



Der SINA Thin Client ist ein Smartcard-gesicherter Arbeitsplatz ohne eigene Festplatte. Auf dem Client werden lediglich Bildschirmausgaben gängiger Terminal-Server-Protokolle eines im geschützten Bereich stehenden Servers verarbeitet. Durch die kryptographisch gesicherte Netzwerkverbindung können bis zu STRENG GEHEIM klassifizierte Daten über ein potenziell unsicheres Netzwerk „remote“ bearbeitet werden.

Der SINA Thin Client genügt höchsten Sicherheitsansprüchen und ist – je nach Einstufung der Daten – als Desktop PC und auch als Laptop erhältlich. Der Zugriffsschutz wird durch eine Smartcard bzw. einen USB-Smartcard-Token mit PIN gewährleistet. Die Netzanbindung erfolgt verschlüsselt über ein integriertes IPsec-VPN-Gateway.

Der SINA Thin Client

- ist ein sicherer VS-Arbeitsplatz innerhalb eines Behördennetzes.
- ist ideal als sicherer Heimarbeitsplatz über eine kostengünstige Internet-Anbindung (z. B. über den IVBV oder den IVBB) an das Behördennetz anzubinden.
- ermöglicht die Bearbeitung von klassifizierten Daten in bis zu sechs Sessions.
- führt zur Kostenersparnis durch Nutzung eines SINA Thin Clients anstatt separierter einstufigsspezifisch eingesetzter PCs.
- macht zudem physikalisch getrennte Netzwerke überflüssig – die Kosten für Einrichtung und Unterhaltung entsprechender Infrastrukturen können auf einen Bruchteil der bisherigen Kosten reduziert werden.
- unterstützt mit ICA, RDP, X11 und NX alle gängigen Terminal-Server-Protokolle.

Ihre Vorteile:

- Bearbeitung und Übertragung unterschiedlich eingestufter Daten
- Zugriff von einem Arbeitsplatz auf verschiedene Terminal-Server
- Unterstützung aller gängigen Terminal-Server-Protokolle

Die Technologie

Der SINA Thin Client ist ein Smartcard-gesicherter Arbeitsplatz, auf dem selbst keine sensiblen Daten vorgehalten werden. Vielmehr werden hier mittels Terminal-Server-Protokoll nur Bildschirmausgaben (Sessions) der in einer Sicherheitsdomäne stehenden Server verarbeitet. Dazu werden die Eingaben des Benutzers am SINA Thin Client über das Netzwerk an den Server übermittelt. Der Server wiederum sendet grafische Informationen in Form von Bildschirmausgaben an den Arbeitsplatz zurück. Die geschützten Daten und Dokumente an sich verbleiben somit zu jedem Zeitpunkt in der sicheren Server-Umgebung, und unterschiedlich eingestufte Daten bleiben sicher voneinander getrennt.

Der SINA Thin Client arbeitet online und wird von CD-ROM oder Flash-Speicher gestartet. Die Kommunikation zum Terminal-Server wird durch eine im SINA-Betriebssystem integrierte, mit der in der SINA Box identischen IPsec-VPN-Funktionalität abgesichert.

Alle initialen Konfigurationsdaten und Sicherheitsbeziehungen des SINA Thin Clients werden auf einer Smartcard in einem speziell geschützten Bereich gespeichert. Durch das SINA Management kann für jeden Client-Benutzer individuell gesteuert werden, welche Zugriffe im geschützten Netzwerk möglich sind.

Auf dem SINA Thin Client können in einer Sicherheitsdomäne bis zu sechs Sessions parallel betrieben werden. Die strikte Trennung zwischen den einzelnen Sessions ist durch die zugrunde liegende Plattform stark abgesichert.

Für die Verarbeitung und Übertragung von Informationen höherer Einstufungen (> VS-NfD bzw. NATO RESTRICTED) wird der SINA Thin Client mit abstrahl- und manipulationsgeschützter PC-Hardware eingesetzt. In Abhängigkeit der jeweiligen Geheimhaltungsgrade werden unterschiedlich

starke Verschlüsselungsverfahren, teilweise auf Basis spezifischer Kryptohardware, angeboten.

Zulassungen

Der SINA Thin Client ist abhängig vom dimensionierten Abstrahlschutz und integrierter Anti-Tamper-Funktionalität zugelassen für die Übertragung von Daten bis zu den Einstufungen STRENG GEHEIM und NATO SECRET.

Bezugsquellen

Behörden können SINA über den Rahmenvertrag BA 4867/01 des Beschaffungsamtes des Bundesministeriums des Innern beziehen. Nicht-behördliche Kunden können SINA direkt über secunet oder über autorisierte SINA-Wiederverkäufer beziehen.

Thin Client-Software

Kryptographische Verfahren	
Symmetrisch:	AES, 3DES, (HMAC-) SHA1, (HMAC-) RIPEMD 160
Versions- und hardwareabhängig:	Behördliche Verfahren (Chiasmus / Libelle (PEPP-Board))
Asymmetrisch:	RSA, EC-GDSA, Diffie-Hellman (MODP und ECP)
Standards	
	RFC 2104 (HMAC), 2401-2412 (IPSec), 2459 (X509v3), 2510/2511 (CMP), 3281 (Attribute Certificates) ISO/IEC 15946-2 (EC-GDSA)
	IP v4
Auf Anfrage:	IP v6, v4/v6- und v6/v4-Tunnelling
QoS	
	QoS DiffServ Codepoints (DSCP), Bandbreitenmanagement pro Sicherheitsbeziehung
Terminal-Server-Protokolle	RDP (4.0, 5.0 und 5.2), ICA (6.x) , X11, NX

Thin Client-Hardware: Varianten:



LE



Desktop



SECRET

Netzschnittstellen	10/100 MBit/s Tx	10/100 MBit/s Tx 100 MBit/s Fx (ST)	100 MBit/s Fx (ST)
Max. Verzönung	–	SDIP-27 B	SDIP-27 A
Anti-Tamper	–	optional	vorhanden

secunet Security Networks AG

IT-Sicherheit und deren zukunftsweisende Anwendung ist die Kernkompetenz der secunet Security Networks AG. Die Entwicklung und Implementierung von Sicherheitslösungen für sensible Daten machen das Unternehmen zum gefragten Spezialisten. Exzellentes technologisches Verständnis spiegelt sich in den Beratungs-Dienstleistungen und fertig modulierten Produkten wider. Die fortschreitende Digitalisierung von Prozessen und Kommunikationswegen aller Art stellt secunet täglich vor neue Herausforderungen. Mit großem Know-how setzt das Unternehmen für die IT-Sicherheit Maßstäbe im Markt. Zur umfassenden Kundenstruktur gehören nationale sowie internationale Unternehmen und Konzerne ebenso wie der öffentliche Sektor. Rund 230 hochqualifizierte und erfahrene Mitarbeiter an sieben Standorten in Deutschland sowie Tochterunternehmen in der Schweiz und der Tschechischen Republik sorgen für Innovationsvorsprung, reibungslose Projektabwicklung und Rund-um-die-Uhr-Support.

Herausgeber:



secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen
Tel.: +49 - 201 - 54 54 - 0
Fax: +49 - 201 - 54 54 - 123
E-Mail: info@secunet.com
www.secunet.com