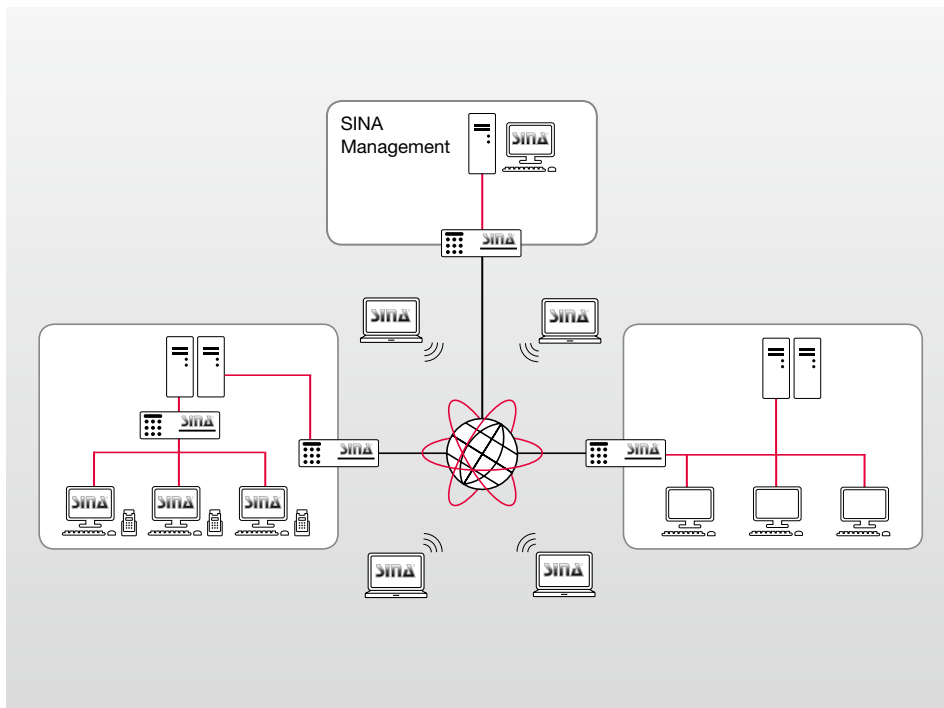


## Configuration and administration of your SINA infrastructure



### Benefits:

- » **Central administration of SINA components**
- » **Separate roles for crypto-administration and configuration management**
- » **Can be adjusted to different levels of complexity**
- » **Statically (offline) or actively controlled (online) configuration**

SINA Management centrally administers and configures all components of the SINA product range encrypting at network layer 2 or 3. With the help of SINA Management, the networks to be secured are set up, configured and administered. The graphical user interface enables the easy configuration of access rights among the SINA components and networks.

### SINA Management functionality

SINA Management compiles configuration data, like certificates, IP address configuration and routing information and writes this data to a trusted and protected storage medium (smart card or USB token with integrated smart card). The configuration data is securely stored on the smart cards, where they are available to the SINA components.

With SINA Management, infrastructures with many thousands of SINA components can be administrated. Here, the following sample parameters/properties can be configured:

- Network configuration of SINA components
- Security associations and their distribution over a directory service
- Revocation lists of compromised or vulnerable components as well as no longer authorised SINA administrators
- Cryptographic algorithms and parameters (e.g. period of validity for keys) for specific security associations
- Generation of authentication keys for SINA L2 Boxes
- Secure online updates of cryptographic parameters
- Generation and online updating of signature and encryption certificates for SINA L3 Boxes and user
- Application-specific user profiles for (terminal) server access
- Configuration profiles for SINA clients
- Media-specific access control lists (ACLs) for monitoring external interfaces (e.g. USB)
- Secure online software updates of SINA components

SINA Management can initiate specific actions with the SINA components, including prompting the certificate updates, gathering and importing status information relevant to operations and rebooting the system. SINA components accept these requests via the network, provided the network has been configured by SINA Management.

Thanks to the modular setup of the servers and administration consoles, flexible usage of SINA Management is possible. It can be installed as a stand-alone system on a single system or hierarchically installed and used separately across multiple servers. This modularity allows for a multitude of configurations and redundant scenarios.

### SINA Management components

#### SINA PKI

Certificate management is based on a public-key infrastructure (PKI) and creates key pairs and certificates upon issuing the smart cards. These are then used to securely authenticate SINA users or SINA components when establishing a connection using digital signatures. When creating the smart cards, additional cryptographic parameters are stored to them, PIN letters and postal information are generated and entries on the issuing process and period of validity are saved to a database. Here, the basic components of certificate management are certification authority (CA), registration authority (RA) and a CMP (Certificate Management Protocol) server.

#### LDAP directory service

With the help of the LDAP directory service, online management makes it possible to update the intercommunication of SINA components online,

distribute updates and revocation lists for emergencies and modify some cryptographic parameters of the SINA system. In order to reduce the possibility of downtime, the LDAP server can also be set up redundantly.

#### Time server (NTP)

The NTP service enables to safeguard uniform system times of related SINA components and of the SINA Management system.

#### Syslog server

The log data generated by SINA components are received and stored by the syslog server.

#### System requirements

SINA Management supports standard hardware with the Red Hat Enterprise Linux operating system (RHEL, version 5 or higher) and can be operated on corresponding RHEL-compatible hardware.

#### Systems monitoring

Monitoring SINA systems is possible using the several integration options of the monitoring information (syslog, SNMP) in existing standard network management systems.

#### Approvals

Over the course of the approval process of the respective SINA components, the individual software versions of SINA Management are also evaluated by the BSI (German Federal Office for Information Security) and approved for operation.

### About SINA

secunet developed SINA – the Secure Inter-Network Architecture – for the German Federal Office for Information Security (BSI). The product family of crypto systems enables the secure processing, storage and transmission of classified information as well as other sensitive data – according to approval requirements.

The product portfolio covers different gateways, line encryptors, clients and management systems which have been in use in the public sector, armed forces and companies handling classified information for many years. Selected SINA components are approved for processing and transmitting classified information up to and including the classification levels NATO SECRET and SECRET UE.

More information:  
[www.secunet.com/en/management](http://www.secunet.com/en/management)

**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](mailto:info@secunet.com)  
[www.secunet.com](http://www.secunet.com)