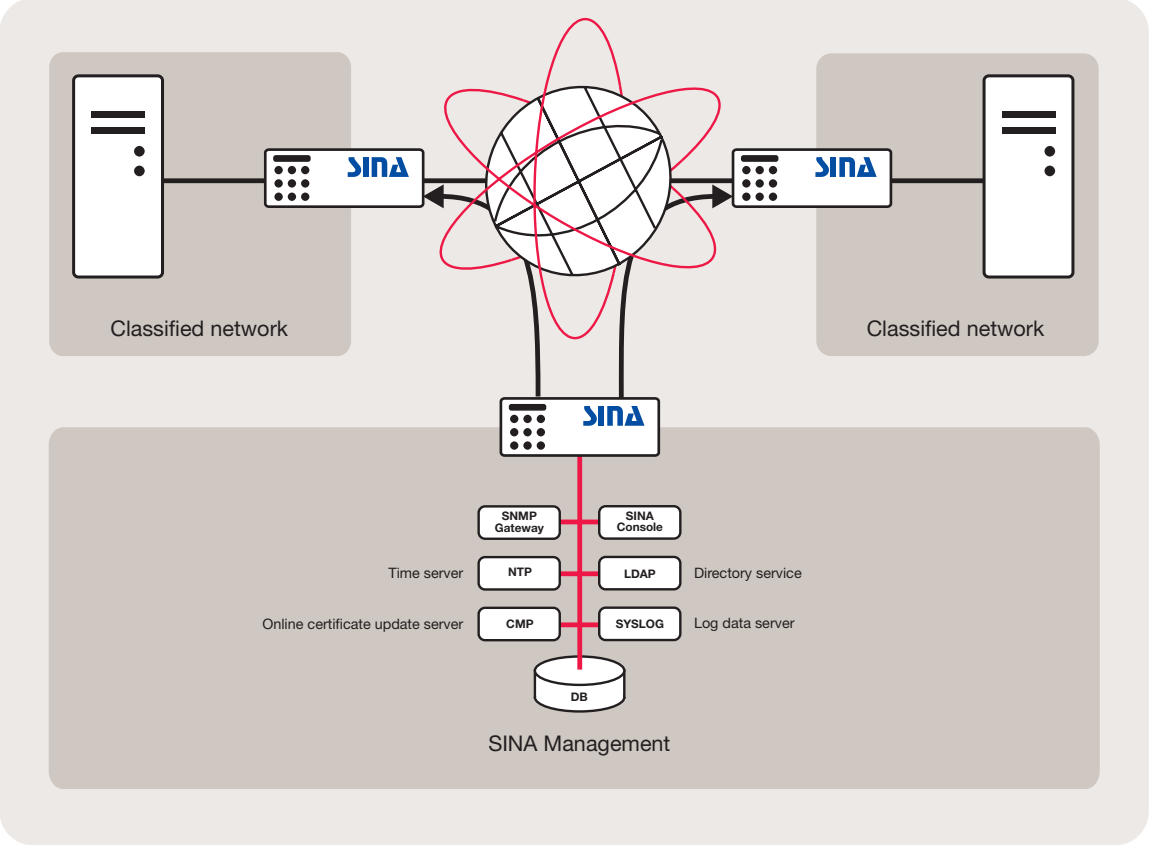
SINA Management

SOLUTION



SINA Management is used for configuration and administration of SINA components in the network. The management system can be installed on a dedicated server or distributed over several systems. It enables user-friendly configuration management and is highly configurable and extensible to protect against system failure and data loss.

The technology

All components of a SINA network are administrated centrally by the SINA Management. Configuration data, e.g. IP address configuration and routing information, is entered and made available to the systems via a trustworthy storage medium (smart card or USB token with integrated smart card) by the **configuration management**. It is also used for simple and intuitive configuration of security associations even in very complex networks. The use of online management makes it possible to update security associations of the SINA components online, distribute updates and blacklists in emergency situations, and change several cryptographic parameters of the security associations or of the SINA system by means of the **LDAP directory service**.

Your advantages:

- Simple administration of security associations
- Modular design
- Scalability
- Redundancy
- User-friendliness

Crypto management, which is based on a public key infrastructure, generates pairs of keys and certificates when smart cards are issued. These cards are used for secure authentication of SINA users or SINA Gateways by means of digital signatures when connections are established. During generation (also "personalisation") of the smart cards, additional cryptographic parameters are loaded to the smart card, PIN letters and mail data are generated and details concerning the issuing process and validity period are stored in the database.

The underlying components of the crypto management are a **certification authority (CA)** and a **registration authority (RA)** as well as a **CMP server** (CMP: Certificate Management Protocol).

The RA serves as the interface between the user and the CA; it identifies the administrator and, together with the SINA Management, creates the necessary user data on the smart cards or USB tokens.

When the CA is operated in online mode, it is possible to issue certificates for several RAs as well as update certificates in the field automatically before expiration by means of the SINA systems themselfs. The **Certificate Management Protocol (CMP)** is used between a CMP server (a CA) and a CMP client (an RA or SINA system).

Additional optional servers are syslog servers as well as time servers: the **syslog server** accepts and stores the log files generated by SINA components. **Time servers (NTP)** synchronise the clocks of the SINA components and the SINA Management.

Operation monitoring

For security reasons, it is not currently possible to operate interactive protocols such as SNMP directly with SINA components in the network. Interaction with a network- and system management can be carried out via the SINA SNMP Gateway, which converts a specified set of information concerning the status of a SINA system into a standardised MIB format. This can then be processed with standard network monitoring tools.[1]

Alternatively, a wide variety of customer-specific options to analyse SYSLOG information is available.

Modularity and scalability

The overall SINA Management is highly scalable as a result of the large number of modularly structured servers and operational components. It can run on a dedicated PC (all-in-one management), or several redundant and/or hierarchical servers can be set up. LDAP, Syslog and NTP can be deployed as redundant systems on different servers at different sites. Management can also be divided into crypto management and configuration management, which can then be run at various sites or operated by different administrators. This division in particular meets the requirements in many public authority use cases (separate cryptographic administration).

The modularity allows for many configurations and redundant scenarios which protect against system damage and subsequent data loss. This ensures the continued operation of SINA components even if parts of the SINA Management fail.

Approvals

The SINA Management itself has no approvals. The respective versions are released by the BSI.

Sources of supply

You can purchase SINA directly through secunet or through authorised SINA distributors.

[1] scales up to about 100 systems

secunet Security Networks AG

IT security and its trend-setting usage is the core competence of secunet Security Networks AG. The development and implementation of IT security solutions for sensitive data turn secunet into a specialist in great demand. Excellent technological understanding is reflected in our consulting services and modulated products. Progressive digitalization of processes and communication channels of all kind pose new challenges for secunet day-to-day. Due to our large know-how we set standards in the IT security market. Our extensive clientele comprises national and international companies and affiliated groups as well as the public sector. About 230 highly qualified and experienced employees at seven branch offices in Germany as well as at further offices in subsidiaries in Switzerland and the Czech Republic are engaged in the creation of innovations, the optimal settlement of projects and our twenty-four-seven support.

Editor:

secunet

secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen, Germany
Phone: +49 - 201 - 54 54 - 0
Fax: +49 - 201 - 54 54 - 123
E-mail: info@secunet.com
www.secunet.com