

DIGITAL SIGNATURE SERVICES (DSS)

Who We Are

Since 1995, Kyberpass has been helping organizations to overcome the challenges of building and deploying high-trust applications for corporate enterprises. Kyberpass recognized two very important issues. First, building high-trust applications should not be a one-off integration of a series of security technologies done on a custom basis for a specific customer. Rather it should be a highly integrated, re-useable platform, which hides the details and complexity of the underlying technologies. Second, trust is only as good as the underlying party providing the trust. For this reason, Kyberpass was one of the first companies to recognize and implement the Identrus business integration solution. Identrus banks are trusted third parties (TTPs), which underpin the entire trust infrastructure.

The Business Problem

As companies re-engineer their business processes to remove costs and improve efficiencies, a major challenge is the security of those processes. Companies are moving to electronic systems for:

- Regulatory filings
- Electronic payments
- IP protection
- Business forms processing

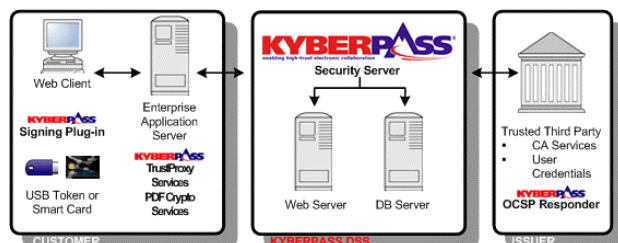
As these business objects move electronically throughout an organization, how can they be kept secure?

The Implementation Challenge

Many large organizations have taken an enterprise, corporate IT, approach to securing applications. Kyberpass supports such companies with the Kyberpass TrustPlatform and TrustServices. While this approach is well understood and established, it does require a significant commitment of time and financial resources to implement within an organization.

An Alternative Approach – Kyberpass Digital Signature Services (DSS)

Kyberpass has introduced a Managed Services version of the Kyberpass TrustPlatform, called Kyberpass Digital Signature Services, or DSS. Kyberpass DSS is intended for those customers who do not want to install their own corporate TrustPlatform infrastructure, or who are too small to justify the cost of a fully implemented security infrastructure.



With Kyberpass DSS companies can have the application security benefits of the Kyberpass TrustPlatform without having to establish a complete trust infrastructure or a certificate authority (CA).

The Components of DSS

As a managed service, the Kyberpass DSS provides the following components:

- A Smart Card or USB token with a digital certificate from a trusted CA for each user
- Downloadable client plug-ins for client browsers
- Kyberpass TrustServices to enable your applications
- PDF Signing and proxy software for your application servers
- A secure connection to the Kyberpass Security Server for managing and validating signatures
- Real-time certificate validation checking [Online Certificate Status Protocol (OCSP)]
- Auditing, logging and signing validation history
- A single monthly fee based on the number of users

The Benefits

Kyberpass DSS allows companies to implement high-trust applications and secure electronic collaboration in a very short period of time. Applications can be enabled in less than two weeks, and once enabled, applications can link to the Kyberpass DSS trust infrastructure almost immediately. Companies can act as their own vetting authorities and enroll users into the system very quickly. Users receive their digital credentials and are ready to collaborate anywhere in the world. Kyberpass DSS is very low impact on corporate IT resources and is highly scalable.

User Cases – Applications That Can Benefit

Electronic Drug Submissions – today's drug approval process requires the collaboration of several dispersed groups. A true secure electronic collaboration is only possible with digital signatures used to sign electronic documents.

Electronic Mortgages – the paper intensive mortgage process can benefit from an electronic re-engineering process where all parties, including the notaries, sign with digital certificates.

Insurance Forms – accountability and timing of insurance form submittals is important for fraud reduction. Digital signatures with secure time stamps help to eliminate this problem.

IP Protection – recording and time stamping research documentation to establish discovery, especially in electronic notebooks, is now possible with digital signatures.

Legal – signing and time stamping electronic documents such as contracts, depositions, corporate filings.

For more information:
Corporate Headquarters: Kyberpass Corporation
1111 Prince of Wales Drive, Ottawa, Ontario, Canada K2C-3T2

Tel. 800.845.1140
Direct. 613.727.6556
Fax. 613.727.8238
www.kyberpass.com

© 2005 Kyberpass Corporation
All rights reserved. Kyberpass is a registered trademark. All other names and brands are the property of their respective owners.