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 code signing ("CS") certificate lifecycle management business practices in its Microsoft PKI Services Certificate Policy ("CP") and Microsoft PKI Services Third Party Certification Practice Statement ("CPS") enumerated in Attachment A, including its commitment to provide CS certificates in conformity with the applicable Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
  - CS subscriber information was properly collected, authenticated and verified; and
  - the integrity of keys and CS certificates it manages is established and protected throughout their life cycles.

- maintained effective controls to provide reasonable assurance that its CS Timestamp Authority is operated in conformity with Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates requirements

throughout the period May 1, 2021 to April 30, 2022, based on the WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements v2.0.

Microsoft PKI Services does not provide CS Signing Services. Accordingly, our examination did not extend to the controls exercised by these external signing services.

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, based on the WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements v2.0.

Independent Accountant's Responsibilities

Our responsibility is to express an opinion about 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 matter 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.

	Matter Topic	Matter Description
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 – Code Signing 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	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

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 code signing ("CS") CA services.

The management of Microsoft PKI Services is responsible for establishing controls over its CS CA operations, including its CS CA business practices disclosure on its repository, CS key lifecycle management controls, CS certificate lifecycle management controls, and CS Timestamp Authority 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 CS CA services. Based on that assessment, in providing its CS CA services in the United States of America, and in Ireland, Microsoft PKI Services has:

- disclosed its CS certificate lifecycle management business practices in its Microsoft PKI Services Certificate Policy ("CP") and Microsoft PKI Services Third Party Certification Practice Statement ("CPS") enumerated in Attachment A including its commitment to provide CS certificates in conformity with the applicable Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
  - CS subscriber information was properly collected, authenticated and verified; and
  - the integrity of keys and CS certificates it manages is established and protected throughout their life cycles.

- maintained effective controls to provide reasonable assurance that its CS Timestamp Authority is operated in conformity with Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates requirements

throughout the period May 1, 2021 to April 30, 2022 based on the WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements v2.0.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

Microsoft PKI Services does not provide CS Signing Services. Accordingly, our assertion did not extend to the 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

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 3.1.4	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

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

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