# 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, 2018, to June 30, 2019, for its root and subordinate CA certificates as listed in Appendix A, IdenTrust has:

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

| | |
|---|---|
| Trust ID | Certificate Policy v4.3<br>Certification Practices Statement v4.3<br>Privacy Policy |
| ACES | Certificate Policy v3.2<br>Certification Practices Statement v5.5<br>Privacy Policy |
| Trust Network | Certificate Policy*<br>Certification Practices Statement*<br>Privacy Policy |
| IGC | Certificate Policy v1.4.8<br>Certification Practices Statement v1.4.9<br>Privacy Policy |
| Trust Infrastructure | Certificate Policy**<br>Certification Practices Statement**<br>Privacy Policy |
| DOD ECA | Certificate Policy v4.4<br>Certification Practices Statement v2.1<br>Key Recovery Policy v1.0<br>Key Recovery Practice Statement v1.2<br>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 lifecycles;
  - 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 WebTrust Principles and Criteria for Certification Authorities Version 2.1.

*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.

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. Our examination did not extend to controls at external registration authorities, individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

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.

*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.

*Opinion*

In our opinion, 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 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 for Certification Authorities seal 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
November 4, 2019

# ASSERTION OF MANAGEMENT AS TO ITS DISCLOSURE OF ITS PRACTICES AND ITS CONTROLS OVER ITS CERTIFICATION AUTHORITY OPERATIONS DURING THE PERIOD 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), Trust Network, IdenTrust Global Common (IGC), Trust Infrastructure, and Department of Defense External Certification Authority (DOD ECA), and provides the following Certification Authority services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution (using online repository)
- Certificate revocation
- Certificate suspension
- Certificate validation (using online repository)
- Subordinate CA and cross-certification

The 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 v4.3<br>Certification Practices Statement v4.3<br>Privacy Policy |
| ACES | Certificate Policy v3.2<br>Certification Practices Statement v5.5<br>Privacy Policy |
| Trust Network | Certificate Policy*<br>Certification Practices Statement*<br>Privacy Policy |
| IGC | Certificate Policy v1.4.8<br>Certification Practices Statement v1.4.9<br>Privacy Policy |
| Trust Infrastructure | Certificate Policy**<br>Certification Practices Statement**<br>Privacy Policy |

| | |
|---|---|
| DOD ECA | Certificate Policy v4.4<br>Certification Practices Statement v2.1<br>Key Recovery Policy v1.0<br>Key Recovery Practice Statement v1.2<br>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.

The management of IdenTrust is also responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices management, CA environmental controls, CA key lifecycle management controls, certificate lifecycle management controls, and subordinate CA and cross-certificate lifecycle management 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.

IdenTrust management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in IdenTrust management's opinion, in providing its CA services at its Salt Lake City, Utah, USA, and Centennial, Colorado, USA, locations, throughout the period July 1, 2018, to June 30, 2019, IdenTrust has:

- Disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - Certification Practice Statements (see table above for versions examined); and
  - Certificate Policies (see table above for versions examined);
- 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 lifecycles;
  - The integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - 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 lifecycle management operations is maintained; and
  - CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity

based on the WebTrust Principles and Criteria for Certification Authorities Version 2.1 including the following:

**CA Business Practices Disclosure**

- Certification Practice Statement
- Certificate Policy

**CA Business Practices Management**

- Certificate Policy Management
- Certification Practice Statement 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
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

**CA Key Lifecycle Management Controls**

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction[1]
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Escrow (not supported)
- CA Key Transportation (not supported)[2]
- CA Key Migration (not supported)

[1] IdenTrust prohibits the archiving of CA private keys
[2] IdenTrust does not escrow CA private signing keys

## Subscriber Key Lifecycle Controls

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

## Certificate Lifecycle 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 Validations

## Subordinate CA and Cross Certificate Lifecycle Management Controls

- Subordinate CA Certificate and Cross Certificate Lifecycle Management

Donald S. Johnson

Donald S. Johnson
Chief Information Officer
November 4, 2019

## APPENDIX A – IDENTRUST ROOT AND ISSUING CAs

| Root CA | SubCA | SHA256 Fingerprint |
|---|---|---|
| IdenTrust Commercial Root CA1 | | 5D56499BE4D2E08BCFCAD08A3E38723D50503BDE706948E42F55603019E528AE |
| | IdenTrust Commercial CA Root CA 1 | AAE38F67F0A626805928507B078D89D5598D760D17335927B46606ECDFA1B946 |
| | TrustID CA A12 | 5AE464BD2F83901FC33EF2B50CD880F5118C8DBEB1EB4A4E94B2FB05128805C2 |
| | TrustID Server CA A52 | B39C4A4596D3191AFA3B3D254D28E5C482FCD0D500E0A9337F99277CB8A2EEF8 |
| | Booz Allen Hamilton BA CA 01* | DCCA716167F029AA9A309EE8CA3FF1F4017D1A1F3D1981BDFF9E5AF3F503682A |
| | TrustID HID Enterprise CA 1 | 64EB21A8003655488E9620EDC2B217CBCD559253C453E735E552706695CE1878 |
| | TrustID SAIC Public E-mail Issuing CA | AD8D498C08DA249936BABCDDA07206C13C71E75D16BE3120BEA2D8E5720C0BB1 |
| 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 CA Root CA 1 | 91B18588225035BB2F231FEF7695E497B289934B65CB87CFC2212271EBECB58C |
| | IdenTrust Commercial CA 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.