PGP — Grundlagen und Anwendung

Peter J. Holzer

15. September 2001

Überblick

- Wozu Kryptographie?
- Funktionsweise
- PGP-Varianten
- PGP User Interface
- Keymanagement
- Keyserver
- mutt
- RPM

Kryptographie wozu?

1. Nachrichten verschlüsseln (encrypt)

2. Nachrichten unterschreiben (sign)

1. Wie?

Alles ist irgendwann crackbar!

Aufwand zum Cracken und Lebensdauer der Nachricht sind die entscheidenden Punkte.

⇒ Das Cracken der verschlüsselten Nachricht muß gerade länger dauern, als die Nachricht nützlich sein kann.

Funktionsweise

2. Symmetrische Verfahren

Verwenden *einen* Key zum *Ver*schlüsseln und *Ent*schlüsseln.

DES, 3-DES, IDEA, . . .

3. Asymmetrische Verfahren

Verwenden *zwei* Schlüssel (öffentlich, privat)

RSA

4. Hashes

Bilden eine (eindeutige) Prüfsumme.

MD5 (128 bit), Unix-Password-Crypt (12 + 66 bit)

PGP Verschlüsselung

Die Nachricht selbst wird

1. komprimiert
2. mit *symmetrischem* Verfahren (IDEA, 3DES, ...) verschlüsselt

Der IDEA Key wird mittels *asymmetrischem* Verfahren (RSA, ElGamal, ...) verschlüsselt

Kein Problem, da symmetrisches Verfahren „stärker“ als asymmetrisches.

Verschlüsselung für mehrere Empfänger: Der symmetrische Key wird für jeden Empfänger verschlüsselt.

PGP Signaturen

Default Signatur (nicht direkt lesbar)

Klartextsignatur

1. Nachricht wird komprimiert (nur für Default Signatur)

2. Über die Nachricht wird eine MD5 Prüfsumme gebilded

3. Die MD5 Prüfsumme wird RSA signiert

PGP-Varianten

	PGP 2.x	PGP 5+	GPG
Asymm.	RSA	RSA, El-Gamal, (...?)	RSA, El-Gamal, ...
Symm.	IDEA	IDEA, 3DES, (...?)	3DES, ...
Hash	MD5	MD5, SHA1, (...?)	MD5, SHA1, RIPEM160
Plugins	nein	nein	ja
Lizenz	MIT	„non-commercial use“ gratis	GPL

PGP User Interface

- Commandline-orientiert
- Interaktiv vs. Batchanwendung
  - Abfrage fehlender Parameter
  - Passphraseabfrage
  - ausführliche Meldungen
  - `-f` und `PGPPASSFD`

GPG Userinterface

```
% gpg --help
gpg (GnuPG) 1.0.6
Copyright (C) 2001 Free Software Foundation, Inc.
[...]
Home: ~/.gnupg
Unterstützte Verfahren:
Cipher: 3DES, CAST5, BLOWFISH, RIJNDAEL, RIJNDAEL192, RIJNDAEL256, TWOFISH
Pubkey: RSA, RSA-E, RSA-S, ELG-E, DSA, ELG
Hash: MD5, SHA1, RIPEMD160

Aufruf: gpg [Optionen] [Dateien]
Signieren, prüfen, verschlüsseln, entschlüsseln
Die voreingestellte Operation ist abhängig von den Eingabedaten

Befehle:

 -s, --sign [Datei]              Eine Unterschrift erzeugen
     --clearsign [Datei]         Eine Klartextunterschrift erzeugen
 -b, --detach-sign               Eine abgetrennte Unterschrift erzeugen
 -e, --encrypt                   Daten verschlüsseln
 -d, --decrypt                   Daten entschlüsseln (Voreinstellung)
 [...]
```

PGP Userinterface

Was?

- -e textfile her_userid [other userids]
- -s textfile [-u your_userid]
- ciphertextfile [plaintextfile]

Wie?

- -a (ASCII-Armor)
- -b (detached signature)
- -f (Filter)

Keymanagement

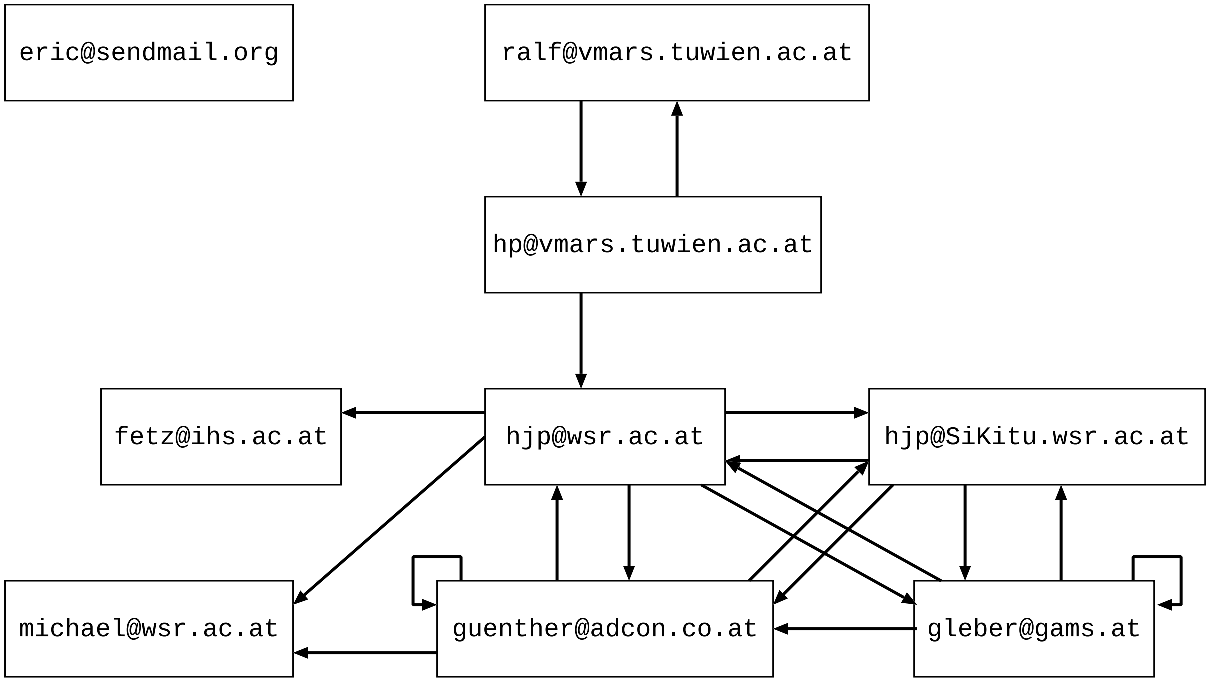
Keyring „Schlüsselbund“ mit allen Schlüsseln.
private — public

Signatures Bestätigung, daß Public Key zu einer Person gehört.

Introductions & Trust Wem glaube ich, wenn er mir jemandem vorstellt.

Web of Trust Transitiv?

Web of Trust


eric@sendmail.org
ralf@vmars.tuwien.ac.at
hp@vmars.tuwien.ac.at
fetz@ihs.ac.at
hjp@wsr.ac.at
hjp@SiKitu.wsr.ac.at
michael@wsr.ac.at
guenther@adcon.co.at
gleber@gams.at

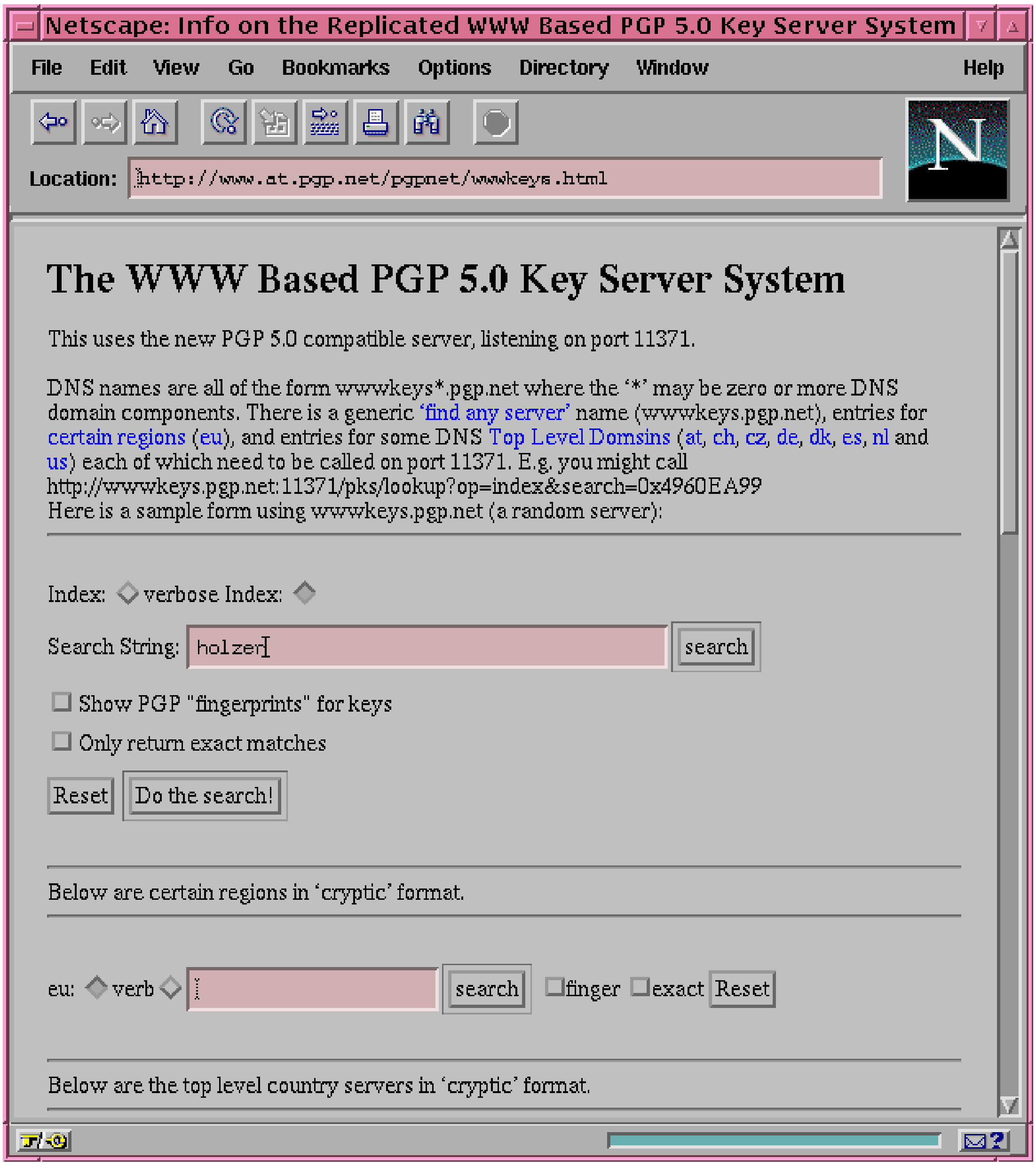
PGP Userinterface: Key Management

```
% gpg --help
[...]
     --list-keys                  Liste der Schlüssel
     --list-sigs                  Liste der Schlüssel und ihrer Signaturen
     --gen-key                    Ein neues Schlüsselpaar erzeugen
     --delete-key                 Schlüssel aus dem öff. Schlüsselbund entfernen
     --sign-key                   Schlüssel signieren
     --lsign-key                  Schlüssel nur auf diesem Rechner signieren
     --edit-key                   Unterschreiben oder Bearbeiten eines Schl.
     --import                     Schlüssel importieren/kombinieren
     --export                     Schlüssel exportieren
     --send-keys                  Schlüssel zu einem Schlü.server exportieren
     --recv-keys                  Schlüssel von einem Schlü.server importieren
```

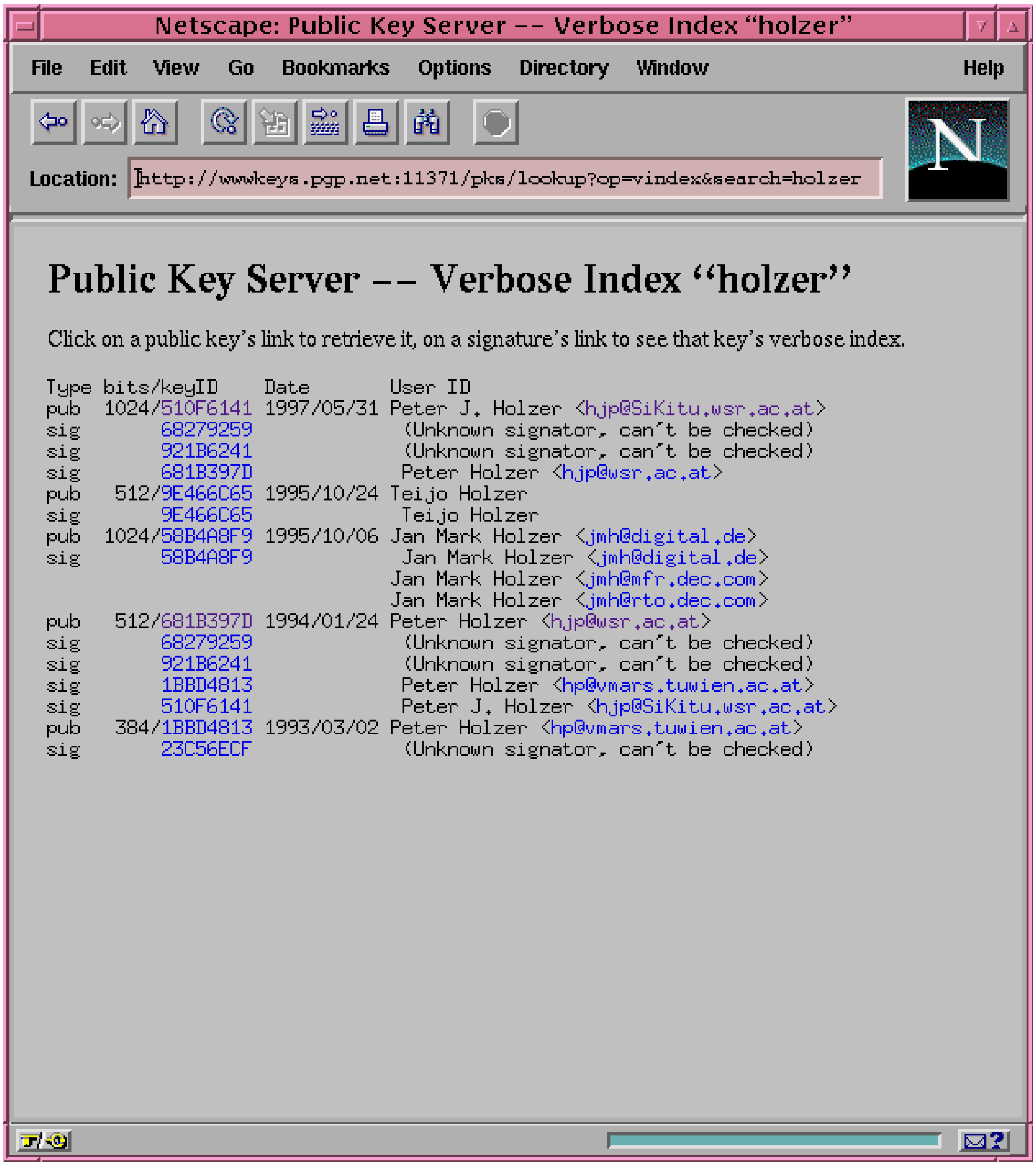
Keyserver

- Netz (mehr oder weniger) synchronisierter Server
- Abfrage über http oder email
- öffentlich, keine Checks

Keyserver


Netscape: Info on the Replicated WWW Based PGP 5.0 Key Server System
File Edit View Go Bookmarks Options Directory Window Help
Location: http://www.at.pgp.net/pgpnet/wwwkeys.html
The WWW Based PGP 5.0 Key Server System
This uses the new PGP 5.0 compatible server, listening on port 11371.
DNS names are all of the form wwwkeys*.pgp.net where the '*' may be zero or more DNS domain components. There is a generic 'find any server' name (wwwkeys.pgp.net), entries for certain regions (eu), and entries for some DNS Top Level Domsins (at, ch, cz, de, dk, es, nl and us) each of which need to be called on port 11371. E.g. you might call http://wwwkeys.pgp.net:11371/pks/lookup?op=index&search=0x4960EA99
Here is a sample form using wwwkeys.pgp.net (a random server):
Index: verbose Index:
Search String: holzer search
Show PGP "fingerprints" for keys
Only return exact matches
Reset Do the search!
Below are certain regions in 'cryptic' format.
eu: verb search finger exact Reset
Below are the top level country servers in 'cryptic' format.

Keyserver



Netscape: Public Key Server -- Verbose Index "holzer"

File Edit View Go Bookmarks Options Directory Window Help

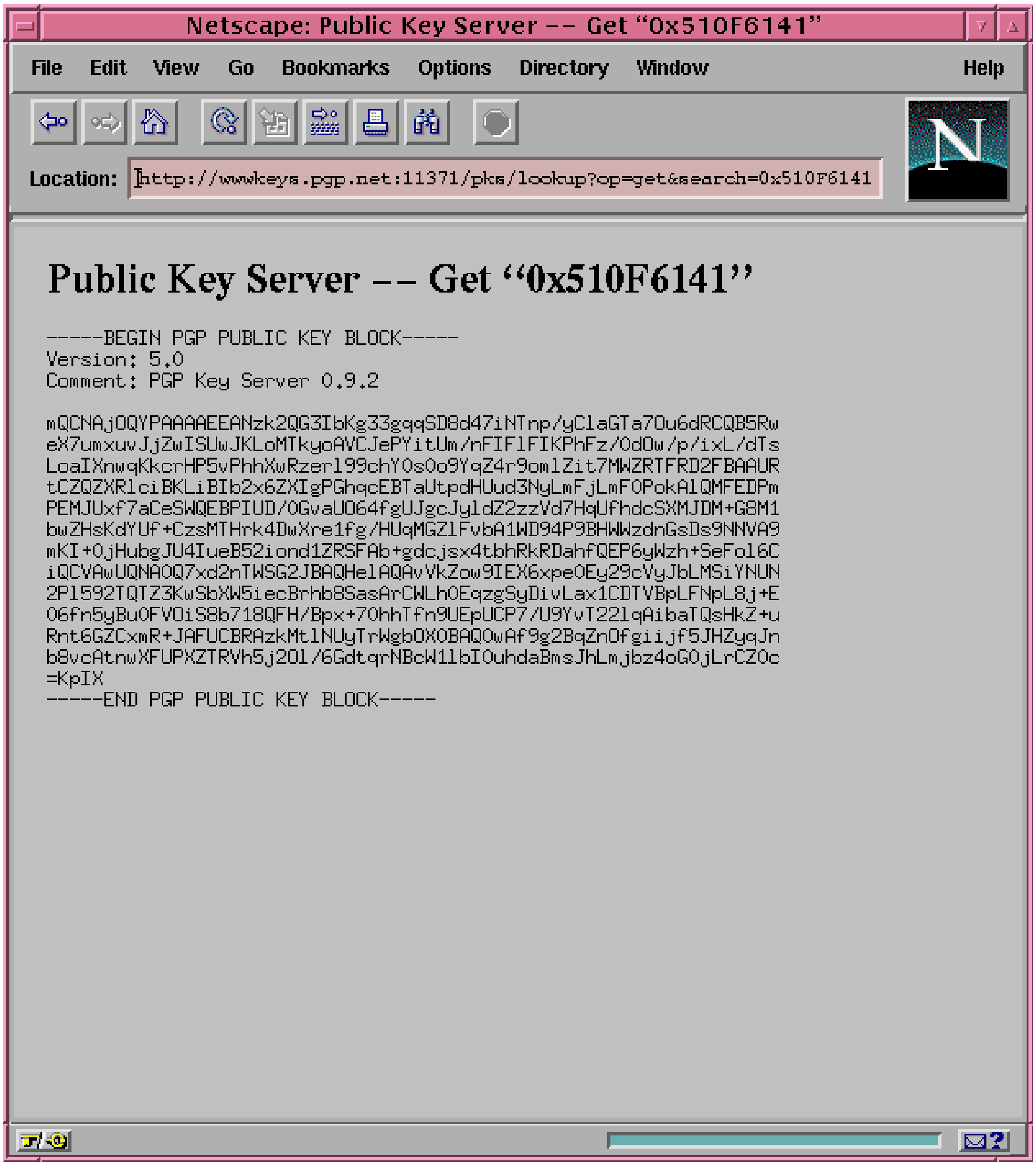
Location: http://wwwkeys.pgp.net:11371/pks/lookup?op=vindex&search=holzer

Public Key Server -- Verbose Index "holzer"

Click on a public key's link to retrieve it, on a signature's link to see that key's verbose index.

```
Type bits/keyID    Date       User ID
pub  1024/510F6141 1997/05/31 Peter J. Holzer <hjp@SiKitu.wsr.ac.at>
sig       68279259             (Unknown signator, can't be checked)
sig       921B6241             (Unknown signator, can't be checked)
sig       681B397D             Peter Holzer <hjp@wsr.ac.at>
pub   512/9E466C65 1995/10/24 Teijo Holzer
sig       9E466C65             Teijo Holzer
pub  1024/58B4A8F9 1995/10/06 Jan Mark Holzer <jmh@digital.de>
sig       58B4A8F9             Jan Mark Holzer <jmh@digital.de>
                              Jan Mark Holzer <jmh@mfr.dec.com>
                              Jan Mark Holzer <jmh@rto.dec.com>
pub   512/681B397D 1994/01/24 Peter Holzer <hjp@wsr.ac.at>
sig       68279259             (Unknown signator, can't be checked)
sig       921B6241             (Unknown signator, can't be checked)
sig       1BBD4813             Peter Holzer <hp@vmars.tuwien.ac.at>
sig       510F6141             Peter J. Holzer <hjp@SiKitu.wsr.ac.at>
pub   384/1BBD4813 1993/03/02 Peter Holzer <hp@vmars.tuwien.ac.at>
sig       23C56ECF             (Unknown signator, can't be checked)
```

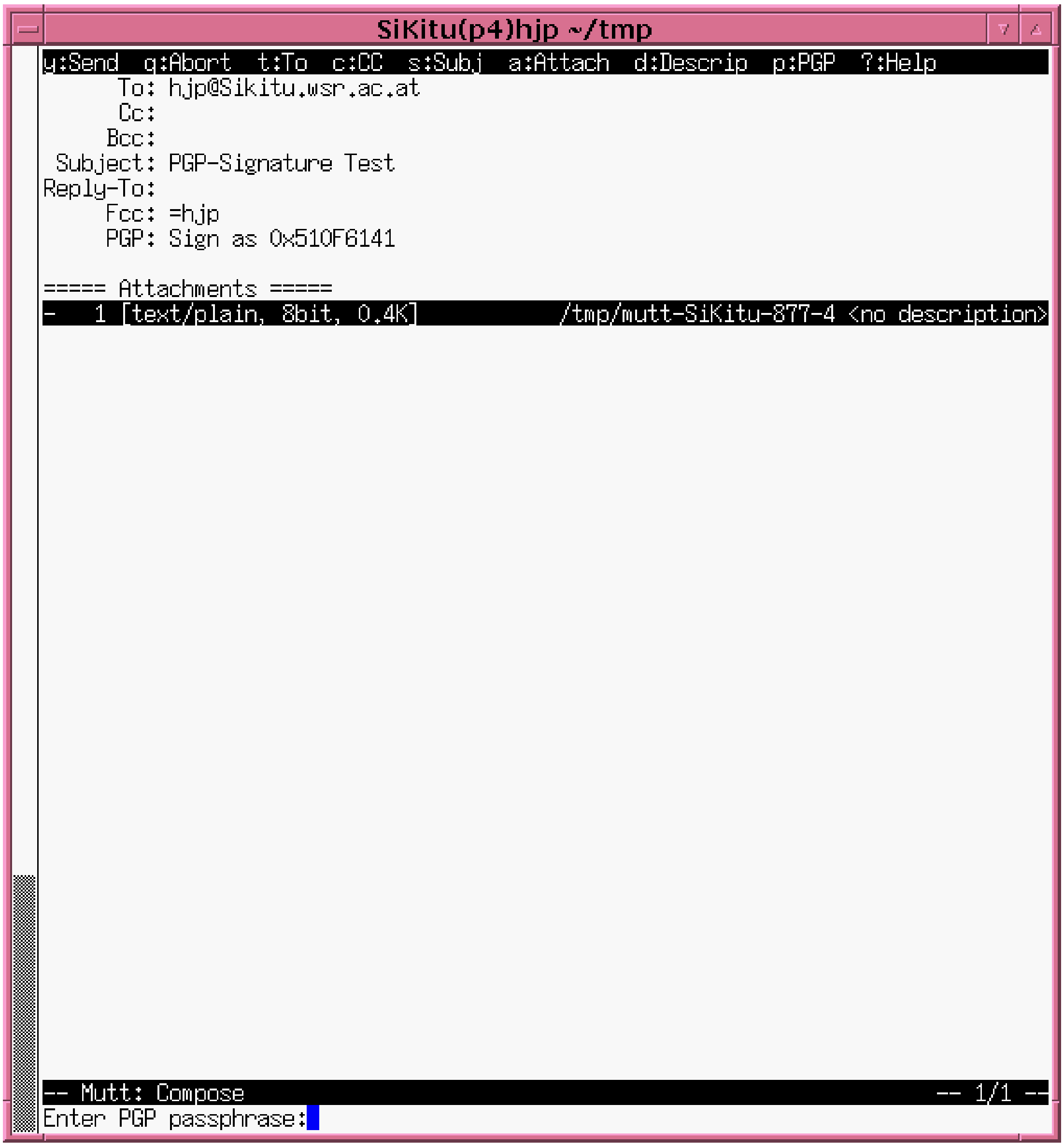
Keyserver


Netscape: Public Key Server -- Get "0x510F6141"
File
Edit
View
Go
Bookmarks
Options
Directory
Window
Help
Location:
http://wwwkeys.pgp.net:11371/pks/lookup?op=get&search=0x510F6141
Public Key Server -- Get "0x510F6141"
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 5.0
Comment: PGP Key Server 0.9.2
mQCNAjOQYPAAAAEEANzk2QG3IbKg33gqqSD8d47iNTnp/yClaGTa7Ou6dRCQB5Rw
eX7umxuvJjZwISUwJKLoMTkyoAVCJePYitUm/nFIFlFIKPhFz/OdOw/p/ixL/dTs
LoaIXnwqKkcrHP5vPhhXwRzerl99chYOsOo9YqZ4r9omlZit7MWZRTFRD2FBAAUR
tCZQZXRlciBKLiBIb2x6ZXIgPGhqcEBTaUtpdHUud3NyLmFjLmFOPokAlQMFEDPm
PEMJUxf7aCeSWQEBPIUD/OGvaUO64fgUJgcJyldZ2zzVd7HqUfhdcSXMJDM+G8M1
bwZHsKdYUf+CzsMTHrk4DwXre1fg/HUqMGZlFvbA1WD94P9BHWWzdnGsDs9NNVA9
mKI+OjHubgJU4IueB52iond1ZRSFAb+gdcjsx4tbhRkRDahfQEP6yWzh+SeFol6C
iQCVAwUQNAOQ7xd2nTWSG2JBAQHelAQAvVkZow9IEX6xpeOEy29cVyJbLMSiYNUN
2Pl592TQTZ3KwSbXW5iecBrhb8SasArCWLhOEqzgSyDivLax1CDTVBpLFNpL8j+E
O6fn5yBuOFVOiS8b718QFH/Bpx+7OhhTfn9UEpUCP7/U9YvT22lqAibaTQsHkZ+u
Rnt6GZCxmR+JAFUCBRAzkMtlNUyTrWgbOXOBAQOwAf9g2BqZnOfgiijf5JHZyqJn
b8vcAtnwXFUPXZTRVh5j2Ol/6GdtqrNBcW1lbIOuhdaBmsJhLmjbz4oGOjLrCZOc
=KpIX
-----END PGP PUBLIC KEY BLOCK-----

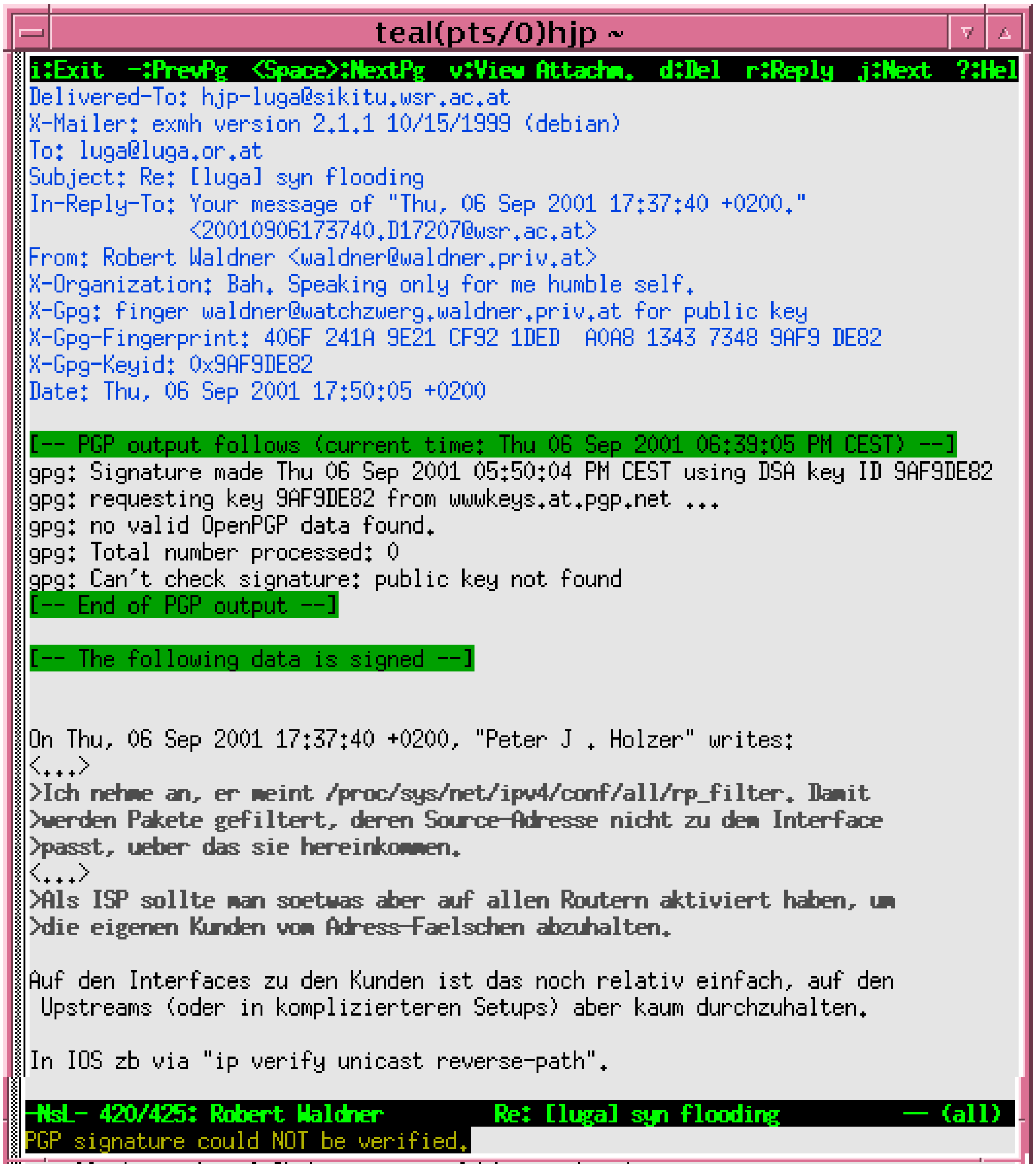
mutt

- Curses-basierter Mailer
- RFC 1847/2015 (Security Multiparts/PGP-MIME)
- Ruft PGP als externes Programm auf
- Gut integriert (keine „Wrapper“-Scripts, Password-Caching)

mutt

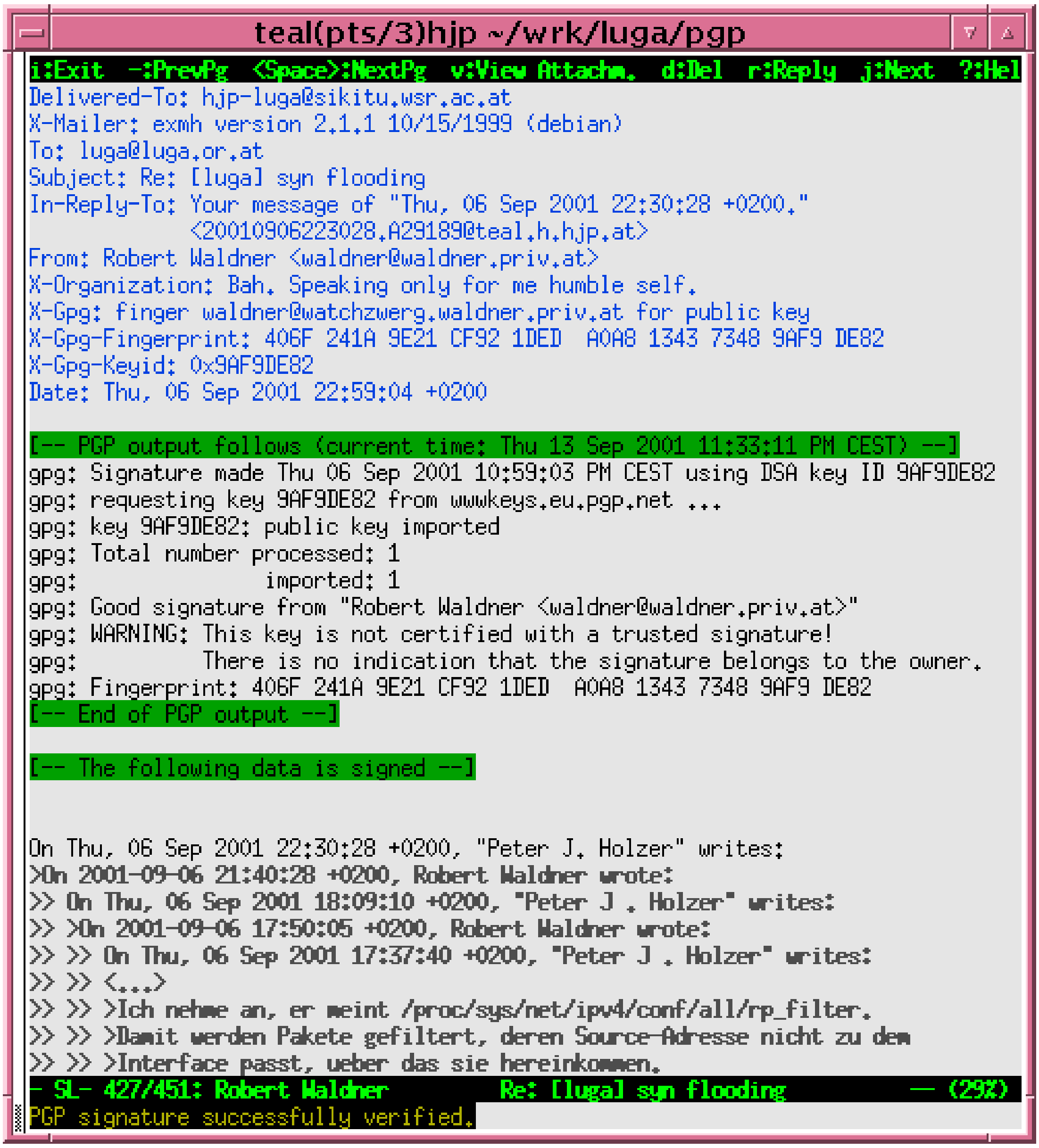

SiKitu(p4)hjp ~/tmp
y:Send q:Abort t:To c:CC s:Subj a:Attach d:Descrip p:PGP ?:Help
To: hjp@Sikitu.wsr.ac.at
Cc:
Bcc:
Subject: PGP-Signature Test
Reply-To:
Fcc: =hjp
PGP: Sign as 0x510F6141
===== Attachments =====
- 1 [text/plain, 8bit, 0.4K] /tmp/mutt-SiKitu-877-4 <no description>
-- Mutt: Compose -- 1/1 --
Enter PGP passphrase:

mutt



```
teal(pts/0)hjp ~
i:Exit  -:PrevPg  <Space>:NextPg  v:View Attachm.  d:Del  r:Reply  j:Next  ?:Hel
Delivered-To: hjp-luga@sikitu.wsr.ac.at
X-Mailer: exmh version 2.1.1 10/15/1999 (debian)
To: luga@luga.or.at
Subject: Re: [luga] syn flooding
In-Reply-To: Your message of "Thu, 06 Sep 2001 17:37:40 +0200."
             <20010906173740.D17207@wsr.ac.at>
From: Robert Waldner <waldner@waldner.priv.at>
X-Organization: Bah. Speaking only for me humble self.
X-Gpg: finger waldner@watchzwerg.waldner.priv.at for public key
X-Gpg-Fingerprint: 406F 241A 9E21 CF92 1DED  A0A8 1343 7348 9AF9 DE82
X-Gpg-Keyid: 0x9AF9DE82
Date: Thu, 06 Sep 2001 17:50:05 +0200

[-- PGP output follows (current time: Thu 06 Sep 2001 06:39:05 PM CEST) --]
gpg: Signature made Thu 06 Sep 2001 05:50:04 PM CEST using DSA key ID 9AF9DE82
gpg: requesting key 9AF9DE82 from wwwkeys.at.pgp.net ...
gpg: no valid OpenPGP data found.
gpg: Total number processed: 0
gpg: Can't check signature: public key not found
[-- End of PGP output --]

[-- The following data is signed --]


On Thu, 06 Sep 2001 17:37:40 +0200, "Peter J . Holzer" writes:
<...>
>Ich nehme an, er meint /proc/sys/net/ipv4/conf/all/rp_filter. Damit
>werden Pakete gefiltert, deren Source-Adresse nicht zu dem Interface
>passt, ueber das sie hereinkommen.
<...>
>Als ISP sollte man soetwas aber auf allen Routern aktiviert haben, um
>die eigenen Kunden vom Adress-Faelschen abzuhalten.

Auf den Interfaces zu den Kunden ist das noch relativ einfach, auf den
 Upstreams (oder in komplizierteren Setups) aber kaum durchzuhalten.

In IOS zb via "ip verify unicast reverse-path".
-NsL- 420/425: Robert Waldner        Re: [luga] syn flooding          -- (all)
PGP signature could NOT be verified.
```

mutt



```
teal(pts/3)hjp ~/wrk/luga/pgp
i:Exit  -:PrevPg  <Space>:NextPg  v:View Attachm.  d:Del  r:Reply  j:Next  ?:Hel
Delivered-To: hjp-luga@sikitu.wsr.ac.at
X-Mailer: exmh version 2.1.1 10/15/1999 (debian)
To: luga@luga.or.at
Subject: Re: [luga] syn flooding
In-Reply-To: Your message of "Thu, 06 Sep 2001 22:30:28 +0200."
             <20010906223028.A29189@teal.h.hjp.at>
From: Robert Waldner <waldner@waldner.priv.at>
X-Organization: Bah. Speaking only for me humble self.
X-Gpg: finger waldner@watchzwerg.waldner.priv.at for public key
X-Gpg-Fingerprint: 406F 241A 9E21 CF92 1DED  A0A8 1343 7348 9AF9 DE82
X-Gpg-Keyid: 0x9AF9DE82
Date: Thu, 06 Sep 2001 22:59:04 +0200

[-- PGP output follows (current time: Thu 13 Sep 2001 11:33:11 PM CEST) --]
gpg: Signature made Thu 06 Sep 2001 10:59:03 PM CEST using DSA key ID 9AF9DE82
gpg: requesting key 9AF9DE82 from wwwkeys.eu.pgp.net ...
gpg: key 9AF9DE82: public key imported
gpg: Total number processed: 1
gpg:               imported: 1
gpg: Good signature from "Robert Waldner <waldner@waldner.priv.at>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
gpg: Fingerprint: 406F 241A 9E21 CF92 1DED  A0A8 1343 7348 9AF9 DE82
[-- End of PGP output --]

[-- The following data is signed --]


On Thu, 06 Sep 2001 22:30:28 +0200, "Peter J. Holzer" writes:
>On 2001-09-06 21:40:28 +0200, Robert Waldner wrote:
>> On Thu, 06 Sep 2001 18:09:10 +0200, "Peter J . Holzer" writes:
>> >On 2001-09-06 17:50:05 +0200, Robert Waldner wrote:
>> >> On Thu, 06 Sep 2001 17:37:40 +0200, "Peter J . Holzer" writes:
>> >> <...>
>> >> >Ich nehme an, er meint /proc/sys/net/ipv4/conf/all/rp_filter.
>> >> >Damit werden Pakete gefiltert, deren Source-Adresse nicht zu dem
>> >> >Interface passt, ueber das sie hereinkommen.
- SL- 427/451: Robert Waldner        Re: [luga] syn flooding            -- (29%)
PGP signature successfully verified.
```

mutt

```
SiKitu(p4)hjp ~/tmp
i:Exit  -:PrevPg  SPC:NextPg  v:Attach  d:Del  r:Reply  j:Next  ?:Help
Date: Tue, 27 Jan 1998 22:00:42 +0100
From: "Peter J. Holzer" <hjp@SiKitu.wsr.ac.at>
To: hjp@Sikitu.wsr.ac.at
Subject: PGP-Encryption Test
X-Mailer: Mutt 0.88
In-Reply-To: <19980127215714.57718@SiKitu.wsr.ac.at>; from Peter J. Holzer on
+Tue, Jan 27, 1998 at 09:57:14PM +0100

[-- PGP output follows (current time: Tue Jan 27 22:00:52 1998) --]

Good signature from user "Peter J. Holzer <hjp@SiKitu.wsr.ac.at>".
Signature made 1998/01/27 21:01 GMT
[-- End of PGP output --]

[-- The following data is PGP/MIME encrypted --]

On Tue, Jan 27, 1998 at 09:57:14PM +0100, Peter J. Holzer wrote:
> Das ist eine signierte Mail.

Das ist eine streng geheime Antwort. Sie ist verschlüsselt und
signiert. Nur der Absender und der Empfänger kann sie lesen.

        hp

--
   _  | Peter J. Holzer             | Lecture by Linus Torvalds:
|_|_) | Sysadmin WSR                |     "World Domination 101"
| |   | hjp@wsr.ac.at               | Lecture by Bill Gates:
__/   | http://wsrx.wsr.ac.at/~hjp/ |     "World Domination 404"

[-- End of PGP/MIME encrypted data --]





-N- 261/261: Peter J. Holzer        PGP-Encryption Test                -- (all)
Invoking PGP...
```

RPM

1. Key von aus *sicherer* Quelle besorgen (CD, Web-Server?, FTP-Server?)

2. % gpg –import RPM-GPG-KEY

3. % gpg –lsign security@redhat.com

RPM

1. % rpm –checksig -v openssl-0.9.5a-7.6.x.i386.rpm
   openssl-0.9.5a-7.6.x.i386.rpm:
   MD5 sum OK: 52d0a49855c85a1cf271ea43431f25c2
   gpg: Signature made Wed 18 Jul 2001 06:40:15 PM CEST
   using DSA key ID DB42A60E
   gpg: Good signature from Red Hat, Inc <security@redhat.com>"

The End

My tragic tale I won't prolong,
Rickety tickety tin,
My tragic tale I won't prolong,
And if you do not enjoy my song,
You've yourselves to blame if it's long,
You should never have let me begin, begin,
You should never have let me begin.

Tom Lehrer: The Irish Ballad

E-Mail: hjp@hjp.at

URL: http://www.hjp.at/publ/pgp/pgp-anwendung-2001.ps.gz

Dank an:
Robert Walder (Organisation Keysigning Party)
Günther Leber (Kryptographie Vortrag 1998)
VIBE (Organisation Workshop)