



Secure Internet Traffic



COMPANYCRYPT®

The encryption module for MIMESweeper

CompanyCRYPT the encryption module for MIMESweeper

Technische Spezifikationen

Produkt

CompanyCRYPT ist ein Zusatzmodul für Clearswift MIMESweeper mit dem die unternehmensweiten Policies für E-Mailsicherheit um die zentrale E-Mail-Verschlüsselung und digitale Signatur erweitert werden. Die E-Mail-Lösung unterstützt beide Verschlüsselungsstandards S/MIME und OpenPGP und erreicht damit eine Marktabdeckung von 100%.



Leistungsmerkmale

Sicherheit

- ❖ Geschützte Übertragung von wertvollen Unternehmensdaten und personenbezogenen Daten per E-Mail
- ❖ Gesetzeskonforme Verschlüsselung der E-Mail-Daten
- ❖ Sicherung der E-Mails vor Manipulation während der Übertragung
- ❖ Vollständige Anwendung aller Security-Policies incl. Inhaltsüberprüfung, Virenschutz und Anti-Spam auch auf verschlüsselte E-Mails
- ❖ Optimale Sicherheitslösung für den Einsatz in MIMESweeper-Infrastrukturen
- ❖ Hochsichere und performante Systemarchitektur durch MIMESweeper-Integration

Funktionen

- ❖ Universelle Verschlüsselungsszenarien, wie "Best Effort" oder "Always Encrypt"
- ❖ Option zur Festlegung der Verschlüsselungs-/Signaturmethoden durch individuell angepasste MIMESweeper-Policy
- ❖ Flexible E-Mail-Verschlüsselung (Body und Anhänge oder nur Attachment-Verschlüsselung)
- ❖ Anwendergesteuerte Aktivierung verschiedener Schutzverfahren (Endanwender kann Funktionen durch Schlüsselworte steuern)
- ❖ Unterstützung der Standards S/MIME und OpenPGP
- ❖ Spontane „Ad Hoc Verschlüsselung“ für Empfänger, die keine Verschlüsselungstechnologie einsetzen
- ❖ Verwendung bewährter und geprüfter Sicherheitsalgorithmen auf Basis von GnuPG und OpenSSL
- ❖ Support für Domänen-, Team- und Gatewayzertifikate
- ❖ Eigene Onboard-Certification Authority (CA) mit Support für lokale CRL (Certificate Revocation List)
- ❖ On-Demand Schlüssel- und Zertifikatsgenerierung
- ❖ Vollautomatischer Import von Schlüsseln und Zertifikaten
- ❖ Site-to-Site Verschlüsselung (Sicherung des gesamten Mailverkehrs zwischen zwei oder mehr Domänen)
- ❖ Umfassende Signaturprüfung über komplette Ausstellerkette
- ❖ Integrierter Update-Checker

MIMESweeper Integration & Einsatz

- ❖ Einfache Installation und schnelle Inbetriebnahme durch nahtlose Integration auf höchstem Technologiestandard direkt in die MIMESweeper-Content-Security-Lösung
- ❖ Keine Investition in zusätzliche Hardware und Wartung dank Plug-In Konzept
- ❖ Harmonische Integration in die bestehende E-Mail-Infrastrukturen (Keine Änderungen am E-Mail-Routing oder dem Fail-Over-Konzept nötig)
- ❖ Umfangreiche Auswahl von Verschlüsselungs-Szenarien werden im MIMESweeper bereitgestellt und ermöglichen somit eine flexible Anpassung der Verschlüsselungsregeln
- ❖ Unabhängig von der internen Groupwarelösung wie Lotus Notes, Microsoft Exchange oder Groupwise
- ❖ Beliebig skalierbar von Installationen auf Einzelsystemen bis zum geografisch verteilten Einsatz im MIMESweeper-Clusterverbund
- ❖ Serverbasiert und damit transparent für den Endanwender
- ❖ Hohe Akzeptanz bei den Anwendern – kein zusätzliches Training notwendig



Administration

- ❖ Zentrales Management und Schlüsselverwaltung auch für verteilte Umgebungen
- ❖ Sichere, intuitive Verwaltung per Weboberfläche (HTTPS)
- ❖ Keyserver-Funktion (automatischer Schlüsselaustausch) für S/MIME und OpenPGP durch MIKE (Mail Initiated Key Exchange)
- ❖ Verwaltung vertrauenswürdiger Aussteller im eigenen Trust-CA-Store
- ❖ Automatisiertes, zeitgesteuertes Backup und Restore der Konfiguration, Schlüssel und Zertifikate
- ❖ Detaillierte Statistiken und grafische Traffic-Reports sind über das MIMESweeper-Reporting verfügbar
- ❖ Geringer Administrationsaufwand durch die Automatisierung von Schlüsselimport, Schlüsselerzeugung, Schlüsselaustausch, Aktualisierung der lokalen CRL Liste und Systemsicherung

Highlights:

- ❖ Automatische Ver- und Entschlüsselung, zentral und ohne Benutzer-Interaktion
- ❖ Vollständige Unterstützung der Standards S/MIME und OpenPGP
- ❖ Ad Hoc Encryption zur sofortigen Verschlüsselung auch an Kommunikationspartner ohne Verschlüsselungstechnologie
- ❖ Einfache Integration direkt in das Content Security-Gateway MIMESweeper ohne zusätzliche Hardware
- ❖ Ermöglicht die vollständige Anwendung aller Security-Policies incl. Inhaltsüberprüfung, Virenschutz und Anti-Spam auch auf verschlüsselte E-Mails
- ❖ Zentrales Management und Schlüsselverwaltung
- ❖ Beliebig skalierbar durch MIMESweeper-Clustering



Systemanforderungen

Hardware

Nachfolgend finden Sie die Anforderungen für den MIMesweeper für SMTP und CompanyCRYPT.

- ❖ Mind. Pentium III (Dual Core 2 GHz empfohlen)
- ❖ Ab 1 GB RAM (2 GB RAM empfohlen)
- ❖ 20 GB Festplattenspeicher

Software

- ❖ Windows 2000 Server
Windows Server 2003 Standard oder Enterprise
- ❖ MAILsweeper for SMTP 4.x oder MIMesweeper for SMTP 5.x

Standards & Formate

- ❖ SMTP, HTTP(S)
- ❖ S/MIME (RFC 2633), OpenPGP (RFC 3156, RFC 2440, RFC 4880)
- ❖ X.509, PEM, DER, KEY, PKCS#7, PKCS#12
- ❖ OpenPGP-Schlüssel, PGP/MIME, PGP/Inline
- ❖ Asymmetrische Verschl.: RSA, RSA-E, RSA-S, ELG-E, DSA, ELG
- ❖ Symmetrische Verschl.: DES, 3DES, CAST5, AES (128/192/256), RC2, RC5, BLOWFISH, TWOFISH
- ❖ Hash: MD5, SHA1, RIPEMD160, SHA (224/256/384/512)

Schlüsselerzeugung

- ❖ 1024 Bit – 4096 Bit (OpenPGP und S/MIME)

Schlüsselimport

- ❖ 168 Bit – 4096 Bit (OpenPGP und S/MIME)
- ❖ OpenPGP: beliebige Dateiendung (ASCII- oder binär-codiert)
- ❖ S/MIME: X.509 v3 beliebige Dateiendung (DER- o. PEM-codiert)
- ❖ Private oder öffentliche Schlüssel/Zertifikate, sowie CA Zertifikate oder selbstsignierte Schlüssel

S/MIME – Weitere Merkmale

- ❖ Auswahl zwischen „Opaque“- oder „Detached“-Signatur bei allen Signaturaufgaben
- ❖ S/MIME-Attachments ohne Kennzeichnung im SMTP-Datenbereich (unspezifischer Content-Type)
- ❖ Unterstützung für zweckgebundene Zertifikate (Nur Verschlüsselung oder nur Signatur)
- ❖ Berücksichtigung der S/MIME v3 Erweiterungen (z. B. Nutzungsrestriktionen)
- ❖ Vorinstallierte Root-Zertifikate von bekannten CAs im eigenen Zertifikatsspeicher

PGP – Weitere Merkmale

- ❖ Persönliche oder Firmensignatur nur für Nachrichtentext
- ❖ Nur Attachment-Verschlüsselung
- ❖ Automatische Entschlüsselung einzelner verschlüsselter PGP-Dateianhänge (Binär- oder ASCII-Codiert, *.PGP *.GPG *.ASC)

Ad Hoc Verschlüsselung – Weitere Merkmale

- ❖ Passphrasengeschütztes Sicherungsverfahren ohne Zertifikate und Schlüsselaustausch
- ❖ Symmetrische Verschlüsselung nach AES-128 CBC
- ❖ Automatisch generiertes oder manuelles Passwort
- ❖ Verschlüsselung der kompletten Mail (Betreff, Body, Attachments)

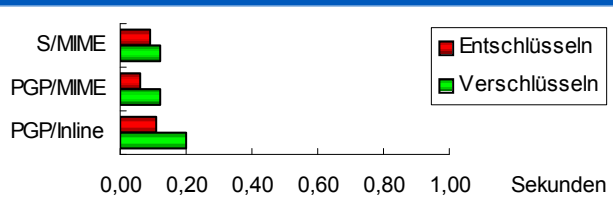
Performance

Die hohe Verarbeitungsgeschwindigkeit der Lösung beim Ver- und Entschlüsseln wird auch den Anforderungen von extrem großen Mailumgebungen gerecht.

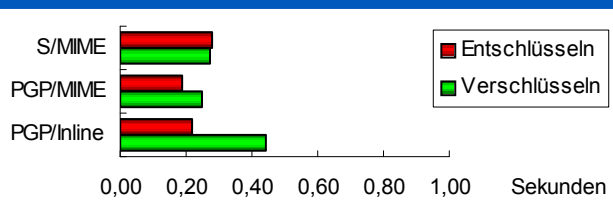
Auf jedem Gateway können Mailvolumina von bis zu 5 Gigabyte pro Stunde verarbeitet werden.

Verarbeitungszeiten

Mailgröße 10 KByte



Mailgröße 1024 KByte (1 MB)



Testparameter/-umgebung:

- Hardware: AMD Athlon 2,7GHz, 1 GB RAM
- Schlüssellänge (Ver- und Entschlüsselung): 2048Bit
- Sym. Algorithmus: AES-128 (PGP) / 3DES (S/MIME)

Überreicht durch:

Kontakt Secure Internet Traffic

Anschrift:
S.I.T. GmbH & Co. KG
Goseriede 4
30159 Hannover
Germany

Telefon:
+49 511 89997 10

Telefax:
+49 511 89997 12

eMail:
info@companycrypt.com

Internet:
www.companycrypt.com

