shellSAFE is a PKI applications suite tailored to fulfill the highest security requirements for workstation protection. Its components protect user data from the very moment he is saving a document until the information reaches his business partners at the other end of the Internet.

Using digital signature, OCSP services and time stamp the applications offer the highest level of assurance that the authenticity and integrity of the data was maintained on its way from the sender to the recipient. Moreover, using a state of the art mechanism - but still a user friendly one, the document owner can be sure all the time that the document he is seeing on his screen it's the one saved on his hard drive.

Document encryption is the digital shield that keeps the electronic thieves away from sensitive information, all the time and all the way from the local hard drive via Internet/Intranet to its final recipients.

The main features offered by shellSAFE Suite are:

- digital signing of documents for data integrity and authenticity
- different types of signatures: cosignature and countersignature
- multiple signatures on the same document
- document encryption/decryption for data confidentiality
- encryption for multiple recipients
- e-mail integration for secure correspondence
- integration into the Microsoft Office Suite and Windows Explorer
- secure storing for sensitive documents
- communication with LDAP, OCSP and time stamp servers
- secure file deletion from magnetic supports
- storage of digital certificates on PKCS#11 cryptographic devices or PKCS#12 vaults

shellSAFE Suite components

- clickSIGN – digital signature and file encryption application
- sendSAFE – digital signature and e-mail encryption application
- diskSAFE– virtual disk encryption
- shredSAFE – file secure deletion from magnetic media

clickSIGN

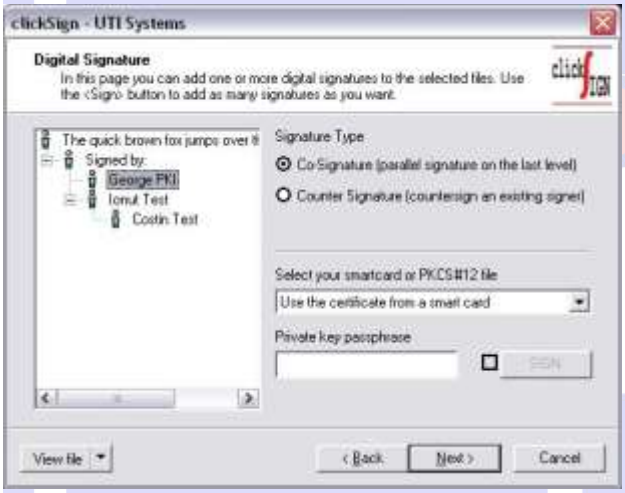
clickSIGN has two interconnected modules: a module integrated with Microsoft Office and a module integrated with Windows Explorer.

Modules functionalities:

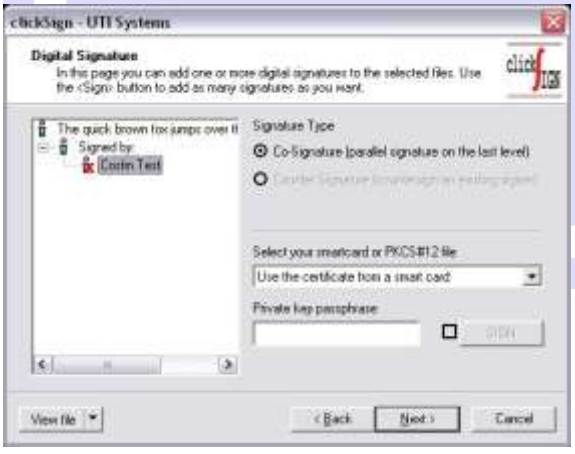
The Microsoft Office module is integrated into the Microsoft Office Suite by adding a button in the toolbar and it is used to encrypt, digitally sign, email and/or locally save the active document.

The Explorer module is integrated into the context menu shown on right click in Windows Explorer and it is used to encrypt, digitally sign and verify the digital signature, decrypt the files and save them as unencrypted or to open them in read only mode.

The digital certificates used to encrypt documents can be accessed as entries of a LDAP server or retrieved from a local certificate store. A file/group of files/folder can be encrypted for a user or for a group and, if needed, the file(s) can be deleted when the cryptographic operations are completed. If shredSAFE application is present, this module can be used to perform a secure shredding of the file.

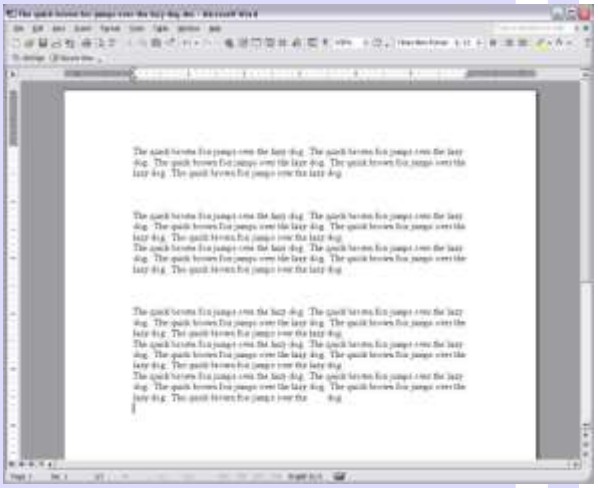


When a signed file is altered clickSIGN interface for signature verification notifies user about this issue.

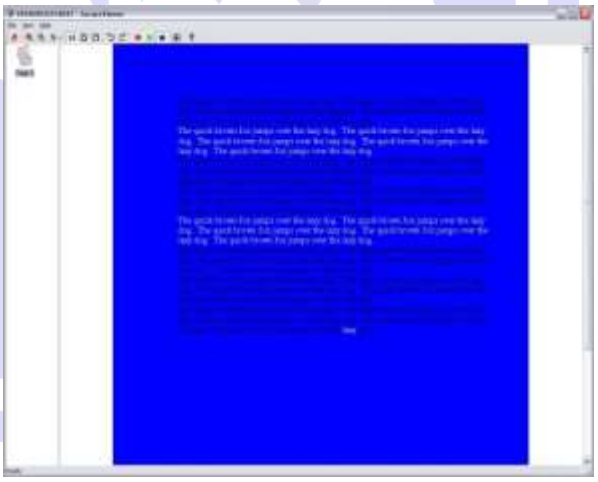


clickSIGN uses a “secure viewer” component to guarantee that the document to be signed displayed on the user’s screen, is the same file in binary format. When integrated with a time stamping service, clickSIGN digital signature is legally valid.

What you see:



What you really sign:



The status of the certificates used for digital signature is verified by using

OCSP or by connecting to a LDAP server and searching the certificate in the current CRL. If the LDAP server or OCSP responder cannot be reached the certificate status is checked versus offline CRL. The user will be notified each time the newest version of the CRL, the LDAP server or the OCSP responder is not available.

sendSAFE

sendSAFE is integrated with Microsoft Outlook for e-mail digital signature and encryption. It performs attachment encryption and/or digital signature and mail body encryption and/or digital signature on S/MIME standard specifications. The messages signed and/or encrypted with sendSAFE can be read with Microsoft Outlook or other S/MIME compliant products.

Similarly to clickSIGN this module can search for encryption certificates on a LDAP server or a local store and the certificate status can be verified using on-line or off-line mechanisms. sendSAFE allows multiple electronic signatures on the same message, automatic address resolution and it is interoperable with time stamp services.

diskSAFE

diskSAFE emulates a virtual file system on an existing HDD. The data stored on this new disk partition is automatically encrypted. When a file from the encrypted file system is moved to a new location, the decryption is performed on the fly. If the smart card with the digital certificates used for encryption is not detected by the OS, the partition is invisible; the encrypted data can be accessed again only when the smart card is connected. In this scenario the access to the encrypted documents is transparent both for the user and application and the sensitive information is fully protected without performing any other security tasks.

Using diskSAFE one can create virtual private disks of any size and can set access rights on the disks based on digital certificates from LDAP servers or local stores. To decrypt and access a disk, user digital certificates can be stored on PKCS#11 cryptographic devices or in PKCS#12 vaults.

With diskSAFE the users can actively protect their confidential files. Valuable paper-based documents are kept in files and are protected from theft and undesired readers in lockers and safes; diskSAFE works in a similar manner with electronic documents. The users may use the encrypted virtual disk as a safe/vault to securely store sensitive files.

shredSAFE

shredSAFE is used to securely delete the information stored on magnetic supports (HDD).

When a file is deleted in a regular way, using Windows mechanisms, it is not erased but only the reference of the file from the FAT table is deleted, the file remains entirely on the disk. Using common software programs the information can be easily retrieved.

shredSAFE zeroises all the file content multiple times so no evidence about the erased data will be accessible in the future.

Technical specifications

Standards

- x509v3 digital certificates
- x509v2 CRL
- LDAPv3 directory
- PKCS#7
- PKCS#11 to interface with smartcards
- PKCS#12
- OCSP (On line Certificate Status Protocol) according to RFC 2560
- S/MIME V1.5 with extensions

Algorithms

- SHA-1, SHA-256 for message digest
- RSA up to 4096 key biths
- AES, 3DES and proprietary algorithm for encryption