IdenTrust™ Trust Network
Community Bank Program

Benefits

Strong Multi-factor Authentication
IdenTrust Trust Network Certificates are based on a public key infrastructure (PKI) and use both a public and private key to provide the strongest authentication available.

Global Interoperability
IdenTrust Trust Network Certificates are legally binding and accepted in more than 175 countries.

Leverage Existing Infrastructure
IdenTrust delivers a complete hosted environment, enabling financial institutions to focus on customer service rather than building and maintaining a digital certificate infrastructure.

P.L.O.T. Enabled
Policies, a Legal framework, Operational standards and Technology access combine to reduce the risks in electronic communications. The members-only network ensures compliance with IdenTrust’s strict Rule Set.

Additional Identity Services Available
Your customers can use IdenTrust bank issued certificates for a variety of electronic commerce applications, including authenticating Online account openings and maintenance, loan origination, treasury management, and electronic invoicing.

Delivering Trust With Encryption and Authentication

IdenTrust™ Trust Network Certificates authenticate machine-to-machine communications during a secure sockets layer (SSL) connection using 128-bit SSL certificates. (SSL is widely used to protect information such as credit card numbers and account information via the Web.) IdenTrust uses standard x.509 v3 SSL certificates that work with all SSL-capable browsers and servers.

The combination of SSL and bank-issued certificates to authenticate and encrypt the data transmission ensures that the individual sending and receiving the information is who they say they are.

IdenTrust supplies two types of Trust Network Certificates:

- SSL Certificates for secure machine-to-machine delivery.
- Bank Certificates for authenticating the identity of the user. These certificates are issued as Business, Consumer, or Server certificates for secure and legally binding electronic commerce.

Log-in and Transactional Authentication and Encryption Ensures Privacy, Security, and Non-Repudiation

IdenTrust works with member banks to issue individual certificates based on globally recognized and regulated Know Your Customer (KYC) rules. All IdenTrust members adhere to a Rule Set developed and agreed to by financial institutions from around the world that provides non-repudiation and limitation of liability.
How IdenTrust™ Trust Network Certificates Work

1. Customers or businesses register with an IdenTrust member bank by supplying their identity information and agreeing to minimum Terms & Conditions specified in the IdenTrust Rule Set.

2. The IdenTrust member bank validates the identity information in accordance with KYC requirements. IdenTrust verifies at least the following:
   a. That the certificate applicant is authorized to act on behalf of the customer organization (Business and Server Certificates only).
   b. That the physical address, phone number, and e-mail address are valid.
   c. That the domain name ownership is valid (Server Certificates only).

3. Once it completes the KYC procedures, the IdenTrust member bank sends an activation information and fulfillment package to the certificate applicant’s verified physical address via an out-of-band delivery method such as postal mail. This package may include software drivers, installation instructions and physical key storage mechanism such as a USB token.

4. Using the activation information, the certificate applicant generates and retrieves their digital certificate.

With IdenTrust Trust Network Certificates, banks can rest assured that they are providing their customers with a secure, proven digital certificate.

Banks know their customers, and customers know (and trust) their banks. IdenTrust Trust Network Certificates leverage that trusted relationship in an Online world.