File-encryption tool secureEFS

A-SIT offers a free tool **"secureEFS"** encrypting files and directories with the Citizen Card on: **http://www.a-sit.at/de/technologiebeobachtung/tools_und_prototypen/secure_efs.php**.

Goals

The tool secureEFS extends the file-encryption mechanism available under Windows and NTFS. It enables its controlled utilization by:

- encrypting the EFS key using the Citizen Card
- protection against disclosure of sensitive data in case of failures
- controlled access by encrypting the secret keys with the citizen card
- use of one or more independent cards to enable access for several users or to recover from lost or defective cards
- support of externally created keys (EFS-certificates) and backups which prevents loss of data.

The system assumes that individual areas are to be encrypted and that other keys or EFS-certificates are not present.

Confidentiality asks for a basic knowledge on where sensitive data are stored during their use and processing.

Preconditions

- Windows2000® or WindowsXP® are required.
- NTFS must be used as file system.
- Before installation of secureEFS an EFS compatible certificate must be provided. For a suitable tool refer to **http://demo.a-sit.at/it_sicherheit/ca_toolkit**.
- No conventional EFS-encryption may be active before the installation of secureEFS.
- A Citizen Card Environment (citizen card software) is required for the encryption and decryption processes that utilize the citizen card

In Operation

Secure EFS uses the file-encryption tools that are readily available in Windows.

When starting the user session (i.e., the GINA login to the system) secureEFS is activated via the Citizen Card and the EFS secret key is deleted from the disk immediately. The secret key is cached in the processor; **the key remains accessible up to the end of the user session**.

- When the user session is closed (i,e., when logging out), an encrypted file can no longer be accessed.
- At a system restart the secret key is read from an encrypted file using the Citizen Card, cached in the processor, and then deleted again.
- In case of maintenance by technicians or system administrators there is no access to the encrypted files.
- A DoD certificated mechanism guarantees the secure deletion of key material.

Encryption and deletion

- The normal file deletion of Windows does not delete the file physically.
- The Windows EFS encryption procedure does not physically delete the file; residual clear text remains on the disk.

Never encrypt just individual files. Create encrypted folders and create encrypted files there.

If you want to encrypt an existing file, copy it into an encrypted area and delete the original file with a suitable secure deletion tool.

Note, that applications occasionally leave files and/or parts of files in temporary folders, which could be analysed despite encryption of the "original" file.

What should be encrypted?

1. Usually, the user directories of the users shall be encrypted.
2. For Web-applications, the cache-areas of the browsers should be encrypted
3. In various mission- and security-critical applications (e.g., e-mail) it is also necessary to encrypt the configuration data of the application.
4. The certificates and passwords granting access to services must be encrypted, in order to avoid any access in case of loss or abuse of the equipment.

Note, that files kept at backup media are not encrypted. Therefore, backup media need to be kept protected.

Note, that until the initialisation of secureEFS has been completed, encrypted files cannot be accessed. Thus, files essential for starting the Windows operating system and/or files of drivers and alike may not be encrypted; otherwise starting the system is not possible.

Loss of keys or tokens

Without taking precautions data cannot be recovered in case of lost or defective cards, deletion of the encrypted EFS key, respectively.

- Take care of keys and tokens.
- Make backups at regular intervals and protect the backup media.

- Use only properly created key material and protect the key backups to be able to recover from defects.
- Further secure EFS instances using the same EFS certificate can be installed in the user environment of other login-accounts. This can serve as an alternative access in case of errors.

Further questions

Send an e-mail to: technology@a-sit.at

Zentrum für sichere Informationstechnologie - Austria
A-SIT
Secure Information Technology Center - Austria

File-encryption secure EFS

E-Government Flyer Nr.207 EN

Tool for the encryption of files and directories using the Citizen Card

DIGITAL AUSTRIA