

LockMagic

Universal Encryption



Product Overview

<https://www.lockmagic.com>

LockMagic Introduction

LockMagic is an Information Asset and Rights Management solution to protect, track, audit and revoke access to sensitive information inside and outside your organization. Our **patented** identity-based encryption technology enables users and administrators to secure and share information anywhere without the complexities of key management. Users grant access to other people by simply using their email addresses eliminating the need to exchange and manage passwords or certificates. The entire process of encryption and decryption is based on people identity making the solution extremely simple to use.

LockMagic integrates with two-factor authentication systems to ensure strong identity verification during access to encrypted content. LockMagic integrates and supports smart-cards, Google Authenticator Smart Phone App and Yubikey tokens.

LockMagic Benefits

One-Click Encryption

LockMagic provides protection to all file types (files, photos, videos, documents, backups and entire folders) and sizes with support for external users. LockMagic secures content with users inside and outside your organization with a single click. Templates and policies make the system highly configurable and robust. Furthermore, partial encryption for Microsoft Word and Excel documents eliminates the need to maintain multiple documents for different users while reducing the impact on search and discovery of information.

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.

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).

Universal Client-less AnyWhere Access

LockMagic provides zero-install protection with an innovative browser-based HTML5 solution. All user data is encrypted and decrypted locally inside the web browser regardless of the user device and without software installation.

LockMagic AnyWhere File Encryption

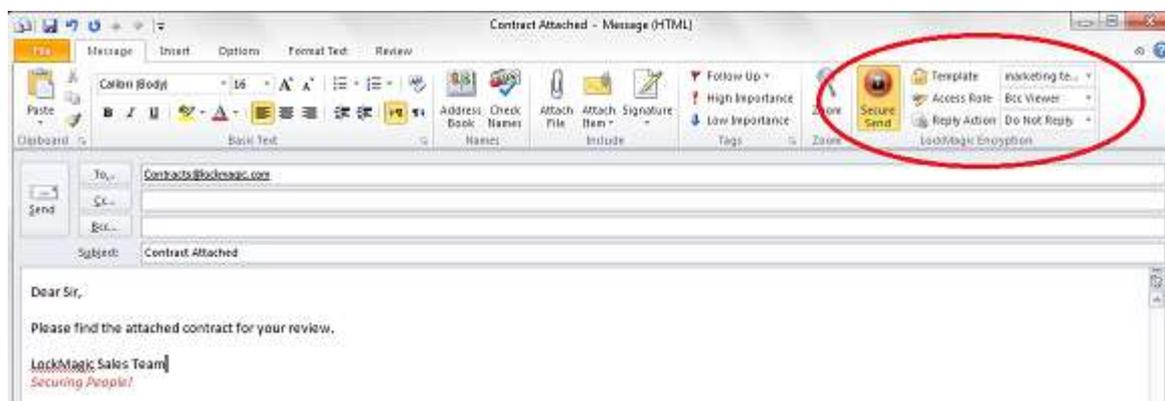
Users encrypt documents and files on their local machine using LockMagic application and store the encrypted files on local drive, flash drive, network share, Sharepoint or cloud storage such as Dropbox or Google Drive. During the encryption process, users specify the users and groups to grant access to the secure content along with the access role such as Owner, Editor or Viewer. Other users access the encrypted content using a LockMagic client and depending on the access role granted the recipient user may be able to own or view-only the content.



For example, users can protect WORD files and share them using email, cloud storage or flash drive. Authorized users can access the encrypted files using their identity without have to share keys or passwords. Users with viewer-role will only be able to view the WORD files on the screen and are prevented from copying the secure content via the clipboard, print-screen, snipping or printing.

LockMagic AnyOne Email Encryption

Lockmagic integrates with Microsoft Outlook Email client 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 the LockMagic extension will automatically open the message when viewed in the reading pane or form. The message and

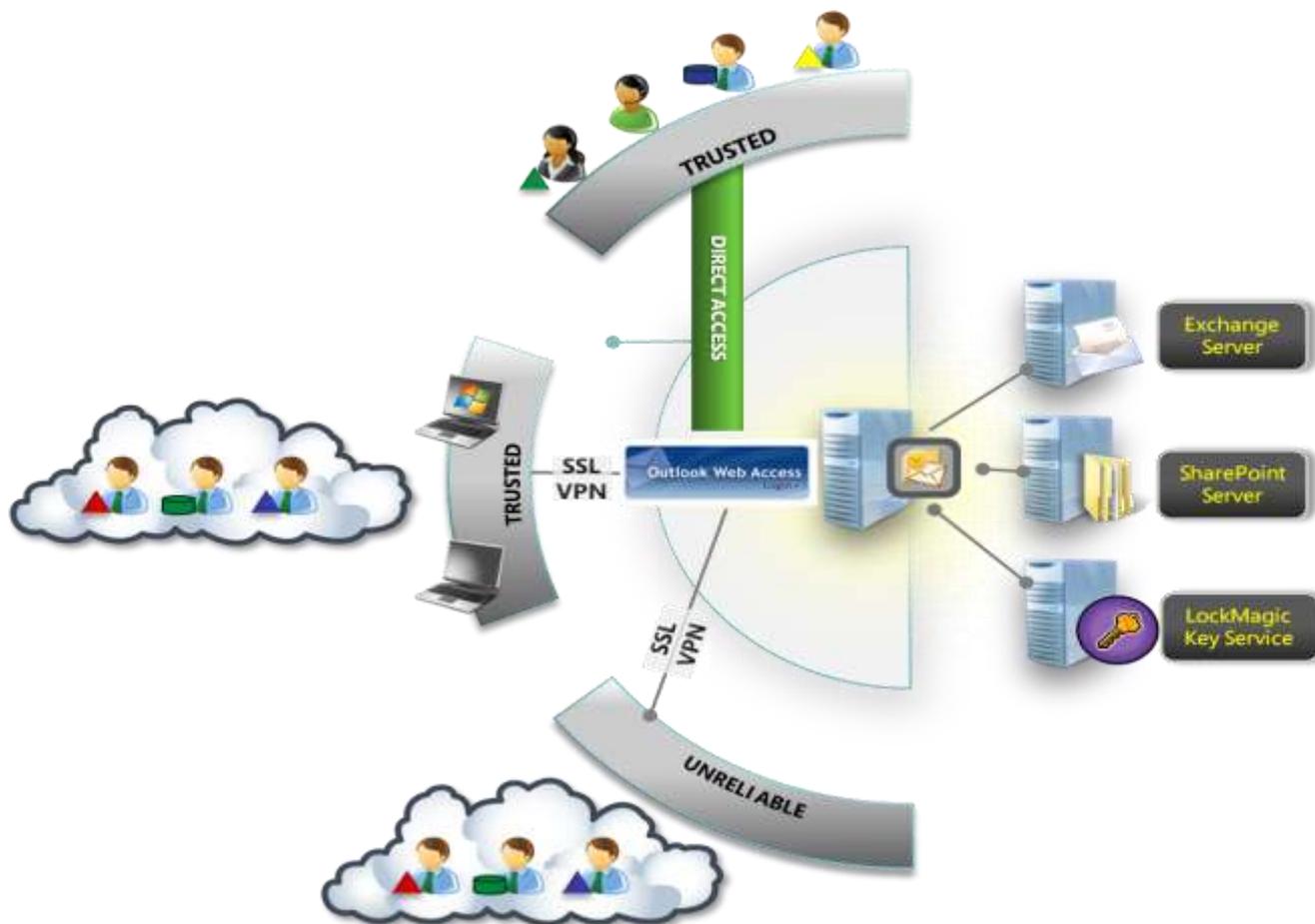
its attachments always remain encrypted in the outlook local files and remote email server.

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

LockMagic Exchange Outlook Web Access Protector

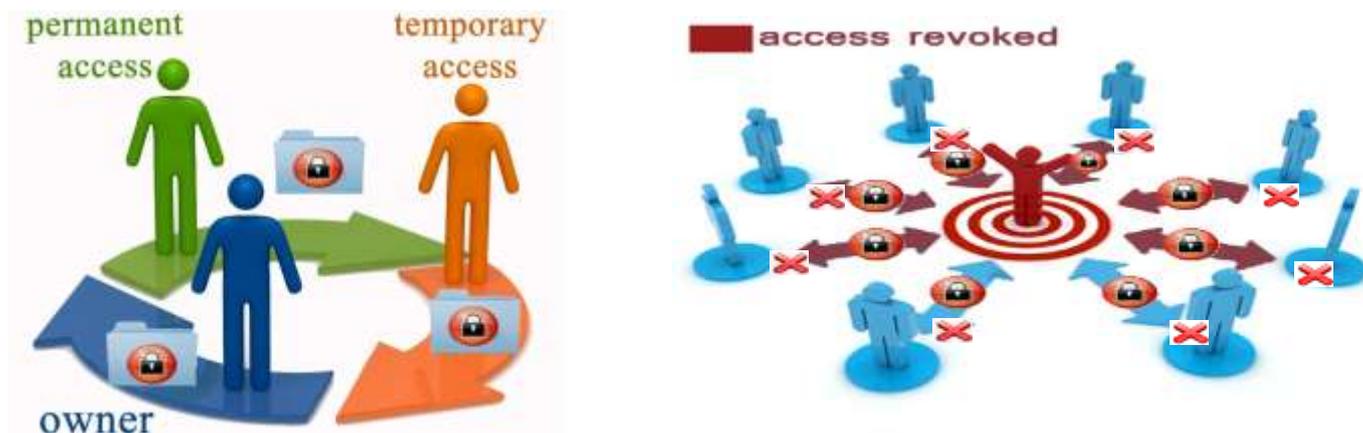
LockMagic integrates as an extension application to Exchange Outlook Web Access (OWA) in a simple and seamless manner. LockMagic for OWA is a Net.ASPX application that enables users to send, reply and view secure email messages over any web browser. Unlike traditional solutions, encryption and decryption are performed inside the client web browser.

Outlook Web Access is deployed as part a Client Access Server that runs independent from the Exchange Store Server. The LockMagic application consists of a set of ASP.NET pages and a managed HTTP transport handler. It is solely deployed on the Client Access Server with simple configuration updates.



LockMagic Content Revocation

LockMagic offers users complete control over content with support for per-document expiry and revocation model. Authors always retain control over their content even after the content has been shared with others. Sharing can be assigned an expiry deadline after which the content becomes inaccessible.



LockMagic per-document revocation model enables content owners to revoke access to shared content at any time to retain control over it. For example, an external partner may have been granted viewer-only access to some sensitive information that the partner is no longer authorized to access. The partner access can be revoke even though the partner has possession of the encrypted content. After revocation the partner will not be able to access the encrypted content and because the partner is only granted viewing rights, the secure content couldn't have been copied, printed, snipped or print-screened.

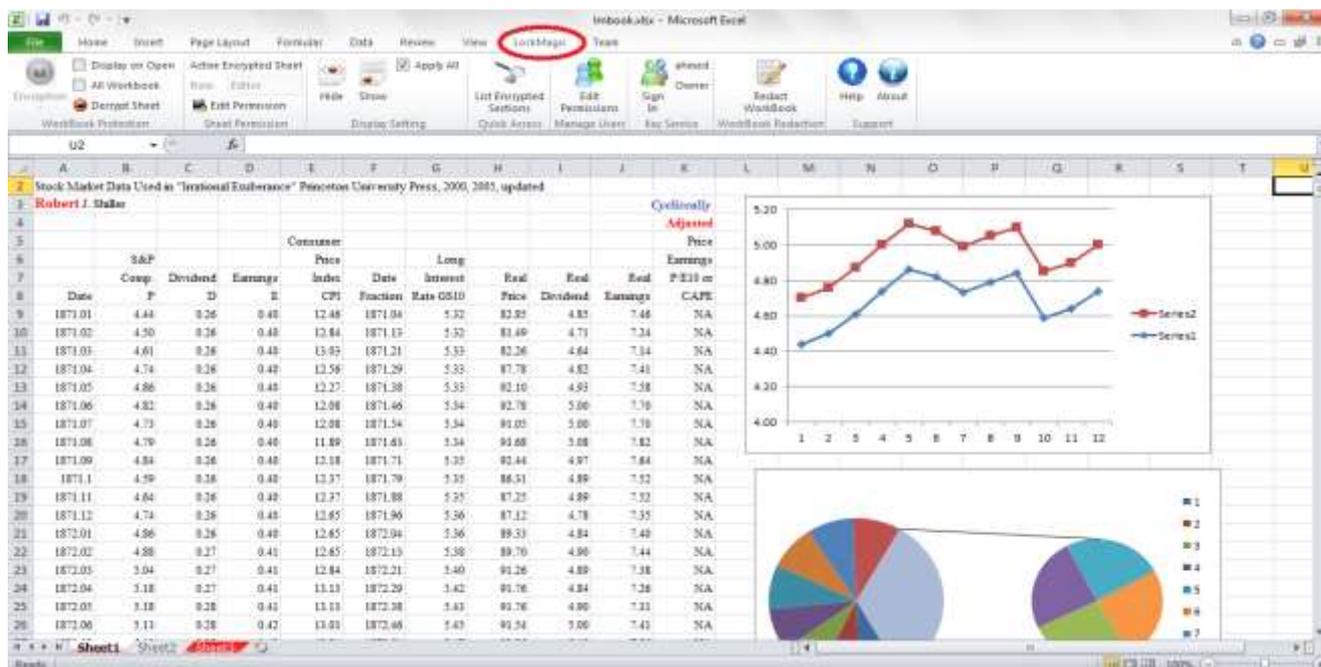
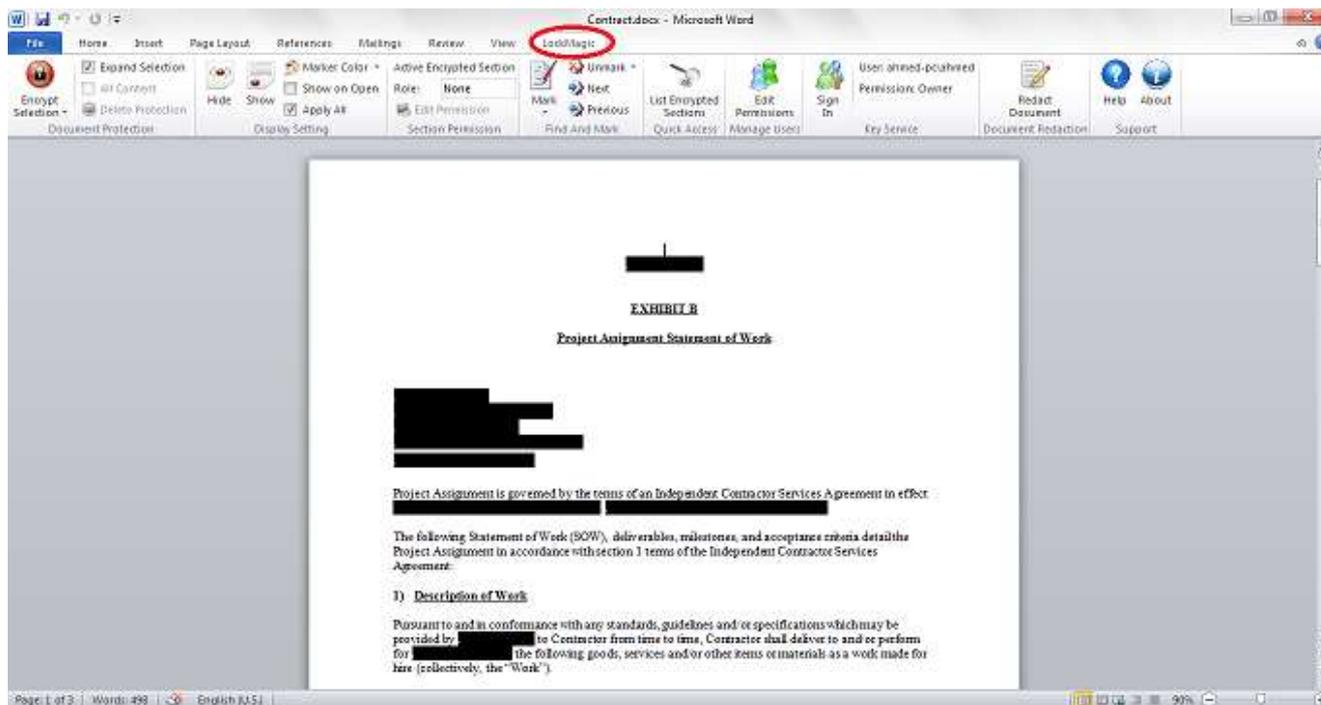
LockMagic Application Integration (SDK)

LockMagic is designed and implemented with extensible in mind offering a software-development kit (SDK) in several languages and platforms including C, Objective C, Javascript, Java and C#. The API is extremely easy to use given the nature of the state-less identity-based architecture. Custom applications can easily integrate LockMagic functionality with little effort. LockMagic own Microsoft Office plugins and web portal are implemented using the SDK APIs and libraries. The platform is available on any device ranging from desktop to mobile devices.



LockMagic Partial Content Encryption

There are many situations when users want to maintain a single copy of a document or spreadsheet to share with multiple people but control which parts of the document other users can view. LockMagic has plug-ins for Microsoft Word and Excel that enables users to encrypt specific parts of the document and spreadsheet eliminating the task of users maintaining multiple copies for different users. Based on the user role, only the authorized parts of the document can be viewed or edited.



LockMagic Client-less Deployment

In many situations users don't want to install any software on their local devices to encrypt and decrypt content. Lockmagic offers a browsed-based HTML5 solution that enables users to encrypt and decrypt content directly inside their web browser. All cryptographic operations are performed inside the client browser without any clear data ever transmitted over the network.



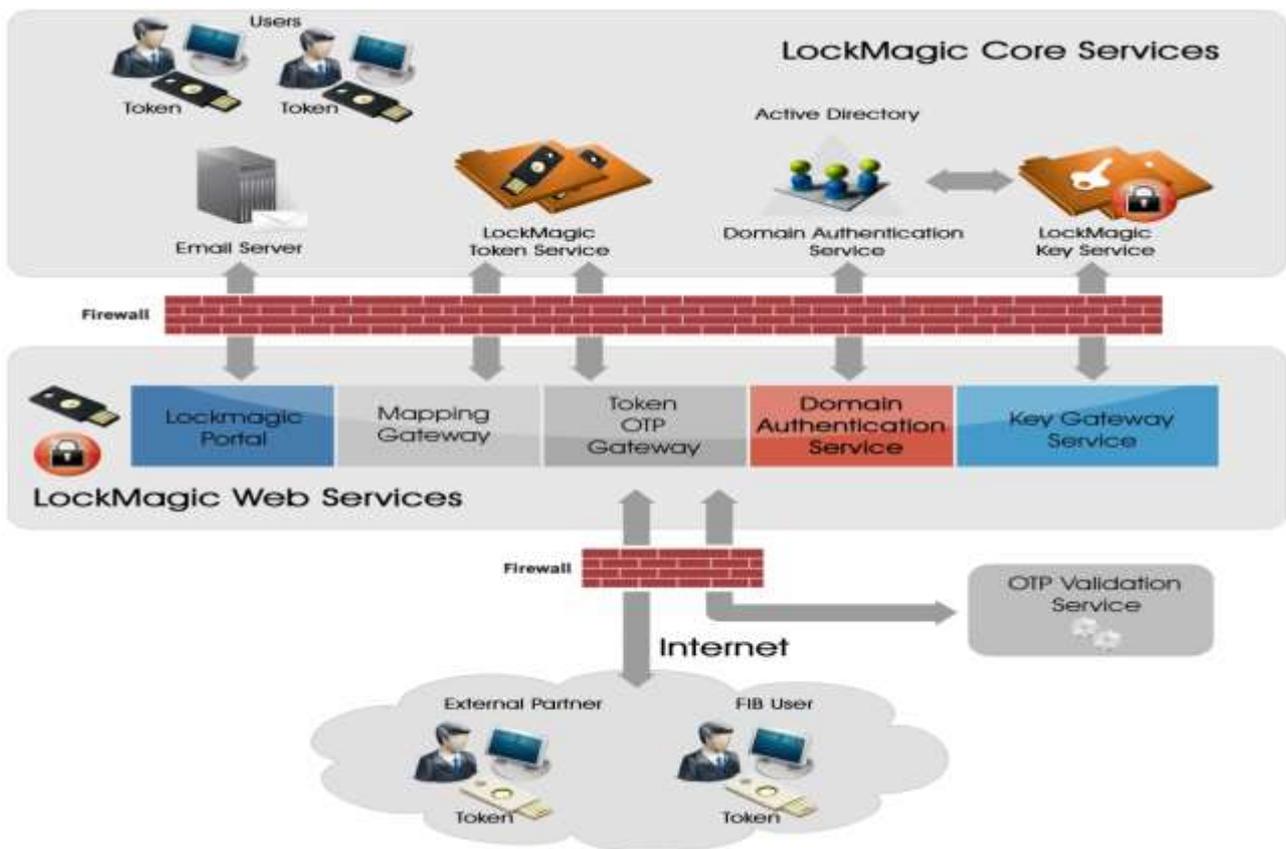
This feature simplifies sharing of secure content with partners and external users and eliminates the need to install client software. Furthermore, users have the ability to access secure content from mobile phones and tablets without installing any application.



LockMagic Strong Authentication

LockMagic integrates with two-factor authentication systems to require strong user authentication when accessing encrypted content. This ensures that high-value information remains protected beyond a simple username and password. Furthermore, LockMagic supports smart-cards and HMAC-based tokens for mobile encryption to ensure endpoint systems remain free from any user keys. The loss or theft of a laptop when LockMagic encrypted content remains secure because the laptop hard disk doesn't contain any keys or secrets that a hacker can then use to gain access to the encrypted content.

A single LockMagic hardware token can be configured for dual purpose to provide a One-Time Password for user authentication to the LockMagic Key Server and the same token along with a user-defined PIN and HMAC-SHA1 to derive a per-user master encryption key.



Enterprises can bind tokens to external partners and contractors private identities and grant them access to the enterprise LockMagic key server without provision identities in the enterprise identity system. External users can author, share and access encrypted content with enterprise users in a normal fashion. For example, a contractor may use his Gmail identity along with LockMagic hardware token to gain access to LockMagic encrypted content. This is achieved without any password or certificate management among users.

LockMagic Quick Features Summary

Core Protection



- One-Click encryption
 - Send encrypted attachments directly from windows explorer
 - Create and save encrypted content in 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 and without any client installation
 - Manage identity of authorized people by providing their email addresses
 - Create trusted groups for offline sharing
 - Create policy templates of authorized users and content control
 - Allow users to recall and activate secure content via LockMagic Content Manager
-

Secure Email



- Provide Microsoft Outlook 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 Office Suite



- Provide Microsoft Word /plug-in to encrypt partial and whole documents
 - Provide Microsoft Excel plug-in to encrypt individual worksheets or entire workbook
 - Provide user-defined password to encrypt content in addition to user identities
 - Provide content expiration on secure content
 - Provide viewer, editor and owner roles to control user access to encrypted content
 - Provide read notifications to content owner
 - Specify policies, list of emails addresses and certificates via templates
-

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
-



- LockMagic mobile application allows user to email encrypted messages, share encrypted files and access encrypted content using their mobile devices.

Cloud Encryption Service



- Allow users to send secure email messages using web browser
 - Allow users to access key service over Internet
 - Allow users to encrypt and decrypt files using web browser
 - Allow users to send and receive messages over web browser
 - Allow users to revoke access secure content using 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
 - Allow users to share content securely from Dropbox and Google Drive
-

Token Mapping Service



- Allow users register soft and hardware tokens online through self-service
- Authenticate users to services using one-time password from token or phone
- Use smart mobile phone as token using Google Authenticator App
- Single touch on hardware token to enter password
- Store encryption key on token protected with user pin for mobile and offline key
- Verifies token serial identifier to validate ownership based on registration
- Validates token against allowed devices using token serial identifier
- Accessible by internal and External users.
- Provides strong two-factor authentication
- Use different token colors for different configurations and roles

Additional Information

More Information can be found at <http://www.lockmagic.com/learn.aspx>