



FORT FOX FILE ENCRYPTOR: FFFE

Send secure files over any unclassified network. Safely.

The Fort Fox File Encryptor is a hardware device used to encrypt and decrypt data. An encrypted file can be subsequently sent over any unclassified network safely and with its confidentiality protected. Equipped with a special-purpose cryptographic chip, the File Encryptor has been approved by the Dutch intelligence service, AIVD, for transmitting encrypted classified information over the internet.

HIGH-SECURITY OFFLINE FILE ENCRYPTION

Several (governmental) organizations deploy non-interconnected, high-security networks spread over multiple physical locations. These organizations use file transfer to communicate with each other, across these separate high-security networks. Thanks to its hardware-based encryption, the high-security, offline Fort Fox File Encryptor (FFEE) enables encrypted files to be transferred in a variety of ways: including over the internet, as well as on CD or data stick delivered by insecure mail. More importantly, its security has been approved by the AIVD* up to level SECRET (or 'Stg. GEHEIM', according to the State-Secret Classification in the Netherlands).

TAMPER-RESISTANT

The File Encryptor is based on the Philips C-Kaart application and replaces the AROFLEX. The File Encryptor and its encryption and decryption functions are driven by both, hardware - in the form of the PCMCIA-type FFFE Card - containing the cryptographic core - and software, installed on

a laptop computer. The FFFE-Card's casing is also tamper-evident and the internal hardware tamper-resistant. Furthermore, its software performs multiple security checks to ensure that the system has not been tampered with.

SECURITY MANAGEMENT

Regarding security management, each organization has its own 'Security Domain'. Organizations can appoint, per Domain, managers who have the ability and permission to program new cards and define individual users and groups. Each FFFE Card represents a physical location/system and enables multiple users to work with the system in question. Creating security groups simplifies the security management procedure, made even easier by the File Encryptor management software. This software allows an organization to assign and manage user security and access to its various File Encryptor facilities.





| | |
|-----------------------|---|
| Encryption & security | <ul style="list-style-type: none"> • AIVD-approved up to SECRET Level (or 'Stg. GEHEIM', according to the State-Secret Classification in the Netherlands) • Fully hardware-based for optimal security and reliability • Housing is tamper-evident • Hardware is tamper-resistant • Only users selected at encryption time can decrypt the data • Integrity checks done on firmware, FFFE software and computer system files • Flexibility and full control over Security Domain management • Secure memory with emergency erase • Enforces Red/Black device security (preventing using Black devices as Red and vice versa) • Key updates can be sent over existing channels i.e. no physical transfer needed • Files can be encrypted files offline and then safely stored on memory stick, CD, floppy disk, or transferred over an insecure connection. • Any type of file can be encrypted • The maximum file size is limited by the Windows operating system encryption • Minimal increase in file size due to encryption |
| Hardware | <ul style="list-style-type: none"> • Based on the PCMCIA (PC-Card) industry standard and therefore usable in desktops and laptops • Can optionally be delivered with an installed, configured and tested laptop, or on a Black and Red USB memory stick. SMS hardware is optional • Much faster than the AROFLEX |
| Software | <ul style="list-style-type: none"> • Available for Microsoft Windows 2000 (approved) and Windows XP (approved) |
| User | <ul style="list-style-type: none"> • Simple Point & Click Windows interface • Up to 15 users (and one manager) per card, unlimited per domain • Allows for the creation of security groups Easily encrypted for multiple recipients through the use of security groups |

DEPLOYMENT

Files to be encrypted can contain, for instance, images, videos and documents. Of course, the File Encryptor can also be used to encrypt and store data securely offline on CD, data stick or a hard drive.

File encryption is simple, thanks to the following three-step procedure:

1. Start the File Encryptor Windows application
2. Authenticate user
3. Right-click file to be encrypted and select Encrypt

The encrypted file can subsequently be attached to an e-mail message, for instance. On the receiving end, e-mail recipients just need to double-click the attached file to decrypt it to its original format and content.

For more information, please contact:

Fox-IT BV
 Olof Palmestraat 6
 P.O. Box 638
 2600 AP Delft
 The Netherlands

Phone: +31 (0)15 284 79 99
 Fax: +31 (0)15 284 79 90
 E-mail: sales@fox-it.com
 Website: www.fox-it.com

Algemene Inlichtingen- en Veiligheidsdienst



Per undas adversas

* The AIVD is the Netherlands General Intelligence and Security Service. Our products are evaluated and approved by this organization before they can be used by the government for the protection of state secrets.

