



SINA Box H and SINA Box P are VPN gateways for the secure connection of IP-based networks based on the IPsec standard. They are approved by the German Federal Office for Information Security BSI (Bundesamt für Sicherheit in der Informationstechnik) for the highest security requirements. Cryptographic keys, configuration data and security associations are protected by means of a smart card and a special cryptographic hardware with BSI's crypto chip PLUTO.

#### About SINA Box H / P

SINA Boxes allow for the cryptographically secure connection of sensitive/classified local networks of companies and public authorities as well as the access of corresponding SINA clients by mobile users. There are excellent reasons for using SINA Box:

- With SINA Boxes, it is possible to connect local networks of different sites via potentially insecure networks (e.g. the Internet) in a highly secure and cost-effective way.
- The SINA Box H is the only IP-based cryptosystem which has been granted approvals for the transfer of classified information up to the level TOP SECRET by the German Federal Office for Information Security BSI. Classified data and data networks can therefore be secured for all national classification levels according to directives concerning the handling of classified information.

#### 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, specific cryptographic methods stipulated by the BSI are implemented in hardware.

#### Your advantages:

- Approved up to TOP SECRET, NATO SECRET (SINA Box H) as well as SECRET UE (SINA Box P)
- Optional extensions for high availability
- Cost-effective way to connect sites, of all classification levels

The software is contained on a manipulation-protected CD-ROM or Flash memory and is integrity-checked in conjunction with a smart card on system start up. All initial configuration settings and security associations of the SINA Box are stored in a specially protected area of the SINA smart card. When the SINA Box is started, the security associations between all SINA Boxes of the respective network are set up as an IPsec VPN tunnel and, if necessary, additional security associations or configuration data are loaded from the SINA Management server. This makes using the SINA Box very simple in terms of configuration, installation and replacements in case of hardware defects as well as flexible with regard to security management.

SINA Management is used for central configuration of all SINA Boxes in the network. The SINA Management ensures 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 tasks with regard to SINA smart cards (generation or the update of keys and cryptographic parameters, personalisation, PIN letters, etc.). In addition, SINA Boxes are monitored with the help of logging mechanisms.

**Availability**

The availability and reliability of the SINA Box can be boosted by means of a scalable backup and hot failover extension. When a SINA Box is run using a hot failover configuration, in the event of a failure, there is an automatic switchover to the second SINA Box, which takes on the functions of the defective SINA Box. The switchover is completed – as of Version 2.0 – in an extremely short time frame because it is possible to continue to use dynamically generated keys.

**Approvals**

SINA Box H is approved for the transfer of data up to the classification level TOP SECRET and NATO SECRET, SINA Box P is approved for SECRET UE.

**Sources of supply**

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

Cryptographic methods	
Symmetric	Special BSI algorithm on PLUTO crypto chip, HMAC-SHA1, HMAC-RIPEMD160
Asymmetric	EC-GDSA, Diffie-Hellman (ECP)
Standards	
	RFC 2104 (HMAC), 2401-2412 (IPsec), 2459 (X509v3), 2510/2511 (CMP), 3281 (Attribute Certificates) ISO/IEC 15946-2 (EC-GDSA)
	IP v4
On request:	IP v6,v4/v6 and v6/v4 tunnelling
QoS	
	QoS DiffServ Codepoints (DSCP) Bandwidth management per security association

**Versions:**



1HU<sup>1</sup>



3HU

Crypto performance (throughput MBit/s)	80	80
Network interfaces	2x 100 MBit/s Fx	4x 100 MBit/s Fx (1000 MBit/s Fx on request)
Max. zoning	SDIP-27 B	SDIP-27 A
Anti-tamper	integrated	integrated

<sup>1</sup>Can only be used up to SECRET. NATO SECRET or SECRET UE requires SDIP-27 A hardware.

**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](http://www.secunet.com)