REPORT OF INDEPENDENT CERTIFIED PUBLIC ACCOUNTANTS

To the Management of IdenTrust Services, LLC:

We have examined the assertion by the management of IdenTrust Services, LLC ("IdenTrust") that in providing its TrustID, Access Certificates for Electronic Services (ACES), Trust Network, IdenTrust Global Common (IGC), Trust Infrastructure, and Department of Defense External Certification Authority (DOD ECA) 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, IdenTrust has:

- Disclosed its business, key life cycle management, certificate life cycle management, and CA environmental control policies and practices as follows:

Trust ID	Certificate Policy Certification Practices Statement Privacy Policy
Access Certificates for Electronic Services (ACES)	Certificate Policy Certification Practice Statement Privacy Policy
Trust Network	Certificate Policy* Certification Practice Statement* Privacy Policy
IdenTrust Global Common (IGC)	Certificate Policy Certification Practice Statement Privacy Policy
Trust Infrastructure	Certificate Policy** Certification Practice Statement** Privacy Policy
Department of Defense External Certification Authority (DOD ECA)	Certificate Policy Certification Practice Statement Key Recovery Policy Key Recovery Practice Statement Privacy Policy

* Documentation distribution is limited to IdenTrust Trust Network Participants, subscribers, and relying parties.

** Document is available to subscribers and relying parties upon request.

- Maintained effective controls to provide reasonable assurance that:
    - IdenTrust's Certification Practice Statements are consistent with its Certificate Policies; and
    - IdenTrust provides its services in accordance with its Certificate Policies and Certification Practice Statements;
- Maintained effective controls to provide reasonable assurance that:
    - The integrity of keys and certificates it manages is established and protected throughout their life cycles;
    - The Subscriber information is properly authenticated (for the registration activities performed by IdenTrust); 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 AICPA/CPA Canada Trust Services Principles and Criteria for Certification Authorities Version 2.0 ("WebTrust for Certification Authorities Principles and Criteria").

IdenTrust's 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 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.

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.

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, 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.

In our opinion, for the period July 1, 2017, to June 30, 2018, IdenTrust's management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, based on the AICPA/CPA Canada WebTrust for Certification Authorities Principles and Criteria.

This report does not include any representation as to the quality of IdenTrust's services beyond those covered by the WebTrust for Certification Authorities Principles and Criteria, nor the suitability of any of IdenTrust's services for any customer's intended purpose.

The WebTrust seal of assurance for Certification Authorities on IdenTrust's Website 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

IdenTrust
part of HID Global

ASSERTION OF MANAGEMENT AS TO ITS DISCLOSURE OF ITS PRACTICES AND ITS CONTROLS OVER ITS CERTIFICATION AUTHORITY OPERATIONS DURING THE PERIOD FROM JULY 1, 2017, TO JUNE 30, 2018

July 31, 2018

IdenTrust Services, LLC (IdenTrust) operates as a Certification Authority (CA) for its programs known as TrustID, Access Certificates for Electronic Services (ACES), Trust Network, IdenTrust Global Common (IGC), Trust Infrastructure, and Department of Defense External Certification Authority (DOD ECA), for its root and subordinate CA certificates as listed in Appendix A. IdenTrust provides the following Certification Authority services:

- Subscriber key management services
- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution (using online repository)
- Certificate revocation
- Certificate suspension
- Certificate status information processing (using online repository)
- Integrated circuit card life cycle management

IdenTrust makes use of external registration authorities for specific subscriber registration activities as disclosed in IdenTrust's business practice disclosures.

Management of IdenTrust is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosures as follows:

Trust ID	Certificate Policy Certification Practice Statement Privacy Policy
Access Certificates for Electronic Services (ACES)	Certificate Policy Certification Practices Statement Privacy Policy
Trust Network	Certificate Policy* Certification Practice Statement* Privacy Policy

IdenTrust Global Common (IGC)	Certificate Policy Certification Practice Statement Privacy Policy
Trust Infrastructure	Certificate Policy** Certification Practice Statement** Privacy Policy
Department of Defense External Certification Authority (DOD ECA)	Certificate Policy Certification Practice Statement Key Recovery Policy Key Recovery Practice Statement Privacy Policy

* Documentation distribution is limited to IdenTrust Trust Network Participants, subscribers, and relying parties.

** Document is available to subscribers and relying parties upon request.

Management of IdenTrust is also responsible for establishing and maintaining effective controls over its Certification Authority operations, including service integrity (including key and certificate life cycle management controls), and CA environmental 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 provide only reasonable assurance with respect to IdenTrust's Certification Authority operations. Furthermore because of changes in conditions, the effectiveness of controls may vary over time.

Management has assessed the controls over its CA operations. Based on that assessment, in IdenTrust management's opinion, in providing its CA services at its primary and secondary locations, IdenTrust, during the period from July 1, 2017, to June 30, 2018:

- Disclosed its key and certificate life cycle management business and information privacy practices in its
  - Certification Practice Statements; and
  - Certificate Policies;
- Maintained effective controls to provide reasonable assurance that:
  - IdenTrust's Certification Practice Statements are consistent with its Certificate Policies; and
  - IdenTrust provides its services in accordance with its Certificate Policies and Certification Practice Statements;
- Maintained effective controls to provide reasonable assurance that
  - The integrity of keys and certificates it manages is established and protected throughout their life cycles;
  - The integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles;

- The Subscriber information is properly authenticated (for the registration activities performed by IdenTrust); 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 life cycle management operations is maintained; and
  - CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity

in accordance with the AICPA/CPA Canada Trust Services Principles and Criteria for Certification Authorities Version 2.0 (WebTrust for Certification Authorities Principles and Criteria") including the following:

CA Business Practices Disclosure

- *CA Business Practices Management*
  - Certification Practice Statement Management
  - Certificate Policy Management
  - CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- Systems Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

Service Integrity

- *Key Life Cycle Management Controls*
  - CA Key Generation
  - CA Key Storage, Backup, and Recovery
  - Public Key Distribution
  - Key Usage
  - Key Archival and Destruction[1]

[1] IdenTrust prohibits the archiving of CA private keys

- CA Key Compromise
- CA Cryptographic Hardware Life Cycle Management
- CA Key Escrow (not supported)[2]

- *Subscriber Key Lifecycle Management Controls*
  - CA-Provided Subscriber Key Generation Services (not supported)
  - CA-Provider Subscriber Key Storage and Recovery Services (not supported)
  - Integrated Circuit Card (ICC) Life Cycle Management (not supported)
  - Requirements for Subscriber Key Management (not supported)

- *Certificate Life Cycle Management Controls*
  - Subscriber Registration
  - Certificate Renewal
  - Certificate Rekey (not supported)
  - Certificate Issuance
  - Certificate Distribution (using an online certificate management system)
  - Certificate Revocation
  - Certificate Suspension (for all programs except ECA)
  - Certificate Validation

- *Subordinate CA Certificate Life Cycle Management Controls*
  - Subordinate CA Certificate Life Cycle Management

Donald S. Johnson
Chief Information Officer

[2] IdenTrust does not escrow CA private signing keys

APPENDIX A – IDENTRUST ROOT AND ISSUING CAs

Root CA	SubCA	SHA256 Fingerprint
IdenTrust Commercial Root CA1		5d56499be4d2e08bcfcad08a3e38723d50503bde706948e42f55603019e528ae
	TrustID CA A1	24a1e02228bf0371be1f3587c4fc2656ee25fb0d40ddd97986bf47d46180bb75
	TrustID CA A12	5ae464bd2f83901fc33ef2b50cd880f5118c8dbeb1eb4a4e94b2fb05128805c2
	TrustID Server CA A52	b39c4a4596d3191afa3b3d254d28e5c482fcd0d500e0a9337f99277cb8a2eef8
	BAH BA CA 01	dcca716167f029aa9a309ee8ca3ff1f4017d1a1f3d1981bdff9e5af3f503682a
IdenTrust Public Sector Root CA 1		30d0895a9a448a262091635522d1f52010b5867acae12c78ef958fd4f4389f2f
	IdenTrust ACES CA 2	c5480d7bff952d1be86178ff713f11f51cf74232ee5676fc5a170d4a6a6fe50a
DST Root CA X3		0687260331a72403d909f105e69bcf0d32e1bd2493ffc6d9206d11bcd6770739