

SafeStick®

White Paper

General Summary

SafeStick® is a password protected USB Flash Drive with automatic hardware encryption.

USB class: Mass Storage
Encryption: AES 256 bit
Key storage: Hardware
Password: Compulsory, complex
Volumes: Public CD-ROM, Private removable disk
Storage: Highest grade NAND flash
Capacity: 512MB to 32GB

Revision

Johan Söderström	Original document creation	2008-04-03
Johan Söderström	revision 1.0	2008-04-18

Security Overview

Password Evaluation

The authentication scheme in SafeStick is simple. No information can be read from the flash memory until a password is evaluated correctly by the USB controller. The USB controller will not accept any unlock command not containing a correct password.

Hardware Encryption

All encryption is made in hardware before it is stored on the flash memory. In the same way, information read from the flash memory will be decrypted before it is sent to the host computer. The host computer will never take part in any encryption or decryption of stored information. The AES encryption uses 256 bit random keys and standard CBC mode.

Key Protection

The AES keys used for encryption will only be available to the USB controller. As opposed to software based solutions there is no possibility to obtain information about encryption keys from the host computer. All information stored on flash is protected by a unique key inside the controller.

Brute Force Protection

The USB controller will keep track of all failed login attempts in an internal counter and when this counter reaches 20 it will lock the device down and throw away the encryption key. This ensures that a user password cannot be obtained through brute force attacks.

When SafeStick is locked down it must be reset to factory settings to function. This will erase all information on flash and generate new encryption keys.

Compulsory Complex Passwords

A user is required to choose a complex password that cannot easily be guessed and there is no function to disable the password protection. This will ensure that all information is stored securely at all times.

Software Protection

The SafeStick software is itself encrypted and protected against debugging and tampering as is the communication with the device. All commands sent to SafeStick are encrypted with a 1024 bit RSA key and verified by the USB controller.

Automatic Lock Down

In case SafeStick is left in a computer unattended, it will lock down automatically after a few minutes of inactivity. This feature will prevent unauthorized access of information on SafeStick even if it is left unlocked on a public computer. SafeStick will also sound a reminder if left in the USB port when the user logs out from Windows. The time for automatic lock can be configured by the end user.

Other Advantages

Interoperability

Since the encryption is made on hardware level, SafeStick will after authentication has been made behave like any other USB drive. Any solution deployed in the company network will treat the storage area as a standard file system on a removable device. It is therefore possible to use SafeStick together with enterprise level information management systems, port control software and even device encryption software.

User applications such as office suites will also be able to work directly against SafeStick and there is no need to store any information on a hard drive of a previously unknown computer's when saving or using documents on SafeStick as would be required using software based encryption.

Standalone User Interface Software

SafeStick carries its own user interface on a public, read only partition presented as a CD-ROM. This user interface communicates with the SafeStick hardware and will enable users to interact with SafeStick on any computer without the need of installing any software, drivers or using administrative privileges. All parts and protocols are based on the USB standard supported by drivers included in all Windows versions since Windows 2000 SP4. No software will be installed or copied on to the host computer.

Localization

SafeStick supports multiple languages and the user can choose between these in order to get the best user experience.

SafeStick Add-On Features & Management

The SafeStick solution offers a wide range of add-on features making it extremely flexible. It is possible to tailor the configuration to the organizations requirements. The management features are handled mainly through SafeConsole, the SafeStick Management Console.



Password Recovery

In order to enable recovery of important data on SafeStick when users have forgotten their passwords, SafeConsole will give the IT department the possibility to restore a password on SafeStick without losing information, even for remote users without physical access to the office.

SafeConsole stores encrypted authentication information on SafeStick. This information can be decrypted only by the IT department with their private keys. All information is protected by RSA 1024

bits PKCS1 encryption and OAEP padding offering semantic protection. This means that information cannot be guessed even when all possible clear text values are known to an attacker.

The scheme is based on challenge response. When a user has forgotten a password he or she may send a unique request code to their IT department or help desk. The help desk feeds the user code into the Safe Console server web interface and receives a Personal Unblocking Key (PUK) code. The PUK, once sent to the user, is used to reset the SafeStick password and allows the user to choose a new password.

All codes are random, unique and can be used one time only. No code can be used to unlock a SafeStick other than to which it belongs.

The server software is a Java based web application that can be deployed on any web server supporting Java and JSP. The web application supports an internal user database in order to restrict access to the application but can also be connected to Active Directory in order to do this.

Certificate carrier for soft certificates

SafeStick is able to store any number of X-509 certificates in its internal storage. These certificates will be accessible to the host computer and any service or application when SafeStick is unlocked. The functionality is the same as with a smart card or dongle with a few differences.

1. No driver or application is needed.
2. The solution is based on soft certificates and the private key are protected with encryption.
3. SafeStick can store multiple certificates with corresponding private keys.

Automatic login to online services

When SafeStick is unlocked it can provide an automatic login to an online service for its user. Credentials to the service along with its URL are saved encrypted in SafeStick's hidden storage. As SafeStick is unlocked, the credentials are unencrypted and used to log in the user to the online service with a single mouse click.

SafeStick Zone Builder

Zone builder provides single sign on to SafeStick on trusted computers within the company network. Users can change lost passwords and set up trust relationships with team workers.

Security is based on PKI and users certificates.

The solution also enables control over the overall SafeStick access for all users.

Enforce password changes

SafeStick is configurable to enforce a change of passwords in given intervals. After 120 days or 100 successful logins, the password must be changed by the user. A policy will also restrict the new

password to be significantly different from the previous password. The period between password changes can be configured.

Temporary Share

Consultants often share files with each other and customers. In order to do this without exposing their own sensitive files or passwords, SafeStick offers a temporary share where certain files can be shared with others protected with a temporary pin code. This pin code is also useful in order to allow other people add files to SafeStick without unlocking the private area.

Portable applications

SafeStick offer an ideal platform to store portable applications like VPN clients, browsers or mail clients. To make the usage of these quick and easy, SafeStick provides a quick launch menu upon login. With a simple click the selected application will launch.

Contact

BlockMaster AB
Jutahusgatan 8
222 29 Lund
+46 46-276 51 00
info@blockmaster.se

Johan Söderström
CTO
+46 46-276 51 05
+46 735-00 00 75
johan@blockmaster.se