

# Secured eFile

Collaborative Access of Encrypted Files and Folders

Authors: Daniel Nilsson and Jeff Sherwood

July 21, 2011

## Content

Introduction – File/Folder Security Issues .....	3
The nightmare for IT security managers - employees .....	4
Compliance with laws and regulations .....	4
Secured eFile .....	6
Securing a file/folder – end user perspective .....	6
Changing access rights – empower the end user .....	8
Unsecuring a file/folder – end user perspective .....	9
Security travels with the file/folder - anywhere .....	9
Share and collaborate with external parties .....	10
Kill access rights when sharing data with external parties .....	10
EPM – Enterprise Protection Method .....	11
EPM central management .....	11
<i>Automatically assign access to users and groups</i> .....	11
<i>Limit who the end user can share secure documents with</i> .....	12
<i>Advanced directory management</i> .....	13
<i>Same document, several copies</i> .....	14
Encryption technology at a glance .....	14
<i>Encryption protocols and algorithms</i> .....	14
<i>The encryption process</i> .....	15
<i>The encryption procedure step by step</i> .....	15
<i>Cryptzone content encryption concept</i> .....	16
Key management .....	16
SEP (Simple Encryption Platform) Enterprise Management .....	17
Central management .....	17
Global Object Synchronization .....	17
Role based administration .....	18
System access rules and procedures .....	19
Seamless integration with existing infrastructure .....	19
Flexible deployment .....	19
Policy management .....	19
License management .....	20
Central password management .....	20
Deployment Architecture Diagram .....	21
Watch videos of Secured eFile .....	22
Summary .....	23

## Introduction – File/Folder Security Issues

Protecting intellectual property and sensitive information is a top security concern for any organization today. Co-workers need to share documents and files with colleagues, customers and partners on a daily basis, and frequently those items contain confidential information.

The issue for IT is that “we want to give easy collaborative access, but we also need to protect the confidential information”. IT staff must ask hard questions regarding security, even though they may not be security experts. “How do we provide collaborative access to files/folders, but at the same time ensure that only those people who need to access the stored files/folders have access rights?” “What happens when an individual or a group of people needs immediate access to a secured file/folder: who manages the access rights, can access rights be arranged in advance, can access rights be managed centrally as well as at the endpoint?”

Sensitive information is stored in many different environments and comes in many different flavors. So another question to ask is: “How do we protect a file/folder when it’s on a network-shared drive, copied to a user’s desktop or put on a USB flash drive, or emailed to several people?”

Collaboration is a hot topic and a growing trend for businesses throughout the world.

Collaboration is a hot topic and a growing trend for businesses throughout the world. Companies realize that people working together have a multiplying effect on user productivity. Another challenge arises when you have an employee working on a secured file/folder and they want to share the file/folder with a customer or partner who doesn’t have your encryption software. What needs to happen? How do you solve that problem?

Some companies don’t host their own servers. How can they provide security for their files/folders using encryption when a different company is hosting their servers?

And the most important question that should be on security professionals’ minds is “How do we deal with Regulatory Compliance, especially in a collaborative environment?”

Governments throughout the world have determined that when businesses encrypt, they have created a “safe harbor”. In other words, if there is a data breach there are no penalties or requirements to advise “injured parties” that sensitive information has been lost. Laws & regulations now mandate companies to encrypt information. If they don’t, then the fines, penalties and legal expenses are punitive!

The overall cost of non-compliance is significant because the liability is more than just a fine. The greatest impact is on the overall value of the corporation in the stock market and on corporate revenues. The questions set out above, as well as others, are important and require a comprehensive answer.



30% of organizations have experienced malicious theft of data by employees.

## The nightmare for IT security managers - employees

The Worldwide State of the Endpoint Survey 2010 by the Ponemon Institute<sup>1</sup> claims that over 60% of companies lose sensitive data as a result of negligent employees. 50% of the companies interviewed indicated that work flow and security training was the biggest challenge to preventing data loss and protecting data against new security threats. Also the study found that nearly 30% have experienced malicious theft of data by employees, evidence of the growing insider threat in the recession as more people have lost their employment. Now IT managers are worried about what data recently terminated employees are taking with them, especially on portable devices not owned by the organization!

The biggest threat is not the traditional cyber-criminal writing malicious code in a virtual location, but trusted employees sitting within or working outside of corporate walls. Employees represent a significant risk factor as they are privy to the organization's information and within arm's reach of that data. Knowing that infrastructures and perimeters have been fortified, sophisticated cyber criminals have begun to target end users as the entry point into an organization's network.

More than two in five office workers admit to taking sensitive data with them to a new employer when they leave a job.

A survey made by Cyber-Ark<sup>2</sup> of 600 office workers in London and New York focused on the lack of ethics and security within the workplace. While 85 percent of the respondents admitted to knowing that downloading corporate information from their employer was illegal, a quarter of those surveyed said they would take the data regardless of the penalties.

## Compliance with laws and regulations

HIPAA HITECH Act, GLBA, BASEL II, SOX, California SB 1386, EU Data Protection Directive,

Many organizations now fall under the oversight of government and industry regulations that mandate control over private information, including HIPAA in healthcare, GLBA and BASEL II in finance, Payment Card Industry DSS standards, Sarbanes-Oxley for financial and general business activities and Red Flag Rules for finance and consumer protection. Additionally more than 42 states in the United States have passed data privacy or breach notification laws that require organizations to notify consumers and businesses when their sensitive information may have been exposed. One high-profile example is California SB 1386. The EU Data Protection Directive was first introduced in 1995 and has since been updated and implemented by all member countries.

As recently as September 24, 2009, the United States announced the HIPAA HITECH Act that provides a "safe harbor" for Protected Health Information. A safe harbor is created through the use of encryption technology to achieve the goal of protecting sensitive and confidential information. The significance of the new law is based upon the United States Government's desire to mandate a conversion of patient records from paper to electronic format. This is expected to provide significant cost savings in the management of health records and the US Government is paying for the cost of conversion. The issue is that providing information workers with access to electronic records delivers sensitive information to people who should not have access to the information. The new law specifically states that ePHI (electronic Protected Health Information) must be either encrypted or destroyed. There are no other options. The first violation would be a \$10,000 penalty for each occurrence and a maximum of \$250,000 per year and can increase to \$50,000 with a max of \$1,500,000 per year.

<sup>1</sup> [www.lumension.com](http://www.lumension.com)

<sup>2</sup> [www.cyber-ark.com](http://www.cyber-ark.com)

The Gramm-Leach-Bliley Act (GLBA) has already had an impact on financial services organizations. Federal agencies are grappling with the Federal Information Security Management Act. Publicly listed companies are looking at what role information security will play in assuring their internal controls, as required by the Sarbanes-Oxley Act Section 404. Companies that do business in California are sorting out SB 1386, which requires them to have processes in place to notify customers whose personal information has been compromised. Yet no other industry has done as much to comply with such regulations, or been as open about their compliance efforts, as the healthcare industry. Most CIO's are complying with HIPAA HITECH, California or New York State Privacy Law and Sarbanes-Oxley because the potential impact to their businesses could be traumatic.

The Health  
Insurance Portability  
and Accountability  
Act

The Health Insurance Portability and Accountability Act of 1996 was passed by United States Congress to improve the efficiency and effectiveness of the health care system, and reduce the incidence of fraud. There are three components of the basic security rule - confidentiality, integrity and availability of electronic, protected health information. The focus of this policy is to increase the secure automation of patient records and electronic health care information transfers. With the advent of automated health systems there are increasing numbers of transfers of information between users, which poses more security and privacy risks – risks that have never existed before. In recognition of this, the drafters of this legislation included provisions for the regulation of information privacy and information systems security. Additionally, "Access Control" provides users with rights and privileges to access and perform functions using information systems, applications, programs and files.

EU Data Protection  
Directive

The EU Data Protection Directive (Directive 95/46/EC) has been implemented by all member states and the purpose is that "Everyone has the right to respect for his private and family life, his home and his correspondence." This regulation applies to any operation involving personal data including collection and storage of the data. The directive requires organizations to handle all personal data in a manner that is secure and appropriate. More information can be found on the following location: [http://ec.europa.eu/justice\\_home/fsj/privacy/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm)

## Secured eFile

Secured eFile enables people to share files and folders securely with individuals and groups inside and outside the organization. The easy-to-use file encryption tool empowers users to secure the information and indicate precisely who else in the organization needs access. A central management console allows administrators to deploy security policies across the organization, while built-in technology takes care of managing access rights, user authentication and encryption keys. With Secured eFile you ensure that information is accessible to the users, customers and partners who need it, and protected against those who don't.

### Securing a file/folder – end user perspective

The success of any application lies in its ability to fulfill the end user's request for a simple task to be done. At the same time the application needs to have the depth and flexibility to satisfy the user's more complex needs. In other words it has to be easy to use but comprehensive enough to work in their business environment.

When an end user wants to secure a file or folder, he/she simply expands the contextual menu. The interface will show four choices:

1. Secure "file/folder name" - Will encrypt the selected file/folder at once.
2. Secure "file/folder name" as copy - Will create a copy of the selected file/folder and then encrypt the copy at once.
3. Send "file/folder name" to eFolder – Will send the selected file/folder to an encrypted folder of the user's choice (a list of secured folders on the computer will be listed automatically).
4. Send "file/folder name" as a copy to eFolder – Will send a copy of the selected file/folder to an encrypted folder of the user's choice (a list of secured folders on the computer will be listed automatically).

Figure 1

The picture shows the contextual menu the end user gets when right-clicking a file/folder. Here the end user can select one of the 4 different choices.

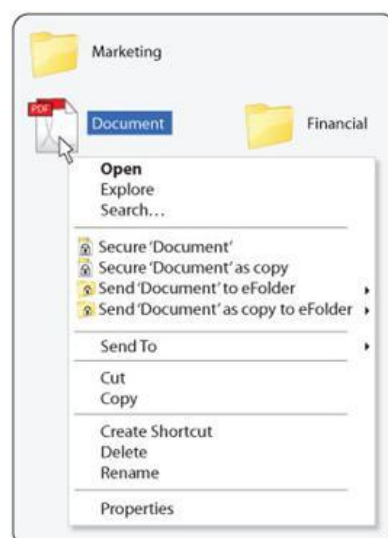


Figure 1

If the user selects choice 3 or 4 the file/folder will be secured at once. If the user selects choice 1 or 2, an "Access Rights Wizard" will launch and the user will be asked to set up access rights for other users. The security concept is that the access rights of a file/folder are created at the point of encryption with the default access rights being limited

to the user who created the file/folder - the File/Folder Creator. The File/Folder Creator will then have the choice of adding access rights for other users and groups (within the organization's Active Directory®).

So why doesn't the file/folder simply inherit the access rights from that group? Many laws and regulations state that access to files/folders containing sensitive information should be limited to as few individuals as possible. Therefore, Cryptzone believes that encryption software should empower the end user to add access rights to each file/folder they create. Secured eFile forces an action to add access rights and therefore ensures that only those who should have access will actually get access.

Figure 2

Access Rights Wizard – Here the end user can add unique access rights to a file/folder.

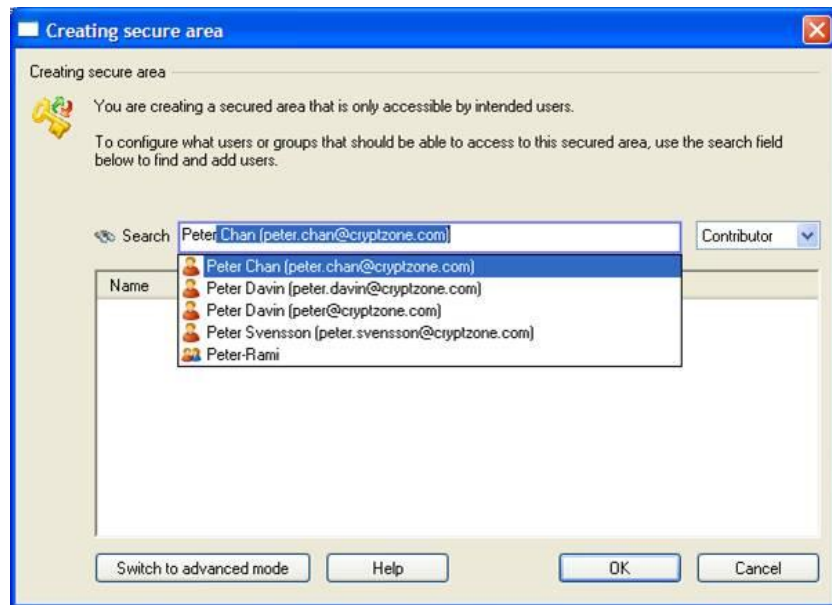


Figure 2

Figure 2 shows an example of how an end user can add access rights to a file/folder by simply typing the name of an AD user, AD group, created group or Secure Group.

Figure 3

Access Rights Wizard – Several users and groups can now access the file/folder.

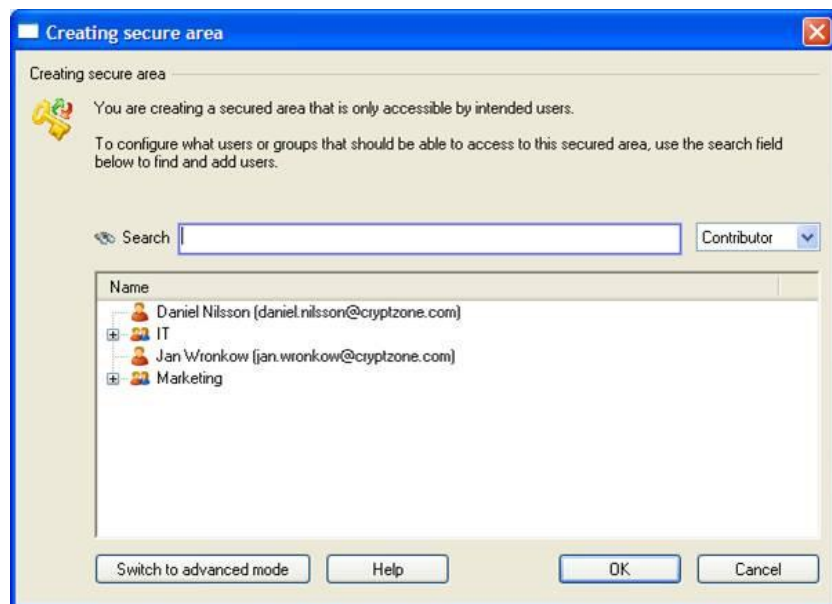


Figure 3

The administrator of the Secured eFile solution can centrally set up "sharing rights" for each user or group of users. As an example, it is possible to set up Secured eFile so users in the Human Resources department can only add access rights for other members of Human Resources.

When the user has finished adding access rights, he/she simply presses "OK" and the solution will finish the encryption process of the file/folder. When a file/folder is encrypted, the software will add a "key" symbol to the icon of the file type to show that it is secured. This is a very important feature since it will clearly show the end user which file/folders are secured.

Figure 4

The interface – It is easy for an end user to see if a file/folder is encrypted and secured. An encrypted file/folder has an icon with a key over it.



Figure 4

### Changing access rights – empower the end user

An important part of the Secured eFile solution is the possibility for an end user to change access rights to any file/folder.

Figure 5

Access Rights Wizard – When changing access rights, the wizard will show an advanced view making it possible for the end user to add and remove access rights and access roles.



Figure 5

An end user can only change access rights to a file/folder that he/she has created or where the user has administration rights to a file/folder created by someone else. The Access Rights Wizard can be reached by opening the context menu for a file/folder and then choosing Change Access. These rights can be administered centrally or at the endpoint.

Once the Access Rights Wizard is open, the user will be able to see all the users and groups that have access to the file/folder and will be able to add or remove users and groups. The user can also add one or several manual passwords for external sharing of the file/folder. If a group has access rights, the user can expand the group and see who the members are. This feature is especially important since it allows the user to verify the members of a group so that access rights are not inadvertently granted to the wrong people. In a large organization, the end user has to trust that IT administrators and security managers will create functional groups that will meet their needs. With Secured eFile, the end user is empowered to make the secured group decision and set the exact access rights that are appropriate for a specific file/folder.

For every user and group it is possible to set different Access Roles. The concept is to give the advanced users more alternatives and empower them to control in great detail what others can and cannot do with a file/folder. The system has three different levels:

- **Manager** – The Document Creator is always the Document Manager and will be able to set and change access rights to the file/folder. It is also possible to configure it so that other users will also be Document Managers.
- **Contributor** – Any other user or group added will automatically be assigned the Contributor role. Contributors have access to the file/folder to read and edit. A Contributor cannot change access rights or unencrypt the file/folder.
- **Reader** – If a user has Read permissions, they will only be able to open the file/folder to read its content. The user will not be able to change the file/folder. Please note that a user with Reader privileges can still copy data from a file/folder and paste it into a new file/folder. The Reader Privilege only blocks saving actions for the currently opened file/folder but will not block the information being copied elsewhere.

## Unsecuring a file/folder – end user perspective

An end user can remove the encryption from a file/folder at any time. This can be done by opening the context menu and choosing "Unsecure". When a file/folder is unsecured, the encryption will be removed and the file/folder will be stored in an unsecure manner. Please note that only users with Manager Access rights are allowed to unsecure a file/folder.

## Security travels with the file/folder - anywhere

A file/folder rarely exists in only one location or in one version. Files/folders tend to live in many environments and as the files/folders evolve, old versions are saved for later reference. Additionally, end users love to save local copies of a file/folder or send the file/folder to colleagues internally using email.

To support this environment, files/folders secured with Secured eFile will be able to travel and be stored securely on shared network drives, FTP servers, application servers, desktops, laptops, USB flash drives, CD/DVDs and external hard drives. Another strong and important feature of Secured eFile is secure backup. If a backup of the file/folder is made, the backup copy will automatically be secured.

Secured files/folders are able to travel and be stored securely on shared network drives, FTP servers, application servers, desktops, laptops, USB flash drives, CD/DVDs and external hard drives.

## Share and collaborate with external parties

Secured eFile offers the ability for users to share and work with encrypted data both internally within the organization and with external parties like customers and partners. If a user needs to share data with an external contact, there are three ways for the external contact to be able to open the encrypted file or folder.

1. The receiver of the file/folder can download a free Secured eFile Reader. When the Reader software is installed the receiver simply double-clicks the file/folder and types in the password to open it. The password is created by the Document Creator and is communicated in whatever way they choose. For example the password can be communicated by phone, IM, FAX, a letter, text message, SMS, etc.
2. If you want to provide regular collaboration with the external receiver, it is possible to send the receiver an installation package and a license. The license can be managed using Cryptzone's Simple Encryption Platform (SEP) advanced license management system.
3. The third and final way is to create self-running, executable packages. End users can do this by right-clicking an encrypted file or folder and choosing to convert it to an executable. The executable can be placed on a CD/DVD, USB stick, etc. Secured eFile is one of the few solutions on the market where encrypted data can be opened and read from a CD or DVD directly. A password is created by the end user and communicated to the receiver. The receiver of the executable can then open, edit and save files/folders secured within the executable user interface.

## Kill access rights when sharing data with external parties

Secured eFile provides its operators with the capability to control and possibly kill access rights for any data that have been shared with internal and external individuals. The system can be configured so that the SEP client will be forced to sync with the SEP Server using an HTTPS connection. This means that the SEP Client will require internet connectivity to authenticate and access the data, enabling the synchronization of encryption keys, licenses and policies. Additionally, executable packages (without the client) can be controlled through the same method. The following are examples of how the software can be set up:

1. End users can create self-running executable packages that will require the receiver to authenticate using a username and password. The self-running executable package will connect to the central SEP Server to verify the authentication. It is possible for the document creator (end user) or the administrator to remove access for the external person at any time.
2. The organization can send a SEP Client installation package to customers and partners. The SEP client will be able to connect to the central SEP Server hosted and controlled by the organization. The customer or partner will then authenticate with the central SEP Server using a username and password that has been set up by the system administrator. The organization's users will be able to secure files and share them with the customer and partner. It is possible for the document creator (end user) or the administrator to remove the access for the external person at any time.

EPM is the security concept for how Secured eFile handles encryption keys.

## EPM – Enterprise Protection Method

The Enterprise Protection Method (EPM) is the security concept for how Secured eFile handles encryption keys. The EPM is initiated through the creation of a transparent encryption key by the client and by adding that key to a secured document. This encryption key is then saved and transparently sent to the server as a Global Object and distributed to the clients that will have access to the document.

The content within the document is secured with that key but the key will never be visible to the user. The only way to open the document is to retrieve the key from the server by authenticating as a user who is a member of the access list. This access list can be created by the end user and can also be centrally controlled. The access list can contain both users and groups. Users who are members of an added group will have access to the key as long as they remain members of the group.

## EPM central management

EPM can be centrally managed by policy within the Simple Encryption Platform (SEP) Management Console. It is possible to set up policy rules that control:

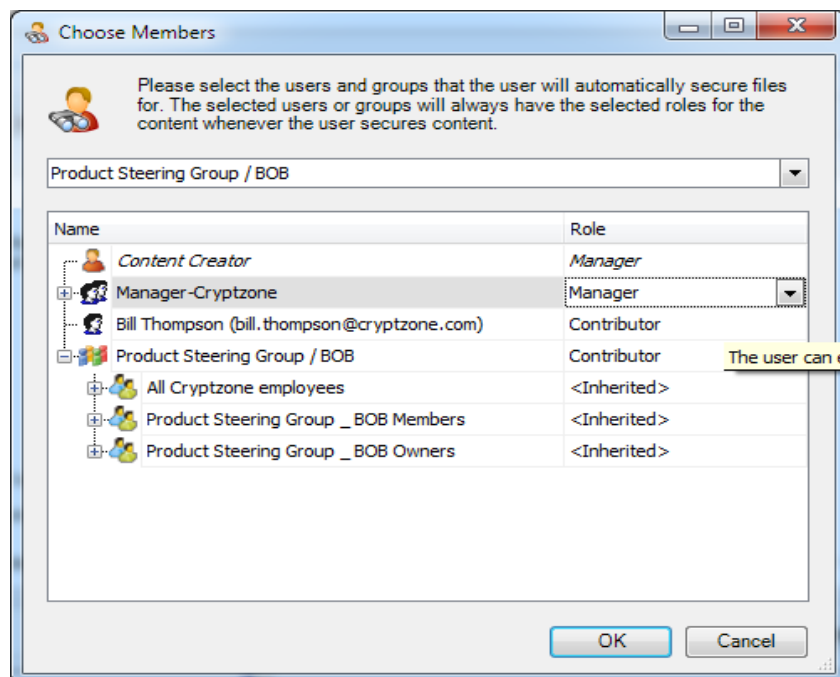
- If a document should automatically have access assigned to specific users and groups when it is secured;
- Which users, groups and passwords an end user can give access to when securing a document.

## Automatically assign access to users and groups

This option ensures that any document that is secured by the EPM Stealth Key also contains the default Active Directory users, groups and/or SharePoint users and private external groups.

Figure 6

The IT manager can easily assign access to users and groups. The picture shows the user interface where the IT manager can add users and groups that will get automatic access to documents secured by a user with this certain policy. In the shown example, the AD group Manager-Cryptzone and AD user Bill Thompson are added. In addition, a SharePoint site is added, ensuring that all members of the site will have access.



### Limit who the end user can share secure documents with

When this option is activated, the user will be asked - during the encryption process - to provide a list of users or groups that the document is intended for. It is possible to limit the choices the user has in this interface through the central policy. The user will be limited to the following (as shown below) based on the entities that are defined by the central policy.

- If a directory is set as a limit, the user can secure for the directory, or all the descendants of the group (children, grandchildren, etc.)
- If a group is set as a limit, the user can secure for the group, or all the descendants of the group (children, grandchildren, etc.)
- If users are set as a limit, the user can only add access rights to individual users and not groups.
- If a specific user is set as a limit, the user can secure for the specified individual user.
- If all entities are set as a limit, the user can secure for all directories, groups, users and Secured Groups including children, grandchildren, etc.
- If a Secured Group is set as a limit, the user can only secure for the selected Secured Group (not the children of the group). The user still needs to be part of a Secured Group for this to be allowed.

Figure 7

IT managers can limit who the end user can share secured documents with. The picture demonstrates how it is possible to limit different entities for the user.

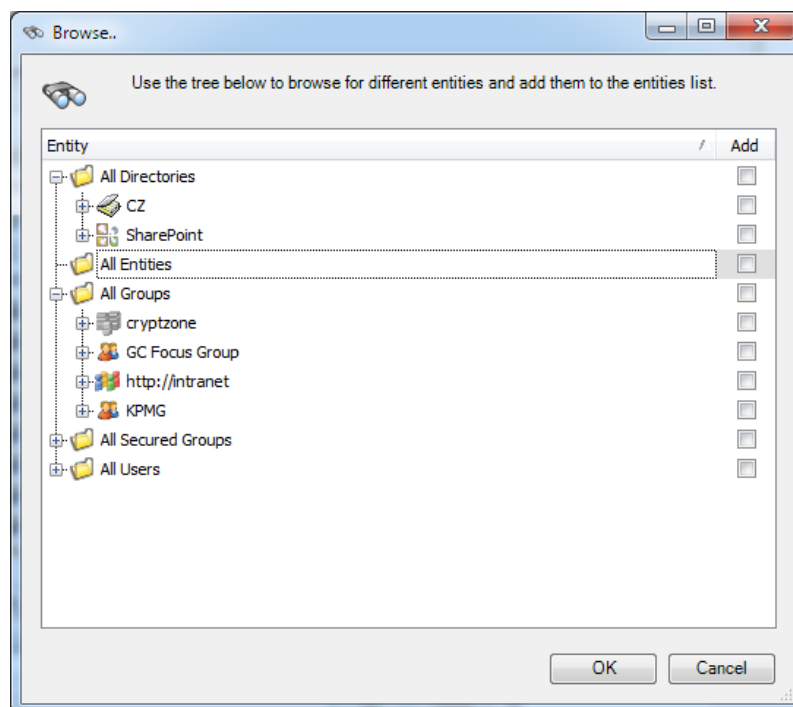


Figure 8

IT managers can limit who the end user can share secured documents with. In the example the user will be able to secure for all AD and SharePoint users and groups.

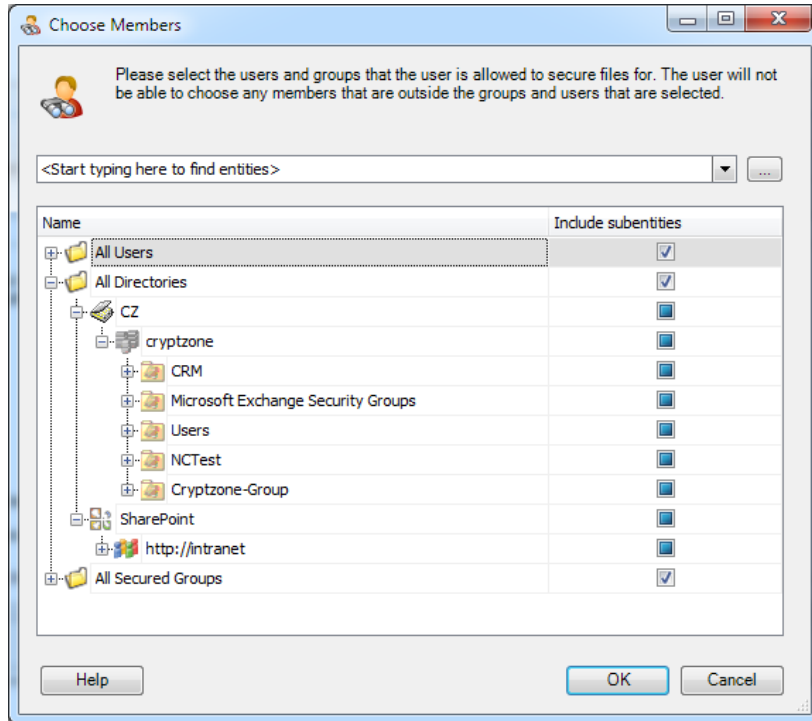


Figure 8

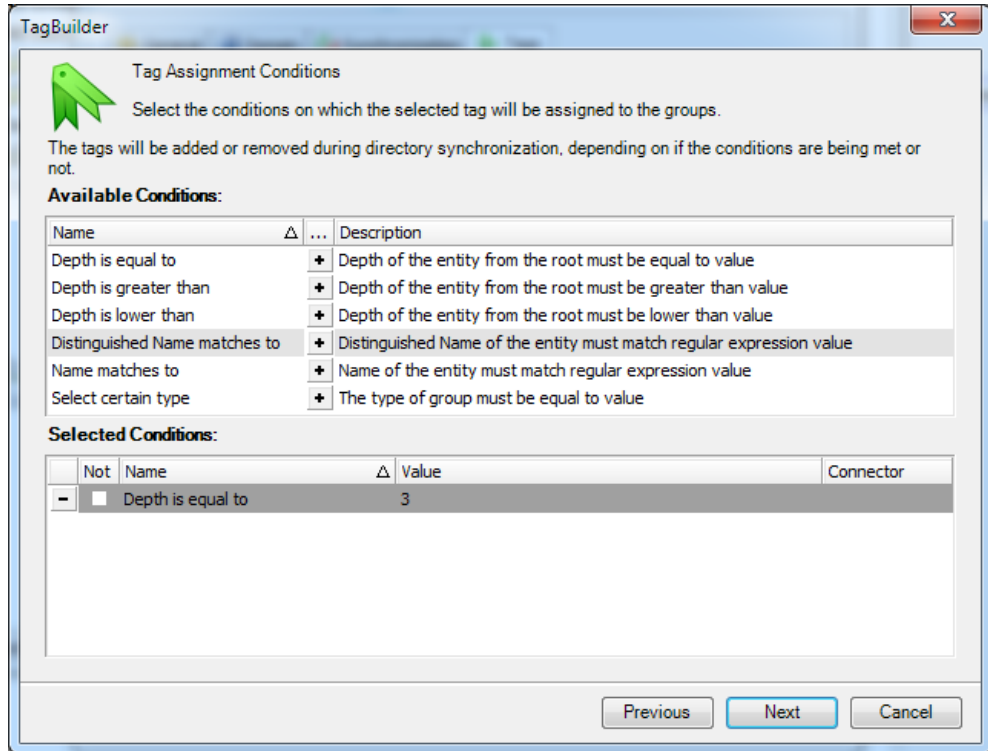
### Advanced directory management

For organizations with a large and complex user base, it is important to be able to set up smart rules. The SEP Management Console Tag Builder provides the capability to add tags to groups in Active Directory and SharePoint. The tags can be based on a group's position in AD and SharePoint, type of the group, name of the group or a combination of several influencing factors.

The following is an example of the ability to identify business units within AD using the tagging system. When the administrator is building access rules, the administrator can set rules based on the business unit tag.

Figure 9

IT managers can tag groups to make it easier to manage access rules.



### Same document, several copies

When a document is secured, it will be assigned a unique ID called the Global Object ID. The EPM Stealth Key itself is not part of the secured content. The secured content is merely referencing the document's Global Object ID that is holding the EPM Stealth Key and stored centrally. The benefit of EPM is that whenever secured content is copied, the Global Object ID will reference the same EPM Stealth Key and if the EPM Stealth Key is changed in a document, it will be effective for all the copies of the document that are referencing the same key.

Example: John secured a document and adds the groups Marketing and HR, and the user Jack to the access list. John emails the secured document to Jack. John then removes the group HR from the access list. Both the original document John has and the copy Jack has will have the group HR removed from the access list.

### Encryption technology at a glance

#### Encryption protocols and algorithms

The encryption of documents, files, folders, databases and client profiles are all done with an AES 256 encryption algorithm. The library used is Crypto++ version 5.3.0 which is a FIPS 140-2 validated library. More information can be found at <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm> under the company name Wei Dai, certification 819.

The communication between the SEP client and the SEP server is secured through a SSL tunnel encrypted with 128 bit AES.

Files/folders that are secured on a network shared drive and opened by the SEP client are always transported securely using AES 256 encryption to the local computer where they will be unsecured and displayed to the end user.

When a secured file/folder is moved to storage locations like CD, DVD, USB flash drive,

The solution uses FIPS certified AES 256 encryption algorithm.

network drive, email, and Microsoft Exchange, the file/folder will be secured using AES 256 encryption.

When a backup is done of secured files/folders, the files/folders will be stored encrypted using AES 256 encryption.

### The encryption process

All encryption and decryption takes place on the local end user client where the process is initiated.

### The encryption procedure step by step

The process starts with a client getting instructions to encrypt a file/folder.

1. A random 256 bit encryption key is generated.
2. The random key is encrypted with different extra keys, depending on the policy.

These keys can be EPM keys, private password, shared secrets from secured groups, master password, recovery password or custom passwords. The different passwords are hashed multiple times before encryption using SHA256 for brute force attack protection.

3. A key slot is generated for each key and the encrypted random key is stored in the key slots.
4. The file/folder content is encrypted with the random key generated in step 2.
5. Temporary files are wiped securely from disk and memory to remove possibility of indirect information leaks.

Figure 10  
Cryptzone content encryption concept

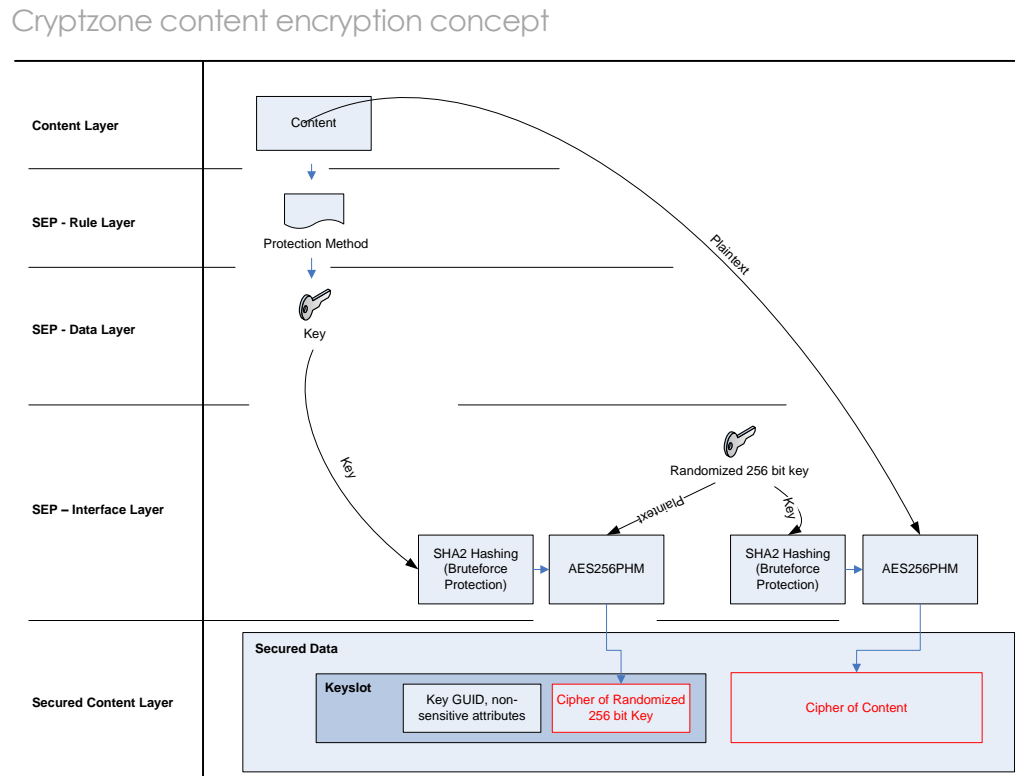


Figure 10

The encryption procedure is illustrated in the "Cryptzone content encryption concept". To better understand the concept map, note that there are actually two keys involved, one normal encryption key and one fully randomized 256 bit key. The randomizer uses a seed constructed from several factors including, but not limited to, processor tick count, user input and hashing and other hardware factors. With each new key the seed pool gets scrambled.

### Key management

Historically, key management within encryption solutions has always been an issue and an expensive solution to purchase and manage. Secured eFile is a fully automated solution. EPM Stealth Keys are automatically generated and synchronized between server and clients and there is no need for any kind of manual key management.

## SEP (Simple Encryption Platform) Enterprise Management

The SEP Management Console has been empowered greatly to fit larger enterprises with over 100,000 users. Focus has been on enhancing the member- and policy- systems, as well as a high-end security role system, MSI deployment features and a template design system.

Figure 11

SEP Management Console – Here the IT Administrator can manage users, groups, licenses, policies, security roles and secured groups.

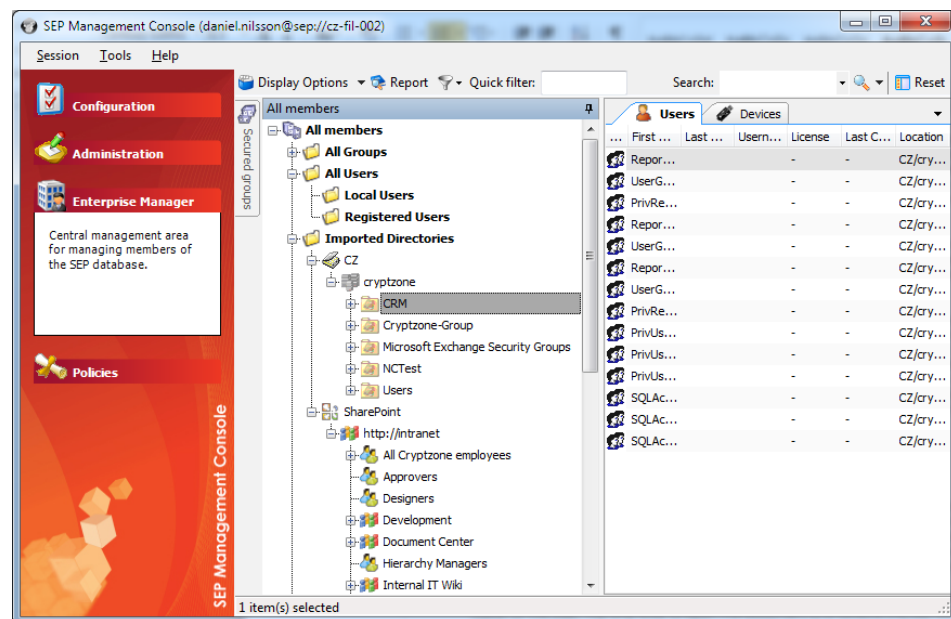


Figure 11

### Central management

The Enterprise Server centrally manages and enforces security policies for all Cryptzone products. It has the ability to create custom environments, specific settings and permissions for different groups as well as specific users and then to deploy this across the entire network. This managed system allows users to log in to an environment that is appropriate to their needs and consistent from one client to the next.

### Global Object Synchronization

The Global Object Synchronization is a very important building block in the Simple Encryption Platform and the concept relates to how the data objects and information within the SEP Platform are distributed between the components and users.

An object can be anything such as a security policy, a template, a specific privilege definition, a key object, a password, a licensing descriptor, a log file, or a shared secret. Each object represents a piece of information that together build and uphold the core values of SEP. Each object carries a unique Global Object ID and valid references to tell where it originates from. Every user is centrally associated to several global objects and as soon as a user connects with an SEP client, a built-in synchronization mechanism performs two-way synchronization to give the user access to newly created objects or existing ones. This is the quick overview but there are additional layers to the concept.

Each object represents a piece of information that together build and uphold the core values of SEP.

The SEP Server evaluates, based upon privileges, who should have each object and makes sure it gets distributed accordingly across the network.

Another example would be if a user encrypts a document, thereby giving it a new Global Object, additional objects such as keys and security attributes may be created and associated with it. The secured document references these objects by ID, and accessing components will use this information to give the end-user a potential access point. All users need to do is attempt to access the document - they will cryptographically gain access to it if the chain of objects referenced allows for it, and the key object is available.

Global Objects are generally created and handled within SEP. This means the synchronization processes in the system don't differentiate between the types of objects and they are treated in the same way according to a pre-set rule book. The SEP Server evaluates, based upon privileges, who should have each object and makes sure it gets distributed accordingly across the network. This process is transparent to end users and provides IT management with confidence that there is a strong audit trail and documented history of user actions and events.

Another value of Global Object Synchronization is that, regardless of how many policies, templates and encryption keys an end user has, the system can easily synchronize this data to any machine connected to the SEP server. A user can even have several machines with the software installed and use the software at all machines that share the same central profile.

### Role based administration

The platform allows for permissions to be defined for individuals and groups enabling a flexible, multi-tiered administration system with effective delegation of access rights and responsibilities through dedicated user-roles. The system comes with three predefined roles; Master Administrator, Administrator and Help Desk. These roles fits most organizations but can easily be modified for a better fit.

Figure 12  
Security Roles – The picture shows the Security Roles feature where it is possible to create different security roles for users in the SEP Management Console.

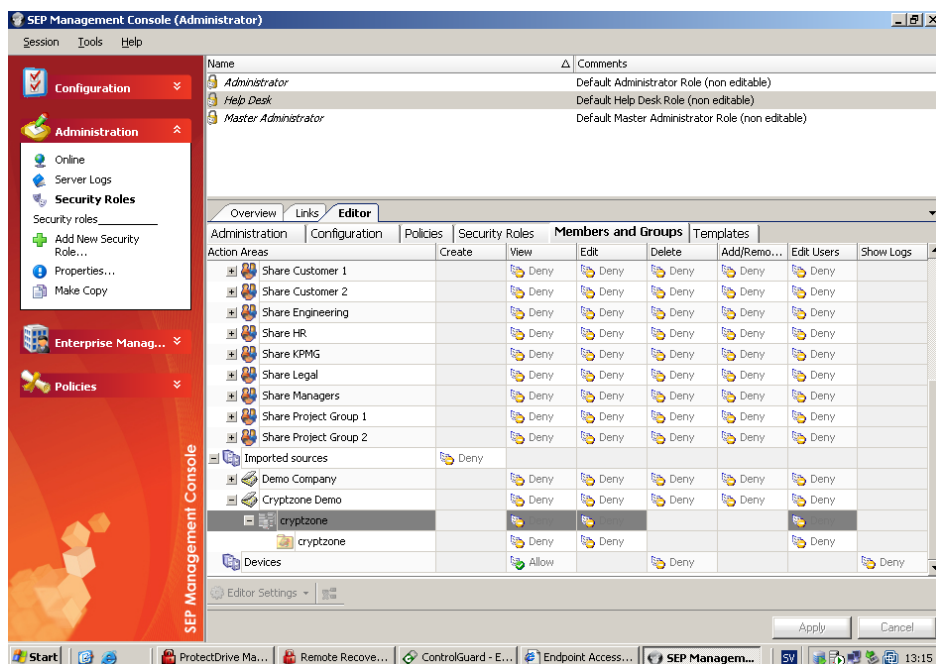


Figure 12

## System access rules and procedures

Client authentication can be customized depending on the need for user identity verification, from single sign-on (SSO) using Windows authentication to authenticating users every time a secured document is opened. SEP Server authentication can be either Windows authentication or user name and password. The roles assigned to the user then dictate what is possible to view, edit and create.

## Seamless integration with existing infrastructure

Leveraging existing directory applications such as Active Directory or LDAP functionalities, the SEP provides a one-way synchronization process to centrally administer security policies for user groups. The SEP is located on top of the existing infrastructure as a thin layer, designed to be flexible and extensible for interoperability with existing infrastructure.

## Flexible deployment

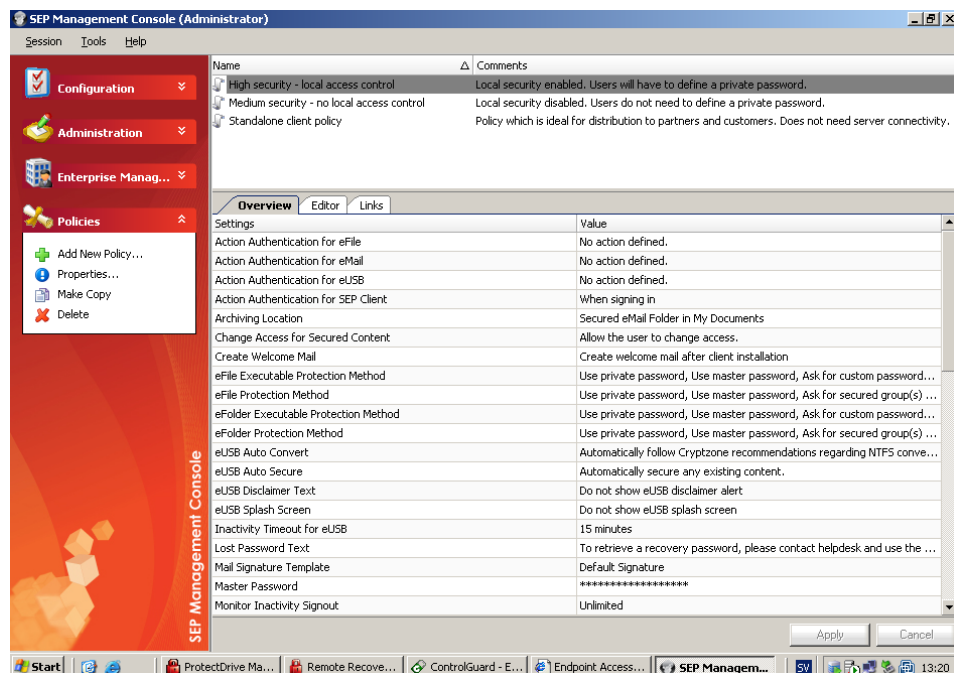
The SEP is designed to be able to run in multiple environments including as a managed service, hosted location and/or in the company's existing IT infrastructure. The SEP is delivered with the first encryption application, which allows organizations to quickly roll out new applications by simply downloading a new license.

## Policy management

SEP Management Console offers an easy and scalable way to deploy security policies and monitor security to ensure compliance. IT managers can centrally define, enforce and monitor information policies from a single, enterprise-wide console, ensuring a consistent policy across all users in the organization, or customized policies for groups within the organization.

Figure 13

Policy management – It is possible to create one or several policies and then deploy to users, groups and/or entire ADs. The system comes with ready to go policies created by Cryptzone Professional Services team.



## License management

License management has always been a problem for IT administrators. Questions such as "How many licenses do I have?", "Who has the licenses?", "Can I move the licenses to different users?", or "Do I have to buy new licenses for new employees?" are difficult questions to answer as situations changes.

The quota can be used and reused in both directions, i.e. removing a license from a user will move it back to the pot of licenses.

The SEP has a built-in license management system. How it works is that a customer buys a pot of licenses. The SEP is connected to Active Directory and uses the same structure and group names as AD. It is possible to delegate licenses to a user or a group during runtime. This in turn will automatically reduce the overall number of licenses. The quota can be used and reused in both directions, i.e. removing a license from a user will move it back to the pot of licenses.

With a few clicks a report can be created showing which licenses a user has, for which products, and when the user last used the application .

The licensing implementation also adapts to changes being made in AD and the system will automatically assign licenses to users as new ones get added, and remove licenses from users who have left the organization. This indirectly means that licenses can easily be moved around and transferred between users with a simple click action. Our license interface makes it possible to see how many licenses are left in the pot, and with a few clicks a report can be created showing which licenses a user has, for which products, and when the user last used the application. Also worth mentioning is that the licensing concepts are designed with ease of use in mind for desktop home users, flexibility in mind for SAAS- and ASP- providers, and scalability and manageability in mind for enterprises. Licensing should be a tool to control product accessibility within a company. Not a pain.

Licenses can also be issued on a temporary basis to external parties or consultants and then withdrawn upon demand. Depending on which license the user profile has included, the client will enable or disable the products dynamically.

## Central password management

Synchronizing user profiles to an SEP client also means giving access to secure groups, secure channels, EPM Stealth Keys and policy settings for passwords, which can be controlled through policies. Users can use Windows authentication or their SEP Password to access all encrypted data. The SEP Management Console will manage user rights and access to secured data using the infrastructure already invested in – Active Directory. If the organization doesn't have its own structure it is possible to use the SEP Management Console to create one.

## Deployment Architecture Diagram

The SEP solution consists of several components:

- SEP Server – Run as a service on the main server. The SEP clients connect and synchronize with the SEP Server to get updated policies, license and encryption keys.
- SEP Management Console - .NET based management application that can run on the server or at any desktop. This means it is possible to do management from any location of choice.
- Microsoft SQL Server – The SEP solution uses the SQL server to store all vital data like policies, license keys, users, encryption keys, etc.
- Directory Services – The SEP solution is connected to the Directory Services to read from the directory to organize users, groups and for authentication of internal users.
- SEP Client installation package – Generated inside the SEP Management Console and then deployed on any endpoint that should have the ability to encrypt emails.

Figure 14

The SEP solution deployment architecture diagram.

### Cryptzone deployment architecture diagram

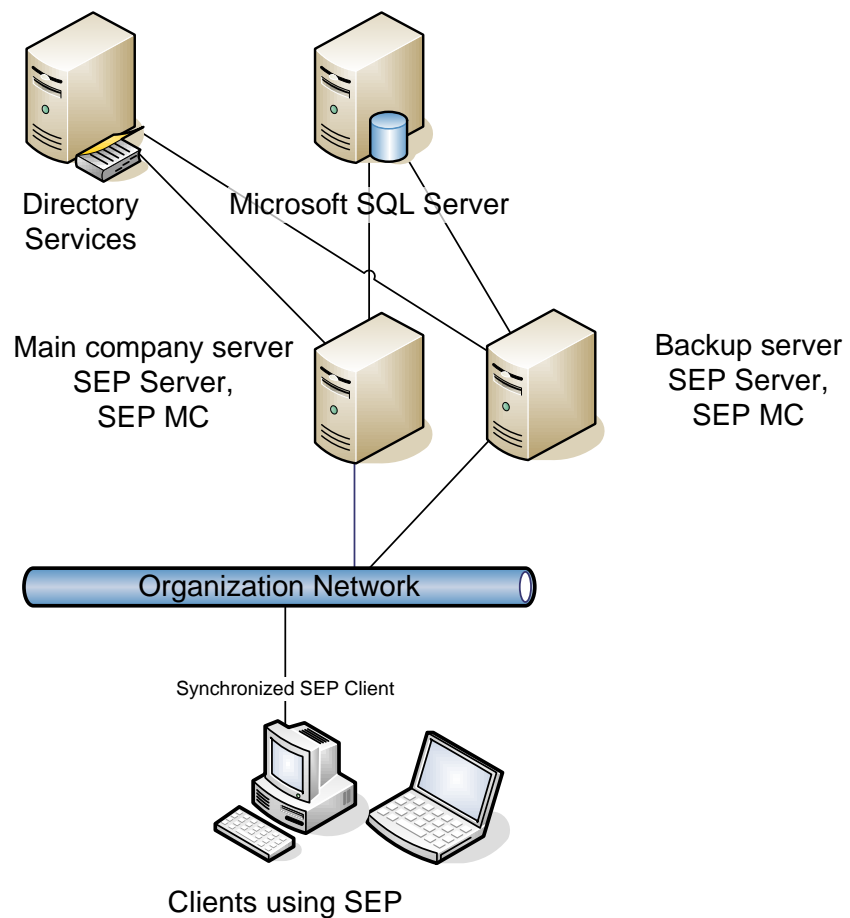


Figure 14

## Watch videos of Secured eFile

The best way to experience how easy Secured eFile is for both end users and administrators to please watch the following videos.



How to secure a file

<http://www.youtube.com/watch?v=iBrbLQ2SDHU>



How to secure a folder

<http://www.youtube.com/watch?v=4OZlxbB-u-4>



How to manage access rights

<http://www.youtube.com/watch?v=0Qk70hKbQjo>



How to create portable secure packages that can be shared with customers and partners

<http://www.youtube.com/watch?v=xQkysiEMFR4>



SEP Management Console - Roles manager

<http://www.youtube.com/watch?v=XuKU6DaIBNU>



SEP Management Console – License management

<http://www.youtube.com/watch?v=vURToitxgN8>



SEP Management Console – Manage policies

<http://www.youtube.com/watch?v=DDTk6iAhSVI>

## Summary

The intent of this document is to give the reader a thorough understanding of Cryptzone's Secured eFile solution. Collaboration will be the foundation of business in the coming decade but regulatory compliance demands file/folder encryption to protect sensitive and confidential information when "data is at rest". The reality is that it costs too much in penalties, loss of corporate value and the loss of public opinion not to secure sensitive data. Deployment of Secured eFile should be considered an insurance policy against significant financial liability.

We need to give information workers the tools to protect sensitive and confidential information. Secured eFile does exactly that. In the introduction, several hard questions for IT administrators were introduced. In this section we would like to take the opportunity to answer these questions.

Who should manage user rights?

**Question:** How do we provide collaborative access to files/folders, but at the same time ensure that only those people who need to access the stored files/folders have the "user rights" to do so? And what happens when we have a group of people who need access to a sensitive file/folder? Who manages the rights?

**Answer:** Secured eFile integrated with the operating system will offer the same collaboration services that the operating system does and enable IT and the creator of the file/folder to manage "user access rights". IT can create groups of people or departments that have access rights. A Document Creator can decide to add individuals, groups and departments before, during and after the creation of the file/folder.

How can files/folders be protected while being moved between different storage locations?

**Question:** How do you protect a file/folder when it's on a network-shared drive or moved to a user's desktop or emailed? Sensitive information is often stored in many different environments.

**Answer:** With the Secured eFile solution, encrypted files/folders carry user rights wherever they go. This protects them from when the bad guys try to access them.

How can we share secured files/folders with customers and partners?

**Question:** The users have secured files/folders and they want to send them to a customer or partner but the partner doesn't have your encryption software. What happens? How do you do it?

**Answer:** Well, there are a number of ways to transport an encrypted file/folder. The user can download the encrypted file/folder and attach it to an email and provide a link to a FREE Secured file/folder Reader. The second way is to download the file/folder and turn it into an executable file and then burn it on a CD/DVD.

Security and hosted servers.

**Question:** Many companies are using hosted servers. They have strong concerns about security and want to encrypt files/folders but how do you provide security when somebody else is hosting?

**Answer:** This is not a concern with Secured eFile. It doesn't matter where your servers are hosted. Secured eFile secures and un-secures on the desktop to make sure that no matter where the file/folder is secured or where it travels to it will be handled in a secure manner.

**Question:** How do we deal with Regulatory Compliance?

**Answer:** The SEP Management and Client solutions are compliant throughout the world with government legislation and industry regulations including HIPAA, HITECH, Sarbanes-Oxley, HIPAA, Payment Card Industry DSS standards, the EU Data Protection Directive and GLBA. For Cryptzone the most important thing is that our technology helps our customers meet regulatory compliance requirements. We use the strongest encryption method – AES 256 – as well as the Enterprise Protection Method (EPM). It is virtually impossible for anyone to hack files/folders when they are secured. All the user has to do is touch the “secure” button and everything else will be taken care of.

The Cryptzone Group is a technology innovator of proactive controls to mitigate IT security risk. We bring together the people, processes and technology to mitigate information security risks identified in the four key areas of Policy Compliance, Content Security, Secure Access and Endpoint Security. Headquartered in Sweden, the company has offices in the UK, USA and Poland, as well as an extensive partner network with more than 150 global partners. For more information about the company and its solutions visit [www.cryptzone.com](http://www.cryptzone.com) or contact us directly:

**Cryptzone Headquarters Sweden**  
Drakegatan 7, SE-412 50 Gothenburg

Tel: +46 (0)31 773 86 00  
Fax: +46 (0)31 773 86 01

**US Sales office**

Tel: 949.279.6177  
Fax: 212.898.1190

**UK Sales office**

Tel: +44 370 013 1600  
Fax: +44 370 013 1601