IdenTrust™
part of HID Global

IdenTrust Services, LLC

WebTrust for Certification Authorities – SSL Baseline with Network Security Report

July 1, 2023, to June 30, 2024

Attestation and Compliance Services

schellman
Quality, above all.

TABLE OF CONTENTS

Section I

Independent Accountant Report

REPORT OF THE INDEPENDENT ACCOUNTANT

To the Management of IdenTrust Services, LLC ("IdenTrust"):

Scope

We have examined IdenTrust management's assertion that for its TrustID and Department of Defense External Certification Authority (DoD ECA) Certification Authority ("CA") operations at its Salt Lake City, Utah, USA, and Centennial, Colorado, USA, locations, for its CAs as enumerated in Appendix A, IdenTrust has:

- Disclosed its SSL certificate lifecycle management business practices in its certification practice statements (CPS) and certificate policies (CP) as follows:

Trust ID	Certificate Policy (v 4.8.5, 4.8.6, 4.8.7, 4.9.0) Certification Practices Statement (v 4.8.5, 4.8.6, 4.8.7, 4.8.8, 4.8.9, 4.9.0) Privacy Policy
DOD ECA	Certificate Policy (v4.5) Certification Practices Statement (v2.3) Key Recovery Policy v1.0 Key Recovery Practices Statement v1.2 Privacy Policy

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the IdenTrust website and provide such services in accordance with its disclosed practices.

- Maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL Subscriber information is properly authenticated (for the registration activities performed by IdenTrust).
- 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.
- Maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum.

throughout the period July 1, 2023, through June 30, 2024, based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – v2.7.

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

Certification Authority's Responsibilities

IdenTrust's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – v2.7.

Practitioner's Responsibilities

Our responsibility is to express an opinion on IdenTrust management's assertion based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

- obtaining an understanding of IdenTrust's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of IdenTrust's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
- selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management business practices;
- testing and evaluating the operating effectiveness of the controls; and
- performing such other procedures as we considered necessary in the circumstances.

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.

We are required to be independent and to meet our other ethical responsibilities in accordance with the Code of Professional Conduct Established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

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

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Opinion

In our opinion, IdenTrust 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.

Other Matters

Without modifying our opinion, we noted the following other matters during our procedures:

Matter Topic		Matter Description
1	Certificate with Missing Details Flagged by OCSP Watch	IdenTrust disclosed in Bugzilla #1838315 that on June 7, 2023, a system outage caused the issuance of a pre-certificate without a serial number, flagged by the SSLMate OCSP Watch monitoring tool. IdenTrust traced the problem to a hardware malfunction and implemented a code revision to prevent recurrence on 9/30/2023. While this issue was resolved during the current audit period, it was disclosed during the previous audit period.
2	basicConstraints not flagged "Critical" Per Certificate Practice Statement	IdenTrust disclosed in Bugzilla #1850807 that it discovered some EV TLS certificates had the 'basicConstraints' extensions present, but not marked as critical, as specified in the IdenTrust TrustID CPS.
3	Delay Beyond 5 Days in Revoking Misissued Certificates	IdenTrust disclosed in Bugzilla #1851710 that during the review process for revoking certificates related to Bugzilla #1850807, it was determined that the effected certificates belonged to an enterprise customer, and promptly revoking these certificates, as expected by the Baseline Requirements, would have caused significant operational disruption and harm to those enterprise customers and their end users. This potential harm outweighed the risks of delaying revocation to allow for a more timely and orderly process.
4	Temporarily Expired CRLs	IdenTrust disclosed in Bugzilla #1853447 that four (4) CRLs were found to have been expired. Investigation found that a job-control utility had failed because a major customer was revoking a large number of certificates during the time the utility was attempting to create the new CRL, causing confusion in the system and resulting in a CRL generation shutdown where the CRLs expired before their replacements were available.
5	Expired ICAs CRLs	IdenTrust disclosed in Bugzilla #1854465 that it noticed an IdenTrust ICA was being flagged in CRL Watch, which is a potential violation of Section 4.10.2 of the CA/B Forum Baseline Requirements regarding Service Availability.
6	Expired CRL Served	IdenTrust disclosed in Bugzilla #1870402 that on December 6, 2023, alerts highlighted a failure in the regular CRL checking process. Subsequent examination uncovered that 26 CRLs had expired, spanning a duration of 81-119 minutes. This constituted a breach of the TLS BR Section 4.10.2 regarding 24x7 CRL repositories.
7	Test Certificates Inadvertently Published in Production Environment	IdenTrust disclosed in Bugzilla #1876871 that it identified some test S/MIME and TLS test certificates that were mistakenly issued in the CA production environment instead of the designated CA test environment, bypassing CA/B Forum BRs vetting process. All uncovered certificates were either expired or were revoked within minutes of issuance. The issue was caused by an IdenTrust QA team member who had mistakenly published test scripts for automated processes in the production environment.
8	Temporary Errors in Test Web Pages	IdenTrust disclosed in Bugzilla #1883792 that certificates on its Test Web Pages for the IdenTrust Public Sector room had temporary errors. This was a violation of Baseline Requirements section 2.2 which requires CAs to host test web pages that allow software suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate.

Matter Topic		Matter Description
9	Unintended Creation of a Root CA Certificate	IdenTrust disclosed in Bugzilla #1895006 that on April 30, 2024, during a key generation ceremony for a new Subordinate CA, the execution of a wrong command resulted in the generation of a new Self-Signed Root CA instead of the intended Subordinate CA.
10	TLS ICA with User Notice in Policy Qualifier	IdenTrust disclosed in Bugzilla #1897569 that due to the ‘Unintended creation of a Root CA certificate’ disclosure in Bugzilla #1895006, community comments highlighted that the properly issued Subordinate CA ‘TrustID Enterprise CA 3’ had a ‘User Notice policy qualifier’ in the certificate Policies extension which is not allowed per the TLS Baseline Requirements.

During our assessment, Schellman performed testing of certificate issuance, on a sample basis, and noted that there were no certificate deficiencies identified in any of the samples tested. As a result, our opinion is not modified with respect to these matters.

While IdenTrust disclosed its reported issues in Bugzilla during the period July 1, 2023, to June 30, 2024, we have noted only those disclosures relevant to the CAs enumerated in Appendix A and applicable to the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – v2.7.

Use of the WebTrust Seal

IdenTrust’s use of the WebTrust 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
Columbus, Ohio, USA
August 27, 2024

SECTION 2

MANAGEMENT'S ASSERTION

Management's Assertion

IdenTrust Services, LLC ("IdenTrust") operates the Certification Authority ("CA") services known as TrustID and Department of Defense External Certification Authority (DoD ECA), for its CA certificates as enumerated in Appendix A, and provides SSL CA services.

The management of IdenTrust is responsible for establishing and maintaining effective controls over its SSL CA operations, including its network and certificate security system controls, its SSL CA business practices disclosure on its website, SSL key lifecycle management controls, and SSL 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 only provide reasonable assurance with respect to IdenTrust's CA 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 SSL CA services. Based on that assessment, in providing its SSL Certificate Authority ("CA") services at its Salt Lake City, Utah, USA, and Centennial, Colorado, USA, locations, IdenTrust has:

- Disclosed its SSL certificate lifecycle management business practices in its certification practice statements (CPS) and certificate policies (CP) as follows:

Trust ID	Certificate Policy (v 4.8.5, 4.8.6, 4.8.7, 4.9.0) Certification Practices Statement (v 4.8.5, 4.8.6, 4.8.7, 4.8.8, 4.8.9, 4.9.0) Privacy Policy
DOD ECA	Certificate Policy (v4.5, 4.6, 4.7[1]) Certification Practices Statement (v2.3, 2.4[2]) Key Recovery Policy v1.0 Key Recovery Practices Statement v1.2 Privacy Policy

[1] *Certificate Policy v4.7 was published late in the audit period. IdenTrust has not yet prepared a corresponding CPS for United States DoD ECA approval, nor had it received United Stated DoD ECA response for the CPS submitted in early 2023 for the previous version of the CP.*

[2] *Document was approved by the IdenTrust PMA on April 24, 2023, and is pending approval from the United States DoD ECA prior to being posted to the IdenTrust website.*

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the IdenTrust website and provided such services in accordance with its disclosed practices.

- Maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL Subscriber information is properly authenticated (for the registration activities performed by IdenTrust).
- 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.

- Maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum.

throughout the period July 1, 2023, to June 30, 2024, based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – v2.7.

IdenTrust has disclosed the following matters publicly on Mozilla's Bugzilla platform. These matters were included below due to being open during the period July 1, 2023, to June 30, 2024.

Bug ID	Summary	Opened	Closed	Resolution
1838315	Certificate with Missing Details Flagged by OCSP Watch	6/13/2023	10/12/2023	Resolved Fixed
1850807	basicConstraints not flagged "Critical" Per Certificate Practice Statement	8/30/2023	9/29/2023	Resolved Fixed
1851710	Delay Beyond 5 Days in Revoking Misissued Certificates	9/5/2023	1/4/2024	Resolved Fixed
1853447	Temporarily Expired CRLs	9/15/2023	10/12/203	Resolved Fixed
1854465	Expired ICAs CRLs	9/21/2023	11/2/2023	Resolved Fixed
1870402	Expired CRL Served	12/15/2023	1/24/2024	Resolved Fixed
1876871	Test Certificates Inadvertently Published in Production Environment	1/26/2024	3/15/2024	Resolved Fixed
1883792	Temporary Errors in Test Web Pages	3/5/2024	3/27/2024	Resolved Fixed
1895006	Unintended Creation of a Root CA Certificate	5/3/2024	Open	Assigned
1897569	TLS ICA with User Notice in Policy Qualifier	5/17/2025	Open	Assigned

Donald S. Johnson

Donald S. Johnson
Chief Information Officer
IdenTrust Services, LLC
August 27, 2024

Appendix A

IdenTrust's Root and Issuing CAs

IdenTrust's Root and Issuing CAs

Root CA	SubCA	SHA256 Fingerprint
IdenTrust Commercial Root CA 1		5D56499BE4D2E08BCFCAD08A3E38723D50503BDE706948E42F55603019E528AE
	TrustID Server CA O1	6BAAB0C433D779FD6A4B6D56D6304D5E6EA5DE689FE35A43038A4028F345DF60
	TrustID Server CA E1	743E328F329E194DA252711BF6BFF00CF63B6A4C0AA66B2E1967716910678971
	Booz Allen Hamilton BA CA 01[1]	DCCA716167F029AA9A309EE8CA3FF1F4017D1A1F3D1981BDFF9E5AF3F503682A
	HydrantID Server CA O1	8BB2F6883FED289A521BA27C478482950874E143CACCEC6FC025990C0C46813E
IdenTrust Public Sector Root CA 1		30D0895A9A448A262091635522D1F52010B5867ACAE12C78EF958FD4F4389F2F
	IdenTrust Public Sector Server CA 1	288B35466FB8E228B98832019E1A7956AC3E9F154280CC97486ECC8E2C9CABC1
DST Root CA X3[2]		0687260331A72403D909F105E69BCF0D32E1BD2493FFC6D9206D11BCD6770739
	IdenTrust Commercial Root CA 1	1766FE28F034150CDB62B4469531E4D76FBF3A1EC9684CAB3767C3021AB67E50
	ISRG Root X1	6D99FB265EB1C5B3744765FCBC648F3CD8E1BFFAFDC4C2F99B9D47CF7FF1C24F

[1] The Booz Allen Hamilton (BAH) subordinate CA certificate was signed with a key solely controlled by IdenTrust, and the certificate is subject to the TrustID CP/CPS. Although the subscriber certificates under this subordinate CA 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 on certificates issued by any external registration authorities.

[2] The cross-signed certificates were signed with a key controlled by IdenTrust, and the certificates are subject to the TrustID CP/CPS. The cross-signed certificates are controlled by IdenTrust.