vSEC:ID Signing

Smart Card Signatures and Authentication

vSEC:ID extends applications such as web applications with digital signing capabilities. It supports all major web browsers, and can be integrated into any existing web application. It is an easy-to-use security tool that uses secure tokens (for example smart cards) and PKI-based digital signatures for strong authentication and data integrity. vSEC:ID helps corporations, consumers, trading partners, governments and citizens to perform secure and non-repudiate transactions.

Figure 1: *vSEC:ID overview*

vSEC:ID has two major components, the vSEC:ID Client and the vSEC:ID Server. vSEC:ID Client interacts with the secure tokens to do the cryptographic calculations needed for the secure transactions. vSEC:ID Server performs the cryptographic operations required to verify the signatures made on the client side and for validating the certificates used. The vSEC:ID server can perform OCSP and CRL checks along with the capability to interface to HSMs.

Example of how vSEC:ID can be used

A document to be signed, e.g. for a B2B transaction, is created by the web application on the server. The web server also generates a HTML page which includes the vSEC:ID Client component to display the document to be signed to the user, so that the user "signs what he/she sees". After inserting the smart card (holding a valid certificate) in a smart card reader, and typing in the PIN, the user can sign the transaction with a simple click. Next, the data is transmitted securely from vSEC:ID Client to the web server for verification by the vSEC:ID Server.

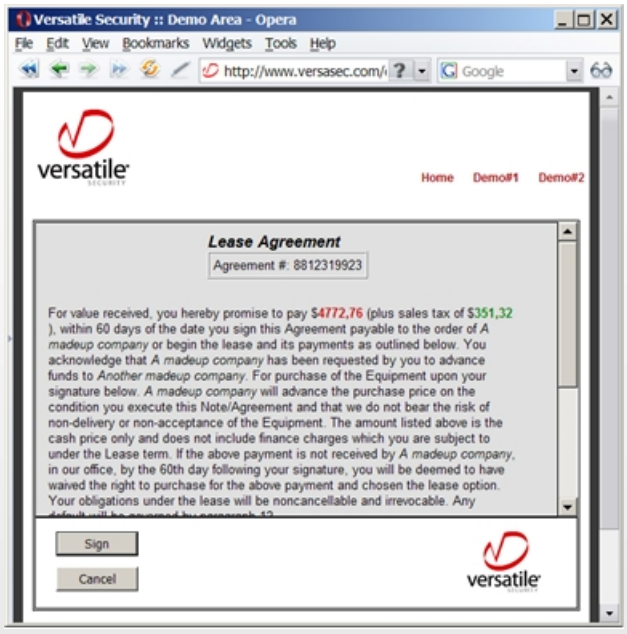

Figure 2: *Web page using vSEC:ID Client*

vSEC:ID Client

The vSEC:ID Client is a lightweight component that interacts directly with secure tokens (no extra middleware needed). The modular and flexible software design makes it easy to adapt to any requirements. All user interfaces and all messages can easily be customized through the APIs. It can be provided to the user as a web component (JavaScript API interfacing with a Java™ applet – zero installation) or as an installation package (can then be shared by many applications and improve operation speed). The fully featured vSEC:ID Client web component can be integrated into any web page to integrate user authentication and digital signatures to web applications.

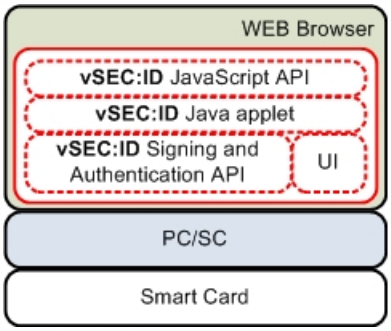

Figure 3: *Web component*

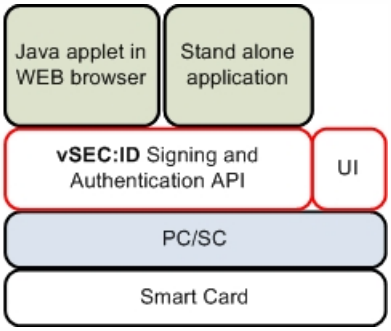

Figure 4: *Installed version*

vSEC:ID Server

The vSEC:ID Server is a high performance server component. It has several interfaces to make it as easy as possible to integrate into any web application. The application interfaces include HTTP, XML and Java. It also interacts with other back-end components such as HSMs through standard interfaces (PKCS#11). It can perform all standard PKI operations, such as sign, encrypt, decrypt, verify and validate certificates.

Technical Specifications

Operating Systems (Client)

- MS Windows 2000, XP, Vista
- Windows Mobile 5, 6
- MAC OSx (contact for details)
- Linux (contact for details)

Operating Systems (Server)

- MS Windows 2003 Server
- Unix systems (contact for details)

Browsers

- IE 5, 6, 7 with Java enabled
- Firefox 2 with Java enabled

Java

- JVM 1.4 or higher

Smart Card Readers

- PC/SC reader

Smart Cards

- Gemalto .NET and GemXpresso, GemSafe
- PKCS #15 1.1, Nordea SEIS, Setec SetCOS, Setec Instant eID, Nidel National eID, Siemens CardOS, Bull TBC80

Document Formats

- Text
- XML
- HTML

Signature Formats

- PKCS#7
- XML DSig

Security features

- Secure document viewer
- Signed policies and configuration
- Timestamping (RFC3161)