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 – Product Release and Security Services - Public Key Infrastructure ("PRSS PKI"):

We have examined PRSS PKI management's assertion that in generating and protecting its PRSS PKI Root CAs listed below on July 26, 2017 at Redmond, Washington, with the following identifying information:

Root Name	Certificate Serial Number	Subject Key Identifier	SHA1 Thumbprint
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	09 cb 59 7f 86 b2 70 8f 1a c3 39 e3 c0 d9 e9 bf bb 4d b2 23	ee 68 c3 e9 4a b5 d5 5e b9 39 51 16 42 4e 25 b0 ca dd 90 09
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	41 ca ff 16 b2 09 4e dc 24 c8 4b e4 5c 16 25 99 f8 26 ef 3b	3a d3 8a 39 ce 4e 88 dc df 46 99 5e 96 9f c3 39 d0 79 98 58
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	c8 cb 99 72 70 52 0c f8 e6 be b2 04 57 29 2a cf 42 10 ed 35	7c a9 01 3d 43 72 15 51 e9 87 38 0b 3e ae 4b 44 2d c0 37 ea
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	63 e7 f4 e0 22 0a cc b0 16 cf b4 3f 06 f5 83 f0 df f9 5b 91	b8 09 5f 5a 89 fb 47 a7 01 7e d7 94 dd 4f 61 1e 27 83 0e 27

PRSS PKI has:

- followed the CA key generation and protection requirements in its:
  - PRSS PKI Certification Practice Statement, Version 2.1, effective April 30, 2014 ("CPS"); and
  - PRSS PKI Certificate Policy, Version 2.1, effective April 30, 2014 ("CP")

- included appropriate, detailed procedures and controls in its Root Key Generation Script for the PRSS PKI Roots CAs dated July 26, 2017

- maintained effective controls to provide reasonable assurance that the PRSS PKI Root CAs were generated and protected in conformity with the procedures described in its CP, CPS, and its Root Key Generation Script

- performed, during the root key generation process, all procedures required by the Root Key Generation Script

- generated the CA keys in a physically secured environmental as described in its CP and CPS

- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge

- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP and CPS

based on CA Key Generation Criterion 4.1 of the Trust Service Principles and Criteria for Certification Authorities v2.0.

PRSS PKI's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

We conducted our examination in accordance with standards for attestation engagements established by the American Institute of Certified Public Accountants and, accordingly, included:

(1) obtaining an understanding of PRSS PKI's documented plan of procedures to be performed for the generation of the certification authority key pairs for the PRSS PKI Root CAs;
(2) reviewing the detailed CA key generation script for conformance with industry standard practices;
(3) testing and evaluating, during the CA key generation process, the effectiveness of controls over the integrity, confidentiality, and availability of all private keys, including back-up copies, and access keys (including physical keys, tokens, and passwords), used in the establishment of the service;

(4) physical observation of all procedures performed during the root key generation process to ensure that the procedures actually performed on July 26, 2017 were in accordance with the Root Key Generation Script for the PRSS PKI Root CAs; and
(5) performing such other procedures as we considered necessary in the circumstances.

We believe that our examination provides a reasonable basis for our opinion.

In our opinion, on July 26, 2017, PRSS PKI management's assertion, as referred to above, is fairly stated, in all material respects, based on CA Key Generation Criterion 4.1 of the Trust Service Principles and Criteria for Certification Authorities v2.0.

This report does not include any representation as to the quality of PRSS PKI's services other than its CA operations at Redmond, Washington, nor the suitability of any of PRSS PKI's services for any customer's intended purpose.

BDO USA, LLP

Certified Public Accountants
St. Louis, Missouri
October 13, 2017

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

PRSS PKI MANAGEMENT'S ASSERTION

Oct 13, 2017

Microsoft - Product Release and Security Services - Public Key Infrastructure ("PRSS-PKI") has deployed a public key infrastructure. As part of this deployment, it was necessary to create a hierarchy consistent of self-signed Root CAs known as its PRSS PKI Root CAs, listed below. These CA's will serve as Root CAs for client certificate services. In order to allow the CA's to be installed in a final production configuration, a Root Key Generation Ceremony was conducted, the purpose of which was to formally witness and document the creation of the CA's private signing key. This helps assure the non-refutability of the integrity of the PRSS PKI Root CAs' key pairs, and in particular, the private signing keys.

PRSS PKI management has securely generated key pairs, each consisting of a public and private key, in support of its CA operations. The key pairs were generated in accordance with procedures described in PRSS PKI's Certificate Policy ("CP"), Certification Practice Statement ("CPS"), and Root Key Generation Script for the PRSS PKI Roots, which are based on CA Key Generation Criterion 4.1 of the Trust Service Principles and Criteria for Certification Authorities v2.0.

PRSS PKI management established and maintained effective controls over the generation of these keys. These controls were designed to provide reasonable assurance of adherence to the above-mentioned practices throughout the root key generation process.

PRSS PKI management is responsible for establishing and maintaining procedures over its CA root key generations, and over the integrity and confidentiality of all private keys and access keys (including physical keys, tokens, and passwords) used in the establishment of the PRSS PKI Root CAs, and for the CA environment controls relevant to the generation and protection of its CA keys.

PRSS PKI management has assessed the procedures and controls for the generation of the CA keys. Based on that assessment, in management's opinion, in generation and protecting its CA keys for the PRSS PKI Root CA's on July 26, 2017 at Redmond, Washington, with the following identifying information:

Root Name	Certificate Serial Number	Subject Key Identifier	SHA1 Thumbprint
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	09 cb 59 7f 86 b2 70 8f 1a c3 39 e3 c0 d9 e9 bf bb 4d b2 23	ee 68 c3 e9 4a b5 d5 5e b9 39 51 16 42 4e 25 b0 ca dd 90 09
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	41 ca ff 16 b2 09 4e dc 24 c8 4b e4 5c 16 25 99 f8 26 ef 3b	3a d3 8a 39 ce 4e 88 dc df 46 99 5e 96 9f c3 39 d0 79 98 58
CN = Microsoft ECC Root Certificate Authority 2017	71 76 7e 8d 58 e4 fc 96 49 c6 3e fb cf 3a bd a7	c8 cb 99 72 70 52 0c f8 e6 be b2 04	7c a9 01 3d 43 72 15 51 e9 87 38 0b

O = Microsoft Corporation L = Redmond S = Washington C = US		57 29 2a cf 42 10 ed 35	3e ae 4b 44 2d c0 37 ea
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	63 e7 f4 e0 22 0a cc b0 16 cf b4 3f 06 f5 83 f0 df f9 5b 91	b8 09 5f 5a 89 fb 47 a7 01 7e d7 94 dd 4f 61 1e 27 83 0e 27

PRSS PKI has:

- followed the CA key generation and protection requirements 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
- included appropriate, detailed procedures and controls in its Root Key Generation Script for the PRSS PKI Root CAs dated July 26, 2017
- maintained effective controls to provide reasonable assurance that the PRSS PKI Root CAs were generated and protected in conformity with the procedures described in its CP, CPS, and its Root Key Generation Script
- performed, during the root key generation process, all procedures required by the Root Key Generation Script
- generated the CA keys in a physically secured environment as described in its CP and CPS
- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge
- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP and CPS based on CA Key Generation Criterion 4.1 of the Trust Service Principles and Criteria for Certification Authorities v2.0.

Chuck Chan
Corporate Vice President, Windows Devices and Networking Technologies

Tony Thropp
Principal SVC Engineering Manager