

# CASE STUDY

# Digital Signature Trust

*“By coupling TrustID’s identity verification services with Kyberpass’ real-time certificate validation, we provide users unrivaled security that further eliminates concerns associated with conducting e-business. Our combined solution allows customers to check the validity of digital certificates, in much the same way a merchant verifies credit cards.”*  
– Scott Lowry, president and CEO of Digital Signature Trust (DST)

## Industry

Internet Security

## The Company

Digital Signature Trust Co. (DST)



DIGITALSIGNATURETRUST

## Business Challenge

Provide a cost-effective means to quickly and easily PKI-enable DST’s customers’ web applications.

## Key Solution Requirements

Kyberpass was required to provide the security components to be integrated into DST’s public key infrastructure (PKI) architecture, which secures the connection between DST and its customers by providing:

- Certificate-based user identification
- Certificate validation using the DST OCSP service
- Monitoring
- Transaction logging
- Attribute-based access control
- No modification to the customer’s application in order to reduce cost and time-to-market

## Key Solution Components

- Kyberpass Web Access TrustPlatform
- Microsoft Windows 2000

## Key Business Results

Kyberpass provided the technology DST required to advance their TrustID® Certificate Program solution offering. This had several interrelated results:

- A cost-effective and fast deployment of Kyberpass technology made it feasible for DST to accelerate TrustID’s time-to-market
- Kyberpass’ middleware approach to PKI-enabling web applications eliminated the high price associated with traditional methods of PKI-enabling web applications
- DST’s customers were able to quickly and easily engage in secure electronic transactions with their own customers and business partners using the DST TrustID Certificate Program

## Business Challenge

Digital Signature Trust (DST) is in the business of providing identity verification services based on digital certificates, digital signatures and public key infrastructure (PKI).

In order for customers to take advantage of their TrustID® Certificate Program the customers’ web applications must first be PKI-enabled. DST chose to PKI-enable their customers’ web applications using third party toolkits. This approach proved to be problematic, and became a significant barrier to successful customer implementations because of the financial and time-consuming burdens it placed on customers. Using third party toolkits is expensive and time consuming because the source code for each application has to be accessed and modified to PKI-enable the application. On average, a single application takes several months to modify and the longer a specialist takes to modify code, the more costs escalate.

What DST needed was a cost-effective means to quickly and easily PKI-enable its customers’ web applications so that the DST customer could use DST’s TrustID Certificate Program, which provides users with a high level of trust and access control in B2B and B2C e-business activities.

## Success Strategy

DST considered Kyberpass the best source to fill this need, and saw an opportunity to eliminate the inherent problems of PKI-enabling applications and expand the TrustID Certificate Program offering using Kyberpass technology.

DST recognized that the Kyberpass Web Access TrustPlatform would blend well with DST’s integrated technical infrastructure (including

Microsoft Windows 2000) to establish a complete PKI architecture for its customers.

Therefore the Kyberpass Web Access TrustPlatform, a comprehensive security policy management solution for web-based B2B and B2C applications operating within an enterprise extranet, web portal or B2B exchange, was employed. Implementing the solution required no modification to existing web applications and provided the following security measures between DST, its customers and DST’s customers’ stakeholders:

- Certificate-based user identification
- Certificate validation using the DST OCSP service
- Monitoring
- Transaction logging
- Attribute-based access control

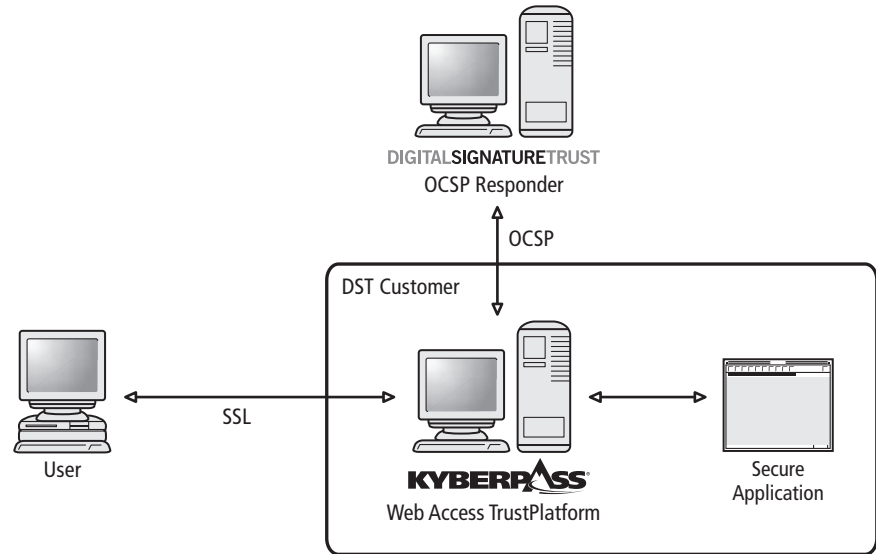
## User Experience

1. The user can either be DST’s customers’ business partner, or an employee trying to gain access to DST’s customer’s secure application. The user is prompted for their TrustID certificate by the user’s web browser, in response to a challenge by the Kyberpass Web Access TrustPlatform that resides on DST’s customer’s site.
2. The OCSP responder provides the Kyberpass Web Access TrustPlatform a real-time validation response: Good, Revoked or Unknown.
3. Assuming the OCSP response is Good, access is granted to DST’s customers’ services or application based on privileges within the Kyberpass profile of the user.
4. A secure B2B or B2C connection is established.

## Business Benefits

Because of the efficiency, low cost and ease of use behind Kyberpass' middleware approach to PKI-enabling web applications, DST is now able to:

- Offer the TrustID Certificate Program up and running in only 5 days
- Offer a TrustID warranty to provide protection to the direct participants of electronic transactions in which a TrustID certificate plays a material role in authenticating the identity of one or more persons to the transaction.
- Pass on the savings to its customers, and maintain the TrustID certificate as the premier certificate to use for e-commerce on the Internet
- Extend the security measures to its pool of stakeholders



Security Architecture for Digital Signature Trust (DST)

## About the Kyberpass Web Access TrustPlatform™

For B2B and B2C applications operating within an enterprise extranet, web portal or B2B exchange, the Kyberpass Web Access TrustPlatform is a comprehensive trust infrastructure providing security policy management and validation services, allowing trusted sessions between users and the applications they're accessing over the Internet.

### Security features include:

- Central control of all security
- Advanced access control including the ability to filter network connections based on IP address, time of day and user attributes
- Ensured data integrity
- Authentication of all data packets using digital signatures
- No modification to the infrastructure or application in securing the application
- Ensured privacy using industry standard symmetric encryption algorithms
- Secondary authentication option using remotely stored pass phrase

### About Kyberpass

Kyberpass® is the leading provider of e-security software for trusted transactions on the Internet. Global enterprises and government organizations use our award-winning TrustPlatform security solutions for rapid creation of trusted B2B exchanges, PKI-enabling of legacy and web applications, employee remote access and digital certificate validation.

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

©2001 Kyberpass Corporation. All right reserved.  
Kyberpass is a registered trademark. All other names and brands are the property of their respective owners.  
Printed in Canada. 1052.01