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

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

REPORT OF 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 at Redmond, Washington, throughout the period May 1, 2017 to April 30, 2018 for its root and issuing CAs enumerated in Appendix A, Microsoft PKI Services has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - PRSS PKI Certification Practice Statement, Version 2.1, effective April 30, 2014; and
  - PRSS PKI Certificate Policy, Version 2.1, effective April 30, 2014

- 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 v2.0. 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 v2.0 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
August 30, 2018

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 PKI Services (formerly known as PRSS PKI) operates the Certification Authority ("CA") services known as the root, issuing, and intermediate 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 in 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, even effective controls can only provide reasonable assurance with respect to Microsoft PKI Services' Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

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 at Redmond, Washington, throughout the period May 1, 2017 to April 30, 2018, Microsoft PKI Services has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its:
    - PRSS PKI Certification Practice Statement, Version 2.1, effective April 30, 2014; and
    - PRSS PKI Certificate Policy, Version 2.1, effective April 30, 2014

- 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 v2.0, 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 and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

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 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.

Chuck Chan
Corporate Vice President, Microsoft Corporation

Tony Throop
Principal Service Engineering Manager, Microsoft Corporation

August 30, 2018

APPENDIX A - IN-SCOPE CAs

Root CAs	Root CA Serial Numbers	Issue Date	Expiration Date	SHA2 Thumbprint
Microsoft Root Certificate Authority 2010	28cc3a25bfba44ac449a9b586b4339aa	6/23/2010	6/23/2035	df545bf919a2439c36983b54cdfc903dfa4f37d3996d8d84b4c31eec6f3c163e
Microsoft Root Certificate Authority 2011	3f8bc8b5fc9fb29643b569d66c42e144	3/22/2011	3/22/2036	847df6a78497943f27fc72eb93f9a637320a02b561d0a91b09e87a7807ed7c61
Microsoft Time Stamp Root Certificate Authority 2014	2fd67a432293329045e953343ee27466	10/22/2014	10/22/2039	65af95f4be86847344634282f941b2e605063ef0c8542f014ca088d182109e4f
Microsoft EV RSA Root Certificate Authority 2017	19fceb6df7cf57844184bdd9e0228e98	7/26/2017	7/26/2042	dfb3c314740596ad5fb97960ef62ad7c1fccead16e74054652d1032e6f140ef
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 Certificate List CA 2011	61116c92000000000007	3/29/2011	3/29/2026	a53a400df29ec7b8c8fce7cfffe47334f43b1642e604dd0307491737ebbc00ce
Microsoft Code Signing PCA 2010	610c524c000000000003	7/6/2010	7/6/2025	9aad6c1a83a1b974ba574a995af35b8ca772da919270db1605a8b81e1bbc896f
Microsoft Time-Stamp PCA 2010	6109812a000000000002	7/1/2010	7/1/2025	86ec118d1ee69670a46e2be29c4b4208be043e36600d4e1dd3f3d515ca119020
Microsoft Windows Group Edition PCA 2015	330000000eb6cc4aa62dd60fb400000000000e	2/16/2015	2/16/2030	f2c03399055918b4266fb73591306b1833519c84696e2d8b00ed66e602ea078c
Microsoft Windows PCA 2010	610c6a19000000000004	7/6/2010	7/6/2025	f01614a7a81ba477f0746cf2de71b20dddec709e756c9ea57cb67f93f25ba9fd
Microsoft Windows Phone PCA 2011	610b5c91000000000005	2/28/2011	6/23/2035	ae378d79d44cc75cee8bae50dd8bcbf2d4ff7c598b62fe75c3ce234c4001afd9
Microsoft Windows Phone Production PCA 2012	330000000bfcf98e584c1550bf00000000000b	7/24/2012	7/24/2027	e6a9b56a89aa3b191d23a6fb7fecb1f09ded4552a682fcf72b1d479c3b23c9ba
Microsoft Windows Production PCA 2011	61077656000000000000	10/19/2011	10/19/2026	e8e95f0733a55e8bad7be0a1413ee23c51fcea64b3c8fa6a786935fddcc71961

Microsoft Windows Third Party Component CA 2012	610baac1000000000009	4/18/2012	4/18/2027	9d08973e4d108da40a1a0b274180e17371134b4dd1621fa5c1f131b739b4b823
Microsoft Windows Third Party Component CA 2014	330000000d690d5d7893d076df00000000000d	10/15/2014	10/15/2029	a0f259a07039908eeb943e223fdf996e5e1e131d9aa6a602ff4672f7b9298aee
Windows Azure StorSimple CA 2013	330000000c8cc7499215880c9000000000000c	10/15/2013	10/15/2028	854b33f368f4d9ba80f4797d8e7150dc8754e7ef9e06acbec16f92c06e20debf
Microsoft Product Activation PCA 2017	3300000012F8893D928A35AC96000000000012	11/9/2017	11/9/2032	c88fdcf5dbf08996439ffd3abf59f2792b268042fac78fb8571ad14ad025aa29
Microsoft Code Signing PCA 2011	610e90d2000000000003	7/8/2011	7/8/2026	56da8722afd94066ffe1e4595473a4854892b843a0827d53fb7d8f4aeed1e18b
Microsoft MarketPlace PCA 2011	611244a2000000000002	3/28/2011	3/28/2031	5a9d217e71180301a044e4cfbde431fdf4c1cfc998b1b6343b5a10aa9e4cde98
Microsoft Marketplace CA G 005	330000003330b9f13b4e6a4af2000000000033	4/23/2015	4/23/2018	1acb2df1818567967cfd139c8522fdebea2645d3c180b269244c1ea2724f0c73
Microsoft Marketplace CA G 006	330000034872f87a3cebd3932000000000034	4/23/2015	4/23/2018	6858e9695edf16c015604d7b4c146f99df0e374176ee134482e6998635824ca7
Microsoft Marketplace CA G 007	330000003570d508224a521b7d000000000035	4/23/2015	4/23/2018	690454775477a86fb3dcc1412fb079940314ffad2c796ce7a7390d0dcf3a2098
Microsoft Marketplace CA G 008	33000000362033204d2485aab8000000000036	4/23/2015	4/23/2018	6468de88eaa4074ddd0bb9d2373bc45e337103a4ae9b1477db64028c9f073df7
Microsoft Marketplace CA G 013	330000003736acb2cda1f02ee2000000000037	4/23/2015	4/23/2018	7fbe6577958a6dd8ecd3443b8ddce108cf76bcb42aefaf73df3c876c09f3f7d4
Microsoft Marketplace CA G 014	330000003831a20d13229e6cde000000000038	4/23/2015	4/23/2018	a34cb0e17d37dc7736dbcf31a78da80fc8d3790c449b1b0f50cebc3e6f65e30a
Microsoft Marketplace CA G 015	33000000391c5461658d75259a000000000039	4/23/2015	4/23/2018	ec148cbc2a80f17f845f898e90c4cc01b2c15c55874fad9b157a50c9961e65e5
Microsoft Marketplace CA G 016	330000003a5c1c2e9fef89044f00000000003a	4/23/2015	4/23/2018	3493f8ffda829195f0a1dbbc05322c3b50f9160288e6686395652ff4ab70a3c2
Microsoft Marketplace CA G 005	330000003EEDE57AA30E2813100000000003E	4/20/2018	4/20/2021	6d015030254f113384bb84df7ae4101e847aa68c9512e06b9fd94b685ec4105c
Microsoft Marketplace CA G 006	330000003F3CA398F2A257D86800000000003F	4/20/2018	4/20/2021	7f593b5bce55f051af287173b0b631b23026c1ed77e5a5690fc5234cd9f39dec
Microsoft Marketplace CA G 007	3300000040C32355D7DCC71E6D000000000040	4/20/2018	4/20/2021	77b9ce9c07d79166705b24105cb154ec6dac2c7d3a0f000fba862f0bce2908dd
Microsoft Marketplace CA G 008	3300000041C7E764017DF7735E000000000041	4/20/2018	4/20/2021	ae2b75de2a6bbbf965e5de098b4f8e4bc823445199be83c4ae6ed371cd492600

Microsoft Marketplace CA G 013	3300000042B36D441C68F2A8A6000000000042	4/20/2018	4/20/2021	4dff346dade949801f59c56c31ac1d61ab322f5b600a1c03120d800c5e8f19ce
Microsoft Marketplace CA G 014	330000043633B9F2A9E4F901500000000043	4/20/2018	4/20/2021	00d876447582f62d97a424aeaa4683c4f015e4a8c9e9e3f9edff7b3ef3dfd205
Microsoft Marketplace CA G 015	33000000447BF66637014247E100000000044	4/20/2018	4/20/2021	301ffb7db07d8cc9a2a0086c0b3175cfc5255afd0d249ad004952ee5e9ee7340
Microsoft Marketplace CA G 016	33000000456DF526E19CB67930000000000045	4/20/2018	4/20/2021	61f3de02889956a8b8664174e0404774fff46de3e20c33378c4cb961c4a671e9
Microsoft Marketplace Production CA 2011	6109cb72000000000026	11/14/2011	11/14/2021	8e8a92ea4bca5e3ce34b39bb1e5fda1a76d14d7d513cb8900d193bec11f79238
Microsoft Secure Server CA 2011	613fb718000000000004	10/18/2011	10/18/2026	83688f2aef71386e0936c4b3013b07e8e0c796d8427716dd48b2a63d79509129
Microsoft Update Secure Server CA 2.1	330000000ab891a2c80a50a5df00000000000a	6/21/2012	6/21/2027	6139e2df97dc93bf7e90a303f75b3968fd06c57316b45e94dcff773707cf2754
Microsoft Update Secure Server CA 2.2	330000000b9aa76bb008015cf800000000000b	6/21/2012	6/21/2027	c1bc7ac733dec68a6a6af944a5a2b4f79f492abaace213811f6ef681d7861b57
Microsoft Update Signing CA 2.1	3300000007b1cc402755483f69000000000007	6/19/2012	6/19/2027	882f36d6f0dabf4b017fc6e8ea6d4f0f2786300d7b8210c3ae5c793f95e1c0c9
Microsoft Update Signing CA 2.2	330000000859e394e054c7175d000000000008	6/19/2012	6/19/2027	24919d52efb9ecbec6c1d24cbc2e10d041b516b9410d6ceb75ff2f348bd0e5c8
Microsoft Update Signing CA 2.3	33000000009528549ad55d42715000000000009	6/19/2012	6/19/2027	46b4d5b761ca7b14d4877c3b2d3f22dbf92bc34b694e971e942517dabeb4b06c
Microsoft Windows Third Party Component CA 2013	33000000149dfbc31f1f63c310000000000014	5/1/2013	5/1/2028	8ef01bb5e07987053659e039e5a72580c88c444bc1a31ab412ce81a4ad53044e
Microsoft Time Stamp PCA 2015	3300000002F9FA0638351073C2000000000002	3/25/2015	3/25/2030	857aec60913116e2b61190b1e86fa001f27e8d165faed492f829313e8212b666
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