



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 Public Key Infrastructure (“PKI”) Services (formerly known as “PRSS PKI”):

We have examined Microsoft PKI Services’ management [assertion](#) that for its Certification Authority (“CA”) operations in the United States of America and the European Union, throughout the period January 1, 2019 to April 30, 2019 for the CAs enumerated in [Appendix A](#) in scope for SSL Baseline Requirements and Network Security Requirements, Microsoft PKI Services has:

- disclosed its SSL certificate lifecycle management business practices in the applicable versions of its Microsoft PKI Services Certificate Policy and Certification Practice Statement enumerated in [Appendix B](#), including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements in its [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

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 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.



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.

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 the services of Microsoft PKI Services other than its CAs enumerated in [Appendix A](#), nor the suitability of the services of any of Microsoft PKI Services for any customer's intended purpose.

Microsoft PKI Services' 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

Certified Public Accountants
July 25, 2019



APPENDIX A - IN-SCOPE CAs FOR SSL BASELINE REQUIREMENTS AND NETWORK SECURITY REQUIREMENTS

Root CAs	Serial Number	Issue Date	Expiration Date	SHA256 Thumbprint
CN = Microsoft EV RSA Root Certificate Authority 2017 O = Microsoft Corporation L = Redmond S = Washington C = US	19 fc eb 6d f7 cf 57 84 41 84 bd d9 e0 22 8e 98	7/26/2017	7/26/2042	dfb3c314740596ad5fb9 7960ef62ad7c1fcceead 16e74054652d1032e6f1 40ef
CN = Microsoft EV ECC Root Certificate Authority 2017 O = Microsoft Corporation L = Redmond S = Washington C = US	3f dc cc 3b 5b dc d2 98 44 ca df 59 d1 d2 eb 1c	7/26/2017	7/26/2042	6aea30bc02ca85afcfec 2f65f60881893c926925f d0704bd8ada3f0f6eddb 699
CN = Microsoft RSA Root Certificate Authority 2017 O = Microsoft Corporation L = Redmond S = Washington C = US	29 c8 70 39 f4 db fd b9 4d bc da 6c a7 92 83 6b	7/26/2017	7/26/2042	ecdd47b5acbfa328211e 1bff54adeac95e6991e3 c1d50e27b527e903208 040a1
CN = Microsoft ECC Root Certificate Authority 2017 O = Microsoft Corporation L = Redmond S = Washington C = US	71 76 7e 8d 58 e4 fc 96 49 c6 3e fb cf 3a bd a7	7/26/2017	7/26/2042	fea1884ab3aea6d0dbe dbe4b9cd9fec86551163 00a86a856488fc488bb4 b44d2



Issuing and Intermediate CAs	Serial Number	Issue Date	Expiration Date	SHA256 Thumbprint
CN = Microsoft EV Server PCA 2018 O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 05 3a 9f 0c 06 fa e1 7f 7b 00 00 00 00 00 05	2/28/2018	2/28/2033	2164a69e46106175 459f1ccc8257157b0 42c13eea588a7f1b 9afd079ffbf28bb
CN = Microsoft Server PCA 2018 O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 02 88 e3 58 f4 e2 07 4b 99 00 00 00 00 00 02	2/28/2018	2/28/2033	334af3b6768a8693 99de242079038d21 d1fda5b9865708d7 427f7f675d588b43
CN = Microsoft EV ECC Server PCA 2018 O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 02 fd 7d 5d 3d db b5 17 10 00 00 00 00 00 02	2/28/2018	2/28/2033	d21facbab9fad08ee ac926fbc6d5062b0 7f6a76f6b2c4c47f5 89418a94149c59
CN = Microsoft ECC Server PCA 2018 O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 02 36 8a d5 48 99 21 bf 9b 00 00 00 00 00 02	2/28/2018	2/28/2033	25d41e8a8543371b 9cada5e7d15221d9 289cf3f034f5808a8 ff9d1d892e8d4de
CN = Microsoft TLS EV Issuing CA 01 O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 06 fe 1e fe d7 bc 72 46 7e 00 00 00 00 00 06	5/31/2018	5/31/2023	4e8cf75cec298a400 11ec6f345a1b0801 daa7f13d4f6df1f1c 8807dc92d0d437
CN = Microsoft TLS EV Issuing CA 05 OU = EOC O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 07 95 3b f3 a9 5f 91 07 55 00 00 00 00 00 07	5/31/2018	5/31/2023	190ee6be09b3c97c 1167dfd7bb366fe40 c066f188a6defb1e0 655a3f700341b1
CN = Microsoft TLS ECC EV Issuing CA 01 O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 03 b5 e4 64 b8 7f 90 c8 83 00 00 00 00 00 03	5/31/2018	5/31/2023	dbed47a27d2df69a f759ead788d33bdd 7bee79a33d3b762a 7806ffcfb3a3acb4



Issuing and Intermediate CAs	Serial Number	Issue Date	Expiration Date	SHA256 Thumbprint
CN = Microsoft TLS ECC EV Issuing CA 05 OU = EOC O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 04 f6 1d d4 6a 69 4a fe 86 00 00 00 00 00 04	5/31/2018	5/31/2023	664e415a24730152 16baeb56708271bc e20277e93b398c53 32ddd8b94c808327
CN = Microsoft TLS Issuing CA 01 O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 03 09 a4 fe b7 d2 c2 ab ca 00 00 00 00 00 03	5/31/2018	5/31/2023	f6be0e24c9bb74db 7674261e7404d7a3 9d0c1862708b8a0a 49d184d8b0c9b914
CN = Microsoft TLS Issuing CA 05 OU = EOC O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 04 3f 51 ec c6 02 13 1c 4c 00 00 00 00 00 04	5/31/2018	5/31/2023	4bc9fe53ce532690 216e157c76c77155 793c9be895d9f671 8ea3d3d1fd694aba
CN = Microsoft TLS ECC Issuing CA 01 O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 03 23 96 17 a3 31 58 4c 3b 00 00 00 00 00 03	5/31/2018	5/31/2023	a383b4a775ab1df5 e3e88507001ccc35 352f44bc82e46694 453fbf50406b4f6c
CN = Microsoft TLS ECC Issuing CA 05 OU = EOC O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 04 8c 75 4d 11 c3 a1 94 12 00 00 00 00 00 04	5/31/2018	5/31/2023	ca61a36f29960ace5 9951f7ccef46e1368 faae5eb3d6c06284 cae56e0918d7f7



**APPENDIX B - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY
VERSIONS IN-SCOPE**

Policy Name	Policy Version	Policy Date
Microsoft PKI Services Certificate Policy	Version 3.1.1	July 10, 2018
Microsoft PKI Services Certification Practice Statement	Version 3.1.2	October 12, 2018




MICROSOFT PUBLIC KEY INFRASTRUCTURE SERVICES' MANAGEMENT ASSERTION

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

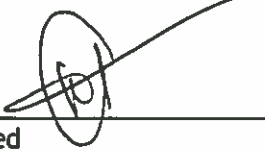
Microsoft PKI Services management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in providing its SSL CA services in the United States of America and the European Union, throughout the period January 1, 2019 to April 30, 2019, Microsoft PKI Services has:

- disclosed its SSL certificate lifecycle management business practices in applicable versions of its Microsoft PKI Services Certificate Policy and Certification Practice Statement enumerated in [Appendix B](#), 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
- 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

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 Director of Software Engineering, Microsoft Corporation

July 25, 2019

APPENDIX A - IN-SCOPE CAs

Root CAs	Serial Number	Issue Date	Expiration Date	SHA256 Thumbprint
CN = Microsoft EV RSA Root Certificate Authority 2017 O = Microsoft Corporation L = Redmond S = Washington C = US	19 fc eb 6d f7 cf 57 84 41 84 bd d9 e0 22 8e 98	7/26/2017	7/26/2042	dfb3c314740596ad5fb9 7960ef62ad7c1fccead 16e74054652d1032e6f1 40ef
CN = Microsoft EV ECC Root Certificate Authority 2017 O = Microsoft Corporation L = Redmond S = Washington C = US	3f dc cc 3b 5b dc d2 98 44 ca df 59 d1 d2 eb 1c	7/26/2017	7/26/2042	6aea30bc02ca85afcfec 2f65f60881893c926925f d0704bd8ada3f0f6eddb 699
CN = Microsoft RSA Root Certificate Authority 2017 O = Microsoft Corporation L = Redmond S = Washington C = US	29 c8 70 39 f4 db fd b9 4d bc da 6c a7 92 83 6b	7/26/2017	7/26/2042	ecdd47b5acbfa328211e 1bff54adeac95e6991e3 c1d50e27b527e903208 040a1
CN = Microsoft ECC Root Certificate Authority 2017 O = Microsoft Corporation L = Redmond S = Washington C = US	71 76 7e 8d 58 e4 fc 96 49 c6 3e fb cf 3a bd a7	7/26/2017	7/26/2042	fea1884ab3aea6d0dbe dbe4b9cd9fec86551163 00a86a856488fc488bb4 b44d2

Issuing and Intermediate CAs	Serial Number	Issue Date	Expiration Date	SHA256 Thumbprint
CN = Microsoft EV Server PCA 2018 O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 05 3a 9f 0c 06 fa e1 7f 7b 00 00 00 00 00 05	2/28/2018	2/28/2033	2164a69e46106175 459f1ccc8257157b0 42c13eea588a7f1b 9afd079ffbf28bb
CN = Microsoft Server PCA 2018 O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 02 88 e3 58 f4 e2 07 4b 99 00 00 00 00 00 02	2/28/2018	2/28/2033	334af3b6768a8693 99de242079038d21 d1fda5b9865708d7 427f7f675d588b43
CN = Microsoft EV ECC Server PCA 2018 O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 02 fd 7d 5d 3d db b5 17 10 00 00 00 00 00 02	2/28/2018	2/28/2033	d21facbab9fad08ee ac926fbc6d5062b0 7f6a76f6b2c4c47f5 89418a94149c59
CN = Microsoft ECC Server PCA 2018 O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 02 36 8a d5 48 99 21 bf 9b 00 00 00 00 00 02	2/28/2018	2/28/2033	25d41e8a8543371b 9cada5e7d15221d9 289cf3f034f5808a8 ff9d1d892e8d4de
CN = Microsoft TLS EV Issuing CA 01 O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 06 fe 1e fe d7 bc 72 46 7e 00 00 00 00 00 06	5/31/2018	5/31/2023	4e8cf75cec298a400 11ec6f345a1b0801 daa7f13d4f6df1f1c 8807dc92d0d437
CN = Microsoft TLS EV Issuing CA 05 OU = EOC O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 07 95 3b f3 a9 5f 91 07 55 00 00 00 00 00 07	5/31/2018	5/31/2023	190ee6be09b3c97c 1167dfd7bb366fe40 c066f188a6defb1e0 655a3f700341b1
CN = Microsoft TLS ECC EV Issuing CA 01 O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 03 b5 e4 64 b8 7f 90 c8 83 00 00 00 00 00 03	5/31/2018	5/31/2023	dbed47a27d2df69a f759ead788d33bdd 7bee79a33d3b762a 7806ffcfb3a3acb4

Issuing and Intermediate CAs	Serial Number	Issue Date	Expiration Date	SHA256 Thumbprint
CN = Microsoft TLS ECC EV Issuing CA 05 OU = EOC O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 04 f6 1d d4 6a 69 4a fe 86 00 00 00 00 00 04	5/31/2018	5/31/2023	664e415a24730152 16baeb56708271bc e20277e93b398c53 32ddd8b94c808327
CN = Microsoft TLS Issuing CA 01 O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 03 09 a4 fe b7 d2 c2 ab ca 00 00 00 00 00 03	5/31/2018	5/31/2023	f6be0e24c9bb74db 7674261e7404d7a3 9d0c1862708b8a0a 49d184d8b0c9b914
CN = Microsoft TLS Issuing CA 05 OU = EOC O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 04 3f 51 ec c6 02 13 1c 4c 00 00 00 00 00 04	5/31/2018	5/31/2023	4bc9fe53ce532690 216e157c76c77155 793c9be895d9f671 8ea3d3d1fd694aba
CN = Microsoft TLS ECC Issuing CA 01 O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 03 23 96 17 a3 31 58 4c 3b 00 00 00 00 00 03	5/31/2018	5/31/2023	a383b4a775ab1df5 e3e88507001ccc35 352f44bc82e46694 453fbf50406b4f6c
CN = Microsoft TLS ECC Issuing CA 05 OU = EOC O = Microsoft Corporation L = Redmond S = Washington C = US	33 00 00 00 04 8c 75 4d 11 c3 a1 94 12 00 00 00 00 00 04	5/31/2018	5/31/2023	ca61a36f29960ace5 9951f7ccef46e1368 faae5eb3d6c06284 cae56e0918d7f7

**APPENDIX B - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE
POLICY VERSIONS IN-SCOPE**

Policy Name	Policy Version	Policy Date
<u>Microsoft PKI Services Certificate Policy</u>	Version 3.1.1	July 10, 2018
<u>Microsoft PKI Services Certification Practice Statement</u>	Version 3.1.2	October 12, 2018