Encryption Software SafeIT

Sensitive data? Play it safe

Despite all the advantages of electronic data transfer, one has to bear in mind that public communication paths such as PSTN, ISDN and especially the Internet are at a very high risk as far as the confidentiality and integrity of transmitted data are concerned. An effective solution to this problem is encryption of sensitive data, eg by the user-friendly and cost-efficient Encryption Software SafeIT from the Rohde&Schwarz subsidiary SIT.

Photo 43 426/2

In recent years the traditional exchange of information by letter or fax has increasingly been replaced or even edged out completely by electronic data exchange. Despite all the advantages of electronic data transfer by e-mail or data carrier, public communication paths such as PSTN, ISDN and especially the Internet are subjected to high risks in terms of data confidentiality and integrity. But also data on notebooks or PCs that can be accessed by a number of users may run these risks.

File encryption with SafeIT

SafeIT encrypts one or more files or whole directory trees with a powerful encryption algorithm. For this purpose a new key is generated for each file. Encrypted data can only be read again if the correct encryption key is known. To save space, files are automatically compressed before encryption as this is no longer possible afterwards.

Operation is straightforward. SafeIT is integrated into the context menu of the Windows Explorer and other applications and can be called up from there (FIG 1). SafeIT runs under Windows™ 95/98/NT4.0/2000. The program may optionally be integrated into other applications such as e-mail programs and Lotus Notes.

To perform the encryption operations, the user logs into SafeIT and gains authorized access by entering the password. To increase protection against unauthorized access, the loaded encryption program can automatically be terminated after a set period of time.

In addition to encryption, SafeIT also allows files or directories to be deleted by overwriting. The original files are then gone and can neither be restored within the operating system nor by means of disk editors.

Key to security

An integrated management tool with graphical user interface serves for managing the encryption keys and configuring other parameters of the program (FIG 2).

Encryption keys can be generated by means of a PRBS (pseudo-random binary sequence) generator or can be entered directly by the user. To exchange keys between sender and receiver of encrypted data, the keys can be exported or imported via files. These files are protected by means of a password or an exchange key.

User keys in SafeIT are protected by passwords. Furthermore file keys can

also be generated from passwords. We should like to point out that the user plays a key role in overall system security, since the security of passwords – like in any other system – plays a decisive role in SafeIT.

No chance for intruders

One drawback of passwords is the fact that they are often changed and that users have to keep their sequence of characters in mind as there are no additional aids provided. In other words, the most powerful encryption is useless if an intruder can easily find out the password that is supposed to protect the encryption program. There are two possible ways of finding out passwords: the trial and error method (brute force) and the use of dictionaries. As for the brute force method, any combination of characters with the length 1, 2, 3, 4 etc. are checked. Passwords should therefore have an adequate length to protect them against such kinds of attack. At least eight characters comprising both digits and special characters are therefore recommended. The dictionary method tries all character sequences from a prepared dictionary.

A good password can easily be memorized but is difficult to guess.

Names of users, initials, names of accounts, vehicle registrations and other personal information and simple variations of them (reverse order, changing upper and lower case characters) are not suitable for passwords. Words in pairs or triples separated by special characters are more suitable for passwords as such combinations make it very difficult for intruders of the dictionary method to crack the password. Also initials of a sentence that can easily be remembered form a powerful password (eg "The sky above Munich was high and blue" becomes "TsaMwhab").

The quality of passwords has to be judged quite critically if an encryption key is to be generated from them. To provide comparable encryption security for a 128-bit key, a random password from a pool of 62 characters would have to have a length of at least 22 characters.

Additional security through PC card

To meet even higher security requirements Rohde&Schwarz SIT offers an encryption product with hardware support as an option. This product is a PC card (PCMCIA) that has the same user interface as SafeIT. In addition to the encryption component the hardware also has a physical PRBS generator for key generation and a secure key storage.

Ralf Dittmar

Reader service card 166/13

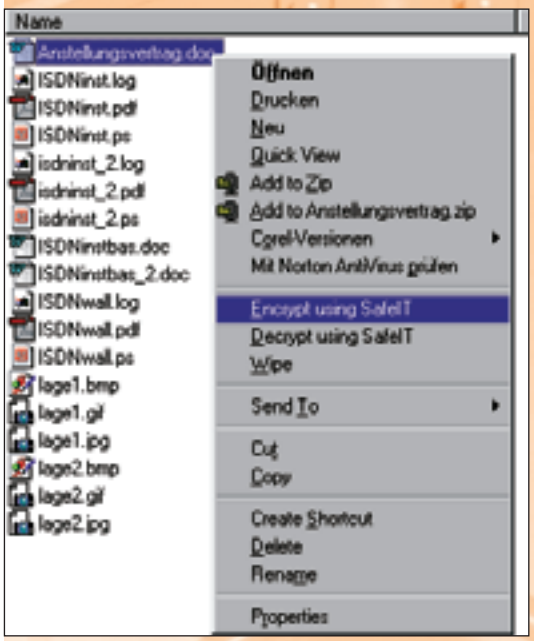

FIG 1 Convenient encryption via context menu

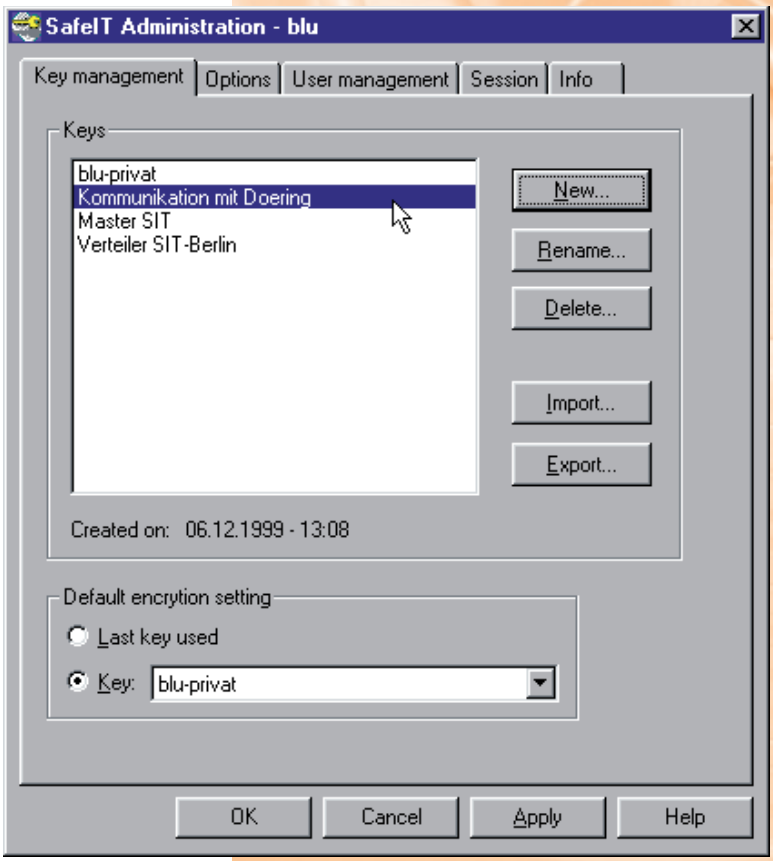

FIG 2 Key management with SafeIT