# Datenschutz und Datensicherheit: PGP

# Panzirsch Robert

# Vortrag vom 5.11.96

**Was ist PGP:**

PGP ist ein Public Key Verschlüsselungsprogramm, ursprünglich von Philip Zimmermann entwickelt und arbeitet nach dem RSA- und IDEA(DES)-Verfahren. PGP steht für Pretty Good Privacy oder "Prima Geschützte Privatsphäre".

**Kosten:**

Die internationale PGP-Version ist Freeware. In den USA, Mexiko und Kanada wird ein Teil von PGP (das RSA-Verfahren) durch nationales Patentrecht geschützt. Auch der Sourcecode ist frei erhältlich.

**Plattformen:**

PC, MAC, UNIX, VAX, ...

**Bezugsquelle:**

ftp://ftp.cert.dfn.de/pub/tools/crypt/pgp/

zB für den PC:

ftp://ftp.cert.dfn.de/pub/tools/crypt/pgp/pc/dos/pgp263i.zip

**Versionen:**

Die in den USA verwendete Version - derzeit 2.6.3 - darf nicht exportiert werden. Es gibt daher auch eine internationale Version, derzeit 2.6.3i. Auch kommerzielle Versionen sind erhältlich.

**Gibt es in PGP Hintertüren:**

Nein. PGP ist als Sourcecode erhältlich - jedermann kann prüfen oder prüfen lassen.

**Bezugsquelle Sourcecode:**

ftp://ftp.cert.dfn.de/pub/tools/crypt/pgp/

zB für den PC:

ftp://ftp.cert.dfn.de/pub/tools/crypt/pgp/pc/dos/pgp263is.zip

**Installation (DOS-Version):**

- c: <enter>
- md \pgp <enter>
- cd \pgp <enter>
- pkunzip -d pgp263i.zip <enter>
- SET PATH=C:\PGP;%PATH% <enter>
- SET PGPPATH=C:\PGP <enter>
- SET TZ=GMT+1DST <enter>

**Verwendung:**

PGP ist Commandline - orientiert.

**Information:**

pgp <enter>

Pretty Good Privacy(tm) 2.6.3i - Public-key encryption for the masses.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-01-18
International version - not for use in the USA. Does not use RSAREF.
Current time: 1996/11/05 13:15 GMT
For details on licensing and distribution, see the PGP User's Guide.
For other cryptography products and custom development services, contact:
Philip Zimmermann, 3021 11th St, Boulder CO 80304 USA, phone +1 303 541-0140
For a usage summary, type: pgp -h

**Hilfe:**

pgp -h <enter>

**Generierung des ersten Schlüsselpaares:**

pgp -kg +nomanual <enter>

Pick your RSA key size:
1) 512 bits- Low commercial grade, fast but less secure
2) 768 bits- High commercial grade, medium speed, good security
3) 1024 bits- "Military" grade, slow, highest security
Choose 1, 2, or 3, or enter desired number of bits: **1**
Generating an RSA key with a 512-bit modulus.
You need a user ID for your public key. The desired form for this
user ID is your name, followed by your E-mail address enclosed in
<angle brackets>, if you have an E-mail address.
For example: John Q. Smith <12345.6789@compuserve.com>
Enter a user ID for your public key:
**Robert Panzirsch <robert@s11esrgw1.tuwien.ac.at>**
You need a pass phrase to protect your RSA secret key.
Your pass phrase can be any sentence or phrase and may have many
words, spaces, punctuation, or any other printable characters.
Enter pass phrase:********
Enter same pass phrase again:********
Note that key generation is a lengthy process.
We need to generate 56 random bits. This is done by measuring the
time intervals between your keystrokes. Please enter some random text
on your keyboard until you hear the beep:
0 * -Enough, thank you.
.....**** .....****
Pass phrase is good. Just a moment....
Key signature certificate added.
Key generation completed.

**Damit wurden auch 2 "Schlüsselringe" erzeugt:**

dir c:\pgp*.pgp <enter>

SECRING PGP 308 05.11.96 13.15
PUBRING PGP 227 05.11.96 13.15
2 Datei(en) 535 Byte

Die Datei PUBRING.PGP ist öffentlich - deren Schlüssel kann man weitergeben.
Die Datei SECRING.PGP und deren Schlüssel sind geheim.

**Öffentlichen Schlüssel in Asciiformat in eine eigene Datei extrahieren:**

pgp -kxa "Robert Panzirsch" <enter>

Extracting from key ring: 'c:\pgp\pubring.pgp', userid "Robert Panzirsch".
Key for user ID: Robert Panzirsch <robert@s11esrgw1.tuwien.ac.at>
512-bit key, key ID 993DBB45, created 1996/11/05
Extract the above key into which file? **c:\robert**
Transport armor file: c:\robert.asc
Key extracted to file 'c:\robert.asc'.

**Die Datei c:\robert.asc enthält dann:**

Type Bits/KeyID Date User ID
pub 512/993DBB45 1996/11/05 Robert Panzirsch <robert@s11esrgw1.tuwien.ac.at>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i
mQBNAzJ+JJkAAAECALYtDqpYoLUX3BX8wV5NPSWbmropMHramrSC8Odlc+LqJHfJ
VU3lYq8CFupNy2wRGIRo+yn8uprxZ/Et8pk9u0UABRO0MFJvYmVydCBQYW56aXJz
Y2ggPHJvYmVydEBzMTFlc3JndzEudHV3aWVuLmFjLmF0PokAVQMFEDJ+JJln8S3y
mT27RQEBynEB/icfgNifUlmsHTY9WGlCfROctSTcrPnVxS04WguMR/rypvMh5MVf
c5chFsLXKBaf8bPjhsk2KXrTWRrhNgybz4o=
=Q9M+
-----END PGP PUBLIC KEY BLOCK-----

**Bekommt man nun so einen Schlüssel, kann man ihn auf den Bund hängen:**

pgp -ka gerhard.asc <enter>

Looking for new keys...
pub 512/B50B06A9 1996/11/05 Gerhard
Checking signatures...
pub 512/B50B06A9 1996/11/05 Gerhard
sig! B50B06A9 1996/11/05 Gerhard
Keyfile contains:
1 new key(s)
One or more of the new keys are not fully certified.
Do you want to certify any of these keys yourself (y/N)? **<enter>**

**Schlüsselbund auflisten:**

pgp -kv <enter>

Key ring: 'c:\pgp\pubring.pgp'
Type Bits/KeyID Date User ID
pub 512/B50B06A9 1996/11/05 Gerhard
pub 512/993DBB45 1996/11/05 Robert Panzirsch <robert@s11esrgw1.tuwien.ac.at>
2 matching keys found.

**Datei signieren:**

pgp -sta test.txt -u "Robert Panzirsch" -o test.sig <enter>

A secret key is required to make a signature.
You need a pass phrase to unlock your RSA secret key.
Key for user ID: Robert Panzirsch <robert@s11esrgw1.tuwien.ac.at>
512-bit key, key ID 993DBB45, created 1996/11/05
Enter pass phrase: ********
Pass phrase is good. Just a moment....
Clear signature file: test.sig

**Signatur prüfen:**

pgp test.sig <enter>

File has signature. Public key is required to check signature.
.
Good signature from user "Robert Panzirsch <robert@s11esrgw1.tuwien.ac.at>".
Signature made 1996/11/05 13:15 GMT using 512-bit key, key ID 993DBB45
Plaintext filename: test

**Datei test.txt:**

Das ist ein Testtext ...

**Datei test.sig:**

-----BEGIN PGP SIGNED MESSAGE-----
Das ist ein Testtext ...
-----BEGIN PGP SIGNATURE-----
Version: 2.6.3i
Charset: cp850
iQBVAwUBMn4w/WfxLfKZPbtFAQE57wH9GOFyUpO20QwHAGaCltiA8PjW6p88tqqb
rh7lfUOOPQgpH7JIL0QbcYq+zDjzBvkdRYCivKB89uLcuTAQ3q24IQ==
=Khfa
-----END PGP SIGNATURE-----

**Datei verschlüsseln:**

pgp -ea test.txt "Gerhard" -o test.tx_ <enter>

Recipients' public key(s) will be used to encrypt.
Key for user ID: Gerhard
512-bit key, key ID B50B06A9, created 1996/11/05
.
Ciphertext file: test.tx_

**Datei entschlüsseln:**

pgp test.tx_ -o test.txt <enter>

File is encrypted. Secret key is required to read it.
Key for user ID: Gerhard
512-bit key, key ID B50B06A9 , created 1996/11/05
You need a pass phrase to unlock your RSA secret key.
Enter pass phrase: ********
Pass phrase is good. Just a moment.....
Plaintext filename: test.txt

**Datei test.txt:**

Das ist ein Testtext ...

**Datei test.tx_:**

-----BEGIN PGP MESSAGE-----
Version: 2.6.3i
hEwDZ/Et8pk9u0UBAgCkhf8yMFerC+Tl8k4oCBzOb229KX46G2wCWcvaHYVDPmgp
mNV3T+2Ir573R6axfDxG0PlEF9kSbE+c7i5w/uN/pgAAADkUgtObqckWdk7DWeh3
sqVsJLc/AikGnu0/bSGUbKc1hxL4ST6YS1DTplpCKPZcErmfBfRp3dltO6Q=
=pjCf
-----END PGP MESSAGE-----

**Verschlüsseln:**

Es wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und mit dem privaten Schlüssel (und Passwort) des Empfängers entschlüsselt.

(Auch das Verschlüsseln für mehrere Empfänger ist möglich !)

**Signieren:**

Es wird mit dem privaten Schlüssel (und Passwort) des Senders signiert und mit dem öffentlichen Schlüssel des Senders geprüft.

**Frontends:**

Es gibt eine Vielzahl von Frontends für PGP.
Natürlich auch für MS-Windows, zB das Freeware Programm PGPWIN.

**Mailprogramme:**

Teilweise mit direkt eingebautem PGP Interface, teilweise mittels externer Addons.

**Weiterführende Informationen:**

http://web.mit.edu/network/pgp.html
http://www.thur.de/ulf/krypto/pgp.html
http://www.ifi.uio.no/pgp
http://www.uni-mannheim.de/studorg/gahg/PGP/
http://www.aimnet.com/~jnavas/winpmail/helpers.html
http://www.panix.com/~jgostl/wpgp
http://world.std.com/~franl/pgp/utilities.html
http://bi-node.teuto.de/~christopher/pgp/
http://www-swiss.ai.mit.edu/~bal/pks-toplev.html
ftp://ftp.cert.dfn.de/pub/tools/crypt/pgp/
ftp://toxicwaste.mit.edu/pub/keys/help