



IDENTRUST SERVICES, LLC

ROOT KEY GENERATION CEREMONY  
INDEPENDENT ASSURANCE REPORT

APRIL 24, 2024

Attestation and Compliance Services



**Proprietary & Confidential**

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

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.

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

# TABLE OF CONTENTS

SECTION 1 INDEPENDENT ASSURANCE REPORT.....	1
SECTION 2 MANAGEMENT'S ASSERTION .....	4
SECTION 3 IDENTRUST ROOT CA KEYS.....	6

# 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 April 11, 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 \(CP\) v4.9.0 dated March 12, 2024, for TrustID.](#)
  - [IdenTrust Certification Practice Statement \(CPS\) v4.9.0 dated March 12, 2024, for TrustID.](#)
- Included appropriate, detailed procedures and controls in its Root Key Generation Script dated March 18, 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:

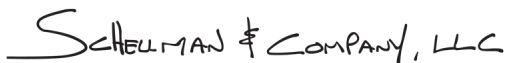
- obtaining an understanding of IdenTrust's documented plan of procedures to be performed for the generation of the certification authority key pairs for the IdenTrust Root keys;
- reviewing the Root Key Generation Script for conformance with industry standard practices;
- testing and evaluating, during 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 April 11, 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  
May 30, 2024

# 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 v4.9.0, IdenTrust's Certification Practices Statement v4.9.0 for TrustID, and the ECC Root CA 2 Key Generation Script dated March 18, 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 April 11, 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 \(CP\) v4.9.0 dated March 12, 2024, for TrustID](#).
  - [IdenTrust Certification Practice Statement \(CPS\) v4.9.0 dated March 12, 2024, for TrustID](#).
- Included appropriate, detailed procedures and controls in its Root Key Generation Script dated March 18, 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  
May 30, 2024



# SECTION 3

## IDENTRUST ROOT KEYS

## IDENTRUST ECC ROOT KEYS

Issuance Date	Subject DN	IdenTrust Serial Number	SHA256 Thumbprint
Apr-11-2024	CN=IdenTrust Commercial Root TLS ECC CA 2 O=IdenTrust C=US	40018ECF000DE911D7447B73E4C1F82E	983D826BA9C87F653FF9E8384C5413E1D59ACF19DDC9C98CE CAE5FDEA2AC229C
Apr-11-2024	CN=IdenTrust Commercial Root SMIME ECC CA 2 O=IdenTrust C=US	40018ECF12B1F35BEEF6DD8A91003773	3B48B18D6F20B2369A7D4056A0F5736E7650D653802305A50E8 3B9C3376D9E18
Apr-11-2024	CN= CN=IdenTrust Commercial Root Client-Auth ECC CA 2 O=IdenTrust C=US	40018ECF19ABACF92F2CE47AC971229B	21E9B3A3A7957B52BF5B9A113CDE238619DEC8B068735152EA A9B996BA5B8575
Apr-11-2024	CN=IdenTrust Commercial Root Timestamp ECC CA 2 O=IdenTrust C=US	40018ECF28EBD1D9BAFE32AC34125F43	7BA2E6514976AF28A6001CDA8EADE532F7A1AAAF25E4731DF 8A04DB00E7801CA