

INDEPENDENT ACCOUNTANT'S REPORT

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

Scope

We have examined MS PKI Services management's [assertion](#) that for its Certification Authority ("CA") operations at locations enumerated in [Attachment C](#), for its CAs as enumerated in [Attachment A](#), MS PKI Services has:

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

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

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

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

Certification authority's responsibilities

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

Practitioner's responsibilities

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

Our independence and quality control

We are required to be independent and to meet other ethical responsibilities in accordance with the Code of Professional Conduct established by the American Institute of Certified Public Accountants ("AICPA") and Code of Ethics for Professional Accountants (including International Independence Standards) issued by the International Ethics Standards Board of Accountants' ("IESBA").

We have complied with those requirements. We applied the Statements on Quality Control Standards established by the AICPA and the International Standards on Quality Management issued by the International Auditing and Assurance Standards Board (“IAASB”) and, accordingly, maintain a comprehensive system of quality control.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at MS PKI Services and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls and other factors present at individual subscriber and relying party locations. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Emphasis of matters

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

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

While the MS PKI Services management’s [assertion](#) enumerates matters disclosed publicly on Mozilla’s Bugzilla reporting system throughout the period May 1, 2025 to April 30, 2026, we have only noted those matters relevant to the CAs enumerated in [Attachment A](#) and applicable to the [WebTrust Principles and Criteria for Certification Authorities, v2.2.2](#).

Opinion

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

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

Use of the WebTrust seal

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

Deloitte & Touche LLP

Deloitte & Touche LLP
July 28, 2026

ATTACHMENT A

LIST OF IN SCOPE CAs

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

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

CA IDENTIFYING INFORMATION

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
1	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	1498266DC7CCD8F4053677BB999EC85	ECC	sha384ECDSA	2/27/2018 20:42	2/27/2043 20:50	N/A	0	43EF7087B89DBFEC8819DCC6C46B750D75343308	CACA93B9D23D2B6FA76E8B8471931E0DF3EC6F63AF3CDBB936CA1954A1872326
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	3FD48E8BAAD2F26E1BDE06C7584BB720DD1A972D111F5A4999BC44B08FB4960D
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	'33000000149843474594317849000000000014	ECC	sha384ECDSA	9/28/2018 17:55	9/6/2035 17:55	N/A	Time Stamping (1.3.6.1.5.5.7.3.8)	E847C8429AB09DAE6F0B283B98158FE3B1E880B2	D4D27BC233F38B4414617E72871F54D40758AB988072D9FFEC31AEDA60ECC6D0
3	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	28CC3A258FBA44AC449A9B586B4339AA	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	6/22/2035 21:01	N/A	Time Stamping (1.3.6.1.5.5.7.3.8)	CBD1F2CE48FD019FEA56AA57D17E9958F83FFFE0	A303E478DD3CBC0E47A290FD5B59AF5C017A95E4886EC354EC6DA8B9380EE399
7	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Azure Attestation PCA 2019	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	3300000037756C792A2979DF3D0000000000037	RSA	sha256RSA	5/30/2019 22:48	5/30/2034 22:58	N/A	0	ad475e6ccfa9d55a75355dfa28a17578289f71ad	D8A4236A2BD59061D008139D2071EA7BEF642E1B959A0CE662666B438D2C095
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	61116C920000000000007	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	A53A400DF29EC7B8C8FCE7CFFFE47334F43B1642E604DD0307491737EB8C00CE
9	1	C=US O=Microsoft Corporation CN=Microsoft Certificate List CA 2024	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	330000001D30D6F149DCD42E1D000000000001D	RSA	sha384RSA	8/22/2024 20:32	6/23/2035 22:04	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Windows Update (1.3.6.1.4.1.311.76.6.1)	306e265901fa54f32fbffc613b2647f5a61a3ae2	56625EC7886445706FE74CCD2ABF69B7C9C9CCDE3C7354903AF1C8F0E30E9D1C
10	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Code Signing PCA 2010	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	610C524C0000000000003	RSA	sha256RSA	7/6/2010 20:40	7/6/2025 20:50	N/A	0	E6FC5F7BBB220058E4724EB5F421742332E6EFAC	9AAD6C1A83A1B974BA574A995AF35B8CA772DA919270DB1605A8B81E1B8C896F
11	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Code Signing PCA 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	610E90D20000000000003	RSA	sha256RSA	7/8/2011 20:59	7/8/2026 21:09	N/A	0	486E6455005D382AA1737372B56DA8CA750295	56DA8722AFD94066FFE1E45595473A4854892B843A0827D53F87D8F4AEED1E18B
12	1	C=US O=Microsoft Corporation CN=Microsoft Code Signing PCA 2024	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	33000000393B863719BF061D670000000000039	RSA	sha384RSA	8/8/2024 20:54	3/22/2036 22:13	N/A	0	E847C8429AB09DAE6F0B283B98158FE3B1E880B2	3DADFAF812DD18BAEF45834CCBD188F3CD97139E2ED1ACA69C2DD63082142F8F
13	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Content Distribution Secure Server CA 2.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	3300000035D47483932E18187C0000000000035	RSA	sha256RSA	12/7/2018 20:12	12/7/2033 20:22	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	DEAA37759FD493A715504C4578E761BA37027F4B	64EBAE10EF707ECF156B560A1C9236455A5E9F1C16F270996E41D5F0DFEDA561
14	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Content Distribution Secure Server CA 2.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	3300000036A26D4F583DFDC1130000000000036	RSA	sha256RSA	12/7/2018 20:12	12/7/2033 20:22	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	84D6BFD9B25E9D87E3B2C0864CD39CC168B60E67	B90776868F9AA9F0048D2BBEC85908CD2735A36BACB5886AF5C3458303703471
15	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Certificate List PCA 2018	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	33000000037742B6E32092D50F0000000000003	ECC	sha384ECDSA	3/1/2018 21:40	3/1/2033 21:50	N/A	0	7aa29b3c3676b7033c6ccf439e509c86758055ce	C307C2757F1026AA755DC7830E43C61BA30BFE178FB9F92B621B830B3DA21C83
16	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Code Signing PCA 2018	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	3300000002B2A4C58304AE1E1000000000002	ECC	sha384ECDSA	3/1/2018 21:40	3/1/2033 21:50	N/A	0	862aaefa129e681f41ad660d486b1a707ff7c5c8	E673905E74CCA3307C5E2C7D1E78DCA1F6F2783A21F8B02B58472E304C680DB8
17	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Content Distribution Secure Server CA 2.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	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)	455478B823ACADE42A8CB014152B49C8E8191EE	E39F93F3B2B40FD3C41DE7DFA7D0B0CB6C4D8F97CBAB2BB81C178F4B5F3C7EED
18	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Content Distribution Secure Server CA 2.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	330000000ADB1A07295C828D7700000000000A	ECC	sha384ECDSA	12/7/2018 20:05	12/7/2033 20:15	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	D3C732531923973ECA3FFC83992F92CB3CD3D2C0	959D932A756F59612F2D757926D8AD3B11CB2684CA9203AE281F5CC26049BE94
19	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Time Stamp PCA 2018	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC TS Root Certificate Authority 2018	330000000278C1161CA7F6D350000000000002	ECC	sha384ECDSA	3/1/2018 21:48	3/1/2033 21:58	N/A	0	e8674bb61257af7710de40335764afc23e54881	5E72C836123C6EA5DE54A3697DE416EE167C2AC62C7C89F61BEB89C735160A7

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
20	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Update Secure Server CA 2.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	3300000004A1F5B5883D3F0022000000000004	ECC	sha384ECDSA	9/28/2018 21:34	9/28/2033 21:44	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	1641B107C78BF3D2061490260ADB812BC04462C3	21158AD4DCE10197239A87EBEB4D8D47E9E9BE716AD497A2E036774CAF5072CF
21	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Update Secure Server CA 2.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	33000000087B3662C012063EB4000000000008	ECC	sha384ECDSA	12/7/2018 20:05	12/7/2033 20:15	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	9dea50acb6663e22781d9640142b719e31c6d8c4	6345FD68446C011FD442A04A37E8407A51E548DE61A6685633134EDD67292F1A
22	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Update Signing CA 2.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	33000000051A3AE66A9EE4F897000000000005	ECC	sha384ECDSA	9/28/2018 21:34	9/28/2033 21:44	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Unknown Key Usage (1.3.6.1.4.1.311.76.6.1)	D2465153A49F6324F2E8D2B2AB854C9E32FFD852	73DF319F3BF18FA9C9D0B38DAABA98038C4F867D3C9CE609737DFA682BDA1FFB
23	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Update Signing CA 2.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	3300000006DEA087FB82845B90000000000006	ECC	sha384ECDSA	9/28/2018 21:34	9/28/2033 21:44	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Unknown Key Usage (1.3.6.1.4.1.311.76.6.1)	0478de0ab9f5c19eaa7c890c02a50d9f7546a76f	3EBC65CCB963BAA55AFA2F0D24A20044C7D17D97208EA2B318778C505CB7C08F
24	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Update Signing CA 2.3	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	3300000007E8141B8B05B5FBA30000000000007	ECC	sha384ECDSA	9/28/2018 21:34	9/28/2033 21:44	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Unknown Key Usage (1.3.6.1.4.1.311.76.6.1)	9ac2f5ae2b21ef6c239eeddbeab84b4da520dc0d	C67E5F87209E33B857566DBF525FC0869EF8C715E5BA4A752DAE2A38DB16E14C
25	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Marketplace PCA 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Marketplace PCA 2011	611244A20000000000002	RSA	sha256RSA	3/28/2011 21:09	3/28/2031 21:19	N/A	0	0F53CB3F166125FE60891DD3B97CE890AD8394D1	5A9D21E71180301A044E4CFBDE431FDF4C1CFC998B1B6343B5A10AA9E4CDE98
26	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=AOC CN=Microsoft Marketplace CA G 021	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Marketplace PCA 2011	3300000005C3AB23618FF8DF7B1000000000005C	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	5292df39da46425b8a6e6b1de33a43ac7ad5254b	2C9A04FCCAB13082EEBC3E2CE4023901EAF623D522F6D29C9B9788759A7C35D
27	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=AOC CN=Microsoft Marketplace CA G 022	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Marketplace PCA 2011	330000000567DB266D0825D8B990000000000056	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	4782e488d37806f136d0d1f7818f1e1428240d4b	9F2C808A8705320E19FC4F34211C580667469B7033C40F239265249F792D6286
28	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=AOC CN=Microsoft Marketplace CA G 023	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Marketplace PCA 2011	330000000570D7B1FC64FD44E7B00000000000057	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	26dc3df5a3eb8950dbc65c17db4b3a1238a5d97	DF0BCA1D35DD79B1B7D7CFE769ADE9D2BCAA61766ED39CA1AD0CCDCF839C7F4
29	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=AOC CN=Microsoft Marketplace CA G 024	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Marketplace PCA 2011	33000000053E45C4DC84039D4C00000000000053	RSA	sha256RSA	5/14/2019 18:51	5/14/2024 18:51	N/A	0	aa47be1b68e38ec4bac55ca1703ea61d9c2c1cf2	6466C53BCAA7631A2B932C6CA883CB7A6069AA15E0834D0F567E269EA56B4F33
29	2	C=US S=Washington L=Redmond O=Microsoft Corporation OU=AOC CN=Microsoft Marketplace CA G 024	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Marketplace PCA 2011	33000000058E5873D5CF575E4140000000000058	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	75151394260a61aec9fb8f914766a6bae680023d	14EC068F3D53E4B0FE038CBC416EBFE8E1CC728536EDEE9103EE69E729F7F3E4
30	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=EOC CN=Microsoft Marketplace CA G 025	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Marketplace PCA 2011	330000000591BBE16AF06B6A400000000000059	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	2bc8e3a408a6a0c5195c5bcc3ece5e70982f3d5c	F811DEA5AFCF25FBC3EEAB33918B83C3CE4A241B8445AC1123D65F8A84A32308
31	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=EOC CN=Microsoft Marketplace CA G 026	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Marketplace PCA 2011	330000000584E9A3269B8AD800D000000000005B	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	8e6f5ca466c1e11a8183c97d9ef5d246ed88216c	76B81CDC8C9C89EA598F3F7875F332FD9C0DE67B117438585692311706AF4E86
32	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=EOC CN=Microsoft Marketplace CA G 027	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Marketplace PCA 2011	3300000005A16D74E269F012BD4000000000005A	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	3e7e0234a965526b487ad0d6806ec0df60e78b03	21EC00EA4D12FA20874663CF04DA6f63660CC1EBE80E1D2C12F3D78CB8BCA9BA
33	1	C=US S=Washington L=Redmond O=Microsoft Corporation OU=EOC CN=Microsoft Marketplace CA G 028	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Marketplace PCA 2011	330000000545A16CB93E5310AE80000000000054	RSA	sha256RSA	5/14/2019 18:51	5/14/2024 18:51	N/A	0	1280f52d7a2fe950e886076b5ef8a839b9f5785f	951D2F622C2B542C00F70E19833F15F880B113BD2D30980643C0020DBD729A94
33	2	C=US S=Washington L=Redmond O=Microsoft Corporation OU=EOC CN=Microsoft Marketplace CA G 028	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Marketplace PCA 2011	3300000005D9F04EC95B702B46F000000000005D	RSA	sha256RSA	11/4/2024 17:45	11/4/2029 17:45	N/A	0	1280f52d7a2fe950e886076b5ef8a839b9f5785f	12D43CDF626305E3A496CE63F27674FCB627AE4506A276E3EF3200BEEA129806
34	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Marketplace Production CA 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Marketplace PCA 2011	33000000055C8066B8323972909000000000055	RSA	sha256RSA	9/9/2021 22:42	9/9/2030 22:52	N/A	0	74e66f4536729ab9b034c787052fd5eb61271c22	CA92943AB468CB89604A97F909AE31C04577F5ADCBF7565F40C5837A072A5FE4
35	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Secure Server CA 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Marketplace PCA 2011	613FB7180000000000004	RSA	sha256RSA	10/18/2011 22:55	10/18/2026 23:05	N/A	0	3656896549CB85B92F3CAC4216504D918933D791	83688F2AEF71386E0936C4B3013B07E8E0C796D8427716DD48B2A63D79509129
36	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Time Stamp CA 2015	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	3300000002F9FA0638351073C20000000000002	RSA	sha256RSA	3/25/2015 21:18	3/25/2030 21:28	N/A	0	212FBE3E2C5C9A59E5D5AD0BE971941D79515F84	857AEC60913116E2B61190B1E86FA001F27E8D165FAED492F829313E8212B666
37	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Time-Stamp PCA 2010	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	6109812A0000000000002	RSA	sha256RSA	7/1/2010 21:36	7/1/2025 21:46	N/A	0	D5633A5C8A3190F3437B7C461BC533685A856D55	86EC118D1EE69670A46E2BE29C4B4208BE043E36600D4E1DD3F3D515CA119020
37	2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Time-Stamp PCA 2010	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	3300000015C5E76B9E029B4999000000000015	RSA	sha256RSA	9/30/2021 18:22	9/30/2030 18:32	N/A	Time Stamping (1.3.6.1.5.5.7.3.8)	D5633A5C8A3190F3437B7C461BC533685A856D55	EBEC1EDD9E140D9C105CC62B15A915C5443DDC514A35E5773C09AFB0274C7BA5
38	1	C=US O=Microsoft Corporation CN=Microsoft Update Metadata Signing CA 3.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	3300000003E2DD309B9002F6FA9000000000003E	RSA	sha384RSA	3/13/2025 19:20	12/13/2035 19:30	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Unknown Key Usage (1.3.6.1.4.1.311.76.6.1)	ba9b5bc7b6ada704090c26a396d1a718894f903a	5CEF267491F3f59ED097124935155F1BD3756E32B7A432FE097EA170C5F339F
39	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Update Secure Server CA 2.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	3300000000AB891A2C80A50A5DF000000000000A	RSA	sha256RSA	6/21/2012 17:33	6/21/2027 17:43	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	D2F23D8474861B5085AA5DE5A5079AF047D32E69	6139E2DF97DC93BF7E90A303F75B3968FD06C57316B45E94DCFF773707CF2754
40	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Update Secure Server CA 2.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	3300000000B9AA76B8008015CF8000000000000B	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)	A4F2918745D77C968B35C8B6311AD4CAEFA5604C	C18C7AC733DEC68A6AF944A5A2B4F79F492ABAACE213811F6EF681D7861B57

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
41	1	C=US O=Microsoft Corporation CN=Microsoft Update Secure Server CA 3.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000003B8123BBB6A0B4EB6B0000000003B	RSA	sha384RSA	3/13/2025 18:12	12/13/2035 18:22	N/A	0	34cf450d3a7fb272280e6056130e83607dea65c3	63E747F977AD8C8A0177004062E89AF20884610F4642EBD44589D2BEAC8E3EA2
42	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Update Signing CA 2.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	3300000007B1CC402755483F69000000000007	RSA	sha256RSA	6/19/2012 22:53	6/19/2027 23:03	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Unknown Key Usage (1.3.6.1.4.1.311.76.6.1)	AD94768F83AD0E03A3E83BB0D73468D4793A7DDC	882F36D6F0DABF4B017FC6E8EA6D4F0F2786300D7B8210C3AE5C793F95E1C0C9
43	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Update Signing CA 2.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000000859E394E054C7175D000000000008	RSA	sha256RSA	6/19/2012 22:53	6/19/2027 23:03	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Unknown Key Usage (1.3.6.1.4.1.311.76.6.1)	5D5D6BF8B4B214A48BADA6752B96A3B8DC49155AD	24919D52EFB9ECBEC6C1D24CBC2E10D041B516B9410D6CEB75FF2F348BD0E5C8
44	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Update Signing CA 2.3	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	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)	D0F3FA5FF546F5CB83D88FAE8F8CEC861CDF61C8	46B4D5B761CA7B14D4877C3B2D3F22DBF92BC34B694E971E942517DABEB4B06C
45	1	C=US O=Microsoft Corporation CN=Microsoft Update SIH Signing CA 3.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000003F207459BF58D5933300000000003F	RSA	sha384RSA	3/13/2025 19:36	12/13/2035 19:46	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Microsoft Trust List Signing (1.3.6.1.4.1.311.10.3.1), Root List Signer (1.3.6.1.4.1.311.10.3.9), Revoked List Signer (1.3.6.1.4.1.311.10.3.19)	b47e049719dfbf77f235edbb457d74d9818b0605	79475879DE5120750B09AD1D87DE80A93596130D8C5E7B3810A5CF707C3A3A19
46	1	C=US O=Microsoft Corporation CN=Microsoft Update SLS Signing CA 3.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000003C5595271D82CD079300000000003C	RSA	sha384RSA	3/13/2025 18:37	12/13/2035 18:47	N/A	0	2ef850e59e729d830a2c2207b9049878e667b461	4A8FD639FD1F2A94F5F0710F3A2AA3C5E1E5D60AB2AB5618D24BA5A5480F02B2
47	1	C=US O=Microsoft Corporation CN=Microsoft Update SLS Signing CA 3.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000003D86A3B3AD845F230000000000003D	RSA	sha384RSA	3/13/2025 19:04	12/13/2035 19:14	N/A	0	A92902398E16C49778CD90F99E4F9AE17C55AF53	B2625F512F768288485B2A7759B3968ABE3D97199BDFD9D0E903D06E3F9781C0
48	1	C=US O=Microsoft Corporation CN=Microsoft Windows Code Signing PCA 2024	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	330000001C489F81DFA1B0B77700000000001C	RSA	sha384RSA	8/8/2024 21:36	6/23/2035 22:04	N/A	0	1e82df0ed78cb3d70234830edaabad65b9afb8ec	3DADFAF812DD1BBAEF45834CCBD188F3CD97139E2ED1ACA69C2DD63082142F8F
49	1	C=US O=Microsoft Corporation CN=Microsoft Windows Component Preproduction CA 2024	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000003AE8F966B913AC7751000000000003A	RSA	sha384RSA	8/8/2024 22:07	3/22/2036 22:13	N/A	0	67223fe1b42ea930bfb409daedec03cd0da44b48	B4065016A9886B3D56F94814A8BA391B50A28D3020C9054DE0AF9222C9FF3272
50	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Windows PCA 2010	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	610C6A190000000000004	RSA	sha256RSA	7/6/2010 20:40	7/6/2025 20:50	N/A	0	D14FA98A0708CEF4241898E500FF3D6791D37BC	F01614A7A81BA477F0746CF2DE71B20DDDEC709E756C9EA57CB67F93F25BA9FD
51	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Windows Phone PCA 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	610B5C910000000000005	RSA	sha256RSA	2/28/2011 22:11	6/23/2035 22:04	N/A	0	FD399547DEEF1ACE48502070072F7EFE7E7468F5	AE378D79D44CC75CEE8BAE50DD8BCBF2D4FF7C598B62FE75C3CE234C4001AFD9
52	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Windows Phone Production PCA 2012	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	330000000BFCF98E584C1550BF00000000000B	RSA	sha256RSA	7/24/2012 22:23	7/24/2027 22:33	N/A	0	4498DF99096EB8D642212E9B9EDF266EC38E954B	E6A9B56A89AA3B191D23A6FB7FECB1F09DED4552A682FCF72B1D479C3B23C9BA
53	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Windows Production PCA 2011	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	610776560000000000008	RSA	sha256RSA	10/19/2011 18:41	10/19/2026 18:51	N/A	0	A92902398E16C49778CD90F99E4F9AE17C55AF53	E8E95F0733A55E8BAD7BE0A1413EE23C51FCEA64B3C8FA6A786935FDDCC71961
54	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Windows Third Party Component CA 2012	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	610BAAC10000000000009	RSA	sha256RSA	4/18/2012 23:48	4/18/2027 23:58	N/A	0	6171A787AFF69D521764F52932800BE7912AB84	9D08973E4D108DA40A1A0B274180E173711348ADD1621FA5C1F131B739B4B823
55	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Windows Third Party Component CA 2013	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	33000000149DFBC31F1F63C310000000000014	RSA	sha256RSA	5/1/2013 20:44	5/1/2028 20:54	N/A	0	7792047827B20B49077597EEE9EB5E265C094475	8EF01BB5E07987053659E039E5A72580C88C444BC1A31AB412CE81A4AD53044E
56	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Windows Third Party Component CA 2014	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000000D690D5D7893D076DF00000000000D	RSA	sha256RSA	10/15/2014 20:31	10/15/2029 20:41	N/A	0	C83A9CA74AC323F2257EB9DAAB29530E5400C3A1	A0F259A07039908EEB943E223FDF996E5E1E131D9AA6A602FF4672F7B9298AEE
57	1	C=US O=Microsoft Corporation CN=Microsoft Windows Third Party Component CA 2024	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	330000001B2DC28C2D7F55CC0B00000000001B	RSA	sha384RSA	8/8/2024 20:14	6/23/2035 22:04	N/A	0	1c649345e78c7ab68873cad7e9ad3c5052977b9e	86C83B2BBDCC9CD3C45F85AE11013B93F268FE97D36B3695A863D163138CF48C
58	1	C=US O=Microsoft Corporation CN=VS Package Repositories CA	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	330000003876C4AE8B39AAE393000000000038	RSA	sha384RSA	1/20/2022 19:46	3/22/2036 22:13	N/A	0	c101c3929cec3c609f99399a770838b5700383d5	AC415BBB3EE2E11B5EFD1180888026B02736A82480C26AB7569FC19195344202
59	1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Windows Azure StorSimple CA 2013	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000000C8CC7499215880C9000000000000C	RSA	sha256RSA	10/15/2013 18:09	10/15/2028 18:19	N/A	0	c45e0e66efe4c73a33532a9c7e3986be1cc21f50	854B33F368F4D9BA80F4797D8E7150DC8754E7EF9E06ACBEC16F92C06E20DEBF
60	1	C=US O=Microsoft Corporation CN=Windows Production PCA 2023	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	330000001785BD56094BF8C821000000000017	RSA	sha384RSA	6/13/2023 18:34	6/13/2035 18:44	N/A	0	86ed0bae3f5a09d23d1e2119557f9f315322f800	4F771E28419476AF6791F116F65E963812EE85F841A8184E85F592BA3D51A4BF
61	1	C=US O=Microsoft Corporation CN=Windows UEFI CA 2023	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2010	330000001A888B9800562284C1000000000001A	RSA	sha256RSA	6/13/2023 18:58	6/13/2035 19:08	N/A	0	aefc5fbbbe055d8f8daa585473499417ab5a5272	076F1FEA90AC29155EBF77C17682F75F1FDD1BE196DA302DC8461E350A9AE330
62	1	C=US O=Microsoft Corporation CN=Microsoft ECC Update SIH Signing CA 3.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	330000000B51C891E4C25D195B00000000000B	ECC	sha384ECDSA	5/14/2025 18:31	5/14/2035 18:41	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Windows Update (1.3.6.1.4.1.311.76.6.1)	5647460ab47ea6dcfa68660af5d415e9f1ade3ec	4999A388B1EEB582C2EFC698B53832C8EFA4780F2E22F2D167F43CB561185D64
63	1	C=US O=Microsoft Corporation CN=Microsoft ECC Update SIH Signing CA 3.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	330000000CA807CE95DB1EAC4E000000000000C	ECC	sha384ECDSA	5/14/2025 19:21	5/14/2035 19:31	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Windows Update (1.3.6.1.4.1.311.76.6.1)	bce549c26e16ef08b5d2529f2d2cd0c082fb216b	1987938D55A9620A08EE0C07B183A33244A205D56E4A908AAE5107A21B477076
64	1	C=US O=Microsoft Corporation CN=Microsoft ECC Update Metadata Signing CA 3.1	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft	330000000D8DF141274A790FED00000000000D	ECC	sha384ECDSA	<u>5/14/2025 19:50</u>	5/14/2035 20:00	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Windows Update (1.3.6.1.4.1.311.76.6.1)	03158374881299fd1d93fba3a8a69061b5c58391	040465673A9CD31E2502966CA8F4A7E29C0C9740F1FB415A32984A29C2639A16

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
			ECC Product Root Certificate Authority 2018									
65	1	C=US O=Microsoft Corporation CN=Microsoft ECC Update Metadata Signing CA 3.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft ECC Product Root Certificate Authority 2018	330000000E47DE4BC44F2A752300000000000E	ECC	sha384ECDSA	5/14/2025 20:17	5/14/2035 20:27	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Windows Update (1.3.6.1.4.1.311.76.6.1)	e41e6824aea275f3fd60a8398501781e43c8eae	317B7AA4A5210C4E2687D1D6F8DFA389351D8B70CE6BC286C9601C8BA221366A
66	1	C=US O=Microsoft Corporation CN=Microsoft Update SLS Signing CA 3.3	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000000403A68CBD2FE3C5D170000000000040	RSA	sha384RSA	5/14/2025 20:44	12/14/2035 20:54	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Windows Update (1.3.6.1.4.1.311.76.6.1)	dab0c80606ce46b43efad276bc768c12c1be6925	A2FA09B8D81D1C5CE24255688973FB05144DB97213B51A320B31D5EFBEC7D62D
67	1	C=US O=Microsoft Corporation CN=Microsoft Update Metadata Signing CA 3.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000000413B26B270125071BF0000000000041	RSA	sha384RSA	5/14/2025 21:13	12/14/2035 21:23	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Windows Update (1.3.6.1.4.1.311.76.6.1)	dfb1fcf411c0982e5983342dc76307b909ea59c9	362AD926C3A4CCDF49E498779E7989FOFF766F759CEF8A679AEE9075000C568A
68	1	C=US O=Microsoft Corporation CN=Microsoft Update Secure Server CA 3.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	33000000042E9F495BE713B179E0000000000042	RSA	sha384RSA	5/14/2025 21:36	12/14/2035 21:46	N/A	Server Authentication (1.3.6.1.5.5.7.3.1)	cdf81db6f42bce47a5b520c1b510a238ab55a073	3748B0AA073F4639BEC3DF60698CC38A4D5CD360D3346001943D32041356AABE
69	1	C=US O=Microsoft Corporation CN=Microsoft Update SIH Signing CA 3.2	C=US S=Washington L=Redmond O=Microsoft Corporation CN=Microsoft Root Certificate Authority 2011	330000000437FA0F1707E4C1F750000000000043	RSA	sha384RSA	5/14/2025 22:00	12/14/2035 22:10	N/A	Code Signing (1.3.6.1.5.5.7.3.3), Windows Update (1.3.6.1.4.1.311.76.6.1)	b442d960df4706e8702a73bd419a61830a7c7d03	816FB2FBD75D47F0C33D0C7821C47AEFB5A61BB00B9B0B1E475ADC5F5961EDD0

ATTACHMENT B

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

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

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

ATTACHMENT C

LIST OF MS PKI SERVICES' LOCATIONS IN-SCOPE

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

MICROSOFT PUBLIC KEY INFRASTRUCTURE SERVICES MANAGEMENT'S ASSERTION

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

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

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

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

MS PKI Services management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in MS PKI Services management's opinion, in providing its CA services at locations enumerated in [Attachment C](#), MS PKI Services has:

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

Throughout the period May 1, 2025 to April 30, 2026 based on the [WebTrust Principles and Criteria for Certification Authorities, v2.2.2](#), including the following:

CA Business Practices Disclosure

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

CA Business Practices Management

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

CA Environmental Controls

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

CA Key Lifecycle Management Controls

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

Subscriber Key Lifecycle Management Controls

- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

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

Subordinate CA and Cross Certificate Lifecycle Management Controls

- Subordinate CA Certificate and Cross Certificate Lifecycle Management

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

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

Sr.	Bugzilla ID	Bugzilla Title	Created On	Resolved On	Status
1	1962829	Microsoft PKI Services: Policy document bug	April 28, 2025	April 25, 2026	Resolved
2	1962830	Microsoft PKI Services: Subscriber certificate change made that was not compliant with CPS	April 28, 2025	June 20, 2025	Resolved
3	1965612	Microsoft PKI Services: Failure to Revoke in 5 Days for 1962829	May 9, 2025	May 4, 2026	Resolved
4	1970968	Microsoft PKI Services: Incorrect Revocation Reason Code	June 6, 2025	July 8, 2025	Resolved
5	1974592	Microsoft PKI Services: Pre-Sign Linting Validation did not occur in ICA creation	June 28, 2025	August 30, 2025	Resolved

Sr.	Bugzilla ID	Bugzilla Title	Created On	Resolved On	Status
6	1979475	Microsoft PKI Services: End Entity Certificate Mis-issuance against CPS (BasicConstraints)	July 28, 2025	January 20, 2026	Resolved
7	1990801	Microsoft: improper disclosure of CRL	September 26, 2025	November 3, 2025	Resolved
8	1999850	Microsoft PKI Services: OCSP Non-Compliance	November 13, 2025	July 1, 2026	Resolved
9	2007221	Microsoft PKI Services: Improper Disclosure of CRL	December 19, 2025	March 2, 2026	Resolved
10	2008847	Microsoft PKI Services: Sample Site Certificates expired	January 7, 2026	February 16, 2026	Resolved
11	2009539	Microsoft PKI Services: Improper Disclosure of CRLs – IDP – Existing CAs	January 10, 2026	February 16, 2026	Resolved
12	2009541	Microsoft PKI Services: Failure to report within 72 hrs - Sample Site Certs Expired	January 10, 2026	February 11, 2026	Resolved
13	2009542	Microsoft PKI Services: Improper Disclosure of CRLs – IDP – New CAs	January 10, 2026	February 16, 2026	Resolved
14	2009543	Microsoft PKI Services: Improper Disclosure of CRLs – Does Not Match CA Subject	January 10, 2026	February 9, 2026	Resolved
15	2009545	Microsoft PKI Services: Improper Disclosure of CRLs – Protocol Scheme	January 10, 2026	February 11, 2026	Resolved
16	2021175	Microsoft PKI Services: Failure to update action item status within 3 days	March 5, 2026	April 3, 2026	Resolved
17	2026452	Microsoft PKI Services: Failure to publish Full Incident Report for Bugzilla 2021175 within 14 days	March 26, 2026	April 22, 2026	Resolved
18	2026453	Microsoft PKI Services: Failure to report Bugzilla 2026452 within 72 hrs	March 26, 2026	April 22, 2026	Resolved
19	2034251	Microsoft PKI Services: Failure to Update Full Incident Report within 14 days of discovering new root cause	April 23, 2026	May 13, 2026	Resolved

Microsoft Public Key Infrastructure Services
July 28, 2026

ATTACHMENT A

LIST OF IN SCOPE CAs

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

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

ATTACHMENT B

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

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

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

ATTACHMENT C

LIST OF MS PKI SERVICES' LOCATIONS IN-SCOPE

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