

# IdenTrust™ Certificate Enablement Toolkit

*Rapid Integration and Certification*

## Certificate enablement and IdenTrust™ Compliant Certification Made Easy

As the electronic world becomes increasingly more prone to fraud, financial institutions and their customers are recognizing the need for strong authentication, or Multi Factor Authentication as defined by the National Institute of Standards and Technology (NIST) in the United States. To adopt this approach, web based applications must be modified to accept digitally signed data. They are then able to validate in real time, the digital certificates and signatures every time they are presented. Today, most applications utilize usernames and passwords to control access and use.

While the Federal Financial Institution Examination Council (FFIEC), through its guideline on Multi Factor Authentication, has been instrumental in moving financial institutions to something stronger than usernames and passwords, the approach that many have taken is still vulnerable to fraud. The strongest authentication, according to NIST, is a hard token used in conjunction with a Public Key Infrastructure (PKI) based solution. IdenTrust offers this type of solution that is interoperable globally, and utilizes legally binding contracts that carry non-repudiation and limitation of liability for the IdenTrust certificates.

In conjunction with our technology partners (T) who provide tokens, smart cards and browser based access credentials, IdenTrust adds the policies (P), legal infrastructure (L), and operational rules (O) to deliver the PLOT. Thus, unlike a solution using only a one time password (OTP) for access credentials, IdenTrust enables the token to be used in conjunction with the private key/public key pair identity authentication, to validate the user as well as the access credentials.

To facilitate business applications to take advantage of the PLOT, IdenTrust has developed an enablement toolkit designed to expedite the integration of certificates and to streamline testing of the application for compliance with IdenTrust specifications. The IdenTrust Certificate Enablement Toolkit provides developers with a set of libraries (APIs) necessary to configure a Web application to accept digitally signed data, to verify a digital signature or to validate an IdenTrust certificate, all in compliance with IdenTrust specifications.

Application providers wishing to dramatically reduce their time and cost to certificate-enable their Web applications and to accelerate certification from IdenTrust that their application is IdenTrust™ Compliant, can do so by using the IdenTrust tested components provided in the IdenTrust Certificate Enablement Toolkit.

## Benefits

- Accelerates certificate enablement of Web applications and reduces integration costs
- Easy to integrate with any Web application just by configuring few parameters
- Built using industry leading IAIK strong security libraries
- Provides interface to access a Hardware Security Module
- Robust logging and debugging capabilities
- Accelerates certification by IdenTrust that enabled applications are IdenTrust™ Compliant
- Supports signing and verification of data signed under either PKCS7 or XML DSig specifications
- Supports creation and validation of parallel digital signatures
- Can be implemented in transaction processing or batch mode
- Can be deployed on a server or a desktop

## System Requirements:

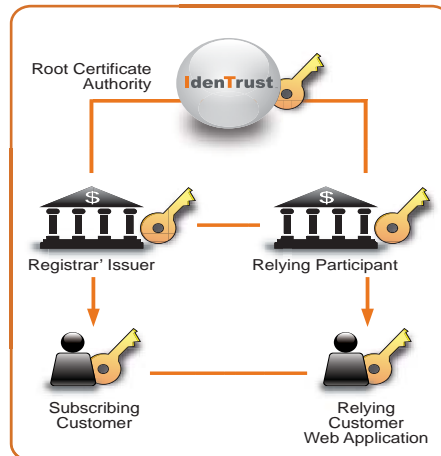
- Java 1.4 or above
- Operating System: Solaris/Linux/Windows



## IdenTrust Delivers What You Need

Included in the toolkit is IdenTrust tested software that, in compliance with IdenTrust specifications: verifies a digital signature or a user's IdenTrust certificate, generates the signed Online Certificate Status Protocol ("OCSP") validation requests, securely sends and receives the messages among IdenTrust Participants and the IdenTrust Root Certificate Authority necessary to validate the signer's certificate and all others in the validation chain, and, communicates validation status back to the application.

Applications can be made IdenTrust "certificate aware" very easily, allowing a financial institution to enable several applications quickly and in parallel. Financial institution customers will transition to certificate use and become comfortable with using them more rapidly when more applications require their use.



## In Summary

By enabling a business application to be certificate aware, and specifically IdenTrust certificate aware, independent software vendors (ISV) can offer their customers the flexibility to choose an additional level of trust for their deployments. Additionally, if the application interacts with corporate customers of the institution, the IdenTrust enablement expands Straight Through Processing (STP). Through its global interoperability and the non-repudiation carried by anything signed with an IdenTrust digital certificate, corporations can streamline their interactions with their banks and reduce both their operational overhead and turnaround time for requests such as delegation of authority, signatory changes, and, opening/closing of accounts. Thus, through the use of the DSMS Toolkit, ISVs can expedite application enablement and, increase overall value for both the financial institution and its customers.

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

For more information on the IdenTrust™ Certificate Enablement Toolkit or other solutions,

### Corporate Headquarters

55 Hawthorne Street, Suite 400  
San Francisco, CA 94105  
USA

T: +1.866.IDENTRUST

F: +1.415.486.2901

E: [sales@IdenTrust.com](mailto:sales@IdenTrust.com)

### European Office

288 Bishopsgate  
London, EC2M 4QP  
United Kingdom

T: +44 20 3008 8330

F: +44 20 3008 8331

E: [sales@IdenTrust.com](mailto:sales@IdenTrust.com)

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, visit the Web site at [www.IdenTrust.com](http://www.IdenTrust.com).

**IdenTrust**  
WE PUT THE TRUST IN IDENTITY