C6A19000000000004	RSA	sha256RSA	7/6/2010 20:40	7/6/2025 20:50	N/A	0	D14FA98A0708CEF4241898E500FFF3D6791D37BC	F01614A7A81BA477F0746CF2DE71B20DDDEC709E756C9EA57CB67F93F25BA9FD
42	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Windows Phone PCA 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	610B5C91000000000005	RSA	sha256RSA	2/28/2011 22:11	6/23/2035 22:04	N/A	0	FD399547DEEF1ACE48502070072F7EFE7E7468F5	AE378D79D44CC75CEE8BAE50DD8BCBF2D4FF7C598B62FE75C3CE234C4001AFD9
43	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Windows Phone Production PCA 2012	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	330000000BFCF98E584C1550BF00000000000B	RSA	sha256RSA	7/24/2012 22:23	7/24/2027 22:33	N/A	0	4498DF99096EB8D642212E9B9EDF266EC38E954B	E6A9B56A89AA3B191D23A6FB7FECB1F09DED4552A682FCF72B1D479C3B23C9BA
44	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Windows Production PCA 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	61077656000000000008	RSA	sha256RSA	10/19/2011 18:41	10/19/2026 18:51	N/A	0	A92902398E16C49778CD90F99E4F9AE17C55AF53	E8E95F0733A55E8BAD7BE0A1413EE23C51FCEA64B3C8FA6A786935FDDCC71961
45	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Windows Third Party Component CA 2012	CN=AP Root Certificate Authority 2013	610BAAC1000000000009	RSA	sha256RSA	4/18/2012 23:48	4/18/2027 23:58	N/A	0	6171A787AFFF69D521764F52932800BE7912AB84	9D08973E4D108DA40A1A0B274180E17371134B4DD1621FA5C1F131B739B4B823
46	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Windows Third Party Component CA 2013	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	33000000149DFBC31F1F63C310000000000014	RSA	sha256RSA	5/1/2013 20:44	5/1/2028 20:54	N/A	0	7792047827B20B49077597EEE9EB5E265C094475	8EF01BB5E07987053659E039E5A72580C88C444BC1A31AB412CE81A4AD53044E
47	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Windows Third Party Component CA 2014	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000000D690D5D7893D076DF00000000000D	RSA	sha256RSA	10/15/2014 20:31	10/15/2029 20:41	N/A	0	C83A9CA74AC323F2257EB9DAAB29530E5400C3A1	A0F259A07039908EEB943E223FDF996E5E1E131D9AA6A602FF4672F7B9298AEE
48	1	C=US O=Microsoft Corporation CN=VS Package Repositories CA	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	330000003876C4AEB839AAE393000000000038	RSA	sha384RSA	1/20/2022 19:46	3/22/2036 22:13	N/A	0	c101c3929cec3c609f99399a770838b5700383d5	AC415BBB3EE2E11B5EFD11808B8026B02736A82480C26AB7569FC19195344202
49	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Windows Azure StorSimple CA 2013	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000000C8CC7499215880C9000000000000C	RSA	sha256RSA	10/15/2013 18:09	10/15/2028 18:19	N/A	0	c45e0e66efe4c73a33532a9c7e3986be1cc21f50	854B33F368F4D9BA80F4797D8E7150DC8754E7EF9E06ACBEC16F92C06E20DEBF
50	1	C=US O=Microsoft Corporation CN=Windows Production PCA 2023	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	330000001785BD56094BF8C821000000000017	RSA	sha384RSA	6/13/2023 18:34	6/13/2035 18:44	N/A	0	86ed0bae3f5a09d23d1e2119557f9f315322f800	4F771E28419476AF6791F116F65E963812EE85F841A8184E85F592BA3D51A4BF
51	1	C=US O=Microsoft Corporation CN=Windows UEFI CA 2023	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	330000001A888B9800562284C100000000001A	RSA	sha256RSA	6/13/2023 18:58	6/13/2035 19:08	N/A	0	aefc5fbbbe055d8f8daa585473499417ab5a5272	076F1FEA90AC29155EBF77C17682F75F1FDD1BE196DA302DC8461E350A9AE330

ATTACHMENT B

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

CP Name	Version	Date
Microsoft PKI Services Certificate Policy	3.1.7	July 27, 2023
Microsoft PKI Services Certificate Policy	3.1.6	February 22, 2023

CPS Name	Version	Date
Microsoft PKI Services Corporate Certification Practice Statement	3.1.7	May 22, 2023
Microsoft PKI Services Corporate Certification Practice Statement	3.1.6	Jan 19, 2022

Microsoft

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

MICROSOFT PUBLIC KEY INFRASTRUCTURE SERVICES MANAGEMENT'S ASSERTION

Microsoft Public Key Infrastructure Services ("MS PKI Services") operates the Certification Authority ("CA") services as enumerated in Attachment A, and provides the following CA services:

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

The management of MS PKI Services is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to MS PKI Service's CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

MS PKI Services management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in MS PKI Services management's opinion, in providing its CA services in the United States of America, and in Ireland, MS PKI Services has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in the applicable versions of its Certificate Policies and Certification Practice Statements as enumerated in Attachment B
- maintained effective controls to provide reasonable assurance that
  - MS PKI Services' Certification Practice Statements are consistent with its Certificate Policies; and
  - MS PKI Services provides its services in accordance with its Certificate Policies and Certification Practice Statements
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by MS PKI Services); and
  - subordinate CA certificate requests are accurate, authenticated, and approved
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

Throughout the period May 1, 2023 to April 30, 2024 based on the WebTrust Principles and Criteria for Certification Authorities, v2.2.2, including the following:

CA Business Practices Disclosure

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

CA Business Practices Management

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

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- System Development, Maintenance, and Change Management
- Disaster Recovery, Backups, and Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Transportation
- CA Key Migration

Subscriber Key Lifecycle Management Controls

- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA and Cross Certificate Lifecycle Management Controls

- Subordinate CA Certificate and Cross Certificate Lifecycle Management

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

Microsoft Public Key Infrastructure Services
July 05, 2024

ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs

1. Microsoft ECC Product Root Certificate Authority 2018
2. Microsoft ECC TS Root Certificate Authority 2018
3. Microsoft Root Certificate Authority 2010
4. Microsoft Root Certificate Authority 2011
5. Microsoft Root Certificate Authority 2014
6. Microsoft Time Stamp Root Certificate Authority 2014

Intermediate CA Certificates

7. Microsoft Azure Attestation PCA 2019
8. Microsoft Certificate List CA 2011
9. Microsoft Code Signing PCA 2010
10. Microsoft Code Signing PCA 2011
11. Microsoft Content Distribution Secure Server CA 2.1
12. Microsoft Content Distribution Secure Server CA 2.2
13. Microsoft ECC Certificate List PCA 2018
14. Microsoft ECC Code Signing PCA 2018
15. Microsoft ECC Content Distribution Secure Server CA 2.1
16. Microsoft ECC Content Distribution Secure Server CA 2.2
17. Microsoft ECC Time Stamp PCA 2018
18. Microsoft ECC Update Secure Server CA 2.1
19. Microsoft ECC Update Secure Server CA 2.2
20. Microsoft ECC Update Signing CA 2.1
21. Microsoft ECC Update Signing CA 2.2
22. Microsoft ECC Update Signing CA 2.3
23. Microsoft MarketPlace PCA 2011
24. Microsoft Marketplace CA G 021
25. Microsoft Marketplace CA G 022
26. Microsoft Marketplace CA G 023
27. Microsoft Marketplace CA G 024
28. Microsoft Marketplace CA G 025
29. Microsoft Marketplace CA G 026
30. Microsoft Marketplace CA G 027
31. Microsoft Marketplace CA G 028
32. Microsoft Marketplace Production CA 2011
33. Microsoft Secure Server CA 2011
34. Microsoft Time Stamp CA 2015
35. Microsoft Time-Stamp PCA 2010
36. Microsoft Update Secure Server CA 2.1
37. Microsoft Update Secure Server CA 2.2
38. Microsoft Update Signing CA 2.1
39. Microsoft Update Signing CA 2.2
40. Microsoft Update Signing CA 2.3
41. Microsoft Windows PCA 2010
42. Microsoft Windows Phone PCA 2011
43. Microsoft Windows Phone Production PCA 2012
44. Microsoft Windows Production PCA 2011
45. Microsoft Windows Third Party Component CA 2012
46. Microsoft Windows Third Party Component CA 2013
47. Microsoft Windows Third Party Component CA 2014
48. VS Package Repositories CA
49. Windows Azure StorSimple CA 2013
50. Windows Production PCA 2023
51. Windows UEFI CA 2023

ATTACHMENT B

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

CP Name	Version	Date
Microsoft PKI Services Certificate Policy	3.1.7	July 27, 2023
Microsoft PKI Services Certificate Policy	3.1.6	February 22, 2023

CPS Name	Version	Date
Microsoft PKI Services Corporate Certification Practice Statement	3.1.7	May 22, 2023