

E-Mail Verschlüsselung und elektronische Signatur

Prinzipiell sind Daten, die über das Internet übermittelt werden, leicht von Dritten einsehbar, sofern keine besonderen Vorkehrungen zu deren Verschlüsselung getroffen werden. Es gibt mittlerweile etablierte und relativ einfach anzuwendende Verfahren zur kryptographischen Verschlüsselung von E-Mail und von Internet-Seitenabrufen.

Für E-Mail sind das insbesondere das PGP-Verfahren ("Pretty good Privacy"), und S/MIME. Ein entsprechendes Plugin ist meist kostenlos für die gängigen Internetbrowser bzw. E-Mail-Programme erhältlich.

PGP erlaubt das Verschlüsseln einer E-Mail an einen Empfänger, dessen sogenannter *öffentlicher Schlüssel* bekannt ist. Der Empfänger kann die Nachricht dann mit dem nur ihm bekannten *privaten Schlüssel* lesen.

Um überprüfen zu können, ob eine Nachricht auch wirklich vom angegebenen Absender stammt und auch nicht unterwegs verändert wurde, ermöglicht PGP es, E-Mails elektronisch zu signieren. Hier kann mit dem privaten Schlüssel eine Signatur erzeugt werden, die dann vom Empfänger mit dem öffentlichen Schlüssel des Absenders auf Echtheit getestet werden kann.

Öffentlicher Schlüssel von RA Schmidt

Den zur Verschlüsselung von Mails an mich bzw. zum Überprüfen meiner Signaturen notwendigen öffentlichen Schlüssel können Sie sich hier herunterladen. Des weiteren ist der Schlüssel über PGP-Keyserver verfügbar.

Schlüssel-Fingerprint: 461F 9A2F 2EA4 D283 4814 FD60 5DC8 19DB 0826 4CD3

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.1 (MingW32)

```
mQGIBEJJP98RBACUKqQ2CpQ/aIGcp/uIuSZIfJQHwQkv2NWwJGwP5Iw1z8ad5j8V
PF7cDUKgb7U6h2hrbC2NGmBLxiu8A97Ybx9kXuyRwbpHyXWYG4/AyCptJgfrmbxP
L5tvxiF7L5endaQIcVsTUPHf45G6noKhe1sfwJEORpze3uNtaz0Q+P5zWwCgubPS
rSuR5tYs+yRX7oorHgWI7V0D/3beb2NmG3i juPZbadH4AY5wzWEGDmjWakY6n36D
a/1P172njQ213GWhZmTmYcKHnzYKIuUk jf/0mxtzS/XQNCB7bA0WBDBZy5Oby1s8
+F4tu9vaB0sMt5q+fW6FwXi/Aa/Ct19MplXLY79CQbfWw5fPtDCcEzhT174tv3gG
Xj8XA/4sR8cHWLuuMsLuADHoumx3aL0s+rooj1Yzn67fjE8qEFGy1ZH8kxhER5eS
4SNuthetJIU5NYuVymGwCRPTJ8LGvkrLSneOPoGdKexNmJavgB+aF+k2o2fkuLSP
fcjyya6w0ns6+f+Hd9OIN6187p6d4p2R2gtIc0o5akJdayKnpLRTUmVjaHRzYW53
YWx0IHVuZCB0b3RhcibGcm1lZHJpY2ggU2NobWlkdCAoRC0zNTM5MiBHaWVzc2Vu
KSA8aW5mb0BhbndhbHQt c2NobWlkdC5kZT6I ZAQTEQIAJAUCQk1kdAIBIwUJCWYB
gAYLCQgHAwIDFQIDAxYCAQIEaQIXgAAKCRBdyBnbCCZM00n0AJ9Fkx9iKhjdWWWX
P6N5KZQwB/iAAQCgoOMwT3aLFFMBie65Xn6Nz0l+yv25BA0EQk1ZihAQALR8GmB/
0PQp0PiPqCwYVx62VYY6JLgXNb4sIS7uKR09/8SDw1zIRt1cu8AxkUCAOoxVrHn9
ald4IIsXerBF4RLSLl1kT1okLa9IpTAvXsHyhWeCFD+a0wmmXYJjjzDGRSxW0d1FE
0ZIoXB4HLcbNV4WNFjPkYEXbtwoF3RyAfbmsKgxFRnGCiDQMaQU8Vu7q5RpJpL/H
HuOqtJm5wNSb3XsuqH2PLiIlu0VsaIWwYbFXQVshJ/9NDFbHT81oaAb2+WNAEFp04
RaGr21WBGAIR/oCEP6qT9ijyz/ZM4e3v4ZLhOZcktU1fM4cPCdPPen8WMRPDXlw+
/vp+ospykHuhcrVaFgNL2H+WTEDEKEo7uvdhm3eehyIep9FwqDtZnrqwaH9tRzOm
ckcDcBwdb7BZZk94A69mUwQyy3sQ01TJWmxYeNLHkEVFHZumnVAZMbKHFHItpeSA
```

Rechtsanwalt und Notar Friedrich Schmidt, Giessen: verschlüsselte Mail

Bk6GwWs+/UE9/qY1FdMWyTD5VCZRYnzXl/SBD9rhFVYsYGTbMDx2YQeE2e7vk660
pBpYUNC2OBvmm069NqWu2viNFhh5u/19dnbP8zU2ON164Mo4raLyKTAuUPiGJrSo
HUFBkBRH3cAyDgGTJxag3YHVGnddL58JksDT8i17/w+uKE+iwlqZjLzL6+IJ8UWz
wZSOfBhZPZz/j+J0icD32WJdBX/wKydFN9JvAAMFD/9zjfbZxkAYGrTr4yH7hU3Q
Mq8uoR0Wpuj0Pk03RHFVbTY5b+FXnJUibgw1/TC1gQFIEE00P7gpPcgvB+fMhEZ
sBivagEgFwf22nefq9kEWkthglkCUtx1jyIhKAXBBRC92uVWl9aSa8iGSaA7Lksx
Ib6kCFMNg8bFyp2A4PeEO5UItuDxcCvIrWYxxdDzkH2OpghYDvS45gsOeHxVhdC
pBzaqzsyTL68cdJI6nlf01CxnMqZuX5Xxt6r8HGIVw2rFfxncX85ZHHwfSSva1CP
bNk2ttCFS43S8CAR881h1Uzi5KROon3hEFbewzmk/2K7p6HTIcJLrvl8EsEKHMC
JTProm+PtgJKqAkRpepUKo+BXrcovoOpr8Vy/u/rC3x782EdKzMDBdxfulnAe514
AEjZOgvlYFj3AjdE5+tPDtzvXiZo99XFh7xW3Jjd3onZgTQSEENLK1Qvi0R+KHc
DEEPiE6jp65mXCwWRHxS8fg7xzGo/NGGVsaL9ne/dctqKoP/spp5GEyNraa7kIZz
r37vzaFeuGCGaEk24/x9EgoRwr4QULKpp3/Qn3vygE78Pe5Rf7j51J0ont10OrMy
6MS8s/MUIL04mj+VKbBvHc0DQFsQsyPGGAsqYLax8msWpWZxm143S8Jwdcj2VjTd
78wofdwuOod4ExQW4QfE4hMBBgRagAMBQJCSVmKBQkJZgGAAAOJEF3IGdsIJkzT
hB4AoJwJFt6Y1vm5hBYycBqhP8HdJ2E4AKCGwbxNVOrkiWkRzi8IUDqxC/Aq6Q==
=MU6H

-----END PGP PUBLIC KEY BLOCK-----

Programmempfehlung

Ich empfehle Ihnen das E-Mail-Programm *Mozilla Thunderbird* in Verbindung mit der Erweiterung Enigmail für sichere E-Mail-Kommunikation. Thunderbird gilt als weniger fehleranfällig als Microsofts Outlook, ist zudem Open-Source-Software und lizenzkostenfrei im Internet erhältlich. Eine deutschsprachige Seite zu Thunderbird finden Sie hier.

Für Microsofts Outlook Express ist ebenfalls eine PGP-Erweiterung verfügbar

Beide Erweiterungen basieren auf dem Programm GnuPG, welches eine Open-Source-Implementierung der PGP- und S/MIME-Protokolle darstellt.