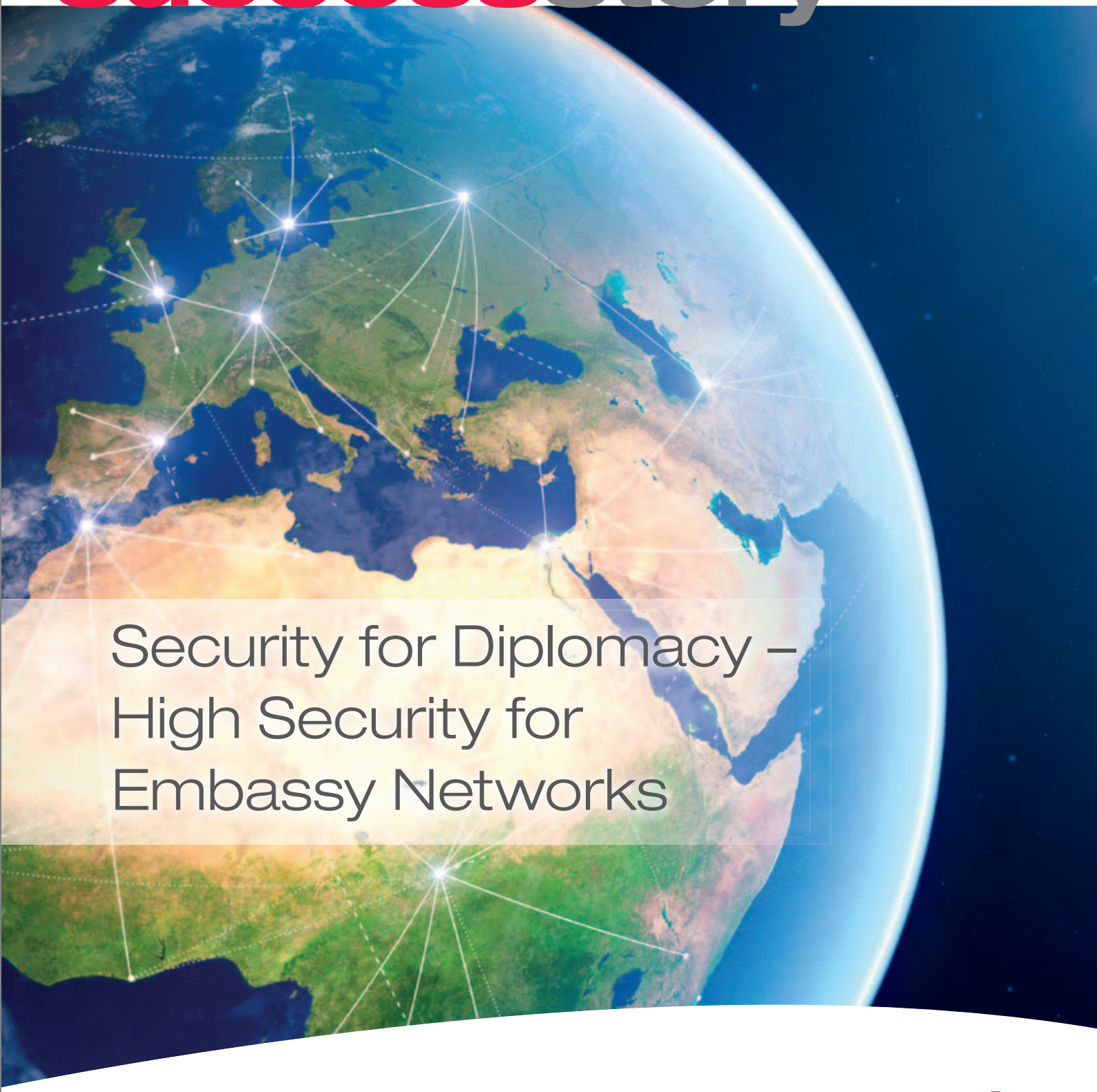
successstory



Security for Diplomacy – High Security for Embassy Networks

secunet

Today the consistent deployment of strong cryptography, along with key management that regulates access to data, are the only ways to protect against risks such as Stuxnet and wikileaks.

Dr. Rainer Baumgart, CEO secunet, Behörden Spiegel 2011

challenge

The foreign ministries of many nations are the heart of national diplomacy and their embassies and consulates represent a country abroad. Confidential and, depending on the political circumstances, critical information flows across national boundaries.

Such information can often be of great interest to third parties and any kind of publication may have serious consequences for diplomats or even the home country. Therefore this data requires special protection and its availability must be ensured everywhere at all times. The requirements placed on embassies and their networks are high and diverse:

- Secure processing, storage and transfer of data
- Rapid and secure communication, including in regions where special circumstances in terms of the political situation or infrastructure apply
- High availability via DSL, ISDN, leased line or satellite
- Reduction of network costs
- Integration of many different applications and services
- Simple commissioning in overseas diplomatic representations, even without IT specialists
- Handling of differently-classified documents (need-to-know)

benefits

- Approval at many countries up to the highest national level of confidentiality
- High secure transfer of all data
- Use of all IP-enabled communication channels e.g. Internet
- Also usable in areas with poor provider infrastructure, e.g. via satellite
- Ready for use also under extreme climatic conditions
- Model reliant tempest and manipulation protection
- Emergency deletion function for emergencies
- Availability of all necessary information to all employees
- Simultaneous information to all embassies around the world
- No need of IT know-how at embassies' sites
- Shipping possibility with commercial transport services at all classification levels
- Technology made in Germany

What you might need from us ...

Our customers have to choose their options when planning to secure their embassy network in terms of redundancy, throughput, tempest … Experienced secunet consultants will help you to define the best solution.

However, a typical deployment scenario for securing data transfer, VoIP and video conferencing might include:

- ✔ n x SINA L3 Box S 30M for each embassy. Our smallest SINA device, ideal for all locations with only small available bandwidth.
- ✔ 2 x SINA L3 Box S 200M for the central location. Higher throughput up to 200 MB/s, redundant set-up.
- ✔ 1 x SINA Management. Enables the central administration of all SINA devices from the Ministry of Foreign Affairs.
- ✔ n x SINA Workstation for travelling users. Secure data handling, online and offline.
- ✔ 1 week SINA Training for administrators at the central location.

On your request we'll of course be of help with all services, from planning to network integration and roll-out.

solution: Ten years' experience in protecting of embassy networks

For years many foreign ministries have entrusted the IT security of their globally distributed diplomatic representations to secunet. In all embassy networks it maintains, secunet deploys the secure inter-network architecture SINA developed in conjunction with the Federal Office for Information Security. This architecture enables the secure processing, storage and transfer of confidential information across open networks. SINA arose out of the desire to create solutions that meet the high security requirements of ministries, public authorities and the defence sector.

SINA can cost-effectively secure and safeguard electronic communication in any country of the world in line with the existing infrastructure, whether via leased lines, Internet or satellite. This enables any IP-compatible network to be used for data transfer up to a classification of TOP SECRET.

A role concept manages the access rights of all authorised employees. A uniform infrastructure is able to strictly separate differently-classified data – from unclassified to TOP SECRET – meaning that all official employees can only see what is specifically intended for them. Within this role concept special rights can be defined that, for example, give the ambassador access to all the information for his or her respective area of responsibility.

The daily work in embassies and consulates additionally requires a high level of mobility. This mobility also places high demands on the ICT facilities. Here, too, security has the highest priority, which can be taken as read with SINA.

Embassies and consulates play an important role when applying for visa and passports. For many years secunet is a trusted partner and advisor to national and international organisations such as the German Border Control, ICAO and others with regard to developing new standards with an emphasis on biometrics in ID documents. secunet's solutions, which are deployed internationally, comprise all aspects of the eID lifecycle – from applying for a document and enrolment to production and issuance up to usage during identity checks and finally returning the document.

deployment

Secure embassy data link

The ongoing coordination and information exchange with headquarters in the home country is central to the work of the embassies around the world. Today a lot of information that requires high levels of protection is transferred electronically.

By using SINA the information cannot be read, manipulated or redirected at any time as the entire data stream is encrypted during transfer. This protection is achieved using a virtual private network solution (VPN) which is configured between sites and is suited to the rapid exchange of confidential and secret communications, including via the public Internet. All diplomatic representations are equipped with a SINA L3 Box that is responsible for the encryption of the data and setting up the connection in the VPN.

The SINA L3 Box is a gateway that does not contain any encryption material or cryptographic functions itself. Only when used in connection with a smartcard and a PIN can the data on the network be encrypted and decrypted. This means that the SINA L3 Box can be stored without restrictions and sent even with commercial mail services. If the embassy needs to be abandoned in an emergency, leaving the box behind does not represent a security risk: depending on the model all that is required is the removal of the smartcard or the activation of an emergency deletion button.

SINA®

Federal Office for Information Security

*SINA is a joint development of BSI and secunet.

Secure mobility

Alongside the secure network connection with SINA L3 Boxes, the SINA product range caters for travelling employees or honory consuls, home workspaces and offices off the ministry or embassy site. The SINA Terminal is suitable for stationary deployment. This is a computer with no hard disc that merely functions as an input and output terminal and shows an image of the data on screen. The data itself remains on the servers at HQ at all times. The SINA Terminal is geared towards data transfer of all security classifications and is particularly suited to remote workspaces. Here, too, the role concept applies and only allows previously defined access to data.

Mobile employees can be supplied with a notebook on which they can securely process, store and transfer data while they are out and about. Unlike the SINA Terminal, data can also be stored locally on the encrypted hard disc. A secure VPN connection to the SINA network is set up via each connection, even via a public hot spot or via satellite.

Secure telephony

Encrypted telephone calls or videoconferences can also be conducted within the SINA network. Telephone calls are made via Voice over IP (VoIP), meaning that no costs are incurred for secure telephone lines. In the SINA Workstation the two software functions telephony and videoconferencing are preinstalled as standard depending on the model. Embassy workers can make phone calls from any Internet connection in the world via a headset connected to the notebook – protected against unwanted taps in the net at all times.

success

Foreign Ministries who implemented their world-wide embassy network with secunet not only reduced costs of the networking, but also improved the collaboration of the sites and sped up working processes. Information security and high availability do not necessarily rule out cost savings. Individual customers have calculated savings since the deployment of SINA to be up to 75%: the use of public networks for setting-up an embassy network means that no expensive dedicated embassy leased lines need to be deployed. The deployment of VoIP via the SINA network not only increases the tap-proofing of telephone, but is also considerably cheaper than a normal tap-proof phone line. The communication costs alone can thus be reduced in the long term for an embassy network fitted with SINA.

The operational environment, maintenance and simplified roll-out scenarios can also have a cost-saving effect: depending on the model the SINA L3 Box is shielded from radiation and protected from manipulation and therefore does not require any specially protected environment or rooms (e.g. Faraday cage). It can be set up in regular offices and can also be commissioned by employees without specialist IT knowledge. The commissioning and administration of the system are handled conveniently online by the IT department in the home country.

secunet Security Networks AG

secunet is one of Germany's leading providers of superior IT security. In close dialogue with its customers – enterprises, public authorities and international organisations – secunet develops and implements high-performance products and state-of-the-art IT security solutions. Thus, secunet not only keeps IT infrastructures secure for its customers, but also achieves intelligent process optimisation and creates sustainable added value.

At secunet, more than 270 experts focus on issues such as cryptography (SINA), e-government, business security and automotive security aiming always to be one step ahead of competitors in terms of quality and technology. secunet emphasises on long-term relationships with its customers in an atmosphere based on partnership, as demonstrated by our successful security relationship with the Federal Republic of Germany which has been active since 2004.

secunet

secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen
Germany
Phone: +49-201-5454-0
Fax: +49-201-5454-1000
E-mail: info@secunet.com
www.secunet.com

04/2012