

## REPORT OF THE INDEPENDENT ACCOUNTANT

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

### Scope

We have examined IdenTrust Services, LLC’s (“IdenTrust”) [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 lifecycle management, certificate lifecycle management, and CA environmental control practices in its certification practice statements and certificate policies as follows:

Trust ID	<a href="#">Certificate Policy (v4.7.9, 4.8.0, 4.8.1, 4.8.2, 4.8.3)</a> <a href="#">Certification Practices Statement (v4.7.9, 4.8.0, 4.8.1, 4.8.2, 4.8.3)</a> <a href="#">Privacy Policy</a>
Trust Network	Certificate Policy v3.1a* Certification Practices Statement v3.1a* <a href="#">Privacy Policy</a>
IGC	<a href="#">Certificate Policy v1.5.5</a> <a href="#">Certification Practices Statement v1.5.5</a> <a href="#">Privacy Policy</a>
Trust Infrastructure	Certificate Policy v3.1a** Certification Practices Statement v3.1a** <a href="#">Privacy Policy</a>
DOD ECA	<a href="#">Certificate Policy v4.5</a> <a href="#">Certification Practices Statement v2.3</a> <a href="#">Key Recovery Policy v1.0</a> <a href="#">Key Recovery Practice Statement v1.2</a> <a href="#">Privacy Policy</a>

\* *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;
  - 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, 2021, to June 30, 2022, 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, certificate rekey services, certificate suspension services, CA-provided subscriber key generations services, CA-provided subscriber key storage and recovery services, Integrated Circuit Card (ICC) lifecycle management, and subscriber key management. Accordingly, our examination does not extend to controls that would address those criteria.

#### *Certification Authority's Responsibility*

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 Version 2.2.2.

#### *Practitioner's Responsibilities*

Our responsibility is to express an opinion on IdenTrust'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 judgement, 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.

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 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.

## *Emphasis of Matters*

IdenTrust has disclosed that during the period July 1, 2021, to June 30, 2022, the following incidents were identified and disclosed to the CA/B Forum community as follows:

- On October 6, 2021, IdenTrust discovered that intermittent interruptions of DNS service had occurred for the IdenTrust DST X3 CA Root that expired normally on September 30, 2021. IdenTrust began an investigation on October 6, 2021, and system engineers noted large volumes of network traffic directed at the IdenTrust network boundary, causing site connectivity to be intermittent. The result was slow response times and timeouts for customers attempting OCSP validations and other certificate lifecycle events for the expired certificate, in addition to requests for the new certificate chain and subsequent OCSP and other validation requests. Concurrently but outside of IdenTrust control, networks and systems worldwide had issues validating traffic and DNS, causing slow responses and timeouts that compounded issues for customers trying to access IdenTrust sites. IdenTrust rerouted validation requests to its disaster recovery site while it continued to troubleshoot the issue. IdenTrust additionally determined a secondary root cause was the CRLs used by the disaster recovery system had not been updated completely according to normal production protocol. New CRLs were pushed to the disaster recovery system the same day, and resolution was confirmed. On May 5, 2022, IdenTrust remediated this issue to avoid recurrence by implementing a Content Delivery Network (CDN) to help support and redistribute the high volume of traffic and correct the automated push for CRL distribution to the DR system.
- On February 23, 2022, IdenTrust conducted an internal review and discovered that there were 4,543 instances where a precertificate was generated but its status was not available in the OCSP responder. Through further investigation, IdenTrust discovered an additional 124 pre-certificates with the same issue. In all cases, precertificates were submitted to certificate transparency logs and the IdenTrust OCSP responders responded with "unauthorized" status. To resolve this issue, on March 14, 2022, IdenTrust registered all identified precertificates in the OCSP database, and confirmed a valid OCSP response for each precertificate. Additionally and to prevent recurrence, on May 23, 2022, IdenTrust updated the TLS issuance process to register each precertificate into the OCSP DB regardless of whether the final certificate is issued.
- On March 4, 2022, IdenTrust reported that during the process of enhancing Intermediate CA (ICA) monitoring, it discovered that the OCSP responder for the root CA 'IdenTrust Commercial Root CA 1', failed to provide status information for 3 valid ICA certificates (non-TLS issuers). The OCSP responder was returning "Unauthorized" status for these 3 ICAs: TrustID HID Enterprise CA 1, TrustID Code Signing CA 1, and TrustID EV Code Signing CA 3. On March 4, 2022, IdenTrust remediated this issue by updating the OCSP responder database with each ICA identified in this incident and verified the receipt of a valid OCSP response. In order to prevent recurrence, the ICA creation procedures were updated to include a post-configuration quality check for verifying receipt of a valid OCSP response for every new ICA. The OCSP responder monitors will be enhanced to test for a valid response for each ICA issued under root CAs subject to Baseline Requirements no later than September 30, 2022.
- On June 3, 2022, IdenTrust reported that during an internal review on May 23, 2022, it discovered that the OCSP response validity period for 14 subordinate CAs did not conform to the description in section 4.9.10 of the TrustID CPS version 4.8.2 published on May 12, 2022. IdenTrust corrected the discrepancy by updating section 4.9.10 of the TrustID CPS and re-publishing on May 27, 2022, as version 4.8.3.
- On June 22, 2022, IdenTrust reported that as a result of an internal self-audit on June 13, 2022, some CRLs for revoked TLS certificates may not have been published within one hour of authenticating a revocation request as required by Section 4.9.8 of the IdenTrust TrustID CPS due to a caching issue on the external load balancers. Between May 21, 2022, and June 13, 2022, 46 revoked TLS certificates may have experienced a greater than an hour delay in publishing the corresponding updated CRLs due to previously cached CRLs remaining persistent on the load balancers. IdenTrust determined that the issue was caused by a missing configuration item in the production load balancers. The configuration was present in the pre-production environment and therefore it was not detected during the testing phase. Upon update in the production environment on June 13, 2022, the issue was corrected.

Our opinion is not modified with respect to these matters. Incidents not relevant to the assessed criteria are included in Appendix B.

*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.

*S*SHELLMAN & COMPANY, LLC

Schellman & Company, LLC  
Certified Public Accountants  
Tampa, Florida  
August 22, 2022

## IDENTRUST MANAGEMENT'S ASSERTION

IdenTrust Services, LLC (IdenTrust) operates the CA services known as TrustID, Trust Network, IGC, Trust Infrastructure, and DOD ECA, 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 as follows:

TrustID	<a href="#">Certificate Policy (v4.7.9, 4.8.0, 4.8.1, 4.8.2, 4.8.3)</a> <a href="#">Certification Practices Statement (v4.7.9, 4.8.0, 4.8.1, 4.8.2, 4.8.3)</a> <a href="#">Privacy Policy</a>
Trust Network	Certificate Policy v3.1a* Certification Practices Statement v3.1a* <a href="#">Privacy Policy</a>
IGC	<a href="#">Certificate Policy v1.5.5</a> <a href="#">Certification Practices Statement v1.5.5</a> <a href="#">Privacy Policy</a>
Trust Infrastructure	Certificate Policy v3.1a** Certification Practices Statement v3.1a** <a href="#">Privacy Policy</a>
DOD ECA	<a href="#">Certificate Policy v4.5</a> <a href="#">Certification Practices Statement v2.3</a> <a href="#">Key Recovery Policy v1.0</a> <a href="#">Key Recovery Practice Statement v1.2</a> <a href="#">Privacy Policy</a>

\* 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 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 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, 2021, to June 30, 2022, 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 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, 2022, to June 30, 2022, 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<sup>1</sup>
- 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 Validations

### **Subordinate CA and Cross 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, certificate rekey services, certificate suspension services, CA-provided subscriber key generations services, CA-provided subscriber key storage and recovery services, Integrated Circuit Card (ICC) lifecycle management, and subscriber key management. Accordingly, our assertion does not extend to controls that would address those criteria.

IdenTrust has disclosed that during the period July 1, 2021, to June 30, 2022, the following incidents relevant to the assessed criteria were identified and disclosed to the CA/B Forum community as follows:

- On October 6, 2021, IdenTrust discovered that intermittent interruptions of DNS service had occurred for the IdenTrust DST X3 CA Root that expired normally on September 30, 2021. IdenTrust began an investigation on October 6, 2021, and system engineers noted large volumes of network traffic directed at the IdenTrust network boundary, causing site connectivity to be intermittent. The result was slow response times and timeouts for customers attempting OCSP validations and other certificate lifecycle events for the

---

<sup>1</sup> IdenTrust prohibits the archiving of CA private keys

expired certificate, in addition to requests for the new certificate chain and subsequent OCSP and other validation requests. Concurrently but outside of IdenTrust control, networks and systems worldwide had issues validating traffic and DNS, causing slow responses and timeouts that compounded issues for customers trying to access IdenTrust sites. IdenTrust rerouted validation requests to its disaster recovery site while it continued to troubleshoot the issue. IdenTrust additionally determined a secondary root cause was the CRLs used by the disaster recovery system had not been updated completely according to normal production protocol. New CRLs were pushed to the disaster recovery system the same day, and resolution was confirmed. On May 5, 2022, IdenTrust remediated this issue to avoid recurrence by implementing a Content Delivery Network (CDN) to help support and redistribute the high volume of traffic and correct the automated push for CRL distribution to the DR system.

- On February 23, 2022, IdenTrust conducted an internal review and discovered that there were 4,543 instances where a precertificate was generated but its status was not available in the OCSP responder. Through further investigation, IdenTrust discovered an additional 124 pre-certificates with the same issue. In all cases, precertificates were submitted to certificate transparency logs and the IdenTrust OCSP responders responded with "unauthorized" status. To resolve this issue, on March 14, 2022, IdenTrust registered all identified precertificates in the OCSP database, and confirmed a valid OCSP response for each precertificate. Additionally and to prevent recurrence, on May 23, 2022, IdenTrust updated the TLS issuance process to register each precertificate into the OCSP DB regardless of whether the final certificate is issued.
- On March 4, 2022, IdenTrust reported that during the process of enhancing Intermediate CA (ICA) monitoring, it discovered that the OCSP responder for the root CA 'IdenTrust Commercial Root CA 1', failed to provide status information for 3 valid ICA certificates (non-TLS issuers). The OCSP responder was returning "Unauthorized" status for these 3 ICAs: TrustID HID Enterprise CA 1, TrustID Code Signing CA 1, and TrustID EV Code Signing CA 3. On March 4, 2022, IdenTrust remediated this issue by updating the OCSP responder database with each ICA identified in this incident and verified the receipt of a valid OCSP response. In order to prevent recurrence, the ICA creation procedures were updated to include a post-configuration quality check for verifying receipt of a valid OCSP response for every new ICA. The OCSP responder monitors will be enhanced to test for a valid response for each ICA issued under root CAs subject to Baseline Requirements no later than September 30, 2022.
- On June 3, 2022, IdenTrust reported that during an internal review on May 23, 2022, it discovered that the OCSP response validity period for 14 subordinate CAs did not conform to the description in section 4.9.10 of the TrustID CPS version 4.8.2 published on May 12, 2022. IdenTrust corrected the discrepancy by updating section 4.9.10 of the TrustID CPS and re-publishing on May 27, 2022, as version 4.8.3.
- On June 22, 2022, IdenTrust reported that as a result of an internal self-audit on June 13, 2022, some CRLs for revoked TLS certificates may not have been published within one hour of authenticating a revocation request as required by Section 4.9.8 of the IdenTrust TrustID CPS due to a caching issue on the external load balancers. Between May 21, 2022, and June 13, 2022, 46 revoked TLS certificates may have experienced a greater than an hour delay in publishing the corresponding updated CRLs due to previously cached CRLs remaining persistent on the load balancers. IdenTrust determined that the issue was caused by a missing configuration item in the production load balancers. The configuration was present in the pre-production environment and therefore it was not detected during the testing phase. Upon update in the production environment on June 13, 2022, the issue was corrected.

Incidents not relevant to the assessed criteria are included in Appendix B.



---

Donald S. Johnson  
Chief Information Officer  
August 22, 2022

**APPENDIX A – IDENTRUST ROOT AND ISSUING CAs**

Root CA	SubCA	SHA256 Fingerprint
IdenTrust Commercial Root CA 1		5D56499BE4D2E08BCFCAD08A3E38723D50503BDE706948E42F55603019E528AE
	TrustID CA A12	5AE464BD2F83901FC33EF2B50CD880F5118C8DBEB1EB4A4E94B2FB05128805C2
	TrustID CA A13	76921EDB7FE5553B0CE9DD4388C8416629EBC0ED0A1A399415AAD5C050E950A0
	TrustID Server CA A52 (expired)	B39C4A4596D3191AFA3B3D254D28E5C482FCD0D500E0A9337F99277CB8A2EEF8
	TrustID Server CA O1	6BAAB0C433D779FD6A4B6D56D6304D5E6EA5DE689FE35A43038A4028F345DF60
	TrustID Server CA E1	743E328F329E194DA252711BF6BFF00CF63B6A4C0AA66B2E1967716910678971
	TrustID Code Signing CA 1 (revoked)	6917B2F8300036EE640CB867EA5D4E8356DC5586C8B5977C8C229C73CCB46DEF
	TrustID EV Code Signing CA 3	BDC61A9F0607410E7132DE9825D5424CC4FFFD28099B1081B2A273C74957FA4
	TrustID EV Code Signing CA 4	59AA2D256962125500C18E98014F54DFC47F815DDFC7715DAF81AA759699E431
	TrustID Timestamping CA 2 (revoked)	5F75F59394D23E4855C66566EED264806FD2859E3C6961BDC8A20D90FA3C46E4
	TrustID Timestamping CA 3	0BF6948ED05F56038876F15F305E1038A5A38981C25FCCE8B68D985950D80495
	TrustID HID Enterprise CA 1	64EB21A8003655488E9620EDC2B217CBCD559253C453E735E552706695CE1878
	TrustID SAIC Public Email Issuing CA	AD8D498C08DA249936BABCDDA07206C13C71E75D16BE3120BEA2D8E5720C0BB1
Booz Allen Hamilton BA CA 01*	DCCA716167F029AA9A309EE8CA3FF1F4017D1A1F3D1981BDFF9E5AF3F503682A	
HydrantID Server CA O1	8BB2F6883FED289A521BA27C478482950874E143CACCEC6FC025990C0C46813E	
IdenTrust Public Sector Root CA 1		30D0895A9A448A262091635522D1F52010B5867ACAE12C78EF958FD4F4389F2F
	IdenTrust Public Sector Server CA 1	288B35466FB8E228B98832019E1A7956AC3E9F154280CC97486ECC8E2C9CABC1
DST Root CA X3 (expired)		0687260331A72403D909F105E69BCF0D32E1BD2493FFC6D9206D11BCD6770739
	IdenTrust Commercial Root CA 1 (cross-signed)**	1766FE28F034150CDB62B4469531E4D76FBF3A1EC9684CAB3767C3021AB67E50
	ISRG Root X1	6D99FB265EB1C5B3744765FCBC648F3CD8E1BFFAFDC4C2F99B9D47CF7FF1C24F
	R3 (cross-signed, expired)**	730C1BD0CD85F57CE5DC0BBA733E5F1BA5A925B2A771D640A26F7A454224DAD3B

Root CA	SubCA	SHA256 Fingerprint
DST Root CA X3 (expired)	R4 (cross-signed, expired)**	5A8F16FDA448D783481CCA57A2428D174DAD8C60943CEB28F661AE31FD39A5FA
ECA Root CA 4		8FA30EA12E781DD5D715736C5AB6746CB13527899C909EB1436BB5D8A71A2BED
	IdenTrust ECA S21	3F8AB6999F084C6F1553510C9C0042EC1FBE367D039A0B457285335219C8440C
	IdenTrust ECA Component S21	F2D4F7E1D5A0840B39988B5112BA73D1A9F849158FBA47826060DCAC17859D2F
	IdenTrust ECA S22	87F627D2EED16D206E9CE3302BE2D28BEBD9D8AE43D0A4322CAEC9C436A86E96
	IdenTrust ECA S22C	C1B718CAF85E4535A07012D6F040B15B2AB3D719DC4D09F4A785E30868097FD8
	IdenTrust ECA S23	13564E34FEE6838BA9C5B042A5BF3F3FF4A80FDB67C74986E7FB306DDFA06479
	IdenTrust ECA Component S23	DBF2107C25639FE95AE2468B4279C9C88BD780AA96470875F8D9C26A2427039B
IdenTrust Global Common Root CA 1		09B15AD8D0CA032861892E55E746AE8DAF1BFDB53A9E5AEE8137D6F89AA111113
	IGC CA 1	50DA52AE7580CE15F163E26A2AF4278D42CA2AAF9AE827CC968A2101282A7CFB
	IGC CA 1	3EE45BEAD5878F0C273743DCFCF1625CD90E88A39D82EE4A01541CB2559BF312
	IGC CA 1	6AB50C761E3EE72C34DB75C2F106E03AF15E2D8E2F6A672EC8FF0966BFD42E78
	IGC Device CA 1	CC0AC905FF000B43AB6CE943EA40AD7DA67AAF1631186453AB44546ED744AAD2
	IGC Server CA 1	7A6DB3693BC4BA02D4197821B534CE4A587CDEE51CE5FA7493DE8DE6090AA601
	Advanced Health Systems, Inc Direct CA 1	5579B0D3B2234CDDD1D31AE9BB646B6A193B8BAE9119326C8C832CE41C6F720D
	Leidos FBCA Cloud PKI CA-1	AEEAE218BF167AB300A271F1D9D404113D67953E6A9957CCAA75E5A642594220
	VA Provider Direct CA 2	611860E2EAFBC241028175567CCE52E901DF08F469BBF47B57ECCBC2692D259B
	VA Patient Direct CA 2	10DBB6273EC2D901EF3A04FDD8568CB4B8CEE5C40A7441F707FAFEEEC48F37ED1

\* 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. 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.

\*\* 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.

## APPENDIX B – OTHER INCIDENTS DISCLOSED BY IDENTRUST

IdenTrust has disclosed that during the period July 1, 2021, to June 30, 2022, the incidents listed below were identified and disclosed to Mozilla. These incidents did not impact the assessed criteria and are included for informational purposes:

- On September 27, 2021, while performing an internal compliance review, IdenTrust determined that the requirement for re-vetting documentation that is older than 398 days was not implemented for Enterprise customers requesting renewal of a certificate via its standard API. This requirement, EV Section 11.14, became effective on June 2, 2021. IdenTrust then identified a total of 124 certificates that had out-of-date vetting. Of these, 22 certificates were issued between April 5, 2021, and June 1, 2021, and thus were technically not in violation of the new requirement, however; an additional 102 certificates were issued between June 3, 2021, and September 24, 2021. To remediate the issue, IdenTrust revoked and replaced all mis-issued certificates in compliance with Section 11.14, and implemented an automated trigger to place all certificate requests where the documentation is approaching the 398-day validation date in a separate validation queue. Requests in this queue require revalidation of vetting documentation prior to approval for issuance.
- On October 19, 2021, IdenTrust reported that not all affected EV TLS certificates disclosed in the September 27, 2021, incident (mis-issued EV TLS certificates) were revoked as expected within 5 days of the incident. The reason for not being able to revoke all affected certificates was due to a significant impact to the affected customer's production services that utilized the identified certificates. IdenTrust remediated this issue by coordinating with the affected customers to revoke and replace certificates as soon as possible. IdenTrust also updated its TLS Subscriber Agreement, adding language to emphasize the obligation to revoke mis-issuances within the CA/B Forum established revocation periods.
- On December 6, 2021, IdenTrust reported the issuance of 1 OV TLS certificate with organization vetting documents that were older than 398 days. IdenTrust remediated this issue by revoking and replacing the certificate, and added technical controls to the validation platform to disallow certificate renewal if the account information is older than 398 days.
- On December 29, 2021, via an internal audit review, IdenTrust discovered that the OCSP Responder certificate issued on December 8, 2021, for the "HydrantID Server CA O1" ICA was missing the "id-pkix-ocsp-nocheck" extension, which is required by Baseline Requirements section 4.9.9. IdenTrust remediated this issue by revoking the certificate and reissuing it to include the "id-pkix-ocsp-nocheck" extension. IdenTrust also updated the master issuance script for such certificates to avoid reoccurrence. A post-issuance linting tool that will detect differences between the intended certificate profile and the freshly issued OCSP Responder certificate is planned for implementation by September 24, 2022.
- On January 26, 2022, an internal review of EV TLS certificates revealed non-compliance with sections 11.1.3 and 9.2.4 of the CA/B Forum EV SSL Guidelines, which require issuing CAs to publicly disclose the sources CA use to vet organizations prior to EV certificate issuance, and to also reference the location of the disclosure in section 3.2.2 of the CA's policy documents. IdenTrust remediated this issue by coordinating the revocation and reissuance of all active EV TLS certificates issued prior to January 26, 2022, publishing the list of sources used to vet EV organizations, and updating the TrustID certificate policy documents
- On February 4, 2022, IdenTrust experienced a connectivity issue for 8 hours that prevented 24X7 consistent CRL and OCSP online responses of 10 seconds or less, per Baseline Requirements section 4.10.2. The issue was caused by traffic hitting the IdenTrust border firewalls during a situation in which they could not pass the traffic, thus creating multiple repeated requests and a traffic bombardment situation. IdenTrust immediately contacted the firewall vendor, and identified the situation as a known problem with one function in the version of the firewall firmware. The firmware problem affected both the primary and disaster recovery sites. Additionally, IdenTrust identified that a set of OCSP responder certificates had been renewed two days before, but the responders had not been restarted to synchronize with the new certificates. IdenTrust opted to turn off the offending function until the new firewall firmware was tested and upgraded during a change window on February 5, 2022, and restarted the OCSP responders to ensure that the renewed certificates were installed properly. In order to prevent reoccurrence, IdenTrust deployed additional

monitoring to identify certificates requiring renewal further in advance of the certificate expiration. The new monitoring will provide seven days advance notice which will persist until the renewed certificates are in place. IdenTrust also strengthened procedures for certificate monthly renewals to ensure all services are confirmed as operational with the new certificates at both the primary and secondary sites.

- On February 11, 2022, IdenTrust discovered an active EV TLS certificate for a government entity with the “jurisdictionStateOrProvinceName” field. As this entity updated its registration to operate in other states, this field should not have been included in the certificate, per EV Guidelines section 1.7.8. IdenTrust remediated this issue by revoking and replacing the certificate, and retrained registration agents in regard to Baseline Requirements for government agencies. In order to prevent reoccurrence, IdenTrust updated its registration and validation procedures to include checklists which must be completed by registration agents to ensure that all Baseline Requirements have been met.
- On February 11, 2022, IdenTrust discovered that an EV TLS test certificate issued to IdenTrust Services, LLC was showing an incorrectly attributed state jurisdiction in violation of Baseline Requirements section 9.2.5. The certificate was revoked on the same day as it was discovered. On February 17, 2022, personnel were retrained to ensure that for EV TLS certificates, the formation state must be selected and matched against the registration number. Additionally and on February 14, 2022, registration procedures were enhanced by adding a checklist which must be completed by registration agents to ensure that all Baseline Requirements items have been met. The checklist must be completed by an agent different from the one who vetted the organization. The document must be digitally signed and uploaded to the account vetting screen.
- On February 25, 2022, IdenTrust reported that during the incident occurring on January 26, 2022, not all EV TLS certificates issued without disclosing the vetting source had been revoked as expected within 5 days of the incident. The reason for not being able to revoke all affected certificates was that some affected customers were unable to replace their certificates within the mandated revocation time as they employed manual methods for replacing certificates. In order to remediate recurrence of delayed revocation, IdenTrust offered automation tools to affected customers at no charge to help reduce the burden and timeline required for certificate replacement. IdenTrust continues to press for the adoption of these tools for both existing and new customers.