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 Core Services Engineering & Operations ("Microsoft CSEO"):

We have examined for Microsoft CSEO's Certification Authority ("CA") operations in the United States of America and territories, throughout the period July 1, 2018 to January 31 2019,

- Microsoft CSEO's disclosure of its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices, the provision of services in accordance with its Certificate Policy/Certification Practice Statement, and

- the effectiveness of Microsoft CSEO's controls over key and certificate integrity, the authenticity and confidentiality of subscriber and relying party information, the continuity of key and certificate lifecycle management operations, and development, maintenance, and operation of CA systems integrity throughout the period July 1, 2018 to January 31, 2019 for the CAs enumerated in Attachment A.

Microsoft CSEO's management is responsible for these disclosures and for maintaining effective controls, based on WebTrust Principles and Criteria for Certification Authorities v2.1. Our responsibility is to express an opinion, based on our examination.

The relative effectiveness and significance of specific controls at Microsoft CSEO 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.

Microsoft CSEO does not escrow its CA keys, does not provide subscriber key lifecycle management services, 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.

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, throughout the period July 1, 2018 to January 31, 2019 for its CAs in Attachment A, in all material respects, Microsoft CSEO:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its DSRE PKI Certificate Policy/Certification Practice Statement for TLS CAs, Version 2.0, Effective May 1, 2018

- maintained effective controls to provide reasonable assurance that:
    - Microsoft CSEO provides its services in accordance with its Certificate Policy/Certification Practice Statement;

- the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
- subscriber information is properly authenticated;
- 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 v2.1.

During our examination we noted the following, which caused a modification of our opinion:

Impacted WebTrust Trust Principles and Criteria for Certification Authorities		Control Deficiency Noted
3.4	Physical and Environmental Security The CA maintains controls to provide reasonable assurance that: • physical access to CA facilities and equipment is limited to authorized individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control; • CA facilities and equipment are protected from environmental hazards; • loss, damage or compromise of assets and interruption to business activities are prevented; and • compromise of information and information processing facilities is prevented.	Microsoft CSEO requires at least two individuals in trusted roles to be present when accessing the CA equipment. During the period two events were identified where procedures were not followed and a single individual accessed the CA equipment.

Because of the nature and inherent limitations of controls, Microsoft CSEO's 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.

In our opinion, except for the matter noted in the preceding table, throughout the period July 1, 2018 to January 31, 2019, Microsoft CSEO has, in all material respects:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its DSRE PKI Certificate Policy/Certification Practice Statement for TLS CAs, Version 2.0, Effective May 1, 2018

- maintained effective controls to provide reasonable assurance that:
  - Microsoft CSEO provides its services in accordance with its Certificate Policy/Certification Practice Statement;
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated;
  - 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 v2.1.

This report does not include any representation as to the quality of Microsoft CSEO's services other than its CA operations at in the United States of America and territories, nor the suitability of any of Microsoft CSEO's services for any customer's intended purpose.

BDO USA, LLP

St. Louis, Missouri
April 9, 2019

ATTACHMENT A – IN-SCOPE CAs

Issuing CAs	Serial Number	SHA1 Thumbprint	SHA2 Thumbprint
CN = Microsoft IT TLS CA 1 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	08 b8 7a 50 1b be 9c da 2d 16 4d 3e 39 51 bf 55	41 7e 22 50 37 fb fa a4 f9 57 61 d5 ae 72 9e 1a ea 7e 3a 42	4f f4 04 f0 2e 2c d0 01 88 f1 5d 1c 00 f4 b6 d1 e3 8b 5a 39 5c f8 53 14 ea eb a8 55 b6 a6 4b 75
CN = Microsoft IT TLS CA 2 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	0f 2c 10 c9 5b 06 c0 93 7f b8 d4 49 f8 3e 85 69	54 d9 d2 02 39 08 0c 32 31 6e d9 ff 98 0a 48 98 8f 4a df 2d	4e 10 7c 98 1b 42 ac be 41 c0 10 67 e1 6d 44 db 64 81 4d 41 93 e5 72 31 7e a0 4b 87 c7 9c 47 5f
CN = Microsoft IT TLS CA 4 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	0b 6a b3 b0 3e b1 a9 f6 c4 60 92 6a a8 cd fe b3	8a 38 75 5d 09 96 82 3f e8 fa 31 16 a2 77 ce 44 6e ac 4e 99	5f fa c4 3e 0d dc 5b 4a f2 b6 96 f6 bc 4d b7 e9 1d f3 14 bb 8f e0 d0 71 3a 0b 1a 7a d2 a6 8f ac
CN = Microsoft IT TLS CA 5 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	08 88 cd 52 5f 19 24 44 4d 14 a5 82 91 de b9 52	ad 89 8a c7 3d f3 33 eb 60 ac 1f 5f c6 c4 b2 21 9d db 79 b7	f0 ee 59 14 ed 94 c7 25 2d 05 8b 4e 39 80 8a ee 6f a8 f6 2c f0 97 4f b7 d6 d2 a9 df 16 e3 a8 7f

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

Microsoft Corporation Core Services Engineering & Operations Management's Assertion

Microsoft Corporation Core Services Engineering & Operations ("Microsoft CSEO") operates the Certification Authority ("CA") services for its CAs enumerated in Attachment A, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation

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

Microsoft CSEO's management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, we noted the following control deficiency which caused the relevant criteria to not be met:

Impacted WebTrust Trust Principles and Criteria for Certification Authorities		Control Deficiency Noted
3.4	Physical and Environmental Security The CA maintains controls to provide reasonable assurance that: • physical access to CA facilities and equipment is limited to authorized individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control; • CA facilities and equipment are protected from environmental hazards; • loss, damage or compromise of assets and interruption to business activities are prevented; and • compromise of information and information processing facilities is	Microsoft CSEO requires at least two individuals in trusted roles to be present when accessing the CA equipment. During the period two events were identified where procedures were not followed and a single individual accessed the CA equipment. **Management Response** Microsoft acknowledges the fact that authorized personnel opened the secure rack to record asset tag numbers without two designated trusted role holders present. Our video evidence shows there was no physical contact with any assets secured in that rack.

	prevented.	There has been no compromise in the integrity or security of the systems that provide TLS certificates. Technical controls have been modified to ensure no further events of this type will occur.

Based on that assessment, in Microsoft CSEO management's opinion, except for the matter described in the preceding table, in providing its CA services in the United States of America and territories, throughout the period July 1, 2018 to January 31, 2019, Microsoft CSEO has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its DSRE PKI Certificate Policy/Certification Practice Statement for TLS CAs, Version 2.0, Effective May 1, 2018

- maintained effective controls to provide reasonable assurance that:
  - Microsoft CSEO provides its services in accordance with its Certificate Policy/Certification Practice Statement;
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated;
  - 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 v2.1, 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 and Maintenance

- 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
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Microsoft CSEO does not escrow its CA keys, does not provide subscriber key lifecycle management services, 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.

Biju Mathew
Principal Service Engineer Management IAM
April 9, 2019

ATTACHMENT A - IN-SCOPE CAs

CA	Serial Number	SHA1 Thumbprint	SHA2 Thumbprint
CN = Microsoft IT TLS CA 1 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	08 b8 7a 50 1b be 9c da 2d 16 4d 3e 39 51 bf 55	41 7e 22 50 37 fb fa a4 f9 57 61 d5 ae 72 9e 1a ea 7e 3a 42	4f f4 04 f0 2e 2c d0 01 88 f1 5d 1c 00 f4 b6 d1 e3 8b 5a 39 5c f8 53 14 ea eb a8 55 b6 a6 4b 75
CN = Microsoft IT TLS CA 2 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	0f 2c 10 c9 5b 06 c0 93 7f b8 d4 49 f8 3e 85 69	54 d9 d2 02 39 08 0c 32 31 6e d9 ff 98 0a 48 98 8f 4a df 2d	4e 10 7c 98 1b 42 ac be 41 c0 10 67 e1 6d 44 db 64 81 4d 41 93 e5 72 31 7e a0 4b 87 c7 9c 47 5f
CN = Microsoft IT TLS CA 4 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	0b 6a b3 b0 3e b1 a9 f6 c4 60 92 6a a8 cd fe b3	8a 38 75 5d 09 96 82 3f e8 fa 31 16 a2 77 ce 44 6e ac 4e 99	5f fa c4 3e 0d dc 5b 4a f2 b6 96 f6 bc 4d b7 e9 1d f3 14 bb 8f e0 d0 71 3a 0b 1a 7a d2 a6 8f ac
CN = Microsoft IT TLS CA 5 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	08 88 cd 52 5f 19 24 44 4d 14 a5 82 91 de b9 52	ad 89 8a c7 3d f3 33 eb 60 ac 1f 5f c6 c4 b2 21 9d db 79 b7	f0 ee 59 14 ed 94 c7 25 2d 05 8b 4e 39 80 8a ee 6f a8 f6 2c f0 97 4f b7 d6 d2 a9 df 16 e3 a8 7f