REPORT OF INDEPENDENT CERTIFIED PUBLIC ACCOUNTANTS

To the Management of IdenTrust Services, LLC:

Scope

We have examined the assertion by the management of IdenTrust Services, LLC ("IdenTrust") that in providing its TrustID, Access Certificates for Electronic Services (ACES), and Department of Defense External Certification Authority (DOD ECA) SSL Certification Authority (CA) services at its Salt Lake City, Utah, USA, and Centennial, Colorado, USA, locations, throughout the period from July 1, 2018, to June 30, 2019, for its root and subordinate CA certificates as listed in Appendix A, management of IdenTrust has:

- Disclosed its SSL Certificate practices and procedures in its certificate policies and certification practice statements

Trust ID	Certificate Policy v4.3 Certification Practices Statement v4.3
Access Certificates for Electronic Services (ACES)	Certificate Policy v3.2 Certification Practice Statement v5.5
Department of Defense External Certification Authority (DOD ECA)	Certificate Policy 4.4 Certification Practice Statement v2.1

  including its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Requirements

- Maintained effective controls to provide reasonable assurance that:
  - Subscriber information was properly collected, authenticated (for the registration activities performed by the CA) and verified;
  - The integrity of keys and certificates it manages is established and protected throughout their life cycles;
- 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;
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity; and
- Maintained effective controls to provide reasonable assurance that:
  - Network and Certificate System Security Requirements as set forth by the CA/Browser Forum were met

  based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.3.

IdenTrust's Responsibilities

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

IdenTrust makes use of external registration authorities for specific subscriber registration activities as disclosed in IdenTrust's business practice disclosures. Our examination did not extend to the controls exercised by the external registration authorities.

The relative effectiveness and significance of specific controls at IdenTrust 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 external registration authorities, individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at external registration authorities, individual subscriber and relying party locations.

Independent Certified Public Accountant's Responsibilities

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). 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.

Inherent Limitations

Because of the nature and inherent limitations of controls, IdenTrust'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.

Emphasis of Matter

IdenTrust has disclosed the following information in response to reported violations of the Baseline Requirements:

- In response to internally mis-issued .int Top Level Domain (TLD) certificates reported in February 2018, IdenTrust revoked the certificates on the same day it became aware of the issue. Additionally, IdenTrust updated its certificate approval process to prevent domain names with .int TLD from being approved.
- In response to a discrepancy identified during an internal systems review with the values of address fields in 12 TLS/SSL certificates compared to the values on record for the applicant organization, IdenTrust revoked these certificates and implemented changes to its certificate registration application in February 2019, to prevent further issuance of certificates with this issue.
- In response to a failure to publicly disclose an unconstrained intermediate CA within seven (7) days of creation, IdenTrust implemented revised procedures in April 2019 to notify the program manager, confirm the subordinate CA is logged into certificate transparency (CT) logs, and add the subordinate CA into Mozilla's CCADB within seven (7) days of creation.

During our assessment, Schellman performed testing of certificate issuance, on a sample basis, and noted that none of the samples tested included the conditions above.

Opinion

In our opinion, for the period July 1, 2018, to June 30, 2019, IdenTrust's 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 IdenTrust's services other than its CA operations at its Salt Lake City, Utah, USA, and Centennial, Colorado, USA, locations, nor the suitability of any of IdenTrust's services for any customer's intended purpose.

IdenTrust's use of the WebTrust Principles and Criteria 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.

Schellman & Company, LLC

Schellman & Company, LLC
Certified Public Accountants
Tampa, Florida
November 4, 2019

ASSERTION OF MANAGEMENT AS TO ITS DISCLOSURE OF ITS PRACTICES AND ITS CONTROLS OVER ITS SSL CERTIFICATION AUTHORITY OPERATIONS DURING THE PERIOD FROM JULY 1, 2018, TO JUNE 30, 2019

November 4, 2019

IdenTrust Services, LLC ("IdenTrust") operates the Certification Authority (CA) services known as TrustID, Access Certificates for Electronic Services (ACES), and Department of Defense External Certification Authority (DOD ECA) and provides SSL CA services.

IdenTrust management has assessed the controls over its SSL CA services. Based on that assessment, in IdenTrust management's opinion, in providing its SSL CA services at its Salt Lake City, Utah, USA, and Centennial, Colorado, USA, locations throughout the period from July 1, 2018, to June 30, 2019, for its root and subordinate CA certificates as listed in Appendix A, IdenTrust has:

- Disclosed its Certificate practices and procedures in its certificate policies and certification practice statements

Trust ID	Certificate Policy v4.3 Certification Practices Statement v4.3
Access Certificates for Electronic Services (ACES)	Certificate Policy v3.2 Certification Practice Statement v5.5
Department of Defense External Certification Authority (DOD ECA)	Certificate Policy 4.4 Certification Practice Statement v2.1

  including its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines

- Maintained effective controls to provide reasonable assurance that:
  - Subscriber information was properly collected, authenticated (for the registration activities performed by the CA) and verified;
  - The integrity of keys and certificates it manages is established and protected throughout their life cycles;
- 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;
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity; and
- Maintained effective controls to provide reasonable assurance that:
  - Network and Certificate System Security Requirements as set forth by the CA/Browser Forum were met

  based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.3.

Emphasis of Matter

IdenTrust has disclosed the following information in response to reported violations of the Baseline Requirements:

- In response to internally mis-issued .int Top Level Domain (TLD) certificates reported in February 2018, IdenTrust revoked the certificates on the same day it became aware of the issue. Additionally, IdenTrust updated its certificate approval process to prevent domain names with .int TLD from being approved.
- In response to a discrepancy identified during an internal systems review with the values of address fields in 12 TLS/SSL certificates compared to the values on record for the applicant organization, IdenTrust revoked these certificates and implemented changes to its certificate registration application in February 2019, to prevent further issuance of certificates with this issue.
- In response to a failure to publicly disclose an unconstrained intermediate CA within seven (7) days of creation, IdenTrust implemented revised procedures in April 2019 to notify the program manager, confirm the subordinate CA is logged into certificate transparency (CT) logs, and add the subordinate CA into Mozilla's CCADB within seven (7) days of creation.

Donald S. Johnson
Chief Information Officer

APPENDIX A – IDENTRUST ROOT AND ISSUING CAs

Name	SubCA	Certificate Thumbprint (sha256)
IdenTrust Commercial Root CA1		5D56499BE4D2E08BCFCAD08A3E38723D50503BDE706948E42F55603019E528AE
	IdenTrust Commercial Root CA 1	AAE38F67F0A626805928507B078D89D5598D760D17335927B46606ECDFA1B946
	TrustID Server CA A5 2	B39C4A4596D3191AFA3B3D254D28E5C482FCD0D500E0A9337F99277CB8A2EEF8
	Booz Allen Hamilton B A CA 01*	DCCA716167F029AA9A309EE8CA3FF1F4017D1A1F3D1981BDFF9E5AF3F503682A
IdenTrust Public Sector Root CA 1		30D0895A9A448A262091635522D1F52010B5867ACAE12C78EF958FD4F4389F2F
	IdenTrust ACES CA 2	C5480D7BFF952D1BE86178FF713F11F51CF74232EE5676FC5A170D4A6A6FE50A
	IdenTrust ACES CA 2	9D1585E63B4D03D9ABBA0C67D46730BADF0FCEBC2081611CF7B9AA572D2D64A4
	IdenTrust ACES CA 2	A59740F91153C0FB1C1E37081CD7198E0BC28B58C1D561DB785CB82B4AD9DF47
DST Root CA X3		0687260331A72403D909F105E69BCF0D32E1BD2493FFC6D9206D11BCD6770739
	IdenTrust Commercial Root CA 1	91B18588225035BB2F231FEF7695E497B289934B65CB87CFC2212271EBECB58C
	IdenTrust Commercial Root CA 1	F49793F8DF83CE64A8C8D50DF366B64E98C2538A2AAAB2019CA0367A1FCC03CB
	Let's Encrypt Authority X1 (cross-signed)**	7FDCE3BF4103C2684B3ADBB5792884BD45C75094C217788863950346F79C90A3
	Let's Encrypt Authority X2 (cross-signed)**	EC0C6CA496A67A13342FEC5221F68D4B3E53B1BC22F6E4BCCC9C68F0415CDEA4
	Let's Encrypt Authority X3 (cross-signed)**	25847D668EB4F04FDD40B12B6B0740C567DA7D024308EB6C2C96FE41D9DE218D
	Let's Encrypt Authority X4 (cross-signed)**	A74B0C32B65B95FE2C4F8F098947A68B695033BED0B51DD8B984ECAE89571BB6

* The Booz Allen Hamilton (BAH) subordinate CA certificate was signed with a key controlled by IdenTrust, and the certificate is subject to the TrustID CP/CPS. While the subscriber certificates under this subordinate CA certificate are issued by IdenTrust, the identification and authentication procedures for these subscriber certificates are performed by Booz Allen Hamilton, an external registration authority. Accordingly, the examination by Schellman & Company, LLC, did not extend to controls exercised or certificates issued by any external registration authorities.

** The cross-signed certificates were signed with a key controlled by IdenTrust, and the certificates are subject to the TrustID CP/CPS. While the cross-signing establishes a trusted relationship, the cross-signed certificates are not controlled by IdenTrust. Accordingly, the examination by Schellman & Company, LLC did not extend to the controls exercised or certificates issued by any external registration authorities.