IdenTrust™
part of HID Global

IDENTRUST SERVICES, LLC

ROOT KEY GENERATION CEREMONY
INDEPENDENT ASSURANCE REPORT

DECEMBER 20, 2024

Attestation and Compliance Services

schellman
Quality, above all.

This report is intended solely for use by the management of IdenTrust Services, LLC (referred to herein as a “specified user”).

If the report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Table of Contents

Section I

Independent Assurance Report

INDEPENDENT ASSURANCE REPORT

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

Scope

We have examined IdenTrust management's assertion that in generating and protecting its Root CA keys, (collectively, "IdenTrust Root keys") on December 17, 2024, at Salt Lake City, Utah, with the identifying information disclosed in Section 3, IdenTrust has:

- Followed the CA key generation and protection requirements in its:
  - Certificate Policy (CP) v4.9.1 dated November 30, 2024, for TrustID; and
  - Certification Practice Statement (CPS) v4.9.1 dated November 30, 2024, for TrustID.
- Included appropriate, detailed procedures and controls in its Root Key Generation Script dated December 13, 2024.
- Maintained effective controls to provide reasonable assurance that the IdenTrust Root keys were generated and protected in conformity with the procedures described in its CP/CPS and its Root Key Generation Script.
- Performed during the root key generation process, all procedures required by the Root Key Generation Script.
- Generated the IdenTrust Root keys in a physically secured environment as described in its CP/CPS.
- Generated the IdenTrust Root keys using personnel in trusted roles under multiple person control and split knowledge.
- Generated the IdenTrust Root keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP/CPS.

Based on CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

Certification Authority's Responsibilities

IdenTrust's management is responsible for these procedures and for maintaining effective controls based on the CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

Our Independence and Quality Control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behavior.

The firm applies International Standard on Quality Control 1, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Auditor's Responsibilities

Our responsibility is to express an opinion on 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. Our examination included:

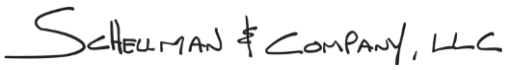
- Obtaining an understanding of IdenTrust's documented plan of procedures to be performed for the generation of the certification authority key pairs for the IdenTrust Root keys;
- Reviewing the Root Key Generation Script for conformance with industry standard practices;
- Testing and evaluating, during the Root key generation process, the effectiveness of controls over the integrity, confidentiality, and availability of all private keys, including back-up copies, and access keys (including physical keys, tokens, and passwords), used in the establishment of the service;
- Physical observation of all procedures performed during the root key generation processes to ensure that the procedures actually performed on December 17, 2024, were in accordance with the Root Key Generation Script for the IdenTrust Root keys; and
- Performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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-CA's services other than its CA operations at Salt Lake City, Utah, nor the suitability of any of IdenTrust CA's services for any customer's intended purpose.



Schellman & Company, LLC
Columbus, Ohio
January 11, 2025

Section 2

Management's Assertion

MANAGEMENT'S ASSERTION

IdenTrust Services, LLC ("IdenTrust") has deployed a public key infrastructure. As part of this deployment, it was necessary to create a hierarchy consistent of self-signed Root CAs known as "IdenTrust Root keys" listed in Section 3. These CAs will serve as Root CAs for client certificate services. In order to allow the CAs to be installed in a final production configuration, a Root Key Generation Ceremony was conducted, the purpose of which was to formally witness and document the creation of the IdenTrust Root private signing keys. This helps assure the non-refutability of the integrity of the IdenTrust Root key pairs, and in particular, the private signing keys.

IdenTrust management has securely generated key pairs, each consisting of a public and private key, in support of its CA operations. The key pairs were generated in accordance with procedures described in IdenTrust's Certificate Policy v4.9.1, IdenTrust's Certification Practices Statement v4.9.1 for TrustID, and the IdenTrust Commercial Root Key Generation Script dated December 13, 2024, which are based on the CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

IdenTrust management established and maintained effective controls over the generation of these keys. These controls were designed to provide reasonable assurance of adherence to the above-mentioned practices throughout the key generation process.

IdenTrust management is responsible for establishing and maintaining procedures over its CA key generations, and over the integrity and confidentiality of all private keys and access keys (including physical keys, tokens, and passwords) used in the establishment of the IdenTrust keypairs, and for the CA environment controls relevant to the generation and protection of its CA keys.

IdenTrust management has assessed the procedures and controls for the generation of the CA keys. Based on that assessment, in management's opinion, in generation and protecting its Root CA keys on December 17, 2024, at Salt Lake City, Utah, with the identifying information provided in Section 3, IdenTrust has:

- Followed the CA key generation and protection requirements in its:
  - Certificate Policy (CP) v4.9.1 dated November 30, 2024, for TrustID; and
  - Certification Practice Statement (CPS) v4.9.1 dated November 30, 2024, for TrustID.
- Included appropriate, detailed procedures and controls in its Root Key Generation Script dated December 13, 2024.
- Maintained effective controls to provide reasonable assurance that the IdenTrust Root keys were generated and protected in conformity with the procedures described in its CP/CPS and its Key Generation Script.
- Performed during the key generation process, all procedures required by its Root Key Generation Script.
- Generated the IdenTrust Root keys in a physically secured environment as described in its CP/CPS.
- Generated the IdenTrust Root keys using personnel in trusted roles under multiple person control and split knowledge.
- Generated the IdenTrust Root keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP/CPS.

Based on the CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

IdenTrust Services, LLC
January 11, 2025

SECTION 3

IDENTRUST ROOT KEYS

IdenTrust Root Keys

Issuance Date	Subject DN	IdenTrust Serial Number	SHA256 Thumbprint
Dec-17-2024	CN=IdenTrust Commercial Root TLS RSA CA 2 O=IdenTrust C=US	400193D667FEF15638F11B7B688C5559	4C53D6746D9502530D235A82F9CF8382F5779D5DDDDBD373ABE1724FC1EFE796
Dec-17-2024	CN=IdenTrust Commercial Root Code Signing RSA CA 2 O=IdenTrust C=US	400193D685B5E01133EFB0CBBFF91B10	BC7C4E46DA2DCF0C25866027B7D164D8EA0D2E82DECA3B520A67070947B7B5D4
Dec-17-2024	CN=IdenTrust Commercial Root SMIME RSA CA 2 O=IdenTrust C=US	400193D69A094D790768B4306300FA68	53850DBA0B62839FED4C0E3E1B95CB7E9C4CF2ED7C3E5AE2D3D3F535EB5A2653
Dec-17-2024	CN=IdenTrust Commercial Root Client-Auth RSA CA 2 O=IdenTrust C=US	400193D6AA3050CF07C80AA8EF327EFB	4F4D24CCFBBECD50C4FCCF0FCF07D7906003AC07E6C8B912012733DE6DD35542
Dec-17-2024	CN=IdenTrust Commercial Root Timestamp RSA CA 2 O=IdenTrust C=US	400193D6B94B794A934045F5C99FC004	D309931736C8F5AAF3C20ADA97FDAF11B5E2D7FD174DC97286ACD613A40AEA55