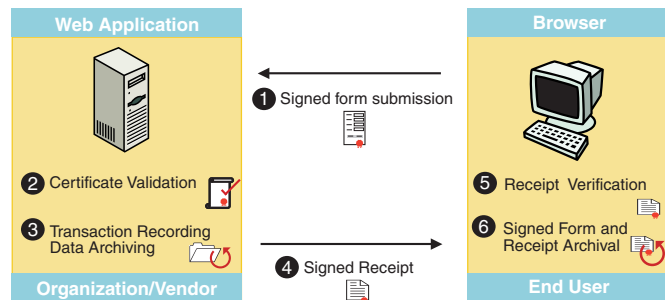


Introduction

E-Lock WebSigner provides for digital signing of on-line information and transactions, so all communication is certified and can be authenticated. It supports signing of HTML, XML, and Adobe based forms and also provides for signing of HTML pages.

With WebSigner, all submitted documents are digitally signed to provide organizations and individuals with non-repudiation since users cannot submit a document without an authorized signature. Also, as users receive receipts that confirm data submissions, receiving organizations cannot deny having received the information. Thus, WebSigner benefits the signing person and/or organization and the receiving person and/or organization.



With WebSigner, organizations can ensure that they receive only trusted and authenticated information for further processing.

This increases organizational efficiency through effective time utilization in the processing of only valid and trusted information.

How it works

E-Lock WebSigner ensures that any information or communication flowing into an organization is authenticated and digitally signed.

By processing only authentic information, the organization saves both time and money by avoiding any legal complications or loss of revenue due to non-repudiation by an end customer.

WebSigner first verifies any data submitted by customers to the web application. It checks that the submitted data has not been altered en route and also checks for validity of the digital certificate of the signer.

Upon verification of the information received, WebSigner archives the information before sending it to the web application for further processing.

The archived form and data submitted by the customer can be regenerated and verified at any point of time by just a single click, allowing the participants to view the originally signed information.

The data can be then verified and the trust and non-repudiation of the submitted document can be established.

Features

- Trusted and authenticated submission of online information
- Time Stamping of the submitted information
- Certificate Validation of digital IDs with OCSP support
- Security Policies for controlling the use of digital signatures
- Section based signing of forms with multiple signature support
- Support for different form formats - HTML and Adobe
- Browser Independence
- Support for automatic signing controls on the client machines
- Support for different security Frameworks - Microsoft, Netscape, and Entrust
- Support for X 509 certificate issued by various PKI vendors

Data Verification

WebSigner first verifies any data submitted by end users to the web application. It checks not only that the submitted data has not been altered en route, but also checks for the validity of the digital certificate of the signer.

Transaction Assurance

SSL (Secure Socket Layer) can establish the credibility of the website that an end user connects to. However, SSL does not extend trust to the individual applications beyond the webserver. In a business transaction, the end user requires the assurance that the vendor or the organization has duly received the data or the information that he/she has submitted.

Enterprise & End User Transaction Assurance

Data Archiving

Upon verification of the information received, WebSigner archives the information before sending it to the web application for further processing. The archived form and data submitted by the end user can be regenerated and verified at any point of time by just a single click, allowing the participants to view the originally signed documents.

Signed Receipts

When end users submit data through forms, WebSigner issues a signed receipt and also creates an archive of the form and the data itself on the end user's local machine.

Complete Non-Repudiation

End users can verify the receipt upon submission of data and validate the organization's digital identity. This provides complete non-repudiation and the assurance that the organization is committed to the information or the order submitted.

Apart from providing non-repudiation and business value to both parties in a transaction, E-Lock has studied other problems facing digital signature implementation and has found that to make an organization's implementation of digital signatures smooth, efficient, and effective, three things must exist:

Platform Independence

Organizations may have web applications functioning on varied platforms such as Windows NT, Unix, and Mac. It is essential for them that digital signatures work and function seamlessly across these platforms. WebSigner is platform independent and resides independently from the web application server. There are therefore no compatibility issues with the existing web server or the web application platform.

Enforced Signing

In order for digital signatures to work effectively within an organization, they need to be implemented every time and for every transaction that takes place. Organizations have no way of ensuring that this happens because they need to rely on user compliance. WebSigner eliminates this reliance on user compliance by forcing users to digitally sign any information before they submit it.

Dynamic Forms

In addition to standard static forms, organizations may also need forms that are generated dynamically based on user input. Naturally, security and digital signature capabilities need to be extended to such dynamically created forms. WebSigner takes digital signing a step further by enabling both static forms and dynamic forms to share the same level of integrity. WebSigner also empowers all generated forms with digital signature technology enabling digital signing of information submitted through these forms.

For more information Sales@elock.com

www.elock.com

The E-Lock range of products is owned by Frontier Technologies Corporation