schellman

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), IdenTrust Global Common (IGC), 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, 2017, to June 30, 2018, 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 v2.4 Certification Practices Statement v3.5
Access Certificates for Electronic Services (ACES)	Certificate Policy v3.1 Certification Practice Statement v5.3
IdenTrust Global Common (IGC)	Certificate Policy v1.4.4 Certification Practice Statement v1.4.5
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. 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 on Matters

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

- In response to internally mis-issued certificates for a new product being built, IdenTrust corrected the certificate profiles in March 2017. The offending certificates were revoked on August 10, 2017.
- In response to improper encoding of wildcard certificates, configuration modifications were made as of August 14, 2017, to prevent further issuance of certificates with this issue.
- In response to improper subject organization names related to certificates issued for government associated entities, IdenTrust implemented controls in August 2017 to prevent the common name use of "U.S. Government" for non-agency entities.
- In response to certificates issued with HTTPS OCSP responder URLs, IdenTrust altered the certificate profiles for certificates issued under the ACES SubCA to include HTTP OCSP URLs.

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

Opinion

In our opinion, for the period July 1, 2017, to June 30, 2018, 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
July 31, 2018

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, 2017, TO JUNE 30, 2018

IdenTrust Services, LLC ("IdenTrust") operates the Certification Authority (CA) services known as TrustID, Access Certificates for Electronic Services (ACES), IdenTrust Global Common (IGC), 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, 2017, to June 30, 2018, 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 v2.4 Certification Practices Statement v3.5
Access Certificates for Electronic Services (ACES)	Certificate Policy v3.1 Certification Practice Statement v5.3
IdenTrust Global Common (IGC)	Certificate Policy v1.4.4 Certification Practice Statement v1.4.5
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.

Donald S. Johnson

Donald S. Johnson
Chief Information Officer
July 31, 2018

APPENDIX A – IDENTRUST ROOT AND ISSUING CAs

Name	Program	Certificate Thumbprint (sha256)
DST ACES CA X6 (Root)	ACES	7C:6D:B2:FF:9D:44:00:91:A9:A0:D7:F9:78:6D:6B:A5:F2:68:2B:74:D8:5E:A0:D2:CE:07:19:16:4C:B8:21:70
IdenTrust ACES CA 1 (Expired)	ACES	B6:C5:DC:24:14:D6:94:DA:F1:B7:2B:83:FD:AB:15:F9:0E:3B:15:13:DE:77:36:41:12:4F:D8:40:B4:E7:F6:5B
IdenTrust Public Sector Root CA 1	ACES	9B:42:82:F5:A4:02:E1:90:16:C4:87:4A:52:DF:33:67:EA:BC:CF:05:BE:85:1A:D0:30:39:F7:77:A6:02:D3:0A
IdenTrust ACES CA 2	ACES	49:6C:5C:4C:59:FB:24:A7:DE:63:61:7C:AA:CA:39:A4:18:31:0B:B8:2F:02:CC:52:EB:B6:72:55:42:79:8C:CE
IdenTrust Global Comment Root CA 1	IGC	E4:D3:B7:00:CF:5D:0F:95:5F:E8:4A:66:B8:AA:34:7A:EF:09:C8:1C:39:2E:6E:EE:62:9B:29:E1:E2:33:58:78
IGC CA 1	IGC	87:E1:47:F5:DF:59:75:68:BC:BA:2C:EA:C0:3D:FB:4E:B6:19:6A:0B:16:93:22:F6:CF:F5:F3:A6:E0:02:97:C3
IGC Server CA 1	IGC	9C:DE:77:46:3B:CC:30:AD:F0:6D:9E:FE:7D:6F:8A:C0:8C:21:37:C8:8E:0A:9F:CC:CD:DF:E6:6D:50:2E:52:AD
Booz Allen Hamilton PIVi CA 01	IGC	72:BF:5A:D3:96:FA:5E:F5:2B:5F:ED:0C:63:2E:4A:DB:AA:43:F9:26:B1:4E:9D:55:1D:2F:2E:DA:8C:B3:A6:75
VA Patient Direct CA 1	IGC	1C:C0:90:DD:BA:B5:6D:F0:08:44:83:3A:33:88:3E:E7:E1:4D:C4:B2:02:CB:97:F2:D7:FD:3F:CB:E9:50:75:62
VA Provider Direct CA 1	IGC	B1:EA:DE:9B:16:43:35:E9:01:55:93:EB:43:2E:3D:69:07:BE:0A:69:4C:13:AD:53:6E:9B:87:A8:67:98:00:30
Leidos FBCA Cloud PKI CA-1	IGC	93:16:7E:E2:2F:6A:5B:2D:62:E1:63:15:51:8B:90:66:25:B4:A8:23:0C:E1:F0:79:56:1C:5A:09:6B:97:BF:CF
DST Root CA X3	TrustID	55:C1:37:2C:7D:6E:D0:38:90:35:49:2B:49:E1:C0:91:CD:00:A5:BA:85:DC:C4:19:0D:23:21:86:B0:21:AE:5A
TrustID CA A1	TrustID	80:AC:E0:65:94:8C:19:5E:7C:EC:E1:04:9B:75:BC:9E:EB:1A:37:E7:62:58:1D:7F:7F:91:82:37:32:19:2C:5B
IdenTrust Commercial Root CA 1	TrustID	1D:03:B9:65:51:1C:E5:0D:0A:0B:AE:1B:54:9E:D7:04:8C:78:3C:FC:BA:9A:A4:0E:A1:1D:35:5B:18:89:65:7C
TrustID Server CA A52	TrustID	85:0D:8E:BF:EA:B2:29:9C:EC:E8:23:66:A2:DC:56:77:23:4B:78:38:AF:69:E3:6B:E6:BA:BD:78:DD:21:C2:01
TrustID CA A12	TrustID	F0:B3:EB:D8:4E:98:8A:78:66:E7:23:4A:F0:79:C8:9C:D0:2A:86:A7:EB:A0:9B:72:75:EF:02:A4:15:C8:8F:C9
BAH BA CA 01	TrustID	90:9C:96:55:2D:CA:BE:91:FB:5B:FD:4A:59:93:CB:B3:95:0C:4E:A8:10:72:21:63:42:59:BF:73:BD:9C:E5:5A
IdenTrust ECA 4 (Non-Issuing, Validation Only)	ECA	40:50:22:2F:58:17:EF:0F:46:A0:35:99:B1:24:ED:2A:0F:9C:4A:43:89:FC:51:0D:5F:9D:21:B7:2F:24:6C:5B
IdenTrust ECA 5 (Non-Issuing)	ECA	31:BE:68:EC:90:22:7E:4D:30:42:F6:3C:07:6B:1F:65:18:34:A7:DB:43:C5:AA:08:1D:B3:8F:B7:2C:31:A9:7E

Name	Program	Certificate Thumbprint (sha256)
IdenTrust S21 Component	ECA	FE:FD:B6:CD:C9:FC:B7:8F:CD:E7:BF:A1:E9:B9:07:77:75:12:A4:D5:E2:20:78:A8:29:81:AE:BC:14:39:CD:EF
IdenTrust S21 (Human)	ECA	AE:DD:A8:9E:0C:65:F6:B9:AA:8F:76:BD:76:08:5A:F6:E4:AD:25:D2:98:99:F5:35:64:46:09:40:19:DC:25:04