



SINA Mobile Disk

SOLUTION



Mobility has become a key issue in today's work environments. The workplace is no longer a fixed location; instead, mobile access to information from the office, on the road or from home is essential. Make your information mobile securely with the SINA Mobile Disk.

The SINA Mobile Disk is a very compact, light-weight USB hard disk that is cryptographically secured. All data on the SINA Mobile Disk is completely encrypted.

The cryptographic functions on the SINA Mobile Disk are performed by the integrated cryptographic processor. This way, there is no performance decrease in read and write operations. In addition, it is not necessary to install software and drivers on the PC. In this manner, the SINA Mobile Disk provides user-friendliness at its best.

Equipped with its own display and an integrated touchpad, the SINA Mobile Disk provides user authentication without requiring the PC system – it is sufficient to entrust your PIN to the SINA Mobile Disk to get access to the confidential information. Viruses and Trojans cannot spy out the key to your data anymore. By the way, the SINA Mobile Disk can also be used as a memory for PKCS#11 certificates which can be easily integrated into your browser.¹

¹ The corresponding driver software needs to be installed.

Your advantages:

- Stronger encryption (256 bit instead of 128 bit)
- PIN is entered directly at the device
- Integrity protection of all data
- Easy and secure use and administration
- High performance

The crypto processor uses technologies that so far have been reserved for highly secure government applications, e.g. SINA. The SINA Mobile Disk now brings this technology to users with high-security demands in the private sector, too.

The SINA Mobile Disk can be used individually without central administration. As a result of the predefined role of the security officer and his/her configuration possibilities, it can also be applied in organisations with roles and security policies.

Benefits

- No risk in case of theft or loss of the SINA Mobile Disk since all information is encrypted and signed
- Maximum security due to PIN entry directly at the SINA Mobile Disk
- 256 bit AES key length (European product)
- Data integrity by means of signature of all data
- Full protection against viruses and spyware as a result of the assignment of access, read and write authorisations for various partitions
- Future-proof by a programmable cryptographic processor and a secure firmware update process
- Transparent and autonomous encryption increases user-friendliness and improves user acceptance
- Attractive design

Characteristics	
	60 GB 100% encrypted hard disk with AES 256 100% signed hard disk with HMAC-SHA1 USB 1.1 or 2.0 Weight: 122 g
	Dimensions in mm (l*w*h) = 114.1*73*22 Integrated USB cable Integrated LCD Touchscreen keyboard
Supported algorithms	
	AES 256 mode CBC or ECB (generation and encryption)
	RSA 2048 (generation, encryption, signature)
	3DES (generation and encryption), MD5 (HMAC) SHA-1 (HMAC), Random number generator according to FIPS 186-2

Administration of the SINA Mobile Disk in Organisations: Simple and Secure

The SINA Mobile Disk is configured by a security officer. This officer defines the security profile of the SINA Mobile Disk before it is shipped to the user. The security profile defines the way in which the user can work with the SINA Mobile Disk.

Examples:

- Cryptographic algorithms available to the user
- Minimum length of the cryptographic keys
- Minimum length of the user password
- Definition of a temporary password to be sent to the user
- Definition of areas on the SINA Mobile Disk which may only be used to store data signed by the security officer (such as a signed operating system)

The security officer can personalise the system manually or automatically. An MDS workstation (MDS - **M**ass **D**eployment **S**tation) is used for automatic personalisation. This MDS contains a list of persons who use a SINA Mobile Disk. The security profiles of these users are also managed by the MDS.

Administration	
	2 profiles (user and security officer)
	Definition of the user profile through the security officer
	Optional MDS workstation
	Secure update of the FPGA via USB interface
APIs	
	PKCS#11 MS-CAPI
Certification	
	Common Criteria EAL3+ (under evaluation)
Miscellaneous	
	Secured via Crypto Ignition Key (CIK)

secunet Security Networks AG

IT security and its trend-setting usage is the core competence of secunet Security Networks AG. The development and implementation of IT security solutions for sensitive data turn secunet into a specialist in great demand. Excellent technological understanding is reflected in our consulting services and modulated products. Progressive digitalization of processes and communication channels of all kind pose new challenges for secunet day-to-day. Due to our large know-how we set standards in the IT security market. Our extensive clientele comprises national and international companies and affiliated groups as well as the public sector. About 230 highly qualified and experienced employees at seven branch offices in Germany as well as at further offices in subsidiaries in Switzerland and the Czech Republic are engaged in the creation of innovations, the optimal settlement of projects and our twenty-four-seven support.

Editor:



secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen, Germany
Phone: +49 - 201 - 54 54 - 0
Fax: +49 - 201 - 54 54 - 123
E-mail: info@secunet.com
www.secunet.com