

IdenTrust™ Super DSMS Server

Hosted Online Signature Verification and Certificate Processing

The growth of online business depends upon identity authentication that can be trusted. While solution vendors around the world scramble to find ever more innovative and secure approaches to stay one step ahead of the fraudsters, IdenTrust delivers a trusted infrastructure for issuing and validating digital identities. Online systems equipped to use Public Key Infrastructure (“PKI”) in conjunction with a hard token can provide the strongest authentication according to the National Institute for Standards and Technology (NIST) in the United State. With this approach, digital certificates identifying users can be instantly revoked if the user’s authority is terminated for any reason. Examples of this include termination of employment and a compromising or suspected compromising of the user’s private cryptographic key.

The Application Provider’s Challenge

Enabling Web applications to accept digital signatures and rely upon digital certificates can involve complex integration and management issues. Personnel developing such applications often lack experience in cryptographic system design, and those supporting such applications often lack the ability to maintain a Hardware Security Module (“HSM”) securely storing cryptographic key materials, and may not have access to a high security data center to house it. They may also not be able to maintain the database of signed transaction and certificate validation data. Additionally, many critical applications running in financial institutions were written a long time ago, on older technologies, and thus lack the documentation and expertise needed to easily integrate certificate awareness. As a result, modifications to these applications are held to a minimum and preferably require only an external interface through an API to take advantage of new functionality.

The IdenTrust Hosted Solution

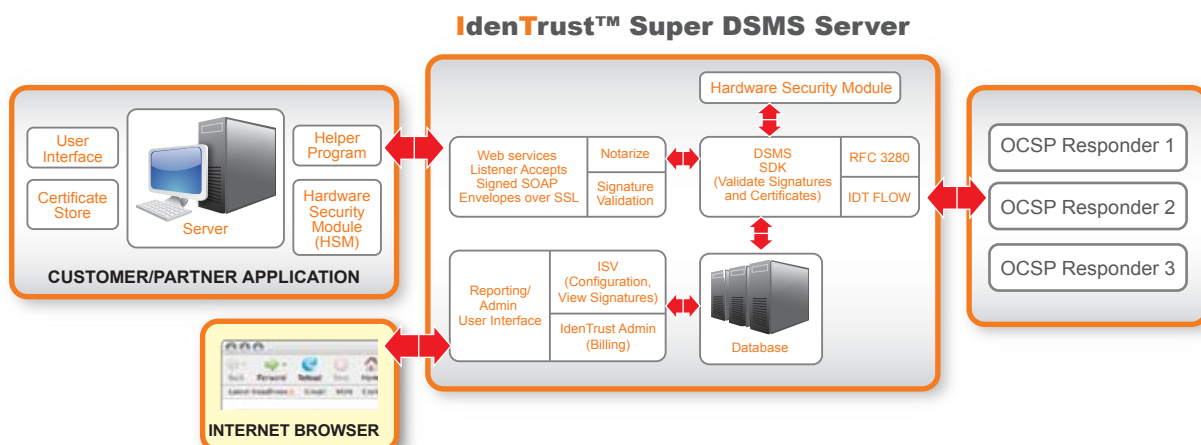
The IdenTrust Super DSMS Server is an IdenTrust hosted and managed service to perform signature verification, certificate validation, and to archive and retrieve the signed data, the signatures, the certificates and their validation status. It allows application developers to rapidly and cost-effectively certificate-enable their Web applications with IdenTrust certificates. IdenTrust hosts both the server and the HSM, and it provides a web interface to application owners to configure and manage their accounts, applications, users and signing keys.

Benefits

- Off the shelf IdenTrust™ Compliant enablement of Web applications to process IdenTrust digital certificates and those of other PKI systems
- Digital certificate and signature verification
- Archive and retrieval of signed transactions and validation status
- Unsigned OCSP and messaging compliant with RFC 3280 support
- Digital notarization support
- Signed Online Certificate Status Protocol (“OCSP”) messaging compliant with IdenTrust specifications

System Requirements:

- Java 1.4 or above
- Operating System: Solaris/Linux/Windows
- Internet Browser IE4+ or Firefox1.2+



About IdenTrust™

IdenTrust enables application providers to minimize the intrusions to their applications by providing them with a set of java libraries that facilitate communication between the Web application and the Super DSMS Server. All the developer needs to do is to incorporate these libraries into its application. When the application receives a signed data packet or user's certificate, the application sends them to the Super DSMS Server over a secure connection. The DSMS Server then verifies the digital signature, generates the validation requests, sends and receives the messages among IdenTrust Participants and the IdenTrust Root Certificate Authority necessary to validate the user's certificate and the others in the validation chain and communicates validation status. This is all completed in compliance with IdenTrust specifications. In addition, the Super DSMS Server archives the signed data, the user's signature, the user's certificate, all other certificates in its validation chain, the validation status of each of them, and the date and time of validation. The Super DSMS Server can also validate certificates using methods not compliant with IdenTrust Specifications, such as unsigned Online Certificate Status Protocol ("OCSP") requests and messaging flows compliant with IETF RFC 3280, enabling flexible deployment architectures.

IdenTrust Super DSMS Server Provides Instant Hosted Certificate Enablement

The IdenTrust Super DSMS Server provides IdenTrust™ Compliant enablement to verify and validate digital signatures with IdenTrust and other PKI certificate systems. It provides archiving and retrieval of signed transaction and certificate validation data, management reporting, system maintenance, secure communications, and a web interface to configure and manage accounts, applications, users and signing keys. It supports both IdenTrust™ Compliant digitally signed OCSP messaging, as well as unsigned OCSP and messaging compliant with RFC 3280, and automatically senses which method to use with any given certificate. For applications requiring validation of an enterprise certificate naming only a business entity, it can store the signing keys in its HSM and use them to notarize and store data and documents originated by the user.

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.

For more information, visit: www.IdenTrust.com

For more information on the IdenTrust™ Super DSMS Server or other solutions, please contact:

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

European Office

288 Bishopsgate
London, EC2M 4QP
United Kingdom

T: +44 20 3008 8330

F: +44 20 3008 8331

E: sales@IdenTrust.com

IdenTrust[™]
WE PUT THE TRUST IN IDENTITY