

## METHOD AND SYSTEM FOR SECURELY ARCHIVING CORE DATA SECRETS

### RELATED APPLICATIONS

This application is a continuation-in-part of U.S. patent application Ser. No. 08/884,864, filed Jun. 30, 1997, by inventors Matthew W. Thomlinson, Scott Field, and Allan Cooper, entitled "Protected Storage of Core Data Secrets," still pending.

### TECHNICAL FIELD

This invention relates to systems and methods that provide central services for securely storing core data secrets such as passwords, cryptographic keys, and sensitive personal or financial codes.

### BACKGROUND OF THE INVENTION

Increasingly, financial and other sensitive transactions are being performed by personal computers. This has increased the need for secure storage of data. Modern cryptography techniques are often used to protect such data from unauthorized access.

New security methods, however, have brought about a need to store and protect "core" data secrets, such as private cryptographic keys, credit card numbers, and other small pieces of secret data. Presently, this responsibility is left to individual application programs or to personal computer users themselves. Although programs are available that allow users to encrypt and store data, such programs cannot typically be used by other application programs. Currently, each application program has to devise a safe and secure method to store such data.

As an example of the problems associated with the current state of the art, consider the issues involved in exploiting smart card technologies. A smart card is particularly well suited as a receptacle for core data secrets such as those described above. In addition, smart cards can be used to authenticate users by requiring each user to insert his or her personal smart card into a receptacle associated with the user's personal computer. Tamper-proof smart cards have been designed for just these purposes.

Problems arise without agreed-upon standards for using such devices. Although a developer could provide capabilities for working with a limited number of smart cards, it would be difficult or impossible to anticipate all the different variations that might eventually arise. This fact makes it impractical to implement smart card technology in various different applications.

Although some storage media such as magnetic hard disks do not present the challenges of smart cards, many software developers simply do not have the background and knowledge required to safely implement modern cryptographic techniques. Even if they did, it would be inefficient for each developer to undertake the complex task of developing a method of storing core secrets. Furthermore, resulting solutions would be incompatible. It would be much more preferable to adopt a common scheme for storing such data, and to avoid having to implement a new solution for every different application program.

The common scheme described below allows a user's core data secrets to be securely stored on the user's local computer. The core data secrets are encrypted on the user's computer with a locally generated encryption key that is derived from a logon secret (such as a password) supplied by a user during a logon procedure. A problem arises in network

environments in which the user's password (or other authentication information) can change without participation of the local computer. This can happen, for instance, when a network administrator resets the user's password. It can also happen when a user changes his or her network logon password when using a different computer. When these events happen, it becomes impossible to regenerate the local encryption key. Thus, the inventors have realized a need to backup the local encryption key for potential recovery. However, it is not desirable to simply store the master key on the user's computer, since this would make it recoverable by hostile entities. Although the local key could itself be encrypted and stored on the local computer, this would involve another key which would then need to be protected. Thus, the invention concerns the storage of local encryption keys and other items that need to be securely stored on the user's local computer.

### SUMMARY OF THE INVENTION

The invention described below provides central protected storage services that can be called by application programs to store core secrets. An embodiment of the invention is implemented as a server process and associated interfaces that can be invoked by application programs to store and retrieve small data items.

The general method and architecture includes a storage server and a plurality of installable storage providers and authentication providers. Each storage provider is adapted to securely store data using a specific type of media, such as magnetic media or smart cards. Details of the storage medium are hidden from the calling application programs. Authentication providers are used to authenticate users by different methods, such as by requesting passwords, by reading smart cards, by retinal scans, or by other ways that might be devised in the future. Again, authentication details are generally hidden from the calling application programs.

Application programs interact with the storage server through well-defined interfaces. A data item can be stored with a simple call to the storage server, and can be retrieved later with a similar call. All encryption, decryption, item integrity checks, and user authentication are performed by the storage server and its associated providers. Because of this, application programs can take advantage of advanced security features without adding complexity to the application programs themselves.

When storing a data item using the protected storage services, an application program can specify rules that determine when to allow access to the data item. Access is generally limited to the computer user that created the data item. Access can similarly be limited to specified application programs or to certain classes of application programs. The storage server authenticates requesting application programs before returning data to them.

A default authentication provider authenticates users based on their computer or network logon. Other authentication providers can also be installed.

A default storage provider allows storage of data items on magnetic media such as a hard disk or a floppy disk. Data items are encrypted before they are stored. The encryption uses a key that is derived from the authentication of the user. Specifically, the key is derived from the user's password, supplied during computer or network logon. In addition, an application program or the user can specify that certain items require an additional password to be entered whenever access to the data is requested.

The default storage provider implements a multi-level key encryption scheme to minimize the amount of encryption