SINA Management

Central administration

Configuring and Managing your SINA Infrastructure

SINA Management centrally manages and configures all components in the SINA product portfolio: SINA line encryptors and Gateways, SINA Clients and SINA Workflow. The networks requiring protection are structurally created, configured and administered with the aid of SINA Management.

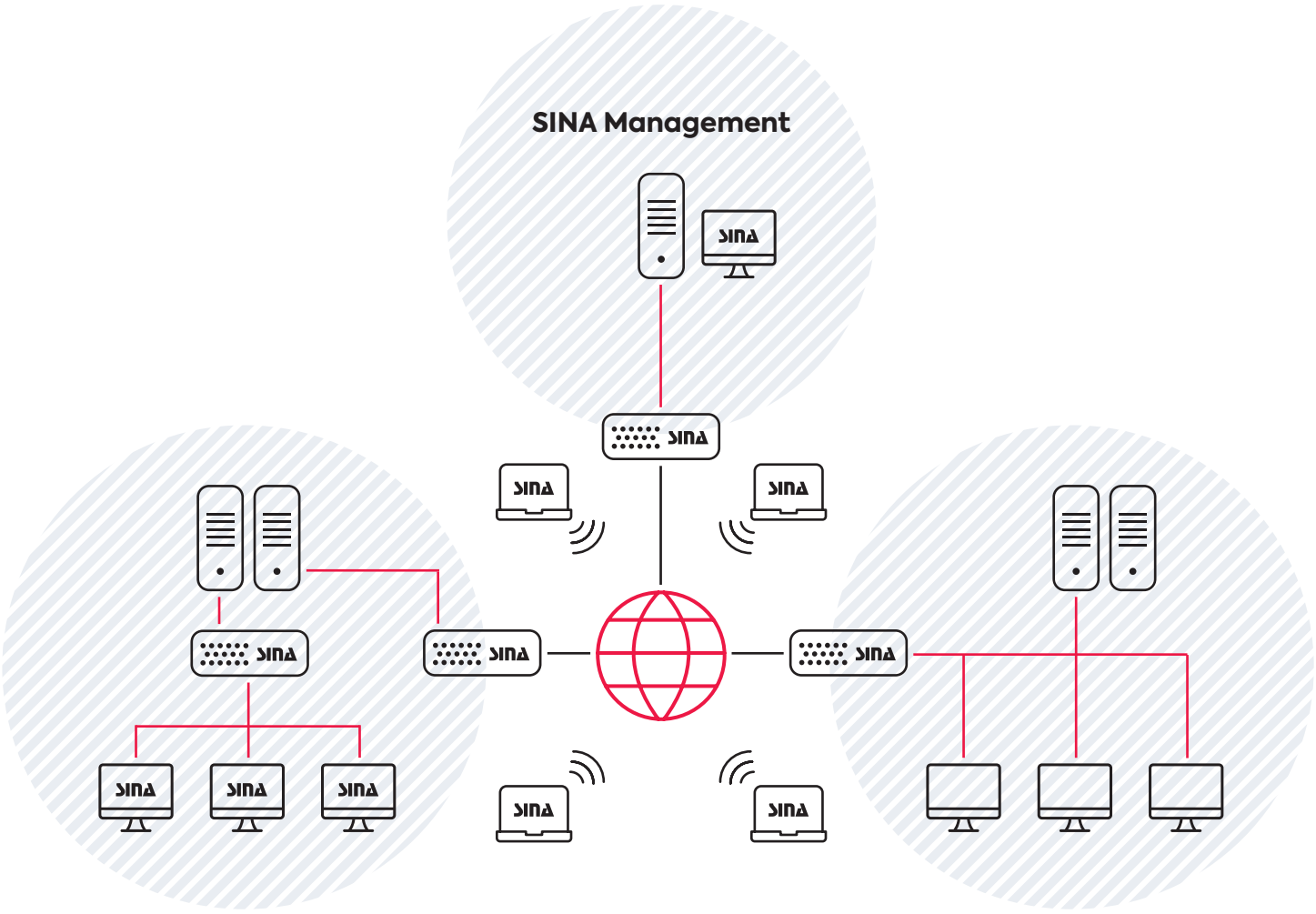
The graphic user interface enables simple configuration of the security associations and access authorisations between the SINA components and networks.

SINA Management functionality

SINA Management administers configuration data such as IP address configurations or routing information for the SINA components, and writes these to a trusted, protected storage medium (smartcard, security token or USB token with integrated smartcard). The configuration data is securely stored on SINA smartcards and made available for the SINA components. In addition the keys and certificates required for secure operation of the components are created in SINA Management, administered there and also written to the storage media.

Infrastructures with up to several thousand SINA devices can be managed with SINA Management. The following parameters and features can be configured when doing so:

- Network configuration of SINA components
- Security associations and their distribution across a directory service
- Blacklist of compromised or consequentially endangered components and SINA administrators no longer in authority
- Cryptographic algorithms and parameters (e.g. key lifetime) for security associations
- Secure online updates for cryptographic parameters and device configuration
- Generation of authentication keys for SINA L2 Boxes (SINA line encryptors)
- Issuing and online updates of signature and encryption certificates for SINA gateways and users
- Issuing of signature and encryption certificates for use in SINA Workflow



- Application-specific user profiles for (terminal) server access
- Configuration profiles for SINA clients
- Media-specific access control lists (ACLs) for controlling external interfaces (e.g. USB)
- Secure online software updates for SINA components

SINA Management can initiate certain actions on SINA components via the network e.g. updating certificates, capturing and reading operationally related status information or system reboots.

SINA Management is versatile to use due to its modular concept. It can be run in stand-alone mode on a single PC or scaled up hierarchically and distributed across multiple servers. This modularity enables a range of configurations and redundant scenarios.

Benefits

- Central management of SINA components and users
- Separate roles for crypto administration and configuration management
- Needs-based scalability for networks of varying complexities
- Static (offline) or actively-controlled (online) configuration

SINA Management components

SINA Console
SINA Console is the central graphic configuration and management interface (GUI) in SINA Management. It enables clear and convenient management of all SINA components, users and their associations with one another, as individual objects or in groups. Smart cards with all the necessary data (specifically configuration settings, keys and certificates) are detailed in SINA Console. PIN letters and despatch information are generated for this, and information regarding the issuance process and the length of validity of keys is stored in the database. Furthermore the data for online management is written to the directory service (LDAP server) in SINA Console.

SINA PKI
Secure authentication during the process of connecting two SINA components is assured using signatures. The certificates required for this are generated by the SINA PKI (Public Key Infrastructure). Basic components of the SINA PKI are a certification authority (CA), registration authority (RA) and a CMP (Certificate Management Protocol) server.

LDAP directory service
The LDAP directory service enables online updating of communications associations for SINA components, distribution of updates and blacklists, and changes to some of the cryptographic parameters in the SINA system. To increase fail-safe operation, the LDAP can be set up as redundant.

Time server (NTP)
The NTP service ensures consistent system times for associated SINA components and SINA Management.

Syslog server
The log data generated by SINA components is received and stored by the Syslog server.

System requirements

SINA Management supports standard hardware with the Red Hat Enterprise Linux (RHEL) operating system.

Systems monitoring

Monitoring of SINA components is enabled by introducing monitoring information (Syslog, SNMP) into the existing network management systems.

BSI approval

The individual SINA Management software versions are assessed by the Federal Office for Information Security Germany (BSI) and approved for operation.

Sources

Authority customers in Germany can acquire SINA components from the framework contract 5070 “Encryptors of the SINA Family” of the Procurement Office of the German Federal Ministry of the Interior. secunet would also be pleased to serve all other national and international customers.

secunet Security Networks AG
Kurfürstenstraße 58 · 45138 Essen · Germany
T +49 201 5454-0 · F +49 201 5454-1000
info@secunet.com · secunet.com

More information:
secunet.com/en/sina

secunet

SINA Management_EN_10/20