



Mit dem SINA Management werden die Konfigurationen und die Administration der SINA-Komponenten im Netzwerk vorgenommen. Das Managementsystem kann auf einem dedizierten Server oder verteilt auf mehreren Systemen installiert werden. Es ermöglicht ein benutzerfreundliches Konfigurationsmanagement und ist gegen Systemausfall bzw. Datenverlust robust konfigurierbar und erweiterbar.

Die Technik

Alle Komponenten eines SINA-Netzwerkes werden zentral vom SINA Management verwaltet. Mit Hilfe des **Konfigurationsmanagements** werden Konfigurationsdaten, wie z. B. IP-Adresskonfiguration und Routing-Informationen erfasst und über ein vertrauenswürdigen Speichermedium (Smartcard oder USB-Token mit integrierter Smartcard) den Systemen zur Verfügung gestellt. Es erledigt außerdem die einfache und intuitive Konfiguration von Sicherheitsbeziehungen auch in sehr komplexen Netzwerken. Durch die Verwendung des Online-Managements ist es möglich, mit Hilfe eines **LDAP-Verzeichnisdienstes** Kommunikationsbeziehungen der SINA-Komponenten online zu aktualisieren, Updates und Sperrlisten für Notfälle zu verteilen sowie einige kryptographische Parameter der Sicherheitsbeziehungen bzw. des SINA-Systems zu ändern.

Ihre Vorteile:

- Einfache Verwaltung von Sicherheitsbeziehungen
- Modularer Aufbau
- Skalierbarkeit
- Redundanz
- Benutzerfreundlich

Mit dem **Krypto-Management**, das auf einer Public-Key-Infrastruktur basiert, werden Schlüsselpaare und Zertifikate beim Ausstellen der Smartcards erzeugt. Mit diesen erfolgt eine sichere Authentifizierung von SINA-Benutzern oder SINA Gateways im Zuge des Verbindungsaufbaus mittels digitaler Unterschriften. Beim Erzeugen (auch „Personalisieren“) der Smartcards werden weitere kryptographische Parameter auf die Smartcard geladen, PIN-Briefe und Versandinformationen generiert und Einträge über Ausstellungsprozess und Gültigkeitsdauer in der Datenbank hinterlegt.

Grundlegende Bestandteile des Krypto-Managements sind dabei eine **Zertifizierungsinstanz (CA)** und eine **Registrierungsinstanz (RA)** sowie ein **CMP-Server** (CMP: Certificate Management Protocol).

Die RA bildet die Schnittstelle zwischen dem Benutzer und der CA, sie identifiziert den Administrator und erstellt zusammen mit dem SINA Management die erforderlichen Benutzeranteile auf den Smartcards oder USB-Token.

Im Online-Betriebsmodus der CA kann das Bereitstellen von Zertifikaten für mehrere RAs sowie ein automatisches Zertifikat-Update (vor Ablauf der Gültigkeit von Benutzerzertifikaten) durch die SINA-Systeme im Feld erfolgen. Dabei kommt das **Certificate Management Protocol (CMP)** zum Einsatz, das zwischen einem CMP-Server (einer CA) und CMP-Clients (einer RA oder SINA-Endgerät) benutzt wird.

Weitere optionale Server sind Syslog-Server sowie Zeitserver: Der **Syslog-Server** dient der Entgegennahme und Abspeicherung der von SINA-Komponenten generierten Logdateien. Durch **Zeitserver (NTP)** erfolgt die Synchronisierung von Systemzeiten der SINA-Komponenten und des SINA Managements.

Betriebsüberwachung

Aus Sicherheitsgründen ist es derzeit nicht möglich, interaktive Protokolle, wie beispielsweise SNMP, direkt mit den SINA-Komponenten im Netzwerk zu betreiben. Die Interaktion mit einem übergeordneten Netzwerk- und

Systemmanagement kann über ein SINA SNMP Gateway erfolgen, das eine fest vorgegebene Informationsmenge über den Zustand einer SINA Box in ein standardisiertes MIB-Format wandelt. Dieses kann anschließend mit handelsüblichen Netzwerküberwachungstools weiterverarbeitet werden.¹

Alternativ werden vielfältige, kundenspezifische Auswertungsmöglichkeiten der SYSLOG-Informationen angeboten.

Modularität und Skalierbarkeit

Das gesamte SINA Management ist auf Grund der Vielzahl der modular aufgebauten Server und Bedienkomponenten hochgradig skalierbar. Es kann sowohl auf einem dedizierten PC (All-in-one-Management) untergebracht werden, oder einer resp. mehrere Serverdienste werden redundant und/oder hierarchisch ausgelegt. LDAP, Syslog und NTP können dabei auf unterschiedlichen Servern an verschiedenen Standorten redundant ausgelegt werden. Auch funktional kann das Management in Krypto- und Konfigurationsmanagement aufgeteilt werden, die wiederum an verschiedenen Standorten untergebracht oder auch durch unterschiedliche Betreiber bereitgestellt werden können. Insbesondere diese Aufteilung deckt sich in vielen behördlichen Einsatzfällen mit den Vorgaben über die Krypto-Verwaltung.

Die Modularität erlaubt damit eine Vielzahl von Konfigurationen und redundanten Szenarien, die vor Systemschäden und dadurch entstehenden Datenverlusten schützen. Damit ist ein Weiterbetrieb der SINA-Komponenten auch bei Ausfall von Teilen des SINA Managements gewährleistet.

Zulassungen

Das SINA Management selbst erhält keine Zulassungen. Die jeweiligen Versionen werden durch das BSI freigegeben.

Bezugsquellen

Behörden können SINA-Technologie aus dem Rahmenvertrag BA 4867/01 des Beschaffungsamtes des Bundesministeriums des Innern beziehen. Nicht-behördliche Kunden können SINA direkt über secunet oder über autorisierte SINA-Wiederverkäufer beziehen.

¹ Nur bis zu einer Anzahl von etwa 100 Systemen verwendbar.

secunet Security Networks AG

IT-Sicherheit und deren zukunftsweisende Anwendung ist die Kernkompetenz der secunet Security Networks AG. Die Entwicklung und Implementierung von Sicherheitslösungen für sensible Daten machen das Unternehmen zum gefragten Spezialisten. Exzellentes technologisches Verständnis spiegelt sich in den Beratungs-Dienstleistungen und fertig modulierten Produkten wider. Die fortschreitende Digitalisierung von Prozessen und Kommunikationswegen aller Art stellt secunet täglich vor neue Herausforderungen. Mit großem Know-how setzt das Unternehmen für die IT-Sicherheit Maßstäbe im Markt. Zur umfassenden Kundenstruktur gehören nationale sowie internationale Unternehmen und Konzerne ebenso wie der öffentliche Sektor. Rund 230 hochqualifizierte und erfahrene Mitarbeiter an sieben Standorten in Deutschland sowie Tochterunternehmen in der Schweiz und der Tschechischen Republik sorgen für Innovationsvorsprung, reibungslose Projektabwicklung und Rund-um-die-Uhr-Support.

Herausgeber:

secunet

secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen
Tel.: +49 - 201 - 54 54 - 0
Fax: +49 - 201 - 54 54 - 123
E-Mail: info@secunet.com
www.secunet.com