Tel: 314-889-1100
Fax: 314-889-1101
www.bdo.com

101 S Hanley Rd, Suite 800
St. Louis, MO 63105

REPORT OF INDEPENDENT ACCOUNTANT

To the Management of Microsoft Public Key Infrastructure ("PKI") Services:

We have examined Microsoft PKI Services management's assertion that for its Certification Authority ("CA") operations in the United States of America and the European Union, as of October 31, 2018 for CAs as enumerated in Appendix A, Microsoft PKI Services has:

- disclosed is SSL certificate lifecycle management business practices in its:
  - Microsoft PKI Services Certificate Practice Statement, Version 3.1.2, effective October 12, 2018; and
  - Microsoft PKI Services Certificate Policy, Version 3.1.1, effective July 10, 2018,

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on the Microsoft PKI Services website, and provided such services in accordance with its disclosed practices

- suitably designed, and placed into operation, 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

- suitably designed, and placed into operation, 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

- suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3. Microsoft PKI Services' management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

The suitability of the design of the 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. We have performed no procedures to evaluate the suitability of the design of the controls at individual subscriber and relying party locations.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

BDO is the brand name for the BDO network and for each of the BDO Member Firms.

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 did not perform any procedures regarding the operating effectiveness of the aforementioned controls for any period and, accordingly, do not express an opinion thereon.

Because of the nature and inherent limitations of controls, Microsoft PKI Services' 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, 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 the European Union, nor the suitability of any of Microsoft PKI Services' services for any customer's intended purpose.

BDO USA, LLP

Certified Public Accountants
St. Louis, Missouri
November 21, 2018

APPENDIX A – IN-SCOPE CAs

Root CAs	Root CA Serial Numbers	Issue Date	Expiration Date	SHA2 Thumbprint
Microsoft EV RSA Root Certificate Authority 2017	19fceb6df7cf57844184bdd9e0228e98	7/26/2017	7/26/2042	dfb3c314740596ad5fb97960ef62ad7c1fcceead16e74054652d1032e6f140ef
Microsoft EV ECC Root Certificate Authority 2017	3fdccc3b5bdcd29844cadf59d1d2eb1c	7/26/2017	7/26/2042	6aea30bc02ca85afcfec2f65f60881893c926925fd0704bd8ada3f0f6eddb699
Microsoft RSA Root Certificate Authority 2017	29c87039f4dbfdb94dbcda6ca792836b	7/26/2017	7/26/2042	ecdd47b5acbfa328211e1bff54adeac95e6991e3c1d50e27b527e903208040a1
Microsoft ECC Root Certificate Authority 2017	71767e8d58e4fc9649c63efbcf3abda7	7/26/2017	7/26/2042	fea1884ab3aea6d0dbedbe4b9cd9fec8655116300a86a856488fc488bb4b44d2

Issuing and Intermediate CAs	Issuing and Intermediate CAs Serial Numbers	Issue Date	Expiration Date	SHA2 Thumbprint
Microsoft EV Server PCA 2018	3300000053A9F0C06FAE17F7B000000000005	2/28/2018	2/28/2033	2164a69e46106175459f1ccc8257157b042c13eea588a7f1b9afd079ffbf28bb
Microsoft Server PCA 2018	330000000288E358F4E2074B99000000000002	2/28/2018	2/28/2033	334af3b6768a869399de242079038d21d1fda5b9865708d7427f7f675d588b43
Microsoft EV ECC Server PCA 2018	3300000002FD7D5D3DDBB51710000000000002	2/28/2018	2/28/2033	d21facbab9fad08eeac926fbc6d5062b07f6a76f6b2c4c47f589418a94149c59
Microsoft ECC Server PCA 2018	3300000002368AD5489921BF9B000000000002	2/28/2018	2/28/2033	25d41e8a8543371b9cada5e7d15221d9289cf3f034f5808a8ff9d1d892e8d4de
Microsoft TLS EV Issuing CA 01	3300000006FE1EFED7BC72467E000000000006	5/31/2018	5/31/2023	4e8cf75cec298a40011ec6f345a1b0801daa7f13d4f6df1f1c8807dc92d0d437
Microsoft TLS EV Issuing CA 05	3300000007953BF3A95F910755000000000007	5/31/2018	5/31/2023	190ee6be09b3c97c1167dfd7bb366fe40c066f188a6defb1e0655a3f700341b1
Microsoft TLS ECC EV Issuing CA 01	3300000003B5E464B87F90C883000000000003	5/31/2018	5/31/2023	dbed47a27d2df69af759ead788d33bdd7bee79a33d3b762a7806ffcfb3a3acb4
Microsoft TLS ECC EV Issuing CA 05	3300000004F61DD46A694AFE860000000000004	5/31/2018	5/31/2023	664e415a2473015216baeb56708271bce20277e93b398c5332ddd8b94c808327
Microsoft TLS Issuing CA 01	330000000309A4FEB7D2C2ABCA000000000003	5/31/2018	5/31/2023	f6be0e24c9bb74db7674261e7404d7a39d0c1862708b8a0a49d184d8b0c9b914
Microsoft TLS Issuing CA 05	33000000043F51ECC602131C4C000000000004	5/31/2018	5/31/2023	4bc9fe53ce532690216e157c76c77155793c9be895d9f6718ea3d3d1fd694aba

Microsoft TLS ECC Issuing CA 01	3300000003239617A331584C3B0000 00000003	5/31/2018	5/31/2023	a383b4a775ab1df5e3e88507001ccc35 352f44bc82e46694453fbf50406b4f6c
Microsoft TLS ECC Issuing CA 05	33000000048C754D11C3A194120000 00000004	5/31/2018	5/31/2023	ca61a36f29960ace59951f7ccef46e136 8faae5eb3d6c06284cae56e0918d7f7

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

MICROSOFT PKI SERVICES MANAGEMENT'S ASSERTION

Microsoft Public Key Infrastructure ("PKI") Services operates the Certification Authority ("CA") services for the root, issuing, and intermediate CAs enumerated in Appendix A, and provides SSL CA services:

Microsoft PKI Services 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 and the European Union, as of October 31, 2018, Microsoft PKI Services has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - Microsoft PKI Services Certificate Practice Statement, Version 3.1.2, effective October 12, 2018; and
  - Microsoft PKI Services Certificate Policy, Version 3.1.1, effective July 10, 2018

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on the Microsoft PKI Services repository, and provided such services in accordance with its disclosed practices

- suitably designed, and placed into operation, 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

- suitably designed, and placed into operation, 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

- suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.3.

Chuck Chan
Corporate Vice President, Microsoft Corporation

Raza Syed
Partner Software Engineering Manager, Microsoft Corporation

Microsoft Corporation is an equal opportunity employer.

Tony Throop
Principal Service Engineering Manager, Microsoft Corporation

November 21, 2018

Microsoft

APPENDIX A - IN-SCOPE CAs

Root CAs	Root CA Serial Numbers	Issue Date	Expiration Date	SHA2 Thumbprint
Microsoft EV RSA Root Certificate Authority 2017	19fceb6df7cf57844184bdd9e0228e98	7/26/2017	7/26/2042	dfb3c314740596ad5fb97960ef62ad7c1fcceead16e74054652d1032e6f140ef
Microsoft EV ECC Root Certificate Authority 2017	3fdccc3b5bdcd29844cadf59d1d2eb1c	7/26/2017	7/26/2042	6aea30bc02ca85afcfec2f65f60881893c926925fd0704bd8ada3f0f6eddb699
Microsoft RSA Root Certificate Authority 2017	29c87039f4dbfdb94dbcda6ca792836b	7/26/2017	7/26/2042	ecdd47b5acbfa328211e1bff54adeac95e6991e3c1d50e27b527e903208040a1
Microsoft ECC Root Certificate Authority 2017	71767e8d58e4fc9649c63efbcf3abda7	7/26/2017	7/26/2042	fea1884ab3aea6d0dbedbe4b9cd9fec8655116300a86a856488fc488bb4b44d2

Issuing and Intermediate CAs	Issuing and Intermediate CAs Serial Numbers	Issue Date	Expiration Date	SHA2 Thumbprint
Microsoft EV Server PCA 2018	33000000053A9F0C06FAE17F7B000000000005	2/28/2018	2/28/2033	2164a69e46106175459f1ccc8257157b042c13eea588a7f1b9afd079ffbf28bb
Microsoft Server PCA 2018	330000000288E358F4E2074B99000000000002	2/28/2018	2/28/2033	334af3b6768a869399de242079038d21d1fda5b9865708d7427f7f675d588b43
Microsoft EV ECC Server PCA 2018	3300000002FD7D5D3DDBB51710000000000002	2/28/2018	2/28/2033	d21facbab9fad08eeac926fbc6d5062b07f6a76f6b2c4c47f589418a94149c59
Microsoft ECC Server PCA 2018	3300000002368AD5489921BF9B000000000002	2/28/2018	2/28/2033	25d41e8a8543371b9cada5e7d15221d9289cf3f034f5808a8ff9d1d892e8d4de
Microsoft TLS EV Issuing CA 01	3300000006FE1EFED7BC72467E000000000006	5/31/2018	5/31/2023	4e8cf75cec298a40011ec6f345a1b0801daa7f13d4f6df1f1c8807dc92d0d437
Microsoft TLS EV Issuing CA 05	33000000079953BF3A95F910755000000000007	5/31/2018	5/31/2023	190ee6be09b3c97c1167dfd7bb366fe40c066f188a6defb1e0655a3f700341b1
Microsoft TLS ECC EV Issuing CA 01	3300000003B5E464B87F90C883000000000003	5/31/2018	5/31/2023	dbed47a27d2df69af759ead788d33bdd7bee79a33d3b762a7806ffcfb3a3acb4
Microsoft TLS ECC EV Issuing CA 05	3300000004F61DD46A694AFE860000000000004	5/31/2018	5/31/2023	664e415a2473015216baeb56708271bce20277e93b398c5332ddd8b94c808327
Microsoft TLS Issuing CA 01	330000000309A4FEB7D2C2ABCA000000000003	5/31/2018	5/31/2023	f6be0e24c9bb74db7674261e7404d7a39d0c1862708b8a0a49d184d8b0c9b914
Microsoft TLS Issuing CA 05	33000000043F51ECC602131C4C0000000000004	5/31/2018	5/31/2023	4bc9fe53ce532690216e157c76c77155793c9be895d9f6718ea3d3d1fd694aba
Microsoft TLS ECC Issuing CA 01	3300000003239617A331584C3B000000000003	5/31/2018	5/31/2023	a383b4a775ab1df5e3e88507001ccc35352f44bc82e46694453fbf50406b4f6c
Microsoft TLS ECC Issuing CA 05	33000000048C754D11C3A19412000000000004	5/31/2018	5/31/2023	ca61a36f29960ace59951f7ccef46e1368faae5eb3d6c06284cae56e0918d7f7