

Distr.
GENERAL

CES/SEM.47/13 (Summary)
30 January 2002

Original: ENGLISH

**STATISTICAL COMMISSION and
ECONOMIC COMMISSION FOR EUROPE**

**COMMISSION OF THE
EUROPEAN COMMUNITIES**

CONFERENCE OF EUROPEAN STATISTICIANS

EUROSTAT

**Joint UNECE/Eurostat Seminar on Integrated Statistical
Information Systems and Related Matters (ISIS 2002)**
(17-19 April 2002, Geneva, Switzerland)

Topic II: Secure communications and data confidentiality

ENCRYPTION ON LAPTOP COMPUTERS

Contributed paper

Submitted by Statistics Sweden ¹

Summary

1. Today's world demands greater mobility and laptops are used more than ever. It only takes a moment for someone to pick up an unattended laptop. What if the thief is not interested in reselling your computer, but is interested in the sensitive information stored on its hard drive? The aim of this research is to scan through available encryption products on the market, choose a product that would satisfy the needs of Statistics Sweden, and implement the solution.
2. The root of these security concerns is sensitive information, which typically exists as unprotected files on your hard drive.
3. Statistics Sweden has a lot of different sensitive registers such as:
 - Secret defense registers
 - National registers covering the whole population, all enterprises and real estate
 - Companies secrets
 - Different surveys (health, income, family planning)
 - Registers covering ill-treated children, drug abuse and criminals. And the fact that people rely on SCB's statistics and information.

Laptops are used widely at Statistics Sweden and the need of encryption is quite evident.

4. Cryptography has been used for thousands of years to keep information secret. There are two types of cryptography: asymmetric cryptography and symmetric cryptography. Symmetric cryptographic works by transforming (encrypting) the plain text (the original data) to cipher text (the protected data) in a way that

¹ Prepared by Behzad Panahi (behzad.panahi@scb.se).

makes it infeasible to reverse the process without the full knowledge of the transformation function. Asymmetric, or public key cryptography also turns plain text into cipher text using an algorithm and a key. The difference lies in the use of a different decryption key, hence the name asymmetric.

5. The decryption (private) key and the encryption (public) key are related to each other, but the former cannot feasibly be derived from the latter. Therefore, the encryption key need not be kept secret, and can be made public. Instead, users of public key need to trust that a given key does belong to a particular owner. The process of certification addresses this issue. Security lies in keeping the private key secret.

Security considerations at Statistics Sweden

6. Considering:

??That the enemy is an individual, not a foreign power.

??The company's policy is relying on products from Microsoft.

??The company has contracts with IBM as well.

7. Due to the uncertainty about the lifetime and future support of the security products, it was mutually decided that Encrypting File System for Windows 2000 would be chosen as the product to be thoroughly investigated and properly implemented on laptops.

Encryption File System for Windows 2000

8. The following issues are addressed by encryption File System for Windows 2000:

??Manual encryption and decryption on each use: Encryption services are not transparent to the user in most products. The user has to decrypt the file before every use and re-encrypt it when finished.

??Leaks from temporary and paging files: These temporary files are left unencrypted on the disk, even though the original document is encrypted, making data theft easy.

?? Weak security: Keys are derived from passwords or pass-phrases. Dictionary attacks can easily breach this kind of security if easy to remember passwords are used.

?? No data recovery: Many products do not provide data recovery services.

How does the EFS encryption work?

9. EFS is based on public-key encryption, using CryptoAPI. Each file is encrypted using a randomly generated key, called *the file encryption key*, which is independent of a user's public/private key pair; thereby stifling many forms of cryptanalysis-based attack on the encrypted files.

10. If the original file is encrypted, EFS encrypts its temporary copies when attributes are transferred during file creation. EFS reside in the Windows 2000 kernel and use the non-paged pool to store file encryption keys, ensuring that they never make it to the paging file.

11. File encryption and decryption is supported on a per file or entire directory basis. Directory encryption is transparently enforced.

12. EFS automatically detects an encrypted file and locates a user's certificate and associated private key in the user's certificate and key stores.

Conclusions

13. It was concluded that Windows 2000 offers an acceptable degree of encryption, suitable for Statistics Sweden. It was decided that all newer laptop computers upgradeable to Windows 2000 would be upgraded, enabling users to use encryption on these laptops.