



# Mail-Verschlüsselung ohne Zertifikat

Mail-Management und Sicherheit. Schnell, simpel und günstig mit Instant Encryption.

**Schnell** – „Up and Running“ in 30 Minuten

**Simpel** - Für Absender und Empfänger, online, offline, auf dem Smartphone oder iPad

**Günstig** - Zu einem Bruchteil der Kosten einer zertifikatsbasierten Verschlüsselungslösung

## Anwender erwarten von der IT, dass sie sicher und unkompliziert über das Medium E-Mail kommunizieren können.

Die Anforderungen der Anwender an das Medium E-Mail sind unterschiedlich. Die Personalabteilung oder der Betriebsrat müssen sensible Dokumente beim E-Mail-Versand schützen und der Vorstand möchte Datei-Anhänge nur verschlüsselt versenden.

In der Praxis bedeutet die Implementierung einer Secure-Messaging-Lösung in der Regel hohe Kosten, zusätzlichen Aufwand für die tägliche Administration und umständliche Wege für E-Mail-Empfänger und Anwender. Die klassischen Wege (S/MIME und PGP) sind in der Einführung und beim laufenden Betrieb teuer und aufwändig. Alternative Web-Abruf-Lösungen sind oft umständlich zu bedienen oder schränken die Möglichkeiten für Empfänger ein (z.B. aus Sicherheitsgründen sind https-Verbindungen deaktiviert).

Lokal installierte Lösungen sind wartungsaufwändig und mögliche Fehlbedienung oder umständliche Handhabung sind für die Anwender ebenfalls problematisch.

**Ob Datenschutzvorgaben, die Notwendigkeit vertraulicher Kommunikation, oder der Schutz vor Manipulation: Die Instant Encryption Technologie powered by MailProtect ist eine Lösung, die sowohl Anwender als auch Administratoren zufrieden stellt:**

- ☐ ohne langwieriges Public-Key-Infrastruktur (PKI) Projekt
- ☐ ohne jede Software-Installation auf den Clients
- ☐ ohne Anwenderschulung oder Help-Desk-Anfragen
- ☐ ohne laufenden Administrationsaufwand
- ☐ ohne einen Hosting-Dienstleister dazwischen

## Wie funktioniert Instant Encryption?

### E-Mail-Versand

Die neue Generation der passwortbasierten Verschlüsselungslösung der BCC nutzt wahlweise PDF oder ZIP Formate. Im Standardfall werden E-Mail-Text und Dokumenten-Anhänge in ausgehenden E-Mails serverseitig konvertiert und als verschlüsselte passwortgesicherte PDF-Datei mit ggf. eingebetteten Dateianhängen versendet. Der Administrator kann

entsprechend dem Bedarf vorab definieren, wie die Verschlüsselungsfunktion genutzt werden soll. Weitere Varianten, wie die Verwendung von 256-Bit verschlüsselten ZIP-Archiven, zur Langzeitarchivierung empfohlenes Format PDF/A oder mit Windows Compressed Folders kompatibel DES 40-Bit Verschlüsselung sind ebenfalls möglich.



### Passwort-Verteilung

Das zum Lesen erforderliche Passwort wird automatisch zufällig generiert und dem Empfänger separat übermittelt, wie z.B. per E-Mail als „Inline Image“, SMS oder Fax. Das Passwort kann auch dem Absender zugestellt werden, wenn er das Passwort telefonisch übermitteln soll. Je nach Konfiguration kann ein Dauerpasswort für den jeweiligen Empfänger oder

Passwörter für jede einzelne E-Mail generiert werden. Das Passwort-Management ist vom Administrator konfigurierbar und weitestgehend automatisiert. So kann ein vergessenes Passwort per E-Mail-Link vom Empfänger angefordert werden und wird automatisch vom Server zugestellt.

