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, 2022 to April 30, 2023, based on the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

Microsoft PKI Services does not escrow its CA keys, does not provide subscriber key generation services, subscriber key storage and recovery services, integrated circuit card lifecycle management for subscribers, 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 v2.2.2.

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.

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 23 out of 45 code signing certificates selected for testing, the Certificate Policies extension was not present.
		For 23 out of 45 code signing certificates selected for testing, the Key Usage extension was not marked as critical.
2	Certificate Status Validation	For two (2) out of two (2) code signing certificates where OCSP status information was provided before the ValidTo date selected for testing, the status information was not available through OCSP responses after expiration.

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 23, 2023

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 3.1.6	February 22, 2023
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 1.0.1	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	3D29798CC5D3F0644A7E0DC9CB1CADE523EA5EC83B335109B605BFEAA7D5F5C1	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
CN = Microsoft RSA Document Signing CA 2023 O = Microsoft Corporation C = US	0E5A11A91688D904D2B7DAFC679545DE958B5C6BED175CF9F1F5FE0FCE2881D0	2/23/2023	2/23/2038

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 Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

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

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

- 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, 2022 to April 30, 2023 based on the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

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

Subscriber Key Lifecycle Management Controls

- Requirements for Subscriber Key Management

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

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 generation services, subscriber key storage and recovery services, integrated circuit card lifecycle management for subscribers, 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

6/23/2023

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

Certificate Policy

Policy Name	Policy Version	Policy Date
Microsoft PKI Services Certificate Policy	Version 3.1.6	February 22, 2023
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 1.0.1	February 15, 2022

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 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	3D29798CC5D3F0644A7E0DC9CB1CADE523EA5EC83B335109B605BFEAA7D5F5C1	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
CN = Microsoft RSA Document Signing CA 2023 O = Microsoft Corporation C = US	0E5A11A91688D904D2B7DAFC679545DE958B5C6BED175CF9F1F5FE0FCE2881D0	2/23/2023	2/23/2038

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

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