

Choosing the right Portable Security Device

When it comes to choosing a Portable Security Device (PSD), some key security factors must be taken into account. At the same time, you must go beyond the marketing hype to make sound decisions based on ensuring the security of your day-to-day business activities.

Driverless is the way to go

A minimum requirement for a PSD is a completely driverless device so that you can seamlessly carry data and applications from one computer to the next, irrespective of type or OS, without the burden of deploying and maintaining drivers. Similarly, administrator privileges on the machine should not be required. Most machines in large organizations are completely locked down and users have no privileges. Some devices need proprietary commands in order to operate, requiring elevated privileges, and will not work on machines where there are no such privileges granted to the user.

Software-based versus hardware-based encryption

Software encryption opens up the possibility of residual information about the encryption keys being left behind and fully exposed in the host's swap file.

Some USB devices use software encryption requiring software to be installed on the host PC. This not only reduces portability but also makes portability impossible for locked-down corporate machines.

In addition to the portability issue, software-based encryption is definitely a less secure way to protect data. Encryption algorithms could be potentially compromised, opening the door to hackers. So hardware encryption is the better choice...but not just any hardware encryption.

The huge difference between 128 and 256-bit AES hardware-based encryption

256-bit AES encryption is not twice as strong as AES - twice 128-bit encryption would be 129-bit encryption. In fact, 256-bit AES is the square of the strength of 128-bit.

That means AES 256-bit encryption is 340,282,366,920,938,000,000,000,000,000,000,000,000,000 times as secure as 128-bit.

And that enormous difference is the reason why AES 256-bit meets the minimum standards for the most data sensitive environments.

Different levels of User Authentication

User Authentication grants access to data stored on a PSD. For the most sensitive data, at least 2-factor authentication should be used.

Password Authentication

The minimum requirement for securely accessing the content stored on a PSD is password protection availability. However, the use of simple password protection won't withstand brute force attacks if the designated password itself is not very complex.

Strong Password Authentication

Strong password authentication relies on the availability of specific rules and policies that make the password difficult to crack.



Choosing the right Portable Security Device

Different levels of User Authentication *(Cont'd)*

Usage policies include:

- Retry limit
- Password reuse threshold (can't reuse any of the X number of the most recent passwords)
- Maximum password life (user is forced to change it periodically)
- Minimum password life (user can't change it rapidly, preventing abuse of the password reuse threshold)

Complexity rules define:

- Minimum password length
- Minimum number of special characters
- Minimum number of numeric characters
- Minimum number of alphabetical characters (lower- and uppercase specifiable individually)

Biometric Authentication

Not all biometric solutions offer the same level of security...the following options need to be taken into account:

- A secure biometric solution should not store any template outside of the security device
- Number of fingers that can be registered should be configurable
- Configurable biometric security levels
- Choice of fall-back mechanisms defining how biometric users will authenticate if biometric authentication fails

Strong Password and Biometric Authentication

The ultimate authentication level is the combination of strong password and biometric authentication, making it impossible to access the PSD without being an authorized user.

Flexibility of authentication options

The level of authentication should be flexible in order to meet the organization's security needs and accommodate the security requirements for specific groups of users.

An organization should be given the flexibility to require dif-

ferent levels of authentication for different user profiles. For example, some senior executives remotely accessing sensitive data could be required to use 2-factor authentication while other employees carrying information internally may just need strong password authentication.

Password or Biometric resets

When users are blocked from their respective devices, there should be options for rescuing the user. This means a way to reset a biometric or password authentication so that the employee can continue to do his or her work with minimal disruption. Organizations may want to think carefully before outsourcing password recovery or data backup services. Giving this type of control to a third party risks compromising critical corporate data and resources. Organizations should have the option of exercising full control over the reset of authentication mechanisms for their security devices.

MXI Security offers the option to manage corporate security device passwords through an internal help-desk function.

Data Recovery

Being able to recover data without the user necessarily being present is often a key requirement to comply with audit and data security regulations.

In addition, the corporate information stored on PSDs often belongs to the organization and PSD management solutions should offer a way to recover corporate data. This may apply, for example, in the situation where an employee is no longer with the company.

Destroying data on authentication failures

Just as data recovery is an important and necessary feature for some organizations, it is equally important to have a data destruction option. Some users may carry data that is so sensitive that its destruction is actually the best security, particularly when too many authentication attempts have failed. This capability should be optional and be fully configurable with a device management solution such as MXI Security's ACCESS

Choosing the right Portable Security Device

Enterprise™. You may not want to tell your CEO that the company business plan has been irrevocably destroyed because of a forgotten password.

Device Recycling

PSDs belong to an organization and should be considered as a corporate asset just like laptops. Do you buy a new laptop every time an employee leaves your company? Then why would you throw away your portable security devices?

The type of PSD you choose for your organization should be recyclable and/or re-assigned to new users as often as needed.

PSD Manageability

The deployment of security devices must be overseen and managed in order to maximize the benefits of data protection, portable applications, secure digital identities and strong user authentication.

Being able to remotely update software and security policies on devices already issued should be a 'must-have' feature, simply to keep up with ever changing corporate requirements and policies.

Furthermore, compliance with data security regulations and corporate governance requires that administrative roles for different tasks be separable and subsequent administrative operations be loggable (segregation of duties). Full administrative control of the devices and usage policies by the organization is also a key compliance requirement.

Asset management in any enterprise is key to ensuring sound security. Knowing exactly what you have in the field contributes greatly to building a security threat-proof matrix. Furthermore, knowing where you are vulnerable and where you are safe is crucial - any security professional can confirm that the greatest threat comes from unknown assets, namely, those assets deployed that you don't know about.

When deploying security devices, you want to make sure you know what person in the organization has what asset. Plus, you must have the ability to generate on-demand reports for a variety of reasons: property theft, security incidents, compliance audit, internal verification and so on. Knowing who has what and what he or she was doing with it reveals the answers to these areas of interest.

Making a smart investment

In order to fully leverage your organization's PSD investment, you may want to consider the benefits of carrying around not only critical data but also your highly sensitive digital identity credentials. An ideal solution is MXI Security's ACCESS Identity™ which enables mission-critical enterprise systems such as single sign-on, remote access, full disk encryption, PKI and others to be fully secured while allowing for total portability.