

enQsig

Vertrauen, Datenschutz und Rechtssicherheit mit einer Lösung



enQsig™ sichert als zentrales Gateway am Eingang des Netzwerkes die Vertraulichkeit der E-Mail-Kommunikation sowie die Unveränderlichkeit von Nachrichten und ermöglicht effiziente Geschäftsprozesse durch gesetzeskonforme elektronische Signatur.

Durch das zentrale Signieren und Verschlüsseln von E-Mails am enQsig Gateway kommunizieren Sie sicher mit Partnern. Da empfangene E-Mails bereits am Gateway entschlüsselt werden, behalten Anwender die volle Kontrolle über ihren E-Mail-Verkehr im Unternehmen: für Virus- und Antispam-Checks, zur Archivierung oder Weiterleitung und Stellvertretung. Die Windows Server-Software kann durch einfaches Freischalten um die Anti-Spam- und Anti-Malware-Funktionen von NoSpamProxy® ergänzt werden.

Signatur – Vertrauensbasis für E-Mail im Geschäftsverkehr.

Verschlüsselung – Datenschutz für sensible E-Mail-Kommunikation.

Qualifizierte Signatur – Sicherer Rechts- und Geschäftsverkehr im Internet.

Vertrauen durch unveränderliche Nachrichten

E-Mail-Kommunikation in Unternehmen ist heute nicht nur der Lebensnerv für das Tagesgeschäft sondern beinhaltet unternehmenskritische Vorgänge. Doch herkömmliche E-Mail-Kommunikation verdient alles andere als hohes Vertrauen, denn sie ist vergleichbar mit dem Transport einer Postkarte durch völlig Unbekannte. E-Mail-Inhalte sind für Fremde lesbar und veränderbar.

Der erste Schritt zur vertrauenswürdigen E-Mail-Kommunikation ist die elektronische Signatur von E-Mails. enQsig führt diese Signatur am Gateway ohne Aufwand für die Benutzer durch. Mit dem standardisierten S/MIME Verfahren wird sichergestellt, dass E-Mails unverändert beim Empfänger ankommen. Falls nicht, meldet dies jede moderne E-Mail-Software dem Empfänger. Zur einfachen Administration kann für geringe Kosten ein Gateway-Zertifikat verwendet werden. Damit ist nur ein einziges „Siegel“ für die E-Mails aller Anwender notwendig. Bei Bedarf können Benutzerzertifikate eingesetzt werden.

Vertraulichkeit für Kommunikation unter Partnern

Der nächste Schritt zu vertrauenswürdiger E-Mail-Kommunikation ist die Verschlüsselung von E-Mails. Damit wird aus der Postkarte sogar mehr als ein verschlossener Briefumschlag. Denn nur der gültige Empfänger kann die E-Mail lesen.

Doch mit dem Nutzen der herkömmlichen E-Mail-Verschlüsselung sind zunächst auch administrative Probleme verbunden, die vor allem die Benutzerakzeptanz gefährden. Benutzer müssen die E-Mail-Verschlüsselung manuell aktivieren und die Zertifikate der Kommunikationspartner verwalten. Desweiteren können verschlüsselte E-Mails bei Weiterleitung nicht gelesen oder auf Viren geprüft werden.

All dem begegnet enQsig durch zentrale Funktionen an der Schnittstelle zwischen Internet und Unternehmensnetz. Die für Ver- und Entschlüsselung benötigten Zertifikate, werden zentral verwaltet und können automatisch aus empfangenen E-Mails ausgelesen werden.

Die am Netzwerk-Eingang entschlüsselten E-Mails können somit auf Spam und Viren geprüft, intern weiter geleitet werden. Ein flexibles Regelwerk erlaubt die zentrale Definition welche E-Mails verschlüsselt werden.

Gesetzeskonform und effizient mit qualifizierter elektronischer Signatur

Auf vertrauenswürdige E-Mail-Kommunikation lässt sich aufbauen, z.B. durch den elektronischen Versand von Rechnungen. Elektronische Rechnungen und andere Dokumente erfordern eine rechtsgültige Unterschrift, die durch eine sogenannte qualifizierte elektronische Signatur erreicht wird. enQsig erstellt qualifizierte elektronische Signaturen automatisiert auf Basis eines Regelwerks und entlastet Anwender vom unhandlichen Umgang mit SmartCards und PIN durch Zentralisierung am Gateway. Kosteneinsparungen durch den elektronischen Rechnungsversand können somit einfach realisiert werden.

Gesetzliche Vorschriften fordern jedoch auch die Validierung qualifizierter elektronischer Signaturen, um deren Rechtsgültigkeit beim Empfang zu dokumentieren. enQsig erledigt dies ohne Benutzereingriff und übergibt die generierten Protokolle an das unternehmensinterne Archivsystem.

Mehrnutzen durch Anti-Spam und Anti-Virus

Bedrohungen und Mehrarbeit durch Spam und Viren sind gerade bei der Umsetzung vertrauenswürdiger E-Mail-Kommunikation ein zusätzliches Hindernis. Da enQsig auf den Technologien des bewährten Anti-Spam-Gateways NoSpamProxy basiert, lassen sich dessen Funktionen einfach durch eine Lizenzenerweiterung freischalten. So kann auf nur einem Gateway und mit einheitlicher Administration auch der Schutz gegen Malware umgesetzt werden.

Systemvoraussetzungen:

- Windows Server 2003 SP 2, Windows Server 2008 (32bit und 64bit)
Die mit * gekennzeichneten Features erfordern Windows Server 2008.
- .NET Framework 3.5 mit SP1
- Microsoft SQL Server, SQL Express Edition
- Microsoft Report Viewer 2008 SP1

Funktionsübersicht:

S/MIME, CMS

Signatur & Verschlüsselung
Signaturprüfung eingehend, Ablehnen möglich
Signatur entfernen, optional
Hashverfahren MD5, SHA1, SHA256*, SHA512*
Verschlüsselungsverfahren DES, RC2 (40-128Bit), TripleDES, AES (128, 192, 256 Bit)*

TLS

Verschlüsselung und Authentisierung der Mailübertragung auf Transportebene

Qualifizierte elektronische Signatur

Signieren
Verifizieren
Prüfprotokoll erstellen (und an Mail anhängen)
Signatur entfernen, optional
Signatur bei bestimmten Anhängen erzwingen

Archivschnittstelle

Übergabe der Mail und aller Anhänge und Protokolle via Dateischnittstelle an Archiv- und DMS-Systeme

Zertifikatsverwaltung

Sammeln eingehender S/MIME Zertifikate
Zuordnung von Zertifikaten zur Domain oder Person
Personen- und Domain-Zertifikate

Regelsystem

E-Mail-Verarbeitung auf Basis eines Regelwerkes (Filter nach Absender, Empfänger und einlieferndem Gateway)

Jobsteuerung

Management temporär fehlgeschlagener qualifizierter Signatur-Aufträge

Nachrichten-Verfolgung und Reporting

Übersicht über Mail-Management mit Informationen zu Signatur- und Verschlüsselungsaktionen
Detailansicht pro Mail

Microsoft Management Console

Verwaltung auf dem Gateway oder vom Remote Arbeitsplatz mit vertrauter Konsole im Microsoft Stil
Rollenkonzept für verteilte Implementierung der Produktkomponenten

Anti-Spam/Anti-Virus

Optional: Aktivierung von Anti-Spam- und Anti-Virus-Funktionen durch Lizenzierung des NoSpamProxy Moduls