Infoblatt DATEV E-Mail-Verschlüsselung

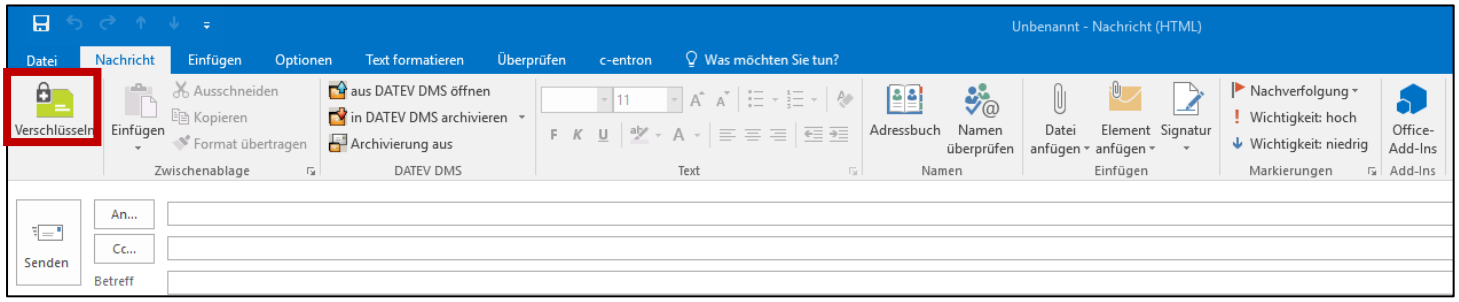
Grundsätzlich dient die DATEV E-Mail Verschlüsselung dem sicheren Versand von E-Mails an jeden Empfänger. Das Installieren von Software ist dazu nicht notwendig. Alle E-Mails werden zentral ver- und entschlüsselt und automatisch auf Viren und Trojaner geprüft. Als Absender wird weiterhin der tatsächliche Absender angezeigt, der Inhalt wird allerdings durch ein von der DATEV vorgefertigten Text ersetzt. Im Anhang der E-Mail erhält der Empfänger eine Datei, über die er zum DATEV E-Mail Verschlüsselungsportal gelangt. Dort kann die eigentliche E-Mail gelesen, sicher beantwortet und z.B. in Outlook exportiert werden.

Erstmalige Nutzung seitens des Empfängers

Haben Sie als Empfänger zum ersten Mal eine verschlüsselte E-Mail erhalten, öffnen Sie bitte die Datei im Anhang. Im DATEV E-Mail Verschlüsselungsportal müssen Sie nun ein Kennwort vergeben. Anschließend werden Sie direkt in das Portal eingeloggt und können die erhaltene E-Mail abrufen. Zukünftig können Sie sich als Empfänger einfach in das Verschlüsselungsportal einloggen und dort nach der Eingabe des persönlichen Kennworts die E-Mails entschlüsseln. Sind die Sicherheitsfrage oder das Kennwort nicht mehr bekannt, kann nur die DATEV dieses zurücksetzen. Bitte wenden Sie sich in diesem Fall daher an postmaster@datev.de.

Wie wird verschlüsselt?

Grundsätzlich wird eine E-Mail über ein Outlook Add-In verschlüsselt. Das Klicken des dargestellen Buttons erzeugt beim Versand das Voranstellen der Zeichenkette [confidential] im Betreff. Durch dieses Merkmal erkennt der DATEVnet E-Mail Server, dass die E-Mail verschlüsselt an den Empfänger verschickt werden soll. Auf dem Smartphone kann das Verschlüsseln durch das Voranstellen von {gesichert} im Betreff aktiviert werden.



Das Outlook Add-In kann in verschiedenen Modi installiert werden.

1. Outlook Add-In ist standardmäßig eingedrückt → E-Mail wird standardmäßig verschlüsselt verschickt (Button kann manuell deaktiviert werden)
2. Outlook Add-In ist standardmäßig nicht eingedrückt → E-Mail wird standardmäßig unverschlüsselt verschickt (Button kann manuell aktiviert werden)

Zusätzlich kann eingestellt werden, dass der Benutzer einen Warnhinweis erhält, sobald die E-Mail unverschlüsselt verschickt wird.

geiger BDT GmbH

Heinz-Fröling-Str. 15 I 51429 Bergisch Gladbach (Köln)
T +49 (0) 2204 76 79 7-0 I F +49 (0) 2204 76 79 7-270
geiger@geiger-bdt.de I www.geiger-bdt.de

Weitere Hinweise

Der Empfänger kann sein bereits vorhandenes SMINE- oder PGP Zertifikat in das Verschlüsselungsportal hochladen. Alternativ dazu kann der Empfänger eine signierte E-Mail an schluesselimport@datev.de schicken. Erkennt die DATEV, dass dem Empfänger ein SMINE- oder PGP Zertifikat zugeordnet ist, wird die E-Mail automatisch mit allen Zertifikaten verschlüsselt. Dadurch werden die eingehenden E-Mails automatisch verschlüsselt.

Nutzer der DATEV E-Mail Verschlüsselung können eingehende E-Mails automatisch entschlüsseln lassen
Für die Smartcard, die in der DATEVnet Administration zur E-Mail Verschlüsselung genutzt wird, muss das Zertifikat online bei DATEV zur Verfügung gestellt sein. Kontrolliert werden kann dies über die Website: http://www.datev.de/emailschluessel. Falls das SmartCard Zertifikat dort nicht auftaucht, müssen Sie es über das PDF Dokument aus dem Info Dokument 1071175 freigeben. Falls das Zertifikat freigegeben ist, werden eingehende verschlüsselte E-Mails durch DATEV automatisch entschlüsselt und unverschlüsselt zugestellt.

Häufige Fehler bei der Nutzung der DATEV E-Mail-Verschlüsselung:

1. Der Empfänger besitzt eine SmartCard, nutzt diese jedoch nicht. Auf der SmartCard ist die E-Mail-Adresse hinterlegt und die Zertifikate wurden freigegeben. Der Empfänger erhält die E-Mails nun automatisch SMINE verschlüsselt und muss zur Entschlüsselung die SmartCard einstecken. Als Empfänger kann anstatt der Verschlüsselung mit dem Outlook Add-In oder dem Voranstellen von [confidential] der Befehl {priv} genutzt werden. Nun wird die E-Mail via Portal Link verschlüsselt. Dort kann der Empfänger dann auch das entsprechende Zertifikat deaktivieren, so dass zukünftige E-Mails via Portal Link eingehen.

2. Der Empfänger nutzt die PGP Verschlüsselung. Wichtig: Die DATEV kann nur PGP verschlüsselte E-Mails verschicken, jedoch PGP verschlüsselte empfangende E-Mails nicht entschlüsseln.

3. Sie haben vor der DATEV E-Mail Verschlüsselung die SMINE Verschlüsselung über die SmartCard genutzt. Dies muss in Outlook deaktiviert werden. Beim Versand von E-Mails muss der Haken „Verschlüsseln" unter dem Reiter „Optionen" deaktiviert werden. Falls sich das SMINE Zertifikat Ihrer SmartCard geändert hat und sie zukünftig weiterhin via SMINE verschlüsseln wollen, geben Sie bitte Ihre Zertifikate frei und teilen Sie dem Empfänger mit, dass die neuen Zertifikate von der o.g. Website importiert werden müssen.

Weitere Informationen rund um die DATEV E-Mail-Verschlüsselung finden Sie auf

www.geiger-bdt.de/leistungen/spezialwissen/datev-e-mail-verschluesselung
www.datev.de/info-db → Suchbegriff ‚E-Mail Verschlüsselung'
www.datev.de/info-db/1071723