

Protiva™ Smart Guardian

||||| A higher level of security for portable data



ENTERPRISE > PRODUCT

One of the biggest information security challenges today is protecting the vast amounts of private and confidential data used by business organizations and government agencies. USB drives are a particular concern because most employees use them to store sensitive information and they can easily be lost or stolen. The economic impact of lost corporate data can be enormous and mitigating this risk has become a necessity. Many organizations are now deploying more personalized solutions to manage the risk of lost data in-transit, including USB data encryption and highly granular port control.

As the leader in digital security, Gemalto offers highly secure end-user devices that manage individual access to networks, applications and data. Its secure USB tokens protect data stored offline by controlling access to the device's flash memory and encrypting the data stored on it. Gemalto solutions for data loss prevention are easy to deploy and can be integrated into an organization's end-point security policies to provide the highest level of security for portable data.

Protiva™ Smart Guardian: simple to use, easy to deploy and support

Smart Guardian is a zero-footprint personal security device that protects

> Key features

- **Zero-foot print** plug-and-play on **multiple operating systems**
- **Works with end-point security products** from Microsoft, Lumension and other vendors
- **Supports PKCS#11** based smart card functionality and connected one-time password authentication
- Meets **FIPS 140-2 level 3 certification**
- Available with **2 and 4 GB memory capacities**

portable data with Gemalto's proven smart card technology. Unlike other secure USB memory products, it provides an unsurpassed level of data protection because all critical functions and cryptographic keys are managed from within the secure environment of the smart card module.

End-users simply insert the Smart Guardian into a USB drive and authenticate by entering a passphrase. The passphrase is validated by the smart card which

unlocks the device and then sensitive files can be copied and encrypted on its secure volume using familiar operations like drag/drop, copy/paste and "save as". It can then be locked and safely removed by selecting the appropriate command from a contextual menu.

Smart Guardian provides a complete, personalized data security solution that is easy for IT administrators to deploy and manage. It supports multiple operating systems and requires no drivers so deployment is quick and efficient. In case of multiple failed passphrase entries above a pre-determined threshold, the device will lock to protect against brute force attacks and unauthorized access to the encryption keys. It can then be unlocked by an administrator either locally or remotely using a PKI-based challenge – response process.

Smart Guardian is supported by Protiva Smart Token Management Service (SmartTMS) an in-house token management platform for enterprises. It enables end-user and administrators to register new devices, update software on the devices, modify registration information, unblock a token and block a lost token.

Protiva™ Smart Guardian

Personalized protection for sensitive data in motion

Overall advantages and benefits

> Highest level of USB data protection with smart card technology

The tamper-proof smart card module inside the Smart Guardian contains a high-performance microcontroller that generates cryptographic keys used to encrypt and decrypt data. The encryption key is secured by the tamper proof smart card, preventing brute force attacks against the device.

Its foundation on smart card technology makes Smart Guardian far superior to PIN-protected USB flash drives that are relatively common but significantly less secure. The security features of the smart card module and secure architecture of the embedded software help protect against hardware and software-based attacks.

> Enforce mobile data security policies

Smart Guardian works with major third-party end-point security products from major industry players and other vendors to provide a comprehensive solution for data loss prevention. It enables highly personalized control of all data stored and accessed on USB drives throughout the enterprise network.

> Lower total cost of ownership compared to other solutions

With support for industry standards, multiple operating systems and PKCS#11-based smart card functionality, Smart Guardian provides a significant cost advantage for organizations that need to deploy portable data protection solutions.



> Easily adapted to existing infrastructure

Smart Guardian has a standard USB interface and runs on Windows and Mac operating systems so it's highly adaptable. Together with the Protiva SmartTMS, it provides a comprehensive solution that is easily integrated into existing IT infrastructures.

> Flexible to support multiple security applications

PKCS#11 support offers the flexibility to implement other applications with the Smart Guardian. These include digital signature, secure remote access, connected one-time password authentication, and other PKI-based services.

> Smart card technology strengthens data security

Smart card technology offers several advantages for secure data storage devices:

Portability and ease of use

Digital certificates and flash encryption keys are always stored on the card, not externally. The smart card device can be used from any system without compromising security.

Access security

Data can only be accessed by the authorized user with two-factor authentication through the smart card operating system.

Cryptography

Smart cards provide a robust set of cryptographic capabilities including key generation, secure key storage, hashing etc. that are used to protect the data stored in the flash memory.

Manageability

Smart cards can block access after predefined number of unsuccessful passphrase entries have occurred. To restore access, a stringent PKI based challenge-response process is used. This prohibits any unauthorized access to the flash encryption keys and protects the authorized user.



www.gemalto.com