

## Die intelligente Software-Appliance für zentrale E-Mail-Sicherheit

Der Versand von E-Mails ist die am meisten genutzte geschäftliche Anwendung im Internet. Trotzdem ist es bisher nicht möglich, alle damit verbundenen unternehmensspezifischen Arbeitsabläufe elektronisch abzubilden. Eine große Herausforderung ist vor allem der sichere Austausch von E-Mail mit vertraulichem Inhalt.

Die Verschlüsselung und Signatur von vertraulichen E-Mails sind zwar grundsätzlich über E-Mail Clients zu realisieren, allerdings ist dazu die Beherrschung der Sicherheitsanwendung durch die Mitarbeiter notwendig. Dies ist nicht immer gegeben. Infolgedessen bleibt die Umsetzung der Sicherheitspolitik eines Unternehmens häufig unvollständig.

SafeGuard MailGateway integriert die kryptographischen Prozesse der Ver- und Entschlüsselung sowie der elektronischen Signatur und Verifikation an zentraler Stelle im Unternehmensnetzwerk. Die Sicherheitslösung ist für den Absender transparent und setzt die unternehmensinternen Sicherheitsrichtlinien für die E-Mail-Kommunikation automatisch um. Die Absender und Empfänger können wie gewohnt per E-Mail kommunizieren, ohne sich um die Vertraulichkeit der Inhalte sorgen zu müssen.

### SafeGuard MailGateway gewährleistet:

- Dass bestehende E-Mail-basierte Workflow-Prozesse einfach und sicher um Vertraulichkeit, Authentizität und Integrität ergänzt werden.
- Die zentrale Umsetzung von E-Mail-Verschlüsselung und -Signatur und ermöglicht somit das Enforcement interner Sicherheitsrichtlinien.
- Dass eingehende und ausgehende E-Mails automatisch für den Adressaten im eigenen Netzwerk entschlüsselt bzw. für den externen Empfänger verschlüsselt werden können.

Für die Ver- und Entschlüsselung von E-Mails sowie die digitale Signatur verwendet SafeGuard MailGateway die etablierten Internet-Standards S/MIME und OpenPGP. Die gesicherte Anbindung externer Kommunikationspartner ohne Sicherheitsinfrastruktur gewährleisten die Alternativen SafeGuard PrivateCrypto und SafeGuard PDFMail. SafeGuard MailGateway ist skalierbar von kleinen Installationen über redundante Installationen bis hin zum organisationsweiten Einsatz im Clusterbetrieb.

## Die Vorteile

### Verbesserte Sicherheit

- » Zentrale Umsetzung der unternehmensweiten Sicherheitspolitik für E-Mail-Verschlüsselung und Signatur
- » Flexibel und sehr detailliert definierbares Regelwerk
- » Unterstützt S/MIME, OpenPGP, SafeGuard PrivateCrypto und SafeGuard PDFMail
- » Integrierte Certification Authority zur automatischen Schlüssel- und Zertifikatsgenerierung
- » Ermöglicht Virenschanning verschlüsselter E-Mails
- » Ideale Erweiterung zu ILP und CMF Systemen

### Einfach einzusetzen

- » Schnelle Installation und Inbetriebnahme durch Software-Appliance-Konzept
- » Nahtlose Integration in bestehende PKI- und E-Mail-Infrastrukturen
- » Integrierter Key-Server für S/MIME und OpenPGP
- » Einbindung von Unternehmensverzeichnisdiensten wie Microsoft ActiveDirectory®
- » Alternative Verschlüsselungsverfahren zur zertifikatslosen E-Mail-Verschlüsselung
- » Unabhängig von E-Mail-Servern wie Lotus Notes, Microsoft Exchange, etc.
- » Skalierbar von kleinen Installationen bis zum unternehmensweiten Einsatz im Clusterverbund

### Einfach handhabbar

- » Transparent für den Benutzer
- » Interoperabel mit den Standards für E-Mail-Sicherheit und somit hohe Benutzerakzeptanz
- » Zentrales Regelwerk und Schlüsselmanagement zur Sicherung des E-Mail-Verkehrs
- » Selbsterklärende Administrationsoberfläche
- » Komfortable Skalierbarkeit, Migration und Wartung

## Sicherheit

- Schutz von wertvollen Unternehmensdaten und personenbezogenen Daten in E-Mails
- Umfassende zentrale und skalierbare Sicherheitslösung für den Einsatz in SMTP-basierten E-Mail-Infrastrukturen
- Flexibel und sehr detailliert definierbares Regelwerk
- Unterstützt S/MIME, OpenPGP, SafeGuard PrivateCrypto und SafeGuard PDFMail
- SafeGuard PDFMail und SafeGuard PrivateCrypto sind die Lösungen für E-Mail Clients ohne S/MIME- oder OpenPGP- Unterstützung
- Automatische E-Mail-Ver- und Entschlüsselung sowie Signatur
- Automatische Schlüssel- und Zertifikatsgenerierung für S/MIME und OpenPGP
- Integrierter Key-Server für S/MIME und OpenPGP
- Unterstützung von Verzeichnisdiensten und Key-Servern

## Systemadministration

- Einfache, zentrale Installation, Konfiguration und Administration von Betriebssystem und Applikation
- Rollenbasierte Administration
- Reporting und Monitoring
- Hohe Performanz und Systemsicherheit
- Komfortables Backup und Restore
- Automatische Update-Server
- Einfache und schnelle Wartung
- Umfassende Online-Hilfe zur Administration
- Flexibler Umgang mit Zertifikatsprüfungen und Vertrauenshierarchien

## Benutzerkomfort

- Transparent für Benutzer
- Definierbare Steuerbefehle für Benutzer und Applikationen
- Definierbare Statusmeldungen für Benutzer
- Hohe Akzeptanz bei den Anwendern – kein zusätzliches Training notwendig

## Systemanforderungen

### Hardware

- » Intel CPU
- » Mind. 512 MB RAM
- » IDE/SCSI/SATA Harddisk
- » IDE/SCSI/USB CD-ROM-Laufwerk
- » Ethernet-Netzwerk-Adapter

## Systemeigenschaften

### Betriebssystem

- » CentOS
- » Unterstützung von VMware®
- » Installation
- » Vollständige Installation von CD-ROM
- » Management
- » Webmanagement inkl. umfangreicher Online-Hilfe

### Schnittstellen und Formate

- » SMTP(S), TLS, HTTP(S), SSH, SCP, FTP, NTP, SNMP
- » LDAP(S), OCSF, HKP
- » S/MIME, OpenPGP, SafeGuard PrivateCrypto, SafeGuard PDFMail
- » X.509, PEM, DER, PKCS#7, PKCS#12, CRL
- » OpenPGP-Schlüssel, PGP/MIME, PGP/Inline

### Kryptographische Standards

- » Asymmetrische Verschlüsselung: RSA, DSA, El Gamal
- » Symmetrische Verschlüsselung: RC2, RC4, DES, 3DES, Blowfish, Twofish, Cast5, AES, AES192, AES256
- » Hash: MD2, MD5, MDC2, SHA, SHA-1, RipeMD160

### Sprachversionen

- » Englisch, Deutsch

SGMG 5.70