



Vertrauen, Datenschutz und Rechtssicherheit mit einer Lösung

E-Mail-Verschlüsselung – Datenschutz für sensible E-Mail-Kommunikation.

PDF-Mail – Passwort-basiert sicher kommunizieren.

Qualifizierte Signatur – sicherer Rechts- und Geschäftsverkehr im Internet.

enQsig® sichert als zentrales Gateway die Vertraulichkeit der E-Mail-Kommunikation mit Unternehmen, Behörden, Verbrauchern und Bürgern durch E-Mail-Verschlüsselung. Die Lösung ermöglicht effiziente Geschäfts- und Verwaltungsprozesse 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. E-Mail-Verschlüsselung wird so anwenderfreundlich und kann mit vielen Partnern eingesetzt werden. Die Windows Server-Software kann durch einfaches Freischalten um die Anti-Spam- und Anti-Malware-Funktionen von NoSpamProxy® ergänzt werden.

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 genießt alles andere als hohes Vertrauen, denn sie ist vergleichbar mit dem Transport einer Postkarte durch gänzlich Unbekannte. E-Mail-Inhalte sind für Fremde lesbar und veränderbar.

enQsig unterstützt die sichere und Datenschutz-konforme E-Mail-Kommunikation durch eine flexible Auswahl von Standard-Technologien und macht so jeden Empfänger weltweit sicher erreichbar.

Der erste Schritt zur vertrauenswürdigen E-Mail-Kommunikation ist die elektronische Signatur von E-Mails. enQsig führt die Signierung am Gateway ohne Aufwand für die Benutzer durch. Mit der E-Mail-Signatur wird sichergestellt, dass E-Mails unverändert beim Empfänger ankommen. Falls nicht, meldet dies jede moderne E-Mail-Software dem Empfänger.

Vertraulichkeit für die E-Mail-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 adressierte Empfänger kann die E-Mail lesen. enQsig verschlüsselt E-Mails nach den Internetstandards S/MIME oder PGP. Für die sichere Ad-hoc-Kommunikation bietet die Softwarelösung alternativ ein Passwort-basiertes Verfahren mittels PDF an.

Mit der Nutzung der herkömmlichen E-Mail-Verschlüsselung sind auch administrative Probleme verbunden, die die Benutzerakzeptanz gefährden. Benutzer müssen die E-Mail-Verschlüsselung manuell aktivieren und die Zertifikate der Kommunikationspartner verwalten. All dem begegnet enQsig mit zentralen Funktionen an der Schnittstelle zwischen Internet und lokalem Netzwerk. Die für Verschlüsselung und Entschlüsselung benötigten Zertifikate werden zentral verwaltet; die am Netzwerk-Eingang entschlüsselten E-Mails können auf Spam und Viren geprüft und intern weitergeleitet werden. Ein flexibles Regelwerk erlaubt die zentrale Definition des Verschlüsselungsverfahrens für E-Mails.



Datenblatt

Zertifikatsmanagement zentralisiert und automatisiert

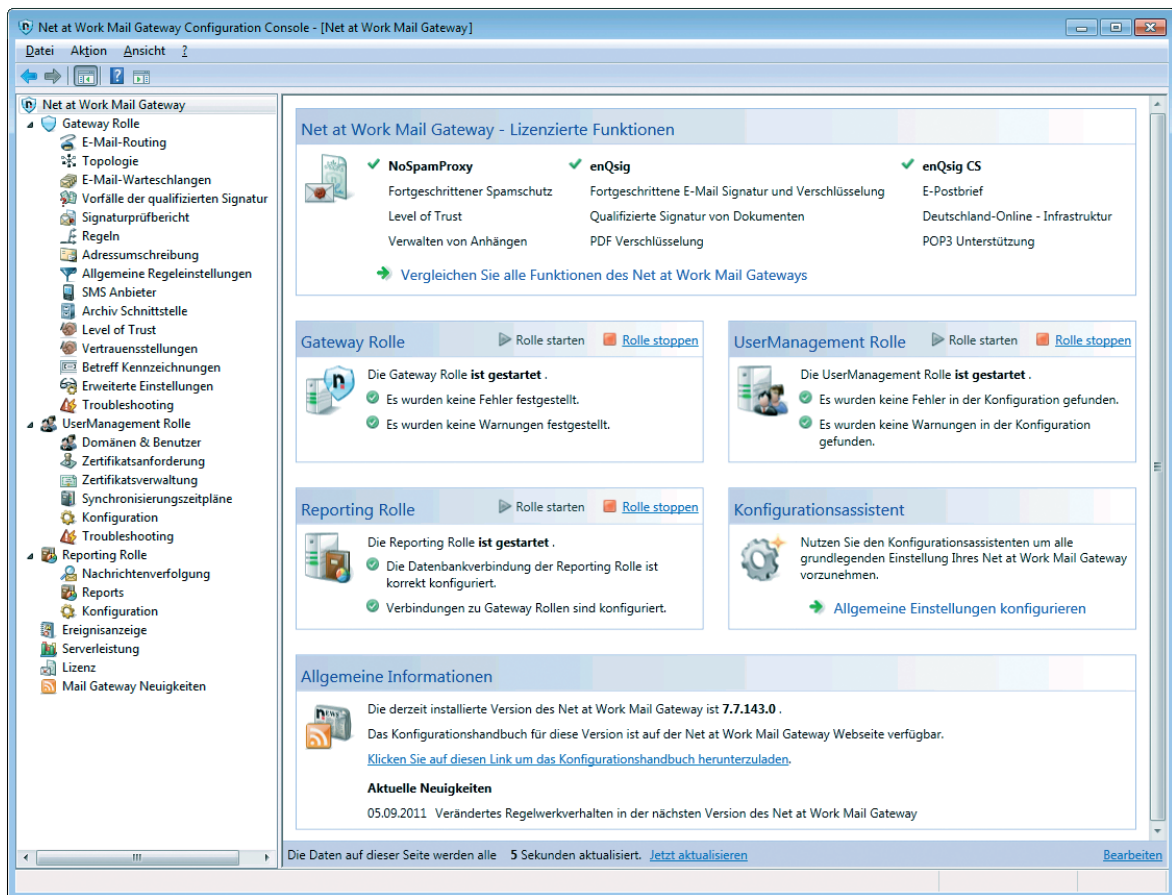
Für die E-Mail-Verschlüsselung nach dem S/MIME Verfahren benötigen Anwender und Unternehmen Zertifikate nach dem X.509 Standard. enQsig zentralisiert und automatisiert die Verwaltung dieser Zertifikate. Anwender sind von den Verwaltungsaufgaben vollständig entlastet und Administratoren profitieren von einer Vielzahl hilfreicher Managementfunktionen.

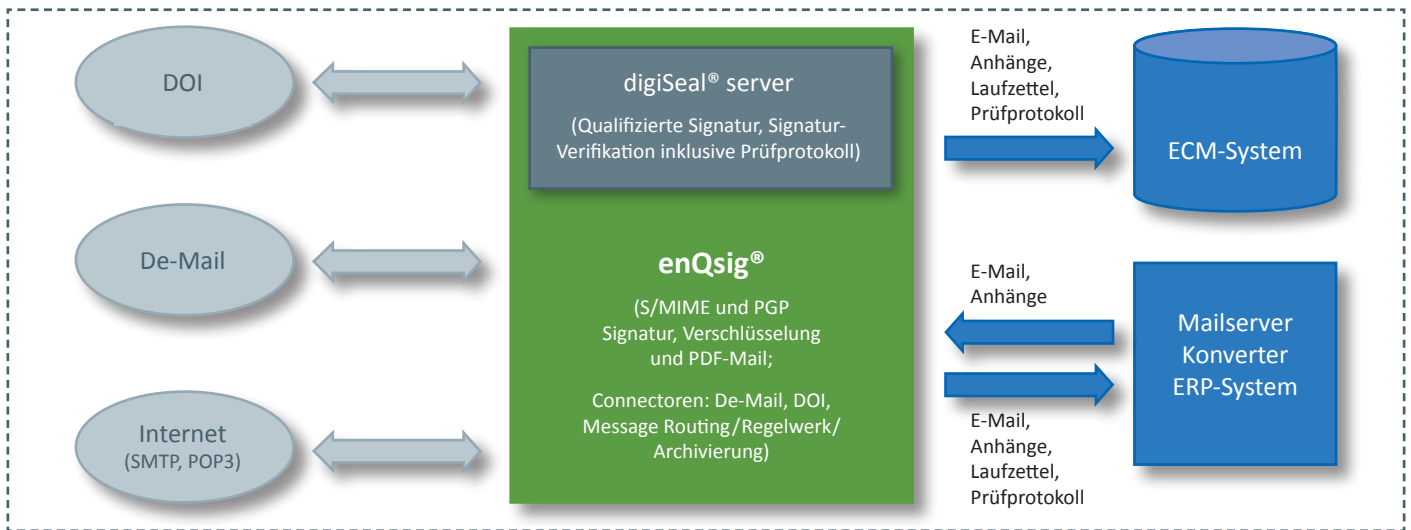
Das Zertifikatsmanagement unterstützt Benutzer- und Domain-Zertifikate beliebiger Trustcenter und importiert öffentliche Schlüssel automatisiert aus eingehenden E-Mail-Signaturen. Für die einfache und schnelle Verteilung von Benutzerzertifikaten ist enQsig mit dem Trustcenter der Deutschen Post SIGNTRUST direkt integriert. Diese sichere Schnittstelle zwischen dem Mail-Gateway und SIGNTRUST führt zu einer erheblichen Erleichterung hinsichtlich des administrativen Arbeitsaufwands und stellt somit eine echte Kosteneinsparung für das Unternehmen dar.

PDF-Mail – Passwort-basiert sicher kommunizieren

Auch wenn die E-Mail-Verschlüsselung auf Basis von Internet-Standards wie S/MIME und PGP die besten Technologien sind, gibt es Situationen bei denen die notwendige Infrastruktur nicht hergestellt werden kann. enQsig bietet mit der automatisierten PDF-Verschlüsselung für E-Mails und Dateianhänge ein passendes Verfahren.

Anwender können enQsig anweisen, die E-Mail mit allen Anhängen in ein PDF zu wandeln und mit einem vorgegebenen Passwort zu verschlüsseln. Das Passwort kann dem Empfänger von enQsig automatisiert per SMS zugesandt oder auf anderem Wege übermittelt werden. PDF-Mail ist vor allem für Unternehmen interessant, die personenbezogene Daten versenden, wie z.B. Versicherungen, Banken, Rechtsanwälte oder Steuerberater.





Komplettlösung für Virtuelle Poststelle und DOI

Im öffentlichen Bereich stellt enQsig die Grundlage für die Implementierung einer Virtuellen Poststelle dar. Die Funktionen für E-Mail-Verschlüsselung bieten hierbei die Basis. Darüber hinaus erfüllt das Produkt aber auch alle weiteren Anforderungen an eine Virtuelle Poststelle. Für alle eingehenden E-Mails kann enQsig einen Signaturprüfbericht („Laufzettel“) erstellen. Alle E-Mails und signierten Dateien können an ein internes Archivsystem übergeben werden.

Im Aktionsplan Deutschland-Online haben die Regierungschefs des Bundes und der Länder entschieden, dass eine abgestimmte Kommunikationsinfrastruktur der Deutschen Verwaltung auf- und ausgebaut wird. Teil dieser neuen Infrastruktur ist ein E-Mail-Routing zwischen Bundes-, Landes- und Kommunalbehörden auf Basis einer zentral durch das DOI-Netz bereitgestellten Routingtabelle. Mit enQsig können Behörden auf eine automatisierte Lösung zur Pflege und Umsetzung dieses Routings zurückgreifen.

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 Dokumentenversand 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.

Vollständige Journal-Archivierung für E-Mail und Dokumente

enQsig bietet eine einheitliche Konfiguration der Funktionen zur E-Mail-Archivierung. Damit kann am Gateway eine vollständige Journal-Archivierung erreicht werden. Im Journal-Archiv werden alle ein- und ausgehenden Nachrichten gespeichert und sind so für Auskünfte und als Beweisgrundlage auch noch nach Jahren verfügbar. Als Speicherlösung stehen neben dem Dateisystem die Archivalschnittstellen zu bekannten ECM-Systemen zur Verfügung.

Mehrwert 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 Lizenzerweiterung 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 (32 Bit und 64 Bit). Die mit * gekennzeichneten Features erfordern Windows Server 2008 oder neuer.
- NET Framework 4.0
- Microsoft SQL Server, SQL Express Edition
- Microsoft Report Viewer 2008 SP1

Funktionsübersicht:

Schlüssel-basierte Verfahren: S/MIME, PGP

- Signatur und Verschlüsselung
- Signaturprüfung eingehend, Ablehnen möglich
- Signatur entfernen, optional
- Signaturprüfbericht (Text, OSCI konform)
- Hashverfahren S/MIME: MD5, SHA1, SHA256*, SHA512*
- Verschlüsselungsverfahren S/MIME: DES, RC2 (40-128 Bit), TripleDES, AES (128, 192, 256 Bit)*
- Hashverfahren PGP: MD5, SHA1, SHA256, SHA384, SHA512, RipeMD-160
- Verschlüsselungsverfahren PGP: TrippleDES, AES (128, 192, 256 Bit), Blowfish, Idea, Twofish-256, Cast-5

Passwort-basiertes Verfahren: PDF-Mail

- E-Mail inklusive Anhängen in PDF wandeln
- PDF-Mail mit Passwort verschlüsseln
- PDF-Nutzungsmöglichkeiten zentral einschränken
- Passwort als SMS versenden, Passwort-Generator
- steuerbar über Betreffzeile, X-Header, Outlook-Plugin oder zentrale Regeln

Zertifikatsverwaltung

- Sammeln eingehender S/MIME-Zertifikate
- Unterstützung Personen- und Domain-Zertifikate
- Automatisierte Zertifikats-Beschaffung mit SIGNTRUST
- Generieren von PGP-Schlüsselpaaren

Regelsystem

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

Connectoren

- DOI – Automatisiertes Routing in das DOI-Netz
- E-Post – Unterstützung mehrerer Absender-Domains
- POP3 – E-Mail-Abruf aus Sammelpostfächern
- SMTP – regelbasiertes Routing über mehrere Connectoren, domain- und userbasiert inklusive TLS

Qualifizierte elektronische Signatur

- Signieren, Verifizieren
- Prüfprotokoll erstellen (und an Mail anhängen)

Jobsteuerung

- Management temporär fehlgeschlagener qualifizierter Signatur-Aufträge

Archivschnittstelle

- Übergabe der Mail sowie aller Anhänge u. Protokolle via Dateischnittstelle an Archiv-, DMS- u. Workflow-Systeme

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