

VPN Gateway for SECRET Data



Benefits:

- » Approved up to and including NATO SECRET (SINA Box H) and SECRET UE (SINA Box P)
- » High availability
- » SINA Management in online operation
- » State-of-the-art technology in complex high-security networks

As a VPN gateway, the SINA Box is a key component of the central IT infrastructure in high-security networks. **The data exchanged between the SINA components is securely transmitted via VPN tunnels.** SINA Boxes connect networks of public authorities or companies via public lines, e.g. the Internet. In addition, access to (terminal) servers by SINA clients is provided via SINA Boxes, which serve as crypto network access points.

The SINA Box H is an IP-based crypto system which has been granted approval for the transmission of classified information up to the levels SECRET UE and NATO SECRET. (National German approval: up to and including STRENG GEHEIM).

The SINA Box H/P has been a recognised standard solution for many years and is used, for example, in the national and international high-security networks of public authorities as well as in Military Command and Control Information Systems and communication systems.

The use of SINA Boxes requires IP-enabled transport networks; this also includes satellite communication lines. The available bandwidth of the satellite lines is effectively used via Sat optimisers.

IT security concept

The SINA Box H/P is based on a holistic IT security concept. In particular, this concept includes

- A hardened and intensively evaluated Linux system platform
- Smart card technology
- IPsec-based cryptography
- Hardware, firmware and software with configuration according to the approval requirements

Cryptographic keys, configuration data and security associations are protected by means of a smart card and the PCI crypto board PEPP.

Secure system boot and operation




Depending on the actual conditions of the IT infrastructure and the project-specific communication requirements, it is possible to use SINA Boxes H/P with several hundred to thousands of security associations. The SINA Box software is reliably loaded from the CD-ROM or Flash memory when the system boots. All initial configuration data and security associations of the SINA Box are stored in a protected area of the SINA smart card. When a SINA Box is started, the security associations to the SINA Management and the communication-relevant SINA Boxes are set up as IPsec VPN tunnels. If necessary, additional security associations or configuration data are loaded from the SINA Management. This makes the SINA Box very comfortable in terms of configuration, installation, and hardware replacements.

The SINA Boxes log data relevant for monitoring during operation. This data can be imported into network management systems where they can be processed and/or visualised as required.

High availability

It is possible to increase the availability and reliability of SINA Boxes by means of redundant configurations. An automatic switchover triggers a second SINA Box to take on the functions of the failed SINA Box.

Models

	SINA Box H Zone 1	SINA Box H/P SDIP 27 A	SINA Box H IP 54
			
Size and/or dimensions	19" 3 HU	19" 3 HU	H x W x D: 120 mm x 345 mm x 446 mm, 19" installation kit
Crypto-module	PCI crypto board PEPP	PCI crypto board PEPP	PCI crypto board PEPP
Symmetric cryptographic methods	Libelle (hardware-implemented)	Libelle (hardware-implemented)	Libelle (hardware-implemented)
Asymmetric cryptographic methods	EC-GDSA, EC-DH	EC-GDSA, EC-DH	EC-GDSA, EC-DH
Crypto data throughput	60 MBit/s	60 MBit/s	60 MBit/s
Network interfaces	4 x 100 MBit Optical fiber or 4 x GBit Optical fiber or 2 x 100 MBit and 1 GBit Optical fiber each	4 x 100 MBit Optical fiber or 4 x GBit Optical fiber or 2 x 100 MBit and 1 GBit Optical fiber each	2 x 100 MBit Optical fiber or 2 x GBit Optical fiber or 1 x 100 MBit and 1 GBit Optical fiber each
Anti-tamper	Integrated	Integrated	Integrated
Protection class	—	—	IP 54

About SINA

secunet developed SINA – the Secure Inter-Network Architecture – for the German Federal Office for Information Security (BSI). The product family of crypto systems enables the secure processing, storage and transmission of classified information as well as other sensitive data – according to approval requirements.

Management

SINA Management is used for central configuration of all SINA Boxes in the network. An integrated public key infrastructure (PKI) along with the corresponding user management supports the main administrative processes with regard to SINA smart cards, in particular their personalisation, the generation or update of keys and cryptographic parameters as well as the administration of the corresponding PINs and PUKs.

Sources of Supply

You can purchase SINA directly through secunet or through authorised SINA distributors.

Approvals

			
	(TOP) SECRET	NATO SECRET	SECRET UE
Software versions	1.4, 2.1	1.4, 2.1	1.4
Crypto parametrisation	H	H	P
TEMPEST	Zone 1 (SDIP 27 Level B)	SDIP 27 Level A	SDIP 27 Level A

The product portfolio covers different gateways, line encryptors, clients and management systems which have been in use in the public sector, armed forces and companies handling classified information for many years. Selected SINA components are approved for processing and transmitting classified information up to and including the classification levels NATO SECRET and SECRET UE.

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

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