BERGT • working it-services • Kantstr. 53 • 14612 Falkensee

Sichere Übermittlung von E-Mails

Sophos integrierte E-Mail-Verschlüsselung

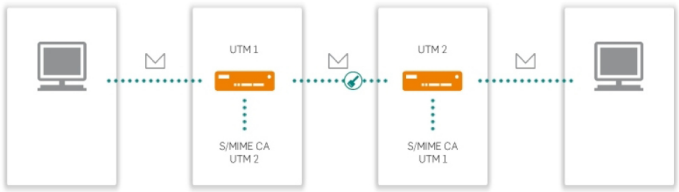
Seitdem E-Mails im privaten und geschäftlichen Bereich das primäre elektronische Kommunikationsmittel geworden sind, sind verständliche Bedenken über Privatsphäre und Authentifizierung aufgekommen. Einfach formuliert: Das E-Mail-Format wird in Klartext übermittelt. Da es darüber hinaus sehr einfach ist, falsche Identitäten anzunehmen, muss der Empfänger feststellen können, ob der Absender auch der ist, für den er sich ausgibt.

S/MIME und PGP

Der Bedarf an E-Mail-Verschlüsselung hat eine Reihe von Standards für die Public-Key-Kryptografie hervorgebracht, vor allem S/MIME und OpenPGP. Sophos UTM unterstützt beide Standards, **welche mit Ihrer bestehenden Sophos-Lizenz genutzt werden können.**

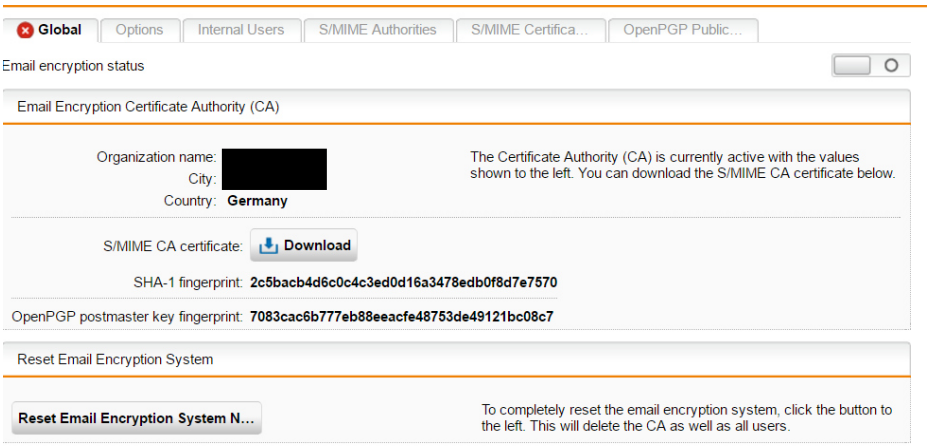
S/MIME (*Secure Multipurpose Internet Mail Extensions*) ist ein Standard für asymmetrische Verschlüsselung und das Signieren von MIME-strukturierten E-Mails. Dieses Protokoll wird üblicherweise innerhalb einer **Public-Key-Infrastruktur** (PKI) eingesetzt und basiert auf einer **hierarchischen Struktur aus digitalen Zertifikaten**, wobei es eine vertrauenswürdige Instanz als Zertifizierungsstelle (CA) benötigt.

Die CA stellt ein Zertifikat aus, bei dem sie eine Identität an ein Paar elektronischer Schlüssel bindet. Dieser Vorgang kann als digitales Gegenstück zu herkömmlichen Identitätsdokumenten wie einem Reisepass angesehen werden. Aus technischer Sicht stellt die CA ein Zertifikat aus, indem sie einen **öffentlichen Schlüssel an einen bestimmten *Distinguished Name*** im X.500-Standard oder an einen *Alternative Name* wie z.B. eine E-Mail-Adresse **bindet**. Ein digitales Zertifikat ermöglicht es festzustellen, ob jemand die Berechtigung hat, einen angegebenen Schlüssel zu verwenden.



1 E-Mail-Verschlüsselung: Mit zwei Sophos UTM-Geräten

Die gesamte E-Mail-Verschlüsselung ist für den Benutzer transparent, sodass **keine zusätzliche Verschlüsselungs-Software auf dem Client** installiert werden muss. Einfach gesagt heißt das, dass zur Verschlüsselung der E-Mails das Zertifikat der Zielpartei oder der öffentliche Schlüssel benötigt wird.



Vorteile

- Nutzung der bestehenden Sophos Lizenz
- Vorhandene UTM Cluster Ressourcen nutzen
- Keine Software-Client-Installation erforderlich
- Im Einsatz befindliche und bekannte Administrations-oberfläche nutzen
- Automatisches ver- und entschlüsseln
- Einsatz von 128-Bit-AESVerschlüsselung (FIPS-konform)
- Unterstützung mobiler Smartphones wie z.B. Android und Windows Mobile
- Unmittelbare Compliance mit E-Mail-Richtlinien zum Schutz vertraulicher und sensibler Daten
- Kein Bedarf an komplizierten Verschlüsselungs-infrastrukturen

SOPHOS

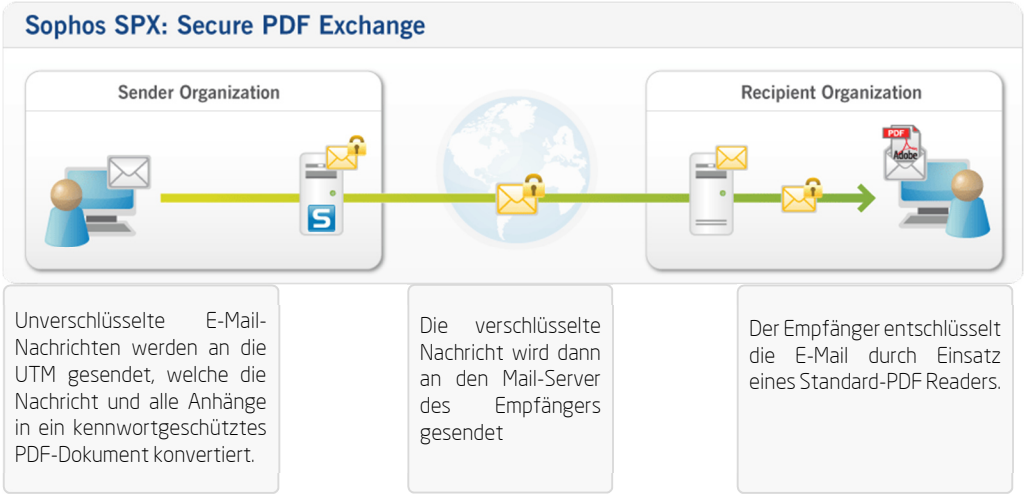
SPX Encryption

SPX Encryption schützt E-Mail-Daten bei ihrer Übertragung und unterstützt Unternehmen durch einfachste Verwaltungsfunktionen und eine transparente, unkomplizierte Bedienung bei der Einhaltung von Gesetzen und Vorschriften.

Funktionsweise

Die SPX-Encryption-Technologie ermöglicht einen zuverlässigen Schutz sensibler Daten bei der Übertragung per E-Mail und lässt sich zugleich einfach implementieren und verwalten: Gemäß den vom Administrator konfigurierten Richtlinien werden ausgehende Nachrichten am E-Mail-Gateway automatisch in verschlüsselte, passwortgeschützte PDF-Dokumente umgewandelt. Durch die SPX-Technologie muss das zur Entschlüsselung erforderliche Passwort nicht zwangsläufig über einen anderen Kanal, zum Beispiel per Telefon, an den Empfänger übermittelt werden - dieser kann das Passwort auch selbst bestimmen. Dafür erhält der Empfänger vor der Zustellung der Nachricht einen Link auf eine https-geschützte Seite innerhalb des Webportals der Appliance, auf der er ein Passwort hinterlegen kann. Danach wird das verschlüsselte PDF-Dokument per E-Mail an den Empfänger gesendet, welches er von jedem E-Mail-Client aus einfach durch Verwendung des von ihm definierten Passworts öffnen kann.

Der Empfänger erhält somit die volle Kontrolle über das Passwort - der Schutz vertraulicher Daten wird dadurch zusätzlich erhöht. Im Gegensatz zu traditionellen, auf Zertifikaten basierenden und oft komplexen Verschlüsselungslösungen ist beim Einsatz der SPX-Verschlüsselung keine Verbindung zum Netzwerk oder einer eigenen Verschlüsselungsinfrastruktur notwendig, um die Nachrichten zu lesen. Die im PDF Dokument enthaltenen Anhänge verbleiben im ursprünglichen Dateiformat (z.B. .doc, .xls, .ppt), können extrahiert und geändert werden.



Vorteile

- Einfache Einrichtung: Verschlüsselungstechnologie in weniger als 10 Minuten einsetzbar
- Keinerlei Änderungen des Benutzer-Workflows durch Beibehaltung gewohnter Bedienprozesse
- Keine Software-Client-Installation erforderlich
- Offline-Einsicht ohne aktive Internet-Verbindung
- Sichere, integrierte Antwort-Funktion
- Einsatz von 128-Bit-AESVerschlüsselung (FIPS-konform)
- Unterstützung mobiler Smartphones wie z.B. Android und Windows Mobile
- Unmittelbare Compliance mit E-Mail-Richtlinien zum Schutz vertraulicher und sensibler Daten
- Kein Bedarf an komplizierten Verschlüsselungs-infrastrukturen
- Individuell anpassbares Vorlagen-Management und flexible Markenoptionen
- Nutzung von plattform-übergreifender Standard-PDF Reader Software
- Nutzung von selbsterstellten Empfängerpasswörtern

SOPHOS

Geringer Administrationsaufwand

Einfache Administration

Traditionelle Verschlüsselungslösungen sind teuer, erfordern ein hohes Maß an Erfahrung bei ihrer Einrichtung und Verwaltung und erweisen sich für den Endbenutzer oftmals als zu komplex. Mit SPX Encryption oder der S/MIME Verschlüsselung integriert Sophos leistungsstarke Verschlüsselungsfunktionen in die Sophos UTM. Insbesondere Kunden, die bereits eine UTM im Einsatz haben, können auf Ihre vorhandene UTM Lizenz und Wissenskenntnisse in der Administration aufsetzten. Die E-Mail Verschlüsselung integriert sich nahtlos in die bestehende Administrationskonsole.. So profitieren Sie von zuverlässigem Datenschutz, ohne Kosten und Komplexität traditioneller, zertifikatbasierter Lösungen in Kauf nehmen zu müssen.

Mit S/MIME und PGP können Unternehmen:

- Ausgehende Nachrichten von internen Benutzern standardmäßig scannen, automatisch signieren und verschlüsseln. Für die Signierung und die Verschlüsselung wird entweder das Zertifikat (S/MIME) oder der öffentliche Schlüssel (OpenPGP) des Empfängers verwendet. Das Zertifikat oder der öffentliche Schlüssel müssen dafür auf der UTM vorhanden sein.
- Verschlüsselte eingehende Nachrichten von externen Benutzern, deren S/MIME-Zertifikat oder öffentlicher OpenPGP-Schlüssel UTM bekannt ist, automatisch entschlüsseln. Um die Nachricht zu entschlüsseln, muss der S/MIME-Schlüssel oder der private OpenPGP-Schlüssel des internen Benutzers auf der UTM installiert sein.
- Verschlüsselte eingehende Nachrichten von externen Benutzern oder für interne, der UTM unbekannte Benutzer zustellen, obwohl sie nicht entschlüsselt werden können. Es liegt dann in der Verantwortung des Empfängers (interner Benutzer), sicherzustellen, dass die E-Mail keine Schadsoftware enthält, beispielsweise durch die Benutzung einer eigenen Firewall.

Mit SPX Encryption können Unternehmen:

- Verschlüsselungstechnologie in weniger als 10 Minuten einsetzbar.
- Über den flexiblen Richtlinienassistenten schnell und einfach Verschlüsselungsrichtlinien definieren sowie Regeln auf Basis zahlreicher Attribute wie z.B. Sender, Empfänger, E-Mail-Inhalt, Attachments, E-Mail-Header-Merkmale usw. erstellen.
- Im Handumdrehen für Compliance mit PCI, HIPAA und anderen rechtlichen Vorschriften sowie Bundes- und Landesgesetzen zur Sicherung des E-Mail-Verkehrs und zum Schutz von Daten sorgen.

Schützen Sie Ihre sensiblen Kundendaten und intellektuelles Unternehmenseigentum vor unbefugten Zugriffen.