

The VPN Gateway for Confidential Data



Benefits:

- » **Approved depending on features and configuration up to classification level CONFIDENTIAL, NATO CONFIDENTIAL as well as CONFIDENTIEL UE**
- » **Highly scalable hardware platforms (10 MBit/s – 1 GBit/s)**
- » **High availability**
- » **Central management**

The SINA Box S is the only IPsec-based VPN gateway with software-based cryptography which is approved by the Federal German Office for Information Security (BSI) for the classification level CONFIDENTIAL. Cryptographic keys, configuration data and security associations are protected by means of a smart card.

SINA Boxes allow for the cryptographically secured connection of sensitive local networks of companies and public authorities via potentially insecure networks (e.g. the Internet). In addition, the SINA Box offers a secure access point to the local network for SINA Thin Clients or SINA Virtual Workstations.

The SINA Box S is the only IP-based cryptosystem with software-based cryptography which has been granted approval for the transmission of classified documents up to the level CONFIDENTIAL by the German Federal Office for Information Security.




Many public authorities and companies have been using SINA Boxes with great success for years now. We provide you with comprehensive

consulting and support in the implementation of your security projects. We know cryptography inside out – and we also know the structures in place at public authorities and big companies. SINA is put to use in large-scale, international networks. Trust in our many years of experience with high-quality crypto components in complex network infrastructures.

Technology

Communication between SINA systems is based on the security principle of a virtual private network (VPN). SINA was designed and developed to be a high-security solution. Consequently, these VPN features are secured by means of specific configuration settings and special security functions. In addition to standardised cryptographic methods of the current IPsec standard, special cryptographic methods stipulated by the BSI are used.

Approvals¹

Component			
SINA Box S	Up to CONFIDENTIAL	Up to NATO CONFIDENTIAL	Up to CONFIDENTIEL UE

For manipulation protection, the software is contained on a CD-ROM or Flash memory and can be checked for integrity in conjunction with a smart card. All initial configuration data and security associations of the SINA Box are stored in a protected area of the SINA smart card. When the SINA Box is started, the configured security associations are set up automatically or on demand as an IPsec VPN tunnel and, if necessary, additional security associations or configuration data are loaded from the SINA Management server (LDAP directory service). This makes using the SINA Box very simple in terms of configuration, installation and replacements in case of defective hardware – no manual device configuration is required; all the data is contained on the smart card and/or available via the directory service.

SINA Management is used for central configuration of all SINA Boxes in the network. It carries out the simple and intuitive configuration of security associations even in complex networks. An integrated public key infrastructure (PKI) along with the corresponding user management takes

care of all administrative transactions with regard to SINA smart cards (the generation or update of keys, certificates and cryptographic parameters, personalisation, PIN letters, etc.). In addition, logging mechanisms help monitor the SINA Boxes.





High availability

The availability and reliability of the SINA Box can be boosted in an active/passive configuration (Hot-Standby). When two SINA Boxes are run in this mode, the passive second box is automatically activated as a result of the switchover in the event of a failure. The switchover is completed in an extremely short time because dynamically generated keys are permanently synchronised between the SINA Boxes (software version 2.0 and higher).

Sources of supply

You can purchase SINA directly through secunet or through authorised SINA distributors. A SINA Business version is available for customers from the private sector.

Hardware specifications

	 Box LE	 Box 1HU	 Box 1000	 Box 3HU
Form factor	Desktop device	1HU rack-mountable	2HU rack-mountable	3HU rack-mountable
Processor	VIA Eden 533	Intel® Pentium M CPU, 1.8 GHz	Intel® Core 2 Quad Q6600, 2.4 GHz	Intel® Pentium 4, 2.4 GHz
Memory	256 MB RAM	1 GB RAM	2 GB RAM	256 MB RAM
Ethernet-Ports	3 x 10/100 MBit	5 x 10/100 MBit	5 x 10/100/1000 MBit	Up to 5 x 10/100/1000 MBit/TP or 100 or 1000 MBit LWL
LCD	–	16 x 2 characters + PIN pad	16 x 2 characters + PIN pad	6 x 2 characters + PIN pad
Dimensions W/H/D in mm	228.3/52.9/170.2	482.6/44/480	482.6/87.9/480	482.6/132/450
Weight	Approx. 1.8 kg	Approx. 12.5 kg	Approx. 18.5 kg	Approx. 16 kg
Power supply	110/240 V, 60 W, external power supply without fan	110/240 V, 150 W, openframe ATX power supply without fan	2 x 100/240 V, 300 W, redundant power supply	115/230 V ATX power supply
Crypto performance	10 MBit/s	90 MBit/s	900 MBit/s	90 MBit/s
Anti-Tamper	–	–	–	Yes
Tempest classification	–	–	–	Zone 1
Approval	RESTRICTED NATO RESTRICTED RESTREINT UE	RESTRICTED NATO RESTRICTED RESTREINT UE	RESTRICTED NATO RESTRICTED RESTREINT UE	CONFIDENTIAL NATO CONFIDENTIAL CONFIDENTIEL UE

Technical data

Basis system	SINA Linux Linux kernel with extensive security extensions
Cryptography:	Symmetric HMAC/Hash Diffie-Hellman Signature processes
Certificates	X509v3 (RFC 2459), (IPsec/PKIX profile: partial RFC 4945) Online certificate update (CMP) Time-controlled (prior to expiration)/manual at the system/management-initiated Attribute certificates (X.501/RFC 3281; clearance/category)
VPN	IPsec (RFC 2401) SPD/SADB policies Bypass Site SA (an IPsec key for several SAs to one gateway) Subnet/subnet, host/subnet, host+port/subnet, host/host Subnet+port/subnet+port, subnet+port/host ESP transport mode/tunnel mode (RFC 2406) IKEv1 (RFC 2407/2408/2409) NAT traversal
Network	IPv4, Static IP address configuration, Dynamic IP address configuration on black interface, PPP, PPPoE, DHCP

¹⁾ Dependent on implemented emission protection and integrated anti-tamper functionality

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



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