

Security Hardware (USB Tokens and Smart Cards)

"USB Tokens" and "Smart Cards", commonly called tokens, both contain a tiny computer chip (secured EEPROM protected memory) for securely storing information. They are different in their form factor and interface. These are two technologically identical yet different things used for similar purposes.



This paper answers common questions asked about security hardware tokens:

- [Why use security hardware token?](#)
- [What does SilentVault solution store on token?](#)
- [Which one to use? USB Token or Smart Card?](#)
- [Some well-known tokens](#)
- [Why Silent Front supplies USB Tokens and not smart cards?](#)
- [How to set up token for use with SilentVault solution?](#)

Why use security hardware token?

The first main advantage of carrying this tiny computer chip whether on "USB Token" or "Smart Card", commonly called tokens, is their flexibility. There is no need, for example, to carry several tokens. One token can simultaneously be an ID, a credit card, a stored-value cash card, and a repository of personal information such as telephone numbers or medical history. **A token can be easily replaced if lost, and, because a password (or other form of security) must be used to access information stored on it, it is totally useless to people other than its legal owner.** At the first attempt to use it illegally, the token would be deactivated by the token protection mechanism itself.

The second main advantage is security. Tokens are encryption devices, so that the user can encrypt and decrypt information on it with a user-selected password. Thus tokens are very flexible in providing authentication.

What does SilentVault store on token?

Due to their Security, Application, Usefulness, Portability, Ease of Use, Durability, Flexibility and Deployment, **SilentVault Professional** ® edition stores the user information on USB token. This user information is required for storing and accessing protected data on the hard-disk. SilentVault only uses PKCS #11, international standard for security hardware tokens, compliant hardware token. (PKCS = Public Key Cryptography Standards).

Which one to use - USB Token or Smart Card?

While “USB Tokens” are typically smaller than a house key and are designed to interface with the universal standard bus (USB) ports found on millions of computers and peripheral devices, “Smart Cards” typically have credit card type interface and usually require a dedicated reader to be installed or plugged to the computer. Silent Front supplies one “USB Token” per license of SilentVault Professional Edition ® solution, when [purchased](#) using the “CD + Security Hardware Delivery” option.

If you decide to purchase, or have already purchased, security hardware from another vendor and need assistance then write to support@silentfront.com Ensure that you purchase a security hardware that is PKCS #11, international standard for security hardware tokens, compliant.

Some well-known tokens

There are several manufacturers of USB Tokens and Smart Cards. Some of them are listed here with their token product memory sizes:

Aladdin EToken PRO	16, 32, 64 KB	
Aladdin EToken R2	16, 32, 64 KB	http://www.aladdin.com
Rainbow IKey 1000/1032	8, 32 KB	
Rainbow IKey 2000/2032	8, 32 KB	http://www.safe-net.com
Schlumberger Cryptoflex	8, 16 KB	http://cyberflex.slb.com

SilentVault works with all tokens and smart cards that are PKCS#11 compliant (PKCS = Public Key Cryptography Standards).

Why Silent Front supplies USB Tokens and not smart cards?

1. **Application:** From an application view both are similar.
2. **Usefulness:** Virtually all PCs produced today have at least one USB port; the user can buy a USB token off the shelves and start using it. The USB Port provided on a PC can be used to connect a USB Token produced by any manufacturer. Most PCs do not have a Smart Card reader and all readers are not compatible with all smart cards. With the recent introduction of lower-cost readers, cost no longer poses a significant barrier.
3. **Portability:** Smart Cards fit nicely inside a wallet and are similar in look and feel to the typical credit card; USB tokens offer the convenience of being stored on a user's key chain. Storing on key chain significantly reduces the chances of losing or misplacing the token. It is not very convenient to remove a smart card from wallet, plug into a reader for use and then remove it from the reader to store back into the wallet. It is easy to plug or unplug a USB token carried on the key chain. However, both can be worn as a necklace and are being used so.

4. **Ease of Use:** USB Token drivers are easily installed on the computer to interface with the USB port and now in most cases are automatic. Smart Card readers can be difficult to install and configure.
5. **Durability:** Both seem to be equally durable. The chips inside both the USB tokens and the traditional Smart Cards cannot be physically tampered, and if they are altered in some way, the chips are designed to automatically destroy themselves. Fewer parts give USB tokens a greater level of durability. If readers and their parts are included in durability assessment then USB tokens have an edge over smart cards.
6. **Flexibility:** Both utilize either a port or hub on a PC. However most smart card readers have either only one or two slots. PC standards have now defined a maximum of 127 USB devices per machine. Moreover, lack of application standards associated with Smart Cards is an obstacle to flexibility.
7. **Deployment:** Smart Card implementations generally require external readers to be installed on each user's machine. Virtually all PCs produced today have at least one USB port.

How to set up token for use with SilentVault?

If you [purchase](#) SilentVault Professional Edition ® using the “CD + Security Hardware Delivery” option, you will receive printed instructions for setting up the USB token on your computer. You can also [download](#) our step-by-step guide for installing the software and the security hardware for proper use.

If you have purchased the security hardware from another vendor then follow the supplier’s instructions. The manufacturer of the USB Token and Smart Card supplies the hardware driver software. Connect your security hardware to your computer and follow the manufacturer’s instructions to install the driver.

If you need assistance on setting up a security hardware that you already have, or wish to purchase it from another vendor, then write to us at support@silentfront.com

Technical Team, Silent Front
<http://www.silentfront.com>