



A higher level
of IT-Security

Protecting Digital Assets

Full Disk Encryption White Paper

Abstract: Full Disk Encryption (FDE) is the safest way to protect digital assets, including both those of your company as well as your customers. If mobile devices such as laptops are stolen, FDE protects the information stored on them while also protecting a corporation's most valued asset: its intellectual property. By encrypting the entire hard drive, data is completely protected without requiring any user interaction, thereby increasing productivity and eliminating user error. Recent advances in FDE have enabled the use of hardware-based encryption, eliminating the need to use valuable CPU time for encryption, increasing performance, and maximizing security.

Table of Contents

1	Executive Summary	3
2	FDE – The Concept	5
	2.1 Secure with Hardware	5
	2.2 Secure Algorithms	6
	2.3 First Hurdle to Hackers: Pre-Boot Authentication	6
	2.4 Two-Factor Authentication	7
3	Business Benefits of Sector-by-Sector Encryption	8
	3.1 Goodbye to Idle Time	8
	3.2 Centralized Management	8
	3.3 Don't Panic!	9
4	Conclusion: Becoming FinallySecure	10
5	Glossary	11
	About SECUDE	12

1 Executive Summary

Maximum Security Is Based on Hardware and Software

- Dr. Sachar Paulus, Chief Security Officer, SAP AG

Our business environment becomes more mobile by the day: globalization has resulted in more travel, shared work spaces, and virtual home offices. Increasingly, companies are replacing desktops with laptops. The falling price of laptops and the integration of mobile personal digital assistants (PDAs) with the corporate IT infrastructure ensure a high level of acceptance for portable computers among users. Experts predict that mobile solutions will one day comprise a market share of more than 50 percent of the total PC market worldwide.

However, mobile devices pose a tremendous security risk: they can easily be stolen or lost, and confidential data can be disclosed. Both the widespread use of and vulnerability of laptops, PDAs, and mobile phones are readily apparent in the numerous high-profile losses that hit the news on an ongoing basis. Government officials and banks alike have had to disclose the loss of laptops containing critical confidential data.

Far worse than the relatively low cost of missing hardware, the loss or theft of a mobile device can have tremendous adverse repercussions for the image of a company. The lost data itself might not even be used maliciously: the mere fact of a security breach marks a company as risky and not under control, threatening an irreparable loss of image and trustworthiness. This is particularly fatal for companies if customer data such as credit card numbers, price lists, or confidential product information gets into the hands of competition. Current laptops have enough hard disk space to hold complete customer databases and often do in the case of salesmen.

Besides facing potential loss of image, companies face increasing pressure to comply with governance requiring measures to secure data. Internationally, laws like Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLB), Basel II, the European Data Protection Directive, and many others have tremendous impact on how data must be secured. SOX, for example, rules that only authorized users can change data for financial reporting. The auditor must ensure that this is really the case. The prospect of heavy fines and/or personal liability imposed on senior executives puts increased pressure on IT departments to ensure that data meant to stay in house stays in house.

With a Full Disk Encryption Solution (FDE), damage in the event of mobile device loss is restricted to the value of the hardware. Without proper access control — ideally using a smartcard or a small hardware token — the data on a hard disk remains secure and confidential, even if the hard drive is physically read bit-by-bit. Product roadmaps, customer data, social security numbers, contracts, prices, and much more are no longer at risk. The company's image remains unscathed and can even benefit, if a coherent and comprehensive security concept is utilized and proactively communicated to the market.

FDE is available in two main varieties, software-based and hardware-based. For existing systems, the software-based solution is best. This solution can be easily and quickly installed on a large number of computers and imposes no additional hardware requirements as the encryption is performed by the computers CPU. Hardware-based FDE uses an encryption processor installed on hard disks from specific manufacturers. This FDE solution performs somewhat better than a pure software-based solution; however, the cost of exchanging hard drives makes it truly suitable only for new laptops.

2 FDE – The Concept

Full Disk Encryption (FDE) prevents unauthorized access to data storage. Booting a system from a different media — e.g., a CD or a USB stick — typically leverages data protection mechanisms that are linked to the operating system. There is a range of bootable CDs, both Linux- and Windows-based, intended explicitly to access hard drives in computers. Full Disk Encryption renders this approach useless because the complete content of the hard drive is encrypted. Even if the hard drive is mounted in a different computer or — even more drastically — if somebody tries to read the data directly from the magnetic disk by opening the hard disk enclosure, the result is the same: documents, spreadsheets, presentations, even the operating system and all applications remain secure and protected against access and manipulation.

More than one way exists to achieve Full Disk Encryption. The fastest way is by implementing a pure software-based solution. Still greater security and performance are achieved with by combining this with special encryption hardware. SECUDE offers both versions with FinallySecure™.

For the software-based solution, a driver in the operating system ensures the protection of data. This driver is responsible for the continuous encryption of all read and write procedures. The driver supports the Windows operating system and works on any hardware platform. The advantage of such a solution is that it can be used on almost any computer. No prerequisites such as specialized hardware apply, and the computer does not have to be dismantled for installation. As such, FinallySecure™ as a software-based solution is ideally suited for existing systems that are out in the field already and must be protected by FDE. It even offers a choice of encryption mechanism. Depending on individual security requirements, the computer can be protected with Blowfish having up to 448-bit key length, DES with 56-bit, DESX with 128-bit, and AES with up to 256-bit.

2.1 Secure with Hardware

Software-based Full Disk Encryption is not without its disadvantage: it exacts high demands on computing power because the operating systems constantly reads and writes data to the hard disk even if the user does not open or save a document. This leads to higher processor loads and performance reductions for read and write processes. The processor typically must perform 8-10 percent more. However, in normal use this is imperceptible to the user. With computers engaged in intensive usage, the application start time may be slightly delayed.

Consequently, the combination of encryption software with encryption hardware is a logical extension of purely software-based FDE solutions. In its hardware-based version, FinallySecure™ supports hard disks that have a built-in encryption controller. This encryption processor bears the complete computation burden during the continuous encryption; the computer's main processor is freed from this burden completely. The positive side for the user is that operations involving applications and

data run without any adverse effects. Files are opened and saved as rapidly as they are without encryption.

Installing a new hard disk in a laptop already in use, including moving all the user data, constitutes a large necessary effort that may not be feasible or justifiable in terms of manpower cost. On the other hand, this form of FDE provides even more security than does the software-based version. With the software implementation, the parameters for encryption are known to the driver and the CPU, theoretically raising the possibility of an attack, even if this attack vector is highly unlikely. With hardware-based encryption, the encryption details cannot be accessed from the outside, being stored in a special memory space within the hard disk's electronics.

With software-based FDE, the initial encryption must be performed upon first startup, a process that can last several hours depending on hard disk size. Using FinallySecure™ with a supported hard disk, this task needn't be performed at all; the computer is protected as soon as the hard disk is mounted to the system and the encryption is always on. Considering the advantages and disadvantages of the two FDE methods, it becomes clear that only the combination of both the software and hardware version can accommodate an enterprise's entire computing environment of newer laptops with FDE hard drives and legacy systems without.

2.2 Secure Algorithms

The core of encryption security is the algorithm in use. The more complex the algorithm and the longer the key, the harder it becomes to break the encryption. The time needed to break high-security algorithms stretches into millions of years even when most modern cracking hardware is used. FinallySecure™ supports the Triple DES algorithm (Data Encryption Standard) with a 168-bit key length. Triple DES is an extended development of DES by Walter Tuchman, one of the original developers of DES, and still belongs among the very secure encryption methods. The DES algorithm uses an effective key length of 56 bits. Using Triple DES, the DES operation is performed three times in a row with three different keys, resulting in a key length of 168 bits.

The high computation effort required for secure encryption and decryption is not a burden if it is performed on dedicated hardware as a special processor on the hard disk. Hard disks in laptop-suitable sizes are available equipped with encryption processors supporting the more modern AES (Advanced Encryption Standard) algorithm with 128-bit key length. It is very important for companies wishing to implement an FDE solution that the manufacturer of the solution uses worldwide accepted standardized algorithms rather than their own proprietary methods. Only with openly available standards can built-in backdoors and undetected errors in the code be avoided.

2.3 First Hurdle to Hackers: Pre-Boot Authentication

With FinallySecure's hardware/software combination, hard disks start their initialization from a special 128 megabyte memory space. Within this space, an extremely secured and hardened Linux system

resides. The Windows partition is hidden at this time by the hard disk's hardware. Only if proper authentication is provided, the computer performs a soft reset and starts the proper operating systems from the data partition. The user needn't present further authentication credentials for the operating systems; FinallySecure™ uses the Windows credentials after authenticating with the FDE solution. Booting from a different source is completely ineffective as a means of bypassing the security.

The keys are saved by FinallySecure™ in an insular part of the hard disk that is externally inaccessible. SECUDE is an active member of the Trusted Computing Group and is currently developing an extension of FinallySecure™ to support TPM (Trusted Platform Modules) for additional security which can be configured by the enterprise administrator. TPM is an industry standard optionally used to store keys in an extremely secure memory area.

2.4 Two-Factor Authentication

Security involves a balance between ease of use and optimal protection. Extreme security measures fail if users perceive the solution as cumbersome and consequently boycott or attempt to circumvent it. Hence, convenience and ease of use are important features. The first level of security requires Windows credentials from the user to allow access to the system. To increase user acceptance, the credentials are handed off to Windows so they need be entered only once.

The high degree of security is achieved with authentication methods that work with two out of three factors: a password, a token, or biometric information. FinallySecure™ currently supports two factor authentication with a broad range of chip cards and USB tokens and will integrate fingerprint readers to allow three factor authentication for the highest level of security possible. Currently FinallySecure™ is configurable to opt between one or two factor authentication to provide enterprises with flexible choices of security level.

To authenticate with two factors, users must insert their cards or tokens in the reader and open it using their passwords; they are then authenticated based on their personal X.509 certificates. After successful authentication by FinallySecure™, boot-up of the main operating system starts after a soft-reset only.

3 Business Benefits of Sector-by-Sector Encryption

Technology should not be an end in itself. Purchase decisions should be made for solutions that contribute something to the company's success. This holds as true in the security arena as well as in any other, even if legislation defines — without considering the consequences for particular corporations — how business organizations are to protect their data. SECUDE's FDE provides a host of arguments for its use.

3.1 Goodbye to Idle Time

Productivity is a key business driver and hardware-based encryption that ensures very high throughput rates enables maximum end-user productivity. For a user this means that working with laptops is as fast and as convenient as ever — while being a lot safer. There are no involuntary lags when a large file is opened or saved, as can occur with software-based solutions.

Even though the hardware-based FDE solution is suitable for all laptops, many companies will not replace the hard drives in existing systems. In these cases, SECUDE recommends the use of the software-based FDE encryption that works without modification of the computer's hardware. From a user's perspective, both solutions are identical; there is no transition period if the user switches to a laptop supporting the hardware-based FDE solution. Even for the administrator the management is identical, since both versions use the same administrative processes.

Currently, FinallySecure™ supports the Momentus 5400 FDE.2 hard disks from Seagate. These fast laptop drives are available with 60, 80, and 160 gigabyte capacity, sizes ideal for corporate use. SECUDE is working with other hard disk manufacturers to support other hard disk models to provide customers with maximum flexibility.

3.2 Centralized Management

Centralized management ranks very high on the wish list of IT-managers. Security solutions are notorious for demanding considerable management effort due to a host of parameters and procedures that must be documented and logged. FinallySecure™ utilizes a different approach: this FDE solution is available as an MSI package, allowing it to be distributed and installed easy, such as via existing distribution methods such as Windows group policies. Since the users login credentials are the same as for Windows, separate management of these is unnecessary.

When a freshly installed FinallySecure™ application is first started, it boots up to the point of the Windows login screen and then waits for a username and password to be entered. Once these are correctly provided, the tool synchronizes them with the secure key storage on the hard drive. For configuration changes, a separate tool —Windows Credential Management — provides administrators with a graphical user interface to create scripts. Parameters, such as what algorithm is being used, are defined using these scripts in enterprise environments.

Furthermore, these scripts allow the Emergency Recovery Information (ERI) of each computer to be saved. With the ERI data, a lost key can be replaced and the data can be accessed. Windows Credential Management also allows the definition of group accounts on laptops, so more than one individual can log onto a single laptop.

The tight integration of this encryption solution with Windows credentials significantly simplifies the rollout and continuous operation of FinallySecure(tm). The hard drives need no preparation and can be used in the laptop immediately. The administrator always has complete control over FinallySecure™; arbitrary changes on the part of users or strangers are impossible. Administration can also be performed remotely via SECUDE's management console.

3.3 Don't Panic!

Strong encryption mechanisms are meant to protect against unauthorized access hence should be very difficult to crack. But what happens when employees forget their password or lose their tokens, perhaps while on the road, and are left without access to their most important tool: their laptops? Using a relatively simple challenge response approach, the Help desk functionality integrated into FinallySecure™ can unlock the system over the phone. The user reads off a numeric combination to the agent at the Help desk, the agent then enters it and reads off a cryptographically generated response key which the user can use to authenticate to the drive and reset his/her password. In addition, the helpdesk is integrated into the SECUDE trustmanager solution to provide the same functionality with the use of smartcards. This approach avoids the lengthy downtime of users unable to access their data or even having to cut short vital business trips.

At the same time, FinallySecure™ allows for easy decommissioning and secure cryptographic erase to make data permanently unreadable. News stories frequently surface about used hard drives holding confidential data being sold on eBay. Most are returned leased PCs with hard drives that should have been reformatted or destroyed. Using FinallySecure™, it is sufficient to destroy the key used to encrypt the data; a process that is virtually instantaneous. With software-based FDE, this method is not impenetrable since the data encryption key could be backed up by the central administrator. However, with hardware-based FDE, even with the data encryption key, the structure of data mapping on the hard drive is still securely locked into the protected area of the hard drive. Even a data forensics expert would have a nearly impossible task to correctly reproduce this information and assemble the data, even with the data encryption key. The information stored is digital white noise and permanently unusable.

4 Conclusion: Becoming FinallySecure

Full Disk Encryption is a mature security technology which provides risk management in terms of protection from data loss as well as compliance with government legislation. A well executed solution is an adaptive technology which can incorporate new technological advances and also ensures no productivity impact on the end user or IT administrator.

FinallySecure™ provides Total Data-at-Rest security with software or hardware based Full Disk Encryption. FinallySecure is the first step in End-to-End security, providing an Adaptive Technology with Risk Management and Productivity gains. This complete security umbrella protects against loss of data, fines from non-compliance, and destruction of brand value. In addition, end user transparency results in an ROI from productivity gains and FinallySecure™ allows for migration from single user to enterprise and software to hardware, all with central management. FinallySecure™ allows your business to survive, adapt, and grow in a heterogeneous IT eco-system.

5 Glossary

- **Asymmetric Encryption**

With asymmetric encryption, each user possesses a public and a private (secret) key. Documents are encrypted with the user's own secret key and the public key of the recipient. To make the document readable, recipients must decrypt the data with the public key of the sender and their own secret keys.

- **Symmetric Encryption**

Symmetric encryption uses the same key to perform both encryption and decryption. Maintaining security requires all users to keep all keys secret.

- **Two-factor Authentication**

Sign-on processes where users must prove their identity to an access technology with two out of three methods: something they know (a password or PIN), something they possess (a token or a chip card), or something they are (biometric data).

- **Biometric data**

Biometric data measures the "features of creatures." In modern information technology, biometric authentication refers to a technology that verifies a person's identity with at least one biometric feature against an authentication system. Currently, fingerprint, iris scan, voice recognition (e.g. www.voicetrust.com), and facial recognition are used. However other technologies are becoming available including lip reading and typing behavior.

- **Blowfish**

Blowfish is an encryption algorithm developed 1993 by Bruce Schneier using 64-bit block length and 32- to 448-bit key length. Schneier waived patenting the algorithm and allows free use of Blowfish. Blowfish is primarily intended to replace the aged DES algorithm. Currently there is no method capable of breaking a fully implemented Blowfish algorithm (16 rounds).

- **AES**

AES (Advanced Encryption Standard) was developed by two Belgian scientists and belongs to the most secure and widely used types of algorithms worldwide. After a standardization process lasting five years, the National Institute of Standards and Technology (NIST) accepted AES in November 2001. Until today (status 2006), AES can be cracked only with side-channel attacks. Secondary effects, such as the power consumption of the processor and timing differentials, are used for analysis.

- **DES**

The Data Encryption Standard (DES) was accepted in 1976 as an official encryption standard in the United States of America, and is in use in numerous products. DES nowadays is no longer used in up-to-date cryptographic solutions because its key length of 56 bits is considered too short and too easily cracked.

- **Triple DES 192**

A further development of DES (Data Encryption Standard), where a key with 192 bits is split into three keys of 64 bits each and then encrypted using a special process. If 3DES (the short form for this standard) is used properly, it is far safer than standard DES.

- **Key**

Typically a sequence of numbers and characters used for encryption and decryption of messages or data.

- **Token**

An item which identifies a user in some way. Traditional tokens such as signet rings or standards could be used to signal allegiance to one group or another. In cryptographic usage there are soft tokens, which represent a piece of data such as certificate used to authenticate, or hard tokens such as a smartcard or a special USB-stick. Besides the token itself, a pass phrase may be required to utilize the token. (See two-factor authentication, described above)

About **SECUDE**

SECUDE International AG, the end-to-end IT Security Products & Solutions Company, is a market leader in the areas of authentication & authorization, encryption, data integrity and the management of digital identities, delivering a higher level of IT Security to organizations around the world. The company offers solutions in single sign-on, role-based access control, and the security of documents, applications and transactions.

SECUDE is a member of IT SEC SWISS AG and was founded in 1996 out of a partnership between SAP AG and the Fraunhofer Institute in Darmstadt, Germany. This partnership resulted in the Secure Network Communication (SNC) module for SAP AG. The company is headquartered in Zurich, Switzerland, with a worldwide customer base and offices in the USA, Germany, Netherlands, Spain and United Arab Emirates.

For further information, please consult www.secude.com

Copyright

Copyright SECUDE International AG 2007.

SECUDE is a registered trademark of iT_SEC SWISS AG.

Seagate Technology and the Wave logo are registered trademarks of Seagate Technology LLC in the United States and/or other countries. Momentum is either a trademark or registered trademark of Seagate Technology LLC or one of its affiliated companies in the United States and/or other countries.

All other trademarks or registered trademarks are the property of their respective owners. And are mentioned herein only for clarification purposes.

SECUDE IT Security

Atlanta, Georgia

Sales: info@usa.secude.com

Technical support: support@usa.secude.com

www.secude.com