

Encryptors for Network Layer 2



Benefits:

- » No need for changes to the network infrastructure
- » Virtually maintenance-free operation
- » Full duplex encryption at line speed
- » IPsec-equivalent security level (with Galois Counter Mode)
- » Configuration according to customer requirements (SFP modules)
- » Approved up to **RESTRICTED**

The SINA L2 Box S product line provides high-performance encryptors for the secure exchange of information in networks (Ethernet). The flexible and modular architecture of the SINA L2 Boxes S supports applications in MAN, WAN and SAN areas at transfer rates of up to 10 Gbit/s. The SINA L2 Box S encryptors protect both point-to-point and multipoint connections.

Together with the IPsec gateways of the SINA L3 Box S product line, the SINA L2 Box S encryptors allow communications to be secured as needed at OSI network layers 2 and 3. Building upon the features of the successful predecessor models used in complex security networks, the new advanced models now also allow multipoint configurations.

Working at low latency, the SINA L2 Boxes S are destined for application scenarios with demanding quality of service or real-time requirements. The SINA L2 Box S product line also features the SINA L2 Box S 10G, the highest performing encryption device in the SINA range for VS-NfD (RESTRICTED) communication.

IT security concept

The devices of the SINA L2 Box S product line are based on a holistic IT security concept. It comprises the following:

- A secure system platform,
- Smartcard technology,
- FPGA-based cryptography (using hardware random number generators) and
- Hardware and firmware dimensioned and configured in compliance with regulations.

IPsec-equivalent security level

The cryptographic mode GCM (Galois Counter Mode) now allows an IPsec-equivalent security level of integrity and replay protection at network layer 2. As an addition to the classical point-to-point encryption still supported using CBC mode (Cipher Block Chaining), GCM additionally supports point-to-multipoint and multipoint-to-multipoint encryption.

Initial System boot and operation

The SINA L2 Box S encryptors load their initial configuration and the keying material required for operation (for device authentication) from a PIN-protected SINA smartcard. This data is read from the smartcard and then stored in the internal memory of the manipulation-protected device. During subsequent operation, this smartcard is no longer required and can be used as a configuration backup for replacement devices. The external smartcard reader only needs to be connected to the device during the boot phase, which means it can be disconnected after this phase so as to be available for other SINA L2 Box S encryptors. Once the configuration has been loaded from the SINA smartcard, the SINA L2 Boxes S are immediately ready for operation. Subsequent operation is then virtually maintenance-free. The only time a new key has to be loaded into the device is when the validity period of the authentication key expires.

The SINA L2 Box S encryptors work with complete transparency, i.e. without defining any specific protocol. VLANs are also individually encrypted. Keys are changed without interrupting the secure connection.

Systems monitoring

The SINA L2 Boxes S support both SNMPv2c and SNMPv3-based systems monitoring. Monitoring reports are sent as syslogs to network management systems or to the responsible SINA Management.




High availability

In point-to-point configurations, high availability of the connection is guaranteed by multiple implementation of the line, including the corresponding SINA L2 Boxes S. This can be achieved analogously for multipoint configurations as well. The key servers required for multipoint configurations can be employed redundantly in the network. All SINA L2 Boxes S feature redundant power supplies, where the power supplies for models 1G and 10G are hot swappable.


Management

The SINA L2 Boxes are easily configurable from a single SINA Management instance. That means, if SINA equipment is already employed in a network environment, then the existing SINA Management can be used to manage the SINA L2 Boxes as well. Point-to-point configurations can be managed without a SINA Management.

Approval-related construction classes

   SINA L2 Box S	
Approval	RESTRICTED, NATO RESTRICTED; RESTREINT UE**
Software and firmware	Version 3.2
Manipulation protection	Integrated
Configuration token	SINA smartcard
Key management	SINA Management (from Version 3.11)

Additional details and performance data

		 SINA L2 Box S 100M	 SINA L2 Box S 1G	 SINA L2 Box S 10G
General technical data				
Design	19"	1 HE	1 HE	2 HE
Weight		4 kg	7 kg	10 kg
Stromversorgung	Redundant	■	■ Hot Swappable	■ Hot Swappable
	110 – 240 V AC 50 – 60 Hz	11 W	90 W	115 W
Heat dissipation		26 BTU/hr	300 BTU/hr	400 BTU/hr
Cryptography				
Throughput	P2P: Frame mode (CBC), full duplex	100 Mbit/s	1 Gbit/s	10 Gbit/s
	MP: GCM mode, full duplex***	up to 99 Mbit/s	up to 995 Mbit/s	up to 9,955 Mbit/s
Latency	Per device	≤ 0.04 ms	≤ 0.008 ms	≤ 0,004 ms
Symmetric encryption method	AES (256 bit, CBC or GCM)	■	■	■
Asymmetric encryption method	ECC (DH-ECKAS)	■	■	■
LAN connections				
Network interfaces		2 x 10/100Base-T TP RJ45	2 SFP slots incl. 1000BASE-SX MM 850 nm (alternative SFPs optionally available)	2 XFP slots incl. 10GBASE-LR SM 1310 nm (alternative XFPs optionally available)
Management interface	10/100Base-T TP RJ45	■	■	■
	Serial DB9	■	■	■
Temperature				
Operation	+1 °C to +40 °C	■	■	■
Transport	-20 °C to +60 °C	■	■	■
Item number		SB15.01	SB15.02	SB15.03

* For further information about the new naming concept refer to: www.secunet.com/en/sina.

** For German national use only.

*** Assuming a maximum packet size (9,000 bytes).

More information:
www.secunet.com/en/sina

secunet

secunet Security Networks AG
 Kronprinzenstraße 30
 45128 Essen, Germany

Phone: +49-201-5454-0
 Fax: +49-201-5454-1000
 E-mail: info@secunet.com
www.secunet.com