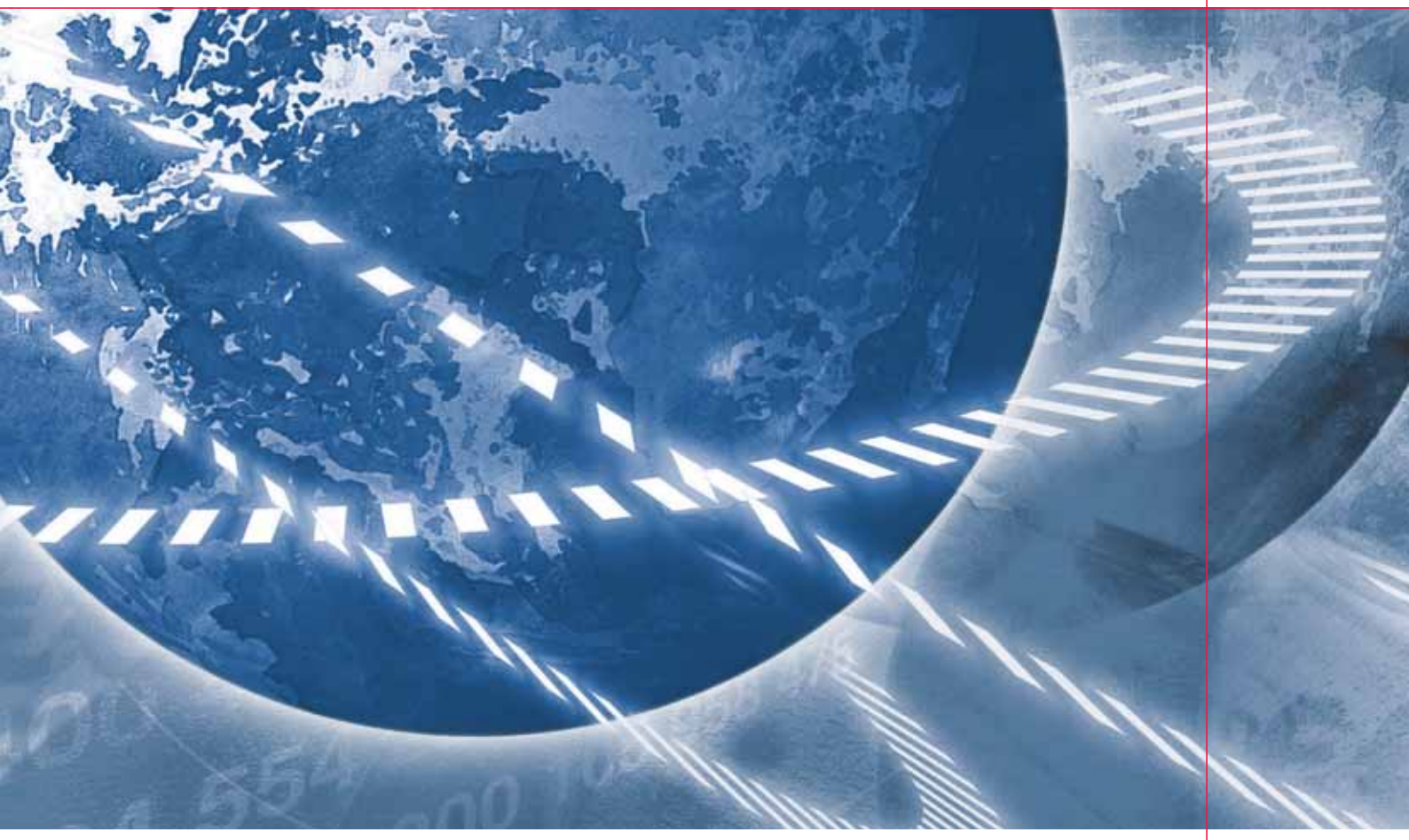
secunet

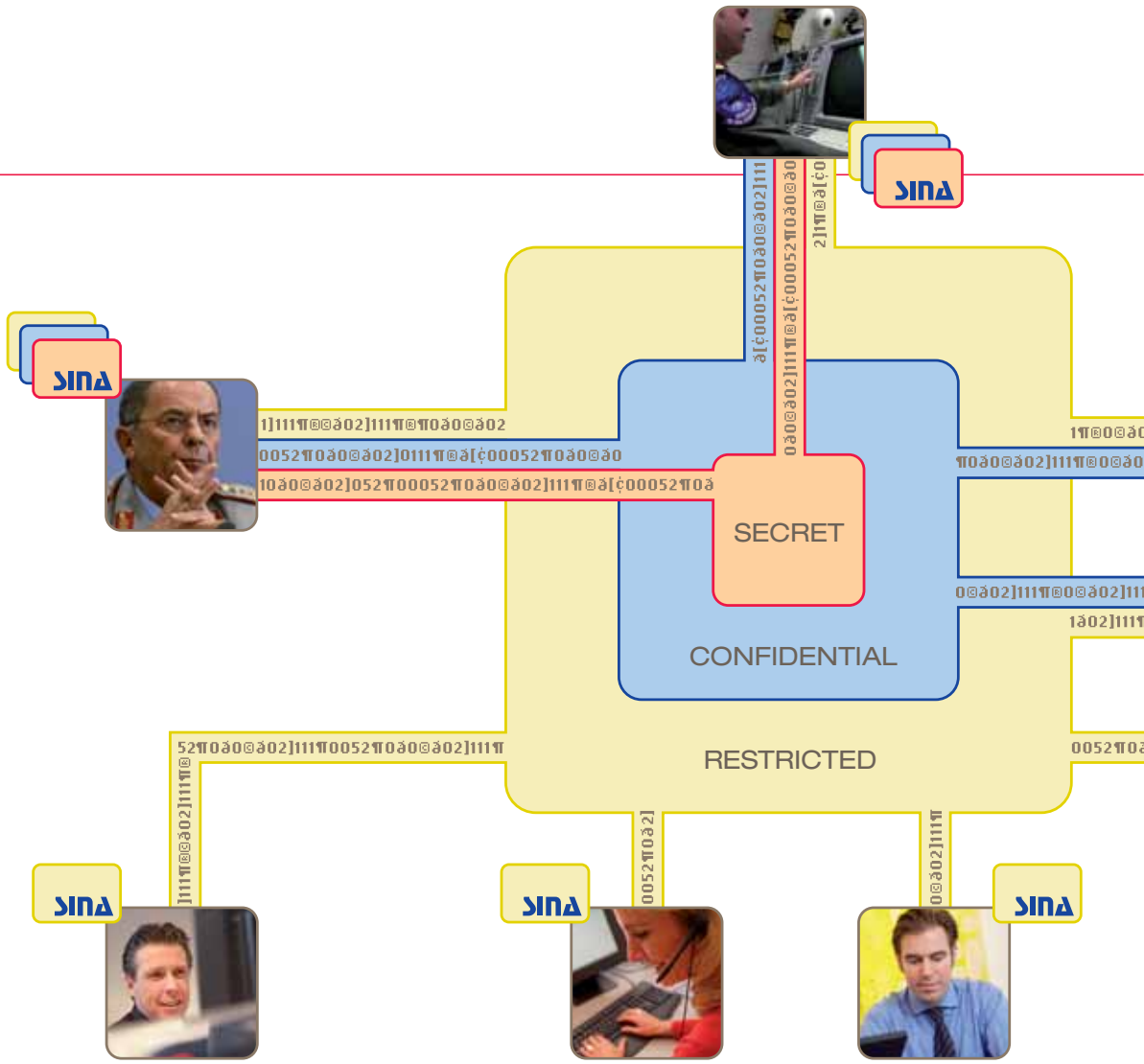
SINA®



Your Global Intranet

Perfect Interplay

High security at all levels



The SINA secure inter-network architecture enables secure processing, storage and transmission of classified documents or other confidential information (e.g. research and financial data) via the Internet. However, SINA is more than just a conventional crypto device, such as a VPN Gateway or a hard drive encrypter: SINA users can work with data of different classification levels. The strict separation of virtual sessions makes SINA the optimum platform for the cost-effective and efficient processing of sensitive information, therefore SINA can serve as a basis for a secure workflow. The feature of separated processing and storing of data with different classification levels has already been established within government authorities; but also makes sense for enterprises: Individual business

areas (administration, research departments, etc.) are then assigned to a corresponding security level and can be kept strictly separated from one another despite a common IT infrastructure. This makes it possible to implement a need-to-know principle across the entire company.

Highly secure

SINA products are approved in Germany by the German Federal Office for Information Security (BSI), in part up to the highest national security classification of TOP SECRET. In addition, there are approvals for NATO SECRET and SECRET UE.

Scalable

SINA products are based on PC hardware scaled to user and application requirements – today and in the future. They are equally suitable for office and mobile applications.

Suited to requirements

SINA ensures confidentiality for various security levels and several application scenarios. The integration of SINA into your existing infrastructure is seamless and transparent.

Cost-efficient

SINA uses any available IP-based communication infrastructure; expensive dedicated lines that offer comparable security are no longer required. Even for high-security requirements, the cost-effective Internet can be used.

Professional High-Security Technology

The basic components

SINA Box

The SINA Box is a VPN Gateway for connecting networks. All data transmitted between the sites equipped with SINA Boxes is highly encrypted. The SINA Box, as a hardened network component, also offers scalable security, protection against manipulation and emission (TEMPEST) at the highest levels. Cryptographic keys, configuration data and security associations are protected by means of a corresponding smart card.

Approval: Up to TOP SECRET, NATO SECRET and SECRET UE.

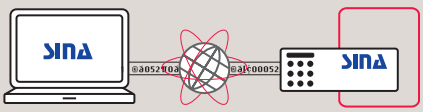
SINA Virtual Workstation

The SINA Virtual Workstation is a highly secure platform for operation of potentially insecure guest operating systems (e.g. Windows or Linux). It enables secure processing and local storage of classified data for mobile and office users in their usual system environment. Network access is possible via a SINA-protected connection to the home network. Access to the SINA Virtual Workstation is secured by means of a smart card (also available in the form of a bootable USB token): If the computer is lost or stolen, the stored data cannot be read by unauthorised persons.

Approval: Up to CONFIDENTIAL, (NATO CONFIDENTIAL)

VPN Gateway

Mobile user



Depending on the required classification level, various types and versions of SINA are available: SINA H, P, S, S/Bypass, Business.

SINA Thin Client

The SINA Thin Client is a workstation without a hard drive which is secured by means of a smart card and which does not store sensitive data on the local system. It only processes screens of standard terminal servers which are located in protected areas. Data and documents therefore remain in the protected area at all times and are secure against attacks and manipulations. Communication with the server is always encrypted. The SINA Thin Client is started from CD-ROM or Flash memory. The SINA Thin Client is also ideal for use as a secure home office solution via an Internet connection.

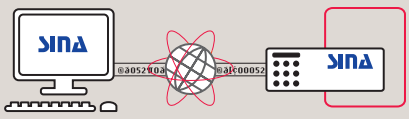
Approval: Up to TOP SECRET, NATO SECRET

SINA Virtual Desktop

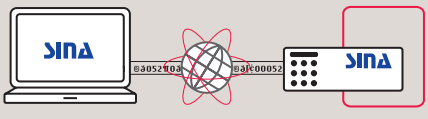
The SINA Virtual Desktop is installed as a virtual operating system on a MS Windows-based workstation. Your usual operating system environment remains unchanged. SINA technology allows you to access internal networks via the SINA Virtual Desktop. Highlight: The SINA Virtual Desktop and sensitive data are encapsulated against the “insecure” workstation system by means of a specially developed security solution (virtualisation). In addition, hard drive encryption and VPN are integrated on the basis of SINA technology.

Under evaluation (aim of the evaluation: RESTRICTED)

Thin Client/terminal server



Mobile user

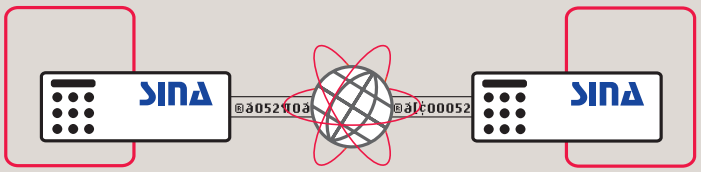


Suited to Requirements

Ready to use any place any time

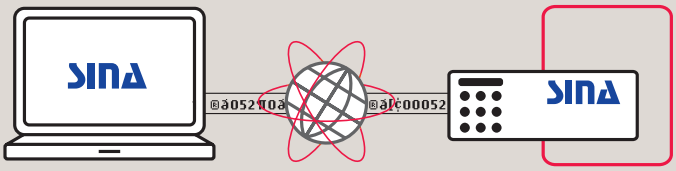
Different application areas entail different security requirements. Consequently, it must be possible to adapt the security system specifically to your requirements. Your data are to be secure at all times, whether you are sitting in the office, working from home or travelling the world with your notebook. With SINA components, a completely individual security solution can be designed, from a simple VPN all the way to a system with different security classification levels. And one thing is for sure: The data that needs protecting never leaves the secure environment of your network.

VPN Gateway



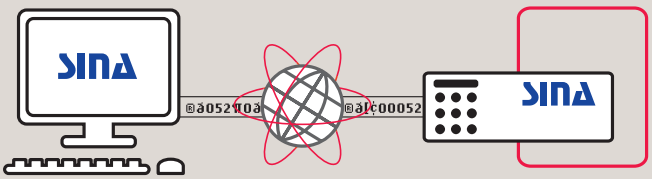
- The basic SINA component authenticates the connection partners at IP level (IPsec security associations)
- Protection of classified data to be transmitted
- Protection of access points to classified networks

Mobile user



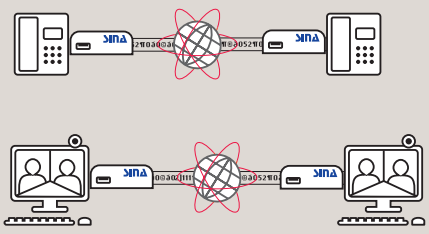
- Secure, mobile workplace with a trustworthy SINA operating system
- Secure and encrypted storage of classified data on the local storage media (cryptographic file system - CFS)
- Users can continue to work with Windows and Office applications for processing protected data

Thin Client/terminal server

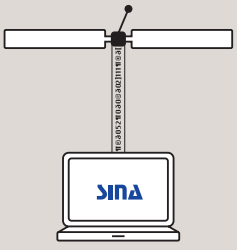


- Secure access to the network
- Employees with different authorisations can use the same workplace
- Cost-effective connection to the company network via the Internet
- Secure stationary or mobile processing of classified data
- Network administrators have secure access to their network via the SINA Thin Client.

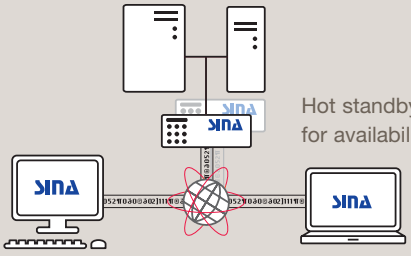
SINA provides considerably more than these basic functionalities:



Secure IP telephony (VoIP) and video conferencing



Secure satellite connection

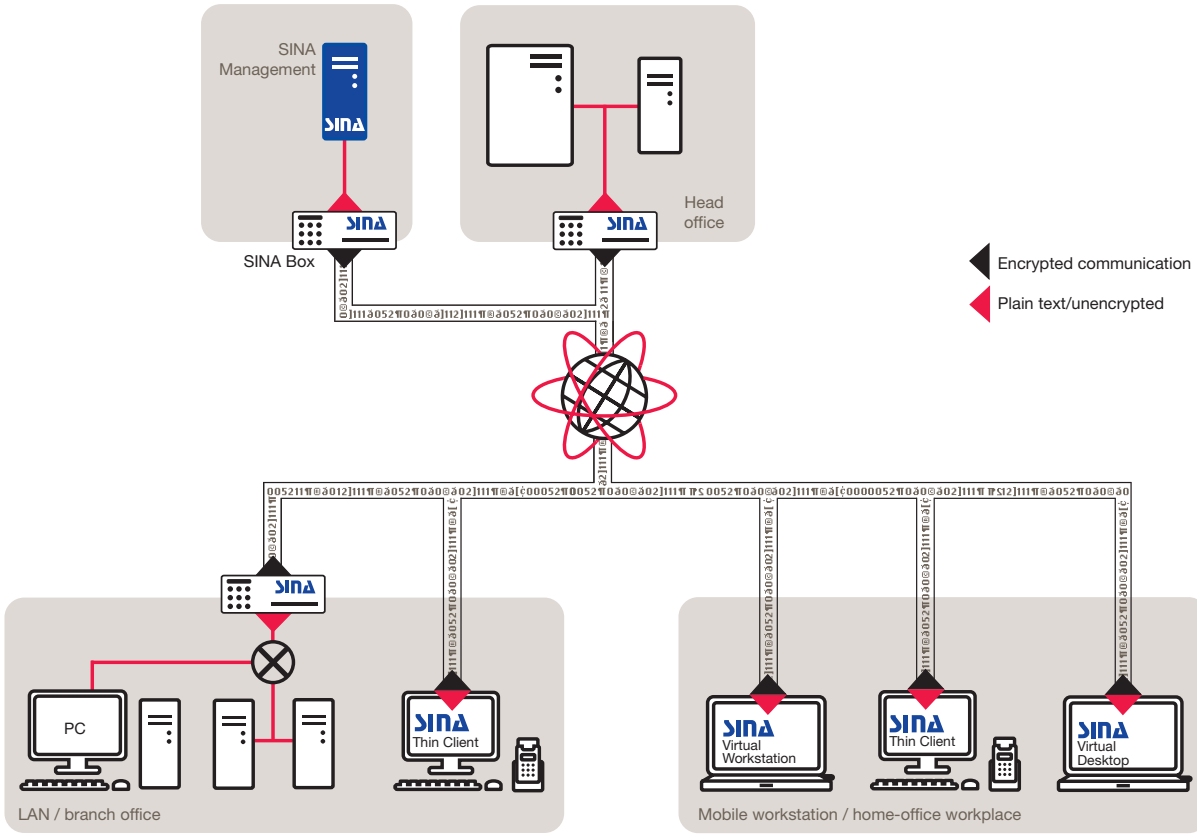


Hot standby solution for availability

Workflow security

Workflow Security

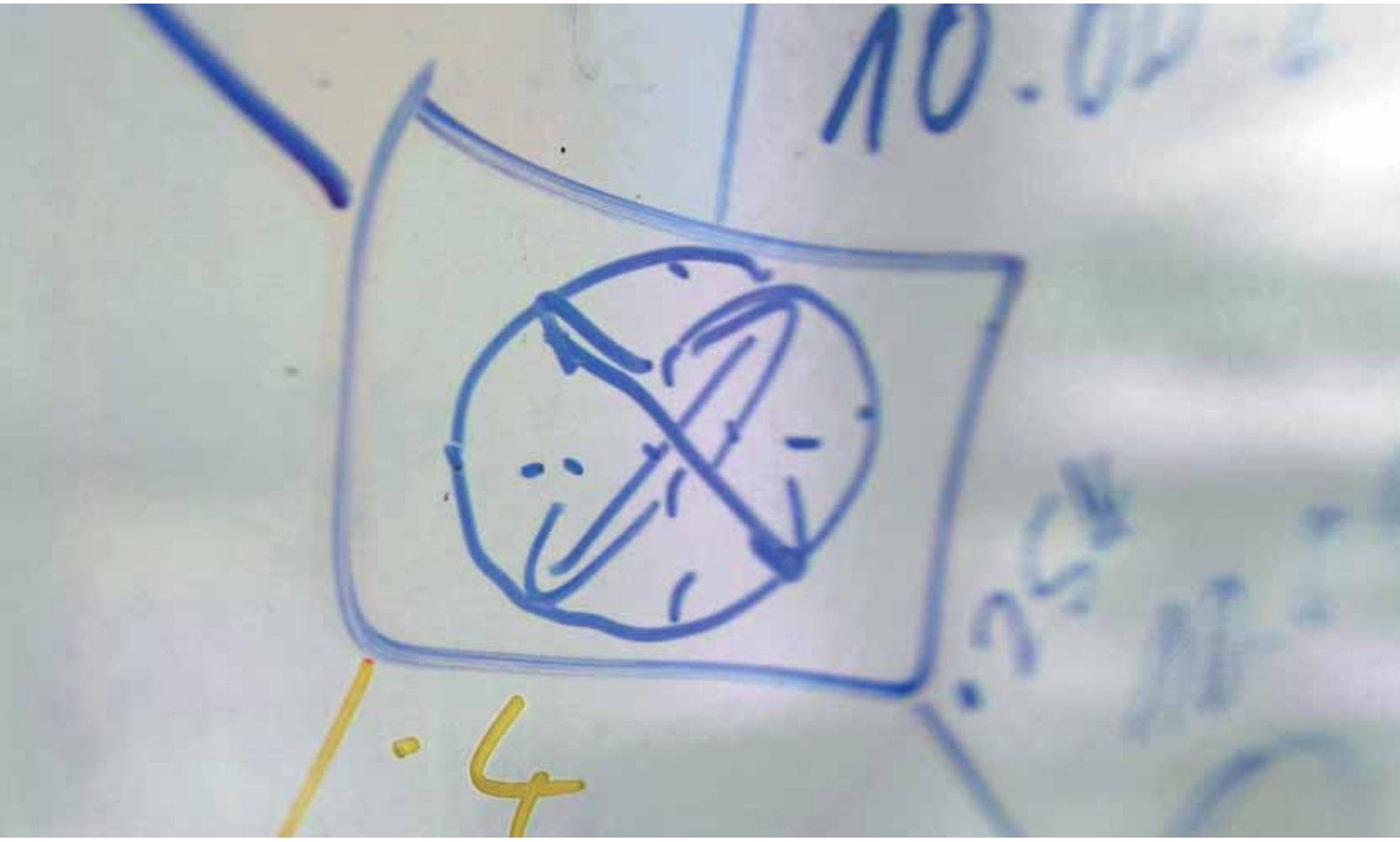
Secure processing, storage and transmission



With SINA, your data is protected against unauthorised access throughout the entire lifecycle – no matter where the data is processed and stored. Protected areas are created to provide this security, e.g. your company's LANs. Furthermore, the notebooks of your staff on the road are also part of this protected company network at all times. The data on the hard drive is not just encrypted but also encapsulated so that it is only accessible to users as required for them to do their work. Unauthorised copying or further processing is prevented as a result of the encapsulation. This way, SINA makes it possible to process and store data that requires protection locally and remotely from any place and at any time. The security associations between authorised communication partners are organised via SINA Management. The security of this Management is ensured by smart cards and a PKI.

Future Perspectives

New developments, prospects



One of the most important milestones in the development of SINA is the technological replacement of PEPP boards by our own crypto hardware based on the latest FPGA technology (SINA CORE). The crypto hardware is developed and produced at secunet in ongoing close cooperation with the BSI. Our research also focuses on the further development of our microkernel and virtualisation technologies as well as on the integration of SINA functions in mobile devices such as smart phones or PDAs. Support of upcoming IP protocols such as Multicast and IPv6 (currently IPv4) is planned. In addition, security gateways and ruggedised SINA components are being developed.

The Highest Standards: SINA and BSI

A successful public/private partnership

SINA powered by secunet

SINA was the result of the challenge to develop a security solution which is appropriate for the high security requirements of public authorities, the federal armed forces and companies handling classified information. The BSI and secunet completed the development work together and created a successful product line.

In order to be granted approval, the individual components are subject to comprehensive testing. Parallel to this they run through BSI's stringent evaluation processes. You can benefit from this too!

>> With secunet, we have found a reliable partner for the development of a security architecture for processing data requiring high-level protection. In the SINA project, the experts from secunet competently proved their flexibility and comprehensive knowledge in the development of highly complex IT security solutions. We are pleased that the Secure Inter-Network Architecture SINA has now come to adopt a global pioneering role in terms of security technology. <<

Dr. Udo Helmbrecht, President, BSI

>> When the German Federal Foreign Office in Berlin communicates with German embassies throughout the world, the very highest security requirements must be met. At the same time, communication must be cost-effective and economical. It was not until the SINA solution suite was implemented that these high requirements could be met despite our limited budget. By providing the option of secure communication via standard Internet lines, secunet has generated sustainable added value for us. The successful co-operation in this project has led us to have secunet develop solutions for further security issues in various areas. <<

Dr. Rolf Theodor Schuster,
CIO, German Federal Foreign Office

secunet

secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen, Germany
SINA hotline +49 18 05 - 76 55 55
(14 cent/min. from the German landline network)

sina@secunet.com
www.secunet.com

Find out more about SINA on www.secunet.com/sina.

SINA 0208