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 & Resilience ("Microsoft DSR"):

Scope

We have examined Microsoft DSR's assertion that for its Certification Authority ("CA") operations in the United States of America, Puerto Rico, and Ireland, for CAs as enumerated in Attachment B, Microsoft DSR has:

- disclosed its SSL certificate lifecycle management business practices in the applicable versions of its Microsoft DSR PKI Certificate Policy/Certification Practice Statement For TLS CAs enumerated in Attachment A, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Microsoft DSR repository, and provided services in accordance with its disclosed practices

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

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

throughout the period July 1, 2020 to June 30, 2021 based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1.

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 – SSL Baseline with Network Security v2.4.1.

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.

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 state of Washington in United States of America, Puerto Rico, and Ireland, nor the suitability of any of Microsoft DSR's 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
1	Certificate Issuance	Microsoft DSR disclosed in Mozilla Bug 1649951 its issuing CAs were inappropriately assigned delegated OCSP responder authority when the certificate was created by DigiCert, Inc. Microsoft DSR and DigiCert, Inc. replaced the issuing CAs and destroyed the related keys.

Matter Topic		Matter
2	Certificate Revocation	Microsoft DSR disclosed in Mozilla Bug 1651461 it was unable to revoke the Microsoft DSR issuing CAs impacted by the OCSP EKU issue within 7 days, because to the number of subscribers relying on the CAs and the timetable to replace the certificates.
3	Certificate Content	Microsoft DSR disclosed in Mozilla Bug 1674561 it identified three (3) issued DV certificates which included OV fields. All three (3) certificates were revoked within the required five (5) day timeline.
4	Audit Logging	Microsoft DSR disclosed in Mozilla Bug 1658995 it identified a gap in the retention of firewall logs for a period of less than two hours. The issue was identified during a manual log review. This is a violation of 7-year retention requirements outlined in the Baseline Requirements.

Use of the WebTrust Seal

Microsoft DSR's use of the WebTrust for Certification Authorities – SSL Baseline with Network Security 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

July 30, 2021

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	2.8	May 15, 2021
DSRE PKI Certificate Policy/Certification Practice Statement for TLS CAs	2.7	March 31, 2021
DSRE PKI Certificate Policy/Certification Practice Statement for TLS CAs	2.6	October 28, 2020
DSRE PKI Certificate Policy/Certification Practice Statement for TLS CAs	2.5	July 23, 2020
DSRE PKI Certificate Policy/Certification Practice Statement for TLS CAs	2.4	April 1, 2020

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

Revoked Issuing CAs			
Subject DN	**SHA256 Thumbprint**	**Valid From**	**Revocation Date**
CN = Microsoft IT TLS CA 1 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	4FF404F02E2CD00188F15D1C00F4B6D1E38B5A395CF85314EAEBA855B6A64B75	5/20/2016	2/16/2021
CN = Microsoft IT TLS CA 2 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	4E107C981B42ACBE41C01067E16D44DB64814D4193E572317EA04B87C79C475F	5/20/2016	2/16/2021

Revoked Issuing CAs			
Subject DN	**SHA256 Thumbprint**	**Valid From**	**Revocation Date**
CN = Microsoft IT TLS CA 4 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	5FFAC43E0DDC5B4AF2B696F6BC4DB7E91DF314BB8FE0D0713A0B1A7AD2A68FAC	5/20/2016	2/16/2021
CN = Microsoft IT TLS CA 5 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	F0EE5914ED94C7252D058B4E39808AEE6FA8F62CF0974FB7D6D2A9DF16E3A87F	5/20/2016	2/16/2021

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 in scope for SSL Baseline and Network Security Requirements and provides SSL CA services.

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

- disclosed its SSL certificate lifecycle management business practices in the applicable versions of its Microsoft DSR PKI Certificate Policy/Certificate Practice Statement For TLS CAs enumerated in Attachment A, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Microsoft DSR repository, and provided such services in accordance with its disclosed practices

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

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

throughout the period July 1, 2020 to June 30, 2021, based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1.

Microsoft DSR has disclosed the following matters publicly on Mozilla's Bugzilla platform:

Bug ID	Summary	Opened	Closed	Resolution
1649951	DigiCert: Incorrect OCSP Delegated Responder Certificate	July 1, 2020	March 11, 2021	FIXED

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

Bug ID	Summary	Opened	Closed	Resolution
1651461	DigiCert: Failure to revoke within 7 days: OCSP EKU issue	July 8, 2020	March 11, 2021	FIXED
1652827	Microsoft: Incomplete Logical Access Review Audit Evidence	July 14, 2020	September 21, 2020	FIXED
1658995	Microsoft: Firewall log data retention	August 13, 2020	October 5, 2020	FIXED
1674561	Microsoft DSRE PKI: DV certificate issued with OV fields	October 31, 2020	May 20, 2021	FIXED

DocuSigned by:
Biju Mathew
EA0E987FDE3C447...

7/30/2021

Biju Mathew
Principal Service Engineering Manager

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

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	2.8	May 15, 2021
DSRE PKI Certificate Policy/Certification Practice Statement for TLS CAs	2.7	March 31, 2021
DSRE PKI Certificate Policy/Certification Practice Statement for TLS CAs	2.6	October 28, 2020
DSRE PKI Certificate Policy/Certification Practice Statement for TLS CAs	2.5	July 23, 2020
DSRE PKI Certificate Policy/Certification Practice Statement for TLS CAs	2.4	April 1, 2020

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

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

Revoked Issuing CAs			
Subject DN	**SHA256 Thumbprint**	**Valid From**	**Revocation Date**
CN = Microsoft IT TLS CA 1 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	4FF404F02E2CD00188F15D1C00F4B6D1E38B5A395CF85314EAEBA855B6A64B75	5/20/2016	2/16/2021

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

Revoked Issuing CAs			
Subject DN	**SHA256 Thumbprint**	**Valid From**	**Revocation Date**
CN = Microsoft IT TLS CA 2 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	4E107C981B42ACBE41C01067E16D44DB64814D4193E572317EA04B87C79C475F	5/20/2016	2/16/2021
CN = Microsoft IT TLS CA 4 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	5FFAC43E0DDC5B4AF2B696F6BC4DB7E91DF314BB8FE0D0713A0B1A7AD2A68FAC	5/20/2016	2/16/2021
CN = Microsoft IT TLS CA 5 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	F0EE5914ED94C7252D058B4E39808AEE6FA8F62CF0974FB7D6D2A9DF16E3A87F	5/20/2016	2/16/2021