Z1 SecureMail End2End

Höchste Sicherheit beim Wirtschaftsschutz durch Ende-zu-Ende-Verschlüsselung und -Signatur

Wann ist Ende-zu-Ende-Verschlüsselung notwendig?

Für Unternehmen wird Ende-zu-Ende E-Mail-Verschlüsselung wichtig, wenn Smartphones und Notebooks für geschäftliche E-Mails genutzt werden. Auch unternehmensinterne E-Mails werden von mobilen Endgeräten über Mobilfunkstrecken oder öffentliches WLAN im Klartext gesendet. Dort können sie einfach abgefangen und mitgelesen oder manipuliert werden.

Ein weiterer Sicherheitsaspekt ist die unverschlüsselte Ablage von E-Mails auf E-Mail-Servern. Das gilt insbesondere beim Einsatz von Cloud-Diensten wie Office 365. Wer nicht möchte, dass Geheimdienste oder Administratoren die dort gespeicherten E-Mails mitlesen, muss auch auf internen Teilstrecken verschlüsseln. Nicht zuletzt verhindert richtig angewendete Ende-zu-Ende-Verschlüsselung Datenleaks, wenn Endgeräte verloren gehen.

Qualitätssiegel für Sicherheit

Zertificon ist offizieller Träger des TeleTrusT Qualitätssiegels „SecurITy made in Germany“.

SecurITy made in Germany

Warum Ende-zu-Ende-Verschlüsselung Unternehmen vor besondere Herausforderung stellt

Ende-zu-Ende-Verschlüsselung bezeichnet die lückenlose Verschlüsselung der Inhalte vom Sendegerät bis zum Empfangsgerät. Nur Sender und Empfänger sind im Besitz der passenden Schlüssel. Diese Technologie, die im Privatbereich gut funktioniert, ist für den flächendeckenden Einsatz in Unternehmen leider wenig geeignet.

Ende-zu-Ende-Verschlüsselung bedeutet für Unternehmen:

Das Unternehmen hat **keine Datenhoheit über ende-zu-ende-verschlüsselte E-Mails.** Nur der Mitarbeiter hat darauf Zugriff.

- Eingeschränkte Einsatzmöglichkeit, denn Sender und Empfänger benötigen die gleiche Verschlüsselungstechnologie
- Aufwändiges Schlüssel- / Zertifikatsmanagement auf jedem Endgerät mit hohem Fehlerpotenzial
- Hoher Administrations- und Wartungsaufwand und damit nicht skalierbar
- Verantwortung für Verschlüsselung beim einzelnen Benutzer
- Nicht zentral auditierbar, daher nicht revisionssicher
- Kein Zugriff für zentrale Contentfilter = hohe Risiken ohne Kontrollmöglichkeit

Die Lösung: Ende-zu-Ende-Verschlüsselung für Unternehmen mit *Organizational End2End*

E-Mails werden auf den Endgeräten der Mitarbeiter ver- und entschlüsselt. Das Unternehmen erhält an sicherer Stelle Zugriff und verschlüsselt anschließend erneut. Diese Form der ende-zu-ende abgesicherten Kommunikation ermöglicht:

- **Die Wahrnehmung der unternehmerischen Kontrollpflichten, z.B. über Contentfilter (Antivirus, Antispam, DLP etc.)**
- **Die Herstellung der Revisionssicherheit und Auditfähigkeit sowie die Durchsetzung der Compliance-Vorgaben**
- **Den wirtschaftlichen, spontanen, hochsicheren E-Mail-Austausch in jedem Verschlüsselungsformat**

Organizational End2End kombiniert Z1 SecureMail End2End & Z1 SecureMail Gateway – unternehmenstaugliche Ende-zu-Ende-Verschlüsselung mit Umverschlüsselung

Organizational End2End ist eine clevere Kombination aus policy-basierter, client- und serverseitiger Verschlüsselung. Die komplexen Prozesse laufen automatisch im Hintergrund. Dem User wird das aufwendige, fehleranfällige Zertifikatsmanagement komplett abgenommen.

Intern wird ausschließlich homogen per S/MIME verschlüsselt. Da S/MIME von den Standard-E-Mail-Programmen unterstützt wird, sind Administration und Wartung sehr effizient.

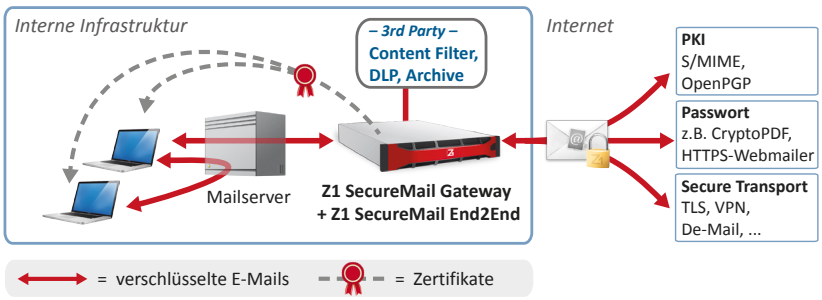

*Abb.1: Bei **Organizational End2End** werden E-Mails am Gateway umverschlüsselt.*

Von und nach extern wird mit dem bewährten Z1 SecureMail Gateway nach Bedarf mit verschiedenen Technologien verschlüsselt. Von S/MIME und OpenPGP bis zu passwortverschlüsselten PDFs oder SecureChannel (TLS, De-Mail, …) sind der sicheren E-Mail keine Grenzen gesetzt (siehe Abb. 1). Entscheidend ist, was die Gegenstelle benutzt. Das Gateway stellt sich flexibel darauf ein. Während der Umverschlüsselung auf dem Z1 SecureMail Gateway können **Contentfilter** wie Archive, Data Loss Prevention sowie Antivirus- und Antispam-Programme auf alle E-Mails zugreifen. *Organizational End2End* ermöglicht Ihnen jederzeit einen hochsicheren E-Mail-Austausch: compliant, effizient, wirtschaftlich – ohne Einschränkungen beim Empfängerkreis.

Personal End2End – komfortabel durchgehend verschlüsseln im Hochsicherheitsbereich

Bei *Personal End2End* werden E-Mails nicht umverschlüsselt; die Verschlüsselung bleibt dabei auf den S/MIME-Standard beschränkt. Diese Form der Ende-zu-Ende-Verschlüsselung ist nur für einzelne, besonders sicherheitssensible E-Mails empfohlen, beispielsweise auf Vorstandsebene. Z1 SecureMail End2End übernimmt dabei das Zertifikatsmanagement inklusive Beschaffung und Validierung aller Zertifikate. Damit ist auch die *Personal End2End*-Verschlüsselung sehr effizient einsetzbar. Der Verschlüsselungsstatus aller E-Mails ist durch Log-Dateien nachweisbar und eine Auditfähigkeit damit gegeben. Allerdings können mit *Personal End2End* keine zentralen Contentfilter genutzt werden.

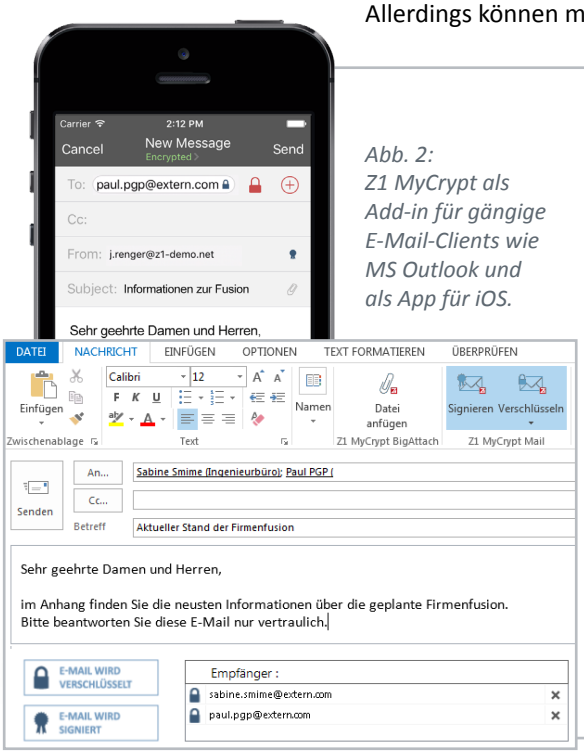

Abb. 2: Z1 MyCrypt als Add-in für gängige E-Mail-Clients wie MS Outlook und als App für iOS.

Am Endgerät mit Bordmittel verschlüsseln …

Die Anbindung mittels ActiveSync- und LDAP-Proxies erlaubt den Einsatz von Z1 SecureMail End2End mit allen Standard E-Mail-Programmen. Ihre Mitarbeiter brauchen sich nicht umgewöhnen, müssen jedoch Verschlüsselung und Signatur aktiv ansteuern. Die zentralen Policies können jedoch ohne App oder Plug-in je nach Plattform nur eingeschränkt oder gar nicht abgerufen werden.

… oder Z1 MyCrypt als App oder Plug-in nutzen

Die Apps (siehe Abb. 2) erlauben eine sehr komfortable Nutzersteuerung und übernehmen das aufwändige und komplexe Zertifikatsmanagement.

Zusätzlich bietet Z1 MyCrypt hochintegrierte Funktionen: Der Nutzer kann sich beispielsweise mit Eingabe einer Empfängeradresse alle Details über konfigurierte Policies und Sicherheitslevel anzeigen lassen. Compliance-Vorgaben können mit Z1 MyCrypt in der Regel problemlos unternehmensweit durchgesetzt werden.

Z1 SecureMail End2End kann parallel zu gängigen Mobile Device Management-Lösungen eingesetzt werden.

Zertificon Solutions GmbH
Berlin, Germany
www.zertificon.com

Tel.: +49 (0)30 5900300-0
E-Mail: sales@zertificon.com
www.globaltrustpoint.com