



# IdenTrust™ Trust Source

*The Platform for Trusted Identities*



## Providing Digital Certificates to Meet All Certificate Policies

All government agencies, financial institutions and corporations have policies and procedures that govern how they run their organizations. These policies and procedures cover operations, finance, human resources, how they manage suppliers, and the like.

As the volume and importance of electronic commerce increases, organizations now need to add policies and procedures to govern the digital certificates that enable trustworthy, secure and legally binding electronic commerce.

But all digital certificates are not created equal. Many of the digital certificates available today contain vague or unclear policies, or policies meant to protect the issuer of the certificate rather than the parties relying on the certificate.

Organizations need to be sure that their provider of digital certificates abides by policies and procedures that are clear, straightforward and protect the organization from legal liability. They also need to ensure that those policies and procedures will withstand the scrutiny of third-party audits.

## The Role of the Certificate Policy

The Certificate Policy, or CP, provides a high level description of the roles, responsibilities and relationships among all parties in an electronic transaction including certificate authorities, registration authorities, certificate manufacturing authorities, repositories, subscribers, relying parties and policy authorities. The CP is critical to the reliability, security and trustworthiness of a digital certificate.

For example, the CP establishes who can serve as a Certificate Authority (CA), how certificates should be managed, when and how audits should be conducted, the legal rights and responsibilities of the parties relying upon the digital certificate and the practices and procedures used to issue the digital certificate and digital signatures, among others.



## Benefits

### Strong Credentials

A Trust Source digital certificate provides much stronger authentication than IDs and passwords.

### Configurable

The Trust Source platform is highly customizable to meet the certificate policies of any government agency, financial institution or corporation.

### Support Standards

The Trust Source platform complies with numerous industry standards such as RFC 3647 Internet X.509 Public Key Infrastructure.

### Eliminate Need for Own Infrastructure

IdenTrust provides Trust Source as a hosted service, eliminating the need to build and maintain an internal digital certificate infrastructure.

### Cost Savings

Sharing the IdenTrust infrastructure with other IdenTrust customers saves money and eliminates the need to purchase hardware and software or maintain data centers or network infrastructures.

### Supports Growth

The Trust Source architecture is fully scalable.

## How IdenTrust Provides Certificate Policies

IdenTrust™ Trust Source is a technology platform that allows government agencies, financial institutions and corporations to offer digital certificates that conform to their own certificate policies. IdenTrust's certification practice statement (CPS) describes how IdenTrust creates, issues, manages and revokes certificates to comply with a particular organizations' CP.

For example, Trust Source can issue digital certificates that comply with the U.S. General Services Administration (GSA) requirements for its Access Certificates for Electronic Services (ACES) digital certificates as well as for the State of Washington and other agencies. Trust Source issues digital certificates that comply with the IdenTrust Trust Network CP.

The Trust Source platform has been subjected to government mandated audits.

In addition to supporting the certificate policies for third-party corporations, financial institutions and government agencies, the TrustSource technology platform supports three types of digital certificates available through IdenTrust:

- TrustID® Individual Digital Certificates (consumer-to-consumer transactions)
- TrustID® Business Digital Certificates (business-to-business transactions)
- TrustID® Server Certificates (SSL)

## Trust Source Key Features

- Trust Source allows you to manage digital certificates in compliance with your organization's certificate policy.
- Trust Source is designed to be used over the public Internet and does not require a dedicated network or expensive hardware.
- In addition to providing a secure and reliable technology platform for digital certificates, Trust Source provides non-technical services such as end-user help desk support, troubleshooting and identity vetting.
- Trust Source conforms to the X.509 standard for public key infrastructure (PKI), providing standard formats for digital certificates and conforming to strict requirements for certificate authorities. X.509 provides more confidence, integrity and reliability than other "web of trust" models of certificate authorities.
- Trust Source conforms to audit standards including the ANSI X9.79-based WebTrust for Certificate Authorities and audit testing including Penetration Testing/Ethical Hacking.
- IdenTrust provides full Trust Source configuration through an ASP model. To access Trust Source, users only need a web browser and Internet access. IdenTrust maintains the system according to service level agreements (SLA) which organizations can customize to meet their needs.

### About IdenTrust™

IdenTrust is the global leader in trusted identity solutions, recognized by global financial institutions, government agencies and departments, and commercial organizations around the world. IdenTrust enables organizations to effectively manage the risks associated with identity authentication; work interoperably with countries around the world; minimize investment in creating their own policies and legal frameworks; and deploy a spectrum of products insuring trust, smarter, faster, and more cost effectively.

The only bank-developed identity authentication system, IdenTrust provides a unique legally and technologically interoperable environment for authenticating and using identities worldwide. The IdenTrust Trust Infrastructure is predicated on a proprietary framework that combines policies, legal framework, trusted operations and technology (P.L.O.T.) to create a comprehensive environment for issuing trusted identities. IdenTrust is the only company to provide a solution incorporating all four of these elements. Customer agreements are valid, binding and enforceable in more than 175 countries. IdenTrust identities are globally interoperable under uniform private contracts recognized in countries around the world. Competing offerings, in contrast, rely on a dizzying maze of public laws that vary from jurisdiction to jurisdiction. Additionally, the IdenTrust Trust Infrastructure maintains the privacy of each and every transaction processed by reading only digital certificate information, not the message itself.

For more information on the IdenTrust™ Trust Source or other solutions, please contact:

**Corporate Headquarters**  
55 Hawthorne Street, Suite 400  
San Francisco, CA 94105  
USA

T: +1.415.486.2900  
F: +1.415.486.2901  
E: [sales@IdenTrust.com](mailto:sales@IdenTrust.com)

**European Office**  
288 Bishopsgate  
London, EC2M 4QP  
United Kingdom

T: +44 (0)203.008.8330  
F: +44 (0)203.008.8331  
E: [sales@IdenTrust.com](mailto:sales@IdenTrust.com)

For more information,  
visit:  
[www.IdenTrust.com](http://www.IdenTrust.com)

**IdenTrust**  
WE PUT THE TRUST IN IDENTITY