

Ihre VS-Daten sicher unterwegs



Ihre Vorteile:

- » **Sichere Bearbeitung, Übertragung und Speicherung von VS-Daten**
- » **Hochsichere SINA Plattform mit Virtualisierung**
- » **Paralleler oder semiparalleler Betrieb unterschiedlich klassifizierter Windows[®]- oder Linux-Sessions („Multi-Level Data Separation“)**

Die SINA Virtual Workstation ist ein Fat Client mit einem Kryptodateisystem und IP-Sec-gesicherter Kommunikation. VPN-Tunnel-gesichert kommuniziert die SINA Virtual Workstation mit Serverbereichen oder Terminal-Serverbereichen. **Somit kann sie flexibel stationär und mobil sowie online oder offline eingesetzt werden.** Über drahtlose oder drahtgebundene Medien (Ethernet) kann auf SINA Netzwerke zugegriffen werden.

Die SINA Virtual Workstation ist in höchstem Maße flexibel und dadurch in vielen verschiedenen Szenarien einsetzbar. Neben den integrierten Thin-Client-Funktionen können auch mehrere virtualisierte Gastbetriebssysteme betrieben werden. Damit eignet sie sich ideal als Ihr sicherer Büroarbeitsplatz, Heimarbeitsplatz und auch für unterwegs.




Andere Sicherheitslösungen bieten Ihnen nur Teilfunktionen. Mit der SINA Virtual Workstation erhalten Sie umfassende Sicherheit in einem Gerät – VPN, Festplattenverschlüsselung und Schnittstellenkontrolle, Smartcard

und sicheres Betriebssystem. Ein Kombinieren verschiedener Einzelkomponenten unterschiedlicher Hersteller ist nicht mehr notwendig, um alle Bedrohungen abzuwehren. Das macht die SINA Virtual Workstation bequem und einfach administrierbar – und umfassend sicher. Über das SINA Management lassen sich mit einer einzigen Administrations-Software alle sicherheitsrelevanten Einstellungen vornehmen. Darüber hinaus ist die SINA Virtual Workstation auch das einzige vom Bundesamt für Sicherheit in der Informationstechnik zugelassene Produkt dieser Art¹.

Hardware-Spezifikation

	SINA Virtual Workstation B	SINA Virtual Workstation S	SINA Virtual Workstation H	SINA Virtual Workstation H
Hardware	Lenovo X201, T410, T510, L512 bzw. Nachfolgemodelle	Desktop Zone 1	Desktop SDIP 27A	Rocky III+
Anti-Tamper	–	Ja	Ja	Ja
Tempestierung	–	Zone 1	Zone 0	Zone 1
Kryptohardware	–	–	PCI-Kryptoboard PEPP	SINA CORE
Zulassung	VS-NfD NATO RESTRICTED RESTREINT UE ²	VS-VERTRAULICH NATO CONFIDENTIAL RESTREINT UE ²	GEHEIM	In Evaluierung: GEHEIM

Zulassungen³

Komponente			
SINA Virtual Workstation	bis GEHEIM	bis NATO CONFIDENTIAL	bis RESTREINT UE ⁴

Ihre Komplettlösung beinhaltet:

- **BSI zugelassene Lösung für VS-NfD, VS-VERTRAULICH und GEHEIM⁵**
 - » Online und Offline Verarbeitung von Verschlusssachen
- **Starke 2-Faktor Authentifizierung**
 - » Smartcard gesicherte Authentifizierung mit PIN
 - » sichere Verwahrung kryptographischer Schlüssel für VPN und Festplattenverschlüsselung
- **Festplattenverschlüsselung**
 - » Sichere Ablage von Verschlusssachen
 - » Entsorgung oder Reparatur des Systems ohne Sicherheitsrisiko
- **Netzwerkverschlüsselung (VPN)**
 - » Sicherer mobiler Zugang ins Behördennetz/VS-Netz
 - » Nutzung öffentlicher Übertragungswege wie WLAN, UMTS
- **Firewall-Funktionalität**
 - » Vollständige Kontrolle auf Netzwerkebene
- **Hardware-Schnittstellenkontrolle**
 - » Daten Import-/Exportkontrolle (z. B. USB-, Bluetooth-Geräte)
- **Betrieb mehrerer Arbeitsplätze in einem System durch Virtualisierung**
 - » Einfache Migration von Arbeitsplätzen auf neue Hardware
 - » Gleichzeitige Bearbeitung unterschiedlicher VS Grade durch strikte Separation
 - » Internetnutzung bei gleichzeitiger Bearbeitung von VS-Informationen, z. B. im Hotel zur WLAN-Nutzung ohne Gefahren für vertrauliche Daten
- **Integrierte Thin Client Technologie**
 - » Nutzung aller Vorteile von Server based Computing, zusätzlich die Möglichkeit eines lokalen Fat Clients
- **Zentrale Verwaltung der Clients**
 - » Ganzheitliche Administration für viele Sicherheitsaspekte aus einer Hand
- **Verschlüsselte VoIP-Kommunikation**
- **Sehr hohe Performance bei gleichzeitig höchster Sicherheit**

Die Technik

Die in der SINA Virtual Workstation umgesetzte Sicherheitsphilosophie basiert auf der Methode der Kapselung unsicherer Anteile. Die Virtualisierungstechnik schottet die sicherheitskritischen Funktionen im SINA Linux Betriebssystem von den potenziell unsicheren Gastbetriebssystemen vollständig ab. Trotzdem ist komfortables Arbeiten in gewohnter Umgebung weiterhin möglich. Der parallele Betrieb mehrerer Gastsysteme ermöglicht die Arbeit in unterschiedlichen Sicherheitszonen, bspw. im VS-Netz und im offenen Internet (WLAN-Hotspot).

Alle Gastbetriebssysteme und Daten sind in kryptographischen Dateisystemen (CFS) sicher gespeichert. Die Kommunikation mit dem zentralen Netzwerk erfolgt über bewährte SINA VPN Technologie (IPsec).

Die initialen Konfigurationsdaten und Sicherheitsbeziehungen der SINA Virtual Workstation werden auf einer Smartcard abgelegt. Ohne die Smartcard lässt sich die SINA Virtual Workstation nicht starten. Die Smartcard dient außerdem als sicherer Speicher für kryptographische Schlüssel und Zertifikate und führt selbständig Signaturfunktionen aus.

Weiterhin können im SINA Linux Betriebssystem die Zugriffe auf externe Schnittstellen des Gerätes (USB, CDROM) aus den unsicheren Gastbetriebssystemen kontrolliert und ggf. unterbunden werden. Zugriffsrechte können benutzer- und einstellungsspezifisch vergeben werden.

Bezugsquellen

Für Behörden: Sie können SINA Technologie aus dem Rahmenvertrag BA 4867/01 des Beschaffungsamtes des Bundesministeriums des Innern beziehen. Für nicht-behördliche Kunden: Sie können SINA direkt über secunet oder über autorisierte SINA Wiederverkäufer beziehen.

Technische Daten

Basissystem	SINA Linux Linux Kernel mit umfangreichen Sicherheitserweiterungen
Kryptographie:	symmetrisch AES 128/192/256 Bit, 3DES, Chiasmus (alle Multiprozessor-Support) HMAC/Hash SHA1, RIPEMD 160 (alle Multiprozessor-Support) Diffie-Hellman ECP Signaturverfahren ECGDSA (ISO/IEC 15946-2)
Krytohardware	SINA CORE (in Vorbereitung)
Zertifikate	X509v3 (RFC 2459), (IPsec/PKIX Profil: partiell RFC 4945) Online Zertifikatsupdate (CMP) zeitgesteuert (vor Ablauf)/manuell am System/Management-initiiert Attributzertifikate (X.501/RFC 3281; Clearance/Category)
VPN	IPsec (RFC 2401) SPD/SADB Policies Bypass Standort-SA (Ein IPsec-Schlüssel für mehrere SAs zu einem Gateway) Subnet/Subnet, Host/Subnet, Host+Port/Subnet, Host/Host Subnet+Port/Subnet+Port, Subnet+Port/Host ESP Transportmode/Tunnelmode (RFC 2406) IKEv1 (RFC 2407/2408/2409) NAT-Traversal
Netzwerk	IPv4, Statische IP-Adresskonfiguration, Dynamische IP-Adresskonfiguration auf schwarzem Interface, PPP, PPPoE, DHCP, Schnittstellen: UMTS/GPRS/WLAN/LAN
Kryptographisches Dateisystem (CFS)	Multi-User (bis zu 100 pro Container), Rollen: Administrator, Nutzer Integritätssicherung pro Block (optional), zufälliger Initialisierungsvektor pro Block (optional), automatischer Schlüsselwechsel im Hintergrund
Management	Online-Management-Agent, LDAP, NTP, SYSLOG
ThinClient	RDP (4.0, 5.0, 5.1 und 5.2), ICA (6.0, 9.0, 10.6), X11, NX
Virtualisierung	Oracle VirtualBox CD/DVD (ReWritable), USB 1.1/2.0, eine virtuelle Harddisk oder ISO-Image, Sound, Gast-OS (Gasttools erforderlich): Windows 2000/XP, 16 Bit-Anwendungen, Windows 7 (32 Bit), Linux 2.4/2.6, Quarantäne-Modus

¹⁾ Stand Juni 2011

²⁻⁴⁾ Der Einsatz im Rat der EU oder einer Unterorganisation erfordert eine Zweitevaluierung durch eine AQUA-Instanz und eine Zulassung durch den Rat (EU-Vorschrift TECH-P-01-02)

⁵⁾ Abhängig vom dimensionierten Abstrahlenschutz und integrierter Anti-Tamper-Funktionalität

⁶⁾ Unterschiedliche Geheimhaltungsgrade erfordern unterschiedliche Hardwareausstattungen und sind ggf. mit eingeschränkter Funktionalität der Software verbunden

Weitere Informationen:
www.secunet.com/vw

secunet

secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen

Tel.: +49-201-5454-0
Fax: +49-201-5454-1000
E-Mail: info@secunet.com
www.secunet.com