BDO

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 Corporation Digital Security & Resiliency (“Microsoft DSR”):

Scope

We have examined Microsoft DSR’s assertion that for its Certification Authority (“CA”) operations in the United States of America and Ireland, for its CAs enumerated in Attachment B, Microsoft DSR has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of its Microsoft DSR PKI Certificate Policy/Certification Practice Statement for TLS CAs (“CP/CPS”) enumerated in Attachment A

- maintained effective controls to provide reasonable assurance that Microsoft DSR provides its services in accordance with its CP/CPS

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles; and
  - subscriber information is properly authenticated

- 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 July 1, 2021 to June 30, 2022 based on the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

Microsoft DSR does not escrow or archive its CA keys, does not provide subscriber key generation services, subscriber key storage and recovery services, integrated circuit card lifecycle management for subscribers, does not provide certificate suspension services, and does not manage any third party subordinate CAs. Accordingly, our examination did not extend to controls that would address those criteria.

Certification Authority’s Responsibilities

Microsoft DSR’s 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 DSR 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 DSR 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 unauthorized 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 DSR’s services other than its CA operations at in the United States of America and Ireland, nor the suitability of any of Microsoft DSR’s services for any customer's intended purpose.

Use of the WebTrust Seal

Microsoft DSR’s 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 29, 2022

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

Policy Name	Version	Effective Date
Microsoft DSR PKI Certificate Policy/Certification Practice Statement For TLS CAs	2.9	April 1, 2022
Microsoft DSR PKI Certificate Policy/Certification Practice Statement For TLS CAs	2.8	May 15, 2021

ATTACHMENT B – IN-SCOPE CAs

Issuing CAs			
Subject DN	**SHA256 Thumbprint**	**Valid From**	**Valid To**

CN = Microsoft RSA TLS CA 01
OU = Microsoft IT
O = Microsoft Corporation
L = Redmond
S = Washington
C = US
	04EEEA8E50B4775B3C24797262917EE50002EC4C75B56CDF3EE1C18CFCA5BA52	7/21/2020	10/8/2024

CN = Microsoft RSA TLS CA 02
OU = Microsoft IT
O = Microsoft Corporation
L = Redmond
S = Washington
C = US
	05E4005DB0C382F3BD66B47729E9011577601BF6F7B287E9A52CED710D258346	7/21/2020	10/8/2024

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

MICROSOFT CORPORATION DIGITAL SECURITY & RESILIENCY MANAGEMENT'S ASSERTION

Microsoft Corporation Digital Security & Resiliency ("Microsoft DSR") operates the Certification Authority ("CA") services for its 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

The management of Microsoft DSR 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, and 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 DSR's CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

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

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of its Microsoft DSR PKI Certificate Policy/Certificate Practice Statement For TLS CAs ("CP/CPS") enumerated in Attachment A

- maintained effective controls to provide reasonable assurance that Microsoft DSR provides its services in accordance with its CP/CPS

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;

  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles; and
  - subscriber information is properly authenticated

- 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 July 1, 2021 to June 30, 2022 based on the WebTrust Principles and Criteria for Certification Authorities v2.2.2, including the following:

CA Business Practices Disclosure

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

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & 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 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

Certificate Lifecycle Management Controls

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

Microsoft DSR does not escrow or archive its CA keys, does not provide subscriber key generation services, subscriber key storage and recovery services, integrated circuit card lifecycle management for subscribers, does not provide certificate suspension services, and does not manage any third-party subordinate CAs. Accordingly, our assertion does not extend to controls that would address those criteria.

DocuSigned by:

Biju Mathew

EA0E987FDE3C447...

Biju Mathew
Principal Service Engineering Manager
8/29/2022

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

Policy Name	Version	Effective Date
Microsoft DSR PKI Certificate Policy/Certification Practice Statement For TLS CAs	2.9	April 1, 2022
Microsoft DSR PKI Certificate Policy/Certification Practice Statement For TLS CAs	2.8	May 15, 2021

ATTACHMENT B – IN-SCOPE CAs

Issuing CAs			
Subject DN	**SHA256 Thumbprint**	**Valid From**	**Valid To**

CN = Microsoft RSA TLS CA 01
OU = Microsoft IT
O = Microsoft Corporation
L = Redmond
S = Washington
C = US
	04EEEA8E50B4775B3C24797262917EE50002EC4C75B56CDF3EE1C18CFCA5BA52	7/21/2020	10/8/2024

CN = Microsoft RSA TLS CA 02
OU = Microsoft IT
O = Microsoft Corporation
L = Redmond
S = Washington
C = US
	05E4005DB0C382F3BD66B47729E9011577601BF6F7B287E9A52CED710D258346	7/21/2020	10/8/2024