



REPORT OF THE INDEPENDENT ACCOUNTANT

To the Management of Microsoft Public Key Infrastructure (“PKI”) Services, a service of Microsoft Corporation:

Scope

We have examined Microsoft 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 B](#), Microsoft PKI Services has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of its Microsoft PKI Services Certificate Policy (“CP”) and Microsoft PKI Services Certification Practice Statement (“CPS”) enumerated in [Attachment A](#)
- maintained effective controls to provide reasonable assurance that:
 - Microsoft PKI Services’ CPS is consistent with its CP; and
 - Microsoft PKI Services provides its services in accordance with its CP and CPS
- 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; 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, 2021 to April 30, 2022 based on the [WebTrust Principles and Criteria for Certification Authorities v2.2.1](#).

Microsoft PKI Services does not escrow its CA keys, does not provide subscriber key lifecycle management services, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.

Certification Authority’s Responsibilities

Microsoft 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 v2.2.1](#).



Independent Accountant's Responsibilities

Our responsibility is to express an opinion on Microsoft PKI Services management's assertion based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

The relative effectiveness and significance of specific controls at Microsoft 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.

Independent Accountant'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 Microsoft PKI Services' services other than its CA operations in the United States of America and in Ireland, nor the suitability of any of Microsoft PKI Services' services for any customer's intended purpose.

Other Matters

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



Matter Topic		Matter Description
1	Certificate Content	Microsoft disclosed in Mozilla Bug 1711147 that eight (8) of its intermediate CAs were missing the certificatePolicies extension.
		Microsoft disclosed in Mozilla Bug 1718991 that four (4) of its intermediate CAs had malformed key usage extensions.
2	Certificate Status	Microsoft disclosed in Mozilla Bug 1740585 that four (4) revocation entries on a CRL were removed before the expiry date of the revoked certificates.

While the Microsoft PKI Services assertion notes all issues disclosed on Bugzilla during the engagement period, we have only noted those instances relevant to the CAs enumerated in [Attachment B](#) and applicable to the [WebTrust Principles and Criteria for Certification Authorities v2.2.1](#).

Use of the WebTrust Seal

Microsoft 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.

BDO USA, LLP

June 17, 2022



ATTACHMENT A - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY VERSIONS IN-SCOPE

Certificate Policy

Policy Name	Policy Version	Policy Date
Microsoft PKI Services Certificate Policy	Version 3.1.4	February 15, 2021
Microsoft PKI Services Certificate Policy	Version 3.1.5	February 15, 2022

Certification Practice Statement

Policy Name	Policy Version	Policy Date
Microsoft PKI Services Certification Practice Statement	Version 3.1.9	March 30, 2021
Microsoft PKI Services Certification Practice Statement	Version 3.2.0	July 12, 2021
Microsoft PKI Services Certification Practice Statement	Version 3.2.1	January 19, 2022



ATTACHMENT B - IN-SCOPE CA CERTIFICATES

Root CA Certificates				
Common Name	SHA2 Thumbprint	SPKI Hash	Valid From	Valid To
Microsoft ECC Root Certificate Authority 2017	FEA1884AB3AEA6D0DBEDBE4B9CD9FEC8655116300A86A856488FC488BB4B44D2	35F53CE1264611E03340FE37E1EC7D4C	7/26/2017	7/26/2042
	358DF39D764AF9E1B766E9C972DF352EE15CFAC227AF6AD1D70E8E4A6EDCBA02	C986C5613DCA70FD04AA44545F2DAF28	12/18/2019	7/18/2042
Microsoft RSA Root Certificate Authority 2017	ECDD47B5ACBFA328211E1BFF54ADEAC95E6991E3C1D50E27B527E903208040A1	B2F7298B52BF2C3CAC4DDFE72DE4D68	7/26/2017	7/26/2042
	C741F70F4B2A8D88BF2E71C14122EF53EF10EBA0CFA5E64CFA20F418853073E0	2AC58957595982F2B62301AF597C699C5	12/18/2019	7/18/2042



Cross-Signed CA Certificates				
Common Name	SHA2 Thumbprint	SPKI Hash	Valid From	Valid To
Microsoft Azure ECC TLS Issuing CA 01	949D6B4B761CA134AD3E7A8571186F580EE887F2C6B568B5140F4157F98D68DD	3993B1F49242DC9B 120D28C55F688403 7FC40FA80285ADCB D59ACE791368CB1F	8/12/2020	6/27/2024
Microsoft Azure ECC TLS Issuing CA 02	9C64A9A43E990E98FBCE8317B2D4C1C07FFE6E032DA8BB6D60A696E2FF038F1F	3A175427EC2BA4F4 6DA57E77B64CAA54 B290A0DA5D0825AF 7BC31041A4034360	8/12/2020	6/27/2024
Microsoft Azure ECC TLS Issuing CA 05	003F71DC4820216575FC5AACFE3B1AEB76F72AEA5B8E8FCEFC80B9F517A4A612	934F4CCE6C2244F9 0F9A4A60994B69AC C93FB802D255E74D 2ED7CE06408CBD71	8/12/2020	6/27/2024
Microsoft Azure ECC TLS Issuing CA 06	2975BAB51D00D862D0E16EEDEF8306A759C65CD4B9F00DAF50ECDFCB4EC396E4	C818E7ADC99C529D A7CA50D15A742F48 F46CA66866D5FFDF 3AE2ABB0D89A49D0	8/12/2020	6/27/2024
Microsoft Azure TLS Issuing CA 01	24C7299864E0A2A6964F551C0E8DF2461532FA8C48E4DBBB6080716691F190E5	347C2EB1B0BBC3CE 382734E6BC8448A3 C34BEC3E92B484CA F69873160B498B4C	7/29/2020	6/27/2024
Microsoft Azure TLS Issuing CA 02	15A98761EBE011554DA3A46D206B0812CB2EB69AE87AAA11A6DD4CB84ED5142A	CC0C1FC76885710E 6F30E09CF6FB7E31 72DD2E5D3C12AB8 DB0E5A00C5D213B0F	7/29/2020	6/27/2024
Microsoft Azure TLS Issuing CA 05	D6831BA43607F5AC19778D627531562AF55145F191CAB5EFafa0E0005442B302	E22E21D2337D3513 ABD7128923E4D0D5 0FD921F5233CC5ED 99652C0D1DCF8E2C	7/29/2020	6/27/2024
Microsoft Azure TLS Issuing CA 06	48FF8B494668C752304B48BFE818758987DEF6582E5F09B921F4B60BB3D6A8DD	5A5F0C158FBDCE28 C61BC4201070802B 97E103EC9D3D9C5A 2D038576210FCF75	7/29/2020	6/27/2024



Intermediate CA Certificates ¹				
Common Name	SHA2 Thumbprint	SPKI Hash	Valid From	Valid To
Microsoft Azure ECC TLS Issuing CA 01	2CAEFBB55E70DF5A8985FE9BC10DD56A40C3DEDAB3DA1530A29682015C5B7C66	3993B1F49242DC9B 120D28C55F688403 7FC40FA80285ADCB D59ACE791368CB1F	1/17/2020	6/27/2024
Microsoft Azure ECC TLS Issuing CA 02	4EC439672A443401A66E27947CC3B5897F132B667F712CC1A37018A3CC85B16A	3A175427EC2BA4F4 6DA57E77B64CAA5 4B290A0DA5D0825AF 7BC31041A4034360	1/17/2020	6/27/2024
Microsoft Azure ECC TLS Issuing CA 05	624D5576A652B2130768BFE84B965EEFFFD91603D25CD5F7155A7DC2789DAC38	934F4CCE6C2244F9 0F9A4A60994B69AC C93FB802D255E74D 2ED7CE06408CBD71	1/17/2020	6/27/2024
Microsoft Azure ECC TLS Issuing CA 06	151A3E5969C6616EB637A8722B174CFD95387AAACE78D57C3BD23F0CB3008186A	C818E7ADC99C529D A7CA50D15A742F48 F46CA66866D5FFDF 3AE2ABB0D89A49D0	1/17/2020	6/27/2024
Microsoft Azure TLS Issuing CA 01	0437AB2EC2C2B4890296C135034B21DB146434B8317EE703AA8AA943C5EA51AE	347C2EB1B0BBC3CE 382734E6BC8448A3 C34BEC3E92B484CA F69873160B498B4C	1/17/2020	6/27/2024
Microsoft Azure TLS Issuing CA 02	D39CE39FF6F449D4F3391EE2004D705EC22F99CFFCA40A88F85DB26454ADDBD1	CC0C1FC76885710E 6F30E09CF6FB7E317 2DD2E5D3C12AB8D B0E5A00C5D213B0F	1/17/2020	6/27/2024
Microsoft Azure TLS Issuing CA 05	AB3203B3EA2017D509726A1D82293EFFCB8C42CEB52C9AF1C0EEE96B5C02BCBA	E22E21D2337D3513 ABD7128923E4D0D5 0FD921F5233CC5ED 99652C0D1DCF8E2C	1/17/2020	6/27/2024
Microsoft Azure TLS Issuing CA 06	7DF4D3EF45798F8C4384FC702BA52A44CE7BD6298B141628D4ABABC7678F6467	5A5F0C158FBDCE28 C61BC4201070802B9 7E103EC9D3D9C5A 2D038576210FCF75	1/17/2020	6/27/2024

¹ The Intermediate CA certificates in this table issued on 3/11/2021 were all revoked on 5/6/2021.



Intermediate CA Certificates ¹				
Common Name	SHA2 Thumbprint	SPKI Hash	Valid From	Valid To
Microsoft ECC TLS Issuing AOC CA 01	5C64B1731A8138DEA7D11C9AE8622891F945EBA46825E7ABFE4754F0A6011AF8	A9DF77A5BFB79FA34CDB975D964A30D9FE7FC4E670BD39BF1B8C2605E843DB54	6/24/2021	6/24/2026
	9D8BB150C07B81C25799B7945978B036E4B49C593C882BE379A58D08E1C25074		3/11/2021	3/11/2026
Microsoft ECC TLS Issuing AOC CA 02	808CA1ABBFE2FF1A9AC71887DDA71FF6FCA6C3B5224827F547515A4D9F7AF209	85FA29EB740D90CE77EDDBE3AB6C66A5DE3FC8BA94D6B2955FB7D33B04231601	6/24/2021	6/24/2026
	12FB2F53AC2D09E62128B00487E8B77D6E4A0F459DD8744D009393BD0DF697B5		3/11/2021	3/11/2026
Microsoft ECC TLS Issuing EOC CA 01	2769381532D96183ED39BDC4E323F3C520FBE6ACF3BDA30222239DDFC44C8380	EDE152DA0C19D6C3BB3168D11E40901919646BB6998CD5E7D0FBE6537FFF42EF	6/24/2021	6/24/2026
	568E4046F384D0FDD9D06A8029E6BF38EED8904C1E0B44F99DA607F68672093E		3/11/2021	3/11/2026
Microsoft ECC TLS Issuing EOC CA 02	659C0F902D6059FBD1FCA528839F20604B80C74364E58F9D48A2291F813ED82D	21CD47E3200B2D7F13567DF9E698EC21ACAC77A8F4A2A1173F4EAB23B2048967	6/24/2021	6/24/2026
	2DEEA0712931179BF1EF721070A30A1AB997F64C683EAB88DCE258D040D9AD25		3/11/2021	3/11/2026
Microsoft RSA TLS Issuing AOC CA 01	481E582A206A7D7040CCDA17CF25D349785A2AB94ED7552AB254DCD38B032ECO	7484F2F1618D35F6F239C05BAD30B8B7AD93C7024D4000D387141417EE3DDBF4	6/24/2021	6/24/2026
	13E295A5A6ECAF8391126E752B131B316675D187266BCF537892F839454B9480		3/11/2021	3/11/2026
Microsoft RSA TLS Issuing AOC CA 02	D77C45C1587731C4632C19D6F3C9FE832626615C879EA053664A4B26EB2293EC	F19A176BC779C77609427F441B995F14CAB9A19D87CDDD92725E4997CB0878BC	6/24/2021	6/24/2026
	2AF3B34A5FD0EDC546E2E714208B6C380A5D5C553EDCA3A306A9E442C2389AAE		3/11/2021	3/11/2026
Microsoft RSA TLS Issuing EOC CA 01	5EA3857EACD4C7CA5ACBCA9C4627E26F3072038D191A29D4C3F9464B2E5F00C6	1F1D8E7685CE8255088F791BFD3FB927F50AC1007091B5BBC3347EFBC5D9A80C	6/24/2021	6/24/2026
	E204F2682F5F630E360256ABD722DFF475432053128FC4274649F65D14EE1A36		3/11/2021	3/11/2026
Microsoft RSA TLS Issuing EOC CA 02	4D55BC4ABEB7D37FAB57E573ACCE83133E36212C864E003FBCB30B5FC248B011	89E1EF9BD893880FCA4C2D0BA71EC93DAF6C0AC14D5A9996F3E16F9763995076	6/24/2021	6/24/2026
	C97634113A97DFD13D516B9B7FA1B886635C725BDF70BC0A7891DF8E3FF0F91C		3/11/2021	3/11/2026



MICROSOFT PUBLIC KEY INFRASTRUCTURE SERVICES MANAGEMENT'S ASSERTION

Microsoft Public Key Infrastructure ("PKI") Services operates the Certification Authority ("CA") services for the CAs enumerated in [Attachment B](#), 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 Microsoft PKI Services is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its [repository](#), 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, controls placed into operation can only provide reasonable assurance with respect to Microsoft PKI Services' CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

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

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of its Microsoft PKI Services Certificate Policy ("CP") and Microsoft PKI Services Certification Practice Statement ("CPS") enumerated in [Attachment A](#)
- maintained effective controls to provide reasonable assurance that:
 - Microsoft PKI Services' CPS is consistent with its CP; and
 - Microsoft PKI Services provides its services in accordance with its CP and CPS
- 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; 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, 2021 to April 30, 2022, based on the [WebTrust Principles and Criteria for Certification Authorities v2.2.1](#), including the following:

CA Business Practices Disclosure

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

CA Business Practices Management

- CPS Management
- CP 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
- Systems 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 Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Transportation
- CA Key Migration

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

Microsoft PKI Services does not escrow its CA keys, does not provide subscriber key lifecycle management services, and does not provide certificate suspension services. Accordingly, our assertion did not extend to controls that would address those criteria.

Microsoft has disclosed the following matters publicly on Mozilla Bugzilla's platform. These matters were included below due to being open during the period May 1, 2021 through April 30, 2022.

Bug ID	Summary	Opened	Closed	Resolution
1693930	Microsoft PKI Services: Policy Documentation, Failure to update Subscriber Certificate Max Validity Period	2/19/2021	7/16/2021	Fixed
1700809	Microsoft PKI Services: Failure to disclose Unconstrained Intermediate within 7 Days	3/24/2021	7/4/2021	Fixed
1705419	Microsoft: Underscore in SAN	4/15/2021	9/20/2021	Fixed
1706860	Microsoft PKI Services: Certificate Mis-issuance, DNSName is not FQDN, Preferred Name Syntax	4/21/2021	6/7/2021	Fixed
1711147	Microsoft PKI Services, Malformed ICAs (missing certificate policy extensions)	5/13/2021	2/9/2022	Fixed
1718991	Microsoft PKI Services, Malformed ICAs (Key Usage Malformed)	7/2/2021	8/6/2021	Fixed
1724530	Microsoft PKI Services: Overdue Audit Reports 2021	8/6/2021	10/3/2021	Fixed
1740585	Microsoft: Unrevoked 4 intermediate certificates	11/10/2021	12/6/2021	Fixed
1718991	Microsoft PKI Services: Failure to disclose Revocation of Intermediate CAs within 7 Days	11/19/2021	12/6/2021	Fixed

33F845FB21044B2

Raza Syed

DocuSigned By: Raza Syed

6/17/2022

Raza Syed
Distinguished Engineer, Product Release & Security Services

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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



ATTACHMENT A - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY VERSIONS IN-SCOPE

Certificate Policy

Policy Name	Policy Version	Policy Date
Microsoft PKI Services Certificate Policy	Version 3.1.4	February 15, 2021
Microsoft PKI Services Certificate Policy	Version 3.1.5	February 15, 2022

Certification Practice Statement

Policy Name	Policy Version	Policy Date
Microsoft PKI Services Certification Practice Statement	Version 3.1.9	March 30, 2021
Microsoft PKI Services Certification Practice Statement	Version 3.2.0	July 12, 2021
Microsoft PKI Services Certification Practice Statement	Version 3.2.1	January 19, 2022

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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



ATTACHMENT B - IN-SCOPE CA CERTIFICATES

Root CA Certificates				
Common Name	SHA2 Thumbprint	SPKI Hash	Valid From	Valid To
Microsoft ECC Root Certificate Authority 2017	FEA1884AB3AEA6D0DBEDBE4B9CD9FEC8655116300A86A856488FC488BB4B44D2	35F53CE1264611E0 3340FE37E1EC7D4C C986C5613DCA70FD 04AA44545F2DAF28	7/26/2017	7/26/2042
	358DF39D764AF9E1B766E9C972DF352EE15CFAC227AF6AD1D70E8E4A6EDCBA02		12/18/2019	7/18/2042
Microsoft RSA Root Certificate Authority 2017	ECDD47B5ACBFA328211E1BFF54ADEAC95E6991E3C1D50E27B527E903208040A1	B2F7298B52BF2C3C AC4DDFE72DE4D68 2AC58957595982F2B 62301AF597C699C5	7/26/2017	7/26/2042
	C741F70F4B2A8D88BF2E71C14122EF53EF10EBA0CFA5E64CFA20F418853073E0		12/18/2019	7/18/2042

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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



Cross-Signed CA Certificates				
Common Name	SHA2 Thumbprint	SPKI Hash	Valid From	Valid To
Microsoft Azure ECC TLS Issuing CA 01	949D6B4B761CA134AD3E7A8571186F580EE887F2C6B568B5140F4157F98D68DD	3993B1F49242DC9B 120D28C55F688403 7FC40FA80285ADCB D59ACE791368CB1F	8/12/2020	6/27/2024
Microsoft Azure ECC TLS Issuing CA 02	9C64A9A43E990E98FBCE8317B2D4C1C07FFE6E032DA8BB6D60A696E2FF038F1F	3A175427EC2BA4F4 6DA57E77B64CAA54 B290A0DA5D0825AF 7BC31041A4034360	8/12/2020	6/27/2024
Microsoft Azure ECC TLS Issuing CA 05	003F71DC4820216575FC5AACFE3B1AEB76F72AEA5B8E8FCEFC80B9F517A4A612	934F4CCE6C2244F9 0F9A4A60994B69AC C93FB802D255E74D 2ED7CE06408CBD71	8/12/2020	6/27/2024
Microsoft Azure ECC TLS Issuing CA 06	2975BAB51D00D862D0E16EEDEF8306A759C65CD4B9F00DAF50ECDFCB4EC396E4	C818E7ADC99C529D A7CA50D15A742F48 F46CA66866D5FFDF 3AE2ABB0D89A49D0	8/12/2020	6/27/2024
Microsoft Azure TLS Issuing CA 01	24C7299864E0A2A6964F551C0E8DF2461532FA8C48E4DBBB6080716691F190E5	347C2EB1B0BBC3CE 382734E6BC8448A3 C34BEC3E92B484CA F69873160B498B4C	7/29/2020	6/27/2024
Microsoft Azure TLS Issuing CA 02	15A98761EBE011554DA3A46D206B0812CB2EB69AE87AAA11A6DD4CB84ED5142A	CC0C1FC76885710E 6F30E09CF6FB7E31 72DD2E5D3C12AB8 DB0E5A00C5D213B0F	7/29/2020	6/27/2024
Microsoft Azure TLS Issuing CA 05	D6831BA43607F5AC19778D627531562AF55145F191CAB5EFafa0E0005442B302	E22E21D2337D3513 ABD7128923E4D0D5 0FD921F5233CC5ED 99652C0D1DCF8E2C	7/29/2020	6/27/2024
Microsoft Azure TLS Issuing CA 06	48FF8B494668C752304B48BFE818758987DEF6582E5F09B921F4B60BB3D6A8DD	5A5F0C158FBDCE28 C61BC4201070802B 97E103EC9D3D9C5A 2D038576210FCF75	7/29/2020	6/27/2024

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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



Intermediate CA Certificates ¹				
Common Name	SHA2 Thumbprint	SPKI Hash	Valid From	Valid To
Microsoft Azure ECC TLS Issuing CA 01	2CAEFBB55E70DF5A8985FE9BC10DD56A40C3DEDAB3DA1530A29682015C5B7C66	3993B1F49242DC9B 120D28C55F688403 7FC40FA80285ADCB D59ACE791368CB1F	1/17/2020	6/27/2024
Microsoft Azure ECC TLS Issuing CA 02	4EC439672A443401A66E27947CC3B5897F132B667F712CC1A37018A3CC85B16A	3A175427EC2BA4F4 6DA57E77B64CAA5 4B290A0DA5D0825AF 7BC31041A4034360	1/17/2020	6/27/2024
Microsoft Azure ECC TLS Issuing CA 05	624D5576A652B2130768BFE84B965EEFFFD91603D25CD5F7155A7DC2789DAC38	934F4CCE6C2244F9 0F9A4A60994B69AC C93FB802D255E74D 2ED7CE06408CBD71	1/17/2020	6/27/2024
Microsoft Azure ECC TLS Issuing CA 06	151A3E5969C6616EB637A8722B174CFD95387AACE78D57C3BD23F0CB3008186A	C818E7ADC99C529D A7CA50D15A742F48 F46CA66866D5FFDF 3AE2ABB0D89A49D0	1/17/2020	6/27/2024
Microsoft Azure TLS Issuing CA 01	0437AB2EC2C2B4890296C135034B21DB146434B8317EE703AA8AA943C5EA51AE	347C2EB1B0BBC3CE 382734E6BC8448A3 C34BEC3E92B484CA F69873160B498B4C	1/17/2020	6/27/2024
Microsoft Azure TLS Issuing CA 02	D39CE39FF6F449D4F3391EE2004D705EC22F99CFFCA40A88F85DB26454ADDBD1	CC0C1FC76885710E 6F30E09CF6FB7E317 2DD2E5D3C12AB8D B0E5A00C5D213B0F	1/17/2020	6/27/2024
Microsoft Azure TLS Issuing CA 05	AB3203B3EA2017D509726A1D82293EFFCB8C42CEB52C9AF1C0EEE96B5C02BCBA	E22E21D2337D3513 ABD7128923E4D0D5 0FD921F5233CC5ED 99652C0D1DCF8E2C	1/17/2020	6/27/2024
Microsoft Azure TLS Issuing CA 06	7DF4D3EF45798F8C4384FC702BA52A44CE7BD6298B141628D4ABABC7678F6467	5A5F0C158FBDCE28 C61BC4201070802B9 7E103EC9D3D9C5A 2D038576210FCF75	1/17/2020	6/27/2024

¹ The Intermediate CA certificates in this table issued on 3/11/2021 were all revoked on 5/6/2021.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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



Intermediate CA Certificates ¹				
Common Name	SHA2 Thumbprint	SPKI Hash	Valid From	Valid To
Microsoft ECC TLS Issuing AOC CA 01	5C64B1731A8138DEA7D11C9AE8622891F945EBA46825E7ABFE4754F0A6011AF8	A9DF77A5BFB79FA3 4CDB975D964A30D9	6/24/2021	6/24/2026
	9D8BB150C07B81C25799B7945978B036E4B49C593C882BE379A58D08E1C25074	FE7FC4E670BD39BF 1B8C2605E843DB54	3/11/2021	3/11/2026
Microsoft ECC TLS Issuing AOC CA 02	808CA1ABBF2FF1A9AC71887DDA71FF6FCA6C3B5224827F547515A4D9F7AF209	85FA29EB740D90CE 77EDDBE3AB6C66A5	6/24/2021	6/24/2026
	12FB2F53AC2D09E62128B00487E8B77D6E4A0F459DD8744D009393BD0DF697B5	DE3FC8BA94D6B295 5FB7D33B04231601	3/11/2021	3/11/2026
Microsoft ECC TLS Issuing EOC CA 01	2769381532D96183ED39BDC4E323F3C520FBE6ACF3BDA3022239DDFC44C8380	EDE152DA0C19D6C3 BB3168D11E409019	6/24/2021	6/24/2026
	568E4046F384D0FDD9D06A8029E6BF38EED8904C1E0B44F99DA607F68672093E	19646BB6998CD5E7 D0FBE6537FFF42EF	3/11/2021	3/11/2026
Microsoft ECC TLS Issuing EOC CA 02	659C0F902D6059FBD1FCA528839F20604B80C74364E58F9D48A2291F813ED82D	21CD47E3200B2D7F 13567DF9E698EC21	6/24/2021	6/24/2026
	2DEEA0712931179BF1EF721070A30A1AB997F64C683EAB88DCE258D040D9AD25	ACAC77A8F4A2A117 3F4EAB23B2048967	3/11/2021	3/11/2026
Microsoft RSA TLS Issuing AOC CA 01	481E582A206A7D7040CCDA17CF25D349785A2AB94ED7552AB254DCD38B032ECO	7484F2F1618D35F6 F239C05BAD30B8B7	6/24/2021	6/24/2026
	13E295A5A6ECA8391126E752B131B316675D187266BCF537892F839454B9480	AD93C7024D4000D3 87141417EE3DDBF4	3/11/2021	3/11/2026
Microsoft RSA TLS Issuing AOC CA 02	D77C45C1587731C4632C19D6F3C9FE832626615C879EA053664A4B26EB2293EC	F19A176BC779C776 09427F441B995F14	6/24/2021	6/24/2026
	2AF3B34A5FD0EDC546E2E714208B6C380A5D5C553EDCA3A306A9E442C2389AAE	CAB9A19D87CDDD9 2725E4997CB0878BC	3/11/2021	3/11/2026
Microsoft RSA TLS Issuing EOC CA 01	5EA3857EACD4C7CA5ACBCA9C4627E26F3072038D191A29D4C3F9464B2E5F00C6	1F1D8E7685CE8255 088F791BFD3FB927	6/24/2021	6/24/2026
	E204F2682F5F630E360256ABD722DFF475432053128FC4274649F65D14EE1A36	F50AC1007091B5BB C3347EFBC5D9A80C	3/11/2021	3/11/2026
Microsoft RSA TLS Issuing EOC CA 02	4D55BC4ABEB7D37FAB57E573ACCE83133E36212C864E003FBCB30B5FC248B011	89E1EF9BD893880F CA4C2D0BA71EC93	6/24/2021	6/24/2026
	C97634113A97DFD13D516B9B7FA1B886635C725BDF70BC0A7891DF8E3FF0F91C	DAF6C0AC14D5A999 6F3E16F9763995076	3/11/2021	3/11/2026



Tel: 314-889-1100
Fax: 314-889-1101
www.bdo.com

101 S Hanley Rd, Suite 800
St. Louis, MO 63105

REPORT OF THE INDEPENDENT ACCOUNTANT

To the management of Microsoft Public Key Infrastructure (“PKI”) Services, a service of Microsoft Corporation:

Scope

We have examined Microsoft 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 B](#), Microsoft PKI Services has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Microsoft PKI Services Certificate Policy (“CP”) and Microsoft PKI Services Third Party Certification Practice Statement (“CPS”) enumerated in [Attachment A](#)
- maintained effective controls to provide reasonable assurance that:
 - Microsoft PKI Services’ CPS is consistent with its CP; and
 - Microsoft PKI Services provides its services in accordance with its CP and CPS
- 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; 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, 2021 to April 30, 2022, based on the [WebTrust Principles and Criteria for Certification Authorities v2.2.1](#).

Microsoft PKI Services does not escrow its CA keys, does not provide subscriber key lifecycle management controls, and does not provide certificate suspension services. Accordingly, our assertion did not extend to controls that would address those criteria.



Certification Authority's Responsibilities

Microsoft 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 v2.2.1](#).

Independent Accountant's Responsibilities

Our responsibility is to express an opinion on Microsoft PKI Services management's assertion based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

The relative effectiveness and significance of specific controls at Microsoft 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.

Independent Accountant'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 Microsoft PKI Services' services other than its CA operations in the United States of America, and in Ireland, nor the suitability of any of Microsoft PKI Services' services for any customer's intended purpose.



Other Matters

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

Matter Topic		Matter Description
1	Certificate Content	For two (2) out of 45 code signing certificates selected for testing, the Certificate Policies extension contained a value corresponding to a DV SSL certificate instead of 2.23.140.1.4.1 corresponding to non-EV Code Signing certificates.
2	Certificate Status Validation	Microsoft's CPS requires Microsoft to provide OCSP responses for 10 years from revocation or expiration of the certificate. For two (2) out of two (2) expired code signing subscriber certificates selected for testing, OCSP provided a response of "Unknown", instead of a response of "Good" or "Revoked".

Use of the WebTrust Seal

Microsoft 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.

BDO USA, LLP

June 17, 2022



ATTACHMENT A - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY VERSIONS IN-SCOPE

Certificate Policy

Policy Name	Policy Version	Policy Date
Microsoft PKI Services Certificate Policy	Version 3.1.4	February 15, 2021
Microsoft PKI Services Certificate Policy	Version 3.1.5	February 15, 2022

Certification Practice Statement

Policy Name	Policy Version	Policy Date
Microsoft PKI Services Third Party Certificate Practice Statement	Version 1.0.0	February 10, 2021
Microsoft PKI Services Third Party Certificate Practice Statement	Version 1.0.1	February 15, 2022



ATTACHMENT B - IN-SCOPE CAs

Root CA			
Common Name	SHA2 Thumbprint	Valid From	Valid To
CN = Microsoft Identity Verification Root Certificate Authority 2020 O = Microsoft Corporation C = US	5367F20C7ADE0E2BCA790915056D086B720C33C1FA2A2661ACF787E3292E1270	4/16/2020	4/16/2045

Intermediate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
CN = Microsoft ID Verified Code Signing PCA 2021 O = Microsoft Corporation C = US	3D29798CC5D3F0644A7E0DC9CB1CADE523EA5EC83B335109B605BFEEA7D5F5C1	4/1/2021	4/1/2036
CN = Microsoft ID Verified CS AOC CA 01 O = Microsoft Corporation C = US	7EE1F718CAE6B4D25D10115A367D84B7704E06BD6F8B498825FD42C852574BE9	4/13/2021	4/13/2026
CN = Microsoft ID Verified CS AOC CA 02 O = Microsoft Corporation C = US	E82D27596C5DDF9F11E8B6981F5D018211BF2580F0619E5954BAD400175F38D0	4/13/2021	4/13/2026
CN = Microsoft ID Verified CS EOC CA 01 O = Microsoft Corporation C = US	2FAA1C92228D5A05E07BAECFAA365F90A9B2F2DD846B014AE95880BAC3A976BB	4/13/2021	4/13/2026
CN = Microsoft ID Verified CS EOC CA 02 O = Microsoft Corporation C = US	B96CCAB201048A0AC2BA07AEA08D6DBEEA1688F55380A369B14A7BE11AEF828D	4/13/2021	4/13/2026



Timestamp Authority CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
CN = Microsoft Public RSA Timestamping CA 2020 O = Microsoft Corporation C = US	36E731CFA9BFD69DAFB643809F6DEC500902F7197DAEAAD86EA0159A2268A2B8	11/19/2020	11/19/2035



MICROSOFT PUBLIC KEY INFRASTRUCTURE SERVICES MANAGEMENT'S ASSERTION

Microsoft Public Key Infrastructure ("PKI") Services operates the Certification Authority ("CA") services for the root and other CAs enumerated in [Attachment B](#), 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 Microsoft PKI Services is responsible for establishing controls over its CA operations, including its CA business practices disclosure on its [repository](#), 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, controls placed into operation can only provide reasonable assurance with respect to Microsoft PKI Services' CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

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

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its Microsoft PKI Services Certificate Policy ("CP") and Microsoft PKI Services Third Party Certification Practice Statement ("CPS") enumerated in [Attachment A](#)
- maintained effective controls to provide reasonable assurance that:
 - Microsoft PKI Services' CPS is consistent with its CP; and
 - Microsoft PKI Services' provides its services in accordance with its CP and CPS
- 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; 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, 2021 to April 30, 2022 based on the [WebTrust Principles and Criteria for Certification Authorities v2.2.1](#).

CA Business Practices Disclosure

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

CA Business Practices Management

- CPS Management
- CP 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 Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Transportation
- CA Key Migration

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey



- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA Certificate and Cross Certificate Lifecycle Management Controls

- Subordinate CA Certificate and Cross Certificate Lifecycle Management

Microsoft PKI Services does not escrow its CA keys, does not provide subscriber key lifecycle management controls, and does not provide certificate suspension services. Accordingly, our assertion did not extend to controls that would address those criteria.

33F845FB21044B2
Raza Syed
DocuSigned By: Raza Syed

6/17/2022

Raza Syed
Distinguished Engineer, Product Release & Security Services

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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



ATTACHMENT A - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY VERSIONS IN-SCOPE

Certificate Policy

Policy Name	Policy Version	Policy Date
Microsoft PKI Services Certificate Policy	Version 3.1.4	February 15, 2021
Microsoft PKI Services Certificate Policy	Version 3.1.5	February 15, 2022

Certification Practice Statement

Policy Name	Policy Version	Policy Date
Microsoft PKI Services Third Party Certificate Practice Statement	Version 1.0.0	February 10, 2021
Microsoft PKI Services Third Party Certificate Practice Statement	Version 1.0.1	February 15, 2022

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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



ATTACHMENT B - IN-SCOPE CAs

Root CA			
Common Name	SHA2 Thumbprint	Valid From	Valid To
CN = Microsoft Identity Verification Root Certificate Authority 2020 O = Microsoft Corporation C = US	5367F20C7ADE0E2BCA790915056D086B720C33C1FA2A2661ACF787E3292E1270	4/16/2020	4/16/2045

Intermediate CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
CN = Microsoft ID Verified Code Signing PCA 2021 O = Microsoft Corporation C = US	3D29798CC5D3F0644A7E0DC9CB1CADE523EA5EC83B335109B605BFEEA7D5F5C1	4/1/2021	4/1/2036
CN = Microsoft ID Verified CS AOC CA 01 O = Microsoft Corporation C = US	7EE1F718CAE6B4D25D10115A367D84B7704E06BD6F8B498825FD42C852574BE9	4/13/2021	4/13/2026
CN = Microsoft ID Verified CS AOC CA 02 O = Microsoft Corporation C = US	E82D27596C5DDF9F11E8B6981F5D018211BF2580F0619E5954BAD400175F38D0	4/13/2021	4/13/2026
CN = Microsoft ID Verified CS EOC CA 01 O = Microsoft Corporation C = US	2FAA1C92228D5A05E07BAECFAA365F90A9B2F2DD846B014AE95880BAC3A976BB	4/13/2021	4/13/2026
CN = Microsoft ID Verified CS EOC CA 02 O = Microsoft Corporation C = US	B96CCAB201048A0AC2BA07AEA08D6DBEEA1688F55380A369B14A7BE11AEF828D	4/13/2021	4/13/2026

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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



Timestamp Authority CAs			
Common Name	SHA2 Thumbprint	Valid From	Valid To
CN = Microsoft Public RSA Timestamping CA 2020 O = Microsoft Corporation C = US	36E731CFA9BFD69DAFB643809F6DEC500902F7197DAEAAAD86EA0159A2268A2B8	11/19/2020	11/19/2035



Tel: 314-889-1100
Fax: 314-889-1101
www.bdo.com

101 S Hanley Rd, #800
St. Louis, MO 63105

REPORT OF INDEPENDENT ACCOUNTANT

To the Management of Microsoft Public Key Infrastructure (“PKI”) Services, a service of Microsoft Corporation:

Scope

We have examined Microsoft 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 B](#), Microsoft PKI Services has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of its Microsoft PKI Services Certificate Policy (“CP”) and Microsoft PKI Services Corporate Certification Practice Statement (“CPS”) enumerated in [Attachment A](#)
- maintained effective controls to provide reasonable assurance that:
 - Microsoft PKI Services’ CPS is consistent with its CP; and
 - Microsoft PKI Services provides its services in accordance with its CP and CPS
- 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; 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, 2021 to April 30, 2022, based on the [WebTrust Principles and Criteria for Certification Authorities v2.2.1](#).

Microsoft PKI Services does not escrow its CA keys, does not provide subscriber key lifecycle management services, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.

Certification Authority’s Responsibilities

Microsoft 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 v2.2.1](#).



Independent Accountant's Responsibilities

Our responsibility is to express an opinion on Microsoft PKI Services management's assertion based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

The relative effectiveness and significance of specific controls at Microsoft 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.

Independent Accountant'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 Microsoft PKI Services' services other than its CA operations in the United States of America and in Ireland, nor the suitability of any of Microsoft PKI Services' services for any customer's intended purpose.



Use of the WebTrust Seal

Microsoft 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.

BDO USA, LLP

June 17, 2022



ATTACHMENT A - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY VERSIONS IN-SCOPE

Certificate Policy

Policy Name	Policy Version	Policy Date
Microsoft PKI Services Certificate Policy	Version 3.1.4	February 15, 2021
Microsoft PKI Services Certificate Policy	Version 3.1.5	February 15, 2022

Certification Practice Statement

Policy Name	Policy Version	Policy Date
Microsoft PKI Services Corporate Certificate Practice Statement	Version 3.1.4	July 28, 2020
Microsoft PKI Services Corporate Certificate Practice Statement	Version 3.1.5	October 19, 2021
Microsoft PKI Services Corporate Certificate Practice Statement	Version 3.1.6	January 19, 2022



ATTACHMENT B - IN-SCOPE CAs

Root CAs			
Subject Common Name	SHA2 Thumbprint	Valid From	Valid To
Microsoft Time Stamp Root Certificate Authority 2014	65AF95F4BE86847344634282F941B2E605063EF0C8542F014CA088D182109E4F	10/22/2014	10/22/2039
Microsoft ECC Product Root Certificate Authority 2018	CACA93B9D23D2B6FA76E8B8471931E0DF3EC6F63AF3CDBB936C41954A1872326	2/27/2018	2/27/2043
Microsoft Root Certificate Authority 2010	DF545BF919A2439C36983B54CDFC903DFA4F37D3996D8D84B4C31EEC6F3C163E	6/23/2010	6/23/2035
Microsoft Root Certificate Authority 2011	847DF6A78497943F27FC72EB93F9A637320A02B561D0A91B09E87A7807ED7C61	3/22/2011	3/22/2036
Microsoft ECC TS Root Certificate Authority 2018	3FD4BE8BAAD2F26E1BDE06C7584BB720DD1A972D111F5A4999BC44B08FB4960D	2/27/2018	2/27/2043
Microsoft Root Certificate Authority 2014	B13DDACB6431E702356A0002730B933C65272F9180D53BCD4577F8D500680A42	10/22/2014	10/22/2039



Intermediate CAs			
Subject Common Name	SHA2 Thumbprint	Valid From	Valid To
Microsoft Time Stamp CA 2015	857AEC60913116E2B61190B1E86FA001F27E8D165FAED492F829313E8212B666	3/25/2015	3/25/2030
Microsoft ECC Update Secure Server CA 2.2	6345FD68446C011FD442A04A37E8407A51E548DE61A6685633134EDD67292F1A	12/7/2018	12/7/2033
Microsoft ECC Update Signing CA 2.1	73DF319F3BF18FA9C9D0B38DAABA98038C4F867D3C9CE609737DFA682BDA1FFB	9/28/2018	9/28/2033
Microsoft ECC Update Signing CA 2.3	C67E5F87209E33B857566DBF525FC0869EF8C715E5BA4A752DAE2A38DB16E14C	9/28/2018	9/28/2033
Microsoft ECC Update Signing CA 2.2	3EBC65CCB963BAA55AFA2F0D24A20044C7D17D97208EA2B318778C505CB7C08F	9/28/2018	9/28/2033
Microsoft ECC Content Distribution Secure Server CA 2.1	E39F93F3B2B40FD3C41DE7DFA7D0B0CB6C4D8F97CBAB2BB81C178F4B5F3C7EED	12/7/2018	12/7/2033
Microsoft ECC Update Secure Server CA 2.1	21158AD4DCE10197239A87EBEB4D8D47E9E9BE716AD497A2E036774CAF5072CF	9/28/2018	9/28/2033
Microsoft ECC Content Distribution Secure Server CA 2.2	959D932A756F59612F2D757926D8AD3B11CB2684CA9203AE281F5CC26049BE94	12/7/2018	12/7/2033
Microsoft ECC Certificate List PCA 2018	C307C2757F1026AA755DC7830E43C61BA30BFE178FB9F92B621B830B3DA21C83	3/1/2018	3/1/2033
Microsoft ECC Code Signing PCA 2018	E673905E74CCA3307C5E2C7D1E78DCA1F6F2783A21F8B02B58472E304C680DB8	3/1/2018	3/1/2033
Microsoft Time-Stamp PCA 2010	86EC118D1EE69670A46E2BE29C4B4208BE043E36600D4E1DD3F3D515CA119020	7/1/2010	7/1/2025
Microsoft Windows Third Party Component CA 2014	A0F259A07039908EEB943E223FDF996E5E1E131D9AA6A602FF4672F7B9298AEE	10/15/2014	10/15/2029
Microsoft Windows Phone Production PCA 2012	E6A9B56A89AA3B191D23A6FB7FECB1F09DED4552A682FCF72B1D479C3B23C9BA	7/24/2012	7/24/2027
Microsoft Windows Phone PCA 2011	AE378D79D44CC75CEE8BAE50DD8BCBF2D4FF7C598B62FE75C3CE234C4001AFD9	2/28/2011	6/23/2035
Microsoft Windows Production PCA 2011	E8E95F0733A55E8BAD7BE0A1413EE23C51FCEA64B3C8FA6A786935FDDCC71961	10/19/2011	10/19/2026
Microsoft Code Signing PCA 2010	9AAD6C1A83A1B974BA574A995AF35B8CA772DA919270DB1605A8B81E1BBC896F	7/6/2010	7/6/2025
Microsoft Windows Third Party Component CA 2012	9D08973E4D108DA40A1A0B274180E17371134B4DD1621FA5C1F131B739B4B823	4/18/2012	4/18/2027
Windows Azure StorSimple CA 2013	854B33F368F4D9BA80F4797D8E7150DC8754E7EF9E06ACBEC16F92C06E20DEBF	10/15/2013	10/15/2028
Microsoft Certificate List CA 2011	A53A400DF29EC7B8C8FCE7CFFFE47334F43B1642E604DD0307491737EBBC00CE	3/29/2011	3/29/2026
Microsoft Windows PCA 2010	F01614A7A81BA477F0746CF2DE71B20DDDEC709E756C9EA57CB67F93F25BA9FD	7/6/2010	7/6/2025
Microsoft Time Stamp Root Certificate Authority 2014	A303E478DD3CBC0E47A290FD5B59AF5C017A95E4886EC354EC6DA8B9380EE399	8/11/2016	6/22/2035
Microsoft Time-Stamp PCA 2010	EBEC1EDD9E140D9C105CC62B15A915C5443DDC514A35E5773C09AFB0274C7BA5	9/30/2021	9/30/2030



Intermediate CAs			
Subject Common Name	SHA2 Thumbprint	Valid From	Valid To
Microsoft ECC TS Root Certificate Authority 2018	D4D27BC233F38B4414617E72871F54D40758AB988072D9FFEC31AEDA60ECC6D0	9/28/2018	6/9/2035
Microsoft Update Signing CA 2.1	882F36D6F0DABF4B017FC6E8EA6D4F0F2786300D7B8210C3AE5C793F95E1C0C9	6/19/2012	6/19/2027
Microsoft Update Signing CA 2.3	46B4D5B761CA7B14D4877C3B2D3F22DBF92BC34B694E971E942517DABEB4B06C	6/19/2012	6/19/2027
Microsoft Update Secure Server CA 2.2	C1BC7AC733DEC68A6A6AF944A5A2B4F79F492ABAACE213811F6EF681D7861B57	6/21/2012	6/21/2027
Microsoft MarketPlace PCA 2011	5A9D217E71180301A044E4CFBDE431FDF4C1CFC998B1B6343B5A10AA9E4CDE98	3/28/2011	3/28/2031
Microsoft Marketplace CA G 028	951D2F622C2B542C00F70E19833F15F880B113BD2D309B0643C0020DBD729A94	5/14/2019	5/14/2024
Microsoft Marketplace CA G 022	2389277AFD831C5D4BD59B3CF9A37DC894F301641E61D3BB8849CD189B0B214C	4/18/2019	4/18/2024
Microsoft Marketplace CA G 026	57F0FDAF21AC56B6C30816572711FEAE9714328FEC7AA6332EF11AF5AAA8ED49	4/18/2019	4/18/2024
Microsoft Marketplace CA G 023	38F09140E246E5AC58156C20B6C9A5230C24235146CFEC51BE26303A787F978C	4/18/2019	4/18/2024
Microsoft Marketplace CA G 027	A61DA8C095F568584F086B1301D719EFE0C84B374006BE2AAE48FCFBF1F0A0D2	4/18/2019	4/18/2024
Microsoft Marketplace Production CA 2011	CA92943AB468CBB9604A97F909AE31C04577F5ADCBF7565F40C5837A072A5FE4	9/9/2021	9/9/2030
Microsoft Marketplace CA G 025	7D6A49D173B551FB4E3351CB4445264F2EC54E170CC4773FD47349A7340A83E3	4/18/2019	4/18/2024
Microsoft Marketplace CA G 021	B879BD0D3DD492E52C7B3E7161794D07D8ED8CE83421188A800315C2E93DCE06	4/18/2019	4/18/2024
Microsoft Marketplace CA G 024	6466C53BCAA7631A2B932C6CA883CB7A6069AA15E0834D0F567E269EA56B4F33	5/14/2019	5/14/2024
Microsoft Update Signing CA 2.2	24919D52EFB9ECBEC6C1D24CBC2E10D041B516B9410D6CEB75FF2F348BD0E5C8	6/19/2012	6/19/2027
Microsoft Content Distribution Secure Server CA 2.2	B90776868F9AA9F0048D2BBEC85908CD2735A36BACB5886AF5C3458303703471	12/7/2018	12/7/2033
Microsoft Code Signing PCA 2011	56DA8722AFD94066FFE1E4595473A4854892B843A0827D53FB7D8F4AEED1E18B	7/8/2011	7/8/2026
Microsoft Content Distribution Secure Server CA 2.1	64EBAE10EF707ECF156B560A1C9236455A5E9F1C16F270996E41D5F0DFEDA561	12/7/2018	12/7/2033
Microsoft Update Secure Server CA 2.1	6139E2DF97DC93BF7E90A303F75B3968FD06C57316B45E94DCFF773707CF2754	6/21/2012	6/21/2027
Microsoft Azure Attestation PCA 2019	D8A4236A2BD59061D008139D2071EA7BEF642E1B959A0CE6626666B43BD2C095	5/30/2019	5/30/2034
Microsoft Secure Server CA 2011	83688F2AEF71386E0936C4B3013B07E8E0C796D8427716DD48B2A63D79509129	10/18/2011	10/18/2026
Microsoft Windows Third Party Component CA 2013	8EF01BB5E07987053659E039E5A72580C88C444BC1A31AB412CE81A4AD53044E	5/1/2013	5/1/2028
VS Package Repositories CA	AC415BBB3EE2E11B5EFD11808B8026B02736A82480C26AB7569FC19195344202	1/20/2022	3/22/2036



MICROSOFT PUBLIC KEY INFRASTRUCTURE SERVICES MANAGEMENT'S ASSERTION

Microsoft Public Key Infrastructure (“PKI”) Services operates the Certification Authority (“CA”) services for the CAs enumerated in [Attachment B](#), 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 Microsoft PKI Services is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its [repository](#), 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 Microsoft PKI Services CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

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

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in the applicable versions of its Microsoft PKI Services Certificate Policy (“CP”) and Microsoft PKI Services Corporate Certification Practice Statement (“CPS”) enumerated in [Attachment A](#)
- maintained effective controls to provide reasonable assurance that:
 - Microsoft PKI Services’ CPS is consistent with its CP; and
 - Microsoft PKI Services provides its services in accordance with its CP and CPS
- 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; 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, 2021 to April 30, 2022, based on the [WebTrust Principles and Criteria for Certification Authorities v2.2.1](#), including the following:

CA Business Practices Disclosure

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

CA Business Practices Management

- CPS Management
- CP 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
- Systems 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 Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Transportation
- CA Key Migration

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

- Subordinate CA Certificate and Cross Certificate Lifecycle Management

Microsoft PKI Services does not escrow CA keys, does not provide subscriber key lifecycle management services, and does not provide certificate suspension services. Accordingly, our assertion does not extend to controls that would address those criteria.

33F845FB21044B2
Raza Syed
DocuSigned By: Raza Syed

6/17/2022

Raza Syed
Distinguished Engineer, Product Release & Security Services

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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



ATTACHMENT A - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY VERSIONS IN-SCOPE

Certificate Policy

Policy Name	Policy Version	Policy Date
Microsoft PKI Services Certificate Policy	Version 3.1.4	February 15, 2021
Microsoft PKI Services Certificate Policy	Version 3.1.5	February 15, 2022

Certification Practice Statement

Policy Name	Policy Version	Policy Date
Microsoft PKI Services Corporate Certificate Practice Statement	Version 3.1.4	July 28, 2020
Microsoft PKI Services Corporate Certificate Practice Statement	Version 3.1.5	October 19, 2021
Microsoft PKI Services Corporate Certificate Practice Statement	Version 3.1.6	January 19, 2022

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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



ATTACHMENT B - IN-SCOPE CAs

Root CAs			
Subject Common Name	SHA2 Thumbprint	Valid From	Valid To
Microsoft Time Stamp Root Certificate Authority 2014	65AF95F4BE86847344634282F941B2E605063EF0C8542F014CA088D182109E4F	10/22/2014	10/22/2039
Microsoft ECC Product Root Certificate Authority 2018	CACA93B9D23D2B6FA76E8B8471931E0DF3EC6F63AF3CDBB936C41954A1872326	2/27/2018	2/27/2043
Microsoft Root Certificate Authority 2010	DF545BF919A2439C36983B54CDFC903DFA4F37D3996D8D84B4C31EEC6F3C163E	6/23/2010	6/23/2035
Microsoft Root Certificate Authority 2011	847DF6A78497943F27FC72EB93F9A637320A02B561D0A91B09E87A7807ED7C61	3/22/2011	3/22/2036
Microsoft ECC TS Root Certificate Authority 2018	3FD4BE8BAAD2F26E1BDE06C7584BB720DD1A972D111F5A4999BC44B08FB4960D	2/27/2018	2/27/2043
Microsoft Root Certificate Authority 2014	B13DDACB6431E702356A0002730B933C65272F9180D53BCD4577F8D500680A42	10/22/2014	10/22/2039

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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



Intermediate CAs			
Subject Common Name	SHA2 Thumbprint	Valid From	Valid To
Microsoft Time Stamp CA 2015	857AEC60913116E2B61190B1E86FA001F27E8D165FAED492F829313E8212B666	3/25/2015	3/25/2030
Microsoft ECC Update Secure Server CA 2.2	6345FD68446C011FD442A04A37E8407A51E548DE61A6685633134EDD67292F1A	12/7/2018	12/7/2033
Microsoft ECC Update Signing CA 2.1	73DF319F3BF18FA9C9D0B38DAABA98038C4F867D3C9CE609737DFA682BDA1FFB	9/28/2018	9/28/2033
Microsoft ECC Update Signing CA 2.3	C67E5F87209E33B857566DBF525FC0869EF8C715E5BA4A752DAE2A38DB16E14C	9/28/2018	9/28/2033
Microsoft ECC Update Signing CA 2.2	3EBC65CCB963BAA55AFA2F0D24A20044C7D17D97208EA2B318778C505CB7C08F	9/28/2018	9/28/2033
Microsoft ECC Content Distribution Secure Server CA 2.1	E39F93F3B2B40FD3C41DE7DFA7D0B0CB6C4D8F97CBA2BB81C178F4B5F3C7EED	12/7/2018	12/7/2033
Microsoft ECC Update Secure Server CA 2.1	21158AD4DCE10197239A87EBEB4D8D47E9E9BE716AD497A2E036774CAF5072CF	9/28/2018	9/28/2033
Microsoft ECC Content Distribution Secure Server CA 2.2	959D932A756F59612F2D757926D8AD3B11CB2684CA9203AE281F5CC26049BE94	12/7/2018	12/7/2033
Microsoft ECC Certificate List PCA 2018	C307C2757F1026AA755DC7830E43C61BA30BFE178FB9F92B621B830B3DA21C83	3/1/2018	3/1/2033
Microsoft ECC Code Signing PCA 2018	E673905E74CCA3307C5E2C7D1E78DCA1F6F2783A21F8B02B58472E304C680DB8	3/1/2018	3/1/2033
Microsoft Time-Stamp PCA 2010	86EC118D1EE69670A46E2BE29C4B4208BE043E36600D4E1DD3F3D515CA119020	7/1/2010	7/1/2025
Microsoft Windows Third Party Component CA 2014	A0F259A07039908EEB943E223FDF996E5E1E131D9AA6A602FF4672F7B9298AEE	10/15/2014	10/15/2029
Microsoft Windows Phone Production PCA 2012	E6A9B56A89AA3B191D23A6FB7FECB1F09DED4552A682FCF72B1D479C3B23C9BA	7/24/2012	7/24/2027
Microsoft Windows Phone PCA 2011	AE378D79D44CC75CEE8BAE50DD8BCBF2D4FF7C598B62FE75C3CE234C4001AFD9	2/28/2011	6/23/2035
Microsoft Windows Production PCA 2011	E8E95F0733A55E8BAD7BE0A1413EE23C51FCEA64B3C8FA6A786935FDDCC71961	10/19/2011	10/19/2026
Microsoft Code Signing PCA 2010	9AAD6C1A83A1B974BA574A995AF35B8CA772DA919270DB1605A8B81E1BBC896F	7/6/2010	7/6/2025
Microsoft Windows Third Party Component CA 2012	9D08973E4D108DA40A1A0B274180E17371134B4DD1621FA5C1F131B739B4B823	4/18/2012	4/18/2027
Windows Azure StorSimple CA 2013	854B33F368F4D9BA80F4797D8E7150DC8754E7EF9E06ACBEC16F92C06E20DEBF	10/15/2013	10/15/2028
Microsoft Certificate List CA 2011	A53A400DF29EC7B8C8FCE7CFFFE47334F43B1642E604DD0307491737EBBC00CE	3/29/2011	3/29/2026
Microsoft Windows PCA 2010	F01614A7A81BA477F0746CF2DE71B20DDDEC709E756C9EA57CB67F93F25BA9FD	7/6/2010	7/6/2025
Microsoft Time Stamp Root Certificate Authority 2014	A303E478DD3CBC0E47A290FD5B59AF5C017A95E4886EC354EC6DA8B9380EE399	8/11/2016	6/22/2035

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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



Intermediate CAs			
Subject Common Name	SHA2 Thumbprint	Valid From	Valid To
Microsoft Time-Stamp PCA 2010	EBEC1EDD9E140D9C105CC62B15A915C5443DDC514A35E5773C09AFB0274C7BA5	9/30/2021	9/30/2030
Microsoft ECC TS Root Certificate Authority 2018	D4D27BC233F38B4414617E72871F54D40758AB988072D9FFEC31AEDA60ECC6D0	9/28/2018	6/9/2035
Microsoft Update Signing CA 2.1	882F36D6F0DABF4B017FC6E8EA6D4F0F2786300D7B8210C3AE5C793F95E1C0C9	6/19/2012	6/19/2027
Microsoft Update Signing CA 2.3	46B4D5B761CA7B14D4877C3B2D3F22DBF92BC34B694E971E942517DABEB4B06C	6/19/2012	6/19/2027
Microsoft Update Secure Server CA 2.2	C1BC7AC733DEC68A6A6AF944A5A2B4F79F492ABAACE213811F6EF681D7861B57	6/21/2012	6/21/2027
Microsoft MarketPlace PCA 2011	5A9D217E71180301A044E4CFBDE431FDF4C1CFC998B1B6343B5A10AA9E4CDE98	3/28/2011	3/28/2031
Microsoft Marketplace CA G 028	951D2F622C2B542C00F70E19833F15F880B113BD2D309B0643C0020DBD729A94	5/14/2019	5/14/2024
Microsoft Marketplace CA G 022	2389277AFD831C5D4BD59B3CF9A37DC894F301641E61D3BB8849CD189B0B214C	4/18/2019	4/18/2024
Microsoft Marketplace CA G 026	57F0FDAF21AC56B6C30816572711FEAE9714328FEC7AA6332EF11AF5AAA8ED49	4/18/2019	4/18/2024
Microsoft Marketplace CA G 023	38F09140E246E5AC58156C20B6C9A5230C24235146CFEC51BE26303A787F978C	4/18/2019	4/18/2024
Microsoft Marketplace CA G 027	A61DA8C095F568584F086B1301D719EFE0C84B374006BE2AAE48FCFBF1F0A0D2	4/18/2019	4/18/2024
Microsoft Marketplace Production CA 2011	CA92943AB468CBB9604A97F909AE31C04577F5ADCBF7565F40C5837A072A5FE4	9/9/2021	9/9/2030
Microsoft Marketplace CA G 025	7D6A49D173B551FB4E3351CB4445264F2EC54E170CC4773FD47349A7340A83E3	4/18/2019	4/18/2024
Microsoft Marketplace CA G 021	B879BD0D3DD492E52C7B3E7161794D07D8ED8CE83421188A800315C2E93DCE06	4/18/2019	4/18/2024
Microsoft Marketplace CA G 024	6466C53BCAA7631A2B932C6CA883CB7A6069AA15E0834D0F567E269EA56B4F33	5/14/2019	5/14/2024
Microsoft Update Signing CA 2.2	24919D52EFB9ECBEC6C1D24CBC2E10D041B516B9410D6CEB75FF2F348BD0E5C8	6/19/2012	6/19/2027
Microsoft Content Distribution Secure Server CA 2.2	B90776868F9AA9F0048D2BBEC85908CD2735A36BACB5886AF5C3458303703471	12/7/2018	12/7/2033
Microsoft Code Signing PCA 2011	56DA8722AFD94066FFE1E4595473A4854892B843A0827D53FB7D8F4AEED1E18B	7/8/2011	7/8/2026
Microsoft Content Distribution Secure Server CA 2.1	64EBAE10EF707ECF156B560A1C9236455A5E9F1C16F270996E41D5F0DFEDA561	12/7/2018	12/7/2033
Microsoft Update Secure Server CA 2.1	6139E2DF97DC93BF7E90A303F75B3968FD06C57316B45E94DCFF773707CF2754	6/21/2012	6/21/2027
Microsoft Azure Attestation PCA 2019	D8A4236A2BD59061D008139D2071EA7BEF642E1B959A0CE6626666B43BD2C095	5/30/2019	5/30/2034
Microsoft Secure Server CA 2011	83688F2AEF71386E0936C4B3013B07E8E0C796D8427716DD48B2A63D79509129	10/18/2011	10/18/2026

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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



Intermediate CAs			
Subject Common Name	SHA2 Thumbprint	Valid From	Valid To
Microsoft Windows Third Party Component CA 2013	8EF01BB5E07987053659E039E5A72580C88C444BC1A31AB412CE81A4AD53044E	5/1/2013	5/1/2028
VS Package Repositories CA	AC415BBB3EE2E11B5EFD11808B8026B02736A82480C26AB7569FC19195344202	1/20/2022	3/22/2036