

E-Lock Is A Data Security Company That Specializes In Electronic Signature Solutions That Help Secure Business Processes And Make Them Compliant With Various Laws And Regulations



E-LOCK OFFERS A RANGE OF ELECTRONIC SIGNATURE SOLUTIONS TO SUIT A VARIETY OF REQUIREMENTS FOR BOTH MICROSOFT CENTRIC AND UNIX BASED SYSTEMS

DESKTOP	Document Signing PROSIGNER, DESKSEAL DESKTOP	
ONLINE	Document Signing DESKSEAL WEB	Form Signing FORMSEAL, XML SIGNING
SERVER	Automated Server Side Signing DESKSEAL SERVICE	
CUSTOMIZATION & INTEGRATION		

APPLICATION EXAMPLES

- ⚙ eGovernance
- ⚙ eProcurement
- ⚙ eBanking
- ⚙ eTendering
- ⚙ Financial Reports
- ⚙ Purchase Orders
- ⚙ Requests and Authorizations
- ⚙ Expense Reports
- ⚙ Medical Forms
- ⚙ Evaluation Reports
- ⚙ Contracts and Agreements
- ⚙ Non Disclosure Agreements

HIGHLIGHTS OF E-LOCK'S SOLUTION

- ⚙ Supports Microsoft, Netscape & Entrust Security frameworks
- ⚙ Support for Microsoft and UNIX platforms
- ⚙ Encryption and Decryption
- ⚙ Support for Common Access Cards (CACs)
- ⚙ Support for USB tokens, soft certificates & hardware tokens
- ⚙ Support for handwritten/scanned signatures
- ⚙ Integration into MS Word, MS Excel and Adobe Acrobat
- ⚙ Ability to mandate signature sequences
- ⚙ Support for organizational policies
- ⚙ Supports CRL, OCSP and CAM validation
- ⚙ Support for time stamping
- ⚙ Audit Trails and Archives
- ⚙ Form data signed in context of entire form
- ⚙ Uses x.509 digital certificates for signing

COMPLIANCE WITH LEGISLATION

- ⚙ E-Sign Act
- ⚙ JITC
- ⚙ HIPAA
- ⚙ 21 CFR Part 11
- ⚙ SOX
- ⚙ EU Law

FREE VERIFICATION

A Free verification utility provided by E-Lock ensures that your customers and users can freely verify signed documents that you send them. This considerably reduces the cost of ownership to an enterprise.

Form Signing FORMSEAL

VIEW AN ONLINE DEMO AT: http://www.elock.com/demo_reg.asp?Product=Formseal

OVERVIEW

E-Lock FormSeal is a digital signature tool that can be integrated into any web application, to enable signing and verification of web based forms. It supports both HTML and Oracle Forms seamlessly. FormSeal uses digital certificates (X.509) for signing.

On receiving the users' data, the FormSeal server component verifies the information before accepting it and returning a receipt to the user for the transaction. All verification occurs on the Server side and verification provides information on the validity, trust, and expiry of the certificate that was used to sign.

FormSeal supports Windows and UNIX/LINUX on both the client and server side. It has been developed using Java to address the key issue of platform

independence and cross-compatibility.

FormSeal also supports digital signing of attachments. Any attachment that you choose to submit will get digitally signed along with the other information in your form.

The main advantage of FormSeal is that not only does the user input (name value pairs) get signed, but the entire form is signed in context of the text, images and code and this provides true non-repudiation since what the user sees is what the user signs.

All transactions are archived and the exact data submitted by a user can be re-created at any time and verified. The verification will display whether the signature is currently valid and also whether it was valid at the time of signing.

KEY FEATURES

- ⚙ Digital Signing of Form Data
- ⚙ PKCS #7 compliant signatures
- ⚙ Signing in context of entire form
- ⚙ Signing of attachments to the form
- ⚙ Data Integrity checks by Server
- ⚙ Certificate Validation by Server
- ⚙ Transaction Archives
- ⚙ Platform Independence
- ⚙ Oracle Forms Support
- ⚙ Integrated Oracle Database Verification

Automated Server Signing DESKSEAL SERVICE

OVERVIEW

E-Lock's automated file signing solution can be run on the Server to sign files in an automated mode without user interaction. Using this solution, thousands of files can be signed on a daily basis automatically.

The solution runs as a Windows Service on the Server machine. You can define an Input Folder on the machine and this folder will be polled at regular intervals (configurable). Any files found will be signed and moved to the defined Output folder.

Multiple folder levels (sub folders) are also supported, in which case the entire Input folder structure will get re-created under the Output folder. A folder called Failed is reserved under the Output folder for files that could not get signed for some reason. Success or Failure in Signing is logged.

The DeskSeal Service supports signing files of any format. Files can be signed using a certificate on the machine or on a smartcard/token. Signatures are enveloped (PKCS #7 format). The resultant signed files are in .p7m format. For PDF files, the signature can be embedded into the PDF (optional). The local machine time is timestamped into the signatures.

The DeskSeal Service consists of:

A Windows Service

Uses the signing control to sign files in a given folder

The DeskSeal Application

Consists of DeskSeal signing and verification controls

A Configuration Manager

To configure settings for automated signing & logging

KEY FEATURES

- ⚙ Automated signing of documents on the Server
- ⚙ Solution runs as a Windows Service on the Server machine
- ⚙ No need for user interaction
- ⚙ Files of any format can be signed
- ⚙ Detailed logging and configuration
- ⚙ Enveloped Signatures (PKCS #7)
- ⚙ Success/Failure in Signing logged
- ⚙ Handwritten Signature / Logo
- ⚙ Flexibility of Signature placement
- ⚙ *Signature can be embedded into PDF files
- ⚙ *Verification through Adobe reader

* to be added soon

Online Document Signing DESKSEAL WEB

VIEW AN ONLINE DEMO AT: http://www.elock.com/demo_reg.asp?Product=Deskseal

OVERVIEW

DeskSeal Web is a solution for signing documents online, in a web environment. Users can either access documents on a website/server and sign them, or they can sign documents from their local machines and upload to the Server.

The screenshot shows a web form with three steps:

- STEP 1:** "Select File to Sign:" with a text input field and a "Browse" button.
- STEP 2:** "Certificate Location:" with radio buttons for "From Certificate Store" (selected) and "From Certificate File (*.pfx/*.p12)". Below "From Certificate File" is another text input field and "Browse" button. A "Certificate File:" label and a "Password:" label with an input field are also present.
- STEP 3:** "Reason to Sign (Optional):" and "Signing Location (Optional):" with text input fields.

Validity (checks for expiry or revocation) and Data Integrity.

Each signed submission is assigned a Transaction ID and by referencing this, the data can be verified at any later time. The Verification provides the user with information on the Data Integrity, Certificate Status (whether valid, expired or revoked) and Certificate Trust. In case of multiple signers, individual verification information is provided per signer.

A free verification utility is provided for offline verification. Signed files can be extracted out of the system, stored on the local machine and can be verified at any time by using the verification software.

Files of any format can be signed and standard x.509 certificates are used to sign. The resultant signed files are in industry standard PKCS #7 format.

Multiple users can sign the same data and each of their signatures can be independently verified.

The Server receives the signed data and performs verification checks to ensure Certificate

Signer 1 Overall Result

- Data verification succeeded
- Certificate not expired
- Certificate not revoked
- Certificate not trusted

Signer Details:	Common Name = Rachel White Organizational Unit = E-Lock Demo Organization = Frontier Technologies Locality = McLean StateOrProvince = VA Country = US Email Address = rachel@elock.com
Signing Time:	Monday, July 12, 2004 2:01:38 PM
Reason:	Approving the document
Location:	McLean, VA

Sample Server Verification Interface per current DeskSeal Web demo

KEY FEATURES

- Web based Signing of documents of any format
- PKCS #7 compliant signatures
- Support for Multiple Signatures
- Data Integrity checks by Server
- Certificate Validation by Server
- Platform Independence
- Audit Trails
- Free E-Lock Reader for Verification
- Encryption & Decryption
- Handwritten Signature/ Logo
- Flexibility of Signature placement

*Signature can be embedded into PDF files

*Verification through Adobe Reader

* to be added soon

CLIENT COMPONENT Common for FormSeal and Deskseal Web

The client component is common for E-Lock's online applications - FormSeal and DeskSeal Web. So with a single client, users can digitally sign information across a variety of applications whether documents or forms.

Clients can be on either Windows or UNIX/LINUX.

The client auto-downloads the first time the user attempts to digitally sign. It enables the user to select an x.509 digital certificate to sign the data/submission.

Document Signing PROSIGNER

DOWNLOAD DEMO SOFTWARE AT: <http://www.elock.com/download/download.asp?Product=prosigner>

SIGN DOCUMENTS DIRECTLY FROM MS WORD, MS EXCEL, ADOBE ACROBAT

ProSigner enables you to digitally sign/encrypt files of any format. In case of MS Word, Excel & Adobe Acrobat, direct integration is provided into these applications and users can sign and verify files using icons and menu items that ProSigner provides within these applications.



RIGHT CLICK SECURITY OPERATIONS

ProSigner integrates seamlessly into the Windows environment, enabling users to "right-click" & perform signing/encryption operations right from their Desktop or Windows Explorer.

MULTIPLE SIGNATURES

Many business documents and approval processes need multiple signatures. With ProSigner, multiple people can sign and approve the same document. An audit trail is maintained which helps track approvals to the document. All signatures can be independently verified. Any change to the content of the document will invalidate the previous signature.

SECTION SIGNING SUPPORT

In some Approval processes, multiple users need to sign and make changes/additions. ProSigner supports this through the use of sections, enabling users to sign & make required changes to the content. This is done

in such a way that the changes can be tracked to the signer in question.

ENCRYPTION TO RESTRICT ACCESS TO CONFIDENTIAL DOCUMENTS

To protect confidential documents, ProSigner uses encryption methods that allow only authorized personnel to decrypt/view the content. Organizations can choose from industry standard encryption algorithms including the high security Advanced Encryption Standard (AES). Other supported algorithms include DES, Triple DES, RC2, RC4

BATCH SIGNING

ProSigner's Batch signing capability makes bulk signing quick and effortless and minimizes the time involved in routine signing tasks. This feature is particularly useful where several business documents require an authorized signature.

HANDWRITTEN SIGNATURES

ProSigner enables associating signature bitmaps or scanned signature images with the digital signature. The bitmap gets inserted into the document alongside the signature details (signer name, time etc). The placement of the signature image and details is configurable.

ACTIVE SIGNATURE BLOCKS

When Word and PDF documents are signed, ProSigner inserts a signature block into the document with information such as the Signer

Name, Time, Reason to sign etc. This signature block is Active or Dynamic, and automatically shows the signature verification status.

SECURE PRINTING - MS WORD

ProSigner supports Secure Printing - the document will always be verified just before printing and gets printed with the most recent verification status. Anyone viewing the printed document can see the verification status.

TIME STAMPING

Many business documents are time sensitive and the time of signing is very essential to the business process. ProSigner allows for time stamping of documents at the time of signing. ProSigner ships with a timestamp client, using which users can connect to a third party trusted time source, which can then be used to time stamp the document.

CERTIFICATE VALIDATION

Provides online, real-time certificate validation for all validation protocols (CRL, OCSP, CAM).

AUDIT TRAIL

Maintains an audit trail that shows when the document was signed, and by whom. This creates accountability in the signing process & serves as a powerful non-repudiation tool.

SECURITY FRAMEWORK

INDEPENDENCE

Supports the MS-Crypto API, Netscape Security framework, and Entrust PKI.

FREE VERIFICATION UTILITY

SECURITY POLICIES

Security Policies are a distinguishing feature of E-Lock's solution. Using Policies, you can define & mandate signature sequences for documents, and no out of turn or unspecified signatures will be allowed. Policies can also be used to mandate the security parameters to be used when signing - for example the certificate to be used, the hash algorithm, whether the document needs to be time stamped etc.

WEB VERSION (* COMING SOON)

ProSigner is also available as a web version, for signing files online & signing form data in context of the entire form. The distinguishing features of this solution are support for Policies & Profiles.

FOR MORE INFORMATION

Contact: info@elock.com

US Office: 703 734 1224

Indian Office: +91 20 25538640