In the name of Allah

Arg disk encryption software

1. Introduction

Nowadays, by the development of information technology, various and modern Forms of storing data have been innovated. New media are able to store higher volume of information with lower costs easily with higher degree of transportability than before. It makes ordinary users, private, governmental and even military organization personnel to have their confidential data on these media ignoring the risk of getting lost or being stolen. Therefore, the risk of exposing intimate and sensitive information always threaten individuals and organizations.

The following is the list of common hazards:

- Unauthorized access to military confidential documents
- Unauthorized access to important financial documents of an organization
- Unauthorized access to projects and artifacts of an organization
- Direct access to the files of a database without authentication
- Stealing personal computer, external hard or flash drive that results in access to personal files

A good solution for protecting data storage media is using disk encryption softwares. In this solution, one or more secure virtual partitions are created on a computer and every file or folder on the partitions will be encrypted. **Arg** disk encryption software, is a product of Payampardaz corporation that uses this solution to provide a security service.

2. Arg software

Arg disk encryption software is a product used to store data securely on various media like hard disks, flash drives, CDs and DVDs. In this software, one or more secure virtual partitions are created on a computer and every file or folder in it will become encrypted. User access to these partitions is fully transparent, it means the user interact with secure virtual partition like other partitions and the **Arg** encrypts data on-the-fly while writing and decrypts it when reading automatically without user intervention. After data encryption,

there is no way for unauthorized accessing to data and data confidentiality is guaranteed on media theft.

Arg uses encryption keys for its operation which are securely stored in a security token named KeyA. Since KeyA token needs Personal Identity Number (PIN), secure partition data is accessible through two-fase authentication. In fact, an unauthorized access to another person's module can't put secured data in jeopardy.

To use secure partitions, the user logs into the software using KeyA module and it's related PIN, then he mounts the virtual partition and a new partition is added to the system partition's list consequently. From now on, the user can use secure partition the same as the other partitions. Finally, the user logs out or just detaches the KeyA module from USB port, so the secure virtual partition data is not accessible anymore.

Arg have the ability of defining several different encryption keys for partitions security. This lets users to give different access levels to encrypted partitions. For example, the user can share a virtual partition that encrypted with an agreed encryption key with a group of colleagues and share another virtual partition with different agreed encryption key with second group.

In the case of losing token, the encrypted partition will be accessible if user buys a new token and transmits the profiles from the backup file which has been created in the time of creating profiles. But if the user also loses the profile backup file, he will not be able to access the encrypted partition and the data will be lost.

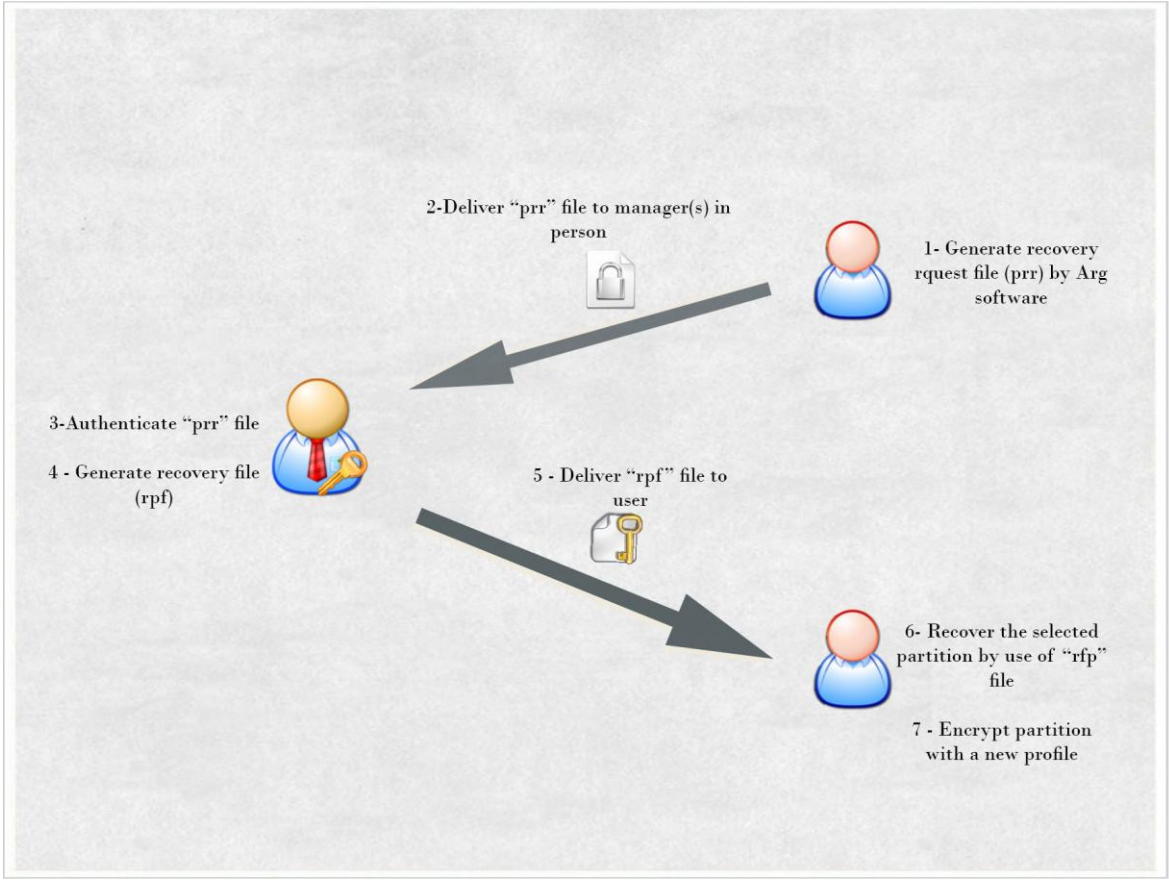
A new feature with name "skeleton key ability" is added to Enterprise Edition of Arg software to make partitions recoverable, even in this situation. In this edition, RSA Asymmetric Cryptography[1] is also done on partitions. This encryption is done by two pairs of RSA keys. Each of these keys are saved on a Keya token and according to the organization's politics, these tokens are given to one or two managers.

Each organization user who uses Arg, has his own token. This token contains username and two public keys which are written on that at the time of programming token.

At the time of creating partition, in addition to encrypting partition with user's profile, RSA encryption is done by use of two public keys.

[1] RSA Algorithm is an Asymmetric Algorithm. In these algorithms, the encrypting and decrypting keys are different. RSA encryption is done by the RSA key pairs, which contains a public key and a private key. Encryption is done by public key which is available for everybody and decryption is done by private key which is secret and it is just accessible for the person who is authorized for decryption

When recovering partition is needed, user should create the Request Recovery File by Arg software and give it to manager(s) in person. This file contains necessary information for Decrypting partition. For Decrypting this file and create recovery file, presence and confirmation of manager(s) who own the two private keys is necessary. Manager(s) will Decrypt the file and create the partition recovery file by attaching their token to the system. Then by accessing to the username which is placed in the source file, and confirming that the file belongs to the person who has brought the file, they give him the recovery file. User will recover his partition in Arg software by use of the recovery file and he will encrypt it again with another profile. Partition recovery process is shown in picture 1.



Picture 1 : partition recovery process

Generating RSA pair key, programming manager tokens, decrypting request recovery file and creating recovery file are all done in Arg Manager software.

3. Characteristics

3.1. Key features

- Supporting NTFS and FAT file systems

- Using a unique encryption algorithm for data encryption (can be ordered by customers)
- Accessing secure partition using **KeyA** token and its related PIN
- Secure partition encryption/decryption transparency from user's perspective, so the user would not get involved with complexities and the **Arg** software does the encryption operation without engaging him
- Fully secured storage of keys in **KeyA** token (keys are unreadable from the token)
- The ability to define several different encryption keys for disks security
- Temporarily decryption of secure partition data in RAM
- The ability to mount secure partitions from a network and portable disks like flash drives, CDs and DVDs
- Filling free spaces of the secure partitions with random bits
- Unauthorized users aren’t able to see secure partition contents like file names, folder names and their contents in addition to disk free spaces
- Supporting windows XP, 7 and 8 operating systems

3.2. Facilities

- The ability to transport secure partition to other computers
- The ability to share the secure partition with other users

- The ability to access a secure partition as Read Only by several users
- The ability to Mount secure partition after logging in automatically
- The ability to open secure partition in windows explorer after mounting automatically
- The ability to prevent user from changing encryption keys by administrator
- The ability to backup header partition and restore it after system crash
- The ability to export encryption keys existing in the **KeyA** token to a file and import them from file to token
- The ability to protect virtual partition from unwanted removal and modification
- The ability to choose drive letter automatically
- The ability to dismount secure partition automatically in case of error detection in the application or operating system

- The ability to dismount secure partition automatically in power saving mode or after logging off, hibernating or activating Screen Saver