SINA® L3 Box H 200M

VPN-Gateway with the Highest Level of National and High International Approvals

Benefits:

- Approved for German national STRENG GEHEIM*, NATO SECRET and SECRET UE/EU SECRET
- PEPP-compatible
- High-performance
- High availability
- Interchangeable network interfaces
- Comfortable Management

As a VPN gateway, the SINA L3 Box H 200M is a key component of the central IT infrastructure in high-security networks. The data exchange between the SINA components is securely transmitted via encrypted VPN tunnels. SINA L3 Boxes connect public authority or corporate networks via the Internet. In addition, access to (terminal) servers by SINA clients is provided via pre-switched SINA L3 Boxes, which serve as cryptographic network access points.

The SINA CORE-based SINA L3 Box H 200M and its predecessor, the PEPP-based SINA Box H, are the only IP-based encryption systems approved by the German Federal Office for Information Security (BSI) for transmitting classified information up to and including German national GEHEIM and STRENG GEHEIM*. Furthermore, the devices are approved for NATO SECRET and SECRET UE/EU SECRET. The focus is on national and international military and governmental high-security networks.

The SINA L3 Box H 200M is substantially more powerful, lighter and more robust compared to the previous model SINA Box H, especially in terms of SINA CORE. With 19" 2 high units, the SINA L3 Box H 200M has a much more compact design. The SINA L3 Box H 200M is flexible in many respects, as can be seen in the reloadable crypto device classes, enhanced temperature ranges, the network interfaces that can be reconfigured directly on the device and more modest power consumption. Furthermore, online updates for operative parameters (data container D2) are supported for SINA CORE modules. In addition, there is the option of service-friendly batteries replacement.

IT security concept

The SINA L3 Box H 200M is based on a holistic IT security concept. It comprises in particular:

- A ruggedized, intensively tested SINA OS system platform
- Smartcard technology
- IPsec-based cryptography
- SINA CORE crypto module and
- Hardware, firmware and software that are dimensioned and configured in accordance with approval standards.

Secure system start and operation

The SINA L3 Box software is coreboot-protected and reliably loaded by the flash memory during system start. All initial configuration data and security associations for the SINA L3 Box are stored in a protected area of the SINA Smartcard. When a SINA L3 Box is started, the security associations to the SINA Management and the primary communications-related SINA L3 Boxes are set up as IPsec VPN tunnels. If necessary, additional security associations or configuration data from the SINA Management are loaded. This greatly simplifies configuration, installation and hardware replacement with the SINA L3 Box.

Systems monitoring

The SINA L3 Boxes log all data related to monitoring during operation. This can be imported into network management systems where it can be processed and/or displayed as required.

High availability

It is possible to increase the availability and reliability of SINA L3 Boxes by means of redundant configurations. An automatic switchover for example triggers a second SINA L3 Box to take on the functions of the failed SINA L3 Box (hot standby) that was previously active.

SINA L3 Boxes also support geo-redundant and load-balancing configurations. In geo-redundant scenarios, alternative communication channels – which can be prioritised as necessary – run via SINA L3 Boxes in different locations. For load-balancing configurations, the SINA L3 Boxes interact with commercially available load balancers.

Satellite communication

Use of SINA L3 Boxes requires IP-enabled transport networks, including satellite communication lines. The available bandwidth of the satellite lines is used effectively in tandem with satellite optimisers.

Management

The SINA L3 Box is configured and controlled centrally by SINA Management. An integrated public key infrastructure (PKI) with associated user management supports essential administrative processes involving SINA Smartcards. This includes, in particular, their personalization, the generation or updating of keys and cryptographic parameters as well as the administration of the associated PINs and PUKs.

Approval-related construction classes

	SINA L3 Box H 200M Z1 	SINA L3 Box H 200M 27A 
Approval	German national GEHEIM, SECRET UE/EU SECRET	German national GEHEIM, STRENG GEHEIM*, SECRET UE/EU SECRET
Boot integrity protection	coreboot	coreboot
Software versions	2.2	2.2
SINA CORE device classes	National v1.0 (PEPP-compatible) EU v1.0 (PEPP-compatible)	National v1.0 (PEPP-compatible) NATO 1.x (PEPP-compatible) EU v1.0 (PEPP-compatible)
Manipulation protection	SINA CORE	SINA CORE
Emission protection	Zone 1	SDIP 27 Level A
Authentication token	SINA Smartcard	SINA Smartcard

Additional details and performance data

General data	
Design	19" 2 U
Weight	12 kg
Power consumption	80 W
Cryptography	
Module	SINA CORE 100
Encryption performance	180 Mbit/s bidirectional
Symmetrical encryption process	Libelle
Asymmetrical encryption processes	EC-GDSA, EC-DH
LAN connections	
Network interfaces	3 x 100/1000 Mbit LWL optical fibre (interchangeable) 1 x 100/1000 Mbit LWL in SINA CORE (interchangeable)
Plug type	LC
Miscellaneous	
Service hatch	For battery replacement
Temperature ranges	
Operation	+15 °C to +45 °C
Transport and storage	-25 °C to +60 °C

* In usage situations where data classified as German national STRENG GEHEIM is being processed, the usage scenario and IT security concept for the SINA L3 Box H 200M must be specifically agreed with the German Federal Office for Information Security (BSI).

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

secunet

secunet Security Networks AG
Essen, Germany

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