UTILITY CERTIFICATE POLICY [IP-UCP]

Operating Rules and System Documentation Release 4.0

Published Date	**15 December 2023**
Last Reviewed Date	**30 November 2023**

IMPORTANT NOTE ABOUT THIS DOCUMENT

The information contained in this document is intended for personnel charged with the management and operation of the IdenTrust System owned and operated by IdenTrust, Inc., those persons named as recipients, or those persons nominated in the circulation list.

It contains confidential information and if you are not the intended recipient you must not copy, distribute or take any action in reliance on it.

If you have received this document in error, please notify IdenTrust immediately by reverse charge telephone call and return the original by mail. You will be reimbursed for postage.

Contact:

IdenTrust, Inc.
5225 Wiley Post Way, Suite 450
Salt Lake City, UT 84116

Tel: +1 (801) 384-3500

This document is controlled and managed under the authority of the IdenTrust Policy Management Authority.

ABSTRACT

This Certificate Policy (CP) is applicable to the IdenTrust Digital Identity Service, which uses Utility Certificates principally for providing confidentiality and integrity services for IdenTrust Participants and their Customers. Certificate issuance and reliance is restricted to Customers of IdenTrust Participants who have signed and agreed to the relevant service terms and conditions and where appropriate this CP.

AUDIENCE

This document is intended as a guideline for contracted Signatories in the IdenTrust System in the construction of their own IdenTrust related Certificate Policies, although it may be adopted as is.. Each Issuer and Participants will construct their own policies and practices to offer IdenTrust Services.

CONTENTS

1 POLICY IDENTIFICATION

Policy Identification when using Hardware Security Modules, Smart cards or hardware tokens.

Policy Name	IdenTrust Utility Certificate Policy [IP-UCP]
Policy Qualifier	This certificate is for the sole use of IdenTrust, its Issuers, Participants and their Customers. IdenTrust accepts no liability for any claim except as expressly provided in its Operating Rules IL-OPRUL.
Policy Status	Definitive
Policy Ref/OID	1.2.840.114021.1.5.3
Date of Expiry	N/A
Related CPS	IdenTrust RCA CPS, [IO-RCACPS] Issuer CPS Registrar CPS

Policy Identification when using a Software Key Storage Type 2.

Policy Name	IdenTrust Utility Certificate Policy [IP-UCP]
Policy Qualifier	This certificate is for the sole use of IdenTrust, its Issuers, Participants and Customers. IdenTrust accepts no liability for any claim except as expressly provided in its Operating Rules IL-OPRUL.
Policy Status	Definitive
Policy Ref/OID	1.2.840.114021.1.8.3
Date of Expiry	N/A
Related CPS	IdenTrust RCA CPS, IO-RCACPS Issuer CPS Registrar CPS

Policy Identification when using a Software Key Storage Type 1.

Policy Name	IdenTrust Utility Certificate Policy [IP-UCP]
Policy Qualifier	This certificate is for the sole use of IdenTrust, its Issuers, Participants and Customers. IdenTrust accepts no liability for any claim except as expressly provided in its Operating Rules IL-OPRUL.
Policy Status	Definitive
Policy Ref/OID	1.2.840.114021.1.11.3
Date of Expiry	N/A
Related CPS	IdenTrust RCA CPS, IO-RCACPS Issuer CPS Registrar CPS

2 POLICY OUTLINE

This Certificate Policy (CP) is applicable to the IdenTrust Digital Identification Service, which uses Utility Certificates principally for providing confidentiality and integrity services for IdenTrust Participants and their Customers. Certificate issuance is restricted to Customers of IdenTrust Participants who have signed and agreed to the relevant service terms and conditions and, where appropriate, this CP. The Certificate subject and issuer may be obfuscated for meeting Participant’s privacy requirements.

The related IdenTrust Root Certificate Authority Certification Practice Statement [IO-RCACPS] provides details of the measures IdenTrust and the Participants have taken to ensure the policies described in this document have been implemented correctly.

3 CP PROVISIONS

3.1 Community & Applicability

The Utility Certificate is to be used by contracted parties within the IdenTrust System.

Utility Certificates are only to be used for the purpose of providing IdenTrust Services. Within the IdenTrust System, a Utility Certificate is permitted to provide the following services:

- Encryption
- Data Confidentiality and Integrity;
- User Authenticity including TLS/SSL
- Secure Key distribution; and
- Client Authentication.

Utility Certificates restrict services to those described above by defining Key usage fields within the Certificate (See Certificate Profile).

3.2 Rights & Obligations

3.2.1 Obligations

3.2.1.1 The Subscribing Customer:

- is obliged to protect their Private Key at all times, against loss, disclosure to any other party, modification and unauthorized use, in accordance with the IdenTrust Operating Rules and relevant contractual agreements and this CP.
- is personally and solely responsible for the confidentiality and integrity of its Private Key.
- is responsible for the accuracy of the data it transmits as part of a Certificate request.
- is required to immediately inform its Registrar if compromise of its Private Key occurs.
- is to immediately inform its Registrar if there is any change in its information that is included in its Certificate or provided during the registration process.
- accepts that its Certificate may be published in an Issuer or owned directory services which may be available to other IdenTrust Customers.
- is responsible to check the correctness of the content of its published Certificate within seven (7) days from its issuance.

3.2.1.2 The Relying Customer:

- is to acknowledge that the assurance provided by a Utility Certificate is not guaranteed in any form by IdenTrust.
- is to understand that a Participant may provide some assurance guarantees on a Utility Certificate. Participants may optionally provide Utility Certificate

Validation Services, which where provided may oblige Relying Customers (via relevant contractual agreements) to check Certificate Status prior to use.

- must only use a Utility Certificate that has not Expired, or been Revoked or been Suspended.
- may obtain its Relying Participant's Certificate status from IdenTrust.
- is to ensure they comply with any local laws and regulations, which may impact their right to use certain cryptographic instruments.

3.2.2 Interpretation & Enforcement

The enforceability, construction, interpretation, and validity of this CP shall be governed by and construed in accordance with the laws of New York State and the parties submit to the exclusive jurisdiction of the New York State courts.

3.2.3 Publication & Repository

Not applicable.

3.2.4 Confidentiality

All Customer information obtained during the registration phase is kept confidential inline with current Data Protection Legislation.

3.3 Identification & Authentication

3.3.1 Initial Registration

Registrars shall provide details of their registration process to their Customers. No specific requirements are mandated for registration of Customers provided with Utility Certificates.

3.4 Operational Requirements

3.4.1 Certificate Application, Issuance & Acceptance

Customers apply to their Registrars (their IdenTrust Participant) for obtaining Utility Certificates. After initial registration and Certification of the Utility Public Key, Customers are issued with their Key Pairs and related Certificates on a hardware device or Software Key Storage (SKS).

After perusal of the Utility Certificate, a Customer's use of their Key Pairs/Utility Certificate constitutes an acceptance of the Key Pairs and Certificate.

3.4.2 Certificate Suspension & Revocation

Utility Certificates may be Suspended or Revoked. Suspension for more than sixty (60) days may automatically causes the Certificate to be Revoked. A Revoked/Suspended Certificate must not be used.

3.4.3 Certificate Renewal

If the Participant intends to renew their Customer's Certificate, Registrars shall provide a new Certificate to their Customer, before expiry of the Utility Certificate.

3.5 Technical Security Controls

3.5.1 Key Pair Generation and Installation

All Key Pairs used in relation with the Utility Certificate are generated in and stored in applicable requirements.

- HSM meeting FIPS 140-2 Level 3 or FIPS 140-3 Level 3
- Smartcards meeting FIPS 140-2 Level 3 or FIPS 140-3 Level 3
- SKS meeting the requirements stated in IT-KSMR

Keys are securely distributed in Hardware Security Modules, Smart cards, hardware tokens, or a SKS devices.

Registrars are responsible for securely generating and installing the Key Pair related to a Utility Certificate in hardware or SKS

3.5.2 Private Key Protection

Private Keys are protected in Hardware Security Modules, Smart cards or hardware tokens or SKS device.

3.5.3 Activation Data

Activation data is to be kept secure and distributed separate from the token holding the Customers' Private Key(s).

3.6 Certificate Profiles

Please refer to the IdenTrust Public Key Infrastructure and Certificate Profiles [IT-PKI] document for a description of X.509 V.3 Certificate attributes.

REFERENCES

[IL-OPRUL]	IdenTrust Operating Rules
[IO-RCACPS]	IdenTrust Root Certificate Authority Certification Practice Statement
[IT-KSMR]	IdenTrust Key Storage Mechanisms Requirements
[IT-PKI]	IdenTrust Public Key Infrastructure and Certificate Profiles

REVISION HISTORY

Version	Description	Date	Author
1.0	Released	March 2000	IdenTrust
1.8	Released	September 2002	IdenTrust
2.0	Released	February 2003	IdenTrust
2.1	Released	June 2003	IdenTrust
3.0	Released	October 2003	IdenTrust
3.1	Released	July 2004	IdenTrust
3.1a	Released	January 2007	IdenTrust
4.0	1) Version updated 2) References updated 3) Logo changed 4) Copyright date changed to 1999-2023 5) IdenTrust address changed 6) Pre-release footer removed 7) Effective date added 8) Document moved from Policy Approval Authority to IdenTrust Policy Management Authority 9) FIPS 140-3 support added, FIPS 140-1 removed 10) IP-UCP may be adopted as is 11) Suspended certificate may be automatically revoked but not required to	December 2023	IdenTrust