



# IDENTITY CERTIFICATE POLICY [IP-ICP]

---

Operating Rules and System Documentation Release 3.1a

*Copyright ©IdenTrust, Inc. 2006. All rights reserved. This document is confidential material, is the intellectual property of IdenTrust, and is intended for use only by IdenTrust, its participating Signatories, and its licensees. This document shall not be duplicated, used, or disclosed in whole or in part for any purposes other than those approved by IdenTrust.*

*IdenTrust™ is a trademark and service mark of IdenTrust, Inc. and is protected under the laws of the United States and other countries.*

## **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.  
795 Folsom St., 1<sup>st</sup> Floor  
San Francisco, California 94107

Tel: +1 866-IDENTRUST (433-6878)

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

## **ABSTRACT**

This Certificate Policy is applicable to the IdenTrust Digital Identity Service, which uses Digital Certificates for providing organization authentication and non-repudiation. 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 Certificate Policy.

## **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. Each Issuer and Participants will construct their own policies and practices to offer IdenTrust Services.

## CONTENTS

<b>1</b>	<b>POLICY IDENTIFICATION</b> .....	<b>4</b>
<b>2</b>	<b>POLICY OUTLINE</b> .....	<b>5</b>
<b>3</b>	<b>CP PROVISIONS</b> .....	<b>6</b>
3.1	COMMUNITY & APPLICABILITY .....	6
3.2	RIGHTS & OBLIGATIONS .....	6
3.2.1	<i>Obligations</i> .....	6
3.2.2	<i>Interpretation &amp; Enforcement</i> .....	7
3.2.3	<i>Publication &amp; Repository</i> .....	7
3.2.4	<i>Confidentiality</i> .....	7
3.3	IDENTIFICATION & AUTHENTICATION.....	7
3.3.1	<i>Initial Registration</i> .....	7
3.4	OPERATIONAL REQUIREMENTS .....	7
3.4.1	<i>Certificate Application, Issuance &amp; Acceptance</i> .....	7
3.4.2	<i>Certificate Suspension &amp; Revocation</i> .....	7
3.4.3	<i>Certificate Renewal</i> .....	7
3.5	TECHNICAL SECURITY CONTROLS .....	8
3.5.1	<i>Key Pair Generation and Installation</i> .....	8
3.5.2	<i>Private Key Protection</i> .....	8
3.5.3	<i>Activation Data</i> .....	8
3.6	CERTIFICATE PROFILES .....	8

# 1 POLICY IDENTIFICATION

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

<b>Policy Name</b>	IdenTrust Identity Certificate Policy [IP-ICP]
<b>Policy Qualifier</b>	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.
<b>Policy Status</b>	Definitive
<b>Policy Ref/OID</b>	1.2.840.114021.1.4.2
<b>Date of Expiry</b>	N/A
<b>Related CPS</b>	IdenTrust RCA CPS, IO-RCACPS Issuer CPS Registrar CPS

Policy Identification when using a Software Key Storage System

<b>Policy Name</b>	IdenTrust Identity Certificate Policy [IP-ICP]
<b>Policy Qualifier</b>	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.
<b>Policy Status</b>	Definitive
<b>Policy Ref/OID</b>	1.2.840.114021.1.7.2
<b>Date of Expiry</b>	N/A
<b>Related CPS</b>	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 Digital Certificates for providing organization authentication and non-repudiation. 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.

Certificate users have been registered by Registrars using a robust registration process thus ensuring a high level of confidence for the binding between a personal identity and a Public Key. Thus a Certificate issued under this CP provides the highest level of assurance for correct authentication of the Subscriber's department and organization.

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

**ONLY CONTRACTED PARTIES WITHIN THE IDENTRUST SYSTEM MAY USE AND RELY UPON AN IDENTRUST IDENTITY CERTIFICATE.**

## 3 CP PROVISIONS

### 3.1 Community & Applicability

Identity Certificates are only to be used by contracted parties within the IdenTrust System.

Identity Certificates are only to be used for the purpose of providing the following IdenTrust services: access control, client authentication, user authenticity including SSL, digital signing and non-repudiation.

Identity 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 its 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 obligated to never store the PIN (Personal Identity Number) or pass phrase, used to protect unauthorized use of the Private Key, in the same location as the Private Key itself or next to its storage media, or otherwise in an unprotected manner without sufficient protection.
- 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 Keys occurs.
- Is to immediately inform their Registrar if there is any change in its information included in its Certificate or provided during the registration process.
- Accepts that its Certificate may be published in an Issuer or Participant owned directory service that 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 exercise due diligence and reasonable judgment before deciding to rely on a Certificate based service, including performing certificate processing in accordance with the technical requirements defined in IT-DSMSSP.
- Only a party that has signed a Customer Agreement with an IdenTrust Participant containing provisions implementing the IdenTrust Required Terms for Customer Agreements [IL-RTCA] may rely upon a signature or certificate of IdenTrust, a

## **IdenTrust Identity Certificate Policy [IP-ICP], Version 3.1a**

Participant or a Subscribing Customer, and only upon the terms contained in that Customer Agreement.

- May obtain its Relying Participant's Certificate status from IdenTrust.
- Is to ensure that it complies with any local laws and regulations, which may impact its 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 shall be kept confidential and in accordance with current Data Protection Legislation.

## **3.3 Identification & Authentication**

### **3.3.1 *Initial Registration***

All Registrars registering Customers for provision of an Identity Certificate shall meet the minimum registration criteria dictated by IdenTrust Minimum Know Your Customer Requirements [IL-KYC]. Registrars shall provide details of their registration process to their Customers.

## **3.4 Operational Requirements**

### **3.4.1 *Certificate Application, Issuance & Acceptance***

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

After review of the Identity Certificate, a Customers' use of their Key Pairs/Identity Certificate shall constitute an acceptance of the Key Pairs and Certificate.

### **3.4.2 *Certificate Suspension & Revocation***

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

### **3.4.3 *Certificate Renewal***

Before expiry of the Identity Certificate, Registrars shall provide a new Certificate to their Customer.

## **3.5 Technical Security Controls**

### **3.5.1 Key Pair Generation and Installation**

All Key Pairs used in relation with an Identity Certificate are generated in and stored in applicable requirements.

- HSM meeting FIPS 140-1 Level 3 or FIPS 140-2 Level 3
- Smartcards meeting FIPS 140-1 Level 2 or FIPS 140-2 Level 2
- SKS meeting the requirements stated in IT-KSMR and IT-PKI

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 an Identity Certificate in hardware or SKS

### **3.5.2 Private Key Protection**

The Identity Private Key is securely protected, as described in section 3.5.1 and can only be used upon secure authentication of the certificate holder, which is required before every use of the key.

### **3.5.3 Activation Data**

Activation data is to be kept secure and distributed separately 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-KYC]	IdenTrust Minimum "Know Your Customer" Requirements
[IL-OPRUL]	IdenTrust Operating Rules
[IL-RTCA]	IdenTrust Required Terms for Customer Agreements
[IO-RCACPS]	IdenTrust Root Certificate Authority Certification Practice Statement
[IT-DSMSSP]	IdenTrust Digital Signature Messaging Systems Specifications
[IT-KSMR]	IdenTrust Key Storage Mechanisms Requirements
[IT-PKI]	IdenTrust Public Key Infrastructure and Certificate Profiles