

ENCRYPTION.

Der Schlüssel zur sicheren E-Mail-Kommunikation.

**Ohne E-Mail-Verschlüsselung kein zeitgemäßer Datenschutz!**

E-Mail-Verschlüsselung – nicht so wichtig? Diese Einstellung hat sich deutlich geändert, wie in vielen aktuellen Umfragen sichtbar wird. Auch der Gesetzgeber fordert mit der Datenschutz-Grundverordnung (DSGVO) den Stand der Technik zum Schutz von personenbezogenen Daten – und damit auch, dass die Übertragung dieser Daten verschlüsselt erfolgen muss.

Vertraulichkeit geht schnell und einfach

Durch zentrale E-Mail-Signatur und E-Mail-Verschlüsselung am NoSpamProxy® Encryption Gateway kommunizieren Sie mit Partnern besonders sicher und einfach. Da Schlüssel und Zertifikate nur auf dem Gateway und nicht auf den Clients verwaltet werden, entfällt für den Anwender der umständliche Umgang mit elektronischen Schlüsseln – und die privaten Schlüssel sind bestmöglich vor Angriffen geschützt. Die Sicherheitsregeln im Sinne der Corporate Governance des Unternehmens werden automatisch zentral umgesetzt. Natürlich werden auch empfangene Nachrichten bereits am Gateway entschlüsselt und stehen dem Anwender wie gewohnt für die Weiterverarbeitung zur Verfügung. Dies ermöglicht den Zugriff über per TLS-Verschlüsselung gesicherte Verbindungen mit Smartphones und Tablets, sowie die Archivierung der E-Mails in unverschlüsselter Form.

S/MIME-Signatur und Verschlüsselung

S/MIME ist der empfohlene und international vereinbarte Standard zur elektronischen Signatur und zur Verschlüsselung von E-Mails. Dabei handelt es sich um ein asymmetrisches Verschlüsselungsverfahren mit öffentlichem und privatem Schlüssel. Um S/MIME nutzen zu können, müssen Sender und Empfänger über ein Zertifikat verfügen. NoSpamProxy® bietet dabei die volle Unterstützung der jeweils neuesten im Standard veröffentlichten Verschlüsselungsverfahren. Ältere Verfahren werden zur Wahrung der Kompatibilität ebenso unterstützt.

PGP Mail: Pretty Good Privacy

Und noch einfacher ist es mit NoSpamProxy®: Natürlich können mit dem Encryption-Modul auch PGP-Schlüssel generiert, importiert und verwaltet werden. Mit der Unterstützung von PGP-Verschlüsselung bietet NoSpamProxy® Encryption eine weitere Möglichkeit zum bequemen Austausch von verschlüsselten Daten und Nachrichten.

PDF Mail: auch ohne Zertifikat oder Schlüssel sicher versenden

Für den häufigen Fall, dass Empfänger keinen PGP-Schlüssel oder kein persönliches Zertifikat haben, bietet NoSpamProxy® Encryption mit der PDF-Mail-Funktion einen weiteren, einfachen Weg für den sicheren Versand von E-Mails und Dokumenten, der keine Anforderungen an den Empfänger stellt. Dazu wandelt NoSpamProxy® Encryption die E-Mail mit allen Anhängen automatisch in ein passwortgeschütztes PDF-Dokument um. Das Passwort wird dem Empfänger automatisiert per SMS zugesandt. Alternativ kann der Empfänger über die Anmeldung im NoSpamProxy-Web-Portal ein eigenes Passwort vergeben. Zum Öffnen des Dokuments braucht er dann lediglich einen PDF-Reader.

E-Mail-Verschlüsselung und Zertifikate

Im Rahmen der sicheren Verschlüsselung von E-Mails sind Zertifikate erforderlich, die für das S/MIME-Verfahren nach dem X.509-Standard oder mit einem PGP-Schlüssel genutzt werden können. NoSpamProxy® Encryption zentralisiert und automatisiert die Verwaltung und den Erwerb dieser Zertifikate. IT-Administratoren profitieren von einer Vielzahl hilfreicher Managementfunktionen.

Weitere Funktionen von NoSpamProxy® Encryption sind die Anbindung an

- DOI (für die Kommunikation zwischen Behörden, die an DOI angeschlossen sind)
- De-Mail (für die Kommunikation per De-Mail mit De-Mail Teilnehmern)

