Arg: Disk Encryption Software

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 **Arg** disk encryption software. This product is used to secure data on various media like hard disks, flash drives, CDs and DVDs. In the **Arg**, one or more secure virtual partitions are created on a computer and every file or folder on the partitions will become encrypted. User access to these partitions is fully transparent, it means that 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 needs a security token named **KeyA** for data encryption. Without accessing to this token and its password, there is no way to read data in the secure virtual partition.

Usages

- Protecting sensitive personal or organizational data on computer hard disk and portable media like flash drives, CDs and DVDs
- Providing secure private space for each user in a multi user system hard disk
- Sharing secure virtual partition in the network, Subsequently just authorized users have permission to read it's content

General characteristics

- Nice and simple user interface
- Supporting English and Persian languages
- Useful helps in all stages for users
- Creating secure virtual partitions
- Transparency of the Secure virtual partition from user's perspective
- The ability to transport secure virtual partition to other computers
- The ability to share secure virtual partition in the network
- Unauthorized users aren’t able to see secure partition contents like file names, folder names and their contents in addition to disk free spaces
- The ability to backup header partition and restore it after system crash

Security Charachteristics

- Native encryption algorithm with the key length of 256 bits (can be ordered by the customer)
- Accessing to secure virtual partitions data through two-phase authentication by KeyA security token and Personal Identification Number (PIN)
- Secure storage of encryption key in the KeyA token
- The ability to backup encryption keys stored in the KeyA security token
- The ability to recover a partition even if it's profile backup file has been lost or the token is rotten
- The ability to define several different security profiles to manage access level
- Filling free spaces in secure partitions with random bits

Compatibility

- Supporting windows XP, 7 and 8 operating systems (all 32 and 64 versions)