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

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

# REPORT OF THE INDEPENDENT ACCOUNTANT

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

## 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, throughout the period May 1, 2020 to April 30, 2021 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, 2020 to April 30, 2021 based on the WebTrust Principles and Criteria for Certification Authorities v2.2.

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.

**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.

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**

Because of the nature and inherent limitations of controls, Microsoft PKI Services' ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

**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 | CPS Disclosure | Microsoft disclosed in Mozilla Bug 1693930 and Bug 1693932 that they had failed to update their CPS to remove deprecated domain control validation methods and their subscriber certificate maximum validity period, respectively. |
| 2 | Certificate Content | Microsoft disclosed in Mozilla Bug 1644936 that they issued 8 OV SSL certificates that were missing locality information. |
| | | Microsoft disclosed in Mozilla Bug 1705419 that they mis-issued a total of 5 certificates that contained underscores in the dNSName entry in the subjectAltName extension. |
| | | Microsoft disclosed in Mozilla Bug 1706860 that they mis-issued a total of 3 certificates that contained dNSName entries that had hyphens at the end of the labels, resulting in a not properly formed FQDN. |
| | | Microsoft disclosed in Mozilla Bug 1711147 that 8 of their intermediate CAs were missing the certificatePolicies extension. |
| 3 | Subject Validation | Microsoft disclosed in Mozilla Bug 1670337 that they were notified of mis-issued certificates where the domains listed in the certificates were not public. The notification and following internal investigation discovered a total of 8 certificates with this error, across 2 domains. |

The World Health Organization classified the COVID-19 outbreak as a pandemic in March 2020. Based on the continued increase in exposure globally, the gravity or length of the impact of the COVID-19 outbreak cannot be estimated at this time.

**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

August 5, 2021

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

| Policy Name | Policy Version | Policy Date |
|---|---|---|
| Microsoft PKI Services Certificate Policy | Version 3.1.2 | August 5, 2019 |
| Microsoft PKI Services Certificate Policy | Version 3.1.3 | July 28, 2020 |
| Microsoft PKI Services Certificate Policy | Version 3.1.4 | February 15, 2021 |
| Microsoft PKI Services Certification Practice Statement | Version 3.1.4 | April 23, 2020 |
| Microsoft PKI Services Certification Practice Statement | Version 3.1.5 | July 28, 2020 |
| Microsoft PKI Services Certification Practice Statement | Version 3.1.6 | August 25, 2020 |
| Microsoft PKI Services Certification Practice Statement | Version 3.1.7 | November 5, 2020 |
| Microsoft PKI Services Certification Practice Statement | Version 3.1.8 | February 15, 2021 |
| Microsoft PKI Services Certification Practice Statement | Version 3.1.9 | March 30, 2021 |

## ATTACHMENT B – IN-SCOPE CAs

| Root CAs | | | | |
|---|---|---|---|---|
| **Common Name** | **SHA2 Thumbprint** | **SPKI Hash** | **Valid From** | **Valid To** |
| Microsoft ECC Root Certificate Authority 2017 | FEA1884AB3AEA6D0DBEDBE4B9CD9FEC8655116300A86A856488FC488BB4B44D2 | 35F53CE1264611E03340FE37E1EC7D4CC986C5613DCA70FD04AA44545F2DAF28 | 7/26/2017 | 7/26/2042 |
| | 358DF39D764AF9E1B766E9C972DF352EE15CFAC227AF6AD1D70E8E4A6EDCBA02 | | 12/18/2019 | 7/18/2042 |
| Microsoft RSA Root Certificate Authority 2017 | ECDD47B5ACBFA328211E1BFF54ADEAC95E6991E3C1D50E27B527E903208040A1 | B2F7298B52BF2C3CAC4DDFE72DE4D682AC58957595982F2B62301AF597C699C5 | 7/26/2017 | 7/26/2042 |
| | C741F70F4B2A8D88BF2E71C14122EF53EF10EBA0CFA5E64CFA20F418853073E0 | | 12/18/2019 | 7/18/2042 |

| Cross-Signed CAs[1] | | | | |
|---|---|---|---|---|
| **Common Name** | **SHA2 Thumbprint** | **SPKI Hash** | **Valid From** | **Valid To** |
| Microsoft Azure ECC TLS Issuing CA 01 | 3458C7F787C30FE9AF3E58A7AB6877B1959AB7CC2C4581B070BDD38C39B84AF7 | 3993B1F49242DC9B120D28C55F6884037FC40FA80285ADCBD59ACE791368CB1F | 5/20/2020 | 6/27/2024 |
| | 949D6B4B761CA134AD3E7A8571186F580EE887F2C6B568B5140F4157F98D68DD | | 8/12/2020 | 6/27/2024 |
| Microsoft Azure ECC TLS Issuing CA 02 | FB862D0849258D7D96B6A2B0158D08142272E4D3CA825BFFC36305F5D28116C5 | 3A175427EC2BA4F46DA57E77B64CAA54B290A0DA5D0825AF7BC31041A4034360 | 5/20/2020 | 6/27/2024 |
| | 9C64A9A43E990E98FBCE8317B2D4C1C07FFE6E032DA8BB6D60A696E2FF038F1F | | 8/12/2020 | 6/27/2024 |
| Microsoft Azure ECC TLS Issuing CA 05 | 2BB470033D5777DAC2D78AF613F1E4657906BE3DF5B6E331EC79F5CD534D879B | 934F4CCE6C2244F90F9A4A60994B69ACC93FB802D255E74D2ED7CE06408CBD71 | 5/20/2020 | 6/27/2024 |
| | 003F71DC4820216575FC5AACFE3B1AEB76F72AEA5B8E8FCEFC80B9F517A4A612 | | 8/12/2020 | 6/27/2024 |
| Microsoft Azure ECC TLS Issuing CA 06 | A5E4A62B601006DC17E4ACAF497777BFD7D2F3E526FC70CA1F22094C8CB39166 | C818E7ADC99C529DA7CA50D15A742F48F46CA66866D5FFDF3AE2ABB0D89A49D0 | 5/20/2020 | 6/27/2024 |
| | 2975BAB51D00D862D0E16EEDEF8306A759C65CD4B9F00DAF50ECDFCB4EC396E4 | | 8/12/2020 | 6/27/2024 |
| Microsoft Azure TLS Issuing CA 01 | 6CA3E5D7720215F94544523E3C474B22DA69C732AE455DC82F8F5EE302EC55FC | 347C2EB1B0BBC3CE382734E6BC8448A3C34BEC3E92B484CAF69873160B498B4C | 5/20/2020 | 6/27/2024 |
| | 24C7299864E0A2A6964F551C0E8DF2461532FA8C48E4DBBB6080716691F190E5 | | 7/29/2020 | 6/27/2024 |
| Microsoft Azure TLS Issuing CA 02 | F7DBAD12E8B62B837BA7F6A01E1672999CFAF6929659B81B07F253576281F7BD | CC0C1FC76885710E6F30E09CF6FB7E3172DD2E5D3C12AB8DB0E5A00C5D213B0F | 5/20/2020 | 6/27/2024 |
| | 15A98761EBE011554DA3A46D206B0812CB2EB69AE87AAA11A6DD4CB84ED5142A | | 7/29/2020 | 6/27/2024 |
| Microsoft Azure TLS Issuing CA 05 | 4D5F5A79AEF092415FF681D9FA958F24FBFD74D26D3FFD153BC61E7C1B9C9920 | E22E21D2337D3513ABD7128923E4D0D50FD921F5233CC5ED99652C0D1DCF8E2C | 5/20/2020 | 6/27/2024 |
| | D6831BA43607F5AC19778D627531562AF55145F191CAB5EFAFA0E0005442B302 | | 7/29/2020 | 6/27/2024 |
| Microsoft Azure TLS Issuing CA 06 | 65F6C2B44154F5C6425F3C1C5B26E5C9E35717AFF6F451BD216A624F48FA06BF | 5A5F0C158FBDCE28C61BC4201070802B97E103EC9D3D9C5A2D038576210FCF75 | 5/20/2020 | 6/27/2024 |
| | 48FF8B494668C752304B48BFE818758987DEF6582E5F09B921F4B60BB3D6A8DD | | 7/29/2020 | 6/27/2024 |

[1] The Cross-Signed CA certificates in this table issued on 5/20/2020 were all revoked on 7/30/2020.

| Intermediate CAs | | | | |
|---|---|---|---|---|
| **Common Name** | **SHA2 Thumbprint** | **SPKI Hash** | **Valid From** | **Valid To** |
| Microsoft Azure ECC TLS Issuing CA 01 | 2CAEFBB55E70DF5A8985FE9BC10DD56A40C3DEDAB3DA1530A29682015C5B7C66 | 3993B1F49242DC9B120D28C55F6884037FC40FA80285ADCBD59ACE791368CB1F | 1/17/2020 | 6/27/2024 |
| Microsoft Azure ECC TLS Issuing CA 02 | 4EC439672A443401A66E27947CC3B5897F132B667F712CC1A37018A3CC85B16A | 3A175427EC2BA4F46DA57E77B64CAA54B290A0DA5D0825AF7BC31041A4034360 | 1/17/2020 | 6/27/2024 |
| Microsoft Azure ECC TLS Issuing CA 05 | 624D5576A652B2130768BFE84B965EEFFFD91603D25CD5F7155A7DC2789DAC38 | 934F4CCE6C2244F90F9A4A60994B69ACC93FB802D255E74D2ED7CE06408CBD71 | 1/17/2020 | 6/27/2024 |
| Microsoft Azure ECC TLS Issuing CA 06 | 151A3E5969C6616EB637A8722B174CFD95387AACE78D57C3BD23F0CB3008186A | C818E7ADC99C529DA7CA50D15A742F48F46CA66866D5FFDF3AE2ABB0D89A49D0 | 1/17/2020 | 6/27/2024 |
| Microsoft Azure TLS Issuing CA 01 | 0437AB2EC2C2B4890296C135034B21DB146434B8317EE703AA8AA943C5EA51AE | 347C2EB1B0BBC3CE382734E6BC8448A3C34BEC3E92B484CAF69873160B498B4C | 1/17/2020 | 6/27/2024 |
| Microsoft Azure TLS Issuing CA 02 | 647EF2DFAFAC46D8FC9C873D7C4BABF3F1C032AE62B58D6DA7B21F92EB1CAE7D | CC0C1FC76885710E6F30E09CF6FB7E3172DD2E5D3C12AB8DB0E5A00C5D213B0F | 1/17/2020 | 6/27/2024 |
| Microsoft Azure TLS Issuing CA 05 | AB3203B3EA2017D509726A1D82293EFFCB8C42CEB52C9AF1C0EEE96B5C02BCBA | E22E21D2337D3513ABD7128923E4D0D50FD921F5233CC5ED99652C0D1DCF8E2C | 1/17/2020 | 6/27/2024 |
| Microsoft Azure TLS Issuing CA 06 | 41830FE41CA1C0BEB2CD319EF4A2D2FD1D2164086509CA4CF90670B0CD0A6A6C | 5A5F0C158FBDCE28C61BC4201070802B97E103EC9D3D9C5A2D038576210FCF75 | 1/17/2020 | 6/27/2024 |

| Intermediate CAs | | | | |
|---|---|---|---|---|
| **Common Name** | **SHA2 Thumbprint** | **SPKI Hash** | **Valid From** | **Valid To** |
| Microsoft ECC TLS Issuing AOC CA 01 | 9D8BB150C07B81C25799B7945978B036E4B49C593C882BE379A58D08E1C25074 | A9DF77A5BFB79FA34CDB975D964A30D9FE7FC4E670BD39BF1B8C2605E843DB54 | 3/11/2021 | 3/11/2026 |
| Microsoft ECC TLS Issuing AOC CA 02 | 12FB2F53AC2D09E62128B00487E8B77D6E4A0F459DD8744D009393BD0DF697B5 | 85FA29EB740D90CE77EDDBE3AB6C66A5DE3FC8BA94D6B2955FB7D33B04231601 | 3/11/2021 | 3/11/2026 |
| Microsoft ECC TLS Issuing EOC CA 01 | 568E4046F384D0FDD9D06A8029E6BF38EED8904C1E0B44F99DA607F68672093E | EDE152DA0C19D6C3BB3168D11E40901919646BB6998CD5E7D0FBE6537FFF42EF | 3/11/2021 | 3/11/2026 |
| Microsoft ECC TLS Issuing EOC CA 02 | 2DEEA0712931179BF1EF721070A30A1AB997F64C683EAB88DCE258D040D9AD25 | 21CD47E3200B2D7F13567DF9E698EC21ACAC77A8F4A2A1173F4EAB23B2048967 | 3/11/2021 | 3/11/2026 |
| Microsoft RSA TLS Issuing AOC CA 01 | 13E295A5A6ECAF8391126E752B131B316675D187266BCF537892F839454B9480 | 7484F2F1618D35F6F239C05BAD30B8B7AD93C7024D4000D387141417EE3DDBF4 | 3/11/2021 | 3/11/2026 |
| Microsoft RSA TLS Issuing AOC CA 02 | 2AF3B34A5FD0EDC546E2E714208B6C380A5D5C553EDCA3A306A9E442C2389AAE | F19A176BC779C77609427F441B995F14CAB9A19D87CDDD92725E4997CB0878BC | 3/11/2021 | 3/11/2026 |
| Microsoft RSA TLS Issuing EOC CA 01 | E204F2682F5F630E360256ABD722DFF475432053128FC4274649F65D14EE1A36 | 1F1D8E7685CE8255088F791BFD3FB927F50AC1007091B5BBC3347EFBC5D9A80C | 3/11/2021 | 3/11/2026 |
| Microsoft RSA TLS Issuing EOC CA 02 | C97634113A97DFD13D516B9B7FA1B886635C725BDF70BC0A7891DF8E3FF0F91C | 89E1EF9BD893880FCA4C2D0BA71EC93DAF6C0AC14D5A9996F3E16F9763995076 | 3/11/2021 | 3/11/2026 |

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

**MICROSOFT PUBLIC KEY INFRASTRUTURE 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, throughout the period May 1, 2020 to April 30, 2021, 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:

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

- 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

based on the WebTrust Principles and Criteria for Certification Authorities v2.2, 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

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

- 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, 2020 through April 30, 2021.

| Bug ID | Summary | Opened | Closed | Resolution |
|---|---|---|---|---|
| **1670337** | Microsoft PKI Services: Certificate Mis-Issuance, DNSNames must have a valid TLD | 10/9/2020 | 6/7/2020 | FIXED |
| **1693930** | Microsoft PKI Services: Policy Documentation, Failure to update Subscriber Certificate Max Validity Period | 2/19/2021 | Open as of Report Date | --- |
| **1693932** | Microsoft PKI Services: Policy Documentation, Failure to update Domain Validation Method | 2/19/2021 | 4/7/2021 | 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 | Open as of Report Date | --- |
| **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 | Open as of Report Date | --- |

33F845FB21044B2
Raza Syed
DocuSigned By: Raza Syed

8/5/2021

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

Microsoft

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

| Policy Name | Policy Version | Policy Date |
|---|---|---|
| Microsoft PKI Services Certificate Policy | Version 3.1.2 | August 5, 2019 |
| Microsoft PKI Services Certificate Policy | Version 3.1.3 | July 28, 2020 |
| Microsoft PKI Services Certificate Policy | Version 3.1.4 | February 15, 2021 |
| Microsoft PKI Services Certification Practice Statement | Version 3.1.4 | April 23, 2020 |
| Microsoft PKI Services Certification Practice Statement | Version 3.1.5 | July 28, 2020 |
| Microsoft PKI Services Certification Practice Statement | Version 3.1.6 | August 25, 2020 |
| Microsoft PKI Services Certification Practice Statement | Version 3.1.7 | November 5, 2020 |
| Microsoft PKI Services Certification Practice Statement | Version 3.1.8 | February 15, 2021 |
| Microsoft PKI Services Certification Practice Statement | Version 3.1.9 | March 30, 2021 |

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

## ATTACHMENT B – IN-SCOPE CAs

| Root CAs | | | | |
|---|---|---|---|---|
| **Common Name** | **SHA2 Thumbprint** | **SPKI Hash** | **Valid From** | **Valid To** |
| Microsoft ECC Root Certificate Authority 2017 | FEA1884AB3AEA6D0DBEDBE4B9CD9FEC8655116300A86A856488FC488BB4B44D2 | 35F53CE1264611E03340FE37E1EC7D4CC986C5613DCA70FD04AA44545F2DAF28 | 7/26/2017 | 7/26/2042 |
| | 358DF39D764AF9E1B766E9C972DF352EE15CFAC227AF6AD1D70E8E4A6EDCBA02 | | 12/18/2019 | 7/18/2042 |
| Microsoft RSA Root Certificate Authority 2017 | ECDD47B5ACBFA328211E1BFF54ADEAC95E6991E3C1D50E27B527E903208040A1 | B2F7298B52BF2C3CAC4DDFE72DE4D682AC58957595982F2B62301AF597C699C5 | 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

Microsoft

| Cross-Signed CAs[1] | | | | |
|---|---|---|---|---|
| **Common Name** | **SHA2 Thumbprint** | **SPKI Hash** | **Valid From** | **Valid To** |
| Microsoft Azure ECC TLS Issuing CA 01 | 3458C7F787C30FE9AF3E58A7AB6877B1959AB7CC2C4581B070BDD38C39B84AF7 | 3993B1F49242DC9B120D28C55F6884037FC40FA80285ADCBD59ACE791368CB1F | 5/20/2020 | 6/27/2024 |
| | 949D6B4B761CA134AD3E7A8571186F580EE887F2C6B568B5140F4157F98D68DD | | 8/12/2020 | 6/27/2024 |
| Microsoft Azure ECC TLS Issuing CA 02 | FB862D0849258D7D96B6A2B0158D08142272E4D3CA825BFFC36305F5D28116C5 | 3A175427EC2BA4F46DA57E77B64CAA54B290A0DA5D0825AF7BC31041A4034360 | 5/20/2020 | 6/27/2024 |
| | 9C64A9A43E990E98FBCE8317B2D4C1C07FFE6E032DA8BB6D60A696E2FF038F1F | | 8/12/2020 | 6/27/2024 |
| Microsoft Azure ECC TLS Issuing CA 05 | 2BB470033D5777DAC2D78AF613F1E4657906BE3DF5B6E331EC79F5CD534D879B | 934F4CCE6C2244F90F9A4A60994B69ACC93FB802D255E74D2ED7CE06408CBD71 | 5/20/2020 | 6/27/2024 |
| | 003F71DC4820216575FC5AACFE3B1AEB76F72AEA5B8E8FCEFC80B9F517A4A612 | | 8/12/2020 | 6/27/2024 |
| Microsoft Azure ECC TLS Issuing CA 06 | A5E4A62B601006DC17E4ACAF497777BFD7D2F3E526FC70CA1F22094C8CB39166 | C818E7ADC99C529DA7CA50D15A742F48F46CA66866D5FFDF3AE2ABB0D89A49D0 | 5/20/2020 | 6/27/2024 |
| | 2975BAB51D00D862D0E16EEDEF8306A759C65CD4B9F00DAF50ECDFCB4EC396E4 | | 8/12/2020 | 6/27/2024 |
| Microsoft Azure TLS Issuing CA 01 | 6CA3E5D7720215F94544523E3C474B22DA69C732AE455DC82F8F5EE302EC55FC | 347C2EB1B0BBC3CE382734E6BC8448A3C34BEC3E92B484CAF69873160B498B4C | 5/20/2020 | 6/27/2024 |
| | 24C7299864E0A2A6964F551C0E8DF2461532FA8C48E4DBBB6080716691F190E5 | | 7/29/2020 | 6/27/2024 |
| Microsoft Azure TLS Issuing CA 02 | F7DBAD12E8B62B837BA7F6A01E1672999CFAF6929659B81B07F253576281F7BD | CC0C1FC76885710E6F30E09CF6FB7E3172DD2E5D3C12AB8DB0E5A00C5D213B0F | 5/20/2020 | 6/27/2024 |
| | 15A98761EBE011554DA3A46D206B0812CB2EB69AE87AAA11A6DD4CB84ED5142A | | 7/29/2020 | 6/27/2024 |
| Microsoft Azure TLS Issuing CA 05 | 4D5F5A79AEF092415FF681D9FA958F24FBFD74D26D3FFD153BC61E7C1B9C9920 | E22E21D2337D3513ABD7128923E4D0D50FD921F5233CC5ED99652C0D1DCF8E2C | 5/20/2020 | 6/27/2024 |
| | D6831BA43607F5AC19778D627531562AF55145F191CAB5EFAFA0E0005442B302 | | 7/29/2020 | 6/27/2024 |
| Microsoft Azure TLS Issuing CA 06 | 65F6C2B44154F5C6425F3C1C5B26E5C9E35717AFF6F451BD216A624F48FA06BF | 5A5F0C158FBDCE28C61BC4201070802B97E103EC9D3D9C5A2D038576210FCF75 | 5/20/2020 | 6/27/2024 |
| | 48FF8B494668C752304B48BFE818758987DEF6582E5F09B921F4B60BB3D6A8DD | | 7/29/2020 | 6/27/2024 |

[1] The Cross-Signed CA certificates in this table issued on 5/20/2020 were all revoked on 7/30/2020.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

| Intermediate CAs | | | | |
|---|---|---|---|---|
| **Common Name** | **SHA2 Thumbprint** | **SPKI Hash** | **Valid From** | **Valid To** |
| Microsoft Azure ECC TLS Issuing CA 01 | 2CAEFBB55E70DF5A8985FE9BC10DD56A40C3DEDAB3DA1530A29682015C5B7C66 | 3993B1F49242DC9B120D28C55F6884037FC40FA80285ADCBD59ACE791368CB1F | 1/17/2020 | 6/27/2024 |
| Microsoft Azure ECC TLS Issuing CA 02 | 4EC439672A443401A66E27947CC3B5897F132B667F712CC1A37018A3CC85B16A | 3A175427EC2BA4F46DA57E77B64CAA54B290A0DA5D0825AF7BC31041A4034360 | 1/17/2020 | 6/27/2024 |
| Microsoft Azure ECC TLS Issuing CA 05 | 624D5576A652B2130768BFE84B965EEFFFD91603D25CD5F7155A7DC2789DAC38 | 934F4CCE6C2244F90F9A4A60994B69ACC93FB802D255E74D2ED7CE06408CBD71 | 1/17/2020 | 6/27/2024 |
| Microsoft Azure ECC TLS Issuing CA 06 | 151A3E5969C6616EB637A8722B174CFD95387AACE78D57C3BD23F0CB3008186A | C818E7ADC99C529DA7CA50D15A742F48F46CA66866D5FFDF3AE2ABB0D89A49D0 | 1/17/2020 | 6/27/2024 |
| Microsoft Azure TLS Issuing CA 01 | 0437AB2EC2C2B4890296C135034B21DB146434B8317EE703AA8AA943C5EA51AE | 347C2EB1B0BBC3CE382734E6BC8448A3C34BEC3E92B484CAF69873160B498B4C | 1/17/2020 | 6/27/2024 |
| Microsoft Azure TLS Issuing CA 02 | 647EF2DFAFAC46D8FC9C873D7C4BABF3F1C032AE62B58D6DA7B21F92EB1CAE7D | CC0C1FC76885710E6F30E09CF6FB7E3172DD2E5D3C12AB8DB0E5A00C5D213B0F | 1/17/2020 | 6/27/2024 |
| Microsoft Azure TLS Issuing CA 05 | AB3203B3EA2017D509726A1D82293EFFCB8C42CEB52C9AF1C0EEE96B5C02BCBA | E22E21D2337D3513ABD7128923E4D0D50FD921F5233CC5ED99652C0D1DCF8E2C | 1/17/2020 | 6/27/2024 |
| Microsoft Azure TLS Issuing CA 06 | 41830FE41CA1C0BEB2CD319EF4A2D2FD1D2164086509CA4CF90670B0CD0A6A6C | 5A5F0C158FBDCE28C61BC4201070802B97E103EC9D3D9C5A2D038576210FCF75 | 1/17/2020 | 6/27/2024 |

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

| Intermediate CAs | | | | |
|---|---|---|---|---|
| **Common Name** | **SHA2 Thumbprint** | **SPKI Hash** | **Valid From** | **Valid To** |
| Microsoft ECC TLS Issuing AOC CA 01 | 9D8BB150C07B81C25799B7945978B036E4B49C593C882BE379A58D08E1C25074 | A9DF77A5BFB79FA34CDB975D964A30D9FE7FC4E670BD39BF1B8C2605E843DB54 | 3/11/2021 | 3/11/2026 |
| Microsoft ECC TLS Issuing AOC CA 02 | 12FB2F53AC2D09E62128B00487E8B77D6E4A0F459DD8744D009393BD0DF697B5 | 85FA29EB740D90CE77EDDBE3AB6C66A5DE3FC8BA94D6B2955FB7D33B04231601 | 3/11/2021 | 3/11/2026 |
| Microsoft ECC TLS Issuing EOC CA 01 | 568E4046F384D0FDD9D06A8029E6BF38EED8904C1E0B44F99DA607F68672093E | EDE152DA0C19D6C3BB3168D11E40901919646BB6998CD5E7D0FBE6537FFF42EF | 3/11/2021 | 3/11/2026 |
| Microsoft ECC TLS Issuing EOC CA 02 | 2DEEA0712931179BF1EF721070A30A1AB997F64C683EAB88DCE258D040D9AD25 | 21CD47E3200B2D7F13567DF9E698EC21ACAC77A8F4A2A1173F4EAB23B2048967 | 3/11/2021 | 3/11/2026 |
| Microsoft RSA TLS Issuing AOC CA 01 | 13E295A5A6ECAF8391126E752B131B316675D187266BCF537892F839454B9480 | 7484F2F1618D35F6F239C05BAD30B8B7AD93C7024D4000D387141417EE3DDBF4 | 3/11/2021 | 3/11/2026 |
| Microsoft RSA TLS Issuing AOC CA 02 | 2AF3B34A5FD0EDC546E2E714208B6C380A5D5C553EDCA3A306A9E442C2389AAE | F19A176BC779C77609427F441B995F14CAB9A19D87CDDD92725E4997CB0878BC | 3/11/2021 | 3/11/2026 |
| Microsoft RSA TLS Issuing EOC CA 01 | E204F2682F5F630E360256ABD722DFF475432053128FC4274649F65D14EE1A36 | 1F1D8E7685CE8255088F791BFD3FB927F50AC1007091B5BBC3347EFBC5D9A80C | 3/11/2021 | 3/11/2026 |
| Microsoft RSA TLS Issuing EOC CA 02 | C97634113A97DFD13D516B9B7FA1B886635C725BDF70BC0A7891DF8E3FF0F91C | 89E1EF9BD893880FCA4C2D0BA71EC93DAF6C0AC14D5A9996F3E16F9763995076 | 3/11/2021 | 3/11/2026 |