



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 Corporation Digital Security & Risk Engineering (“Microsoft DSRE”):

We have examined for Microsoft DSRE’s [assertion](#) that for its certification authority (“CA”) operations in the state of Washington in United States of America, Puerto Rico, and Ireland, throughout the period July 1, 2019 to June 30, 2020 as enumerated in [Attachment A](#), Microsoft DSRE has:

- disclosed its SSL certificate lifecycle management business practices in the applicable versions of its Certificate Policy/Certification Practice Statement enumerated in [Attachment B](#), including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Microsoft DSRE [repository](#), and provided 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 v2.4.1](#). Microsoft DSRE 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 DSRE 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 DSRE’s 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, Microsoft DSRE’s management assertion, as referred to above, is fairly stated, in all material respects.

Without modifying our opinion, we noted the following other matters during our procedures:

Matter Topic		Matter
1	Problem Reporting email provided via CPS was not functioning	The Problem Reporting e-mail provided in Microsoft’s CP/CPS (pkiwg@microsoft.com) was not working for 13 days during the examination period. This was discovered externally and reported to Microsoft. For additional details see Mozilla Bug 1604124 .
2	OCSP responders were returning signed responses for requests not associated with a related CA.	Microsoft uses GlobalSign for its OCSP response services and during the examination period DSRE became aware of an issue where the OCSP service received a request from a CA it was not familiar with and returned a signed unknown response. The responder signed the response with a default OCSP response of unknown. This is in violation of RFC 6960. For additional details see Mozilla Bug 1620727 .
3	Access Review	System account reviews were not performed in a timely manner as required by the Network and Certificate Systems Security Requirements for three months during the examination period. For additional details see Mozilla Bug 1652827 .
4	Incorrect OCSP Delegated Responder Certificate	DigiCert inappropriately assigned DSRE’s issuing CAs as delegated OSCP responders. DSRE and DigiCert were working to replace the issuing CAs and destroy the prior CA keys subsequent to the examination period. For additional details see Mozilla Bug 1649951 .



This report does not include any representation as to the quality of Microsoft DSRE's services other than its CA operations at in the state of Washington in United States of America, Puerto Rico, and Ireland, nor the suitability of any of Microsoft DSRE's services for any customer's intended purpose.

Microsoft DSRE's 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.

The World Health Organization classified the COVID-19 outbreak as a pandemic in March 2020. Based on the rapid increase in exposure globally, the gravity or length of the impact of the COVID-19 outbreak cannot be estimated at this time.

BDO USA, LLP

August 17, 2020



ATTACHMENT A - IN-SCOPE CAs

Issuing CAs	Serial Number	SHA2 Thumbprint
CN = Microsoft IT TLS CA 1 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	08 b8 7a 50 1b be 9c da 2d 16 4d 3e 39 51 bf 55	4f f4 04 f0 2e 2c d0 01 88 f1 5d 1c 00 f4 b6 d1 e3 8b 5a 39 5c f8 53 14 ea eb a8 55 b6 a6 4b 75
CN = Microsoft IT TLS CA 2 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	0f 2c 10 c9 5b 06 c0 93 7f b8 d4 49 f8 3e 85 69	4e 10 7c 98 1b 42 ac be 41 c0 10 67 e1 6d 44 db 64 81 4d 41 93 e5 72 31 7e a0 4b 87 c7 9c 47 5f
CN = Microsoft IT TLS CA 4 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	0b 6a b3 b0 3e b1 a9 f6 c4 60 92 6a a8 cd fe b3	5f fa c4 3e 0d dc 5b 4a f2 b6 96 f6 bc 4d b7 e9 1d f3 14 bb 8f e0 d0 71 3a 0b 1a 7a d2 a6 8f ac
CN = Microsoft IT TLS CA 5 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	08 88 cd 52 5f 19 24 44 4d 14 a5 82 91 de b9 52	f0 ee 59 14 ed 94 c7 25 2d 05 8b 4e 39 80 8a ee 6f a8 f6 2c f0 97 4f b7 d6 d2 a9 df 16 e3 a8 7f



ATTACHMENT B - IN-SCOPE CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY VERSIONS

Policy Name	Version	Effective Date
<u>DSRE PKI Certificate Policy/Certification Practice Statement for TLS CAs</u>	2.3	June 1, 2019
<u>DSRE PKI Certificate Policy/Certification Practice Statement for TLS CAs</u>	2.4	April 1, 2020



Microsoft Corporation Digital Security & Risk Engineering Management's Assertion

Microsoft Corporation Digital Security & Risk Engineering ("Microsoft DSRE") operates the Certification Authority ("CA") services for its CAs enumerated in [Attachment A](#) in scope for SSL Baseline and Network Security Requirements and provides SSL CA services.

Microsoft DSRE's 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 in the state of Washington in United States of America, Puerto Rico, and Ireland, throughout the period July 1, 2019 to June 30, 2020, Microsoft DSRE has:

- disclosed its SSL certificate lifecycle management business practices in the applicable versions of its Certificate Policy/Certificate Practice Statement enumerated in [Attachment B](#) including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Microsoft DSRE [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 v2.4.1](#).

A handwritten signature in black ink, appearing to read "Biju Mathew", written over a horizontal line.

Biju Mathew
Principal Service Engineering Manager
August 17, 2020



ATTACHMENT A - IN-SCOPE CAs

Issuing CAs	Serial Number	SHA2 Thumbprint
CN = Microsoft IT TLS CA 1 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	08 b8 7a 50 1b be 9c da 2d 16 4d 3e 39 51 bf 55	4f f4 04 f0 2e 2c d0 01 88 f1 5d 1c 00 f4 b6 d1 e3 8b 5a 39 5c f8 53 14 ea eb a8 55 b6 a6 4b 75
CN = Microsoft IT TLS CA 2 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	0f 2c 10 c9 5b 06 c0 93 7f b8 d4 49 f8 3e 85 69	4e 10 7c 98 1b 42 ac be 41 c0 10 67 e1 6d 44 db 64 81 4d 41 93 e5 72 31 7e a0 4b 87 c7 9c 47 5f
CN = Microsoft IT TLS CA 4 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	0b 6a b3 b0 3e b1 a9 f6 c4 60 92 6a a8 cd fe b3	5f fa c4 3e 0d dc 5b 4a f2 b6 96 f6 bc 4d b7 e9 1d f3 14 bb 8f e0 d0 71 3a 0b 1a 7a d2 a6 8f ac
CN = Microsoft IT TLS CA 5 OU = Microsoft IT O = Microsoft Corporation L = Redmond S = Washington C = US	08 88 cd 52 5f 19 24 44 4d 14 a5 82 91 de b9 52	f0 ee 59 14 ed 94 c7 25 2d 05 8b 4e 39 80 8a ee 6f a8 f6 2c f0 97 4f b7 d6 d2 a9 df 16 e3 a8 7f



ATTACHMENT B - IN-SCOPE CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY VERSIONS

Policy Name	Version	Effective Date
DSRE PKI Certificate Policy/Certification Practice Statement for TLS CAs	2.3	June 1, 2019
DSRE PKI Certificate Policy/Certification Practice Statement for TLS CAs	2.4	April 1, 2020