LockMagic

Enterprise Encryption Solution

Overview

Blackout Inc,
15127 NE. 24 Street #541,
Redmond, WA 98052
USA

Introduction

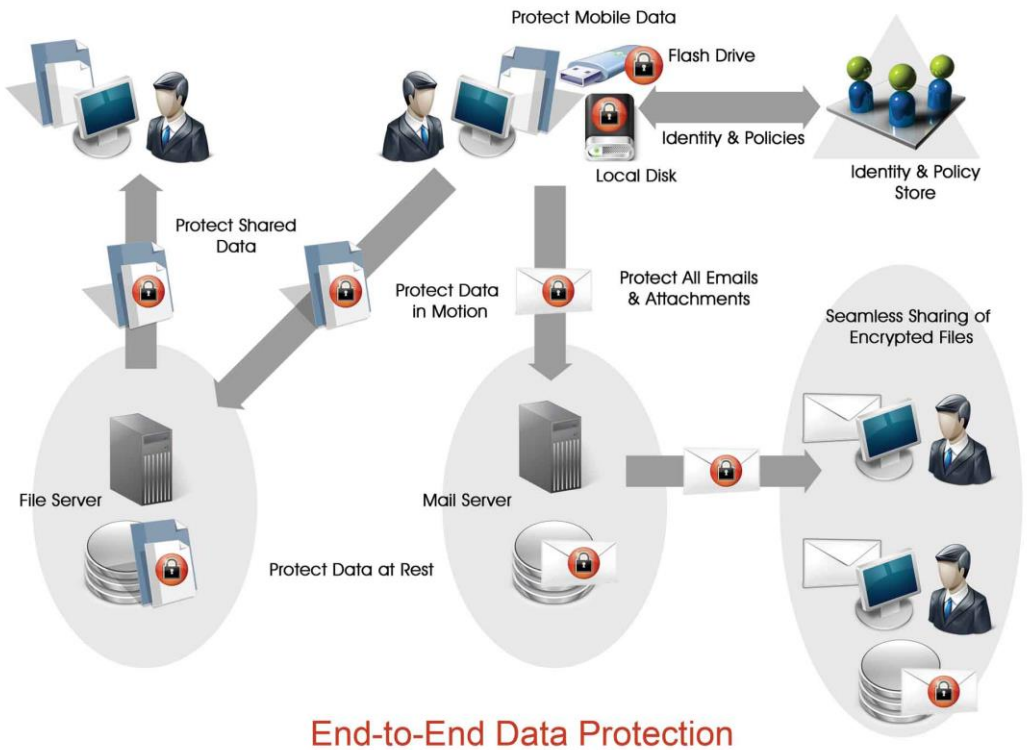
Data protection and leakage prevention are critical requirements for any IT infrastructure and operations. LockMagic allows Enterprise's IT organization to implement a solid information leakage prevention and data protection strategy. This enterprise software product is very easy to use with an exceptionally seamless user experience making it highly effective. It provides a state-of-the-art AES-256 data encryption, signing and compression for better security, storage and auditing. More importantly, it covers a large data security footprint from securing email messages and attachments, file share documents and file to removable media data screening. The entire data protection lifecycle is managed via policies and all secure data accesses are logged by the system for monitoring and auditing.

One of the key challenges in selecting a data security solution is its management and usability. Many solutions have hidden costs associated with managing a secure key database store. LockMagic is a novel identity-based encryption system that addresses these challenges in a simple, easy to use and management-free solution.

Benefits

Applying LockMagic Enterprise solution dramatically empowers Enterprise employees, partners and administrators with the necessary security tools to ensure sensitive corporate data is securely communicated, shared and stored. Users and administrators will be able to accomplish the following:

- Send and receive secure email messages and attachments with anyone in the world.
- Revoke access to secure content when mistakenly sent or shared with unintended users
- Transparently access, share and store secure files in local drive, file shares and removable media
- Central Access Audit Logs enables auditing, alerts and non-repudiation in tamper-free manner.
- Manage user and group access policies of secure content via domain group membership
- Manage authorization of secure content without the need for data re-encryption
- Define secure content policies such as time expiry and 'offline vs online' attributes

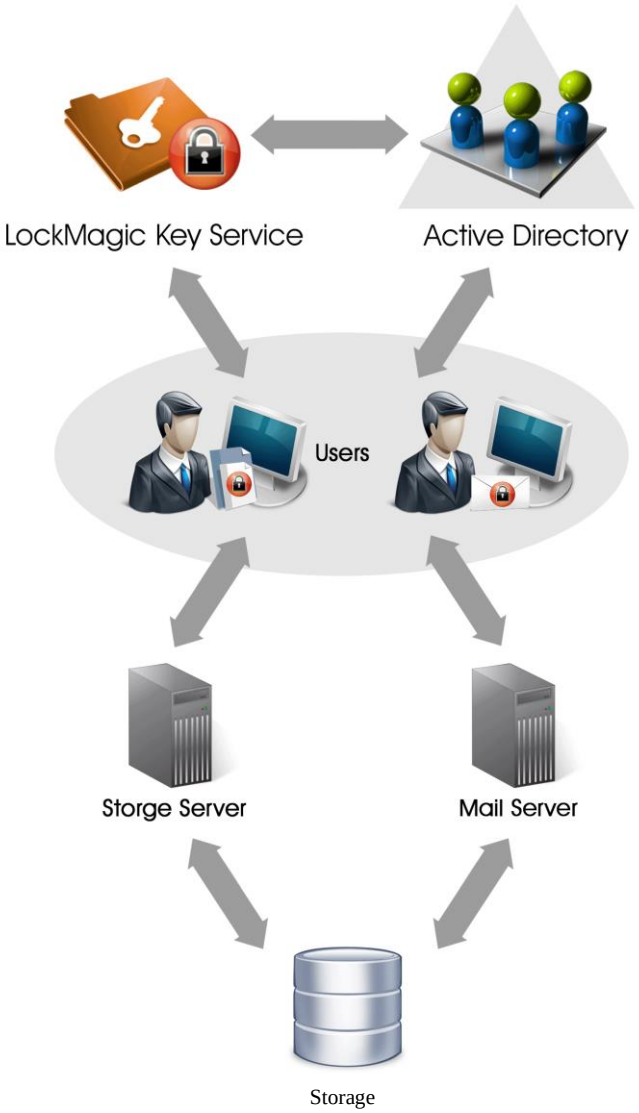


End-to-End Data Protection

Deployment Overview

Our solution consists of a key service and client applications that integrate seamlessly and no impact to existing computing infrastructures. The key service is typically deployed on its own server-class machine and located in a physically secure facility. This server machine will be joined to the domain environment and LockMagic Enterprise key server is installed on it. There are no changes required to Active Directory, Email, Storage or SAN servers.

The client-side components can be transparently installed on user machines from a network share via group policy. Administrators can configure and manage the entire solution using group policy through ADM files.



Enterprise Key Management

LockMagic uses an Identity-based encryption model. Users simply specify the identities (email addresses) of the people they want to share encrypted content with and LockMagic does the rest. There are no passwords to remember or certificates to manage. LockMagic fully transparent design eliminates the need for users to change the way they work to become secure.

Unlike legacy key management solutions that require complex replication and scaling architectures, LockMagic provides "stateless" key management that enables on-demand key access without an ever-growing key store. The result is a system that can be infinitely scaled across distributed physical and logical locations with no additional overhead.

To enable reuse of existing infrastructure investments, the LockMagic Key Management Server offers a federated authentication model that allows for integration with any existing identity management or credential store. User, group, and policy-based authentication rules can be centrally defined on a global or per-application basis.

Benefits of the LockMagic Key Management Model:

- Integrates with any existing authentication or identity management system, including Active Directory, LDAP, Internet Identity and Single Sign-On systems
- Offers enterprise-wide visibility through centralized administration directly from Active Directory, auditing, and reporting
- Eliminates need for complex user key enrollment, key databases, certificate directories, and revocation lists

Key Privacy

When a LockMagic Key service is first instantiated, a base certificate is generated, and its public key is made available to authorized clients. Every LockMagic deployment has its own unique set of certificates. A one-time backup of the service base certificate is performed in order to provide for disaster recovery. There is no other reason to export the service private keys.

Encryption and decryption processes are always performed on the device accessing the data; typically an end-user computing device. Every encryption process of a file or email message locally generates a new symmetric content encryption key. Symmetric content encryption keys are never disclosed, shared, transferred, or exposed on the clear except during the cryptographic operation in memory.

Strong End-to-End Encryption

LockMagic uses state-of-the-art AES-256 encryption standard using Windows FIPS certified implementation with full content encryption. All encrypted content is also signed and protected from external data tampering. All data is encrypted in the source device and decrypted in the destination device. When a user sends a secure email, the entire email message is encrypted, and each block of data is also signed. All encryption meta-data is packaged as part of the encrypted email message. When a recipient opens the secure message, the Lockmagic client running on the recipient device will extract the encryption meta-data and exchanges it with the Lockmagic Key Server to obtain the decryption key. Once the user is verified and validated against the encryption policy, the key server provides the client the key to decrypt and verify the signature blocks.

Stateless Key Management Design

Lockmagic key server provides key management functionalities and doesn't have any access to user data. The server only accepts encryption meta-data to enable transparent encryption between users. Users exchange encrypted content using existing communication and sharing channels. For example, a user sending a secure encrypted email in Outlook, the encrypted content is sent using Outlook client and the Lockmagic key server doesn't see it. User data is never uploaded or stored to Lockmagic Key Servers.

When a user tries to access a LockMagic encrypted content for the first time, the LockMagic application requests access from the LockMagic key service. The user first authenticates with the LockMagic key server and submits the LockMagic token along with a dynamically generated user public key. The key service validates the token integrity and applies its access rights against the requesting user identity. This may require checking the user group membership against Active Directory or LDAP store when groups are included in the access rights list. The key service also enforces any policies found in the token in addition to administrative policies applied directly on the service itself. If the user is allowed access, the key service regenerates the encryption token using the user public key and returns it back to the user. This key tunneling approach enables the LockMagic Key Management Server to be completely stateless.

Zero-Administration & Management

LockMagic state-less key server architecture eliminates costly administrative management tasks and complexities associated with other solutions. Administrators are not burdened with managing and maintaining key stores and databases as in Public Key Infrastructure (PKI) and Rights-Management System (RMS).

Content Protection & Revocation

Users are also able to protect their content from unauthorized copying, printing and snipping while retaining control over the shared content by revoking other people rights at any time. Audit logs and alerts provide information on other people accesses.

Policies

LockMagic support various policies to control access to encrypted content. Transitional encrypted systems based on password and PKI have no ability to enforce any policies or control mechanisms once the encrypted content is received by others. That's because receivers already possess the key to unlock the data. On the other hand, LockMagic requires recipients to first authenticate to a LockMagic Key Service which transforms a user rights to access data into an actual key to unlock the data. This design enables the system to dynamically evaluate and enforce policies defined on the encrypted data without direct access to the data. LockMagic policies include expiry time, read-receipt and *always-on* access.

Content Control

As described above, the LockMagic architecture requires recipients to interact and authenticate with a LockMagic key service to obtain the encryption key to decrypt the data. A unique feature of LockMagic is providing content authors to 'recall' content that is already shared. In other words, LockMagic enables users to "Un-share" data after it has been sent to other people but before it is accessed. When combined with '*always-on*' and *view-role* policies, recipients can be revoked access even if the content is previously accessed. The *view-role* ensures recipients cannot duplicate the secure content via copy/paste, print-screen, save as or printing.

Reporting

The key service maintains a detailed log of every user transaction. This information is captured both in a dedicated Windows event log file and per-transaction file in a specified folder. Each log entry contains information of the requesting user identity, host and full description of the content encryption token policies. Administrators will be able to determine who is accessing what encrypted files and emails from which machines and the status of every access. Unauthorized accesses are quickly detected and reported from the log information. More importantly, each log entry is audit record of the user actions and possession of the secure content providing non-repudiation of secure content.

Secure Email

Lockmagic integrates with Outlook 2003 and 2007 client application to provide seamless end-to-end encryption. One-Click 'Send Secure' button to compose encrypted email messages directly from Outlook application. Email messages are automatically encrypted along with attachments using recipient identities for authorization. There are no end-user actions required to enter password or lookup recipient keys.

When receiving an encrypted message LockMagic extension will automatically opens the message when viewed in the reading pane or form. The message and its attachments always remain encrypted in the outlook local files and remote email server.

Reply and Forward actions of encrypted messages retain the original message encryption property and users are not overwhelmed with re-encryption processes.

Sometimes users mistakenly send sensitive information to unintended recipients. Encryption in this case doesn't help because the unintended users are granted access to the content. LockMagic solves this problem by providing a recall functionality that enables users and administrators to override and block access to secure content at the LockMagic Key Service regardless of the access rights granted during the encryption process. Users who make the mistake of sending the sensitive information to the wrong users can very quickly rectify the security disclosure and block access to the email messages and attachment by using the LockMagic Content Management UI to revoke access to the secure content.

Secure Files and Folders

LockMagic integrates with Windows Explorer to provide a One-Click encryption of folders and files for all file types and sizes. The user selects a file or folder and right-click on 'Copy Encrypted' to generate an encrypted file or folder. The user will be prompted to enter or select the set of email addresses to authorize the files for and the encrypted file can be saved locally, on flash drive or network share. Encrypted files can also be attached to the clipboard for ease of use in copy/paste scenarios. Entire folders can be encrypted in a single 'Copy Encrypted' selection. The encrypted folder can be created local, on a remote server or removable drive or packaged within a single ZIP file.

Users open and save encrypted files are regular files and don't have to change the way they work. Encrypted files are opened transparently from the Windows Shell as regular files. Even updates to encrypted files are transparent to the users and LockMagic propagates user changes to the underlying encrypted files.

Secure Removable Media

Removable devices can be a security threat to any enterprise IT infrastructure because they can be easily lost or concealed to copy data in and out of the corporate network. Furthermore, such devices are typically inserted and shared among many different computers which make removable drives a primary method of propagating viruses.

LockMagic addresses the removable media security threats through its file screening and data access fencing features. Once deployed, LockMagic enables Enterprise IT managers to define data access policies on removable devices. It can transparently encrypt or block data on removable drives to prevent data leakage. It also prevents software viruses from propagating into enterprises infrastructure by blocking programs, drivers and auto-run files from being accessed from removable media.

Technical Details Example of Secure Email Scenario

1- Sending Secure Email

A user is sending a secure encrypted message using Outlook client and LockMagic plugin. The user initiates a secure message either my marking the message as Confidential or by pressing on the LockMagic icon on the Outlook Main Button Panel or the message is transparently encrypted via policy.

The user enters the following into the message form:

1- TO: field is set to list of recipients email addresses
2- BODY: field is set to message content
3- ATTACH: field is list of files to be including as part of email message.

When the user press “Send” the following actions are performed by the LockMagic plugin

1.A Preparation of information:

1- Extract list of user recipients from TO: property to decide ‘who’ has access to message content during decryption process
2- Extract list of file attachments
3- Extract body text from message

1.B Encryption Process:

1- Generate a random symmetric content encryption key (CEK) for AES-256 CBC mode
2- Generate a random signing key
3- Encrypt message body and attachments using CEK to produce $[body]^E$
4- Encrypt signing key, user recipient list and other policies using CEK to produce $[policies]^E$
5- Encrypt CEK using LockMagic Key Service public key to produce $[CEK]^E$
6- Use signing key to sign the byte array of $[CEK]^E$ + $[policies]^E$
7- Use signing key to sign each 64K block of encrypted content
8- Store signature as part of pre-ample header of each encrypted block
9- Compose an encrypted file with $[CEK]^E$ + $[policies]^E$ + $[body]^E$
10- Attach encrypted file as “Message_eml.wef” to the message
11- Replace message body with template message to instruct user how to open secure message.

1.C Sending Process:

1- Outlook client sends encrypted message as regular message marked as confidential to email server
2- Email server receives message and pass it through to list of recipients like any regular message.

2- Receiving Secure Email

A user receives a secure encrypted message using Outlook client and opens it using LockMagic plugin. When the user opens a LockMagic encrypted message the following actions are performed by the LockMagic plugin.

2.A Preparation of information:

1- Extract the attachment file “Message_eml.wef” from email message
2- Connect to LockMagic Key Service
3- Signin user to LockMagic Key Service in non-domain environments if user isn’t already signed in.

2.B Decryption Process:

LockMagic client peforms the following set of actions

1- Extract the sections $[CEK]^{E}$ + $[policies]^{E}$ from encrypted attachment
2- Generate a pair of user keys, private and public, certificate if user doesn’t have one
3- Send via secure RPC or SSL web request the following information to LockMagic Key Service
   a. Metadata block: $[CEK]^{E}$ + $[policies]^{E}$
   b. User identity token
   c. User public key certificate

4- LockMagic Key service will take the following set of actions for each incoming request

   a. Authenticate the incoming request and determine user identity
   b. Apply any policies that restrict the user access such as disabled users
   c. Decrypt $[CEK]^{E}$ using its private key to obtain CEK
   d. Decrypt $[policies]^{E}$ using CEK
   e. Extract signing key from policies set to verify the integrity of entire metadata block to ensure no data tampering has been performed since encryption process
   f. If the signatures mismatch, then request is immediately rejected without further processing
   g. Extract members property from policies set
   h. Lookup user identity in members list and if not found return access denied immediately
   i. Extract expiry time property from policies set
   j. Compare expiry time to current GMT time and if expired return access denied immediately
   k. Extract content unique identifier from policies set
   l. Lookup content ID in local blocked and recalled content store
   m. If content is blocked then return access denied immediately
   n. Once user has been determined to have access the CEK is encrypted with the user public key to produce a new $[CEK]^{Eu}$
   o. Service returns $[CEK]^{Eu}$ and status success to the LockMagic client

LockMagic client will take the following set of actions

5- Receive status and $[CEK]^{Eu}$
6- Decrypt $[CEK]^{Eu}$ using user private key from setup 2. to obtain CEK
7- Extract $[body]^{E}$ from encrypted file and decrypt using CEK to produce clear text body
8- Update message body using clear text body to replace place holder message

Features Summary

Core Protection

- One-Click encryption
- Send encrypted attachments directly from windows explorer
- Create encrypted file, attach it to clipboard to be inserted to an email or copied to any location
- Transparently open and save encrypted files
- Copy an encrypted folder to a destination folder or as single zip file
- Support binary encrypted file format and embedded encrypted HTML format
- Open an encrypted content on a webpage
- Manage identity of authorized people by providing their email addresses
- Create self-signed certificates, import and backup certificates from single management console
- Create template that contains lists of email addresses and certificates to be applied as a single unit
- Allow users to recall and activate secure content via LockMagic Content Manager application

Secure Email

- Provide an Outlook 2003/2007 plug-in to transparently send/receive secure messages
- Encrypting/Decrypting message body and attachments transparently
- Sending read-receipt directly from key service upon access of encrypted message or attachment
- Provide content expiration on email message and attachments

Secure File System

- Enable transparent encryption of files and documents
- Accessing \\secure\<drive name or server name> to create secured files on physical location “drive name:\” or “\\server name”
- Run without admin rights except on initial setup for offline clients
- Run from flash drive or network drive without installation
- Secure all file types
- Protect secure content on workspace from unsigned applications
- Create multiple secure workspaces at the same time
- Specify a list of emails addresses and certificates via templates to be applied to files in workspace to share secure files with others

Secure Removable Media

- Transparent secure file access
- Manage access policies for removable media
- Block access to removable media based on access policy
- Encrypt data on removable media based on data protection policy

Enterprise Key Service

- Transparent integration with Active Directory to derive authorization via group membership
- Transparent key service location discovery via service connection point
- Manage access to encrypted content using security and distribution groups
- Support single-sign on and mutual authentication
- Disable access to key service for specific users via group membership
- Disable access to encrypted content authored by specific users defined in a security group
- Log all user service requests and token accesses
- Recall specified document and email tokens to prevent undesired access
- Enforce time expiry policies on token accesses

Cloud Encryption Service

- Allow users to send secure email messages via web browser
- Allow users to access key service over Internet
- Allow users to encrypt and decrypt files over web browser
- Allow users to encrypt and decrypt messages over web browser
- Allow users to create secure documents via web browser
- Allow users to share secure content with other people using Internet Identities
- Provide LockMagic specific user registration and identity service for external partners
- Allows users to sign in using registered LockMagic identity to access secure content

Usability Analysis

Usability	LockMagic
Integrated directly with existing messaging collaboration systems	• Add-on to Outlook email client • Independent of any messaging server technology: no server-side changes • Client-side encryption/decryption
Easy to deploy easy to use systems with One-click security capability.	• MSI-based installation enables silent deployment • No key or password prompts • Shortcut menus: ‘Send Secure’,’Encrypt’ • Double-click on-demand: ‘Decrypt’
Compatible with SANs and other Storage media and backup systems	• Client-side data protection model that allows independence from storage and backup technologies
Send to anyone capabilities	• Identity-based encryption model that eliminates user key pre-enrollment and exchange
No end-user key exchange or management required.	• Transparently derive authorization information during encryption from recipients list in email messages; eliminating end-user key and password prompts. • Administratively managed encryption templates

Security Analysis

Security	LockMagic
Strong encryption and authentication.	• AES-256 encryption and 4K public keys • Secure RPC or SSL • Mutual Authentication • Single Sign On
End-to-end email security.	• Client-based model that encrypts and decrypts all data on the client-side protecting information on the network and email servers
Non-repudiation of messages	• Service tamper-free audit logs • Unique per-message tokens and encryption keys • Authenticity of tokens
Enterprise access to decryption keys.	• Built-inkey recovery model • Standard certificate key storage • Export certificates via standard tools • Stateless key model: no key database required
Unique enc/dec keys registered for Enterprise only.	• Auto-generated key pairs unique to every machine • No private keys shared or transferred between users or machines

Management Analysis

Management	LockMagic
Rapid deployment.	• MSI-based deployment • Silent install over network • Published policy templates on file share
Centrally manage users & policies	• Central authorization of encrypted content through AD / LDAP • Group Policy management via “adm” files • No data re-encryption on authorization changes • Key service access derived from AD group membership
Private label branding	• Auto-marking of encrypted messages as Private • Reply/Forward of messages preserves encryption property
Interoperable with existing infrastructure.	• No changes (schema, extensions, configuration, …etc) to AD/LDAP, Email server or storage systems • Key Service deployable and isolated on independent server • Centrally manage via policy to enable/disable encryption function • Send clear or encrypted messages independently
Flexible and extensible to the future expansion.	• Standard logging format enables integration with log analysis and management systems • Bulk encryption enables integration with other data security systems • Supports multi-tenancy • Integrates with two-factor authentication systems