



Vertrauen, Datenschutz und Rechtssicherheit mit einer Lösung

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

PDF Mail – passwortbasiert sicher kommunizieren.

De-Mail Gateway – zentraler Zugang und rechtsverbindliche Kommunikation.

enQsig® sichert als zentrales Gateway die Vertraulichkeit der E-Mail-Kommunikation mit Unternehmen, Behörden, Verbrauchern und Bürgern durch E-Mail-Verschlüsselung. Das Gateway ermöglicht effiziente Geschäftsprozesse durch De-Mail-Anbindung und gesetzeskonforme elektronische Signatur.

Durch das zentrale Signieren und Verschlüsseln von E-Mails am enQsig Mail Gateway kommunizieren Sie sicher mit Partnern. enQsig setzt über ein zentrales Regelwerk die Sicherheitsricht-

linien des Unternehmens für die E-Mail-Verschlüsselung durch. 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 Weiterverarbeitung 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 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.

enQsig unterstützt die sichere und datenschutzkonforme 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 diese Signatur 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 das passwortbasierte Verfahren PDF Mail an. Mit der Nutzung 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.

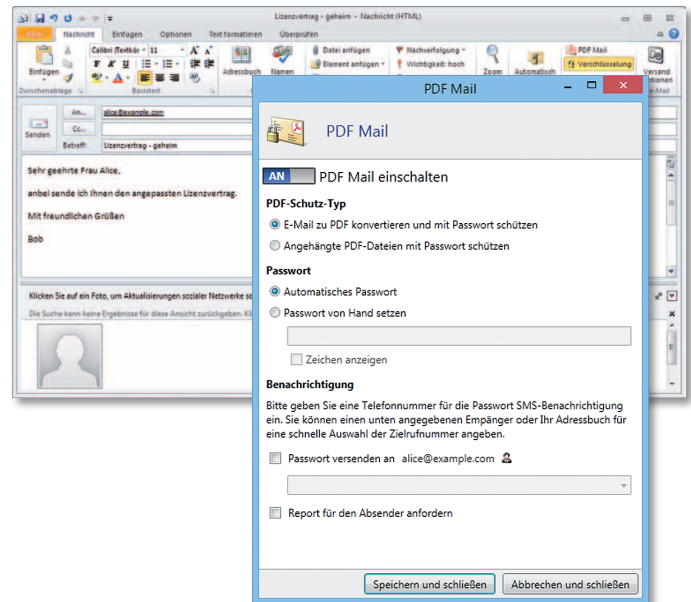
All dem begegnet enQsig durch zentrale Funktionen an der Schnittstelle zwischen Internet und lokalem Netzwerk. Die für Verschlüsselung und Entschlüsselung benötigten Zertifikate werden zentral verwaltet; die durch das Gateway entschlüsselten E-Mails können auf Spam und Viren geprüft und intern weitergeleitet werden. Ein flexibles Regelwerk erlaubt die zentrale Definition, welche E-Mails mit welchen Verfahren verschlüsselt werden.



Datenblatt

PDF Mail: passwortbasiert sicher kommunizieren

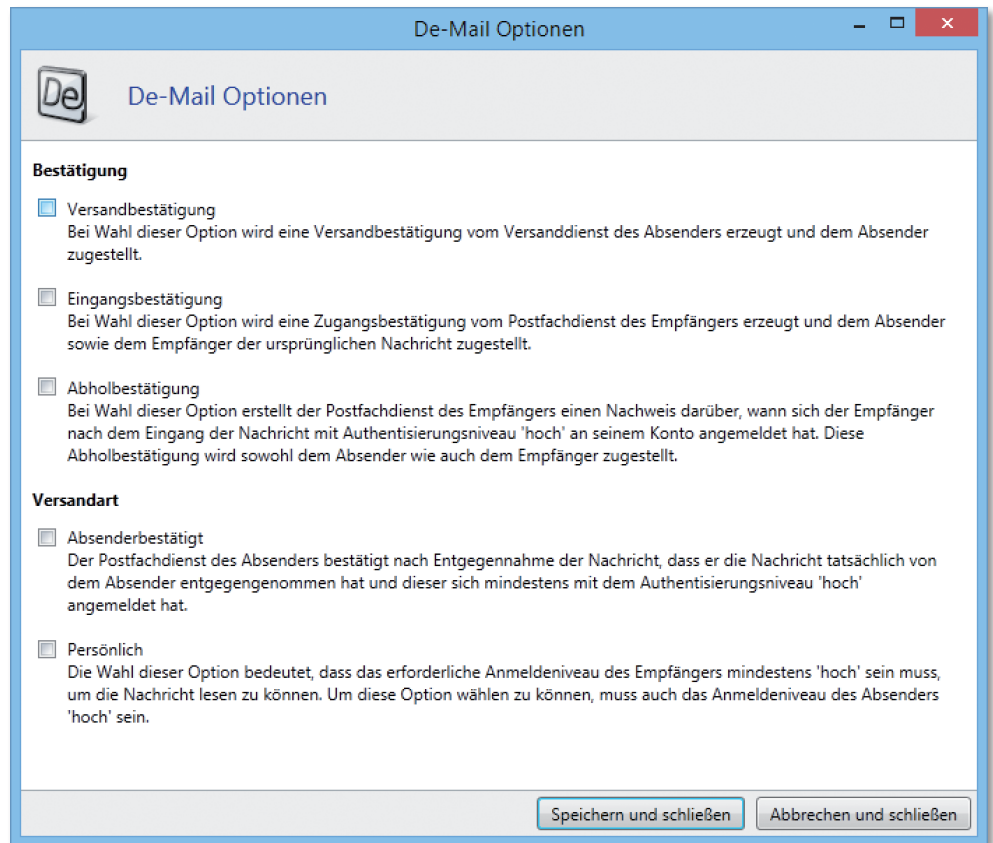
E-Mail-Verschlüsselung auf Basis von Internetstandards wie S/MIME und PGP ist die sicherste Methode. Allerdings unterstützen viele Kommunikationspartner diese nicht. enQsig bietet mit der automatisierten PDF-Verschlüsselung für E-Mails und Dateianhänge ein passendes Verfahren. Anwender können enQsig anweisen, die E-Mail mit allen Anhängen in 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.



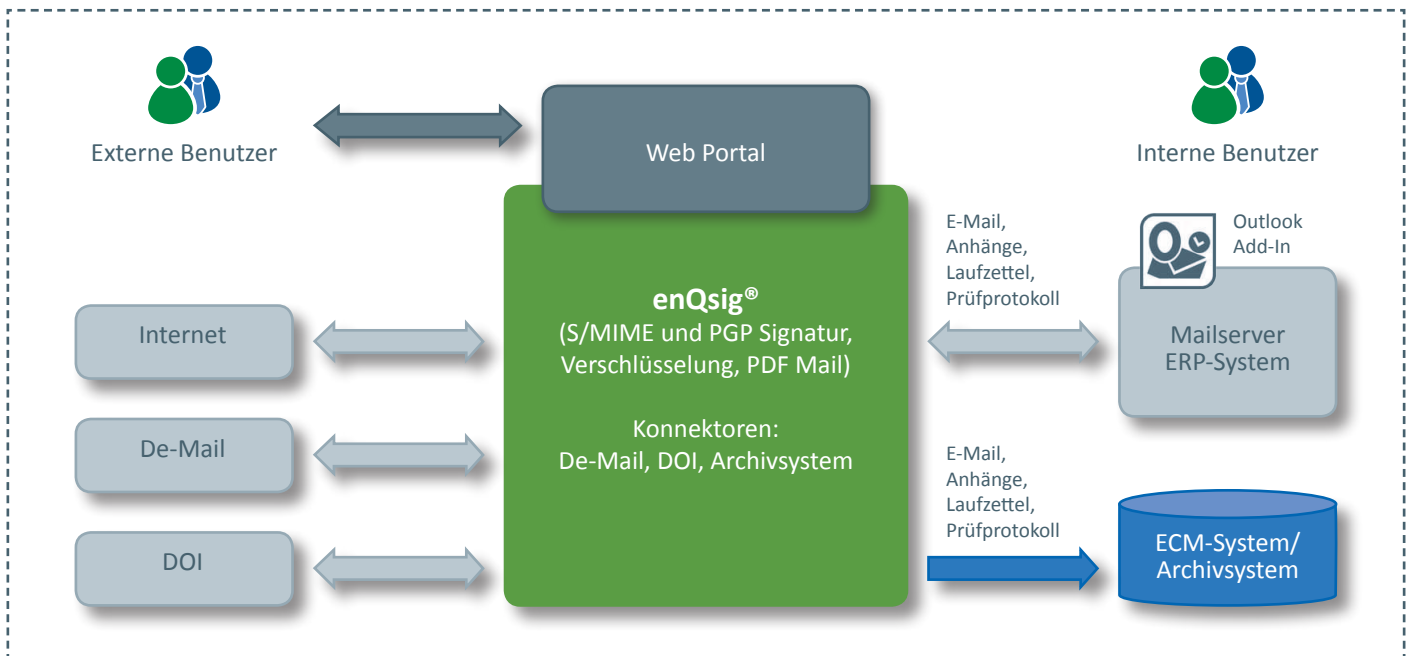
PDF Mail Optionen des Outlook Add-Ins

De-Mail Anbindung mit enQsig: zentral & flexibel

Der De-Mail-Konnektor von enQsig® ermöglicht Unternehmen und Behörden den sicheren und zentralen Zugang zum De-Mail-System. De-Mails können somit direkt aus den internen Mailsystemen versandt und dort empfangen werden. enQsig CS verfügt über Schnittstellen für die Integration von Fachverfahren, ECM- und E-Mail-Systemen. enQsig bietet die Grundlage für Kostensenkungen im Briefverkehr mit Kunden und Bürgern. Durch die Umstellung auf das rechtssichere elektronische System De-Mail können Geschäftsprozesse ohne Medienbruch elektronisch effizient umgesetzt werden. Der De-Mail-Konnektor ist Teil von enQsig und wird als Produktvariante enQsig CS auch separat angeboten.



De-Mail-Optionen des Outlook Add-Ins



Outlook Add-In: Flexibilität für den Anwender

Neben dem zentralen Gateway liefert enQsig ein Outlook Add-In, welches die komfortable Steuerung von Verschlüsselungsfunktionen in der E-Mail-Anwendung erlaubt. Das Add-In ermöglicht Benutzern, Einstellungen für die E-Mail-Verschlüsselung und PDF Mail vorzunehmen und unterstützt darüber hinaus die besonderen Funktionen von De-Mail. Für eine zentrale Verwaltung des Outlook Add-Ins durch Administratoren wird ein Template für Gruppenrichtlinien mitgeliefert.

Zertifikats- und PGP-Management: 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 Domänenzertifikate beliebiger Trustcenter und importiert

öffentliche Schlüssel automatisiert aus eingehenden E-Mail-Signaturen. Für die einfache und schnelle Verteilung von Benutzerzertifikaten hat enQsig eine Schnittstelle für das Trustcenter der Deutschen Post Signtrust integriert. Diese ist eine Erleichterung bei der Administration und ist dadurch eine echte Kosteneinsparung für das Unternehmen. Darüber hinaus können PGP-Schlüssel in enQsig generiert, importiert und verwaltet werden.

Mehrwert durch Anti-Virus

Der integrierte Commtouch-Service enthält neben einer Echtzeit Spam- und Virenerkennung auch die vielfach ausgezeichnete Commtouch Anti-Virus Scan-Engine. Commtouch Anti-Virus bietet effiziente Viren-Erkennung bei geringem Ressourcenbedarf und blockt jede Art von Malware, wie Würmer, Trojaner und Spyware. Die Anti-Virus-Funktion verwendet eine Multi-Layer-, Multi-Engine-Erkennung, die auf Heuristik, Emulation und Signaturen basiert. Das herkömmliche Recurrent Pattern Detection Verfahren (RPD) wird darüber hinaus zusätzlich eingesetzt. So können Viren auch unabhängig vom Verbreitungsgrad sicher erkannt und abgewehrt werden.

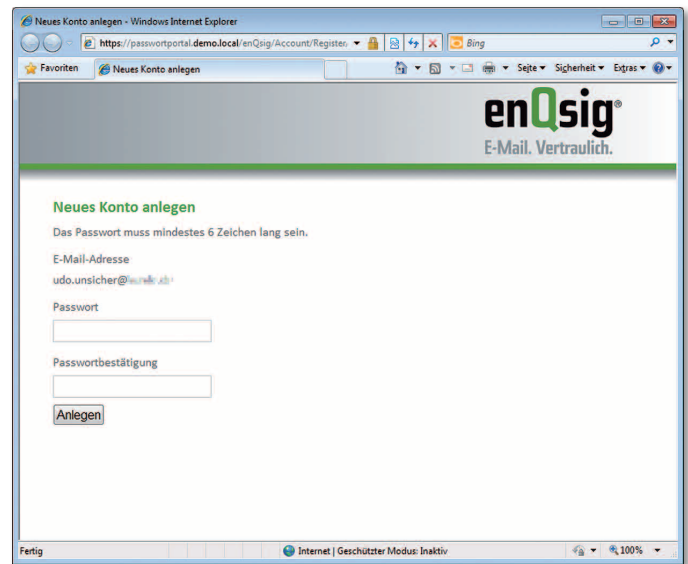


Web Portal: Sichere E-Mail-Kommunikation ohne Zertifikat

enQsig bietet die verschlüsselte E-Mail-Kommunikation mit Partnern ohne besondere Voraussetzungen. Das enQsig Web Portal erweitert das passwortbasierte Verfahren PDF Mail durch seine Self-Service-Funktionen und eine sichere Antwortfunktion.

Das Gateway ermittelt je nach Empfänger die beste Verschlüsselungstechnologie aus S/MIME, PGP oder PDF Mail. Ist für einen Empfänger noch keine Technologie festgelegt, bittet enQsig um die Zusendung eines Zertifikats oder um die Hinterlegung eines Passwortes als Grundlage für PDF Mail. Der Einsatz des Web Portals ermöglicht es dem Empfänger einer PDF Mail, sich auf dem Web Portal des Absenders selber ein Passwort zu vergeben. Dies erleichtert den Umgang mit den verwendeten Passwörtern erheblich und trägt zudem zur höheren Sicherheit bei. Darüber hinaus kann der Empfänger einer PDF Mail mit Hilfe des Web Portals auf diese antworten. Dadurch wird eine gesicherte E-Mail-Kommunikation in beide Richtungen möglich.

enQsig Anwender können sich auf den Datenschutz verlassen, denn E-Mails werden garantiert verschlüsselt.



Dialog zum Hinterlegen eines Passworts

Systemvoraussetzungen:

enQsig

- Windows Server 2003 SP2 oder höher
- .NET Framework 4.0 oder höher
- Microsoft SQL Server 2005 oder höher, SQL Express Edition 2005 oder höher
- Microsoft Report Viewer 2010



enQsig Web Portal

- Windows Server 2008 R2 oder höher mit installiertem IIS
- .NET Framework 4.0
- Express Edition 2008 oder höher, SQL Express Edition 2008 oder höher