Full Disk Encryption

A cryptovision whitepaper

Version 1.0

cv cryptovision GmbH
Munscheidstr. 14
45886 Gelsenkirchen

+49-209-167-2477
info@cryptovision.com

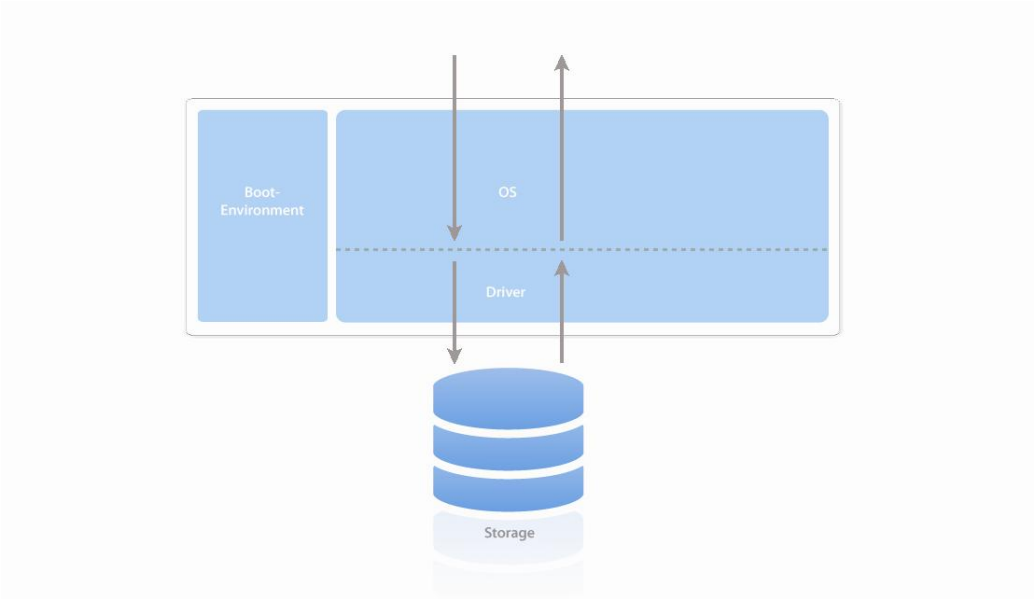
Full disk encryption increases the security of information stored on a laptop significantly. It helps to keep business critical data absolutely confidential. Moreover, full disk encryption helps to meet several legislative requirements. To secure the whole system it is necessary to use two-factor authentication based on smart cards. In case of similar requirements for folder encryption, a server-based solution together with smart card authentication should be used.

Working out of office becomes more and more important in today's fast developing world. Mobile workers spend most of their time on the road, in hotels, and on airports, always hunting for the next business opportunity. Laptops become the most important device – without such a computer their business would stop immediately. Business critical data like contracts with customers and customer information always have to be available. In most cases, the confidentiality and security of such data depends on the physical security of the laptop. If such a mobile device is lost, so is all data stored on it.

Many companies care for IT security of the laptops by using personal firewall and antivirus software to avoid data hijacking. But this doesn't help, if a computer is stolen, or an overtired mobile worker forgets it at the airport. A global study from 2006 shows that 60 percent of information theft is caused by stolen or lost laptops, while only 25 percent is connected to network intrusion. Due to this fact it becomes mission critical for companies to build up defenses by encrypting the whole hard disk.

Moreover, companies have to fulfill legislative requirements. Compliance to international laws like Sarbanes-Oxley Act (SOX), Basel II, the European Data Protection Directive, and many others have enormous consequences on data protection. According to SOX, for example, companies have to make sure that only legitimate users modify data for financial reporting. Such actions are subject to auditing. SOX increases the pressure on IT departments to secure and encrypt data, because a violation of the law might lead to heavy fine and even personal liability.

Benefits of encryption



Operating systems access storage mediums via drivers. The dat stored are usually not encrypted.

Full Disk Encryption (FDE) reduces the damage in case of losing a laptop to the price of the hardware. If FDE is secured by smart card, an attacker has no option to access confidential data. Such data remains encrypted even if someone tries to read every bit stored on the hard disk. Financial planning, customer data, contracts, and internal product information are secured and not exposed to any risk. A company can even use this security mechanism to improve the way customers recognize them by communicating the usage of FDE to the public.

Encryption on laptops eliminates the most significant dangers of data theft. After encryption of the data the result is unreadable ciphertext, which is worthless for any attacker. To make the data readable or accessible, it is necessary to decrypt using the unique credentials of the user stored on a smart card. If these credentials are only available to the user and therefore remain private it is impossible to gain unauthorized access to the data. A smart card provides the best basis to keep personal credentials private. Of course, instead of a smart card an equivalent microchip device can be used. For instance, USB tokens gain more and more popularity, because they don't require a card reader.

The most convenient credentials used on smart cards are digital certificates. A digital certificate can be thought of as a digital passport that is issued to a user. The smart card can be protected with a PIN (at least four digits). This means that possession (smart card) is combined with knowledge (PIN). Such a two-factor authentication provides the highest security level among all practicable authentication methods.

In order to manage digital certificates, a special component (Public Key Infrastructure) is necessary. A Public Key Infrastructure (PKI) is responsible for issuing digital certificates and for an appropriate certificate management.

Encryption on laptops with smart cards and digital certificates is especially attractive, if the smart cards are used for other applications, as well. For instance, an enterprise ID card can be designed as a multi-purpose token suitable for VPN access, operating system login, and physical access. Such an enterprise ID card considerably enhances both convenience and security. For every security mechanism it is important to observe the usability. A security feature might be very secure but it become worthless very fast if it is not accepted by users. Users are familiar with certain ways of doing their work. Implementation of extreme security procedures that

either change or hinder such processes completely will most likely lead to weak security. Users will try to avoid or boycott it. Therefore convenience is (beside security) another important feature of FDE. Having this in mind the best level of security is achieved by two factor authentication: a smart card and a PIN

Encryption options

There are two kinds of FDE available: hardware- or software-based. Software-based FDE is a good solution for existing hard disks, because it can be installed on all computers of a company by centralized software distribution. After initial encryption it works almost seamlessly on existing hard disks and existing data. If a company decides to buy new laptops it is most advisable to order hard disk with encryption feature. Such hard disks are ready for hardware-based FDE. This basically leads to faster encryption because it is computed by an encryption processor installed in the hard drive. The optimized performance is a real advantage of hardware-based encryption, due to the costs for such hard disk it is only feasible for new laptops.

During the installation FDE is placed between the hard disk and the operating system. The operating system does not write or read any data directly from the hard disk. Any data that is read from the hard disk or written to the hard disk by the operation system or any other application is handled by FDE. If data shall be written FDE receives such data from the operating system. Afterwards the data is encrypted before it is written to the hard disk. In case of reading data this works vice versa: encrypted data is read by FDE from hard disk, decrypted and afterwards transferred to the applicable application. This way of handling the data is a very basic security feature of FDE: There is no possibility to write unencrypted data to the hard disk, because neither the operating system nor any other application is able to communicate directly with the hard disk. FDE acts as a broker that encrypts and decrypts any data that is transferred to / from the hard disk.

After first installed on a laptop computer, FDE performs an encryption, where the entire hard drive is encrypted on a sector-by-sector basis.

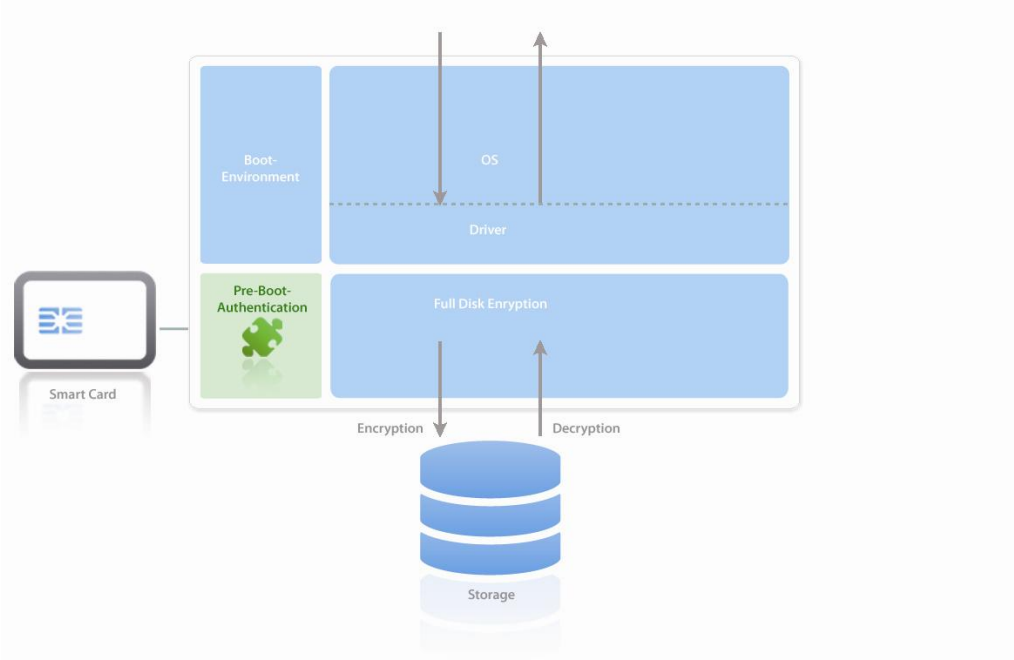
Every encryption is useless if the initial authentication can easily be forged. The optimum level of security is achieved with Pre-Boot-Authentication (PBA) together with authentication methods that work with two factors: a password and a security token like a smart card. All FDE products, which include integration of **cv act *sc/interface***, support two factor authentication. **cv act *sc/interface*** provides the connection between FDE and the smart card.

After switching on the laptop computer PBA is started before the operating system and presents a login screen to the user. The smart card has to be inserted in a smart card reader connected to the laptop and the PIN of the smart card has to be provided by the user. The credentials of the user that are stored on the smart card are used for authentication by PBA. If authentication fails the access to the laptop is denied and no data will be decrypted. After successful authentication the normal boot process of the operating system starts. During operation the encryption / decryption operations are computed transparent, no user interaction is needed.

Folder encryption

FDE is the best way to secure hard disk of mobile users. If very sensitive data stored on a file server have to be secured, the best way to meet this requirement is the usage of folder encryption. In such a case all files that are stored in a specified folder are automatically encrypted and decrypted when opened or stored in another location.

Folder encryption is most commonly used for company's human resources information. Folder encryption fits into such environment because it is also multi-user capable. Every employee of HR department can access such data. Nobody else should be able to access the data therefore every member of HR has to authenticate against the folder encryption software with smart card and PIN.



Full disk encryption can be combined with pre-boot-authentication.

For a group of people accessing the same (encrypted) data companies should think of a centralized enrolment and management of the certificates that are stored on smart cards. **cv act *PKIntegrated*** provides the necessary functionality for certificate management (generating certificates, storing certificates directly on smart card, certificate revocation and renewal).

cryptovision's solution

cryptovision provides **cv act *sc/interface***, the smart card middleware that integrates several smart cards and secures the connection between smart card and computer. **cv act *sc/interface*** is integrated into several FDE products, e. g. Secude FinallySecure, WinMagic SecureDoc and Utimaco Safeguard (information on additional FDE products available). It implements the PKCS #11 standard and includes a Microsoft Cryptographic Service Provider (CSP) as well as its own mini-driver, it can be integrated into nearly every application. **cv act *sc/interface*** is the first smart card middleware that supports ECC algorithms with a key length up to 521 bit. Additionally it is also possible to replace the PIN with a biometric trait, e.g. a fingerprint. Via the Match-on-Card Technology it is assured that sensitive data like a fingerprint is saved on a smart card and not on a PC.

In addition, cryptovision provides the PKI solution **cv act *PKIntegrated*** with highly sophisticated certificate management abilities, which covers the whole lifecycle of a digital certificate (certificate lifecycle management). **cv act *PKIntegrated*** supports an extensible variety of certificate formats, smart cards, certificate revocation lists, online certificate validation via OSCP, certificate registration via SCEP and a range of cryptographic methods and key lengths.

In contrast to almost any other PKI solution, **cv act *PKIntegrated*** was from the beginning not designed as stand-alone component, but as an add-on to an identity management system. This is a considerable benefit, because automated identity management is already in place in many corporations.

Through its nature as an identity management add-on, it is possible to combine identity management and PKI processes. Especially, the registration of new devices or users, the change of device or user attributes, and the deletion of device or user entries can be easily connected with certificate creation, certificate change and certificate revocation. As identity management systems usually contain an extensive set of connectors and drivers, which enable connections to most groupware and human resources solutions, virtually any data source can be

used as a basis for certificate lifecycle management with **cv act *PKIntegrated***.

In addition, the integrated approach **cv act *PKIntegrated*** follows has the additional benefit that it neither needs a user interface of its own nor a database nor additional protection, because all this is provided by the identity management system. **cv act *PKIntegrated*** is therefore a very lean and cost-effective solution.

Many customers use **cv act *PKIntegrated*** with the Novell Identity Management suite. There is a seamless integration of **cv act *PKIntegrated*** into the Novell eDirectory and the Novell Identity Manager (these two components are the core of the Novell Identity Management portfolio). However, **cv act *PKIntegrated*** also interoperates well with other identity management solutions, for instance with the Oracle Identity Management and the IBM Tivoli Identity Manager.

Conclusion

Full disk encryption provides a very high level of security and helps to meet legislative requirements for mobile workers. All data on a hard disk is encrypted and therefore protection of such data is optimal. No data is written unencrypted to the hard disk because all read and write operations are handled by full disk encryption.

cv act *sc/interface* together with smart cards serves as a two factor authentication that provides the optimum level of security for authentication against the hard disk encryption.

Folder encryption is used for information that have to be kept confidential and only accessible for a group of people. In such case security has to be optimized by using smart cards and **cv act *sc/interface*** for authentication.

For FDE and for folder encryption certificates stored on smart cards are managed by **cv act *PKIntegrated***, cryptovision's PKI product.

cryptovision

cryptovision is a leading supplier of innovative IT security solutions based on cryptography. The company specializes in lean add-on components, which can be integrated into nearly any IT system to gain more security in a convenient and cost effective way. Based on its 10 year market experience and broad background in modern cryptography – such as ECC (elliptic curve cryptography) – all cryptovision products continue to provide the most state-of-the-art and future-proof technologies. From small devices like citizen e-ID cards up to large scale IT infrastructures, more than 30 million people worldwide make use of cryptovision products in defense, automotive, financial, government, retail and industry.

References

For more details about cryptovision products refer to: www.cryptovision.com.