PGP — Anwendung

Peter J. Holzer

29. Jänner 1998

Überblick

- PGP User Interface
- Keymanagement
- Keyserver
- mutt
- Was noch?
- Was nicht?
- PGP 5

PGP User Interface

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

PGP Userinterface

```
% pgp -h
Pretty Good Privacy 2.6ui - Public-key encryption for the masses.
(c) 1990-1993 Philip Zimmermann, Phil's Pretty Good Software. 27 May 94
Date: 1998/01/24 12:54 GMT

Usage summary:
To encrypt a plaintext file with recipent's public key, type:
   pgp -e textfile her_userid [other userids] (produces textfile.pgp)
To sign a plaintext file with your secret key:
   pgp -s textfile [-u your_userid]           (produces textfile.pgp)
To sign a plaintext file with your secret key, and then encrypt it
   with recipent's public key, producing a .pgp file:
   pgp -es textfile her_userid [other userids] [-u your_userid]
To encrypt with conventional encryption only:
   pgp -c textfile
To decrypt or check a signature for a ciphertext (.pgp) file:
   pgp ciphertextfile [plaintextfile]
To produce output in ASCII for email, add the -a option to other options.
To generate your own unique public/secret key pair:  pgp -kg
For help on other key management functions, type:   pgp -k
```

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

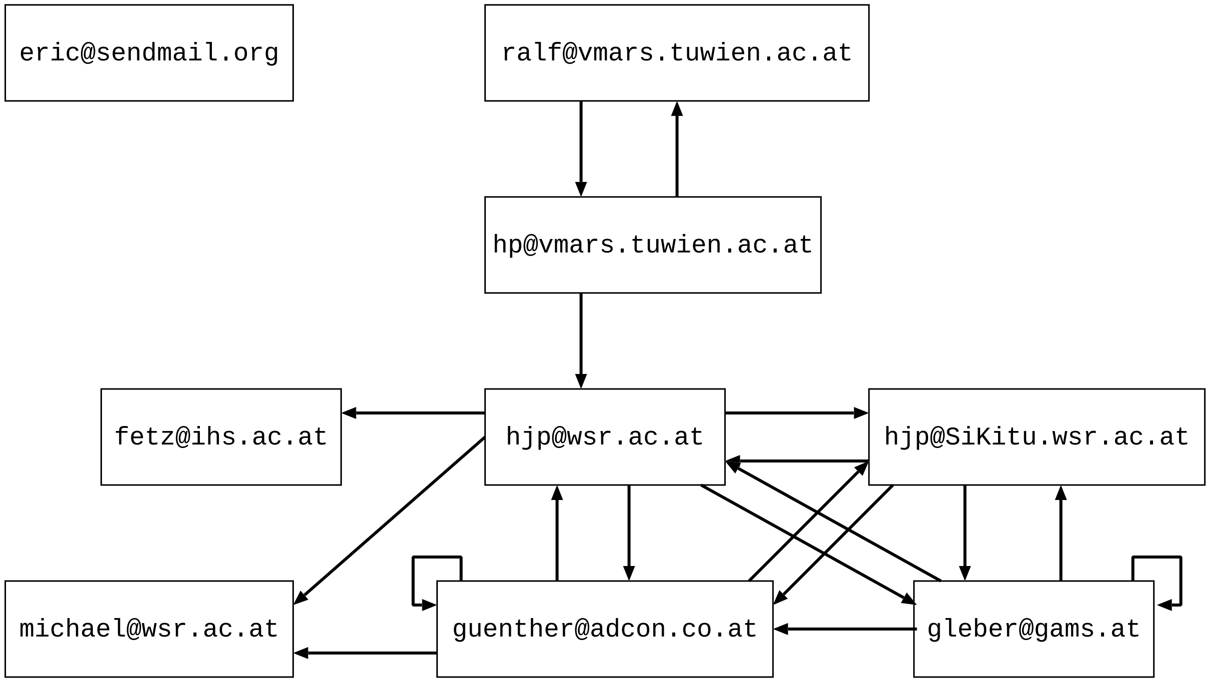
Keyring „Schlüsselbund“ mit allen Schlüsseln.
private — public

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

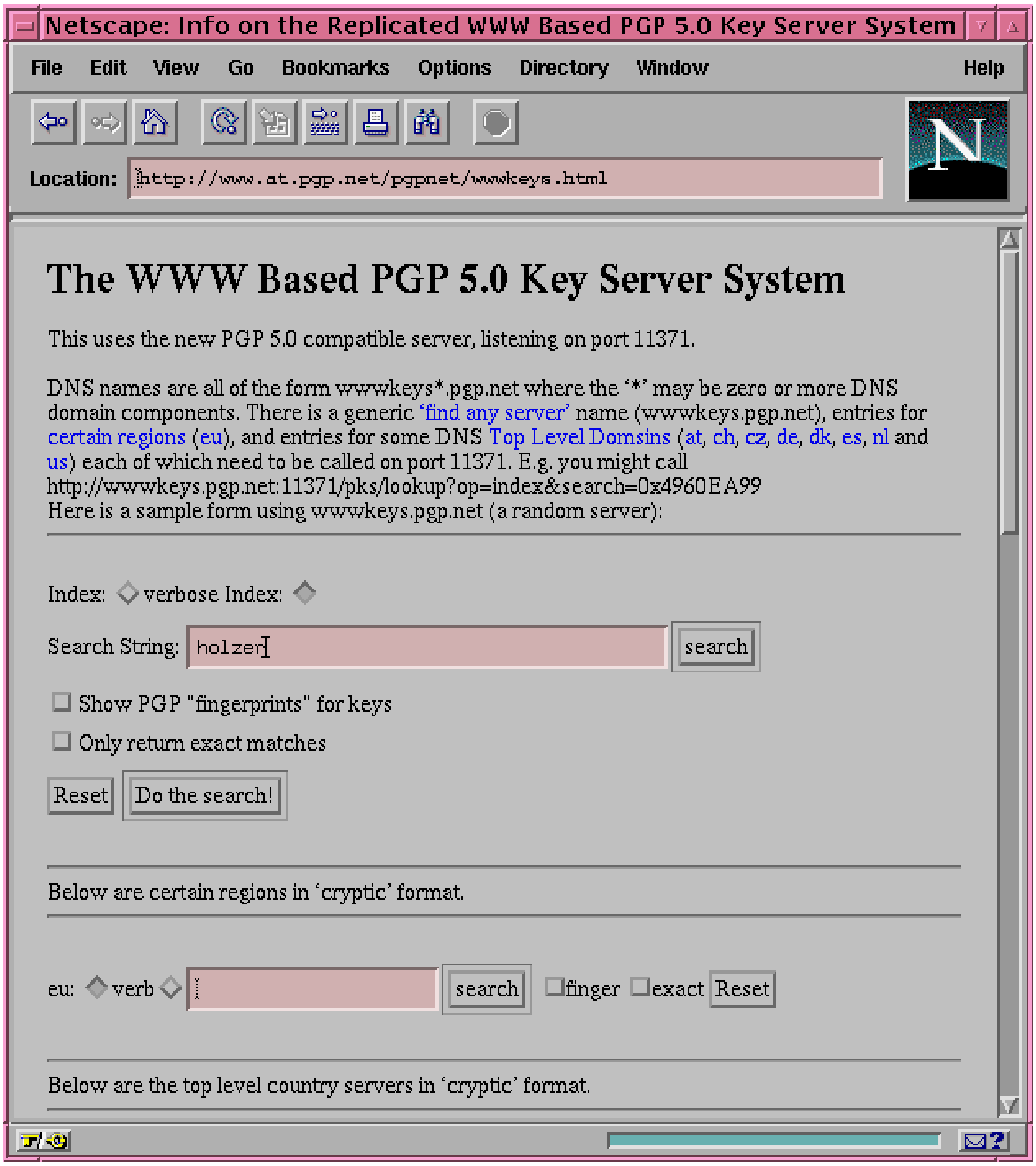
PGP Userinterface: Key Management

```
% pgp -k
[...]
Key management functions:
To generate your own unique public/secret key pair:
   pgp -kg
To add a key file's contents to your public or secret key ring:
   pgp -ka keyfile [keyring]
To remove a key or a user ID from your public or secret key ring:
   pgp -kr userid [keyring]
To edit your user ID or pass phrase:
   pgp -ke your_userid [keyring]
To extract (copy) a key from your public or secret key ring:
   pgp -kx userid keyfile [keyring]
To view the contents of your public key ring:
   pgp -kv[v] [userid] [keyring]
To check signatures on your public key ring:
   pgp -kc [userid] [keyring]
To sign someone else's public key on your public key ring:
   pgp -ks her_userid [-u your_userid] [keyring]
To remove selected signatures from a userid on a keyring:
   pgp -krs userid [keyring]
```

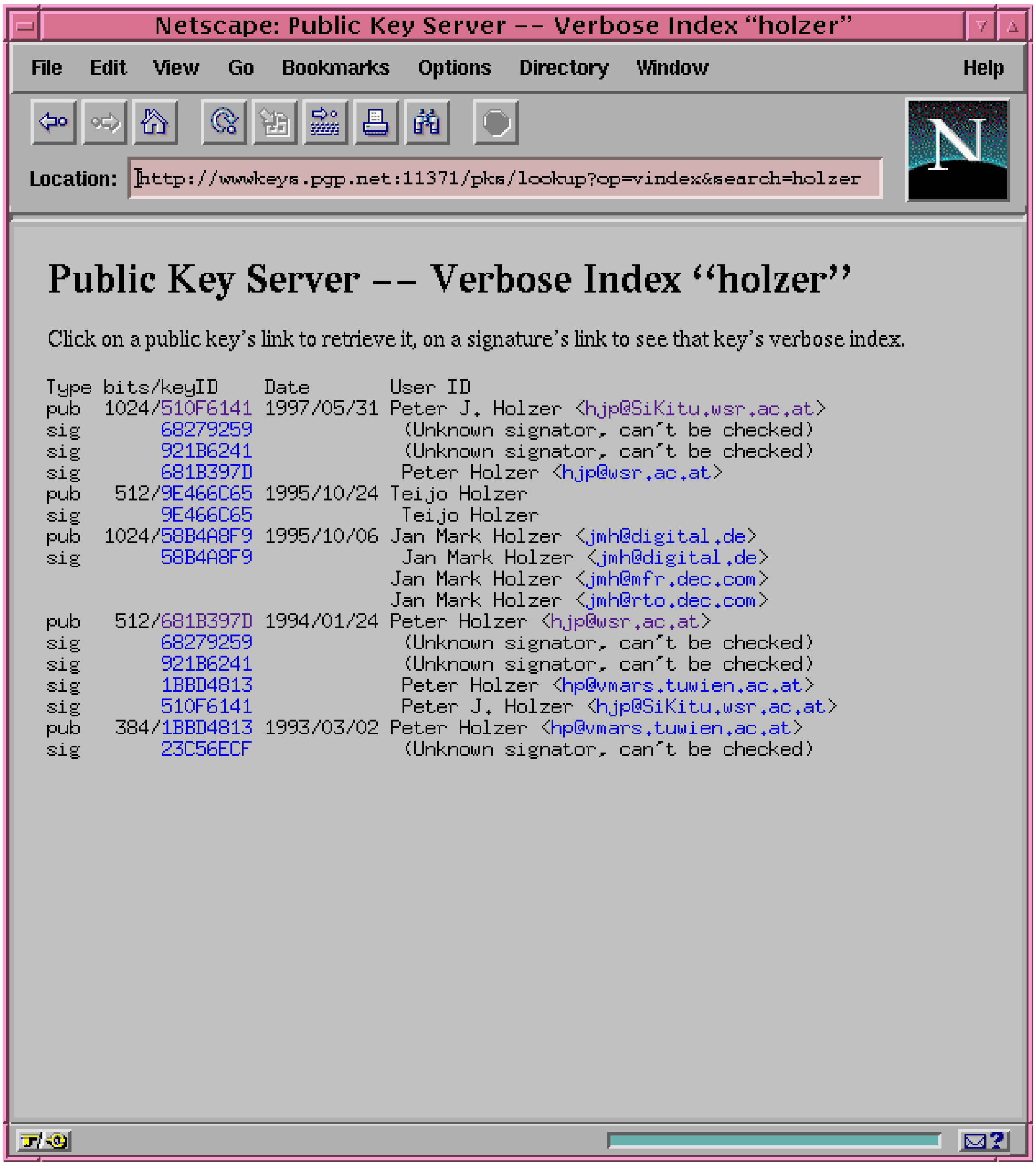
Keyserver

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

Keyserver

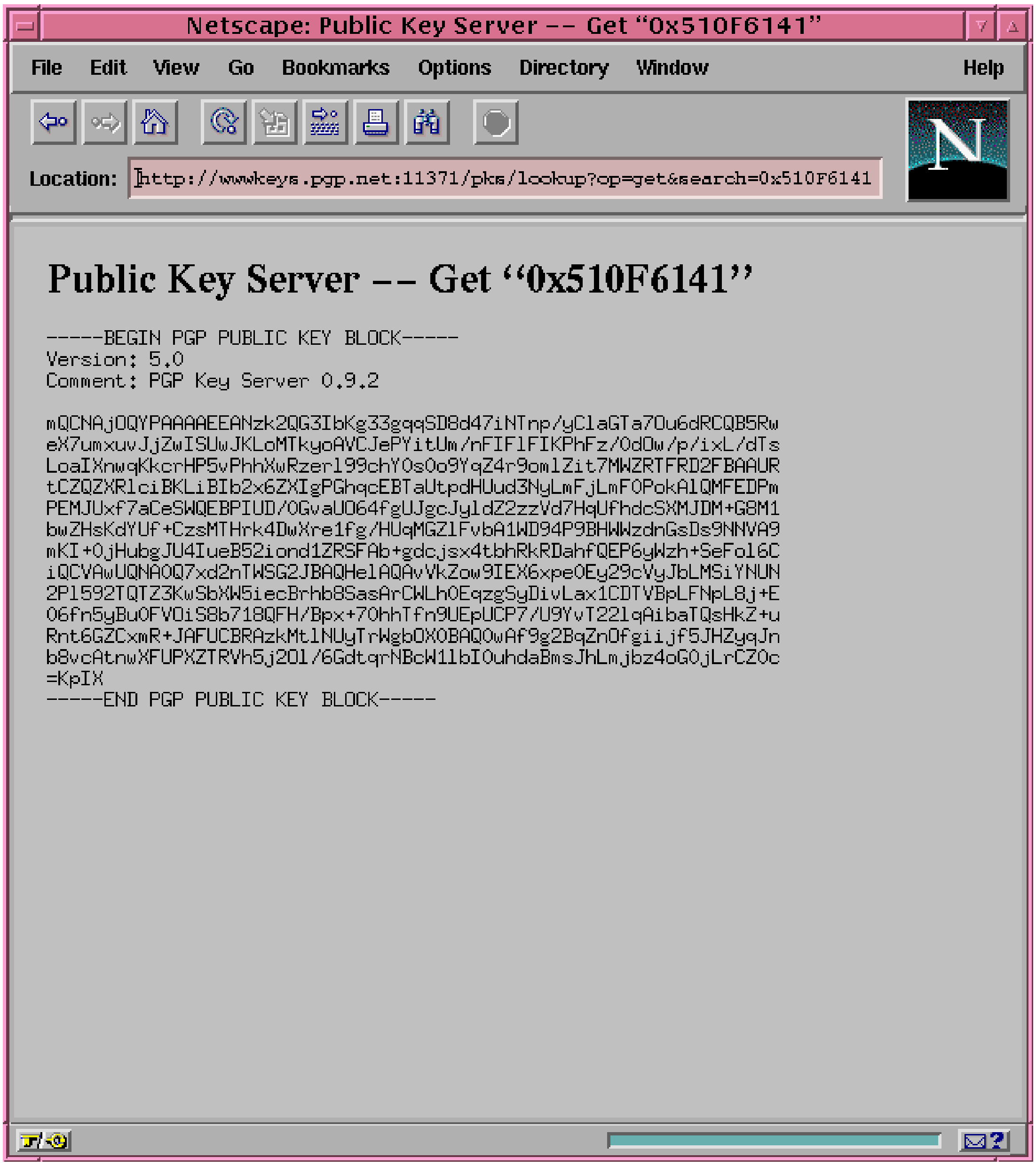

Netscape: Info on the Replicated WWW Based PGP 5.0 Key Server System
File Edit View Go Bookmarks Options Directory Window Help
Location: http://www.at.pgp.net/pgpnet/wwwkeys.html
The WWW Based PGP 5.0 Key Server System
This uses the new PGP 5.0 compatible server, listening on port 11371.
DNS names are 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 Domains (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




```
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)
```

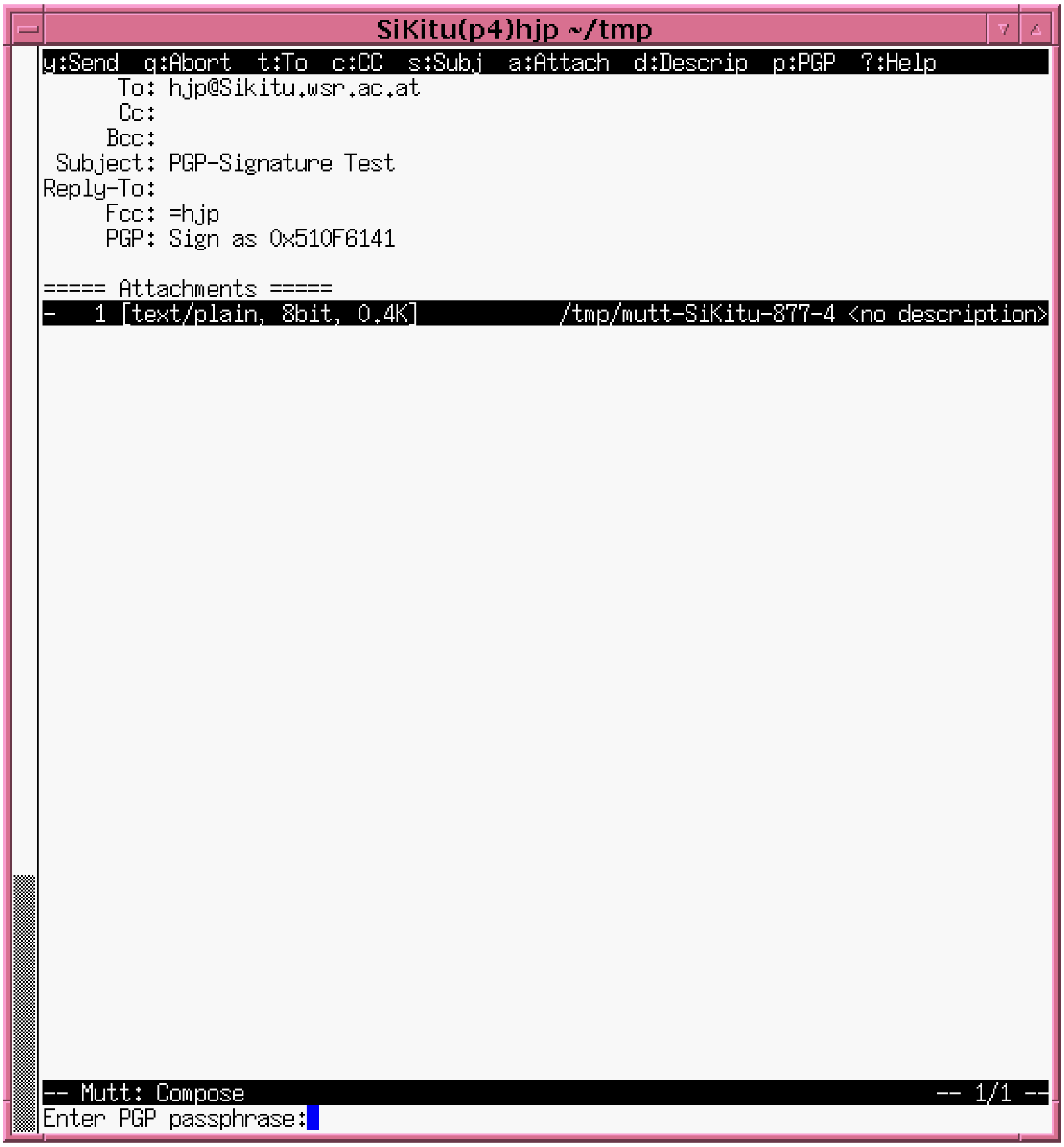
Keyserver


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
tCZQZXRlciBKLiBIb2x6ZXIgPGhqcEBTaUtpdHUud3NyLmFjLmF0PokAlQMFEDPm
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

```
SiKitu(p4)hjp ~/tmp
i:Exit  -:PrevPg  SPC:NextPg  v:Attach  d:Del  r:Reply  j:Next  ?:Help
Date: Tue, 27 Jan 1998 21:57:14 +0100
From: "Peter J. Holzer" <hjp@SiKitu.wsr.ac.at>
To: hjp@Sikitu.wsr.ac.at
Subject: PGP-Signature Test
X-Mailer: Mutt 0.88

[-- PGP output follows (current time: Tue Jan 27 21:57:30 1998) --]

File '/tmp/mutt-SiKit.$00' has signature, but with no text.
Text is assumed to be in file '/tmp/mutt-SiKitu-877-10'.

Good signature from user "Peter J. Holzer <hjp@SiKitu.wsr.ac.at>".
Signature made 1998/01/27 20:57 GMT

[-- End of PGP output --]

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

Das ist eine signierte Mail.

Ihr Inhalt ist für jedermann lesbar. Ebenso kann jeder, der meinen
Public Key kennt, überprüfen, daß die Mail tatsächlich von mir stammt.

        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 signed data --]

-N- 259/259: Peter J. Holzer        PGP-Signature Test                -- (all)
Invoking PGP...
```

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...
```

Wer noch?

- exmh
- Eudora
- MS-Outlook (mit PGP 5)
- INN (Newsserver)
- . . .

Wer nicht?

- Netscape
- MS-Outlook Express
- ...

PGP 5

- Zusätzliche (freie) Algorithmen: DSS/Diffie-Hellman (ElGamal), RIPEMD-160, SHA-1, CAST, TripleDES

- ⇒ Kompatibilitätsprobleme

- Windows-Integration

- Keyserver-Integration