MAXA-SECURITY-TOOLS

Document Revision EN V 2.1d

True Security For Your Data

Preamble

Throughout history, security and self-protection has always been, among everyone's basic requirements and rights. What has changed is society itself - culturally, politically, legally and technically. The vulnerability of today's IT systems to modern attack methods has several similarities to the Cold War with both competing offensive and defensive technologies.

Why Data Security?

It has never been more important to protect confidential information & electronic data – both commercial and private. In these times of global communications and worldwide networking sniffing out electronically-stored data by hackers, crackers, co-workers, unauthorised personnel and other such groups has become relatively easy.

Industrial espionage has been around in the business world for a long time, and has caused billions of dollars worth of damage. Even the service sector, which provides services to the normal citizen, gives cause for concern in security matters. Things have not stood still in the personal data area. 'Social Engineering' methods alone have increased tremendously.

The trade in illegally-obtained data, as a result of insecure data management, has become a highly-profitable industry. The combination of legally-obtained material with that obtained illegally can, when misused, cause serious damage.

Digital technology theoretically permits the capture, transmission and distribution of any image or audio file in an instant. Governments in the industrialised world have caused enormous amounts of data to be accumulated, such that their citizens become numbers. In addition the current or planned number of on-line monitoring of PC users by various governmental bodies is finally bringing about a 'Big Brother' situation.

Well-known examples are:

- Echelon (world-wide system)
- Carnivore (FBI)
- "EU-Trojan"
- Security monitoring cameras
- Criminal investigations
- Illegal pooling of data from multiple databases
- RFID (*Identity cards, passports, pricing labels*)
- Points records for traffic offences

Similarly, in the commercial area, enormous quantities of data are captured and stored daily. In many cases, governments can obtain, or legally demand, access to:

- RFID (*price labels*)
- Credit data
- Loyalty cards
- Bank or credit cards
- Voice and internet providers
- Health bodies (*doctors, health authorities, health insurance companies*)
- Lawyers, tax accountants (*e.g. data trails or exchanges with corresponding lawyers*)

How has this happened?

Attackers have not only refined their methods, they have also become far more efficient. Since operating systems do not pay sufficient attention to these applications, these security gaps must be closed using third-party systems. It is also vital to educate & encourage users, and to provide them with every possible assistance.

The very groups or individuals who bear the heaviest legal responsibilities for the care and confidentiality of data have the least awareness. This includes:

- Lack of security consciousness
- Ignorance of legal responsibilities
- Inactivity by those in positions of responsibility

Anyone who believes that their data is sufficiently protected by Windows encryption, stored on hard disk (*e.g. Windows NTFS*), has been misled. These days there is no problem in accessing electromagnetic radiation from a PC monitor. This can be exploited from a short distance away, e.g. from a parked car, and the resulting data collected and reconstituted. Unauthorised access is made much easier when a user leaves their workstation unattended, without doing enough to block access. A lost or stolen laptop can, if unprotected, be an open book.

Networking PCs means a much greater danger of illegal access to data. The type of networking is actually irrelevant - every data transfer between sender and receiver means that there will be security weaknesses.

The size of the danger posed to data, along with its administration, means the only possibility is for users to secure their data themselves.

What can be done?

In addition to being security-aware, users need to keep up-to-date and to use suitable tools such as that offered by security software (***MAXA-Security-Tools***).

Who should use MAXA-Security-Tools?

Anyone who seriously wishes to protect sensitive data or any individual who from time to time uses the internet and wishes to protect their files from online monitoring.

Who definitely needs MAXA-Security-Tools?

Those in positions of responsibility, and professions where confidentiality is a legal requirement.

Professionals, who are required, by law, to protect the data and confidentiality of their clients and/or customers:

- pharmacists
- doctors
- practicing psychologists
- notaries
- solicitors/attorneys
- tax accountants
- auditors

If media reports are to be believed, there is a real lack of awareness of the changing security situation amongst these professional groups.

Doctors are particularly prominent here ('Self-check' for General Practitioners), closely followed by lawyers' chambers.

Consulting practitioners

- religious matters
- psychosocial consultants

Public positions

- e-Government

Commercial sectors:

- Computer centres
- Associations & societies
- Federations
- Banks
- Insurance companies
- Insurance agents
- Address brokers
- Marketing and market-research companies
- Call-centres
- Telecom providers
- Service providers

What can MAXA-Security-Tools do to help?

MAXA-Security-Tools focus in on the real protection of informational content, i.e. the data itself. Should an unauthorised person choose to search for data files, these would still be protected and the attacker would be frustrated. Should anyone 'happen to' discover data files, there would be nothing of interest, since nothing of value would be visible.

This is where MAXA-Crypt SE (*a module from the MAXA-Security-Tools*) would be employed. MAXA-Crypt SE (*Second Edition*) is a further development of MAXA-Crypt, which to date has never been cracked.

This encryption application is to change one or all the files in a directory, so that access to the contents is only possible using a password or pass-phrase. Emails can be similarly protected, both on- and offline.

A particular feature is that we use a basic key-length of 256 bits, which in practice makes it totally secure. In some ways this exceeds the requirements of the military and the security/intelligence agencies.

How do we manage this?

We do not want to re-invent the wheel (*unless it is necessary*), however we follow the motto 'The best is the enemy of the good'. Starting from the Rijndael algorithm, we have developed an enhanced solution, which practically acts as a security standard.

What is Rijndael?

Everything began from the AES Standard (*Advanced Encryption Standard*). In September 1997 the National Institute of Standards and Technology (NIST) produced the AES, and started looking for a new data encryption algorithm within universities and security companies. The intent was to replace the DES (Data Encryption Standard) and its extension Triple DES, which could not completely satisfy high security requirements. Furthermore, Triple DES placed a heavy workload on the processor, slowing it drastically, making it unsuitable for large volumes of data.

In the first round of the competition, 15 candidates were chosen to go forward. From these, five finalists were selected:

- MARS IBM *(represented by Nevenko Zunic)*
- RC6TM RSA Laboratories *(represented by Burt Kalinski)*
- Rijndael - *Joan Daemen, Vincent Rijmen*
- Serpent Ross - *Anderson, Eli Biham, Lars Knudsen*
- Twofish - *B. Schneier, J. Kelsey, D Whiting, D Wagner, C Hall, N. Ferguson.*

In October 2000, after public trials, Rijndael (pronounced *rine-dahl*) was selected as the new standard. A large number of cryptographic attacks have failed to discover any security weakness, although as with all cryptographic matters it is not possible to prove this mathematically. It was also impossible to discover any security weaknesses in any of the competing products, however Rijndael was chosen because of its high overall rating. The optimal combination of key length and block size flexibility, speed, simple implementation and extendibility were decisive.

NIST calculated that a computer capable of cracking DES within a second (255 key tests per second) would require 149 billion years to crack Rijndael using 128 bits. (*Our universe itself is under 20 billion years old*).
The Rijndael methodology was developed by Joan Daemen and Vincent Rijmen, two Belgian crypto analysts. They took their inspiration from SQUARE, a 128-bit block cipher which they themselves had developed. Rijndael is a symmetrical block cipher with a key length between 128 and 256 bits, in 32-bit steps. Differing block sizes can be used, within the 128 – 256 bit area. The design took into account all known attack methods, e.g. linear or differential crypto analysis, such that attacks using standard methods are no more effective than a brute-force attack (*computer-assisted probing attack*).

According to the laws of Nature, an attack on an encryption which used a 256-bit key length would be senseless, since it cannot succeed within the foreseeable future.

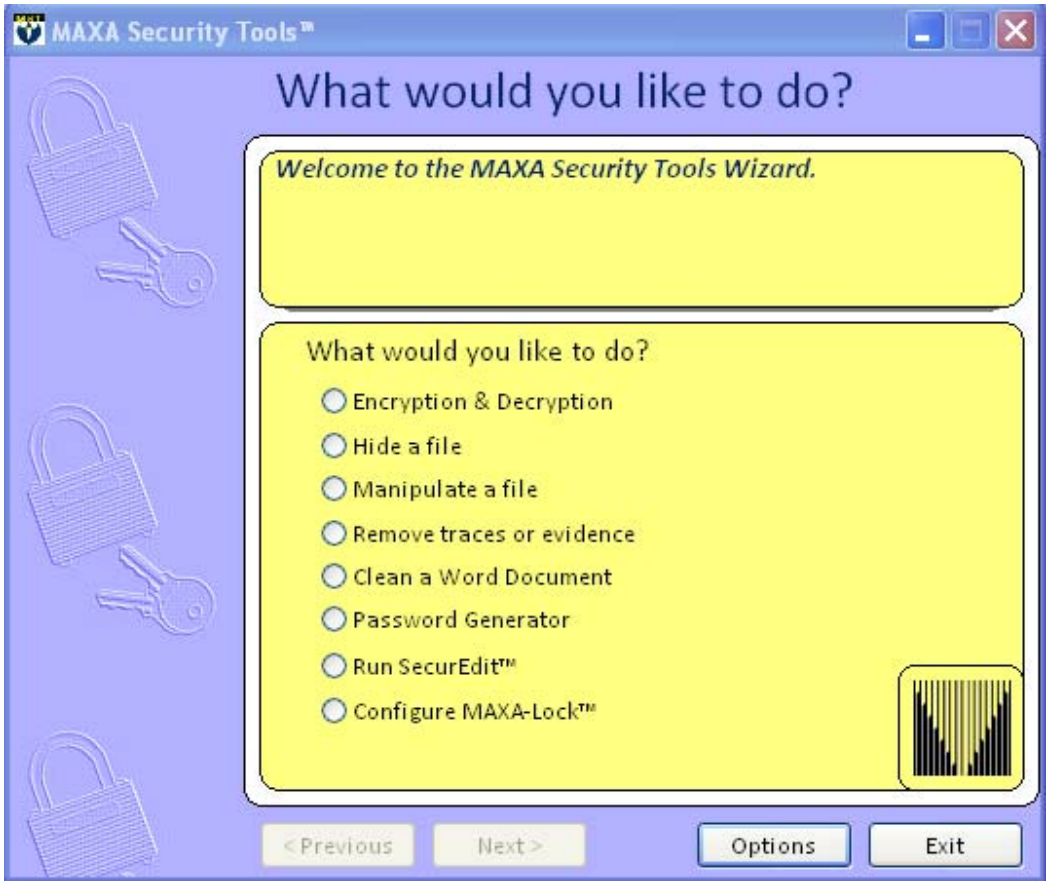
Product overview

MAXA-Security-Tools (***M-S-T***) is a combination of professional security applications (modules) under Windows, which continually evolve. The individual components have been designed for the highest security levels. Some individual modules exceed even military specifications. Many of the applications have no competitors, and are unique.

Menu:

The user-friendly interface does not require any time for familiarisation. The colours used in the menus follow the colour-usage guidelines. Any functions selected have application-orientated support. The implementation of the modules follows standard user interface guidelines.

Individual components:



Encryption/Decryption:

Algorithms with a key-length of 256 bits can defy the power of the largest processors regardless of whether they are using 'brute force' methods or even more modern mathematical solutions such as 'Rainbow Tables'.

What are the differences between the encryption algorithm used by MAXA-Crypt-SE and those used by other systems?

Essentially this is the set of requirements and their implementation. For us it is not about looking at the encryption operation individually. A powerful Formula 1 engine does not guarantee a fast racing car. It is the combination of individually-optimised solution aspects and their synchronised conversion into the resulting components.

What is required for a professional encryption routine?

01 A practical security level of 100%
02 An intelligent encryption algorithm
03 Constant 256-bit key length
04 Secure, bi-directional conversion mechanism
05 No format or size limitations for the encrypted file
06 Encryption of very large files
07 Minimal encryption overhead
08 High size-reduction factor
09 Processing speed
10 Variable file name- and extension-encryption
11 Further processing options with Steganography
12 An intelligent pass-phrase generator with Salt-function
13 Secure deletion ('shredding') of files
14 Virtual keyboard
15 Encrypted email
16 Encrypted print-out
17 No 'Back Door Key'

Our implementation of the list of requirements:

No 01 Security levels

In order to illustrate the MAXA-Crypt SE security from another perspective, here are some figures from the natural world, followed by a small insight into the levels of magnitude which the figures allude to:

Probability of winning the first prize in the lottery	1 in 2^{22}
Probability of being struck by lightning	1 in 2^{33}
Probability of winning the first prize in the lottery and of being struck by lightning on the same day	1 in 2^{55}
Start of the next Ice Age	in 2^{14} years
Age of the Universe	2^{34} years
Number of atoms in the Universe	2^{266}
Size of the Universe	2^{280} cu cm
The time until the Sun becomes a Nova	2^{30} years
The total of possible combinations of 8-bit RC4 (256! - 256^2)	2^{1700}
The total of possible combinations of 16-bit RC4 (65536! - 65536^2)	2^{954068}

Source: Bruce Schneier

This is becoming surreal. In order to have a better understanding, we will theoretically 'construct' a planet as big as our sun, made entirely of microprocessor chips. With this number of chips one can calculate one billion keys per second. And the

sun consists of 10^{57} atoms. A 256-bit key has 10^{77} possibilities. We make the calculation 10^{77} /10^{57}/1,000,000,000/ 3,600/24/365 and the result is 3,672 years – long enough!
We cannot crack a 256-bit key with normal methods. To crack such a key within 100 years we would need 10^{65} chips, each capable of calculating 1 billion keys per second. This is outside the bounds of possibility – it is extremely unlikely that a 256-bit key can be cracked – the amount of energy and the number of chips required are simply too large.

Bruce Schneier, in his book 'Applied Cryptography', shows the limitations by means of thermodynamics: each bit is represented by an amount of energy. If we could channel all the energy of a Supernova, and used to investigate all the possibilities of a key then, according to Schneier, "a typical Supernova produces around 10^{77} ergs of energy: if all these were channelled, we could check all the possibilities of a 219-bit number". This is insufficient for a 256-bit key, so he summarises:

"These figures have nothing to do with computer technology – it is all about the maximum values reachable within the laws of thermodynamics. These show conclusively that Brute Force attacks against a 256-bit key are useless, until the time when computers cease to be made out of any materials, and do not require any space.

No 02 Encryption algorithm:

See Rijndael please

No 03 Encryption levels:

See Bruce Schneier's comments on 256-bit please

No 04 Conversion:

Using **SBST** (***S****ecurity-****B****lock-****S****lice-Transfer*) (*our own system*), a power failure or system lockup would not cause any loss of data.

This is true for both encryption and decryption. A verification check analyses the result and displays it. If a failure occurs, the system will attempt to recognise and correct it.

No 05 Format limitations:

MAXA-Crypt-SE can encrypt all data formats on Windows-compatible systems.

No 06 File sizes:

MAXA-Crypt-SE can successfully encrypt data files up to 0.2 Terra Byte means 200 Giga Byte or 200,000 Mega Byte in size.

No 07 Overhead:

Every professional encryption system should aim to ensure that the encrypted file should be only a little larger than the original file size, as a maximum.

In MAXA-Crypt-SE the maximum possible overhead is a 280 Byte increase in file size. However, in most cases our **SSPR** technology results in a reduction.

No 08 Reduction factors:

The current tendency for file sizes to climb, arising from the increased performance of the hardware used, shows no signs of slowing. We are pursuing another route. Before the encryption process starts, the SSPR software (***S****mart-****S****ize-****P****re-****R****eduction*) checks if the size of the file can be reduced. Reductions of up to 80% are possible, depending on the structure of the file.

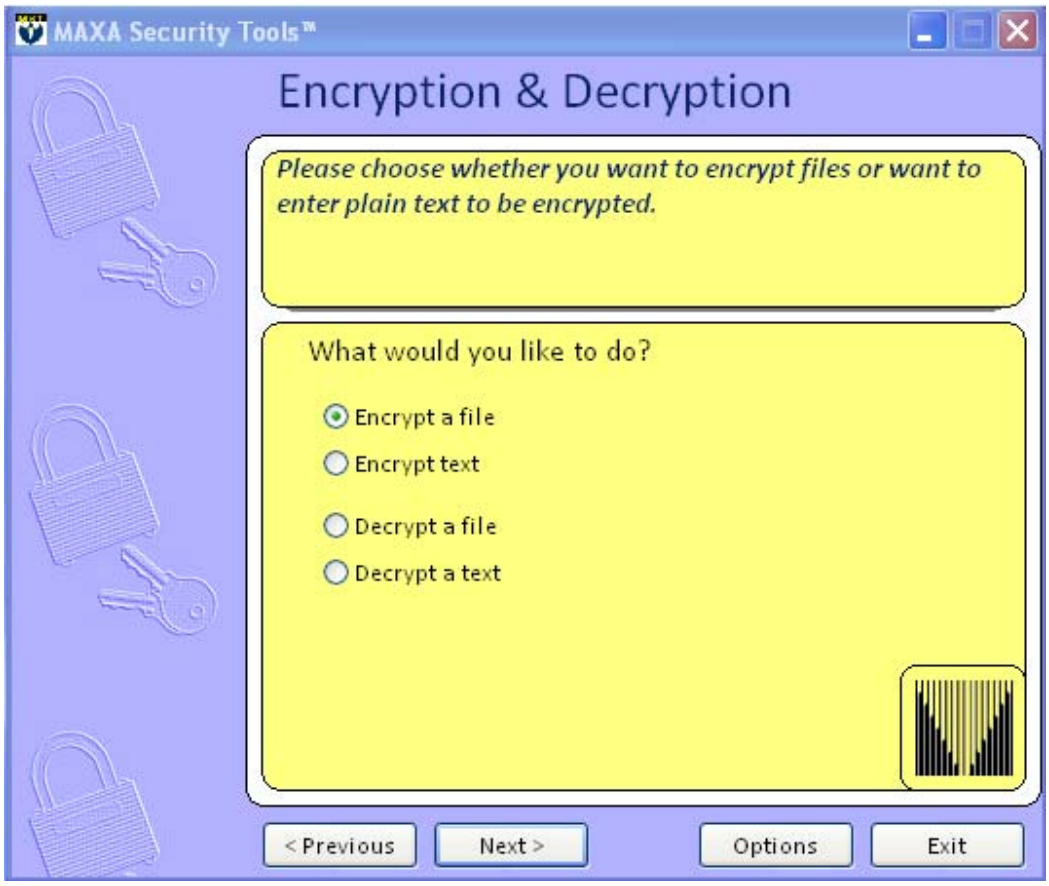
No 09 Speed:

Larger files can give rise to time-related challenges, depending on the Windows environment and its hardware requirements. This can make users very frustrated. We have therefore developed **BSO** (***B****lock-****S****ize-****O****ptimizer*). Working on the basis that there is an 'average' Windows system, with a Gaussian distribution of hardware equipment availability, mathematical methods can be used to improve encryption performance. In some cases, intelligent optimisation of block sizes between RAM-throughput and offline files can bring impressive results.

No 10 File names and extensions:

We see no benefit in keeping file and/or extension names the same. The user should be able to decide for himself which order to use. This is, of course, also possible in mixed-mode format. Our **SDRR** development (***S****mart-****D****escription-****R****ecovery-****R****obot*) permits the user to name or rename one or multiple files as required. It is possible to encrypt several files into a single file, then after decryption to be able to use the original file names.

Encryption & Decryption



No 11 Additional concealment (Steganography):

There are situations where it makes sense to hide an encrypted file within a picture. An automatic menu option offers this facility. When you have the right size relationship between the encrypted file and the picture then the file can be concealed invisibly within the picture without affecting its quality. We are ahead of the competition here since we can use the JPG/JPEG format, instead of the less efficient Bitmap format.

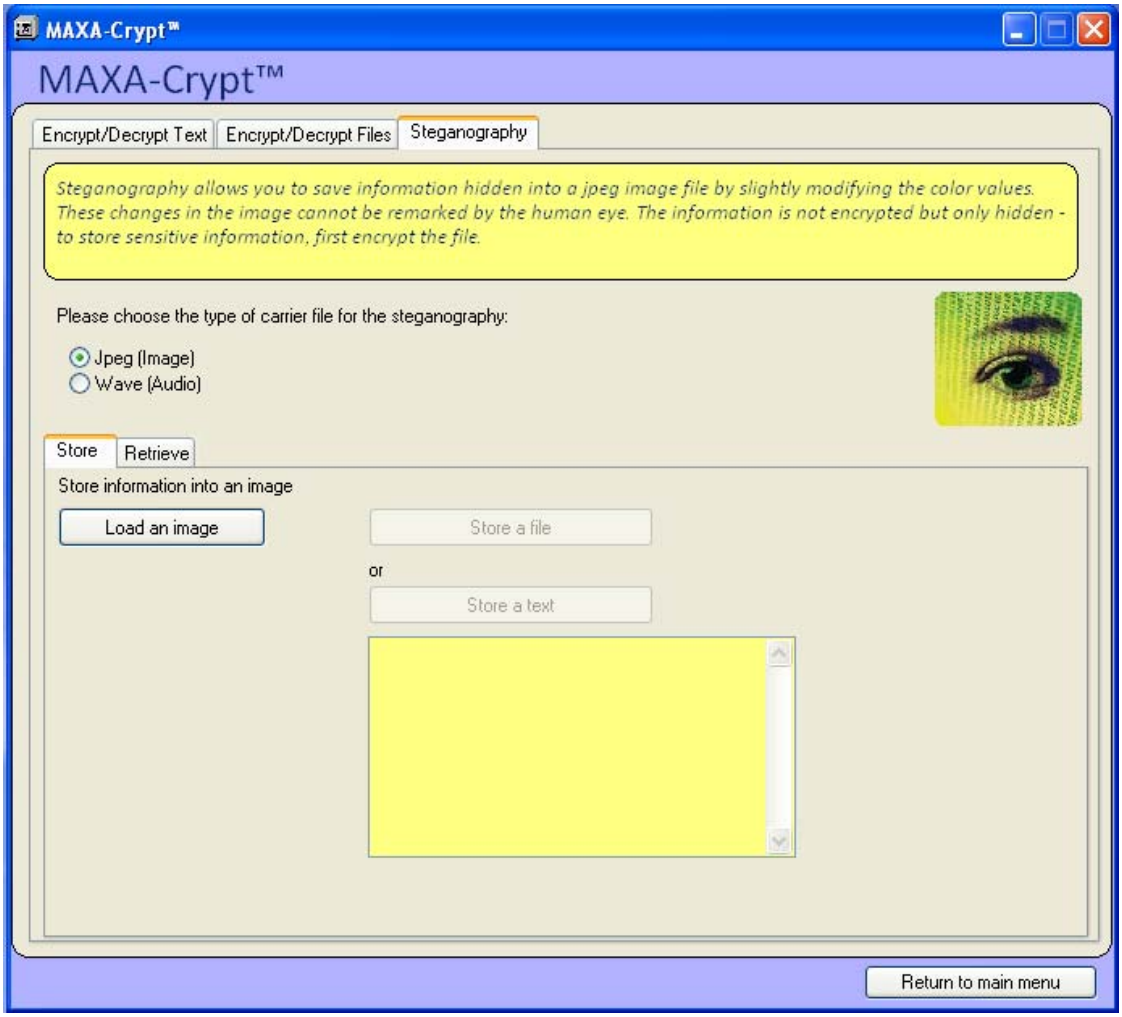
Similarly we can use our **IACG** application (***I**ntelligent-**A**udio-**C**orrelation-**G**enerator*) to hide one or more files within an audio file, with no loss of quality.

If a file has been encrypted with MAXA-Crypt-SE, then the following is possible, as an option: you rip sound files and create a full CD, integrate up to 100 MB of files, then burn a further CD. This volume of data can be hidden safely and invisibly within the CD, without compromising playback functions or sound quality, and undetected by special optical checking methods.

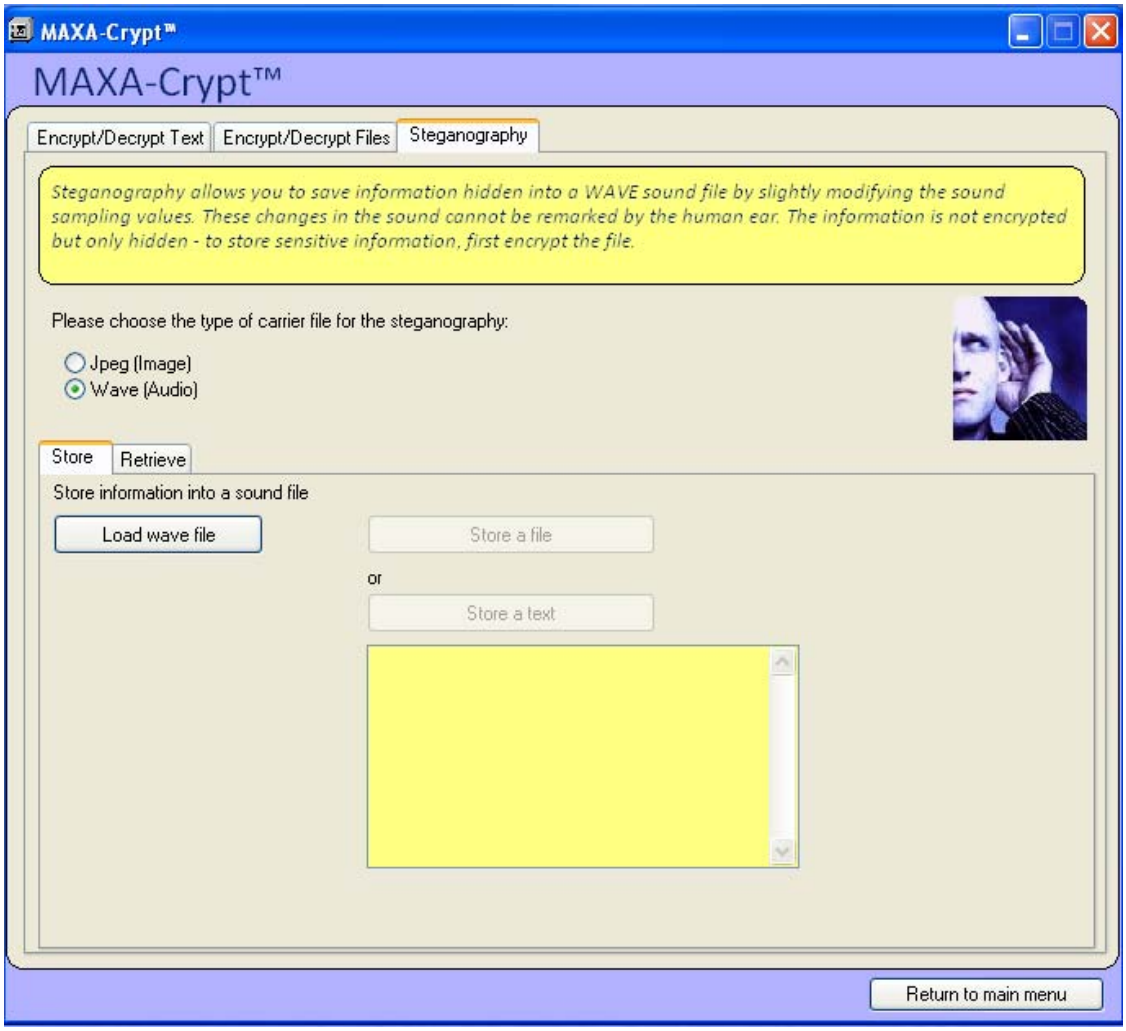
Critics have claimed that this is detectable in a light background tone. This is however more likely to come from other sources, e.g.

- Initial audio recordings (AAA / AAD / ADD)
- digital recording with re-work problems (DAA / DDA)
- digital recording with background noise. (DDD)

Hide Information in a JPG/JPEG - picture



Hide Information in an audio file

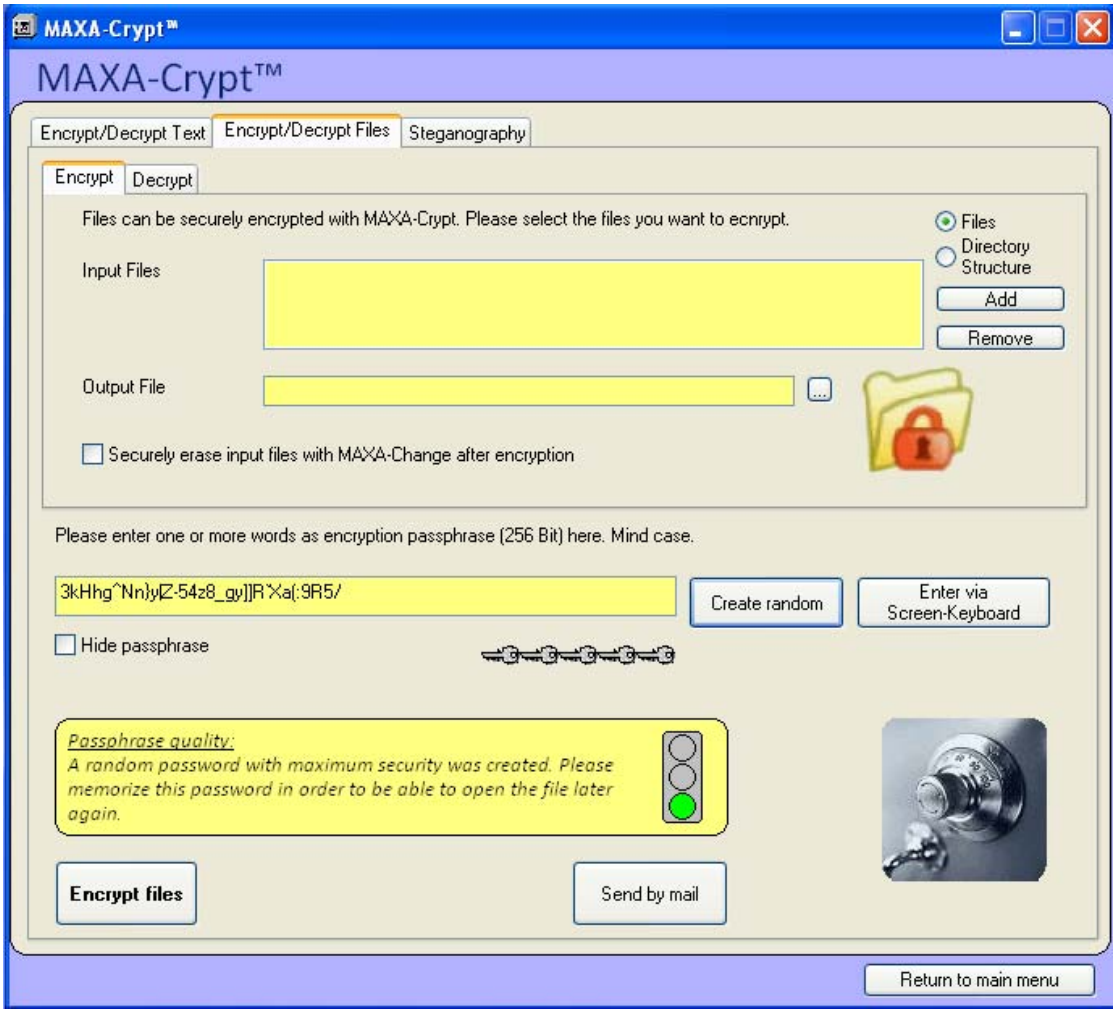


No 12 Pass phrases:

One of the most important techniques in implementing security systems is the creation of passwords. The word implies the singular form. However, a simple word is not enough here, and must be used in combination with alphanumeric and special characters – which brings us to the concept of pass phrases.

Generally the user sees no link between his input and the required security level of the phrase created. A real-time analyser checks the quality of the data entered, in order to ensure that it can be used. A visual security control check shows immediately what security level is involved.

Pass Phrase



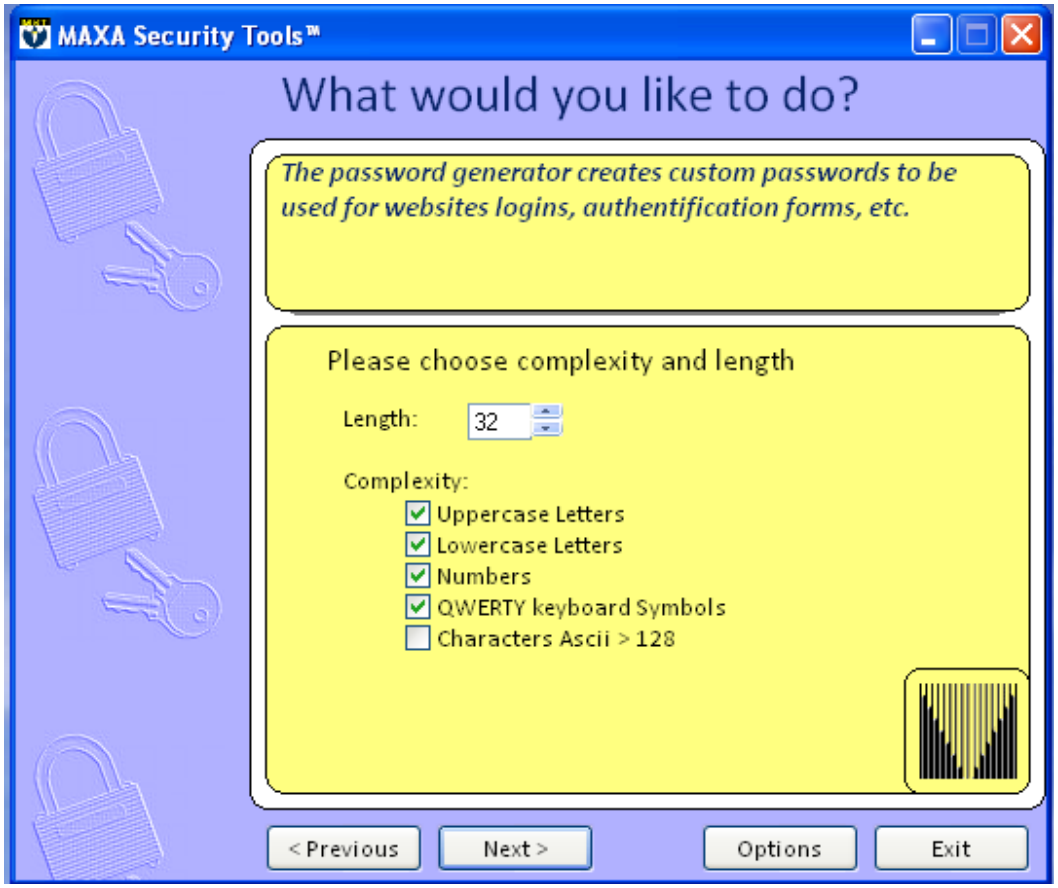
It would however be much more sensible to use our 256-**RCG** (***R**andom-**C**ode-**G**enerator*). This function guarantees the creation of a 256-bit pass-phrase in less than a second.

We believe that using a phrase like this within MAXA-Crypt-SE makes it uncrackable (*under the laws of thermodynamics*), and this is the case regardless of the form of attack.

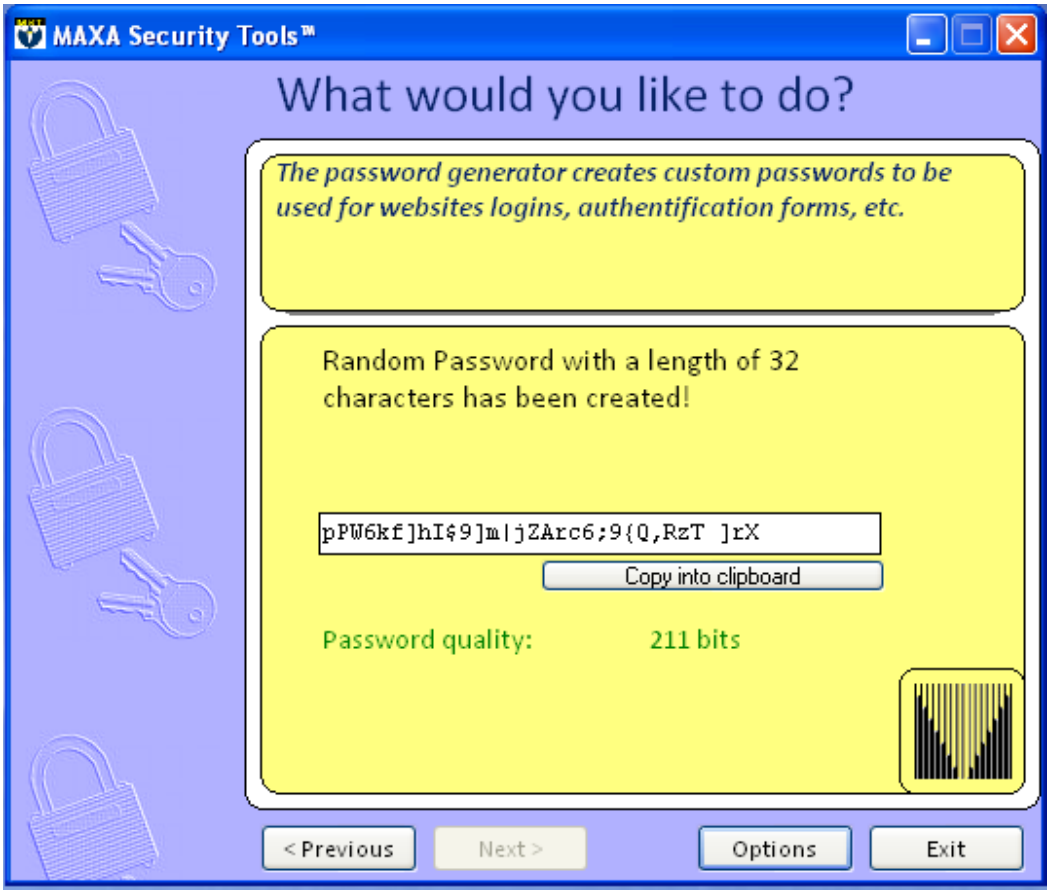
Password:

The pass-phrase generator is exclusively for MAXA-Crypt. The phrases produced are only designed for the Rijndael-related algorithm. For other systems we have developed our own password-generator. To understand this better, here are some basic considerations:

Password Generator



Password Sample



"Password-problems"

Everyone has experienced this. You are trying to create a password, but you can't find one that fulfils the security requirements: either it's too short, or too simple, or too complex, and you can't remember it. In the end, as you run out of patience, you choose one which is familiar, but unfortunately not safe. Generating a password requires self-discipline and a basic understanding of what is involved.

"What makes a weak password?"

There can be many reasons. The simplest is that it is too short: a 2-digit (considering a – z, A – Z, and 0 – 9) has 62^2 possible combinations, i.e. 3844. This would take some time to calculate mentally, but takes only seconds on a PC. Another reason is the password structure. A password "111" is not a viable password. First it is easy to work out, and secondly the hash created from it is too simple. The analysis of passwords is also important. Password analysis comes from an understanding of human psychology, and that people are creatures of habit. Examples are the use of telephone numbers, or account numbers, as passwords. Other examples are the use of certain

popular words such as “God”, “Love”, or part of an email address, all or part of your own name, or the family pet. All of these should be avoided!

“Creating a (relatively) secure password”

A more effective password has upper- and lower-case letters, as well as numbers. It should not have any noticeable pattern, and should be at least 8 characters in length. It should not be a known word in any language, nor should the same password **ever** be used for two accounts. “Sensible” passwords should come somewhere between a recognisable and a non-recognisable set of characters. However, they should contain an alphanumeric mix, with some special characters.

How long should a password be?

This is not easy to answer, and depends on the level of security required. Generally you could say that a minimum of 8 characters is sensible: 8 characters give rise to 191707312997281 combinations using a 61-character set (a-z, A-Z, 1-9). At a typing rate of a million keystrokes a second, that would require a maximum time of some 53252 hours (191707312997281 seconds), i.e. almost 6 years – a long time!

In areas with higher security (company networks, or the like) you could increase this to a minimum of 10 characters (=713342911662882601 combinations, i.e. some 198150808 hours, or some 22700 years). To make things clearer, here is a small table:

Minimum length	Maximum time required (assuming 1million keystrokes/sec)
3 characters	around 0.2 seconds
5 characters	around 14 minutes
8 characters	around 53252 hours
10 characters	around 1179469 weeks
12 characters	around 84168853 years
15 characters	around 19104730610573 years

To explain further: all these results are so-called **maximum times**. This means that someone working at the stated speed tries to crack the password, and succeeds with the very last possible combination, then this will have taken the maximum time. Theoretically however it could have worked with the very first possible combination. So, despite using 15 characters, it only took one hundred-thousandth of a second., It can happen that an attacker cracks a password in only a few seconds – pure chance. So one should not rely on an 8 character password. Furthermore you should also consider the power of computers: we are working with a million keystrokes per second. Networked high-performance computers, working in clusters, could do this much more quickly. The number of combinations comes from $(\text{number of characters})^{\text{length}}$: each character of the password could be one of the total character range. Thus a password of 3 characters, with 62 possible characters, has 62 x 62 x 62 combinations. To obtain the maximum possible time, divide the total by the number of keystrokes per second.

Pessimistically one could say “what’s the point – it’s all a matter of chance”. But, between the maximum time and the theoretical possibility of cracking a password in only a few attempts, there is a potentially uncomfortable wide ‘middle field’ for the attacker: this is where the vast majority of cases would happen - somewhere between many days and many years. So an attacker must assume that initial attacks on an “insecure” password could be in vain.

One should also point out that many access systems reject guest-users, or even normal users, after a certain number of failed attempts. Anyone who wishes to continue to access the system would have to use another identity, or, on the Internet, another IP-address. Attackers can however employ some automation tools for this. To consider how effective such attacks are, we used the following example:

You want to create a ‘secure password’ under Windows, using 10 characters using a mixture of upper- and lower-case letters combined with numbers. This produces the following: Ai0Ksw48Xz. Using Brute Force to discover the password would require several years, no – not nowadays. Tools now exist, based on ‘Rainbow Tables’ which can do the same thing in around 6 minutes, using a Windows design fault.. Even using more characters does not bring the necessary processing time over 15 minutes. One such leading tool uses pre-prepared tables, up to 1Gb in size, for Rainbow Tables.

No 13 Secure deletion:

If required MAXA-Crypt-SE can delete files by overwriting up to 7 times. The following courses can be utilised:

0-times	files are deleted in the ‘normal’ way (non-secure)
1-times	files are overwritten once with zeros
3-times	files are overwritten 3 times, first with 0, then with 255, then 0 again
7-vsitr	files are deleted according to the German VSITR standard.

Security notice:

It is easy to understand the technical background of ‘guaranteed deletion’, however the operating system can cause a problem. Software which encrypts a file and subsequently deletes the original, e.g. MAXA-Crypt-SE, cannot automatically delete all fragments of the file on the disk. There is no log kept of every disk access. Multiple file fragments come about because temporary files are created as documents are amended. Such fragments are normally deleted, but not securely so. Other tasks on the same PC can overwrite the disk areas which the fragments occupied before ‘deletion’. It is not possible to manage this overwriting process.

However, journal-producing file systems such as NFTS are even less suitable! System or workspace areas can only be cleaned up by regularly deleting empty disk

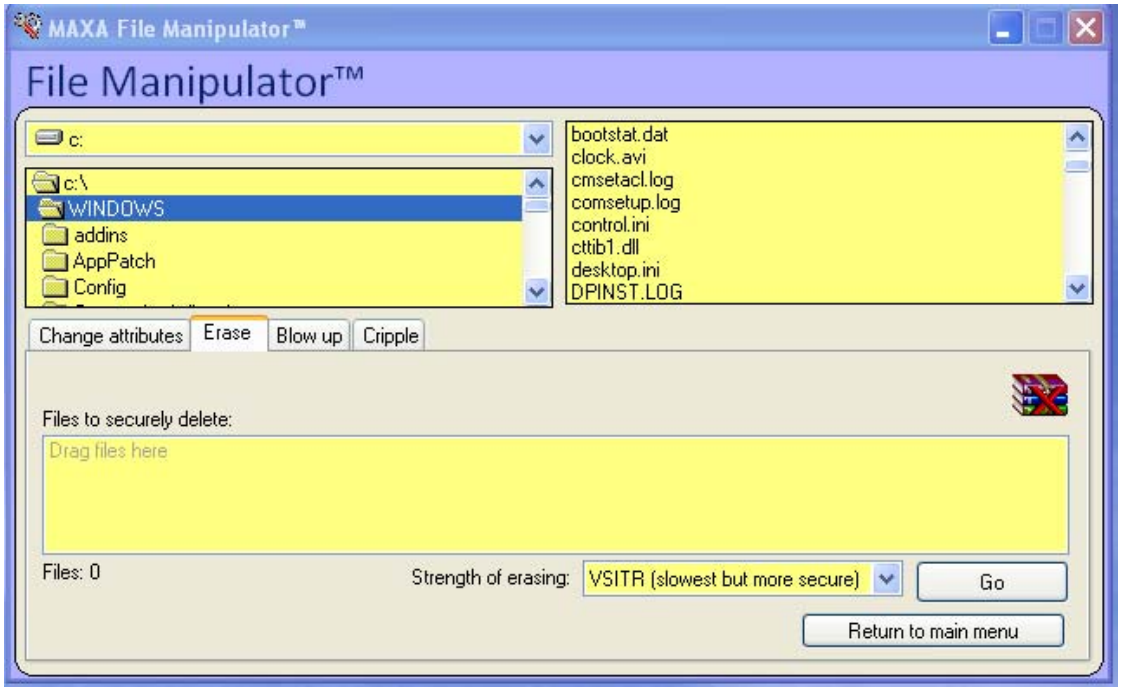
areas. However there are areas used by the Windows operating system in the system area which cannot be deleted securely by the relevant tools.

After MAXA-Crypt-SE has encrypted a file, the cluster-lead of the cryptogram is deleted securely. A cluster-lead is the difference between the space occupied on the disk system and the actual file size.

Anyone concerned that the VSITR standard is insufficiently secure has the following options:

- The KGB deletion routine *(overwrites 256 times)*, but takes a long time.
- Use the Cripple-facility of our file manipulation system, then run a disk-defragmenter (gives a totally secure result)

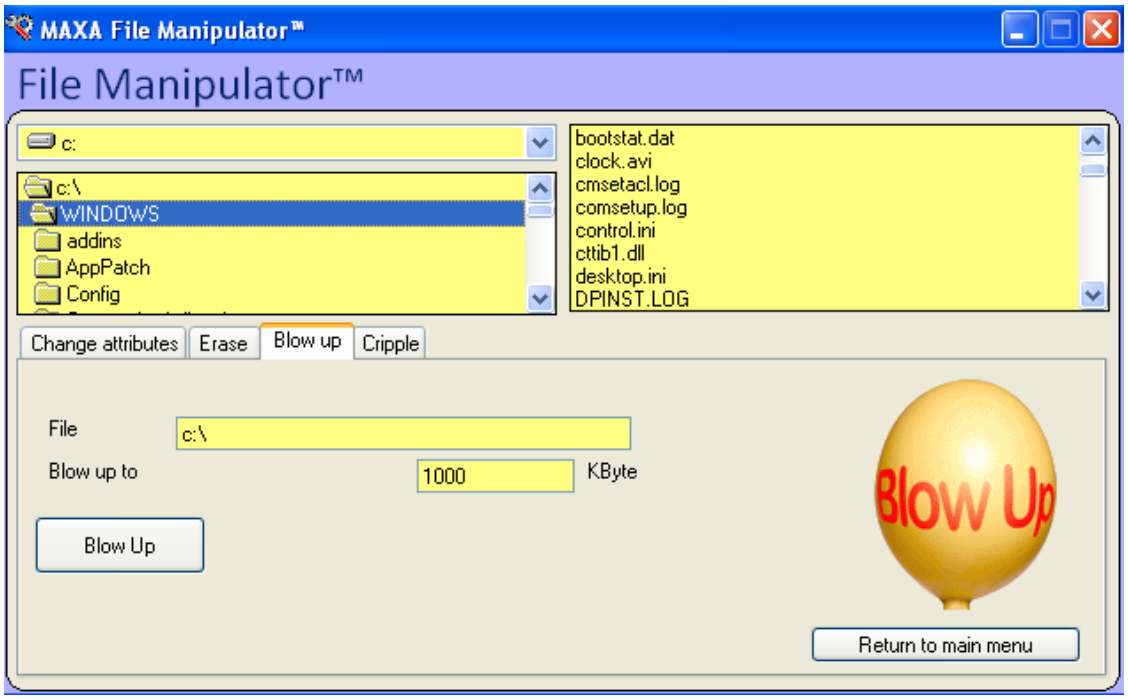
Erase a file



File-manipulator:

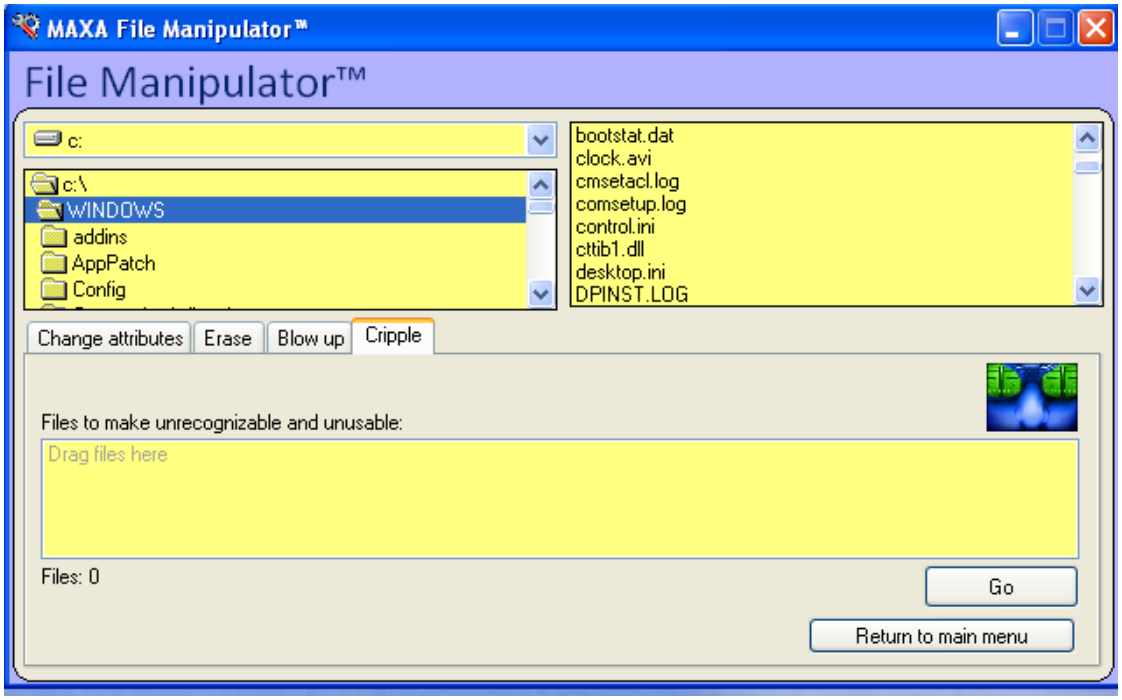
Sometimes it can be impractical, or impossible, to delete or encrypt a file quickly, since the size makes the operation too slow. A deception operation may make more sense.

The simplest and best-known methods are to change the file attributes, but in most cases this is unsafe. It may help to camouflage a file, or inflate it in size. We have developed the **FBU** method (File-Blow-Up): this allows a file to be blown up to the GByte level, whilst generally retaining its capabilities.



Multi Giga Byte sized files or image backups are now being created more frequently. These can be encrypted through the relevant backup program, but this is seldom secure. An effective solution is not viable, as it would take too much time. We have therefore developed a modification system which intelligently changes the relevant file in such a fashion that neither the original functions nor the true contents can be accessed. In many cases where attempts to access this file have been made, the file will respond by prompting for a system close-down, guaranteed to frustrate an attacker.

Cripple a file

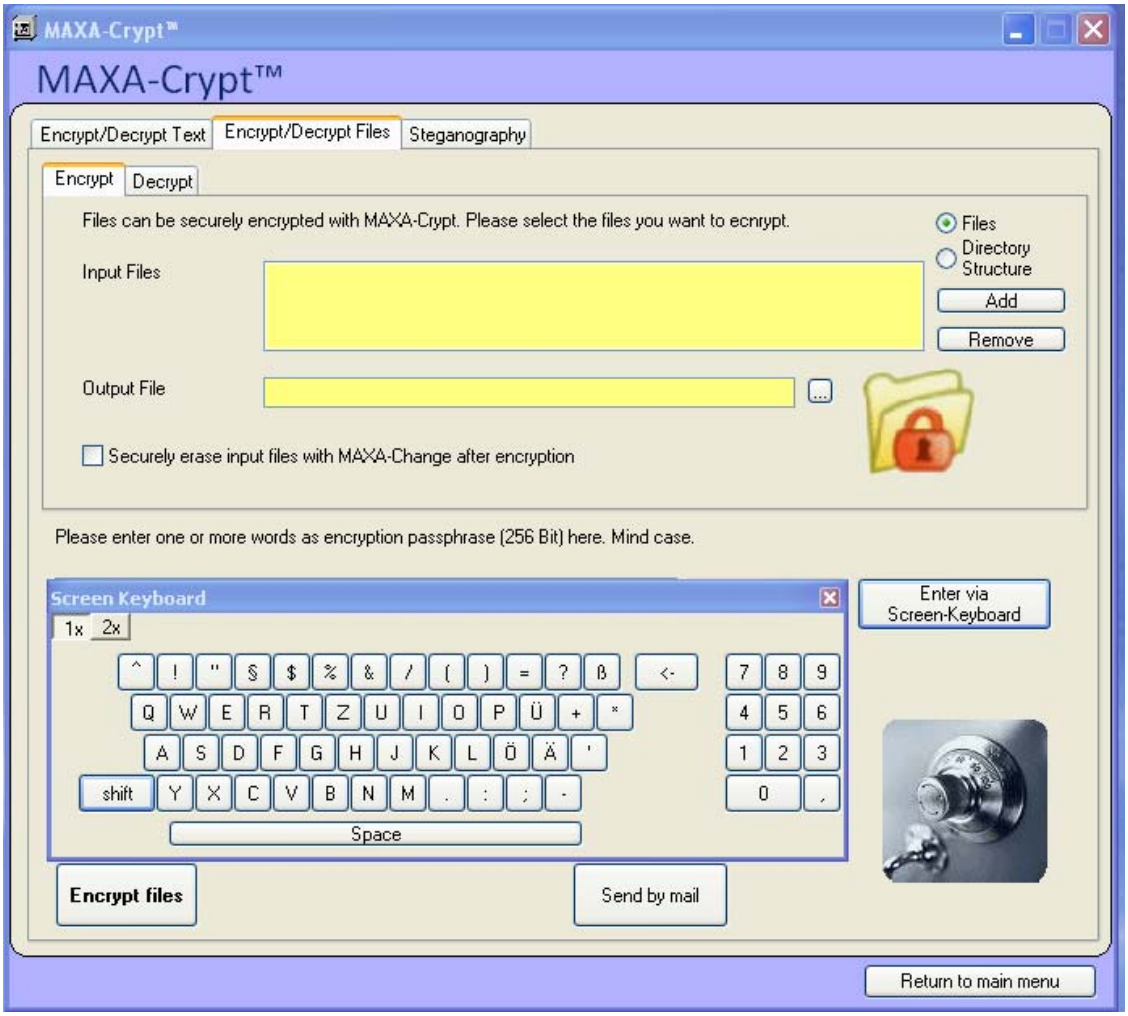


No 14 Virtual keyboard:

Hardware or software key-loggers are being used more and more widely. Commercial companies tend to use software versions, for employee-monitoring purposes, whereas hardware versions are used by public bodies and security services. The aim is to ensure that each key stroke is recorded. Pass-phrases are only secure when they do not fall into the wrong hands.

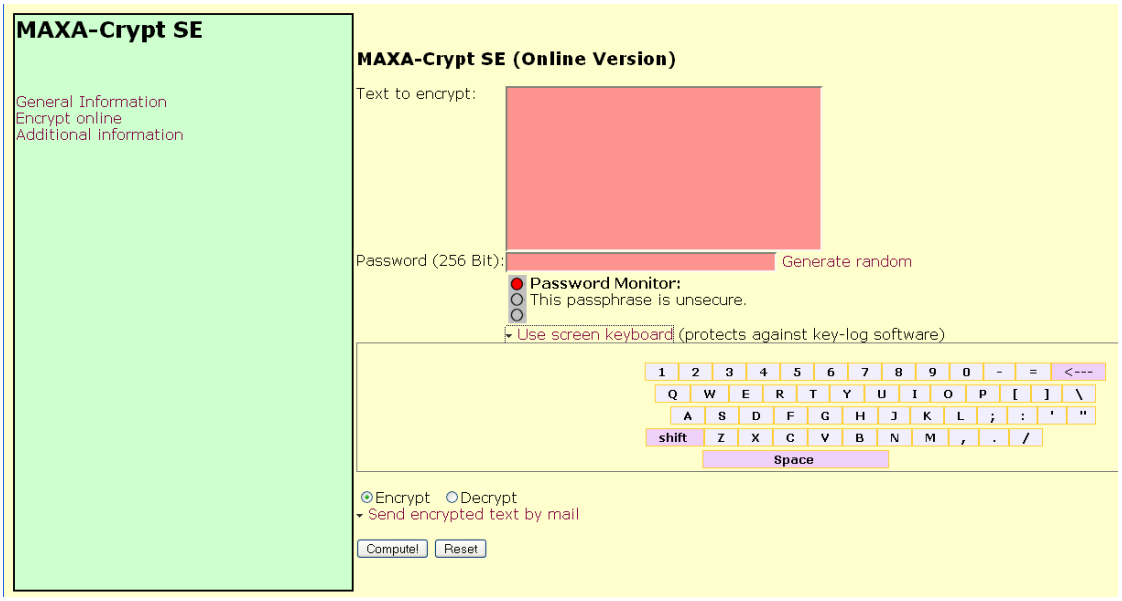
Anyone using a PC in an insecure area (*e.g. work-place, internet café*) should consider this. We have therefore developed a virtual keyboard: with one click the keyboard appears, and the user can enter his password via the screen, using the mouse. This virtual keyboard can be situated anywhere on the screen, and can be doubled in size if required. The keyboard layout comes from the language selected for the operating system.

Off line screen keyboard



Travellers can use an online version, described in the chapter on email encryption. An internet-café user can access this screen by going to

http://online.maxacrypt.org



No 15 Email security:

We support email encryption in a number of ways. Specifically we differentiate between **local** and **remote** usage, and also between file and text-encryption.

A1-) Local files:

We use the previously-described means to encrypt your files, and send them as email attachments.

A2-) Local text:

You can use the method in A1 above, or encrypt text and paste it into your email program using the Clipboard.

Advantages:

- The text-area in the email is encrypted and cannot be read by unauthorised individuals.
- Any such emails go through email servers which would block or filter out email attachments.
- Employers who monitor the employee email contents will be unsuccessful here
- Even if the recipient is in an internet café, he could use our encryption server to decrypt the text.

B2-) Remote transmission of text:

Go to our encryption server (*e.g. from a PC in an internet-café*), encrypt the text there, copy it via the Clipboard into your webmail, then send it in encrypted form to an email address.

Advantages:

- The text-area in the email is encrypted and cannot be read by unauthorised individuals.
- Any such emails go through email servers which would block or filter out email attachments.
- Employers who monitor the employee email contents will be unsuccessful here
- Even if the recipient is in an internet café, he could use our encryption server to decrypt the text.
- Since the data left on the Clipboard is encrypted, it cannot be accessed by anyone else.

No 16 Encrypted printouts:

In some situations it is not possible to transmit data securely, e.g. by email, and data-exchange by magnetic media such as CD-ROM or USB-sticks is not viable.

We can offer an alternative option here: encrypt your data as normal, and print it out onto paper in a non-proportional font. The recipient takes this paper, scans it into his system using standard OCR-software, and decrypts it. Should a read-error happen, this is handled by using our **ACRR** routine (*Automatic-Code-Recovery-Recognition*): this invokes an automatic recovery system to attempt to solve the problem.

Encrypted OCR Text of Paragraph No 16 (as you see above)


```
zAGYXMUzWVPOuyZc1Oe7Uuoyi6W7/YM5sNl0ISqTET5mw9WXhy2byjZZuiLISlwzmBfvDgSpwxfy
bANqZ5HcJ9VjERimPqh5aiMWnsYp4P6wl/msRorX90BCfrEiyHmCb06WiDh7T4SiRliYYdvVK+c8
pw329+rtffjXxPiZBRwR0OjO4r3M7/feGnH3YK7w+W0KoYsHdw+Bpq+Lfqy0SwYnqk+Vt5wB8Txx
Md3BDnUIZrWIqmNBvsv/auXwcNom6m00PfGJ8TSbRyKmwXMsiUty4FdNqkbm4TIVVYGaQsSocJWT
LI4cbNwTlj7H0KGVy9wDCvkWQdoW3QIsmgAs5SIPcSIgs1Fy5j7oC+1GVE7nI5wgSOOjRp8cdVyO
BtrWKedQ9IIxdp9ieTWMkZnr5GwrIyJMNxRlwIoo6ndPH5R5XkoNjR0dhm6CCAQzrqpJW6+jTzVO
LyS82oX3vVJDa4dokVqQLMj52oeGSzeoFZPef/ubYgkadvJPMwjaLDQDg+xLc0sJQQrn9krv7tk2
+buUhf8A1JwhLRW3CAWwFaBWhB3nMWH30zuTV3rNh0PWjiopUTSpdYObpKL1tLiWWs+E3xPNjuFq
PzJ8NTg+ENGI/TUQ1fBS7Pdmm8f4u70+KUF1qDIonh/j9hR6ozbOnuc5l0x4cSkN/Y6rleWE/+k+
mI0ydmAoThtVxIdkHuplaFDcslGY8pG3CQ18VOj9nZFj93Ud3NdIjwEKlcmpfze2y9REc8p/6uC6
IzWbnPwM0yitaMpyaWZFQ5zSs7+kEhWLkkWdeBPQ1QbS9Mnlv0Jy8ziJaXd5xeMBMrETQHqttP9M
bbmNjqayJxPNblCg0ts3baVWch8GwoWVW6jY6fZ26iMNVLQfQW1nCNCZiDG
```

No 17 Back Door Key:

It is well-known that more and more Software-producers are integrating this function *(not always voluntarily)* – but we do not! The architecture of MAXA-Crypt-SE is in itself unsuitable for this function, and of course it would totally negate the philosophy of the product. There is one case *(and only one case)* when this is provided – for large organisations using MAXA-Lock. An employer must have the option of gaining access to the PC of an ex-employee: this option has to be ordered separately, *and has no connection to our encryption techniques.*

DOC-Cleaner:

Microsoft Word is one of the most-widely used word-processing systems, and is installed on many PCs. All the more serious then that Word conceals a great deal of data in each document which can betray a lot about its origins and development history. This can cause risks for both companies and individual users – especially when the documents are sent by email or published on the Web.

Word automatically inserts the user and company name into each document, which is easily found. They are easily located in the Document Properties, and come from the data entered when the Word/Office software was installed. Word also notes who stored the data last and how often it has been amended. A problem arises when someone uses 'Fast save': here text areas which have been apparently deleted by the user are nonetheless stored by Word with the document. An investigator can use a simple text-editor to render this data visible again.

The same is true for the 'Track Changes' option in Word's 'Extras' menu. If the processing history was not deleted after the last editing activity then all deletions, amendments and changes are visible.

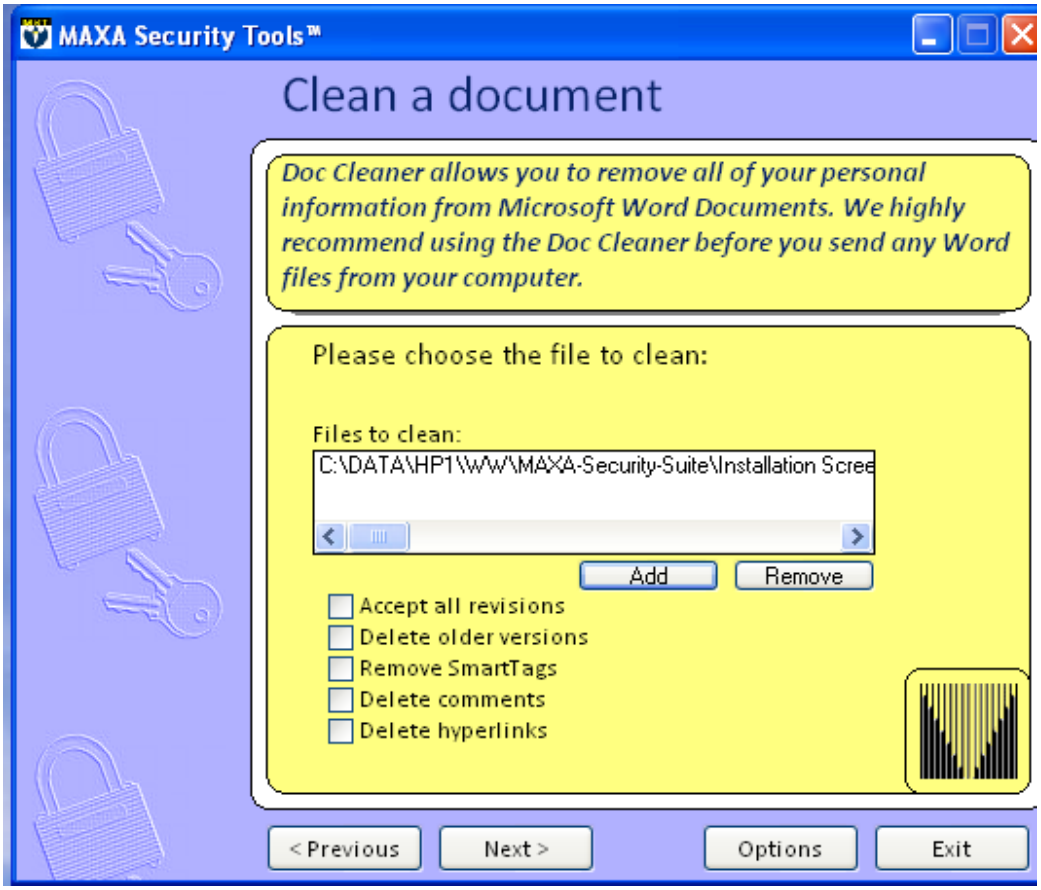
Let's consider a fictitious example: a job reference has been put together by several people, then sent electronically to the employee and others. This individual later applies for a new job, and sends the reference in by email, as a Word-attachment. The recipient of the email switches on 'Track Changes' and can then see the changes which were produced as the reference was produced. The consequence is that the applicant has no chance of getting the job – and will never know the reason.
Anyone who wishes to send their Word documents by email, or put them on the Web, should first clean them up thoroughly. The simplest method is to save the Word document in RTF-format: this strips off all the hidden data, apart from the user- and organisation-names. However this also removes many of Word's features.

Some versions of Word allow data from older versions of the document to become visible . So it frequently happens that an Office file, originally produced on a PC, displays quite differently on a Mac.

The Versions option can be just as dangerous. A user can exploit the 'Versions' option to compile a history of the different versions of the document, and if need be access one of the versions. If the 'Versions' option is not switched off then, if the document is transmitted further, data can accompany it which was never intended for third parties. In many areas standard formats in Word are used to create templates. A powerful example is lawyers practising as communicating-lawyers. Even in the Internet, documents such as legal written opinions have surfaced which have exposed explosive amendments and additions.

It should also be explained that Word is not particularly economical when it stores documents. Our Document Cleaner can deal with all these deficiencies quickly and easily. Experienced users can also use a menu for selective cleansing.

DOC Cleaner



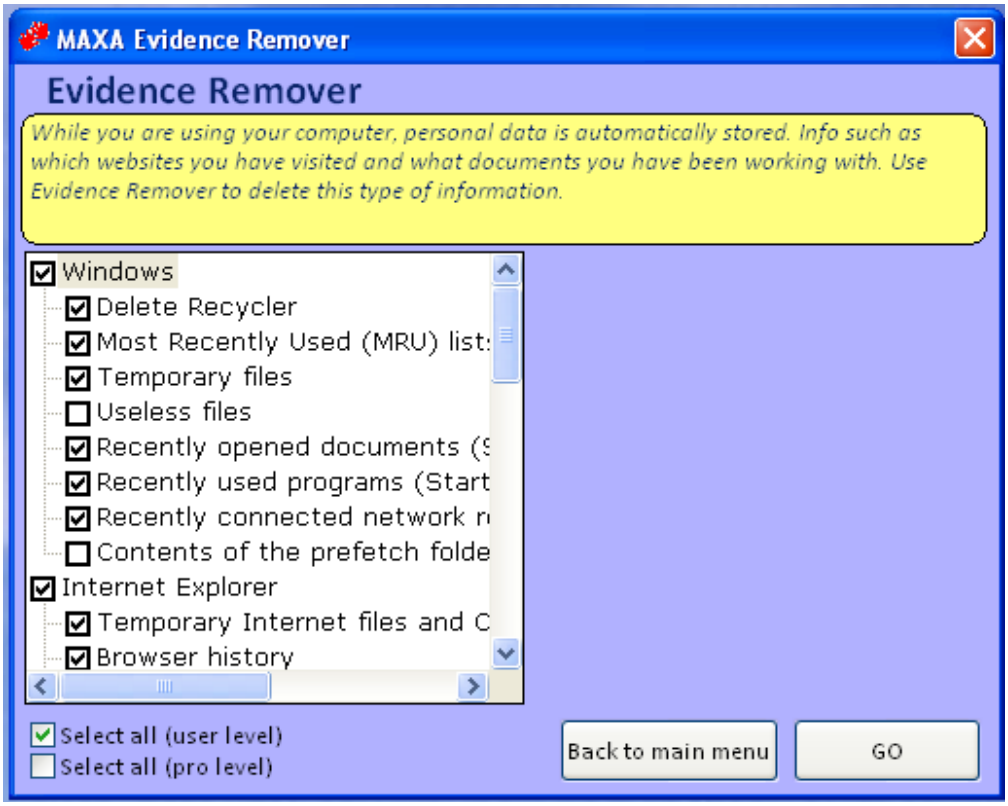
Evidence-Remover

The way that Windows operates produces a large amount of information which not only occupies a lot of space but also contains data not intended for third parties. External applications such as browsers can have the same effect. Thus it is essential to clean up all traces left behind on a PC after an Internet-session. This includes the deletion of the internet-cache contents, activity-history, cookies and offline Web-pages: also the list of recently used or selected documents, and programs utilised.

Our Evidence-Remover is the first in the world to be able to recognise and remove 'Super-Cookies' (**for any browser**) such as Flash Cookies.

Sometimes the installation procedures for some applications can leave vital data behind. These are often not recognisable by the average user. We have therefore created two different user levels, to make these options easier.

Trace remover



MAXA-Lock:

This is a module from MAXA-Crypt-SE which can also be used in stand-alone mode, as additional protection for a PC.

One of the biggest threats occurs when the work-station is left unattended, or is not switched off. It makes sense to leave a PC running, since this extends the useful life by reducing power-ons and power-offs (which in turn reduces temperature variations in the warm-up and cooling phases). Let's take a practical example, and consider the following recommendation:

Many Data Security Laws stipulates that data processing systems holding personal data should be protected from unauthorised access. Additionally, personal data should be protected from unauthorised access or data-processing.

That means that access to unattended PCs should be blocked. Clearly, if this risk is not catered for then there is an obvious security threat. It is now recognised that the

various screensaver solutions are no longer up to the task, since they can easily be bypassed by a hacker. We need to use an external solution instead.

Our software-house has been successfully involved in the security arena for many years. Even today, applications such as MAXA-Crypt are seen as 'uncrackable'. For the wider application market we have now concentrated on some additional focal points, e.g.:

- Automatic access control
- Soft lock
- Intuitive user guidance
- Internet-integration
- Screen-saver emulation
- Info-screen
- Multi-media support
- Skype-integration
- Multilingual (*German, English, Spanish*)

The end-result is a desktop-security software known as MAXA-Lock, the first to offer multi-media capabilities and also Skype-integration.

What is MAXA-Lock?

MAXA-Lock is a Windows software application which helps users to conform to their security requirements by reliably protecting their unattended systems, without them having to be switched off.

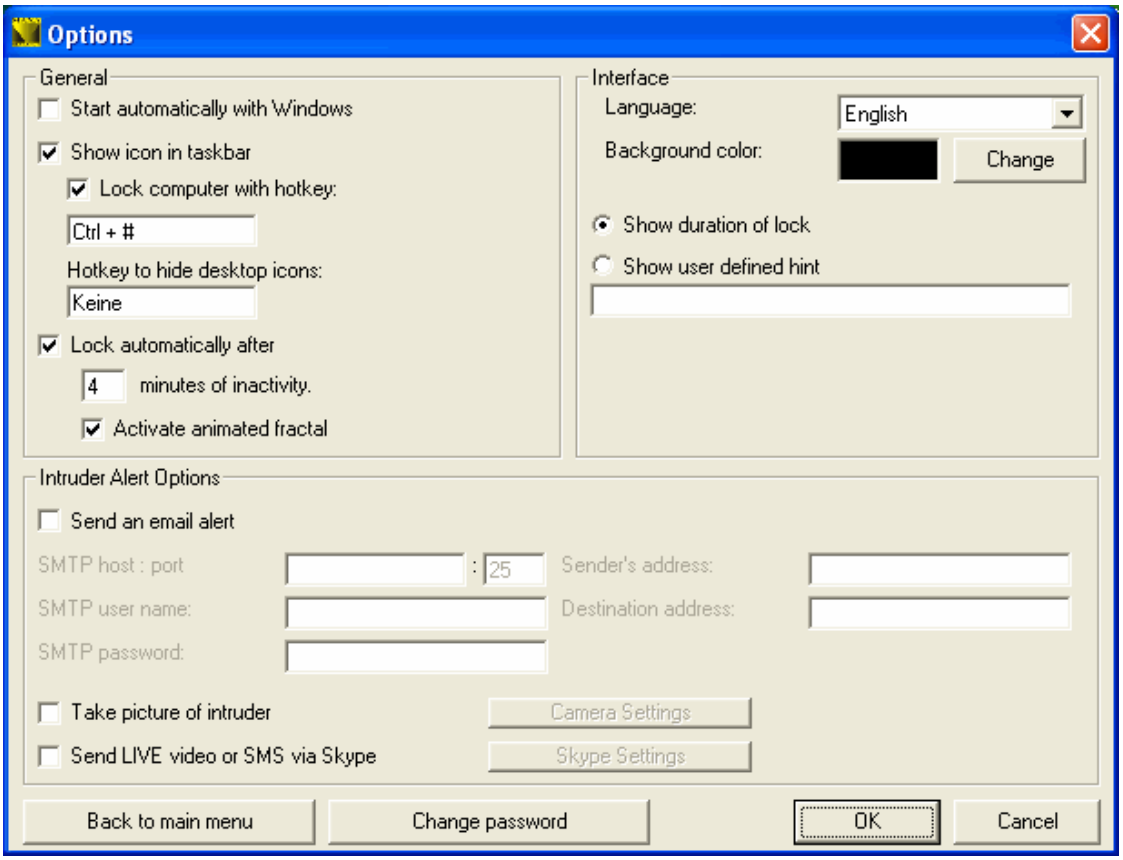
What can MAXA-Lock do?

The software obscures the monitor temporarily, limits the functionality of input devices such as the mouse or keyboard, such that unauthorised personnel cannot view or access the contents of Windows PC. Naturally this also handles unauthorised remote control systems, e.g. from an Internet-café. If a user leaves his PC and forgets to switch on the protection system, a Security Sensor Timer would activate after a selected time period.

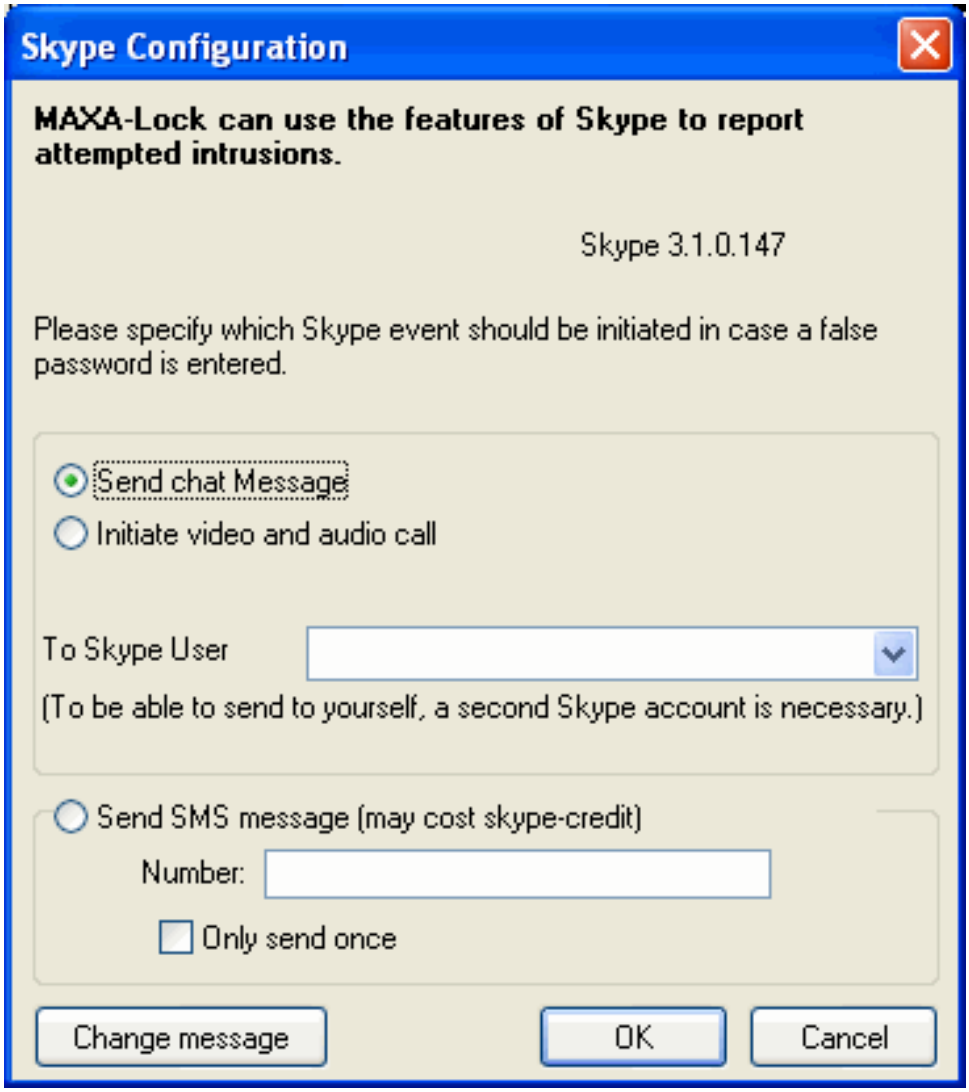
Anyone who works for long periods in front of a PC screen needs to take breaks. Both physical and mental relaxation are important, to relax the mind and improve alertness. We provide optical support by implementing a fractal screen-generator. Complex mathematical calculations generate an infinite sequence of flowing, soothing geometric patterns. The mix of structure, colour and time phases coordinates the

observer's relaxation. Pressing a key or moving the mouse switches the screen back to the security display. The integral Anti-Icon mode causes desktop icons to temporarily disappear from view. Airline travellers can hide from their neighbours which systems are installed on their PC. If for some reason the PC has to be closed down quickly, this can be done via an icon in the MAXA-Toolbar.

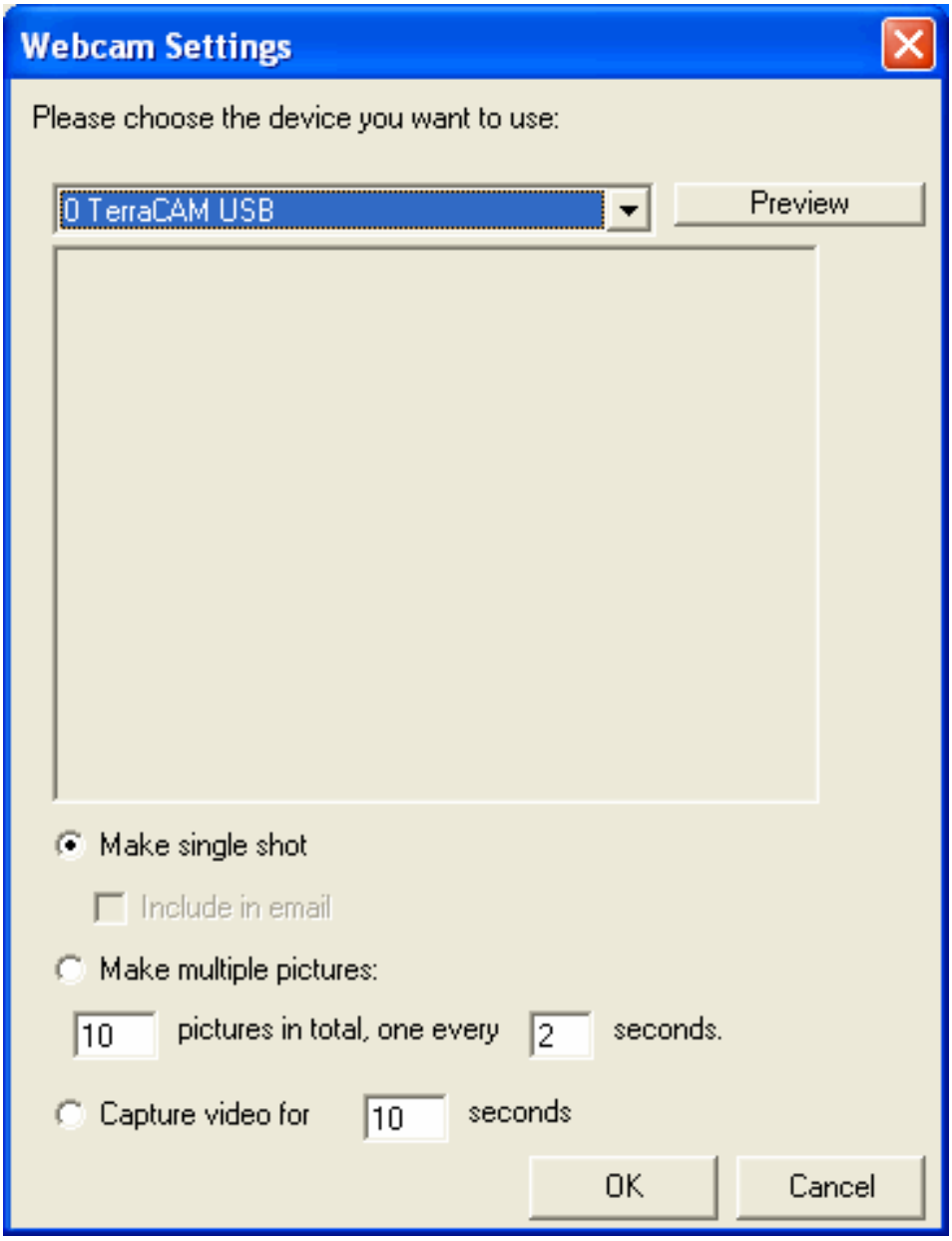
Option Menu



Setup for Skype



Cam Setup



How does MAXA-Lock handle attacks?

If an incorrect pass-phrase is put it, this triggers an alarm procedure to produce various warning-levels. Where practical, warning-levels can be combined.

Mail Mode:

Each wrong pass-phrase is recorded and forwarded by email to a specified address. If multiple PCs are blocked, the PC names are used to differentiate.

Picture Mail Mode:

Each wrong pass-phrase is recorded and forwarded by email to a specified address. If a Web-camera or IP-camera is connected, the image captured will also be forwarded. If multiple PCs are blocked, the PC names are used to differentiate.

Video Mode:

Each wrong pass-phrase is recorded and forwarded by email to a specified address. If a Web-camera or IP-camera is connected, the individual image is captured and a sequence of images or a complete video will be stored: these can be displayed locally after unlocking the workstation.

Skype Mode:

Each wrong pass-phrase is recorded and forwarded via Skype to a specified Skype address as a chat message. If a Web-camera or IP-camera is connected then everything that the camera captures will be forwarded live.

If you concealed the camera somewhere in your room then this will not be obvious to the person being monitored. Anyone with mobile Skype access will be able to utilise this service in both ways. Alternatively the information can be sent via SMS.

Can you be confident in MAXA-Lock?

No security measure is 100% certain secure against attack! However, in practice the effort required can exceed what is practical (physically, thermo-dynamically, etc.) In other words, the effort required bears no relation to the chances of success.

In MAXA-Lock, in addition to the professional software methods employed, we also put in various blocks and counters to the various tricks and tactics used by hackers and crackers. So in order to carry out a practical attack, more and more time will be required. As this goes on, the alarm responses are being triggered and evidence is being gathered. The attacker will soon decide to break off his activities, in order not to compromise himself further.

MAXA-SecurEdit

The disadvantages of a container solution on local disk drives outweigh the advantages. The limited flexibility, static dependency factor and high degree of function- sensitivity make the risks unacceptable.

Data could be irreplaceably lost through faulty installations, operational mistakes, damaged or impairment from 3rd-party applications.

We have therefore chosen a different direction entirely, and developed MAXA SecurEdit. The integrated text-processor (similar to Windows Wordpad) and its ease of use allows purely-executable EXE-files to be created, edited and distributed, out of encrypted text.

Additionally the program can be used as an editor, to produce formatted text, insert pictures or open existing RTF- or ASCII-based files.

These documents can be stored as EXE files, using a pass-phrase. The text-content is then integrated within, and recoverable from, the EXE file, encrypted with Rijndael 256. These executable files can be transmitted or saved, whilst keeping the contents securely encrypted. Such a transmitted EXE file can be opened under any Windows version: using the appropriate password the files can be located and stored in RTF-text format.

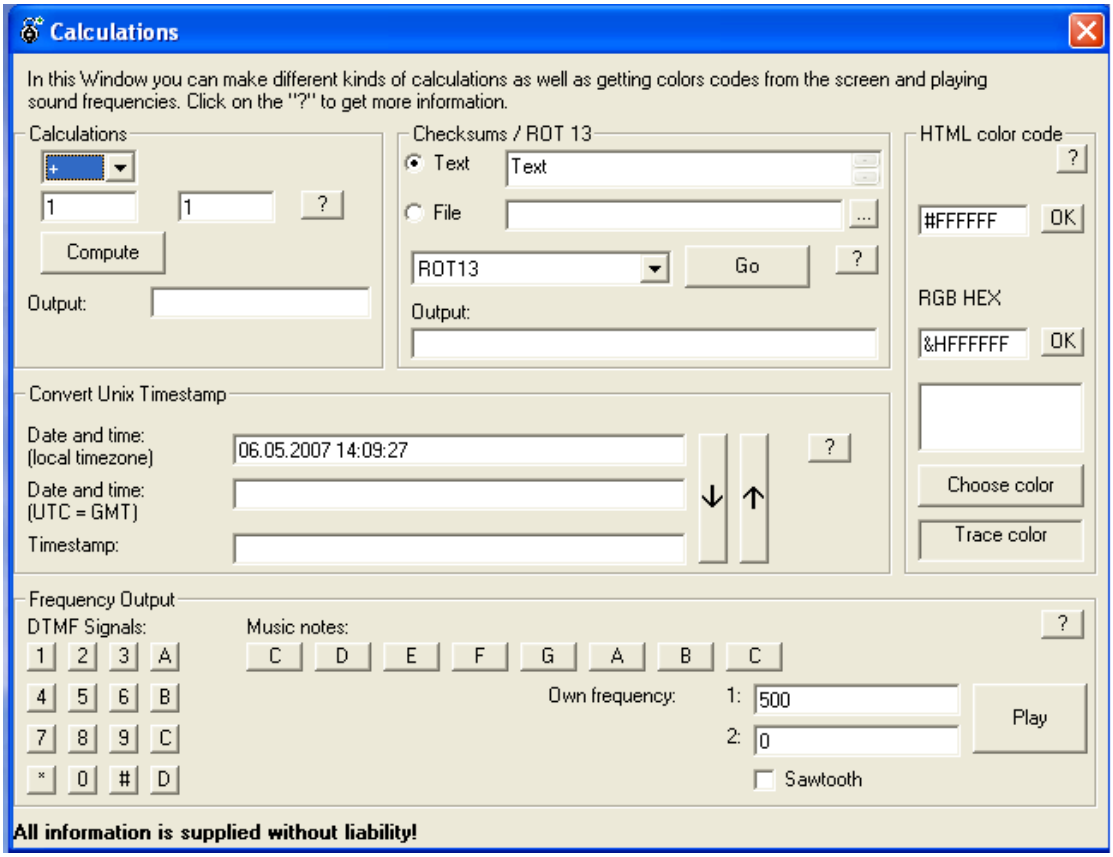
Many email-filtering systems block EXE files, so an option has been included to allow the file to appear as a ZIP file.

A typical example in use. A lawyer can send a complete folder securely by email using FTP. This example could be carried out in many different ways.

MAXA-Security-Tools will be used in many countries, so situations could arise where, deviating from the International ISO standard, non-standard values appear. The appropriate conversion facilities have been developed for such cases. Extra capabilities have been developed for such specialist users, e.g.:

- Calculation functions for numbers theory
- Checksum calculations to uncover data file changes
- Colour-coding tables for visual access-control
- Time calculations
- AT&T signals
- Frequency generator
- Frequency variations

Each of these functions comes with its own Help-facility, so it may be used without major familiarisation training.



What versions of MAXA-Security-Tools are there?

There is a demo version, free-of-charge for private users: note that this version (*MAXA-Security-Tools-Lite*) has some restrictions in capabilities. Updates for this version are also free, as long as the user is registered (*also free-of-charge*).
MAXA-Security-Tools (*Full Version*) is supplied as a licensed package for two installations. This licence is linked to a single user, and is not transferable.

Minimum hardware and software requirements for MAXA-Security-Tools.

Hardware: Pentium II, 266MHz, VGA, keyboard & mouse (*or equivalent*)
Software: Windows 98 / 98 SE /ME / 2000 / XP /Vista or equivalent.

Note:

- Internet access required to register the product on installation.
- If Mozilla Firefox is already installed, M-S-T will automatically integrate itself into the browser.
- Errors & Omissions Excepted
- This paper reflects the technical situation as at MAY 2007
- MAXA and the text and image references are registered trademarks of MAXA Research International, Inc.
- Any other trademarks mentioned are the property of the registered owner.

➢ **E N D**