SINA Virtual Workstation

SOLUTION

Now with approval for CONFIDENTIAL!

SINA Virtual Workstation allows users to process and store classified data even without a terminal server connection. With the availability of a wireless online connection via GPRS, UMTS or WLAN, mobile users have secure access to a SINA network. Maximum confidentiality is always ensured.

About SINA Virtual Workstation

SINA Virtual Workstation comes with a trustworthy, highly secure operating system for processing and local storage of classified data for mobile and office users.

The benefits of SINA Virtual Workstation at a glance:

- As opposed to SINA Thin Client, users cannot only process data in online mode, but also in offline mode – at the same level of security.
- Classified VoIP phone calls in the SINA network can be made with SINA Virtual Workstation.
- The virtualisation technology provides several, individually configured virtual PCs that are completely encapsulated and separate from each other. For the user, this means: SINA-secured use of familiar standard operating systems such as Windows or Linux and their applications.
- The integrated cryptographic file system enables session-specific local storage of data.
- Secure authentication is performed by means of smart card technology. If the computer is lost or stolen, the stored data cannot be read by unauthorised parties.
- Access to external interfaces such as USB devices on which confidential data might leak unprotected is controlled by security policies configured on the SINA Management.

Your advantages:

- **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**

The technology

The security philosophy implemented in SINA Virtual Workstation uses encapsulation technologies separating insecure parts from classified information. The separation of potentially insecure guest operating systems by virtualisation technology prevents the execution of all insecure or inadmissible functions. Convenient work is possible all the same.

All data and the guest operating system itself are completely stored in a cryptographic file system (CFS). Each guest operating system has its own CFS and its own security configuration.

All 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. The central SINA Management allows for management of the access permissions within the protected network for each SINA Virtual Workstation user.

SINA Virtual Workstation is also designed to allow access authorisations to external storage media, such as USB, serial/parallel interfaces or CD-ROM, which can be made available to the guest operating system. Whether such access within a concrete environment is to be permitted or to be prevented – depending on the user and the classification of the processed data – is configured by the administrator via the SINA Management using a so-called media ACL and stored on the user's smart card.

SINA networks are securely accessed by means of the integrated SINA VPN technology.

SINA Virtual Workstation can operate several virtual PCs depending on memory capacity and processor performance in completely separate, encapsulated environments containing data of different classification levels.

Approvals

SINA Virtual Workstation is approved for the transfer of data up to classification level CONFIDENTIAL.

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.

Virtual Workstation software

Cryptographic methods	
Symmetric:	AES, 3DES, (HMAC-) SHA1, (HMAC-) RIPEMD 160
Depending on version and hardware:	Government algorithms (Chiasmus)
Asymmetric:	RSA, EC-GDSA, Diffie-Hellman (MODP and 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
NAT	NAT-T support for IPsec (RFC 3947 for some)
QoS	
	QoS DiffServ Codepoints (DSCP) Bandwidth management per security association
Virtual Workstation hardware (depends on version):	
	Notebook or desktop platform, Intel Core-2 Duo processor > 1.6 GHz 2 GByte RAM
Guest operating systems:	
	Windows 2000, Service Pack 3 and higher
	Windows XP, all Service Packs
	various Linux distributions

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

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

SINA_VW_V01_02/08