IdenTrust™
part of HID Global

IdenTrust Services, LLC

WebTrust for Certification Authorities Report

July 1, 2023, to June 30, 2024

Attestation and Compliance Services

schellman
Quality, above all.

Table of Contents

Section I

Independent Accountant's 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, Trust Network, IdenTrust Global Common (IGC), Trust Infrastructure, 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 business, key and certificate lifecycle management, and CA environmental control practices within its certification 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
Trust Network	Certificate Policy v3.1a[1] Certification Practices Statement v3.1a[1] 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
Trust Infrastructure	Certificate Policy v3.1a[2] Certification Practices Statement v3.1a[2] Privacy Policy
DOD ECA	Certificate Policy (v4.5, 4.6, 4.7[3]) Certification Practices Statement (v2.3, 2.4[4]) Key Recovery Policy v1.0 Key Recovery Practices Statement v1.2 Privacy Policy

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

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

[3] *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.*

[4] *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.*

- maintained effective controls to provide reasonable assurance that:
  - IdenTrust's CPSs are consistent with its CPs; and
  - IdenTrust provides its services in accordance with its CPs and CPSs.

- 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 management operations is maintained; and
    - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity.

throughout the period July 1, 2023, through June 30, 2024, based on the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

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

IdenTrust does not escrow its keys, does not perform key transportation or key migration services, does not provide subscriber key generation services, does not provide certificate rekey services other than as part of certificate renewal or replacement, does not provide certificate suspension services for the ECA services, does not provide CA-provided subscriber key generation services, does not provide CA-provided subscriber key storage and recovery services, does not provide Integrated Circuit Card (ICC) lifecycle management, and does not provide subscriber key management. Accordingly, our examination did not extend to controls that would address those criteria.

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 v2.2.2.

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 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 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 TrustID, Trust Network, IdenTrust Global Common (IGC), Trust Infrastructure, and Department of Defense External Certification Authority (DOD ECA) Certification Authority 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 examination:

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 affected 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 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
5	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.
6	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.
7	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 affecting S/MIME Mailbox-Validation certificates.
8	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.
9	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.
10	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.
11	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.
12	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.
13	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.
14	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.

Matter Topic		Matter Description
15	Unauthorized OCSP Response on a Timestamp Certificate	IdenTrust disclosed in Bugzilla #1905446 seeing a certificate flagged with an “unauthorized” OCSP response error in SSLmate’s OCSP watch in violation of the CPS Section 9.6.1 which requires IdenTrust to maintain an online 24x7 publicly accessible repository of all unexpired certificates.

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 v2.2.2.

Use of the WebTrust Seal

IdenTrust’s use of the WebTrust for Certification Authorities 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
August 27, 2024

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

IdenTrust Services, LLC ("IdenTrust") operates the Certification Authority ("CA") services known as TrustID, Trust Network, IdenTrust Global Common (IGC), Trust Infrastructure, and Department of Defense External Certification Authority (DOD ECA) Certification Authority ("CA"), for its CA certificates as enumerated in Appendix A, and provides the following CA 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 its CA business practices disclosures on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA 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 CA services. Based on that assessment, in IdenTrust's management's opinion, in providing its CA services at its Salt Lake City, Utah, USA, and Centennial, Colorado, USA, locations, IdenTrust has:

- disclosed its business, key and certificate lifecycle management, and CA environmental control 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
Trust Network	Certificate Policy v3.1a[1] Certification Practices Statement v3.1a[1] 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

Trust Infrastructure	Certificate Policy v3.1a[2] Certification Practices Statement v3.1a[2] Privacy Policy
DOD ECA	Certificate Policy (v4.5, 4.6, 4.7[3]) Certification Practices Statement (v2.3, 2.4[4]) Key Recovery Policy v1.0 Key Recovery Practices Statement v1.2 Privacy Policy

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

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

[3] *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.*

[4] *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.*

- maintained effective controls to provide reasonable assurance that:
  - IdenTrust's CPS is consistent with its CPs; and
  - IdenTrust provides its services in accordance with its CPs and CPSs.
- 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 management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity.

throughout the period July 1, 2023, through June 30, 2024, based on the WebTrust Principles and Criteria for Certification Authorities v2.2.2, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

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
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Issuance
- Certificate Distribution (using an online certificate management system)
- Certificate Revocation
- Certificate Suspension (for all programs except ECA)
- Certificate Validation

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate and Cross Certificate Lifecycle Management

IdenTrust does not escrow its keys, does not perform key transportation or key migration services, does not provide subscriber key generation services, does not provide certificate rekey services other than as part of certificate renewal or replacement, does not provide certificate suspension services for the ECA services, does not provide CA-provided subscriber key generation services, does not provide CA-provided subscriber key storage and recovery services, does not provide Integrated Circuit Card (ICC) lifecycle management, and does not provide subscriber key management. Accordingly, our assertion does not extend to controls that would address those criteria.

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	Dalay 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
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
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
1900492	Invalid Organization Identifier in S/MIME Certificates	6/3/2024	6/21/2024	Resolved Fixed
1905446	Unauthorized OCSP Response on a Timestamp Certificate	6/28/2024	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 CA A13	76921EDB7FE5553B0CE9DD4388C8416629EBC0ED0A1A399415AAD5C050E950A0
	TrustID CA A14	7A95A827D6A13C7C191A893D2987E4134ACB403EC9E26E8CD92525A806D794C6
	TrustID Server CA O1	6BAAB0C433D779FD6A4B6D56D6304D5E6EA5DE689FE35A43038A4028F345DF60
	TrustID Server CA E1	743E328F329E194DA252711BF6BFF00CF63B6A4C0AA66B2E1967716910678971
	TrustID Enterprise TLS CA 3	187E3D67BA087B9F9BEF3CD62145E7F9C2747AC362664E98CC55AC426A419028
	TrustID Enterprise TLS CA 3 (Self-Sign)	C46678B11AD9B8B9E46953C38E6F0E3E0C92479070C1512B8A155070E7E4E4FA
	TrustID EV Code Signing CA 3	BDC61A9F0607410E7132DE9825D5424CC4FFFFD28099B1081B2A273C74957FA4
	TrustID EV Code Signing CA 4	59AA2D256962125500C18E98014F54DFC47F815DDFC7715DAF81AA759699E431
	TrustID EV Code Signing CA 5	65D084D249B28C0CE34129263144D2B6836CDEC79060129A94C0B4618DBDB4D2
	TrustID Timestamping CA 3	0BF6948ED05F56038876F15F305E1038A5A38981C25FCCE8B68D985950D80495
	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
	HydrantID Server CA O1	8BB2F6883FED289A521BA27C478482950874E143CACCEC6FC025990C0C46813E
IdenTrust Public Sector Root CA 1		30D0895A9A448A262091635522D1F52010B5867ACAE12C78EF958FD4F4389F2F
	IdenTrust Public Sector Server CA 1	288B35466FB8E228B98832019E1A7956AC3E9F154280CC97486ECC8E2C9CABC1

Root CA	SubCA	SHA256 Fingerprint
DST Root CA X3 [2]		0687260331A72403D909F105E69BCF0D32E1BD2493FFC6D9206D11BCD6770739
	IdenTrust Commercial Root CA 1	1766FE28F034150CDB62B4469531E4D76FBF3A1EC9684CAB3767C3021AB67E50
	ISRG Root X1	6D99FB265EB1C5B3744765FCBC648F3CD8E1BFFAFDC4C2F99B9D47CF7FF1C24F
ECA Root CA 4		8FA30EA12E781DD5D715736C5AB6746CB13527899C909EB1436BB5D8A71A2BED
	IdenTrust ECA S22	87F627D2EED16D206E9CE3302BE2D28BEBD9D8AE43D0A4322CAEC9C436A86E96
	IdenTrust ECA S22C	C1B718CAF85E4535A07012D6F040B15B2AB3D719DC4D09F4A785E30868097FD8
	IdenTrust ECA S23	13564E34FEE6838BA9C5B042A5BF3F3FF4A80FDB67C74986E7FB306DDFA06479
	IdenTrust ECA Component S23C	DBF2107C25639FE95AE2468B4279C9C88BD780AA96470875F8D9C26A2427039B
IdenTrust Global Common Root CA 1		09B15AD8D0CA032861892E55E746AE8DAF1BFDB53A9E5AEE8137D6F89AA11113
	IGC CA 1	6AB50C761E3EE72C34DB75C2F106E03AF15E2D8E2F6A672EC8FF0966BFD42E78
	IGC Device CA 1	CC0AC905FF000B43AB6CE943EA40AD7DA67AAF1631186453AB44546ED744AAD2
	IGC Device CA 2	0603EA410E8613A217E35A06489C8F4316F36A6D3F75635BD425A2DAAEB187E
	Advanced Health Systems, Inc Direct CA 1	5579B0D3B2234CDDD1D31AE9BB646B6A193B8BAE9119326C8C832CE41C6F720D
	Advanced Health Systems, Inc Direct CA 2	6A85C579862C0ADDC77D348E7E12CCA800B3511496C5CD3CD8D02A21CE180D85
	Leidos FBCA Cloud PKI CA-1	AEAAE218BF167AB300A271F1D9D404113D67953E6A9957CCAA75E5A642594220
	SAIC FBCA Cloud PKI CA-1	5D6D6CD106AF14BB3DDC6185949963428341B331232AED56CB1FA8B823B5E51F

[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.