

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 the following Certification Authority (CA) services at its primary and secondary locations for its root CAs:

- DST ACES CA X6
- DST Root CA X3
- IdenTrust Public Sector Root CA 1
- IdenTrust Global Common Root CA 1
- IdenTrust Commercial Root CA 1
- IdenTrust Root Certification Authority (SHA1)
- IdenTrust Root Certification Authority (SHA2)
- and associated subordinate CAs

for the 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) at its primary and secondary locations during the period from July 1, 2015, to June 30, 2016, management of IdenTrust has:

- Disclosed its business, key life cycle management, certificate life cycle management, and CA environmental control policies and practices in its
 - Certification Practice Statements (CPS) and/or
 - Certificate Policies (CP);
- 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

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").

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.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and accordingly, included (1) obtaining an understanding of IdenTrust's key and certificate life cycle management business practices and its controls over key and certificate integrity, over the authenticity and privacy of subscriber and relying party information, over the continuity of key and certificate life cycle management operations, and over development, maintenance and operation of systems integrity; (2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business and information privacy practices; (3) testing and evaluating the operating effectiveness of the controls; and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

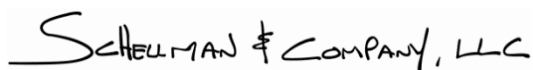
In our opinion, for the period July 1, 2015, to June 30, 2016, IdenTrust's management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, based on the [AICPA/CPA Canada WebTrust for Certification Authorities Principles and Criteria](#).

Because of inherent limitations in controls, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.

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.

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.

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.



Schellman & Company, LLC
Certified Public Accountants
Tampa, Florida
August 19, 2016

ASSERTION OF MANAGEMENT AS TO ITS DISCLOSURE OF ITS PRACTICES AND ITS CONTROLS OVER ITS CERTIFICATION AUTHORITY OPERATIONS DURING THE PERIOD FROM JULY 1, 2015, TO JUNE 30, 2016

August 19, 2016

IdenTrust Services, LLC (IdenTrust) operates as a Certification Authority (CA) for its CAs as the following:

- DST ACES CA X6
- DST Root CA X3
- IdenTrust Public Sector Root CA 1
- IdenTrust Global Common Root CA 1
- IdenTrust Commercial Root CA 1
- IdenTrust Root Certification Authority (SHA1)
- IdenTrust Root Certification Authority (SHA2)
- and associated subordinate CAs

for the 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). 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 Certificate Practice Statement Privacy Policy
----------	--

Access Certificates for Electronic Services (ACES)	Certificate Policy Certification Practice Statement Addendum to Certification Practice Statement Privacy Policy
Trust Network	Certificate Policy* Certification Practice Statement* Privacy Policy
IdenTrust Global Common (IGC)	Certificate Policy Certificate 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, 2015, to June 30, 2016:

- 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 Destruction¹
- 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 (ACES only)
 - Certificate Validation

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



Donald S. Johnson
Chief Information Officer

¹ IdenTrust prohibits the archiving of CA private keys

² IdenTrust does not escrow CA private signing keys