EVOLUTION HOSTING
FULL SERVICE PROVIDER

EMail: support@evolution-hosting.eu · Telefon: 0531 26 25 187

ESecuremail

DIE EINFACHE EMAIL VERSCHLÜSSELUNG

Wie Sie derzeit den Medien entnehmen können, erfassen und speichern die Geheimdienste aller Länder Emails ab, egal ob Sie verdächtig sind oder nicht. Die Inhalte von EMails werden dabei an Knotenpunkten wie dem DECIX in Frankfurt direkt mitgelesen, da Emails ohne Verschlüsselung im Klartext verschickt werden. Potentiell kann jeder auf der Strecke vom Absender bis zum Empfänger den Inhalt mitlesen.

Um dies zuverhindern, setzen Provider üblicherweise die SSL und TLS Verschlüsselung des Übertragungsweges ein. Leider hat nicht jeder Provider diese Verschlüsselungen aktiviert und daher können Sie nicht sicher sein, daß Ihre Email verschlüsselt übertragen wurde.

Mit der *ESecuremail* stellen wir Ihnen eine innovative Lösung vor, mit der alle Ihre Emails auf dem gesamten Transportweg verschlüsselt werden können, ohne das Sie Änderungen an Ihren jetzigen Emailprogramm wie Outlook oder Applemail vornehmen müssen.

Dabei ist es egal, ob der fremde Provider eine SSL/TLS Verschlüsselungen einsetzt oder nicht. Der Inhalt einer Email wird von uns immer verschlüsselt transportiert, wenn der Öffentliche Schlüssel des Empfängers bekannt ist.

Zum Einsatz kommen in der verwendeten GPG Einheit folgende asymetrische PublicKey-Verfahren:

RSA, RSA-E, RSA-S, ELG-E, DSA u.a. mit AES Verschlüsselung.

Da unsere Server alle über die TLS Anbindung verfügen, können Sie Ihre Emails dann sicher vom Server zu Ihrem Emailprogramm übertragen und lesen. Das gleiche gilt auch für das Absenden von Emails.

Mit minimalen Aufwand zur sicheren Kommunikation.

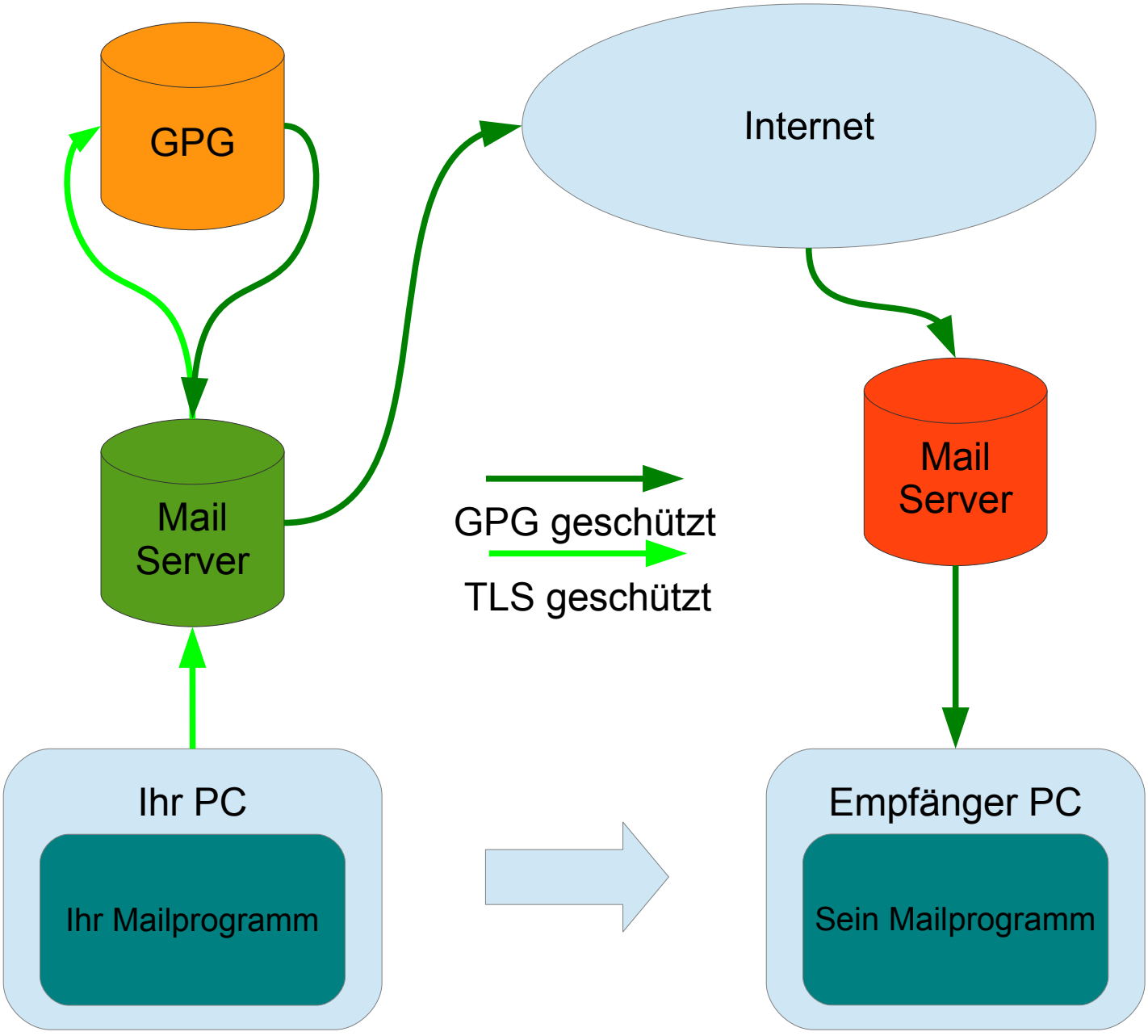
EVOLUTION HOSTING
FULL SERVICE PROVIDER

EMail: support@evolution-hosting.eu · Telefon: 0531 26 25 187

ESecuremail

DIE EINFACHE EMAIL VERSCHLÜSSELUNG

Verschlüsseln: Wie funktioniert das eigentlich ?



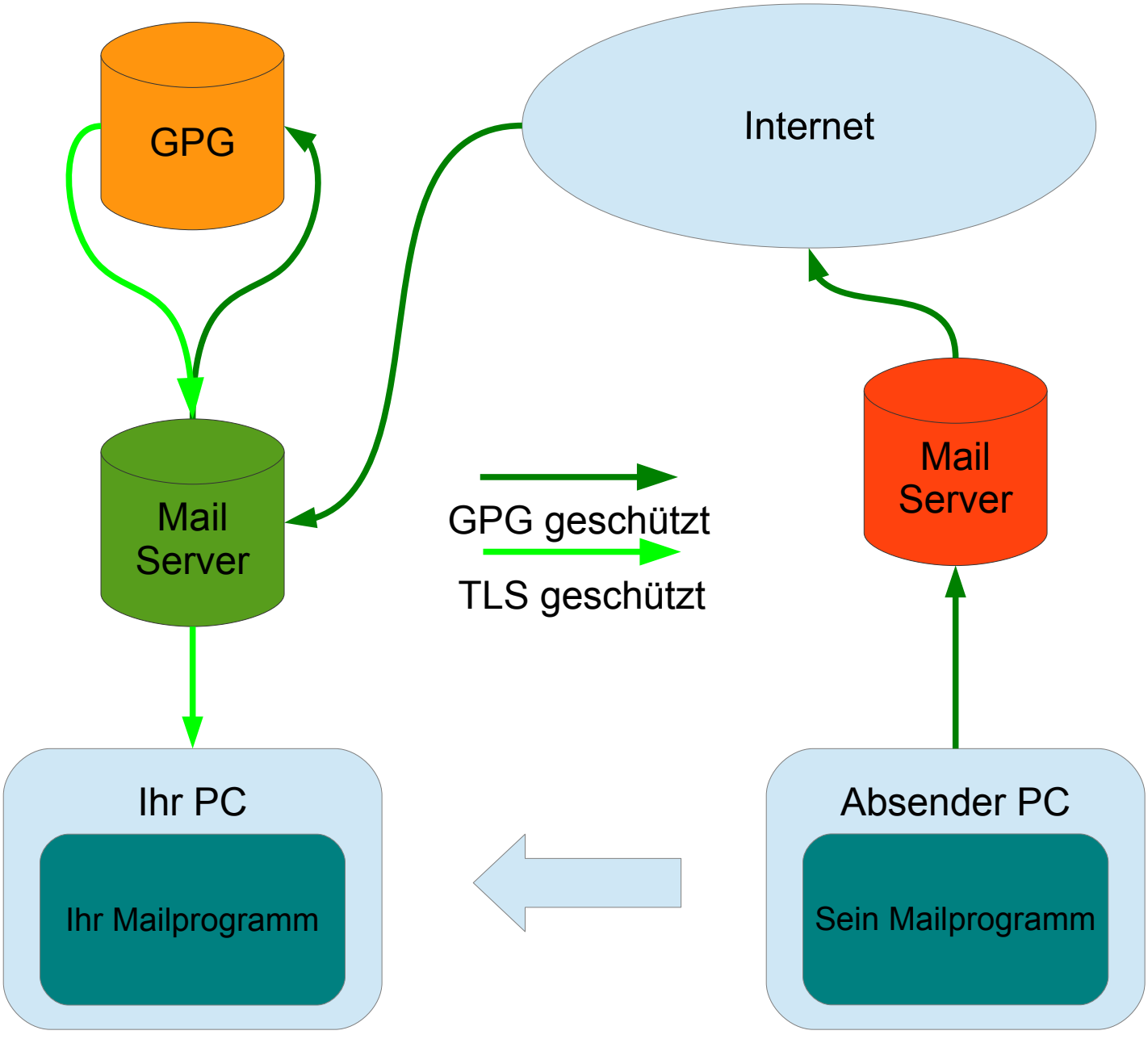
EVOLUTION HOSTING
FULL SERVICE PROVIDER

EMail: support@evolution-hosting.eu · Telefon: 0531 26 25 187

ESecuremail

DIE EINFACHE EMAIL VERSCHLÜSSELUNG

Entschlüsseln: Wie funktioniert das eigentlich ?



EVOLUTION HOSTING
FULL SERVICE PROVIDER

EMail: support@evolution-hosting.eu · Telefon: 0531 26 25 187

ESecuremail

DIE EINFACHE EMAIL VERSCHLÜSSELUNG

Was müssen Sie tun, damit Emails verschlüsselt werden ?

Sie müssen lediglich einmal den öffentlichen Schlüssel Ihres Emailpartners in der Verwaltungsoberfläche zusammen mit seiner Emailaddresse einspeichern. Danach erfolgt automatisch eine Verschlüsselung, sobald Sie eine Email verschicken.

Gilt das auch für Webmail und mein Handy ?

Ja, das gilt auch wenn Sie Webmail einsetzen oder wenn Sie eine Email per Handy schicken, solange Sie dazu das Konto auf unserem Server benutzen.

Was muß ich tun, damit ich verschlüsselte Emails empfangen kann ?

Sie müssen einmal in der Verwaltungsoberfläche einen Schlüssel für Ihr Postfach erstellen lassen. Dieser Vorgang benötigt lediglich etwas Zeit um einen sicheren Schlüssel zu erstellen. Danach geben Sie den erstellten Schlüssel einfach per Email an die Personen weiter, die Ihnen verschlüsselte Emails schicken können sollen.

Ein Partner kann mir keine verschlüsselten Emails senden, da er nicht über PGP oder GPG verfügt. Kommen die Emails trotzdem an ?

Ja, natürlich können Sie weiterhin unverschlüsselte Emails empfangen und senden.

Gibt es Alternativen zu einer Serververschlüsselung ?

Ja, für alle gängigen Betriebssysteme gibt es Desktopanwendungen, welche die Verschlüsselung für denjenigen vornehmen können. Dabei wird der Inhalt der Email per Copy&Paste von einem Programm zum anderen Übertragen und dann verschlüsselt versendet.

EVOLUTION HOSTING
FULL SERVICE PROVIDER

EMail: support@evolution-hosting.eu · Telefon: 0531 26 25 187

ESecuremail

DIE EINFACHE EMAIL VERSCHLÜSSELUNG

Ist die ganze Email mit Betreff verschlüsselt ?

Nein, lediglich der Inhalt der Email ist verschlüsselt. Der Betreff und Absender und Empfänger müssen unverschlüsselt bleiben, da die Email sonst nicht zugestellt werden kann.

Kann ich auch Anhänge schicken ?

Ja, der Inhalt der Email ist egal. Die Größe der Email insgesamt ist auf 50 MB begrenzt.

Was passiert, wenn ich eine Weiterleitung zu einem anderen Postfach vornehme ?

Die Email kommt in diesem Postfach verschlüsselt an. Sie können Sie dort nicht lesen, aber bspw. als Langezeitarchiv lagern. Sobald Sie die Email wieder an Ihre eigentliches Postfach senden, wird Sie entschlüsselt.

Wie lange sind die Schlüssel gültig ?

Die Schlüssel sind 2 Jahre gültig.

Was muß ich danach machen ?

Sie löschen den Schlüssel und legen einen neuen für das Postfach an. Den neuen PublicKey schicken Sie Ihren bisherigen Kontakten zu.

Warum nur 2 Jahre ?

Es ist nicht möglich einen Schlüssel für ungültig zu erklären, außer er läuft ab. Daher die kurze Zeitspanne.

ESecuremail

DIE EINFACHE EMAIL VERSCHLÜSSELUNG

Wie sieht so ein PublicKey eigentlich aus ?

So kann ein PublicKey aussehen. Die Version hängt vom erstellenden Programm ab:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.13 (GNU/Linux)

mQINBFHep0gBEAC8bFP7yzUbkeVz7L/BnYvB25wNG6IfjnU/EKHATK/73jBpo2hG
3LX+SsNDKV+PlPtRBvUIR3/Y8EMnATL8vVHiCcCsRSdrqsVzwfqEzwuux2VALeLm
XXaseOm9iFO9Zyv4mf+4zhEsw8L2dBWUoy93sTRV4VIe05/N7RndrQFxyoTT1lms
9SSJq9LeZaEtzOXoEGrm0fvNoOEeOXal0Z+mgdbjIrmztI0ElgBXGK70D5ix0AWi
+xgkuvou0bg22sNVL0QZM9ZNLDq1+wEExR0G/JEexJ98mAP4EJlrQ6r4iTrXAJa3
2hI4cJW2Gl+mzTqWftU04Uo0uB6rxbp4s9A24lTyVvKqcRQc9sEWbyQQdQvuijHs
WH/xNG+h8iOpVHxIBIDLsHyrueD1wkmDVEjMuV3wSpWeJG1P3wpxRBZACbtilhbR
kFgMf/i6kDO7yk7keg1iMHtVrfDjxX2KxfQoB9LmRm5iynVijKpLDSjFkvwG1mIr
f0o8nJYLjYK/TqgY1aXR+kJMJNXozOwq6u6tdU6MOD7QAoDkhyEB653HaxPGA2Rv
A6rW5FFoknqLnmWwvyTu6QV0ph9CTssWEyqfnP8ClaPuen7bxTOXaboH7gEUYmGf
KjxZqHk3KHRVm2prYDfq0Da8i67/KYqQD94dps3mSeTWqoULzASr74VrvwARAQAB
tCRNYXJpdXMgU2Nod2FyeiA8cml2ZXIyQGNsb3VkLWZvby5kZT6JAj4EEwECACgF
AlHep0gCGy8FCQPCZwAGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJEIdw6tmq
j6ZBYbkP+wYD4onwgtTEY6RMnEAkN3bqfO6Gaa7qn/6c7Mi1Smj1IWHoPX9wAAhn
8gGEmRDR1M4oxEzCEMnIyxpwvmMP6uOYblNlwkX8uiZtaprBeNSjaUZvbnzVBGBa
RyjrzlbWQyCQEIPyD+dMVe8WjytAC2d9DHlFEf+k2A2VLq1Jtayiy3GL9+juA5zv
uOoKdfYy8n3q2SkHnRUaeF/zYrHfdMIZsQv1Ejq2ZaPlNfIRkEhgMbTMqRPKuHVS
xjH43GDEkXfNZsamjg+OSfZDIj+FPAGDF03b+Oa2duzS0oOfXxDkGSL3Ox32yonT
I18Wif6ovgUKLVBEj+UPrwfg388jd6Z2BWHfr4bbTXwAlVpr0ZM06rjX5p7d5zCl
HwElvKgWajxKTMP9Zcf+DFXQnlxYz5+zDKlX3wxyNxQi93dSVVVoYPNgzFm4WnLZ
MucPi4Eu4Uk1B4Erab/SeKrxdaRAvJjcgOFqc8UubZxfItFxo4dsS0J9Kh5RREQN
zYR1IjQD6lZa5OKKO1BYw0OPkqs65QRkPIKpIjoECE6LRcDQkwbBxakeMcQDa3Z0
h48wBaspD9jiL7Q+1gII10nAI+FXHSWrq77nwgWf9IU2vibPmmbhMmWiAxz0lQHK
D6CCuPhGqW6+Ct0y+4K3s58eiuVb1CuqMLRztImotGzhXjwF3K90
=3+9v
-----END PGP PUBLIC KEY BLOCK-----

Lediglich der Inhalt zwischen „BEGIN PGP“ und „END PGP“ unterscheidet sich für verschiedene Schlüssel.

EVOLUTION HOSTING
FULL SERVICE PROVIDER

EMail: support@evolution-hosting.eu · Telefon: 0531 26 25 187

ESecuremail

DIE EINFACHE EMAIL VERSCHLÜSSELUNG

Wie aktiviere ich die Verschlüsselung eigentlich ?

Sie müssen die Verschlüsselung nicht aktivieren, dies erledigt der Server automatisch, wenn Sie eine normale Email an jemanden verschicken für den ein Schlüssel hinterlegt ist.

Wenn Ich von einem meiner Konten an ein anderes meiner Konten eine Email schicke, was passiert dann ?

Solange die Konten auf dem gleichen Server sind, wird die Email innerhalb des Servers unverschlüsselt in das Poastfach des Empfängers geschrieben.

Wenn das empfangende Konto auf einem unserer anderen Server ist, wird die Email normal verschlüsselt und dort wieder entschlüsselt. Dies setzt natürlich für beide Konto die aktivierte GPG Verschlüsselung vorraus.

Kann nicht jeder mit meinem Schlüssel auch meine Nachrichten lesen ?

Nein. Der Public Key ist nur ein Teil eines Asynchronen Verschlüsselungs-algorithmuses. Zum Entschlüsseln kann man nur den privaten Schlüssel benutzen und dieser liegt sicher auf unserem Server.

Kann man die Sicherheit noch steigern, was passiert denn wenn jemand den Server klaut ?

Ja, die Sicherheit kann durch eine weitere Verschlüsselungsschicht des Server noch erhöht werden. Dazu wird das Verzeichnis mit den Emails und die dazu gehörigen Schlüssel in einer verschlüsselten Festplattenpartition gespeichert. Sollte der Server tatsächlich geklaut werden, sind die Emails geschützt.

ESecuremail

DIE EINFACHE EMAIL VERSCHLÜSSELUNG

Das Verschlüsselungsverfahren AES

Der Advanced Encryption Standard (AES) ist ein symmetrisches Kryptosystem, das im Oktober 2000 vom National Institute of Standards and Technology (NIST) als Standard bekanntgegeben wurde. Nach seinen Entwicklern Joan Daemen und Vincent Rijmen wird er auch Rijndael-Algorithmus genannt.

Der Rijndael-Algorithmus besitzt eine variable Blockgröße von 128, 192 oder 256 Bit und eine variable Schlüssellänge von 128, 192 oder 256 Bit. Rijndael bietet ein sehr hohes Maß an Sicherheit; erst mehr als 10 Jahre nach seiner Standardisierung wurde der erste, theoretisch interessante, praktisch aber nicht relevante Angriff gefunden. AES schränkt die Blocklänge auf 128 Bit ein, während die Wahl der Schlüssellänge von 128, 192 oder 256 Bits unverändert übernommen worden ist.

AES ist in den USA für staatliche Dokumente mit höchster Geheimhaltungsstufe zugelassen [1].

Quellen:

[1] U.S. Committee on National Security Systems (CNSS), *National Policy on the Use of the* Advanced Encryption Standard (AES) to Protect National Security Systems and National *Security Information*, CNSS Policy No. 15, Fact Sheet No. 1, June 2003, available at
http://csrc.nist.gov/groups/STM/cmvp/documents/CNSS15FS.pdf