

# Protiva™ Smart Guardian FIPS

||||| Securing Mobile Governmental Data



## ENTERPRISE > PRODUCT

### Personalized protection for sensitive data in motion

One of the biggest information security challenges today is protecting the large amounts of private and confidential data used by business organizations and government agencies. Millions of USB drives are used today as a convenient way to transfer data between systems. For government agencies, the very same benefits that enable employees to work effectively and increase their productivity, pose risks of the loss, theft or misuse of unprotected, confidential data. Many government agencies are now deploying security solutions to manage the risk of data lost at endpoint, including USB data encryption and restrictive port control.

Gemalto, the world leader in digital security, offers a series of portable security devices that protect sensitive mobile data and management platforms for these devices. Gemalto products for data loss prevention are easy to deploy and can be integrated into endpoint security policies to provide the highest level of security for portable data.



### Protiva Smart Guardian: Security that meets compliance

Gemalto's Protiva Smart Guardian (SG) FIPS is a FIPS 140-2 level 3 certified zero-footprint personal security device with personal identity verification (PIV) integrated authentication ability. 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 Gemalto smart card module. Any attempts to tamper with the device will result in destruction of the crypto module rendering it useless to intruders.

Federal agencies have the option to strongly bind the SG FIPS to their employees' government issued PIV credential granting access to the protected storage based upon a successful PIV authentication. Sensitive files can then be copied and encrypted on its secure volume using familiar operations like drag/drop, copy/paste and "save as". Using this kind of multi-factor authentication ensures that only the authorized PIV user has access to the data on the device. Optional on-board anti-virus/ anti-malware solution scans and protects the device from malicious code. It can then be locked and safely removed by selecting the appropriate command from a contextual menu.

SG FIPS 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.

### Advantages and benefits for government agencies

#### > Highest level of security available today

SG FIPS offers FIPS 140-2 level 3 certification for encryption, assuring maximum security for mobile data based on a standard set by the National Institute of Standards and Technologies.

#### > Data protection with smart card technology

The tamper-proof smart card module inside the Smart Guardian FIPS contains a high-performance microcontroller that generates cryptographic keys used to encrypt and decrypt data. The 256-bit AES encryption key, the most secure block cipher encryption standard adopted to date, is secured by the tamper-proof smart card, preventing brute force attacks against the device.

# Protiva™ Smart Guardian FIPS

Its foundation on smart card technology makes SG FIPS far superior to password-protected USB flash drives that are relatively common but significantly less secure. The security features of the smart card module and lock-down mechanism that blocks access to the device when a set number of incorrect passphrase attempts is exceeded, together protect against hardware and software-based attacks.

## > Increasing productivity without compromising security

PIV integrated authentication provides the convenience of only having to remember one PIN. In addition, always-on 100% transparent data encryption takes the burden off from employees for meeting security policies. SG FIPS uses fast SLC memory that offers read and write speeds exceeding 20 Mbps.

## > Enforce mobile data security policies

SG FIPS works with endpoint security products from major third party vendors to provide a comprehensive



### Key features

- > FIPS 140-2 level 3 certification
- > PIV Integrated multi-factor authentication with increased convenience for end-users
- > On board anti-virus and anti-malware solution
- > Zero-foot print plug-and-play on multiple operating systems
- > Tamperproof and waterproof metal body
- > Smart card-based always-on encryption
- > Integration with endpoint security products
- > Available with 2 and 4 GB memory capacities

solution for data loss prevention. It enables highly personalized control of all data stored and accessed on USB drives throughout the enterprise network.

## > Easy IT integration

Smart Guardian has a standard USB interface and runs on Windows and Mac operating systems. It is easily integrated into existing IT infrastructures, thereby reducing IT integration costs.

## Smart card technology strengthens data security

When considering encryption method security and attack resistance, smart card based encryption (hardware-based encryption with smart card support) has clearer advantages than software-based and hardware-based encryption. It is also critical to take into account issues like performance and encryption availability before deciding on the type of encryption to implement.

	Software-based Encryption	Hardware-based Encryption	Smart Card-based Encryption
<b>Brute force attacks (including parallel attacks)</b>	Difficult to prevent	Prevented by blocking copying of data in its encrypted form from the device to the host memory	Immune to attack as encrypted data is never copied from the device to the host memory
<b>Security of Encryption Key at rest/after operation (e.g. resistance to Cold Boot Attacks)</b>	Can be prevented if secure memory is available on the PC	Prevented by not using RAM or other common memory space to store encryption keys, and by the fact that the keys never leave the USB flash drive	Immune to attack as encryption keys are generated and stored on tamper-proof smart card and never leave the USB flash drive
<b>Security of Encryption Key in operation (e.g. resistance to fault attacks, decompiling, dumping, debugging etc.)</b>	Encryption key can be accessed through various software attacks	Encryption key can be accessed through various hardware attacks (Controller Memory could be dumped, Controller Software could be reversed)	Encryption key cannot be accessed as it is copied from the smart card to controller memory only, after user is successfully authenticated
<b>Attacks on Authentication Counter leading to brute force attacks</b>	Not applicable	Resistant to software attacks  Possible physical attacks on auth counter management (dump / restore after decrement, fault attack on decrement etc.)	Software and hardware attacks prevented by EAL4+ certified, tamper resistant storage location. Cannot be compromised and counter decrement cannot be avoided
<b>Malicious code</b>	No way to prevent once the PC and its OS are infected	Prevented by using a security system independent of the PC and its OS	Prevented by using a security system independent of the PC and its OS
<b>Always-on encryption</b>	Can be disabled by user or attacker	Built into device. Encryption is automatic	Built into device. Encryption is automatic
<b>Performance</b>	Slower, since existing processing capacity is used	Fast, since dedicated hardware is used for encryption processes	Fast, since dedicated smart card hardware is used for encryption processes

[www.gemalto.com/enterprise](http://www.gemalto.com/enterprise)