



Protecting Sensitive Data on Shared Networks

How to provide persistent encryption of confidential folders on corporate networks

June 2008

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

© Copyright 2008 Entrust. All rights reserved.

Table of Contents

1	Introduction	1
2	Reasons to Secure Information on Your Networks.....	2
3	Understanding Compliance.....	4
4	Traditional Methods: Client Versus Server	5
5	The Right Choice for Secure File Sharing.....	6
6	Entrust Entelligence Group Share	8
7	Conclusion.....	11
8	About Entrust	12

1 Introduction

While common security risks such as identity theft and online fraud attacks are top of mind, enterprises are also seeking solutions to secure and encrypt important files and folders, protect intellectual property and promote the sharing of information throughout an organization. Enterprises are aware of the immediate risks associated with exposing proprietary files and sensitive data on a shared network.

Products on the market today attempt to solve this problem, but don't provide the necessary protection without adding additional management inconveniences. All corporations use corporate networks as the primary means of collaborating. Even a slight change can have a negative impact on efficiency.

Past offerings have been difficult to manage, resulted in high training costs for administrators and did not provide persistent encryption — a method in which files or folders remain encrypted no matter where they are stored.

The need to comply with a number of industry guidelines has also been the catalyst for new file-sharing products. Coupled with the risk of customer data falling victim to theft and potentially resulting in lawsuits, a decline in brand reputation and the loss of consumer confidence has driven interest in these products.

Additional concerns stem from organizations wanting to separate network management from document ownership, specifically for those enterprises that outsource their IT services to a third party. Maintaining network management capabilities, but limiting access to designated files and folders, is yet another layer of security needed to protect sensitive data.

Entrust's new network folder encryption solution helps address these issues and provides a seamless product that offers automatic, transparent and persistent encryption of sensitive data stored on corporate networks. The solution possesses tighter control of authentication keys, has advanced audit capabilities and provides easy-to-use management for administrators.

2 Reasons to Secure Information on Your Networks

Organizations now face a myriad of technology issues and security concerns that were not a threatening reality years ago. Corporations, financial institutions, large retailers and government agencies must meet compliance standards, safeguard intellectual property, protect customer information and prevent data breaches.

Importance of Securing Intellectual Property

It's no secret that intellectual property is the livelihood of any organization or business. Protecting its value is paramount, especially when considering the manner in which technology makes it easier to access, view, manipulate, modify and transfer information. The compromise of trade secrets, proprietary information and customer data could potentially result in the loss of a company's competitive advantage.

Furthermore, corporations that outsource IT and network services could be at more risk to data breach or information leaks. Deploying a solution that does not limit contractors from performing their duties efficiently, but also secures the appropriate sensitive data, is key. These types of administrators need the appropriate access to manage the network, but don't necessarily require access to folders that may contain confidential information.

Implementing a robust network folder encryption solution can secure this information, as well as ease the concerns of clients, customers, stakeholders, vendors and third parties.

Guarding Your Business

The potential loss of business could be the overarching reason to, in fact, secure corporate networks. Maintaining the confidentiality of client and/or customer data should be the goal of each organization. The possible loss of customer confidence, decrease of brand reputation and the likelihood of law suits are all incentives to adopt a viable network folder encryption solution. While security breaches do happen — even to companies that have safeguards already in place — a pattern of vulnerability could very well sway both existing and potential customers to competitors who are perceived to be more secure.

Managing External Audits

Compliance mandates, not to mention compliance-based audits, are necessary functions to verify that organizations are doing their best to secure and protect sensitive data. Both client-only and server-client network folder encryption solutions have the capability to address these regulations — and the audits that may transpire as a result — but client-server solutions provide advanced auditing capabilities that can provide vital information when needed. Should an unfortunate breach of security occur, client-server solutions can produce a virtual paper trail of who accessed the data, when and from where, as well as identify which individuals may have modified access permissions. Traditional safeguards are not as secure and do not offer the same efficient, easy-to-use auditing capabilities.

Protecting PII

Network folder encryption solutions also address concerns regarding the protection of personally identifiable information (PII) — or personally identifying information — which is any piece of information that can potentially be used to uniquely identify, contact or locate a single individual. Information that is not generally considered personally identifiable, because many people share the same trait, include: common first or last names, general location (e.g., state or city), age, gender, etc. Moreover, multiple pieces of information, none of which are PII, may uniquely identify a person when pieced together to help form a single identity.

The U.S. Senate recognized the need to protect PII and proposed the Privacy Act of 2005 (S. 160), which includes laws that limit the display, purchase or sale of PII without the individual's consent. Another Senate bill, the Anti-Phishing Act of 2005 (S. 472, H.R.1099), will make it illegal to acquire or gain access to PII through “phishing” — the means by which an individual intends to acquire personal, sensitive information by imitating or masquerading as a legitimate business, corporation, organization or agency via electronic communication.

Like the need to safeguard customer data, the need to protect PII is to maintain consumer confidence, reinforce brand reputation and promote bottom-line sales.

Protecting customer data is much less expensive than dealing with a security breach in which records are exposed and potentially misused.

Gartner
“Data Protection Is Less Costly Than Data Breaches”
John Pescatore & Avivah Litan
September 16, 2005

3 Understanding Compliance

The threat of sensitive customer data being stolen, lost or mishandled has led to a number of compliance standards, including the Payment Card Industry (PCI) Data Security Standard, Sarbanes-Oxley Public Company Accounting and Investor Protection Act (SOX) and the Health Insurance Portability and Accountability Act (HIPAA).

These standards are solid guidelines to follow, but are not the only motivation to secure sensitive data and protect intellectual property.

The PCI Data Security Standard

In response to member, merchant and service-provider feedback on the need for a single approach to stronger information security for all card brands, credit card companies collaborated to create common industry security requirements known as the Payment Card Industry Data Security Standard (PCI DSS). Compliance with the PCI Data Security Standard is a requirement for all merchants or service providers that store, process or transmit cardholder data.

The PCI DSS consists of 12 requirements — often referred to as the “dirty dozen” — but only two specifically address the need to protect cardholder data. This pair of rules states that organizations implement a security strategy that will protect the stored data of individuals, as well as encrypt transmissions of cardholder data and sensitive information across public networks.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA), passed by Congress in 1996, seeks to protect the privacy and the security of health information. The HIPAA Security Standard covers the safeguards that should be implemented to protect electronic patient information. Organizations must ensure that private health information is protected both at rest and in transit.

SOX

The Public Company Accounting Reform and Investor Protection Act — known as the Sarbanes-Oxley Act (SOX) — is legislation intended to help reform accounting practices, financial disclosures and corporate governance of public companies. The SOX guidance suggests that organizations need to focus on reviewing the accuracy of financial information and the reliability of systems that generate it. Under the SOX guidelines, companies must demonstrate system and application integrity for tools used to generate financial reports. Verifying and restricting access to financial systems is a critical component of providing strong IT security for financial data.

4 Traditional Methods: Client Versus Server

Traditional network folder encryption solutions use client-only architecture. Unfortunately, safeguards derived from this technology are less secure, difficult to manage and require additional training for the administrators.

The latest development in client-server architecture is persistent, transparent and automatic, so there are no adverse effects on the end-user and administrator training is kept to a minimum. It offers easy deployment and also provides detailed records and logs of user and administrator activity.

Shortcomings of Client-only Solutions

Traditional client-only architecture solutions possess a limited feature set for safeguarding files and folders via encryption, but were the best method of performing the task at the time. Technology advances have made their shortcomings apparent and highlight gaps in security and manageability that otherwise may have been left vulnerable.

In a client-only architecture environment the keys used to decrypt the data are often stored within the folder or computer itself (as opposed to a centrally managed server). With this method, a group of end-users can use a private key to decrypt a file or folder that was encrypted using a public key.

Basic management of folder permissions is difficult. Updating permissions on a large group of folders is overwhelming. To amend access for even a single user would not only require touching each affected folder, but in some instances, re-encrypting the folder's contents as well.

As its name suggests, client-only solutions usually store the decryption keys inside each secure folder. Without a server component, individuals have unrestricted access to protected data when they're not connected to the network, thereby exposing the information to the threat of a data breach. Furthermore, there is no log or report of who accessed content in a given folder.

Advantages of a Centralized Server Architecture

In contrast to client-only solutions, client-server architecture stores all folder settings and decryption keys centrally on a server. This change in thinking allows efficient management of folder settings and decryption keys.

As the flagship feature of a client-server solution, folder administrators can add or remove users from a particular folder via the server and are not forced to modify each and every folder the user is associated with.

Additionally, this foundation allows for detailed logging and tracking of folder access for auditing purposes.

5 The Right Choice for Secure File Sharing

When searching for a network folder encryption solution, several factors should be considered. The majority of these parameters should fall in line with the overall strategy of the organization, its security goals and its technology environment.

Client-server architecture offers a broader set of options and features, including easy-to-use permission/access management, dynamic access and compliance-based auditing. Client-only architecture falls short in these areas, and is also difficult to manage within even small- to mid-sized environments.

While not a complete, comprehensive list, the following provides a baseline framework for beginning a search for a network folder encryption solution.

Network Folder Encryption Criteria

Factor	Description	Example
Centralized Management	The latest solutions include centralized management that offer easy-to-use options for administrators, and can help eliminate or reduce expensive training.	A new employee is hired and requires access to a group of encrypted folders. In one action, an administrator can modify access for folders the person needs, instead of changing access for each folder separately.
Ease of Use	The solution should be automatic and transparent, and not have an adverse effect on the user's work environment. End-users can easily collaborate and share information within the corporation, or with select third parties.	An end-user creates and manages folder access without the need to contact a network administrator.
Persistent Encryption	The inclusion of persistent encryption is a valuable feature that secures a file or folder no matter where it is stored.	A former employee has sensitive files on a USB drive at home. Encryption of the files remains intact, as his/her access is removed from the centrally controlled server.
Leverage Existing Workgroups	The solution should seamlessly integrate with the existing infrastructure for workgroup information.	Workgroups may already be defined in an Active Directory (e.g., global, sales or marketing).

Flexible Authentication	A sophisticated solution should support a variety of authentication methods, including Windows and digital certificates.	The solution could be integrated with other third-party hardware products for storage of digital certificates to enable multifactor authentication.
Compliance Requirements	The new technology must address the appropriate compliance standards, including PCI DSS, HIPAA and SOX, as well as protect PII.	The solution specifically addresses requirements to protect credit card holder data, as mandated by the PCI DSS.

Each network folder encryption solution offers unique feature sets that address an organization's security and encryption concerns. Selecting the solution that integrates smoothly with the work environment, is cost-effective and will adapt to future changes and obstacles is the correct choice for both short- and long-term security strategies.

6 Entrust Intelligence Group Share

The main objective of Entrust Intelligence™ Group Share is to promote the sharing of ideas and information without being burdened by security technology — or the shortcomings of past solution efforts. Entrust Intelligence™ Group Share introduces revolutionary encryption capabilities to an organization's workforce. No longer will data need to be encrypted for a fixed list of encryption certificates; information can now be encrypted for a shared public key. Users will be granted access to the corresponding private key, if appropriate, when the data is decrypted.

The Entrust Intelligence™ Group Share solution, which features patent-protected, client-server architecture, is transparent and automatic, and also uses persistent encryption to secure files and folders even if they exist on an external server, disk, drive or USB device. The file even remains encrypted when copied.

For example, a contractor has switched roles and had access changed from one group of folders to another. The contractor still possess a number of secure files — to which he no longer has permission to access — on a laptop. With persistent encryption, the files remain secure because the contractor still needs to authenticate with the server to access the files' contents.

Another benefit for the end-user is that Entrust Intelligence™ Group Share automatically encrypts all files moved or copied into a protected folder. Users are not asked to make a security decision and do not have to be conscious of the security when working with documents.

To address interoperability, Entrust Intelligence™ Group Share can extend outside the enterprise to allow the transfer and collaboration of information and sensitive data with partners, suppliers and third parties. Organizations often find the need to share a variety of documents, design plans, schematics or financial data. By granting specific parties access, Entrust Intelligence™ Group Share allows the collaboration of vital business assets without compromising security.

An industry-first offering, Entrust Intelligence™ Group Share is an innovative solution that is easy to configure and install, scalable, boasts logging/audit functions and includes useful backup capabilities.

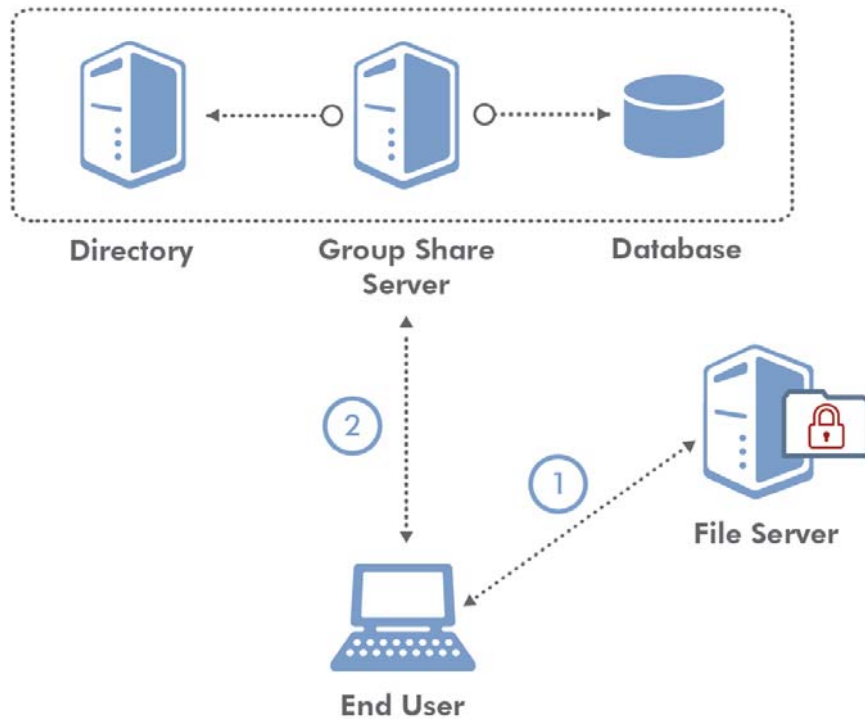
The Group Key Difference

Entrust's patented Group Key technology is the core of the Entrust Intelligence™ Group Share solution. It allows automatic encryption using shared public keys, but users must authenticate to the Group Share server before they can retrieve the corresponding private key to decrypt files. Decryption keys are securely cached locally on the user's computer.

For example, each folder uses a shared key to encrypt all files moved or copied into that folder. The corresponding shared private key is distributed to the specific list of users who have been granted access. This unique property allows an Administrator to change who can access the private decryption key, without touching the affected folders, or re-encrypting the folder contents. Furthermore, the files in the folder are encrypted and decrypted automatically when they are written to or read from a disk. File extensions remain the same, which allows users to continue working with documents as they did before.

How It Works

Entrust Entelligence™ Group Share allows a folder administrator to modify folder permissions instantly, without having to physically alter each and every folder. Permissions can also be changed on files after they are moved out of protected folders, as well as folders backed up offline.



Entrust Entelligence™ Group Share can easily leverage existing Windows groups stored in Active Directory, as well as user-created Group Share groups. This eliminates the need to re-encrypt files/folders when a user joins or leaves the organization. Group Share can restrict folder protection to administrators only, or allow end-users to protect and administer their own folders.

The Entrust Entelligence™ Group Share network folder encryption solution consists of two separate components — the Group Share server and the Group Share client. The server's responsibility is to manage and distribute shared keys to authorized individuals. The client performs all encryption and decryption locally, before sending the files to a network file share. The data is never transmitted over the network unprotected.

Optional Interoperability with a PKI Environment

The convenience of Entrust Entelligence™ Group Share is that it will seamlessly integrate with an existing public key infrastructure (PKI) environment, but is fully operational without one. Entrust Entelligence™ Group Share offers support for Windows authentication and X.509 certificates.

A PKI is designed to manage the digital keys and certificates that make up the digital identities required to transparently automate all security-related processes in an organization. The uses of PKI are varied and serve multiple purposes, but understanding their complexity can often be a daunting task. Within a PKI, a Certificate Authority (CA) is an entity that issues the public keys that verify and authenticate identities.

7 Conclusion

The protection of a customer data and a firm's intellectual property is the primary security concern of organizations today. The loss of customer data can cause degradation to a company's corporate brand, and result in lost consumer confidence and loyalty.

Existing network folder encryption solutions do not adequately address the problem of data breach. They are less manageable because folders must be updated, or contents re-encrypted, whenever permissions change. Some are less secure because they store the decryption keys inside the protected folder, thus making them susceptible to brute-force attacks. They also lack detailed auditing capabilities required to pass compliance-based audits. Collectively, these solutions are a burden on administrators.

Entrust Entelligence™ Group Share addresses these issues with its patent-protected Group Key technology. First, Group Share's Zero Touch Folder Administration allows administrators to change folder permissions without re-encrypting the contents of the folder. Additionally, all folder settings and decryption keys are stored in a centralized server, which reduces the risk of data breach by limiting the lifetime of decryption keys, and provides detailed auditing capabilities. The solution records all permission changes, as well as all attempts to access protected information. Group Share can produce reports that detail what folder was accessed, who accessed the folder, when and from where. This information creates a virtual paper trail that is invaluable during compliance-based audits.

Entrust Entelligence™ Group Share provides organizations with an efficient, manageable security solution that allows workgroups to collaborate and share sensitive information securely across corporate networks. This additional layer of security helps address various privacy standards such as PCI DSS, SOX and HIPAA.

Entrust Entelligence™ Group Share embraces the sharing of sensitive information for collaboration, and it does so by providing a number of cutting-edge security features only available in this solution. With the increasing number of data breach threats and corresponding privacy regulations facing organizations today, Entrust Entelligence™ Group Share is a secure, convenient and manageable solution.

8 About Entrust

Entrust [NASDAQ: ENTU] secures digital identities and information for consumers, enterprises and governments in 1,700 organizations spanning 60 countries. Leveraging a layered security approach to address growing risks, Entrust solutions help secure the most common digital identity and information protection pain points in an organization. These include SSL, authentication, fraud detection, shared data protection and e-mail security. For information, call 888-690-2424, e-mail entrust@entrust.com or visit www.entrust.com.