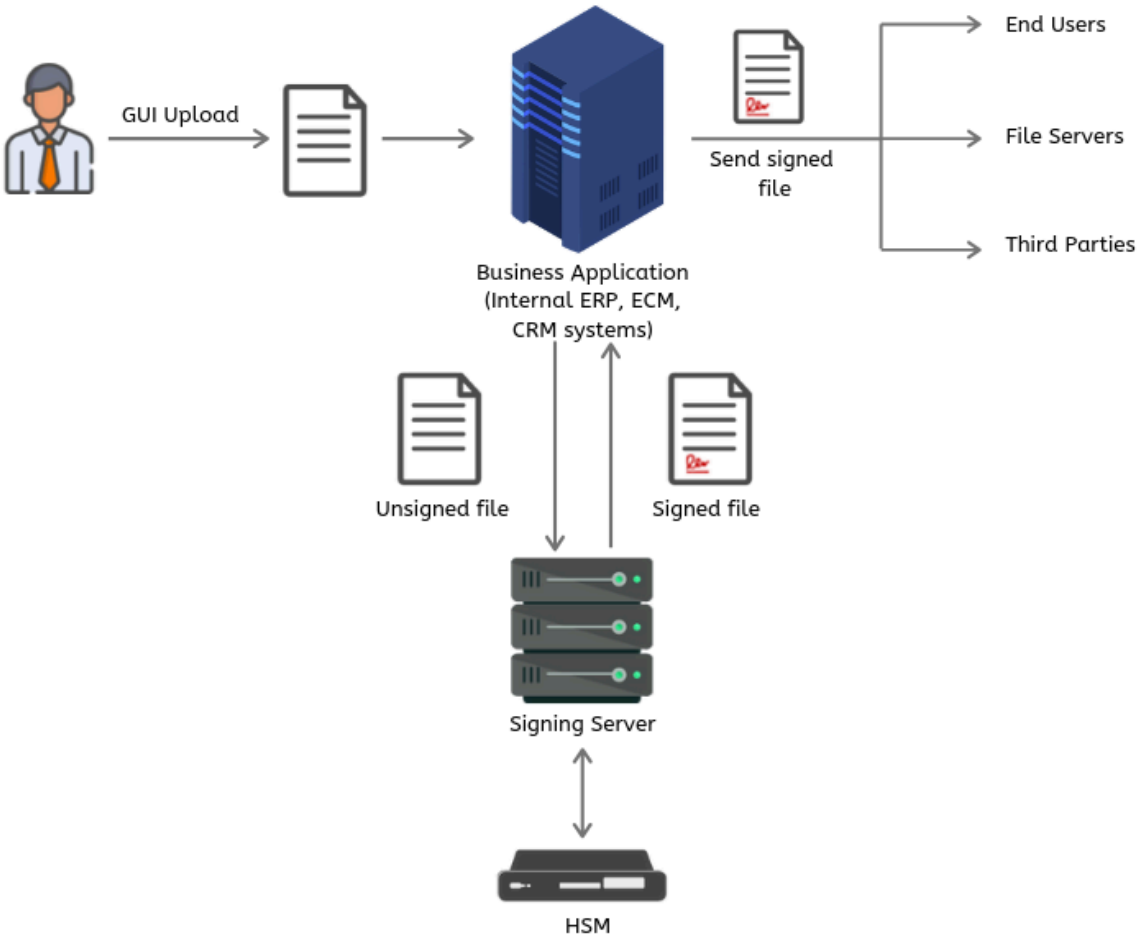
E-Lock SuperSigner SDK

Signing components that can integrate with any web-based application

Copyright © 2024 E-Lock Technologies. All rights reserved.

E-Lock SuperSigner SDK

E-Lock SuperSigner SDK components are in the form of API's, callable from the scripts for PKI based security operations. SuperSigner SDK easily integrates with any 2-tier or 3-tier application developed on Windows or Non-Windows platform giving that application the capability to digitally sign, verify, encrypt, decrypt and time-stamp files. The integration of these components enables developers to provide PKI-based data security and authentication features from within their software.



Signing

Signing components of E-Lock SuperSigner SDK enables users to sign the electronic data. Signatures are in PKCS#7 format, which is an international signature standard. Calling signing API's results in a PKCS#7 (CMS) format signature being created.

Signing components supported:

- Attached Signatures
- Detached Signatures
- Multiple signatures
- Silent signing as well as non-silent signing
- Embedded PDF and PDF/A signing

Copyright © 2024 E-Lock Technologies. All rights reserved.

Attached and detached signatures are supported for in-memory data as well as for electronic files. It also supports multiple signatures for both hierarchical as well as parallel signing modes. Depending on user requirements, signing can be executed silently without any user intervention or it can be executed non-silently in which the certificate selection dialogue box is displayed to the signer with confirmation for signing. E-Lock offers special feature for digitally signing PDF files. It supports embedded signature in PDF files in adobe compatible format, which allows the users to verify these embedded (visible) signatures through Adobe Reader, thus eliminating the need for a separate third-party utility to verify the signatures. This also supports associating a handwritten signature image or company logo with the signature block in the PDF document at any desired position.

E-Lock supports following standards:

- X509 V3 Certificates (RFC 5280)
- Time stamping (RFC 3161)
- PKCS#7 (RFC 2315) / CMS (RFC 5652) – hardware tokens or certificates present in smart cards
- PKCS#11 – HSM's or any PKCS#11 device
- PKCS #12 – Directly using PFX / P12 files
- Online Certificate Status Protocol – OCSP (RFC 2560)
- Supported hashing algorithms – SHA256, SHA384, SHA512 with RSA

Verification

Verification component ideally resides on the server and enables the application to verify the signed data getting submitted. E-Lock verification component does four checks for signature verification to authenticate the signature,

- Data Integrity
- Certificate Trust
- Certificate Expiry &
- Certificate Revocation Check

E-Lock SuperSigner SDK API returns the results of each of these above checks individually. The expiry and revocation checks are done in relation to both current time as well as signing time. Verification component supports verification of multiple signatures, both hierarchical and parallel. The component can return verification results and other information like signer name, signing time, signing reason and location etc. for each of the signatures. Also, it can return the original file that was signed, in case of attached signatures. Verification of both in-memory data as well as signed files is supported. Certificate revocation check is done by automatically downloading CRL using the CRLDP extension in the certificate. The components support access through proxy including authenticated proxies.

Encryption

Encryption component supports PKI based asymmetric as well as symmetric encryption for electronic files and data. Encryption can be implemented on the client end as well as on the server end. In either case, public key of the recipient or password should be available at the point of encryption (client or server). Data can be encrypted for multiple recipients as well. Supports:

- Asymmetric encryption
- Symmetric encryption

Copyright © 2024 E-Lock Technologies. All rights reserved.

Decryption

Decryption component can decrypt any data, which is in the PKCS#7 compliant structure. Users can successfully decrypt a file only if they are one of the recipients for whom the file was encrypted. For decrypting the files, recipients should have private key corresponding to the public key with which the file was encrypted in their USB crypto token or on smart card.

Time-stamp

E-Lock signing components support time-stamp. It allows to stamp the signature with both local time-stamp and third party time-stamp. For local time stamp the caller needs to set the configuration for the local system time be included in the signature at the time of signing. While for the Third party time-stamp it supports RFC3161 compliant timestamp server, which can be specified using Policies.

Licensing

The features and functionality of E-Lock SuperSigner SDK components are governed by E-Lock's licensing scheme.

Server Component

It resides on the application server for verification of the signed data that is submitted or signing the files on server. The license of the server component is specific to the Live IP address of the server on which it is installed

Client Component

It resides on each signer's machine enabling him to sign the data or grant access using his digital certificate. Each client component contains a client license.

Client package (For Windows Platform)

E-Lock SuperSigner SDK client component allows the users to execute the security operations permitted by the application. Client components are available for Windows systems and supports widely used browsers.

Following Client components packages are available to the users:

- **EXE:** E-Lock SignApp application based on WebSockets technology
- **JavaScript Library:** Consists of JavaScript callable APIs that acts as an interface between E-Lock SignApp and host application
- **Sample Scripts:** E-Lock provides sample scripts for the client reference for developing their own workflow

Client package has been tested on following environments:

Platforms: Windows operating system Windows 7, Windows 8, Windows 10

Browsers: Internet Explorer 6.0 and above, Mozilla Firefox version 49 and above, Opera, Google Chrome version 50 and above, Edge first release

Copyright © 2024 E-Lock Technologies. All rights reserved.

E-Lock SuperSigner SDK Server Package (APIs / Web services)

Windows Server E-Lock SuperSigner SDK Windows server package includes COM compliant ActiveX components which can be invoked from languages like C/C++, VB, .Net (C#, VB.Net) etc. This allows integration into Windows desktop as well as Windows server-side applications. It has been tested on following Windows environments:

OS: Windows server 2003/2008/2010/2012/2016 (all editions)
Web Servers: IIS 6.0 and above
Platform: ASP, ASP.Net, C#, C/C++

Non-Windows Server

E-Lock SuperSigner SDK Non-Windows server package includes Java classes and methods that can be invoked directly from any host application. It also provides web-service based implementation which can be consumed by any Enterprise applications like SAP, PeopleSoft HRMS, Oracle EBS, Microsoft SharePoint, Salesforce, etc. The web-services are available both in SOAP as well as REST form. It has been tested on following Non-Windows environments:

OS: Linux (all variants), HP-UX, IBM AIX, Solaris 10
Web Servers: Apache Tomcat 7 and above, JBOSS
Platform: All Java enabled platforms, Open source platforms

About E-Lock

E-Lock is pioneer in the field of Digital and Electronic signature solutions. E-Lock's PKI-based solutions have made digital signatures popular in common business applications and web-based transactions. Compliance with the global standards for digital signatures has allowed E-Lock to serve organizations in more than 30 different countries, spanning several industries, effectively and efficiently. This has resulted in massive customer base for E-Lock in countries like the US, the UK, Australia, Greece, Spain, Hong Kong, Peru, Romania, Kuwait, Portugal, South Africa, Singapore, Lithuania, India, Malaysia, and many more.

For more information:
Visit **www.elock.com**
or write to: **info@elock.com**

Corporate Office:
E-Lock Technologies
209/1B/1A Range Hills Rd, Pune,
Maharashtra, India

Copyright © 2024 E-Lock Technologies. All rights reserved.