SPECTRUM

Unabhängiger KANZLEI Systempartner

E-Mail-Verschlüsselungen

Die E-Mail-Verschlüsselungs-Techniken

Verschlüsselung existiert seit Jahrtausenden. Schon der römische Kaiser Julius Cäsar hat sich mit der „Cäsar-Chiffre“ in der Kryptographie-Geschichte verewigt. Er verschob Buchstaben des Alphabets systematisch um drei Positionen: A wurde also zu D, B zu E und so fort. Solche Systeme funktionieren, solange Empfänger den Schlüssel bzw. den Algorithmus (bei Cäsar: 3 Stellen zurück) kennen, nicht aber gegnerische Spione, die die Nachrichten abfangen. Im Lauf der Jahrhunderte wurden solche Substitutions-Chiffren immer ausgefeilter, auch die berühmte Enigma-Maschine der Nationalsozialisten im 2. Weltkrieg nutzte die Technik noch und der U-Boot-Krieg ging für die Deutschen zuende, nachdem die Alliierten den Code geknackt hatten.

In dieser Ausgabe:

Die E-Mail-Verschlüsselungs-Techniken:

Nachfolgend werden die verschiedenen, gängigen E-Mail-Verschlüsselungs-Techniken für den Steuerberatermarkt erklärt:

1. TLS-Transportverschlüsselung

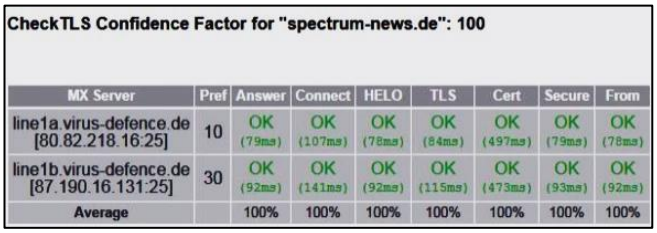
Bei TLS (Transport Layer Security) handelt es sich um ein Protokoll, das Daten über eine verschlüsselte Verbindung im Internet überträgt. TLS ist der Nachfolger des z.B. aus dem eBanking bekannten SSL-Protokolls. TLS-Transport-Verschlüsselung bedeutet, dass der Übertragungskanal zwischen jeweils zwei Mail-Servern (SMTP-Servern) verschlüsselt ist, nicht aber die E-Mails selbst. Wie durch einen sicheren Tunnel (vergleichbar VPN) reisen die E-Mails von einem SMTP-Server zum nächsten bis zum Empfänger. Die während des gesamten Übertragungsprozesses zwischen Mailserver und Client bzw. Internetbrowser verschlüsselte E-Mail bleibt für Schnüffler unlesbar und wird erst wieder in den zugrundeliegenden Klartext umgewandelt, wenn sie beim Adressaten angekommen ist. Auf den E-Mail-Servern und den Rechnern des Absenders und Empfängers liegen die Nachrichten und deren Inhalt jedoch unverschlüsselt vor.

Sicherheitsexperten vergleichen E-Mails gerne mit Postkarten: Sobald sie vom Rechner oder dem Handy aus auf die Reise zum Empfänger gehen, kann sie dazwischen jeder lesen. Das stimmt heutzutage nicht mehr ganz, denn viele Mail-Provider sorgen mittlerweile dafür, dass der Transportweg mit TLS-Verschlüsselung gegen Lauschangriffe gesichert ist.

Die Bundessteuerberaterkammer schreibt in ihrem neuesten Papier von April 2019:

„Die Transport-Verschlüsselung ist grundsätzlich eine Punkt-zu-Punkt-Verschlüsselung, die man sich wie einen Briefumschlag vorstellen kann. Der Inhalt wird bei der Übermittlung zwischen dem Absender und seinem E-Mail-Anbieter sowie zwischen zwei E-Mail-Anbietern untereinander und zwischen E-Mail-Anbieter und Empfänger verschlüsselt bzw. durch einen Briefumschlag geschützt. Allerdings wird die E-Mail beim E-Mailanbieter entschlüsselt, z. B. zur Prüfung (Spam, Viren). Dies ist insoweit unproblematisch, da für E-Mail-Anbieter in Deutschland das Fernmeldegeheimnis nach § 88 TKG gilt. Zusammenfassend bedeutet es, dass die Mails auf dem Internetweg geschützt sind – lediglich auf den Client-Rechnern und den E-Mail-Servern liegen sie unverschlüsselt vor“.

Man kann mit dem Tool www.checktls.com oder www.MXtoolbox.com schnell testen, ob eine E-Mail-Adresse oder eine Domain sauber für den TLS-Betrieb konfiguriert ist. Ein sauberes Check-Ergebnis müsste wie hier aussehen:



CheckTLS Confidence Factor for "spectrum-news.de": 100

MX Server	Pref	Answer	Connect	HELO	TLS	Cert	Secure	From
line1a.virus-defence.de [80.82.218.16:25]	10	OK (79ms)	OK (107ms)	OK (78ms)	OK (84ms)	OK (497ms)	OK (79ms)	OK (78ms)
line1b.virus-defence.de [87.190.16.131:25]	30	OK (92ms)	OK (141ms)	OK (92ms)	OK (115ms)	OK (473ms)	OK (93ms)	OK (92ms)
Average		100%	100%	100%	100%	100%	100%	100%

Es gibt aber auch Probleme mit der TLS-Transport-Verschlüsselung:

1. Die Integrität der E-Mail ist nicht gewährleistet, da die E-Mail erst einmal nicht signiert ist. Man kann aber zusätzliche Signaturverfahren neben der TLS-Verschlüsselung einsetzen. Hat man kein Signaturverfahren, könnten Fake-E-Mails nicht erkannt werden und es könnten so Fake-Mails z.B. bei Mandanten landen. Es passiert jedoch sehr selten, dass Cyber-Kriminelle ihre Schadcode-Mails TLS-verschlüsselt zusenden. Die Gefahr einen falschen Adressaten anzuwählen, wird durch eine Signatur leider auch nicht gelöst.

2. Alle marktgängigen SMTP-Server bei Providern versuchen heute (sofern sie richtig konfiguriert sind und TLS unterstützen) E-Mails nach dem TLS-Transportverschlüsselungs-Verfahren zu übertragen. Teilt jedoch der adressierte SMTP-Server des Empfänger-Providers mit, dass er keine TLS-Transportverschlüsselung unterstützt, dann übertragen die meisten Provider-SMTP-Server die E-Mails eben unverschlüsselt, denn sie wollen die E-Mails ja irgendwie loswerden.

Viele deutsche Provider (Telekom, T-Online, 1&1, WEB.DE, GMX, Freenet, Strato usw.) haben sich verpflichtet, E-Mails ausschließlich TLS-verschlüsselt zu übertragen. Ob nun eine Adressaten-E-Mail-Adresse das TLS-Verfahren unterstützt, könnte man z.B. mit solchen Überprüfungsverfahren wie diesen TLS-Check-Tools feststellen. Wenn man jetzt auf beiden Seiten prüft, ob die Server TLS-mäßig richtig konfiguriert sind, kann man *„mit großer Wahrscheinlichkeit“* davon ausgehen, dass auch TLS-verschlüsselt übertragen wird …. aber eine 100%ige Garantie hat man leider nicht. Z.B. könnte der empfangende Mail-Server gerade eine Störung haben oder dessen Zertifikat könnte gerade abgelaufen und noch nicht erneuert worden sein. Dann würde der sendende Mail-Server trotzdem versenden, nur unverschlüsselt – was aber im Verantwortungsbereich des Empfänger liegt.

Zwangs-TLS-Transport-Verschlüsselung von E-Mails bei SPECTRUM-ASP und SPECTRUM-NET

Es ist optional und **kostenlos** möglich, dass im SPECTRUM-ASP- und im SPECTRUM-NET-Betrieb die Einstellung vorgenommen werden kann, dass alle ausgehenden **E-Mails *zwangsweise* *nur TLS-verschlüsselt verschickt*** werden. Sollte ein Empfänger die TLS-Verschlüsselung nicht unterstützen, wird die E-Mail nicht übertragen und der Absender bekommt den Hinweis, dass die Mail nicht verschickt wurde. Der Absender kann dann entscheiden, ob er dem Empfänger die Mail nicht TLS-Transport-verschlüsselt übertragen möchte, hierzu kann der Absender die Empfänger-Adresse auf eine WhiteList setzen lassen (die Administration hierzu ist bei SPECTRUM-ASP ohne zusätzliche Berechnung).

Darüberhinaus lassen sich auf Empfangsseite für gewisse Absender Zwangs-TLS-Verschlüsselungen einstellen, damit auch der verschlüsselte E-Mail-Empfang sichergestellt werden kann.

In den Mitteilungen der Bundesrechtsanwaltskammer 3/2018 „Anwaltliche Kommunikation per E-Mail – nur verschlüsselt?“ beurteilt Rechtsanwalt Dr. Hendrik Schöttle dies wie folgt juristisch:

> *„Eine Pflicht des Berufsträgers zur Verwendung einer TLS-Transport-Verschlüsselung muss wohl bejaht werden.*
>
> *Diese kann allerdings nur so weit greifen, wie auch die Gegenseite eine solche Verschlüsselung unterstützt. Unterstützt der E-Mail-Provider des Mandanten keine solche Verschlüsselung, hat der Berufsträger zumindest alles getan, um eine Transportverschlüsselung anzubieten. Letztlich obliegt die Auswahl eines zuverlässigen E-Mail-Providers, welcher Verschlüsselungsmaßnahmen anbietet, dem Mandanten selbst“.*

Man muss nicht unbedingt diese Rechtsauffassung teilen, es ist aber trotzdem eine nette Argumentation.

Die Bundessteuerberaterkammer sagt in Ihren aktuellen „Hinweisen zur E-Mail-Kommunikation“ vom 7.2.2019:

> *„Der Steuerberater sollte sicherstellen, dass die E-Mail auf dem Transportweg verschlüsselt ist und sich die Server der E-Mail-Provider des Steuerberaters und des Mandanten in Deutschland befinden. Dies sollte sorgfältig mit dem Mandanten besprochen werden. Bei einem KMU-Mandat könnte beispielsweise darauf geachtet werden, dass von Seiten des Mandanten ein deutscher E-Mail-Provider für die Kommunikation mit dem Steuerberater genutzt wird“.*

Noch besser ist eine „Zwangs-TLS-Transport-Verschlüsselung“ wie es z.B. SPECTRUM optional kostenlos bei seinen SPECTRUM-ASP- und SPECTRUM-NET-Leistungen anbietet
(siehe roter Kasten oben).

4. Es muss nicht unbedingt sichergestellt sein, dass ein empfangender SMTP-Knoten-Server, der eine Mail vom Absende-Server TLS-verschlüsselt erhalten hat, diese Mail auch TLS-verschlüsselt an den nächsten SMTP-Knoten-Server oder den Empfangs-Server wieder TLS-verschlüsselt weitergibt. Dies lässt sich zwar zum Teil mit obigen Check-Programmen überprüfen, nur ist dies zu technisch, um Steuerberatern oder Mandanten hier eine Überprüfungspflicht aufzugeben.

> Aber bei Deutschen Providern wie Telekom, T-Online, 1&1, WEB.DE, GMX, Freenet, Strato usw. ist sichergestellt, dass die TLS-Verschlüsselungs-Kette gewahrt bleibt, aber bei einigen ausländischen Mail-Providern (Google-Mail, AOL, Microsoft-Mail, Yahoo usw.) ist dies nicht unbedingt sichergestellt. SPECTRUM empfiehlt hier zur Absicherung, jedem Mandanten eine entspr. Information zukommen zu lassen, womit er sein Mail-System auf TLS-Konformität überprüfen kann.

2. Verschlüsselung nur von E-Mail-Anhängen

Viele Steuerberater erstellen eine BWA, eine Bilanz, eine Steuererklärung, eine Gehaltsabrechnung, eine Brutto/Netto-Lohnabrechnung usw. mit ihren entsprechenden Fachprogrammen und wählen dann einen PDF-Drucker aus, bei dem man händisch die PDF mit einem Passwort verschlüsseln kann. Man schickt dann dem Mandante (oder z.B. der Bank) die Unterlagen als Anhang zu einer Mail. Hierbei dürfen dann in der eigentlichen Mail keine schützenswerten weiteren namentlich zum persönlichen Lebensbereich gehörende Geheimnisse, Betriebs- oder Geschäfts-Geheimnisse enthalten sein …. *eben gemäß § 203 StGB.*

Dieses Verfahren ist eingeschränkt brauchbar, um zum Teil die berufsrechtlichen Verschwiegenheits-Richtlinien für besonders schützenswerte Dokumente und Auswertungen einzuhalten. Es ist allerdings etwas aufwendig, diese verschlüsselten PDFs zu erstellen und vor allem die Passwörter zu verwalten. Schwierig ist es auch, die E-Mail selbst von Hinweisen und sonstigen schützenswerten Informationen freizuhalten – Steuerfahnder und Insolvenzverwalter interessieren sich z.B. sehr häufig nur für das E-Mail-Absendedatum und für die Betreffzeile.

Problematisch ist hier aber - da dann auch auf der Beraterseite alle verschickten Dokumente verschlüsselt sind – denn sie wurden ja als verschlüsselte PDF erstellt. Erstellt man sie einmal verschlüsselt und einmal unverschlüsselt – was technisch durchaus möglich ist – hat man ggfs. bei einem Rechtsstreit das Problem, nachweisen zu müssen, dass beide Dokumente identisch sind. Darüber hinaus ist der Handhabungs- und Archivierungsaufwand sehr umständlich. In dem Zusammenhang ist auch die Verwaltung der Mandanten-Passwörter häufig ein Problem, denn ggfs. muss man hier eine Historienverwaltung durchführen, wenn der Mandant oder der Steuerberater einen Personalwechsel hat und man die Passwörter wechseln muss. Häufig vergessen Mandanten auch die Passwörter, so dass eine Passwortverwaltung auf Kanzleiseite geboten ist.

Was überhaupt nicht geht, ist die leider draußen immer noch häufig angewandte Praxis, als Verschlüsselungspasswort einfach die in der Kanzlei benutzte zentrale Mandantennummer aus der Eigenorganisation zu verwenden. Wenn man dies macht, kann man auch gleich den kompletten Passwortschutz ausfallen lassen.

3. Ende-zu-Ende-Verschlüsselung

Im Unterschied zur TLS-Transport-Verschlüsselung werden bei der Ende-zu-Ende-Verschlüsselung nicht die Transportwege beim Versand verschlüsselt, sondern jede E-Mail selbst wird vom Anfang bis zum Ende verschlüsselt. Nur Absender und Empfänger können den Inhalt der E-Mail lesen, wenn sie den notwendigen Schlüssel haben.

Eine Ende-zu-Ende-Verschlüsselung basiert heute im Allgemeinen auf einem der beiden technischen Standards **S/MIME** oder **PGP** bzw. **GPG**. Wichtig: Die beiden Standards sind untereinander nicht kompatibel. Dies bedeutet, beide Kommunikationspartner müssen den jeweils gleichen Standard nutzen.

S/MIME (Secure / Multipurpose Internet Mail Extensions) und PGP (Pretty Good Privacy) sind Techniken, die z.Tl. höchst kompliziert eingerichtet werden müssen und für den Normalbürger daher eigentlich nicht handhabbar sind.

Erst Mitte 2018 wurden mehrere Sicherheitslücken (siehe HEISE-Online 25.5.2018: „Krypto-Desaster: Erfolgreiche Angriffe auf E-Mail-Verschlüsselung“) in den Protokollen S/MIME und PGP entdeckt, die unter dem Schlagwort „eFail“ bekannt wurden. Wissenschaftler der Uni Münster gingen sogar so weit, dass sie erklärten, dass z.B. S/MIME *„unrettbar kaputt“* ist (siehe u.a. HEISE-Online vom 14. Mai 2018: „PGP und S/MIME: E-Mail-Verschlüsselung akut angreifbar“).

Am 1.7.2019 berichtet der IT-Newsticker HEISE 36) erneut: *„Mit einem gezielten Angriff auf zwei PGP-Schlüssel demonstrieren Unbekannte, dass*

ein zentraler Teil der kompletten PGP-Infrastruktur wahrscheinlich unrettbar kaputt ist. Dieser Angriff auf die PGP-Keyserver demonstriert die hoffnungslose Situation“.

IT-Experten sind sich zur Zeit nicht mehr sicher, ob man wirklich noch PGP oder S/MIME als Ende-zu-Ende-Verschlüsselung empfehlen kann. Vernünftige Alternativen existieren aber nicht.

Auch ein „voller Schlüsselbund“ mit vielen Schlüsseln ist gar nicht so einfach zu verwalten, es ergibt sich die Frage: „Welcher Schlüssel passte jetzt noch in welches Schloss?“ Und man muss an allen Endgeräten die Schlüssel hinterlegen, sonst ist ein Öffnen am Firmen-PC, am Home-PC, am SmartPhone oder am Tablet nicht möglich.

Risiko: Die E-Mail ist bei S/MIME oder PGP/GPG durchgängig von Endgerät zu Endgerät geschützt und auch bei den E-Mail-Providern, den Telekommunikations-Diensteanbietern und an den Knotenpunkten nicht mehr im Klartext einsehbar:

aber auch nicht auf Schadcode prüfbar!

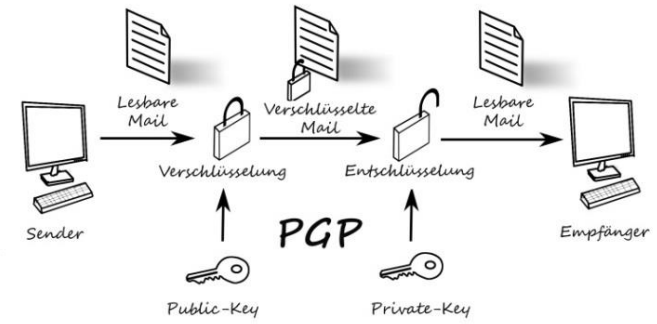
Dies bedeutet, dass alle E-Mail-Sicherungs-Systeme, die Steuerberater heute vorhalten, wie beispielsweise DATEVnet, SPECTRUM-NET usw. (bei denen jede eingehende E-Mail durch eine Art E-Mail-Waschstraße von mehreren hintereinandergeschalteten Virenscannern auf Schadcode geprüft werden) nun Viren, Trojaner usw. nicht mehr erkennen können, da auch diese CyberCrime-Schadcodes für die Übertragung dann ja „mitverschlüsselt“ würden – d.h. erst beim Empfänger, bei der Entschlüsselung wird auch der Virus, der Trojaner wieder entschlüsselt und kann nun beim Empfänger ungehindert Schaden anrichten.

Fazit: Eine Ende-zu-Ende-Verschlüsselung erhöht auch die Gefährdung!

3.1 Ende-zu-Ende-Verschlüsselung: PGP/GPG

PGP beruht auf einer sogenannten Public-Key-Infrastruktur (PKI). Man braucht einerseits einen - für jedermann zugänglichen - „Public-Key“ und andererseits einen geheimen „Private-Key“-Schlüssel.

Jeder Teilnehmer benötigt in diesem System also immer ein Schlüsselpaar mit einem geheimen und einem öffentlichen Schlüssel, die immer zusammengehören. Um PGP-Schlüssel zu erzeugen und zu verwalten, benötigt man Hilfsprogramme, wie z.B. GnuPG. Diese kostenlose Software ist sowohl für Windows als auch für macOS, Linux und Android verfügbar.



Ein Schlüsselpaar wird immer für eine damit verbundene Mail-Adresse erstellt (fest gekoppelt). Wichtig: für jede Mail-Adresse muss man jeweils solche PGP-Schlüssel erzeugen, was bei manchen Kanzleien und Unternehmen – sofern man PGP an den Arbeitsplätzen einsetzen will – schon zu einem nicht unerheblichen Verwaltungsaufwand führt. Nutzt man die PGP-Verschlüsselung nur als globale Verschlüsselung z.B. für eine info@-Adresse (wie es z.B. das LDI-NRW macht), dann stellt sich die Frage, was diese Verschlüsselung überhaupt noch soll, denn dann haben alle Personen, die Zugang zu diesen globalen info@-Adressen haben, auch Zugang zu allen verschlüsselten, vertrauenswürdigen E-Mails.

Beispiel: Öffentl. PGP-Schlüssel LDI-NRW:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP Desktop 10.2.1 (Build 4940)

mQMuBFVLLGURCADNoUGqUX5R69pbFT0wpvTdS62NkSNSrtB5DhIv2Z7VxAgp8pjf
ferREYXo1jWPb5tcuckqiZkBDylrF5aqvZoUllgv4bbjQwirAHYG9sxLYjjt4Lar
B1k4XTnyfOaSz2TNQLmD9kw+Ac7lnXtUIG3bvkEFYZTOntPHkiTs9j2Gbq61FNXd
sYi98iIz8zrq1VXfxr56etbqoXjfnGFhOWdeAu+pgoasSs5kRZj2fMi4pl6OBFtx
h3FfxLSgSaODqYzg1txUpvV7qzSCwXymnMV+psOHM1ePJsSa22up+UY0zu+mJTR
MiWmaM76UetbQpUqJynmfA2+xUWXYanrQJZJAQD/M1O1dPb59NBBUQXeCl8kJvXW
fuegsm5NnJm3drP8eQgAy0uwASUcCas7wT8gjo2FHd0wviedPLAWbCO7jTZsWYY9
NzuYsCC1RA3ATAfVM6hh3OZ/ZXltp1C2g/MasnSqvZqqLB1L0LTuwhnQwD1nbFRa
Aqs1U30Pft19Kfao+Vd8Wv45VnFD63kyc0z/q9/WyLUo4MQ5yD1Xq21QtLN1XShR
DX0Hwscf0eBfw0r1heTwR2viTX2wEjAyr2Nje4u/hEHvUudNoV67hAd+abebxu7v
bEm9FnahjgXeFBTR0BXesa0D7Sx6t60Qb5EMNI8x5t1IvQvWxsPxJurJkP9Hv4e4
QKNREQ7M+urxRgP/xX5epLc6q+Rjx5OoABL2ASwiRQgAiIj96L49tzlof1lgnozH
+WeRUVAGC8q1Mk9szR/gZWMIqdWZ9D5g4gnUeXZpeozHkSk9HCjNoiU4TF5kP235
AZ2nbGBod4rxT/CdOdf1JyaTxLmjKKzXDbe+/UAOus9sAAw6kFjzoRRZGY9kBfyk
veCHi/cb1WRa/vwvpTApOpNaJwzWC1lHVgxpy6oy1Eubq5uTOHtn4fbut4dX8xZ2
lMSICnm3liP0x1f2aluaxN2ieQPPMvG9lmOWuvA18FaU5NKEQyjfh4U5VeFKSZHP
9FxgzqUmUKFQ/9d3/rdiBWvnJX92g+NRO48U86cSN/ImP6STLizoIMcibK2pBAxb
wrQfTERJIESSVyA8cG9zdHN0ZWxsZUBsZGkubnJ3LmRlPokAugQQECgAYgUCVUss
ZQUJCYb3ADAUgAAAAAAgAAdwcmVmZXJyZWQtZW1haWwtZW5jb2RpbmdAcGdwLmNv
bXBncG1pbWUICwkIBwMCAQoCGQEFGwMAAAAFFgADAgEFHgEAAAAGFQgJCgMCAAoJ
EATjGhNq1igR3+IA/iiYgEm+DrVtwsQ1v0o3pcbI67iJemgP4DKxE3OkMvK0APwL
tBlockGDe+sWkURUXXAp0jxNAIGB70chR21f22kHGrkEDQRVSyxlEBAA+Rigflo G
YXpDkJXcBWyHhuxh7M1FHw7Y4KN5xsncegus5D/jRpS2MEpT13wCFkiAtRX1KZmp
nwd00//jocWWIE6YZbjYDe4QXau2FxxR2FDKIldDKb6V6FYrOHhcC9v4TE3V46pG
zPvOF+gqnRRh44SpT9GDhKh5tu+Pp0NGCMbMHXdXJDhK4sTw6I4TZ5dOkhNh9tvr
JQ4X/faY98h8ebByHTh1+/bBc83DE5YrQ2DD4+jWCv2hKCYLrqmus2UPogBIAaB8
lqujEh76Dyr0H3SET8rzF/OkQOnX0ne2QiOCNsEmy2henXyYCQqNfi3t5F159dSS
I5sYjywgp0t8MvZCV7cIfwgXcqK61qIC8wXo+VMROU+28W65Szgg2gGnVqMU6Y9A
VfPQB8bLQ6mUrfdMZIZJ+AyDvWXpF9Sh01D49Vlf3HZSTz09jdvOmeFXk1nN/biu
dE/F/Ha8g0VHMGHOfMlm/aX5u/2RXscBgtNbno2gpXI61Brwv0YAWCv19Ij9WE5J
280gtJ3kkQc2azNsOA1FHQ98iLMcfFstjvbzySPAQ/ClWxiNjrtVjLhdONM0/XwX
V0OjHRhs3jMhLLUq/zzhsSlAGBGNfISnCnLWhsQDGcgHKXrK1QzZlp+r0ApQmwJG
0wg9ZqRdQ2+cfL2J5yIZJrqrol7DVes91hcAAgIP/i0WPAE1tk/LZRA+TxGVpRjm
NgnJxx5a6eCK9MsTkH3Wnrm9hSUMk+n6aCpB9hnivN6mE6GpFDJZdVt59BvDk2+E
SmQCgDufEWQ65R+QGLflz//XSsiI375fLSkDk+SXJHAr0UDWJSGSumzb0JuieWzo
Lv4DoTw25EWUTz4U0gu3kGtqqtBMkLAUfr0fbk6IPv4KiNnEH4PIDT0xWvLdwZRY
/SRyKxziRZrzqUaBOdOYAT6KbDWHtvhX5bDR5w92fcGdAvx9RcpDZlnZLi070bnX
17dhiN74o2HXLj5Lc6zGIcK3TIjGQIHB7C0+Cvn+IjKPiA9RaxayXmtmwCfxhTUm
xn1bQ+KUEC+qz6/JOkUNr1LmplRO8WxN57RwoeWNt2t576iem49PKVlVejkKfzFk
livp+Rw7HqOqX89jMvZTnI7rhyJYqI0fK19bfgdftqq2FmIbZDhtuEaRGYTbnMJw
Hxv3FtjExSHZgOxDRzueewWfyPg+3dtQY626y+/llvqL8FashyoEe6aTHtyfD4dp
EG22ToGDvEQR2Nx5b/enLhbDO7rDkwgdiv9miRgqwv4nlPbTQvscU+USdi7tvWsf
m89HIHmiDyX1ylKhxjm9N8chir9Ii9V26ztMQh7WBAcCrru7Wdly1f+Fn2Kma6da
5WLbxp+95+9UNt/R+WpkiQBqBBgRCAASBQJVSyxlBQkJhvcABRsMAAAAAAoJEATj
GhNq1igRGYoBAIYTj36WFBTCFkle7NYM/FP2/L6DtGl2nIb60Y0UgYmmAQDCZoOf
BFeRcsTCdqEgvuZd03Z4B1ejR9o5OGR4hTXDhQ==
=IqcS
-----END PGP PUBLIC KEY BLOCK-----

Dann bietet aber eine PGP-Ende-zu-Ende-Verschlüsselung nicht mehr Sicherheit als eine TLS-Transportverschlüsselung.

Besonderes Augenmerk sollte man auf die Wahl des Passworts legen. Es sollte nicht das selbe sein, mit dem man sich auch bei Ama-

zon, Google, Facebook usw. anmeldet. Nach der Generierung der beiden Schlüssel sollte man eine Kopie sicher aufbewahren, z.B. auf einem externen USB-Stick (den man natürlich gut aufbewahren sollte). Ein Schlüssel ist übrigens nur eine simple Textdatei, mit unverständlich vielen zusammengesetzten Zahlen, großen/kleinen Buchstaben und Sonderzeichen (siehe Beispiel PGP-Schlüssel des LDI-NRW). Nachdem die Schlüsselerzeugung abgeschlossen ist, wird der selbst erstellte „öffentliche Schlüssel“ als Zertifikat digital unterschrieben bzw. beglaubigt (signiert).

Nun können Sie Ihren Mandanten, Ihren Geschäftspartnern usw. ihren „öffentlichen Schlüssel“ zugänglich machen – z.B. in dem man im Impressum seiner E-Mail-Signatur einen Link zu seiner Homepage aufführt, wo man den „öffentlichen Schlüssel“ zum Download hinterlegt hat. Im Zeitalter vieler Viren- und Trojaner-Mails, die versuchen jemanden zu animieren auf einen Link zu klicken, ist dies aber sicherlich keine allzu gute Lösung. Das Bundesamt für Sicherheit in der Informationstechnik – BSI („E-Mail Verschlüsselung in der Praxis“) warnt zusätzlich: „Wird der öffentliche Schlüssel per E-Mail offen übersandt, ist die Authentizität des öffentlichen Schlüssels nicht sichergestellt, denn z.B. könnte durch eine ‚Man-in-the-Middle-Attacke‘ ein Angreifer diese Mail abfangen und den Schlüssel durch einen manipulierten Schlüssel ersetzen. Der Kommunikationspartner verschlüsselt seine Nachricht dann unwissentlich mit dem Schlüssel des Angreifers, der diese Nachricht dann mit seinem eigenen Schlüssel lesen kann. Eine korrekte Assoziierung des Schlüssels mit der passenden E-Mail-Adresse ist also nicht gegeben“.

Wichtig ist, dass der private Schlüssel niemals in fremde Hände gelangen darf!

Beliebt (aber nicht ganz ungefährlich) ist auch das Hochladen des „öffentlichen Schlüssels“ auf sog. KeyServer im Internet. Diese KeyServer sind so eine Art für jedermann zugängliche PGP-Key-Adressbücher, die oft auch noch miteinander vernetzt sind und die Keys austauschen (Synchronizing-Key-Server - SKS). Das BSI warnt hier wieder: „Wenn der öffentliche Schlüssel auf einen KeyServer hochgeladen wird, wird die Zuordnung zur E-Mail-Adresse von dem Server nicht geprüft – d.h. es können auch andere Personen öffentliche Schlüssel zum KeyServer hochladen. Wird der falsche Schlüssel benutzt, so kann der berechtigte Empfänger die E-Mail nicht entschlüsseln, dafür aber derjenige, der den falschen Schlüssel hochgeladen hat“.

Hat man diese Schlüsselgenerierung nun durchgeführt, muss dem E-Mail-Client wie z.B. MS-Outlook die PGP-Option beigebracht werden. Dies geht z.B. über Tools für die Integration mit sogenannten Outlook-Privacy-PlugIns. Auch für Android-Smartphones und iPhones gibt es entsprechende PlugIns, die man extra laden und installieren muss.

Nun können Sie z.B. als Steuerberater auf Ihrem Kanzlei-System mit dem Outlook-PGP-PlugIn und dem „öffentlichen Schlüssel“ ihres Mandanten (d.h. der Mandant muss natürlich auch erst PGP vorher auf seinem System eingerichtet haben und Ihnen seinen öffentlichen Schlüssel mitgeteilt haben) diesem Mandanten eine PGP-verschlüsselte Mail schicken, die der Mandant dann mit seinem eigenen „privaten Schlüssel“ und seinem Passwort öffnen und lesen kann.

Anachronismen: PGP durfte in seinen Anfangsjahren nicht aus den USA exportiert werden, da Verschlüsselungen, ähnlich wie Waffen, unter das US-Exportgesetz fiel. Um die Exportbeschränkung zu umgehen, wurde dann der Quellcode vom PGP-Erfinder Phil Zimmermann Mitte der 90er einfach in einem Buch „PGP Source Code and Internals“ veröffentlicht, denn Bücher konnten, gleich mit welchem Inhalt, ganz legal die USA verlassen. Eine Schar Freiwilliger hat dann den Programmcode weltweit abgetippt, aus dem dann eine international verfügbare Version von PGP kompiliert wurde.

Das Ur-PGP wurde dann 1997 von der Fa. McAfee aufgekauft und seit 2010 liegen die Rechte bei der Fa. Symantec. Da dann intransparente Situationen bzgl. der Produktrechte und Weiterentwicklungen entstanden, wurde 1998 ein sogenannter OpenPGP-Standard entwickelt, der unter GNU-GPL bekannt geworden ist.

GNU-Privacy-Guard bzw. GnuPG oder einfach kurz GPG ist das heute allgemein genutzte System. OpenPGP und GnuPG sind aber nicht unbedingt miteinander kompatibel.

Zu guter Letzt sei noch der Hinweis erwähnt: Denken Sie daran, dass PGP lediglich die Kommunikationsinhalte wie Texte, Bilder und Anhänge verschlüsselt, die Kopfzeilen der Mails bleiben für jedermann aber lesbar. Es lässt sich also trotz Verschlüsselung leicht nachvollziehen, wann Sie mit wem kommuniziert haben – und, wenn es im Betreff steht, auch worüber. Gerade diese Metadaten sind für Ermittlungsbehörden aber oft interessanter als die Inhalte selbst. Außerdem: Man kann

immer nur verschlüsselte E-Mails mit Internet-Teilnehmern austauschen, die auch selbst PGP auf ihren Systemen eingerichtet haben.

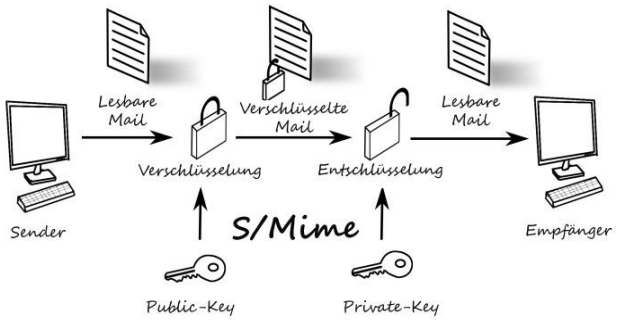
Möchte man also jemandem eine Ende-zu-Ende-PGP-verschlüsselte E-Mail schicken, muss man erst jemanden finden, der das gleiche PGP-System implementiert hat und dessen öffentlichen Schlüssel man kennt.

3.2 Ende-zu-Ende-Verschlüsselung: S/MIME

S/MIME (Secure / Multipurpose Internet Mail Extensions) ist der zweite Standard für die Verschlüsselung von E-Mails. S/MIME funktioniert ebenfalls mit einem öffentlichen und einem privaten Schlüssel. Obwohl S/MIME vom Funktionsprinzip gleich wie PGP ist, verwenden PGP und S/MIME unterschiedliche Schlüsselformate und sind deshalb nicht kompatibel. S/MIME bietet neben der Verschlüsselung auch optional direkt eine Signaturfunktion.

Um S/MIME einzusetzen, benötigt man das besagte Schlüsselpaar privat/öffentlich. Dafür braucht man sogenannte X.509-Zertifikate. Prinzipiell kann man sich die Zertifikate zwar auch selbst erstellen, sinnvoller ist es jedoch und allg. Praxis, kostenpflichtige Zertifikate von einer offiziellen Zertifizierungsstelle zu benutzen. Sie werden dann von den meisten Betriebssystemen als vertrauenswürdig eingestuft und machen somit keine Probleme.

S/MIME basiert also ebenfalls auf einer asymmetrischen Verschlüsselung und verwendet ein Paar mathematisch verknüpfter Schlüssel - einen „öffentlichen Schlüssel“ und einen „privaten Schlüssel“. E-Mails werden mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Die E-Mail kann nur mit dem entsprechenden privaten Schlüssel entschlüsselt werden. Dieser ist im alleinigen Besitz des Empfängers. Wenn der private Schlüssel nicht kompromittiert wird, kann man sicher sein, dass nur der legitime Empfänger auf sensible Daten zugreifen kann.



Jetzt muss man noch z.B. in seinem Mail-Client wie MS-Outlook (Datei - Optionen - Trust Center - Einstellungen für das Trust Center - Sicherheitscenter - E-Mail-Sicherheit - Digitale IDs (Zertifikate) - Importieren/Exportieren) seinen privaten Schlüssel eintragen und danach geht fast alles automatisch: Zur Verschlüsselung einer E-Mail muss der Absender nur den öffentlichen Schlüssel des Empfängers kennen. Ein E-Mail-Client wie MS-Outlook vereinfacht dann die Handhabung, indem er automatisch alle erhaltenen Zertifikate speichert und verwaltet.

Vorteile von S/MIME gegenüber PGP/GPD, bzw. was besonders gut gefällt: Wenn man die Hürde der Zertifikatinstallation einmal genommen hat, geht der Rest quasi von selbst. Man schreibt E-Mails wie gewohnt, signiert und verschlüsselt sie über z.B. in Outlook verwaltete Schlüssel. Schickt jemand eine, mit S/MIME signierte E-Mail, wandert dessen öffentlicher Schlüssel automatisch in eine Private-Key-Verwaltung z.B. in Outlook (bei Apple heißt dies sogar nett „Schlüsselbund-Verwaltung“). Ohne dass man sich darüber Gedanken machen muss, werden dann E-Mails an diesen Empfänger künftig auch immer verschlüsselt übertragen.

Ob man letztlich S/MIME oder PGP/GPG verwendet, ist oft Geschmackssache, allerdings hat S/MIME einen Vorteil: Es ist bereits in vielen Mail-Programmen und Smartphones eingebaut und einfacher in der Handhabung.

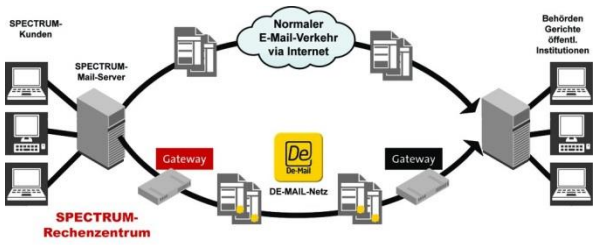
Es kann aber trotzdem wohl festgehalten werden, dass das komplizierte PGP/GPG-Verfahren aber auch das etwas benutzerfreundlichere S/MIME nie zu einem praktikablen, vermehrten Einsatz kommen werden, da alleine das Schlüssel-Austauschverfahren und die Installationsaufwendungen ein zu großes Hindernis für den normalen Nutzer (Mandanten) darstellen …

Die Bundessteuerberaterkammer (BStBK) schreibt im Papier von April 2019 zur PGP- bzw. S/MIME-Verschlüsselung:

„Da der Anwender bei der Ende-zu-Ende-Verschlüsselung selbst aktiv werden muss, um die Technologie nutzen zu können, hat sich diese Technologie nicht flächendeckend durchgesetzt und wird von Mandanten teilweise abgelehnt“.

1.3 Ende-zu-Ende-Verschlüsselung mit DE-MAIL

Eine elegante und sichere Art E-Mails zu übertragen besteht mit dem schon oft für tot erklärten DE-MAIL-Verfahren. Inhalte, die per DE-MAIL übertragen werden, können weder mitgelesen, noch verändert werden. Um zu verhindern, dass zusammen mit einer DE-MAIL Schadsoftware, etwa von dem infizierten Rechner eines Nutzers über die sicheren Kommunikationskanäle von DE-MAIL verbreitet wird, sind die DE-MAIL-Anbieter gesetzlich verpflichtet, eine Prüfung auf Schadprogramme durchzuführen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) überprüft regelmäßig, ob die Sicherheitsauflagen von den DE-MAIL-Anbietern eingehalten werden. Bei DE-MAIL sind die Anbieter verpflichtet, für ein Maximum an IT-Sicherheit und Schutzmaßnahmen zu sorgen. DE-MAIL unterstützt eine zusätzliche Ende-zu-Ende-Verschlüsselung von Nachrichten. Aufgrund weitergehender Sicherheitsmerkmale und Funktionen ermöglicht DE-MAIL nicht nur eine sichere und geschützte Übertragung von Daten, sondern auch die Nachweisbarkeit einer Zustellung an einen bestimmten Empfänger zu einem ausgewiesenen Zeitpunkt. Durch diese technischen Eigenschaften und aufgrund gesetzlicher Regelungen (es gibt ein eigenes DE-MAIL-Gesetz) ermöglicht DE-MAIL beispielsweise die Ersetzung der Schriftform bei Anträgen an Behörden und eine Beweiserleichterung über Absender, Versand, Zugang und den Inhalt einer Nachricht vor Gericht.



Hintergrund: Durch die Bundesregierung wurde am 3. Mai 2011 das DE-MAIL Gesetz verabschiedet. Es regelt den rechtlichen Rahmen zum Angebot und zur Anwendung des neuen Secure Mail Produktes DE-MAIL. Auf der Gesetzesgrundlage ist DE-MAIL ein (weitestgehend) vollwertiger elektronischer Ersatz für die physikalische Briefpost. Durch zertifizierte DE-MAIL-Diensteanbieter (z.B. Deutsche Telekom) wird das DE-MAIL Kommunikationsnetzwerk bereitgestellt. Die Zulassung erteilt das Bundesamt für Sicherheit in der Informationstechnik (BSI) nach Überprüfung bestimmter durch das Gesetz und den sogenannten »Technischen Richtlinien« geforderten Zertifikaten. DE-MAIL Anwender können alle juristischen und volljährigen natürlichen Personen sein. Die Identifizierung der Teilnehmer erfolgt durch Vorlage eines Identifikationsnachweises vor den Identifikationsstellen der DE-MAIL-Diensteanbieter (z.B. einfach in einem Telekom-Shop oder durch den zuständigen Telekom-Betreuer). Die Anwender stellen bei dem DE-MAIL-Anbieter ihrer Wahl einen Antrag auf Eröffnung eines DE-MAIL-Kontos, werden identifiziert, erhalten ihre Zugangsdaten und können DE-MAIL umgehend nutzen.

DE-MAIL & SPECTRUM-ASP bzw. SPECTRUM-NET

Als besondere Maßnahme hat SPECTRUM für SPECTRUM-ASP- und SPECTRUM-NET-Kunden zusammen mit der Deutschen Telekom im SPECTRUM-Rechenzentrum ein DE-MAIL-Gateway installiert, worüber normal in MS-Outlook erstellte, über MS-Exchange verwaltete E-Mails als DE-MAIL verschickt und empfangen werden können. Viele SPECTRUM-Kunden nutzen diesen besonderen Service, weil man so einfach mit den Finanzgerichten und staatlichen Stellen elektronisch kommunizieren kann.

Eine DE-MAIL-Adresse kann für juristische Personen (Unternehmen und Behörden) z.B. lauten: ….@meinefirma.de-mail.de.

Für die DE-MAIL Kommunikation greift die Zustellfiktion gemäß der der Briefpost. Eine DE-MAIL gilt als zugestellt, wenn sie im Postfach des Empfängers eingestellt wird.

Versand- und Zustellbestätigungen durch den DE-MAIL-Diensteanbieter sind vergleichbar mit einem Einschreiben mit / ohne Rückschein.

Der Inhalt einer DE-MAIL wird durch ihren Hash-Wert nachgewiesen, ebenso die Veränderung des Inhaltes. Bei DE-MAIL werden verschiedene Authentisierungsstufen verwendet, die den Grad der Nachweisbarkeit unterstützen. Der DE-MAIL-Nutzer kann sich vom DE-Mail-Diensteanbieter optional per E-Mail oder SMS über neu eingetroffene DE-MAILs im Postfach informieren lassen. Damit muss der

Nutzer nicht permanent aktiv in das Postfach schauen, ob etwas eingetroffen ist oder nicht.

Durch den SPECTRUM-DE-MAIL-Gateway-Betrieb wird DE-MAIL voll in den Outlook- und MS-Exchange-Betrieb der SPECTRUM-NET- bzw. der SPECTRUM-ASP-Anwender integriert.

DE-MAIL ermöglicht eine vertrauliche und nachweisbare elektronische Kommunikation: Versand, Empfang und Inhalte von DE-MAILs können rechtswirksam nachgewiesen werden.

Wichtiger Hinweis: Alle Behörden des Bundes sind durch das "Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften" (E-Government-Gesetz) sogar verpflichtet, einen Zugang für DE-MAIL zur Verfügung zu stellen.

Das **„Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten“** (FördElRV) ändert u.a. viele Bundesgesetze und andere Rechtsvorschriften. Das Gesetz enthält u.a. differenzierte Regelungen, wann ein „sicheres Übermittlungsverfahren“ vorgehalten werden muss. Steuerberater, Steuerbevollmächtigte, Wirtschaftsprüfer oder vereidigte Buchprüfer gehören z.B. nach der Finanzgerichtsordnung (FGO) zu den vertretungsberechtigten Personen, die ihre Mandanten wie Anwälte vor den Finanzgerichten vertreten dürfen. Ein ähnliches Vertretungsrecht gilt für Steuerberater auch für die Sozialgerichte und Verwaltungsgerichte. In der Finanzgerichtsordnung wurde für den „elektronischen Rechtsverkehr mit den Gerichten“ eine Pflicht eingeführt, den elektronischen Rechtsverkehr zu nutzen.

Ab dem 1.1.2018 sind auch Steuerberater (die z.B. Ihre Mandanten vor den Finanzgerichten vertreten) verpflichtet, für den „elektronischen Rechtsverkehr mit den Gerichten“ empfangsbereit zu sein und ab 1.1.2022 Schriftsätzen an Gerichte ausschließlich elektr. einzureichen. Bei den Kammern und Institutionen wurde lange auch ein „besonderes elektronisches Steuerberaterpostfach“ (beSt) – ähnlich der Rechtsanwaltslösung „beA“ – diskutiert, ohne dass es hier zu einer Lösung gekommen ist. Die Steuerberaterkammern empfehlen daher Steuerberatern, die Fälle an Finanzgerichten führen, mangels anderer Alternativen das DE-MAIL-System zu verwenden.

Der Nachteil von DE-MAIL: Beide Seiten müssen einen DE-MAIL-Zugang haben.

Jetzt bieten bieten aber fast alle DE-MAIL-Diensteanbieter (Telekom, Web.de, GMX) Privatpersonen kostenlose DE-MAIL-Postfächer an. Es ist also eine Überlegung für Steuerberater, besonders sensiblen Mandanten auch die DE-MAIL-Nutzung anzubieten.

3.4 Ende-zu-Ende-Verschlüsselung: DATEV E-Mail-Verschlüsselung

Die DATEV-E-Mail-Verschlüsselung ist eine Sonderform der S/MIME- und OpenPGP-E-Mail-Verschlüsselung und basiert auf Kanzleiseite immer auf dem Internet-Zugangssystem DATEVnet. D.h. die teilnehmenden E-Mail-Adressen müssen bei DATEVnet verwaltet werden. Jeder Anwender, der die DATEV-E-Mail-Verschlüsselung nutzen soll, benötigt außerdem eine DATEV-SmartCard. Die SmartCard muss die korrekte E-Mail-Adresse des Anwenders beinhalten und derselben Beraternummer zugeordnet sein wie der DATEVnet-Vertrag.

Die DATEV-E-Mail-Verschlüsselung ist ein DATEV-Fremdprodukt und ist eine Lizenz des schweizerischen SEPPmail-Systems (siehe auch SPECTRUM-SEPPmail-Angebot).

Das Programm DATEV E-Mail-Verschlüsselung dient dazu, eine automatisierte Verschlüsselung von ausgehenden E-Mails, unabhängig von der eingesetzten technischen Infrastruktur des Kommunikationspartners, zu ermöglichen. Mit Nutzung des Produkts DATEV E-Mail-Verschlüsselung beauftragt der Kunde DATEV, die privaten Verschlüsselungsschlüssel der entsprechenden SmartCards zentral in einem Hardware-Sicherheitsmodul zu hinterlegen und zu nutzen, um damit ankommende S/MIME-verschlüsselte E-Mails zentral im DATEV-RZ zu entschlüsseln und danach dem Empfänger auf dem bisher genutzten DATEVnet-Weg unverschlüsselt zuzustellen. Die E-Mails durchlaufen dadurch bei DATEVnet auch alle zentralen Spam- und Virenfilter als unverschlüsselte Mails und gelangen dann ebenfalls unverschlüsselt in das System der Kanzlei. Hier wird also ebenfalls die Verschlüsselungskette aufgebrochen und DATEV kann als DATEVnet-Provider alle E-Mails mitlesen. Eine Ende-zu-Ende-Verschlüsselung gemäß der Ende-zu-Ende-Spezifikation ist dies also nicht …. auch wenn die DATEV Genossenschaft einen hohen Vertraulichkeits-Leumund hat.

Das SEPPmail-Verfahren, auf dem die DATEV-E-Mail-Verschlüsselung ja basiert, ist da sehr gut durchdacht und bietet entspr. Automatismen: Z.B. sucht entsprechend der Steuerung durch den Absender das DATEV-E-Mail-Verschlüsselungs-Gateway auf Basis der E-Mail-Adresse des Empfängers in verschiedenen öffentlichen Schlüssel-Verzeichnisdiensten (Synchronizing-Key-Server - SKS) im Internet nach hinterlegten öffentlichen Schlüssel für jeden Empfänger oder nutzt die dem Absender bekannten DATEV-SmartCard-Daten, sofern der Mandant so etwas besitzt. Die E-Mail wird dann mit allen gefundenen öffentlichen Schlüsseln verschlüsselt und kann mit einem der Schlüssel geöffnet werden. Das gilt auch wenn für eine E-Mail-Adresse mehrere gültige, öffentliche Schlüssel gefunden werden. Die angewendeten Verschlüsselungsverfahren sind S/MIME und OpenPGP/MIME.

Man kann also sagen, dass SEPPmail die meisten Handhabungsprobleme mit S/MIME bzw. OpenPGP geschickt gelöst hat.

Wenn der Mail-Empfänger über keine Verschlüsselungszertifikate (DATEV mIDentity oder DATEV SmartCard) verfügt, kann er seine E-Mail online in einem intuitiv bedienbaren DATEV-Web-Portal entschlüsseln. Der Empfänger braucht also nicht unbedingt eine DATEV SmartCard. Wenn für eine Empfängeradresse kein öffentlicher Schlüssel gefunden werden kann, wird vom System ein alternatives Verschlüsselungsverfahren genutzt, das eine verschlüsselte HTML-Datei (secure-email.html) als Anhang einer DATEV-E-Mail an den Empfänger schickt. Wenn der Empfänger diese secure-email.html mit einem Browser öffnet, wird er zu einem speziellen Web-Portal der DATEV geleitet. Bei der ersten Nutzung dieses Web-Portals muss sich der Empfänger einmalig registrieren, wobei er selbst ein Passwort vergeben und eine Sicherheitsfrage wählen und beantworten muss. Die Antwort auf diese Sicherheitsfrage wird benötigt, falls das Passwort einmal vergessen wird. Bei jeder weiteren Anmeldung an dem DATEV-Web-Portal muss der Empfänger nur noch sein Passwort angeben. Der Empfänger (Mandant) kann dem Absender aus dem Web-Portal auch gesichert antworten.

Der Vorteil dieses DATEV-E-Mail-Verschlüsselungsverfahrens liegt darin, dass die S/MIME-verschlüsselten Antwort-E-Mails die der Mandant an die Kanzlei schickt, nicht auf dem Server der Kanzlei entschlüsselt werden (und mitverpackte Viren dann bei der Entschlüsselung ihr Unwesen treiben könnten), sondern dass die Antwort-E-Mails der Mandanten zentral im DATEV-RZ entschlüsselt werden und die zentralen Viren-Scanner von DATEVnet für eine möglichst saubere Mail-Zustellung sorgen.

Dieser Vorteil der DATEV-E-Mail-Verschlüsselung, dass auch weiterhin E-Mails in der DATEVnet-Sicherheits-Zentrale überprüft werden, ist jedoch auch ein großer Nachteil dieses Verfahrens: denn in Wahrheit ist es keine Ende-zu-Ende-Verschlüsselung mehr …. Der Provider (DATEV) kann alle Mails mitlesen ….

Zur Information hier die Kosten der DATEV-E-Mail-Verschlüsselung: z.B. kosten 5 User 12,00 € pro Monat +USt, 10 User 23,00 € pro Monat +USt, 20 User 42,50 € pro Monat +USt, 40 User 75,50 € pro Monat +USt plus die Kosten von DATEVnet: DATEVnet-Netz-Basis 36,00 € pro Monat +USt plus DATEVnet-Router 10,00 € pro Monat +USt plus pauschale Nutzungsgebühr von 99,00 € pro Monat +USt. D.h. eine E-Mail-Verschlüsselung für ein 10 User-System kostet bei DATEV 168,00 € pro Monat +USt und für ein 20 User-System 187,50 € pro Monat +USt.

Kritische Anmerkung von SPECTRUM zu diesem DATEV-Web-Portal-Verfahren:

Auch wenn SPECTRUM selbst das SEPPmail-Verfahren im Angebot hat, hier ein paar kritische Anmerkungen zu dem Verfahren:

Der Anwender, der keinen öffentlichen S/MIME und OpenPGP/MIME Schlüssel hat - welches heute wohl 99% aller Mandanten eines Steuerberaters sein dürften - bekommt Mails mit diesem secure-email.html-Link mit der Absenderkennung der DATEV – *nicht mit der Absenderkennung der Kanzlei.* In dieser Mail ist dann ein Link angegeben, den der Mandant anklicken soll, um zu einem DATEV-WEB-Portal weitergeleitet zu werden.

Aus Sicherheitsgesichtspunkten hält SPECTRUM dieses Verfahren für äußerst gefährlich: Tagtäglich werden die Anwender gewarnt, nicht auf jeden Link einer angeblichen DHL-, Amazon-, Deutsche Bank-, Volksbank-, Sparkassen-Mail zu klicken, da es sich um Fake-Mails handeln kann, die nur ähnlich wie das Original aussehen, aber per Link den Anwender dann zu Schadcode-Seiten im Internet von CyberKriminellen führt. Warum sollten CyberKriminelle nicht demnächst auch Fake-Mails mit DATEV-Absenderkennung verschicken?

Außerdem entspricht dieses DATEV-E-Mail-Verschlüsselungsverfahren nicht den Prinzipien für eine richtige Ende-zu-Ende-Verschlüsselung, denn die Verschlüsselung wird bei der DATEV ja aufgebrochenhoben und die DATEV spielt hier eine unverschlüsselte *„Man-in-the-Middle“*-Rolle, weil hier zentral alle Verschlüsselungen aufgebrochen werden und dann in die Kanzlei unverschlüsselt weitergeleitet werden. Dann kann man auch bei der TLS-Transportverschlüsselung bleiben, wo ja lediglich die Provider mitlesen könnten.

Das DATEV-E-Mail-Verschlüsselungsverfahren basiert auf dem Produkt SEPPmail, siehe auch entsprechendes alternatives SEPPmail-Angebot von SPECTRUM im roten Kasten.

3.5 Ende-zu-Ende-Verschlüsselung: mit Container-Verschlüsselungs-Verfahren

Ein sehr beliebtes, weil einfach zu handhabendes E-Mail-Verschlüsselungs-Verfahren ist die sogenannte „Container-Technik“. Hierbei wird die E-Mail nebst allen Anhängen in eine verschlüsselte ZIP-Datei oder eine PDF-Datei Container-mäßig mit einem Passwort „verpackt“ und dann wiederum als neutrale Mail an den Adressaten verschickt. D.h. der Empfänger erhält eine standardisierte E-Mail z.B. mit einer verschlüsselten PDF-Datei im Anhang, die nur mit einem vom Absender übermittelten, Passwort geöffnet und entschlüsselt werden kann.

SPECTRUM-PDF-Mail

Container-Mail-Verschlüsselung

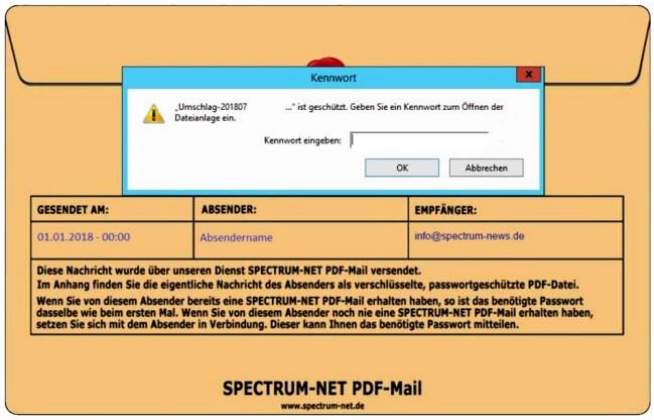
Mit SPECTRUM-PDF-Mail ist es möglich, eine Ende-zu-Ende-verschlüsselte E-Mail an beliebige Empfänger zu verschicken ohne sich darüber Gedanken machen zu müssen, ob der Empfänger irgendwelche Verschlüsselungssoftware benutzt. Man erstellt einfach wie gewohnt seine E-Mail (mit JPG-, PDF-, DOC-, XLS-Anhängen usw.) und wenn man in Outlook auf den "Sende"-Knopf drückt, wird man gefragt ob man "normal" oder "verschlüsselt" versenden will - danach geht alles automatisch. Der Empfänger bekommt die E-Mail in einem „PDF-Umschlag“ (256 Bit AES verschlüsselt) und kann diese PDF mit dem Passwort öffnen, welches einmal (beim ersten Mal) für ihn vom SPECTRUM-System erstellt wird. In einer zentralen Datenbank auf dem SPECTRUM-System werden alle Empfänger-Passwörter gespeichert und automatisch verwaltet. Dieses Passwort gilt für alle E-Mails und für alle Arbeitsplätze des Absenders für diesen E-Mail-Empfänger (es sei denn, dass man dies in einem Web-Portal auf Wunsch des Kunden ändert).

Die zentrale eMail-Verschlüsselung SPECTRUM-PDF-Mail kostet monatlich nur **4,50 €** +USt für beliebig viele E-Mails und beliebig viele Benutzer.

Nachfolgend wird die Funktionsweise eines solchen Container-Verschlüsselungs-Verfahrens anhand des **SPECTRUM-PDF-Mail**-Verfahrens erklärt. Mit SPECTRUM-PDF-Mail ist es möglich, eine verschlüsselte E-Mail an beliebige Empfänger zu verschicken, ohne sich darüber Gedanken machen zu müssen, ob der Empfänger eine E-Mail-Verschlüsselungssoftware benutzt. Wie der Name PDF-Mail schon sagt, basiert das Container-System in dem die komplette E-Mail mit allen Anhängen usw. verschickt wird auf dem Dokumentenaustauschformat PDF. PDF bietet die Möglichkeit Dateien einzubetten und alles mit AES 256 sicher zu verschlüsseln und mit einem Passwort zu versehen.

Diese PDF-Containertechnik wird bei SPECTRUM-PDF-Mail genutzt und dieses kann auf allen Betriebssystemen – sei es nun Windows, Linux, Mac und auf iPhone/Androide-Smartphones – gelesen werden.

Hinweis: Leider unterstützt Apple auf seinen Geräten (iMac, Macbook, iPhone, iPad) standardmäßig nicht die aktuelle Verschlüsselungstechnik AES 256 in PDF Dateien. Diese ist jedoch notwendig, um die Anforderungen der EU-DSGVO zu erfüllen. Der einfachste Weg verschlüsselte PDF-Mails auf Apple-Geräten lesen zu können ist, dass man sich den aktuellen und kostenlosen Adobe Acrobat Reader herunterlädt. Damit lassen sich dann auch auf Apple-Geräten PDF-Mails problemlos öffnen.



Vorgehensweise: Sie schreiben ganz normal eine E-Mail in Ihrem Outlook – wie Sie es schon immer gemacht haben: Sie tragen die Empfänger in „An“, „CC“ und „BCC“ ein, Sie geben einen Betreff an, Sie fügen beliebige Anhänge hinzu. Sie schreiben einen Text – und wenn Sie fertig sind, klicken Sie wie gewohnt auf den Schalter „Senden“. Nun geht ein Fenster auf und fragt, ob sie verschlüsselt oder unverschlüsselt versenden wollen. Das war‘s schon! Auf Ihrer Absenderseite bleiben Ihre Mails unverschlüsselt, Sie können sie normal verwalten und archivieren. Sie brauchen sich auch keine Passwörter merken. Sie müssen auch keine Passwortverwaltung aufbauen, wenn die Passwörter einmal geändert werden. Für alle Mails aus Ihrer Kanzlei, aus Ihrem Betrieb an die gleiche Empfänger-Mail-Adresse gilt immer das gleiche Passwort – es sei denn, sie wollen es einmal ändern (über das SPECTRUM-NET-Web-Portal).

Im Anschluss erhalten Sie einen Sendebericht als Versand-Bestätigungs-Mail mit dem vom System zentral vergebenen Passwort.

Die Übergabe des Passwortes sollte datenschutztechnisch natürlich auf einem anderen Kommunikationsweg erfolgen als der Versand der PDF-Mail, z.B. telefonisch, per Fax, per SMS oder per Brief.

Noch einfacher geht heute Ende-zu-Ende-E-Mail-Verschlüsselung nicht mehr!

4. Datenaustausch via Portal bzw. gesichertem Cloud-Speicher

Bei der E-Mail-Verschlüsselung muss besonders negativ bewertet werden, dass - wenn man selbst auch verschlüsselte Mails erhält - man nie weiß welcher „Schmutz“ da ggfs. „mitverpackt und zugeschickt“ wird, gemeint sind hier Viren, Trojaner und sonstige Schadcodes. Hier haben sich über Internet-Portale erreichbare, Viren-gesicherte und Zugriffs-gesicherte Cloud-Speicher als Datendrehscheiben bewährt.Sicher sind solche Cloud-Speicher wie DropBox, Apples iCloud, Microsoft-OneDrive, Google-Drive, WeTransfer und sonstige Filesharing-Lösungen bekannt. Deren Speicher liegen aber fast alle außerhalb Deutschlands bzw. außerhalb der EU, so dass auf Grund der fehlenden Rechtssicherheit bzgl. der Datenschutzgesetzgebung eine geschäftliche Nutzung nicht angebracht ist. Außerdem verbietet die AO 146 (Abgabenordnung) die Aufbewahrung von geschäftlichen Unterlagen außerhalb Deutschlands bzw. man braucht eine Einzelgenehmigung des jeweiligen Finanzamtes.

Außerdem sind diese Cloud-Speicher oft auch Viren-Schleudern, d.h. von der einen Seite werden Dateien hochgeladen und huckepack wandern Viren und Trojaner mit, die auf der anderen Seite dann nach dem Herunterladen ihr Unheil anrichten. Außerdem sind die täglichen IT-Newsticker voll davon, dass diese Cloud-Speicher wieder einmal gehackt wurden und 1000e von Passwörtern entwendet wurden.

Unter Datenschutz-Gesichtspunkten kann man klar festhalten, dass unter Berücksichtigung des § 203 StGB und des § 146 AO für Steuerberater die Nutzung von solchen Cloud-Speichern in ausländischen RZs bzw. bei US-Firmen mit amerikanischer Rechtslage und somit US-Geheimdienstezugriff wie bei Drop-Box, Apples iCloud, Microsoft-OneDrive, Google-Drive usw. nicht gestattet ist!

4.1 Datenaustausch via SPECTRUM-WEB-Tresor

Hier bietet SPECTRUM z.B. als Alternative zur klassischen E-Mail-Übertragung die Portal-Lösung **SPECTRUM-WEB-Tresor** an. Hier kann der Zugriff einfach mit Login + Passwort oder hochgesichert mit einem Token erfolgen. Außerdem können die Dateien im WEB-Tresor zusätzlich mehrstufig verschlüsselt werden. Sie können so z.B. absolut sicher Ihrem Mandanten über den SPECTRUM-WEB-Tresor als Cloud-basierte sichere Datendrescheibe die sensiblen Daten für die Lohn- und Gehaltsabrechnung, BWA's, Zwischenbilanzen, Vertragsentwürfe usw. zur Verfügung stellen – eine Übertragung per E-Mail wäre hierfür viel zu unsicher.

Dieses Verfahren kann auch als eines der wenigen Systeme bi-direktional vom Mandant genutzt werden und hierüber z.B. Lohnabrechnungs-Zeiterfassungen (Prämien), Arbeitsverträge, ESt-Belege, Notarverträge usw. absolut vertraulich zur Verfügung gestellt werden. Und damit keine Viren mitwandern, wird der SPECTRUM-WEB-Tresor ständig auf Viren gescannt.

Der SPECTRUM-WEB-Tresor kann auch als kontinuierliche **WEB-Akte** genutzt werden, in die Mandant und Kanzlei chronologisch alle Schriftsätze und Unterlagen eines Vorgangs für den gemeinsamen Zugriff verwalten.

SPECTRUM-WEB-Tresor, -WEB-Akte & WEB-Schließfach

Der SPECTRUM-WEB-Tresor kostet Kanzleien für beliebig viele Mandanten und für beliebig viele WEB-Tresore incl. einem Grundspeichervolumen von 5 GB monatl. **9,50 €** +USt jedes weitere 1 GB kostet 1,00 € p.M. +USt

Eine weitere Anwendung ist das **WEB-Schließfach**, d.h. man verwaltet hier Policen, Verträge, Exposés, Urkunden, Gutachten, Zertifikate usw..

Beim WEB-Tresor kann man auch einfach Dokumente mit seinem SmartPhone „abknipsen" oder „mobil scannen" oder sich selbst per E-Mail zustellen lassen. Immer wenn die Kanzlei oder der Mandant etwas Neues in den WEB-Tresor eingestellt hat, klickt man einen Button und schon wird die andere Seite sofort darüber informiert. Der Vorteil für Kanzleien besteht darin, dass man über ein einfaches Portal alle Mandanten-Tresore übersichtlich verwalten kann. So lassen sich beispielsweise mittels des SPECTRUM-WEB-Tresors Dateien mit einem größeren Speichervolumen problemlos über das Internet austauschen. Dieses Vorhaben würde mit einer E-Mail aufgrund von Größenbeschränkungen meistens scheitern.

4.2 Datenaustausch via DATEV-CloudBox

Funktionell ist die neue DATEV-CloudBox teilweise vergleichbar mit dem SPECTRUM-WEB-Tresor. Auch dieser DATEV-Cloud-Speicher wird kontinuierlich auf Viren geprüft. Wie SPECTRUM-WEB-Tresor ist das Produkt DATEV-CloudBox ausschließlich von Kanzleien bestellbar, Mandanten erhalten den Zugriff auf die DATEV-CloudBox durch ihren Steuerberater. Auch mit der DATEV CloudBox können Kanzleien mit Ihren Mandanten hochsensible Dateien austauschen. Die Nutzung erfolgt online und ortsunabhängig aus der Cloud.

Zur Authentifizierung wird hier immer eine DATEV-SmartCard oder DATEV-SmartLogin verwendet. Auch bei der DATEV-Cloudbox können Dokumente einfach per Drag & Drop hochgeladen werden und eine flexible Raum- und Ordnergestaltung ermöglicht die strukturierte Ablage von Informationen.

Die DATEV-CloudBox ist ein Fremdsystem und die DATEV hat das Produkt bei einer Fa. Dracoon in Lizenz erworben. Die DATEV CloudBox verfügt daher über ein eigenes Rechtemanagement, welches nicht in Verbindung mit der DATEV-Rechteverwaltung steht.

DATEV-CloudBox kostet pro registriertem Benutzer 5,50 € +USt. Mit der ersten Bestellung werden dann 1 GB Speicher verfügbar. Jeder eingetragene Benutzer in der DATEV CloudBox nimmt eine Benutzerlizenz in Anspruch, es gibt kein Lizenzlimit. Die Abrechnung erfolgt monatlich auf Basis der maximalen Anzahl eingetragener Benutzer. Ab dem 4. eingetragenen Benutzer inkl. Administrator erhöht sich das Speichervolumen der DATEV Cloudbox mit jedem weiteren eingetragenen Benutzer, um jeweils 500 MB. Das Speichervolumen ist nicht personengebunden, sondern bezieht sich auf das Gesamtvolumen der DATEV CloudBox. Der Administrator ist von der Berechnung ausgeschlossen. Benötigt man mehr Speicher, muss man ggfs. pro 0,5 GB weitere CloudBoxen à 5,50 € +USt bestellen, auch wenn man ggfs. keine weitere CloudBox benötigt.

4.3 Datenübertragung via SFTP-Server

Manche Steuerberater betreiben auch einen eigenen FTP-Server, auf den Mandanten mit einem FTP-Client gesichert mit dem Secure-File-Transfer-Protocol (SFTP) zugreifen können, um Daten hoch- oder herunterzuladen. Die Datenübertragung durch das Internet ist zwar sicher und es ist die weltweit am meisten genutzte Übertragungstechnik für einen sicheren Transfer von Daten - Berufsgeheimnisträger sollten diese Übertragungstechnik aus Sicherheitsgründen aber nicht Mandanten anbieten, denn der Mandant kann so unbewusst mit Viren, Trojanern usw. auf das Kanzlei-IT-System zugreifen, ggfs. an andere Mandantendaten gelangen, den Kanzlei-Server mit Schadcode infizieren und auch die Windows-Zugriffsverwaltung ist kein sicherer Zugriffsschutz zur Einhaltung der Verschwiegenheitsvorschriften nach § 203 StGB.

Hinweis in eigener Sache:

In dem Schreiben „Hinweise zur E-Mail-Kommunikation“ vom 7. Februar 2019 macht die Bundessteuerberaterkammer (BStBK) „Reklame“ für die Marketing-Initiative „E-Mail MADE IN GERMANY“. Mitglieder dieser Initiative sind u.a. Telekom, T-Online, 1&1, WEB.DE, GMX, Strato (alles Marken der Fa. United Internet) und Freenet. Diese Initiative bietet als Provider standardmäßig eine TLS-Transport-Verschlüsselung und exklusive Mail-Server-Verarbeitung ausschließlich in Rechenzentren in Deutschland nach den deutschen Datenschutzstandards an.

Beim IT-Informationsdienst von HEISE ist nachzulesen, dass die Mitgliedschaft bei dieser Marketing-Initiative „E-Mail MADE IN GERMANY“ ca. 30.000 € kosten soll, aufgrund der laufenden TÜV-Audits. Ein von SPECTRUM eingeholtes Angebot zur Mitgliedsaufnahme für ein solches TÜV-Audit, bewegte sich ebenfalls in dieser Größenordnung plus jährlicher Rezertifizierungskosten. Unter Wikipedia ist ergänzend nachzulesen: „die Initiative könne zwar in der Theorie alle Anbieter aufnehmen, aber in der Realität wird die Teilnahme anderer Anbieter systematisch verhindert“ und man bezeichnet diese Initiative lediglich als Marketing-Luftblase.

Der Chaos-Computer-Club CCC bezeichnet die Initiative „E-Mail MADE IN GERMANY“ in Abwandlung als „Bullshit made in Germany“ und kommentiert „E-Mail made in Germany“ als Mogelpackung: das Transportverschlüsselungs-Verfahren der Initiative sei seit mehr als 10 Jahren als RFC standardisiert und somit würden diese Firmen nur Versäumnisse nachholen. RFC = Request for Comments sind technische und organisatorische Dokumente zum Internet-Aufbau und -Betrieb, die als „Internet-Standards“ weltweit festgeschrieben sind.

Hinweis: bei SPECTRUM ist die TLS-Transport-Verschlüsselung standardisiert und das SPECTRUM-Rechenzentrum befindet sich in Deutschland, genauer in Düsseldorf. Es gelten somit die vollen deutschen Datenschutzstandards und SPECTRUM hält die technischen Vorgaben dieser Marketing-Initiative „E-Mail MADE IN GERMANY“ ein. Das SPECTRUM-NET-System bietet ergänzend sogar eine „Zwangs-TLS-Verschlüsselung“ und geht damit über die Spezifikation der Marketing-Initiative „E-Mail MADE IN GERMANY“ hinaus. Aufgrund der hohen Kosten – für nichts – hat SPECTRUM entschieden, dieser Initiative nicht beizutreten. Wie zu vernehmen ist, befindet sich SPECTRUM damit in „guter Gesellschaft“, denn auch solche vergleichbaren Produkte wie DATEV-net gehören ebenfalls nicht dieser Initiative an.

SPECTRUM COMPUTER-SYSTEMHAUS GMBH
Max-Planck-Str. 17, 40699 Erkrath, Telefon: +49 211 695 602 0, Fax: +49 211 695 602 99, E-Mail: info@spectrum-news.de