SINA® Virtual Workstation

Sensitive Data Secure on the Road

Benefits:

- **Secure processing, transfer and storage of classified data**
- **Highly secure SINA platform with virtualisation technology**
- **Parallel or semi-parallel operation of MS Windows® or Linux sessions (“multi-level data separation”) with different classification levels**

SINA Virtual Workstation is a fat client with a cryptographic file system and IPSec-protected communication. Protected by a VPN tunnel, the SINA Virtual Workstation communicates with server areas or terminal server areas. This makes flexible use possible: stationary or mobile, online or offline. SINA networks can be accessed via wired (Ethernet) or wireless media.

SINA Virtual Workstation is extremely flexible and can therefore be used in many different scenarios. In addition to the integrated Thin Client functions, it is possible to operate several virtualised guest operating systems. This makes it your ideal secure workstation for the road.

Other security solutions offer you only partial functions. SINA Virtual Workstation provides you with comprehensive security in a single device – VPN, hard drive encryption and interface control, smart card and secure operating system. It is no longer necessary to combine various individual components to cover all the threats. This makes SINA Virtual Workstation convenient and simple to administrate – as well as being extremely secure. SINA Management allows all security-relevant settings to be made with one single administration software. In addition, SINA Virtual Workstation is the only product of this kind which is approved by The German Federal Office for Information Security (BSI)[1].

Hardware specifications

	SINA Virtual Workstation B	SINA Virtual Workstation S	SINA Virtual Workstation H
Hardware	Lenovo X200, T400, T500, R500 or next generation	GeTAC P 470, Rocky III+	Rocky III+
Anti-tamper	–	–	Yes
Tempest classification	–	Zone 2	Zone 1
Crypto hardware	–	–	SINA CORE
Approval	RESTRICTED NATO RESTRICTED RESTREINT UE[5]	CONFIDENTIAL NATO CONFIDENTIAL RESTREINT UE[5]	In evaluation: SECRET

Desktopversion in preparation.

Approvals[3]

Component			
SINA Virtual Workstation	Up to CONFIDENTIAL[4]	Up to NATO CONFIDENTIAL	Up to RESTREINT UE[5]

Your complete solution includes:

- **BSI-approved solution for EU RESTRICTED and German CONFIDENTIAL[2]**
  - » Online and offline processing of classified documents
- **Strong 2-factor authentication**
  - » Authentication secured by means of a smart card with PIN
  - » Secure storage of cryptographic keys for VPN and hard drive encryption
- **Hard drive encryption**
  - » Secure storage of classified documents
  - » System disposal or repair without security risks
- **Network encryption (VPN)**
  - » Secure mobile access to public authority's network/ "Classified" level network
  - » Use of public transmission channels such as WLAN, UMTS
- **Firewall functionality**
  - » Complete control at network level
- **Hardware interface control**
  - » Data import/export control (e. g. USB, Bluetooth devices)
- **Operation of several workstations in one system by means of virtualisation**
  - » Simple migration of workstations to new hardware
  - » Simultaneous processing of data at different classification levels as a result of strict separation
  - » Internet usage with simultaneous processing of classified information, e. g. in hotels using WLAN without jeopardizing confidential data
- **Integrated Thin Client technology**
  - » Use of all the advantages of server-based computing, plus the option of a local fat client
- **Central administration of clients**
  - » Holistic administration for many aspects of security from a single source
- **Encrypted VoIP communication**
- **Very high performance combined with the highest levels of security**

The technology

The security philosophy implemented in SINA Virtual Workstation uses the method of encapsulation to separate insecure parts. The virtualisation technology completely seals off security-critical functions in the SINA Linux operating system, away from potentially insecure guest operating systems. All the same, users can work comfortably with the environment they are familiar with. Parallel operation of several guest systems make it possible to work in various security zones, e. g. in the "Classified" level network and in the open Internet (WLAN hotspot).

[1] As of February 2010
[2] Different hardware equipment is required for different classification levels and may involve limited functionality of the software
[3] Depending on sized emission protection and integrated anti-tamper functionality
[4] Individual SECRET approval has been declared in a specific configuration of the hardware for a dedicated scenario
[5] Use in the European Council or a sub-organisation requires a second evaluation with an AQUA instance and approval by the Council (EU directive TECH-P-01-02)

All guest operating systems and data are securely stored in cryptographic file systems (CFS). The proven SINA VPN technology (IPsec) is used for communication with the central network.

The initial configuration settings and security associations of the SINA Virtual Workstation are stored on a smart card in a specially protected area. SINA Virtual Workstation cannot be started without the smart card. In addition, the smart card provides secure storage for cryptographic keys and certificates and independently executes signature functions.

Furthermore, in the SINA Linux operating system it is possible to check and, if required, prevent access to external interfaces of the device (USB, CD-ROM) from insecure guest operating systems. Access rights can be assigned on a user-specific or classification-specific basis.

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.

Technical data

Basis system	SINA Linux Linux kernel with extensive security extensions
Cryptography: Symmetric HMAC/Hash Diffie-Hellman Signature processes	 AES 128/192/256 bit, 3DES, Chiasmus (all multiprocessor support) SHA1, RIPEMD 160 (all multiprocessor support) ECP ECGDSA (ISO/IEC 15946-2)
Crypto hardware	SINA CORE (in preparation)
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, Interfaces: UMTS/GPRS/WLAN/LAN
Cryptographic File system (CFS)	Multi-user (25 per container), roles: administrator, user Integrity protection per block (optional), Random initialisation vector per block (optional), Automatic key change in the background
Management	Online Management Agent, LDAP, NTP, SYSLOG
ThinClient	RDP (4.0, 5.0, 5.1 and 5.2), ICA (6.0, 9.0, 10.6), X11, NX
Virtualisation	Sun VirtualBox CD/DVD (ReWritable), USB 1.1/2.0, virtual hard drive or ISO image, Sound, Guest OS (guest tools required): Windows 2000/XP, 16-bit applications, Windows 7 (32 bit), Linux 2.4/2.6, Quarantine mode

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

secunet

secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen, Germany

Phone: +49 - 201 - 54 54 - 0
Fax: +49 - 201 - 54 54 - 1000
E-mail: info@secunet.com
www.secunet.com