



IDENTRUST SERVICES, LLC

SECURE E-MAIL (S/MIME) REPORT

JULY 1, 2023, TO JUNE 30, 2024

Attestation and Compliance Services



Proprietary & Confidential

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

SECTION 1	INDEPENDENT ACCOUNTANT'S REPORT	1
SECTION 2	MANAGEMENT'S ASSERTION	6
APPENDIX A	IDENTrust's ROOT AND ISSUING CAS.....	9

SECTION 1

INDEPENDENT ACCOUNTANT'S REPORT

REPORT OF THE INDEPENDENT ACCOUNTANT

To the Management of IdenTrust Services, LLC (“IdenTrust”):

We have examined IdenTrust management’s assertion that for its S/MIME Certification Authority (CA) operations at its Salt Lake City, Utah, USA, and Centennial, Colorado, USA, locations, for its CAs as enumerated in Attachment A, IdenTrust has:

- disclosed its S/MIME certificate lifecycle management business practices in its certificate practices 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
IGC	Certificate Policy (v 1.5.6, 1.5.7, 1.5.8) Certification Practices Statement (v1.5.6, 1.5.7, 1.5.8, 1.5.9) Privacy Policy

including its commitment to provide S/MIME 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 S/MIME certificates it manages is established and protected throughout their lifecycles; and
 - S/MIME 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 that are incorporated by reference.

throughout the period July 1, 2023, to June 30, 2024, based on the [WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.0.0](#).

Certification Authority’s Responsibilities

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 – S/MIME Certificates v1.0.0.

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. 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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 S/MIME 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	Temporarily Expired CRLs	IdenTrust disclosed in Bugzilla #1853447 that four (4) CRLs were found to have 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.

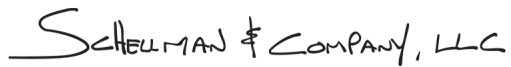
Matter Topic		Matter Description
2	S/MIME Certificates Issued in Violation of New S/MIME Baseline Requirements v1.0	IdenTrust disclosed in Bugzilla #1853783 that it discovered that 114 S/MIME certificates had been issued after September 1, 2023, in violation of the certificate details specified in CA/B Forum S/MIME Baseline Requirements version 1.0, which had come into effect on that day.
3	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.
4	S/MIME Certificates with Invalid Document Identification Schemes	IdenTrust disclosed in Bugzilla #1861782 that the customer support team confirmed that customers retrieving S/MIME Mailbox-Validated certificates were encountering errors due to missing individual identity details. This was caused by a software release aimed at capturing individual identity validation for S/MIME certificates mistakenly affected S/MIME Mailbox-Validation certificates.
5	S/MIME Certificates Issued Without CAB Forum OID 2023-1020	IdenTrust disclosed in Bugzilla #1861783 that while inspecting Enterprise certificates, it discovered having S/MIME certificates that were lacking the anticipated CA/B Forum OID expected after August 31, 2023. This was caused by not disabling API access to issue these S/MIME certificates by four (4) enterprise customers who were migrated to a different certificate program.
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	Invalid Organization Identifier in S/MIME Certificates	IdenTrust disclosed in Bugzilla #1900492 that while testing a new PKI linting tool for S/MIME certificates, it discovered an active S/MIME certificate with an invalid Organization Identifier scheme for GOVUS entities. This was due to an invalid validation scheme in the in-house application code.

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 – S/MIME Certificates v1.0.0.

Use of the WebTrust Seal

IdenTrust's use of the WebTrust for Certification Authorities – S/MIME Certificates 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.

A handwritten signature in black ink that reads "SCHILLMAN & COMPANY, LLC". The signature is written in a cursive, slightly stylized font.

Schellman & Company, LLC
Columbus, Ohio
August 27, 2024

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT’S ASSERTION

IdenTrust Services, LLC (“IdenTrust”) operates the Certification Authority (“CA”) services known as TrustID, Department of Defense External Certification Authority (DoD ECA), and IdenTrust Global Common (IGC) for its CA certificates as enumerated in Appendix A, and provides S/MIME CA services.

The management of IdenTrust is responsible for establishing and maintaining effective controls over its S/MIME CA operations, including its network and certificate security system controls, its S/MIME CA business practices disclosure on its website, S/MIME key lifecycle management controls, and S/MIME 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 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 S/MIME CA services. Based on that assessment, in providing its S/MIME Certification Authority (CA) services at its Salt Lake City, Utah, USA, and Centennial, Colorado, USA, locations, IdenTrust has:

- disclosed its S/MIME certificate lifecycle management business practices in its certificate practices statements (CPS) and certificate policies (CP) as follows:

Trust ID	Certificate Policy (v4.8.5, 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
IGC	Certificate Policy (v1.5.6, 1.5.7, 1.5.8) Certification Practices Statement (v1.5.6, 1.5.7, 1.5.8, 1.5.9) Privacy Policy


including its commitment to provide S/MIME 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 S/MIME certificates it manages is established and protected throughout their lifecycles; and
 - S/MIME 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 that are incorporated by reference.

throughout the period July 1, 2023, to June 30, 2024, based on the [WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.0.0](#).

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
1853447	Temporarily Expired CRLs	9/15/2023	10/12/2023	Resolved Fixed
1853783	S/MIME Certificates Issued in Violation of New S/MIME Baseline Requirements v1.0	9/18/2023	1/26/2024	Resolved Fixed
1854465	Expired ICAs CRLs	9/21/2023	11/2/2023	Resolved Fixed
1861782	S/MIME Certificates with Invalid Document Identification Schemes	10/27/2023	1/4/2024	Resolved Fixed
1861783	S/MIME Certificates Issued Without CAB Forum OID	10/27/2023	1/4/2024	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
1900492	Invalid Organization Identifier in S/MIME Certificates	6/3/2024	6/21/2024	Resolved Fixed



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 CA A13	76921EDB7FE5553B0CE9DD4388C8416629EBC0ED0A1A399415AAD5C050E950A0
	TrustID CA A14	7A95A827D6A13C7C191A893D2987E4134ACB403EC9E26E8CD92525A806D794C6
	TrustID HID Enterprise CA 1	64EB21A8003655488E9620EDC2B217CBCD559253C453E735E552706695CE1878
	TrustID HID Enterprise CA 2	AF0926CB0E3C5A37B76F30370583C3CD63BBEC2B33CC8459849CA69D4F9C7CDE
	TrustID SAIC Public E-mail Issuing CA	AD8D498C08DA249936BABCDDA07206C13C71E75D16BE3120BEA2D8E5720C0BB1
	TrustID SAIC Public E-mail Issuing CA 2	944586DADCE409FC51017EF473B9ADDA6EF7589F70B21430507FD245809B3BF9
	Booz Allen Hamilton BA CA 01 ^[1]	DCCA716167F029AA9A309EE8CA3FF1F4017D1A1F3D1981BDFF9E5AF3F503682A
	Booz Allen Hamilton BA CA 02 ^[1]	04787DADF6D09BEE0E5F76451B0D485A1DAE6F9091D8A781710ABAC3FBD980DA
IdenTrust Public Sector Root CA 1		30D0895A9A448A262091635522D1F52010B5867ACAE12C78EF958FD4F4389F2F
	IdenTrust Public Sector Server CA 1	288B35466FB8E228B98832019E1A7956AC3E9F154280CC97486ECC8E2C9CABC1

^[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.