Safe DOC
The Ultimate Data Encryption

IT IMAGING
SECURE · ARCHIVE · RETRIEVE

TECHNICAL DESCRIPTION (SEPTEMBER 2015)

The **SafeDoc** application is using 3 different methods to encrypt/decrypt files:

**AES_S Algorithm:(„very“ secure)**
Standard AES 256 Encryption/Decryption
→ Needs 1 Key

**AES_M Algorithm:(„extremely“ secure)**
Standard AES 256 Encrytption/Decryption
→ Using Changing Key

**AES_X Algorithm:(„completely“ secure)**
No further details can be disclosed on this method.

## Changing Key Encryption/Decryption

- It runs on top of AES256 standard encryption
- Is using the (custom) Changing Key algorithm
- The Encryption / Decryption will apply a different change key
- The change is dynamic
  - Static: The change of the current key is always in the same manner
  - Dynamic: Every change is different than the other

## Number of possible combinations

- One change is calculated with different functions, each with endless possibilities having additionally a variety of independently changing calculation depths. Using the maximum calculation depth is a „full reproductive change“ and it has a complexity of countless possible combinations.

- The resulting key will be a certain X bit. The total permutation will have zillions of possible combintions.

## Platform availability

- The **SafeDoc** application is currently available on Windows and Linux systems. Additional availability in the mobile sector is planned.

Naardenstraat 44 • 5045 ML Tilburg • The Netherlands • Tel: +31-(0)13-5711626
E-mail: info@it-imaging.com • Website: www.it-imaging.com

# Questions & Answers

➢ **Is it possible to get some conclusion about Change Keys ?**
**No ...**
When you manage to decode the first change, you have a certain Key A
When you then manage to decode the next change, you have another Key B
And so on ...

➢ **From two Keys do you have a chance find out the change of the Key?**
**No ...**
Additionally to the above the Key Change mechanism will change every time

➢ **Is the change hard coded in the program?**
**No …**

➢ **If you hack the program, can you conclude the change?**
**No …**
Keys and the changes are defined by the Keys (themselves) and not by the program

➢ **If you hack the program and find out how it works, can you conclude the change?**
**No …**

Let's assume you apply the Key Encryption on a text. With some effort you may find out the first change, then the 2nd, then the 3rd and so on. You would need to repeat this endless times, yet you still would not find any structure or system or an underlying rule.

➢ **Is this method not too slow for encrypting or decrypting a big number of files ?**
**No …**
The algorithm has been tuned over several versions using different methods for optimum performance dealing with big number of files and / or big size of files. Furthermore it can handle sub-directory structures of any depth with a high speed encryption / decryption despite the complexity of the used algorithm.

➢ **Why is SafeDoc faster and at the same time more efficient than existing competitors ?**
**No …**
International studies are showing the weakness of DATA protection versa system servers or network protection.
Even if unauthorized access breaks into the system, there is misuse or access possible to sensitive data, protected by **SafeDoc** .
The stolen data is simply unusable.

Safe DOC
The Ultimate Data Encryption

IT IMAGING
SECURE · ARCHIVE · RETRIEVE

TECHNICAL DESCRIPTION (SEPTEMBER 2015)

# Questions & Answers

➢ **Why is not simple to use encryption and protection from the big players ?**
Most existing products are working toward full disk encryption or a complete system protection, which makes them slow, vulnerable and resource intensive.
**SafeDoc** offers a selective approach of different levels in data security instead of "all-in-one". This way it is an extention to an even higher level of security rather than a replacement.

➢ **Why is SafeDoc encrypion superior to existing main players, like Symantec Mcafee ?**
**SafeDoc** is a completely new approach toward encryption, which has not been cracked yet by anyone. It is not a main player product, yet going far beyond the currently known secure encryptions. At the same time it is completely unknown to hackers being a new niche player.

➢ **Is this method totally secure and impossible to crack ?**
**No …**

Everything is breakable. But, it takes a really unusual and heavy effort to crack it. If it is combinded with one (AES_M) or with even more encryptions (AES_X) it offers an unprecedented level of high protection of your data. To „crack" this you need to know all of the following:

- The algorithm
- Multiple passwords
- Miscellaneous additional information (not disclosed)

➢ **How are the passwords protected ?**
The algorithm does not take any strings of the password. It uses byte arrays.
Capturing the password from keyboard (screenshot) can be avoided by using KeyFiles:

- KeyFiles should be created on a different machine
- KeyFiles contain the actual (random) passwords
- KeyFiles are themself encrypted using AES256
- KeyFiles are a pair of asynchronous passwords with special protection

# Product Demo

- Customers can upload sample data on our website www.it-imaging.com which will be encrypted
- Once the text document has been encrypted by **SafeDoc** the customer can download it from our website http://www.it-imaging.com/ and try to open it in order to see the value-added protection

Naardenstraat 44 • 5045 ML Tilburg • The Netherlands • Tel: +31-(0)13-5711626
E-mail: info@it-imaging.com • Website: www.it-imaging.com