

Kyberpass TrustPlatform™

Background

Since 1995 Cyberpass Corporation has been developing enterprise security solutions for business-critical applications. As one of the early companies supporting the Identrus trust model, Cyberpass has focused its efforts on 'high-trust' applications and transactions, where validated authentication of digital signatures is essential.

TrustPlatform

The Cyberpass TrustPlatform™ Version 6 has been extended to support multiple verticals with special emphasis on enabling legally admissible digital signatures for regulatory compliance and IP protection. As businesses re-engineer their processes to take advantage of electronic content management and collaboration, the Cyberpass TrustPlatform enables the security of transactions subject to regulatory scrutiny. Compliant with Identrus' authentication, signing and validation, the SAFE (Secure Access For Everyone) pharmaceutical industry initiative, and the FDA's 21 CFR Part 11, the Cyberpass TrustPlatform meets many of the industry standards for authentication and digital signature requirements.

More Than a DSMS

The Digital Signature Messaging System (DSMS) Services is but one important component of the Cyberpass TrustPlatform. The DSMS Services provides the essential links between the software application and the trusted third parties (TTPs) standing behind the validation of entity credentials.

Security Server Components

Each component of the Cyberpass Security Server performs a particular function:

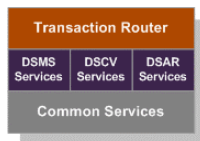
TRANSACTION ROUTER— analyzes a certificate validation request and routes the validation to either the DSMS Services (Identrus™ certificates) or the DSCV Services (non-Identrus certificates)

DSMS SERVICES – enables trusted verification of digital signatures within enterprise applications; meets Identrus requirements; can be hosted for large-scale deployments

DIGITAL SIGNATURE AND CERTIFICATE VALIDATION (DSCV) SERVICES – enables trusted verification of digital signatures within enterprise applications; supports non-Identrus certificates from all the major PKI vendors; can be hosted for large-scale deployments

DIGITAL SIGNATURE AUTHENTICATION RECORD (DSAR) SERVICES – used to provide trusted stand-alone (non-proprietary) permanent records about the validity and authenticity of the signer (or signers) of a data item

COMMON SERVICES – a mandatory component that includes cryptographic libraries, audit logging, secure transport, and TrustProxy Services



As a modular solution, the Cyberpass Security Server is configurable according to enterprise requirements. For example, a standard application requiring Identrus validation would require the Common Services and the DSMS Services. Whereas, an internal PKI validation would require the DSCV Services with the Common Services

Application Server

The Cyberpass Security Server is normally hosted within the corporate IT infrastructure and acts as a security hub, linking enterprise applications with the trusted back-end security infrastructure (e.g. internal or external PKI).

In many instances applications will be hosted on an Application Server and additional Cyberpass components are necessary.

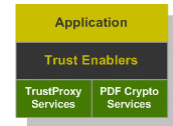
Application Server Components

TRUST ENABLERS – the application programming interface (API) Trust Enabler classes are code classes (C++, Java, or ActiveX),

which provide the API "hooks" to the application for signing actions

TRUSTPROXY SERVICES –provides a secure link between the application and the Cyberpass Security Server

PDF CRYPTO SERVICES – a complete security suite for Adobe® PDF documents including signing, logging, trusted server-controlled signing and validation



Client Desktop

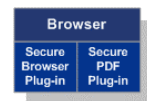
The Cyberpass TrustPlatform includes a set of optional Plug-ins that can be installed on workstations to interact with the Cyberpass Security Server for providing client-side digital signature capabilities. The Plug-ins are designed to support standard X.509 digital certificates stored in:

- Industry-standard PKCS#12 profile containers
- Industry-standard PKCS#11 smart cards
- Microsoft CAPI-compliant smart cards or tokens
- Entrust profile (.epf) containers

Client Desktop Components

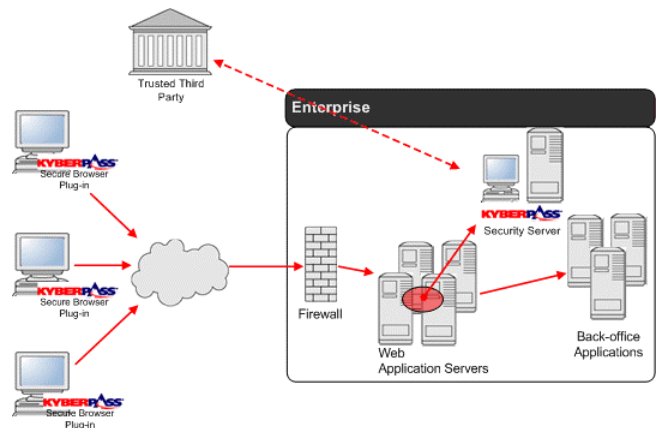
SECURE BROWSER PLUG-IN - operates with industry-standard Web browsers including Microsoft Internet Explorer and Netscape Navigator. It allows users to apply digital signatures to data objects sent from Web servers

SECURE PDF PLUG-IN - allows users to sign and validate PDF files from within Adobe® Acrobat®



Putting it All Together

The Cyberpass TrustPlatform is a suite of security components, which "trust-enable" enterprise business applications. The Cyberpass TrustPlatform provides a secure link between applications and back-end trust infrastructures, including the ability to enable legally admissible digital signatures on documents. It supports signing on PDF, XML, and proprietary data formats.



Corporate Headquarters
 Cyberpass Corporation
 1111 Prince of Wales Drive
 Ottawa, ON, Canada K2C 3T2

Tel 800.845.1140
 Direct 613.727.6556
 Fax 613.727.8238
www.kyberpass.com