



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’s [assertion](#) that for its Certification Authority (“CA”) operations in the United States of America and the European Union, throughout the period November 1, 2018 to December 31, 2018 for the CAs enumerated in [Appendix A](#), Microsoft PKI Services has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of its Microsoft PKI Services Certificate Policy and Certification Practice Statement enumerated in [Appendix B](#)
- maintained effective controls to provide reasonable assurance that:
 - Microsoft PKI Services’ Certification Practice Statement is consistent with its Certificate Policy
 - Microsoft PKI Services provides its services in accordance with its Certificate Policy and Certification Practice Statement
- 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;
 - subscriber information is properly authenticated; and
 - subordinate CA certificate requests are accurate, authenticated, and approved
- 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

based on the [WebTrust Principles and Criteria for Certification Authorities v2.1](#). 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.

Microsoft PKI Services does not escrow CA keys, does not provide subscriber key lifecycle management services, and does not provide certificate suspension services. 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 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 Microsoft PKI Services' services beyond those covered by the [WebTrust Principles and Criteria for Certification Authorities v2.1](#) for CAs enumerated in [Appendix A](#), nor the suitability of any of Microsoft PKI Services' services for any customer's intended purpose.

Microsoft PKI Services' 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

Certified Public Accountants
St. Louis, Missouri
April 17, 2019



APPENDIX A - IN-SCOPE CAs

Root CAs	Serial Number	Issue Date	Expiration Date	SHA256 Thumbprint
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	df b3 c3 14 74 05 96 ad 5f b9 79 60 ef 62 ad 7c 1f cc ee ad 16 e7 40 54 65 2d 10 32 e6 f1 40 ef
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	ec dd 47 b5 ac bf a3 28 21 1e 1b ff 54 ad ea c9 5e 69 91 e3 c1 d5 0e 27 b5 27 e9 03 20 80 40 a1
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	6a ea 30 bc 02 ca 85 af cf ec 2f 65 f6 08 81 89 3c 92 69 25 fd 07 04 bd 8a da 3f 0f 6e dd b6 99
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	ec dd 47 b5 ac bf a3 28 21 1e 1b ff 54 ad ea c9 5e 69 91 e3 c1 d5 0e 27 b5 27 e9 03 20 80 40 a1



Subordinate 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	21 64 a6 9e 46 10 61 75 45 9f 1c cc 82 57 15 7b 04 2c 13 ee a5 88 a7 f1 b9 af d0 79 ff bf 28 bb
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	33 4a f3 b6 76 8a 86 93 99 de 24 20 79 03 8d 21 d1 fd a5 b9 86 57 08 d7 42 7f 7f 67 5d 58 8b 43
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	d2 1f ac ba b9 fa d0 8e ea c9 26 fb c6 d5 06 2b 07 f6 a7 6f 6b 2c 4c 47 f5 89 41 8a 94 14 9c 59
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	25 d4 1e 8a 85 43 37 1b 9c ad a5 e7 d1 52 21 d9 28 9c f3 f0 34 f5 80 8a 8f f9 d1 d8 92 e8 d4 de
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	4e 8c f7 5c ec 29 8a 40 01 1e c6 f3 45 a1 b0 80 1d aa 7f 13 d4 f6 df 1f 1c 88 07 dc 92 d0 d4 37
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	19 0e e6 be 09 b3 c9 7c 11 67 df d7 bb 36 6f e4 0c 06 6f 18 8a 6d ef b1 e0 65 5a 3f 70 03 41 b1
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	db ed 47 a2 7d 2d f6 9a f7 59 ea d7 88 d3 3b dd 7b ee 79 a3 3d 3b 76 2a 78 06 ff cf b3 a3 ac b4



Subordinate 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	66 4e 41 5a 24 73 01 52 16 ba eb 56 70 82 71 bc e2 02 77 e9 3b 39 8c 53 32 dd d8 b9 4c 80 83 27
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	f6 be 0e 24 c9 bb 74 db 76 74 26 1e 74 04 d7 a3 9d 0c 18 62 70 8b 8a 0a 49 d1 84 d8 b0 c9 b9 14
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	4b c9 fe 53 ce 53 26 90 21 6e 15 7c 76 c7 71 55 79 3c 9b e8 95 d9 f6 71 8e a3 d3 d1 fd 69 4a ba
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	a3 83 b4 a7 75 ab 1d f5 e3 e8 85 07 00 1c cc 35 35 2f 44 bc 82 e4 66 94 45 3f bf 50 40 6b 4f 6c
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	ca 61 a3 6f 29 96 0a ce 59 95 1f 7c ce f4 6e 13 68 fa ae 5e b3 d6 c0 62 84 ca e5 6e 09 18 d7 f7



**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 PKI SERVICES MANAGEMENT'S ASSERTION

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

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subordinate CA certification

The management of Microsoft PKI Services 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, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA 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, controls placed into operation can only provide reasonable assurance with respect to Microsoft PKI Services' CA operations.

Microsoft PKI Services management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in Microsoft PKI Services management's opinion, in providing its CA services in the United States of America and the European Union, throughout the period November 1, 2018 to December 31, 2018, Microsoft PKI Services has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of its Microsoft PKI Services Certificate Policy and Certification Practice Statement enumerated in [Appendix B](#)
- maintained effective controls to provide reasonable assurance that:
 - Microsoft PKI Services' Certification Practice Statement is consistent with its Certificate Policy; and
 - Microsoft PKI Services provides its services in accordance with its Certificate Policy and Certification Practice Statement
- 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;
 - subscriber information is properly authenticated; and

- subordinate CA certificate requests are accurate, authenticated, and approved
- 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

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
- CP and CPS Consistency

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

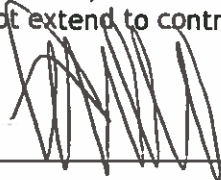
- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution

- Certificate Revocation
- Certificate Validation

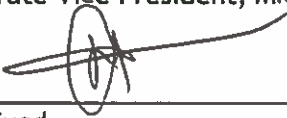
Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

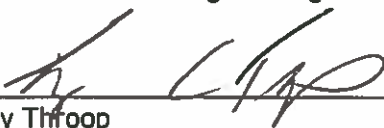
Microsoft PKI Services did not escrow CA keys, does not provide any subscriber key lifecycle management services, and does not provide certificate suspension services. Accordingly, our assertion did not extend to controls that would address those criteria.



Chuck Chan
Corporate Vice President, Microsoft Corporation



Raza Syed
Partner Software Engineering Manager, Microsoft Corporation



Tony Throop
Principal Service Engineering Manager, Microsoft Corporation

4/17, 2019

APPENDIX A - IN-SCOPE CAs

Root CAs	Serial Number	Issue Date	Expiration Date	SHA256 Thumbprint
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	df b3 c3 14 74 05 96 ad 5f b9 79 60 ef 62 ad 7c 1f cc ee ad 16 e7 40 54 65 2d 10 32 e6 f1 40 ef
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	ec dd 47 b5 ac bf a3 28 21 1e 1b ff 54 ad ea c9 5e 69 91 e3 c1 d5 0e 27 b5 27 e9 03 20 80 40 a1
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	6a ea 30 bc 02 ca 85 af cf ec 2f 65 f6 08 81 89 3c 92 69 25 fd 07 04 bd 8a da 3f 0f 6e dd b6 99
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	ec dd 47 b5 ac bf a3 28 21 1e 1b ff 54 ad ea c9 5e 69 91 e3 c1 d5 0e 27 b5 27 e9 03 20 80 40 a1

Subordinate 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	21 64 a6 9e 46 10 61 75 45 9f 1c cc 82 57 15 7b 04 2c 13 ee a5 88 a7 f1 b9 af d0 79 ff bf 28 bb
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	33 4a f3 b6 76 8a 86 93 99 de 24 20 79 03 8d 21 d1 fd a5 b9 86 57 08 d7 42 7f 7f 67 5d 58 8b 43
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	d2 1f ac ba b9 fa d0 8e ea c9 26 fb c6 d5 06 2b 07 f6 a7 6f 6b 2c 4c 47 f5 89 41 8a 94 14 9c 59
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	25 d4 1e 8a 85 43 37 1b 9c ad a5 e7 d1 52 21 d9 28 9c f3 f0 34 f5 80 8a 8f f9 d1 d8 92 e8 d4 de
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	4e 8c f7 5c ec 29 8a 40 01 1e c6 f3 45 a1 b0 80 1d aa 7f 13 d4 f6 df 1f 1c 88 07 dc 92 d0 d4 37
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	19 0e e6 be 09 b3 c9 7c 11 67 df d7 bb 36 6f e4 0c 06 6f 18 8a 6d ef b1 e0 65 5a 3f 70 03 41 b1
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	db ed 47 a2 7d 2d f6 9a f7 59 ea d7 88 d3 3b dd 7b ee 79 a3 3d 3b 76 2a 78 06 ff cf b3 a3 ac b4
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	66 4e 41 5a 24 73 01 52 16 ba eb 56 70 82 71 bc e2 02 77 e9 3b 39 8c 53 32 dd d8 b9 4c 80 83 27

Subordinate CAs	Serial Number	Issue Date	Expiration Date	SHA256 Thumbprint
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	f6 be 0e 24 c9 bb 74 db 76 74 26 1e 74 04 d7 a3 9d 0c 18 62 70 8b 8a 0a 49 d1 84 d8 b0 c9 b9 14
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	4b c9 fe 53 ce 53 26 90 21 6e 15 7c 76 c7 71 55 79 3c 9b e8 95 d9 f6 71 8e a3 d3 d1 fd 69 4a ba
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	a3 83 b4 a7 75 ab 1d f5 e3 e8 85 07 00 1c cc 35 35 2f 44 bc 82 e4 66 94 45 3f bf 50 40 6b 4f 6c
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	ca 61 a3 6f 29 96 0a ce 59 95 1f 7c ce f4 6e 13 68 fa ae 5e b3 d6 c0 62 84 ca e5 6e 09 18 d7 f7

**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