

## Frequently Asked Questions

### General Product Questions

**Q:** What does SAFE stand for?

**A:** Secure Access For Enterprise

**Q:** Why does Lexar offer multiple SAFE solutions?

**A:** Lexar® JumpDrive SAFE S3000 FIPS is specifically engineered for government, military, and enterprise users who require ultra high security to meet agency directives

Lexar JumpDrive SAFE S3000 is designed for users looking for enterprise-level security that is scaled to meet the budget and performance demands of small businesses.

**Q:** What makes Lexar JumpDrive SAFE unique?

**A:** Lexar JumpDrive SAFE combines 3 key elements to provide a secure flash drive.

- A)** Hardware-based AES 256-bit Encryption on all stored data
- B)** Tamper-proof smart card to manage all security critical computations
- C)** Rugged metal housing to protect against physical damage

**Q:** What does FIPS stand for?

**A:** Federal Information Processing Standards. Publicly announced standards developed by the United States Federal government

**Q:** Why does the Gemalto brand name appear on the application graphical user interface (GUI)?

**A:** Lexar JumpDrive SAFE is jointly developed by Lexar and Gemalto, combining Lexar's secure solid state storage technology and Gemalto's .NET smart card technology.

**Q:** What is the difference between the Lexar JumpDrive SAFE S3000 and Lexar JumpDrive SAFE S3000 FIPS?

**A:**

Lexar JumpDrive SAFE S3000 FIPS	Lexar JumpDrive SAFE S3000
Up to 30MB/sec Read* • Up to 22MB/sec Write*	Up to 30MB/sec Read* • Up to 8MB/sec Write*
2, 4, 8GB	2, 4, 8, 16GB
Tamper-resistant rugged, waterproof metal housing	Rugged metal housing
FIPS 140-2 Level 3 validated	Based on same security level implementation
Certified for Windows Vista®	Works with Windows Vista
Desktop-based device management	Web-based device management option

**Q:** Does the encryption reduce the drive performance?

**A:** No, the hardware-based 256-bit AES engine performs on-the-fly encryption and does not impact performance.

## General Use Questions

**Q:** Do I need to install a driver and/or software for Lexar JumpDrive SAFE?

**A:** No, the Lexar JumpDrive SAFE is fully plug and play and does not require any drivers or software to be installed on the host computer.

**Q:** Do I need administrator privileges (on Operating Systems) for Lexar JumpDrive SAFE to work?

**A:** No, the Lexar JumpDrive SAFE does not require administrator privileges to work.

**Q:** What is the web-based device management service?

**A:** The Lexar JumpDrive SAFE (not the FIPS edition) can be managed using the Token Lifecycle Manager, a web-based service that enables user to recover from a lost password, block a lost drive, and securely update the firmware and software on the drive.

**Q:** I have issues on the Token Lifecycle Manager. Where can I get help?

**A:** The TLM service is supported by our partner Gemalto. For all TLM related inquiries, please email us at [TLM@gemalto.com](mailto:TLM@gemalto.com)

## Data Security Questions

**Q:** How does encryption protect my data?

**A:** All drive content is encrypted with the NIST standard AES encryption algorithm and stored in ciphered form on the flash memory. The encryption key used to perform the encryption is stored securely on the embedded tamper-proof smart card, protecting it from unauthorized access. Without the knowledge of the encryption key, it is exceedingly difficult to extract the data from the cipher, even if one is able to disassemble the drive to access the flash memory.

**Q:** Why is hardware-based encryption more secure?

**A:** A software-based encryption runs on top, and utilizes the shared memory space of the computer operating system to store such contents as encryption keys. Other processes on the operating system may be able to access the same memory space, and in so doing, compromise security.

A hardware-based encryption uses the memory space within the device itself, eliminating the risk of access by other processes external to the flash drive.

**Q:** How does the smart card protect my data?

**A:** The smart card provides the following protection:

- **Tamper-proof storage:** Smart cards provide a means of securely storing data on the card. This data can only be accessed through the smart card operating system with authorized access rights. This feature is utilized to store the encryption key, the login password, and the other security parameters.
- **Isolation of security-critical computations:** Operations involving authentication, key generation, and storage are isolated from other parts of the device and host computer that do not have a "need to know." These operations are all performed on the smart card only.
- **Strong Authentication:** The smart card blocks access to JumpDrive SAFE after a predefined set of login attempts have exceeded. The smart card deploys a stringent PKI-based challenge-response process for authentication. This prohibits any unauthorized access to the flash encryption keys and protects the authorized user. The smart card protects against password dictionary attacks through an increasing delay after each incorrect attempt (before the next login can be attempted.)

**Q:** Why is smart card-based authentication more secure than other methods of authentication?

**A:** The secure microcontrollers used in Gemalto smart cards have security features manufactured into the ICs that thwart attackers from accessing any sensitive information that is stored in the card. Gemalto smart card technology is extremely difficult to duplicate or forge and has built-in tamper protection. Smart card chips include a variety of hardware and software capabilities that detect and react to tampering attempts and help counter possible attacks. This reflects in Common Criteria level EAL 5+ certification achieved by the Gemalto smart card micro-controller. In addition, smart card technology provides secure hardware-based key generation and storage and standard PKI-based challenge-response process to unblock access.

Gemalto smart card technology provides security benefits at a number of levels that other hardware-based authentication mechanisms cannot match.

**Q:** How does the Lexar JumpDrive SAFE S3000 behave if it comes under a password dictionary attack?

**A:** The Lexar JumpDrive SAFE S3000 permits up to 5 login attempts. The Lexar JumpDrive SAFE S3000 also introduces an increasing delay after each incorrect attempt before the next login can be attempted. Once the attempts are exceeded, the device rejects further login attempts until the user provides the correct answer to the security question.

**Q:** Are copies of the password and cryptographic key saved on the host computer?

**A:** No. Both the password and cryptographic key are stored securely only on the smart card.

**Q:** What happens if I forget my password?

**A:** The Lexar JumpDrive SAFE S3000 allows password reset once the correct answer is provided to the security question. A new password must be set but no data is erased.

If however a user forgets the answer to the security question and exceeds 5 login attempts, the Lexar JumpDrive SAFE S3000 becomes permanently disabled and cannot be recovered.

**Q:** Does the Lexar JumpDrive SAFE S3000 perform any operations that leave traces on the host computer?

**A:** No. All operations are contained within the drive, leaving no trace on the host machine.

**Q:** How are the encryption keys generated?

**A:** The encryption keys are generated by the smart card's Random Number Generator (RNG) and are stored securely in the smart card's non-volatile memory. The keys are not stored in the flash memory or the host computer, or transmitted across the USB port.

**Q:** How is the Lexar JumpDrive SAFE S3000 password protected?

**A:** The login password is hashed before being transmitted to Lexar JumpDrive SAFE S3000, and then stored in the tamper-proof smart card. The password validation uses challenge-response process combining with zero-knowledge transfer mechanism. The authentication is performed on the smart card only; there is no way to retrieve the stored password from the smart card. Access is granted only when password has been validated by the smart card. If login attempts are exceeded, the device rejects further login attempts.

**Q:** Does the Lexar JumpDrive SAFE S3000 support complex passwords?

**A:** The JumpDrive SAFE S3000 supports complex passwords, but does not enforce it. The main reason for a complex password is to deter software-based password dictionary attacks. The SAFE S3000 defeats such attacks with the smart card. The smart card permits only a limited number of login attempts and introduces an increasing delay after each incorrect attempt before the next login can be attempted.

\*Speeds based on internal testing. Actual performance may vary.

Actual usable memory capacity may vary. 1GB equals 1 billion bytes.

Security safeguards, by their nature, may possibly be circumvented. Lexar does not guarantee the product will be 100% resistant to all possible attacks.

©2009 Lexar Media, Inc. All rights reserved. Information is subject to change without notice. Lexar, the Lexar logo, and JumpDrive are trademarks of Lexar Media, Inc. Windows Vista is a trademark of the Microsoft group of companies. All other trademarks or registered trademarks are the property of their respective owners. Lexar Media, Inc. is a subsidiary of Micron Technology, Inc.