# Das Programm

Grundlage für die Entwicklung des Programms XGpgSig war die interessante Diskussion in der Newsgruppe „hamster.de.tools“ mit den Thema „**Headersignatur**“ Siehe: Google-Gruoups Nachrichten
(speziell für Newsgruppen) sollten mit einen Header „`X-PGP-Sig`“ als signierte Nachrichten versehen sein.

## Altes Format

Ursprünglich hatte solche Nachrichten dieses Format:

```
Message-ID: <47EF7D9D.40206700@example.com>
Date: Sun, 30 Mar 2008 13:46:37 +0200
From: Thomas Mustermann <test@example.com>
User-Agent: Thunderbird 2.0.0.12 (Windows/20080213) Hamster/2.1.0.15
MIME-Version: 1.0
Newsgroups: de.test
Subject: Testnachricht
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: 7bit

-----BEGIN PGP SIGNED MESSAGE-----
Hier ist eine Testnachricht.
TEST...TEST....TEST....TEST....
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.8 (MingW32)

iQEVAwUBR/Yr91WX8k69M166AQHHXwf/WM8LpnoDO9ghHsUJm4aRGbKiEL3qHy8x
j6sJNiQZMAQA0NRl6l7ctmoupEuwdseZ8x4jUvSuNea8BKtGLOIeHTwVdZCAO6d5
ZLgqIRMrEnQZnjoPeNloBm92ewZhe+Z1okmJgdtISLbldFAFsuG4Ol70RVp/Qun8
b3hsOB/900YaSTX0ILQzn6eks0H1Njt0DQaNxy34czCSmVZfwFv4CQmQOXFga0QT
5pu/dekbbnsWy/DNM3qh57DOEbFeQNGq3TsLVyrvri35VoQe7SsiK1iaRXG0pWC3
PrTJ0b1YfCJ51N3Yff00+gd7wEDi3EXdHOuEtbw7zBwcKZKC6t89Eg==
=uDDq
-----END PGP SIGNATURE----
```

## Neues Format

Und hier die bevorzugte Form:

```
Message-ID: <47EF7D9D.40206700@example.com>
Date: Sun, 30 Mar 2008 13:46:37 +0200
```

```
From: Thomas Mustermann <test@example.com>
User-Agent: Thunderbird 2.0.0.12 (Windows/20080213) Hamster/2.1.0.15
MIME-Version: 1.0
Newsgroups: de.test
Subject: Testnachricht
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: 7bit
X-PGP-Sig: GnuPG_v1.4.8_(MingW32) Date,From,Newsgroups,Subject
iQEVAwUBR/Yr91WX8k69M166AQHHXwf/WM8LpnoDO9ghHsUJm4aRGbKiEL3qHy8x
j6sJNiQZMAQA0NRl6l7ctmoupEuwdseZ8x4jUvSuNea8BKtGLOIeHTwVdZCAO6d5
ZLgqIRMrEnQZnjoPeNloBm92ewZhe+Z1okmJgdtISLbldFAFsuG4Ol70RVp/Qun8
b3hsOB/900YaSTX0ILQzn6eks0H1Njt0DQaNxy34czCSmVZfwFv4CQmQOXFga0QT
5pu/dekbbnsWy/DNM3qh57DOEbFeQNGq3TsLVyrvri35VoQe7SsiK1iaRXG0pWC3
PrTJ0b1YfCJ51N3Yff00+gd7wEDi3EXdHOuEtbw7zBwcKZKC6t89Eg==
=uDDq

Hier ist eine Testnachricht.
TEST...TEST....TEST....TEST....
```

Es werden nur bestimmte Header und der Nachrichtentext zur Signierung verwendet.
Das von Programm „XPgpSig“ von Jürgen Haible hatte PGP verwendet. XGpgSig setzt nun auf GnuPG auf.

# 1.1 Programmparameter

Das Programm XgpgSig wird über die Eingabeaufforderung gesteuert.
Hierzu muß man bestimmte Parameter eingeben. Folgende Parameter gibt es:

| Parameter | Bedeutung |
|---|---|
| `sign` | Anweisung zur Signierung |
| `verify` | Anweisung zur Prüfung einer Signatur |
| `Help` | Zeigt Hilfe an |
| `?` | Zeigt Hilfe an |
| `-i <Pfad>` | Nachricht zum Signieren (vollständiger Pfad) |
| `-o <Pfad>` | Fertige, signierte Nachricht (vollständiger Pfad) |
| `-s <ID>` | Unterschreiben mit Schlüssel-ID |
| `-p <Pfad>` | Vollständiger Pfad zur GPG.EXE |
| `-k <Passwort>` | Kennwort zur Signierung [ab Version 0.0.2.4 vorhanden] |
| `-h <Name>` | Zuweisung des Hash Algorithmus zur Signierung und Prüfung [ab Version 0.0.2.5 vorhanden] |

# 1.2 Die INI-Datei „XgpgSig.ini“

### "XGpgSig" - Version 0.0.x

In diesen Versionen wird GNUPG in der Version 1.x verwendet.

Die INI-Datei ist der einfachste Weg bestimmte Veränderung vor der Signierung vorzunehmen.

Hierbei kann man sich der Scriptsprache von Hamster bedienen.

| Sektion | Eintrag | Wert |
|---|---|---|
| XGpgSig | GnuPG | Vollständiger Pfad zur GPG.EXE<br>z.B. C:\GnuPG\ (Wird nur verwendet, wenn Option -p nicht verwendet wird.) |
| XGpgSig | RunGPG | Optionen zum Signieren mit der GPG.EXE<br>z.B. –pgp2 –no-comments –clearsign<br>Standard: –pgp2 –no-comments –clearsign |
| XGpgSig | SigHeader | Header die zur Signierung benutzt werden sollen. Format: ":HEADER:HEADER:HEADER:„<br>z.B. :Subject:Control:Date:From:Sender:<br>Standard:<br>:Subject:Control:Message-ID:Date:From:Sender:Newsgroups:Approved:Followup-To:Supersedes: |
| XGpgSig | KillTmp | 0 oder 1 |
| XGpgSig | PWait | Integer Wert in Millisekunden, z.B. 300 |
| XGpgSig | ShowGPG | 0 oder 1 |
| XGpgSig | SigHash | Kennzeichnung des Hash Algorithmus |
| Log | LogBadSig | 0 oder 1 |
| Log | LogGoodSig | 0 oder 1 |
| PW | Passwort | Ihr Passwort |
| PW | KeyID | Ihre Schlüssel ID |

Hier ein Beispiel einer INI-Datei (liegt auch dem Programm bei)

XgpgSig.ini

```
[XGpgSig]
GnuPG=G:\Programme\GNU\GnuPG\
SigHeader=:From:Subject:Newsgroups:
RunGPG=--no-comments –clearsign
KillTmp=0
PWait=300
ShowGPG=0
SigHash=MD5
[Log]
LogBadSig=1
LogGoodSig=0
[PW]
Password=passwort
KeyID=0xGnuKey
```

## "XGpgSig" - Version 0.1.x

In diesen Versionen wird GNUPG in der Version 2.x verwendet.
Gegenüber der obrigen Versionen wird GNUPG anders über die Kommandozeile aufgerufen.

Die INI-Datei ist der einfachste Weg bestimmte Veränderung vor der Signierung vorzunehmen.
Hierbei kann man sich der Scriptsprache von Hamster bedienen.

| Sektion | Eintrag | Wert |
|---|---|---|

| | | |
|---|---|---|
| XGpgSig | GnuPG | Vollständiger Pfad zur GPG2.EXE<br>z.B. C:\GnuPG\ (Wird nur verwendet, wenn Option -p nicht verwendet wird.) |
| XGpgSig | RunGPG | Optionen zum Signieren mit der GPG2.EXE<br>z.B. –batch –no-comments<br>Standard: –batch –no-comments |
| XGpgSig | SigHeader | Header die zur Signierung benutzt werden sollen. Format: ":HEADER:HEADER:HEADER:„<br>z.B. :Subject:Control:Date:From:Sender:<br>Standard:<br>:Subject:Control:Message-ID:Date:From:Sender:Newsgroups:Approved:Followup-To:Supersedes: |
| XGpgSig | KillTmp | 0 oder 1 |
| XGpgSig | PWait | Integer Wert in Millisekunden, z.B. 300 |
| XGpgSig | ShowGPG | 0 oder 1 |
| XGpgSig | SigHash | Kennzeichnung des Hash Algorithmus |
| Log | LogBadSig | 0 oder 1 |
| Log | LogGoodSig | 0 oder 1 |
| PW | Passwort | Ihr Passwort |
| PW | KeyID | Ihre Schlüssel ID |

Hier ein Beispiel einer INI-Datei (liegt auch dem Programm bei)

XgpgSig.ini

```
[XGpgSig]
GnuPG=G:\Programme\GNU\GnuPG\
SigHeader=:From:Subject:Newsgroups:
RunGPG=--batch --no-comments
KillTmp=0
PWait=300
ShowGPG=0
SigHash=MD5
[Log]
LogBadSig=1
LogGoodSig=0
[PW]
Password=passwort
KeyID=0xGnuKey
```

# 1.3 Sektionen der INI-Datei

XGpgSig verwendet ab der Version 0.1.x einen anderen internen Aufruf der Kommandozeile.
Zudem wird nur noch GNUPG 2.x verwendet und ist gegenüber den älteren Versionen daher inkompatibel.
Abweichungen in der INI-Datei sind hier extra aufgeführt, alle anderen Parameter bleiben gleich.

## 1.3.1 Sektion "XGpgSig" - Eintrag "GnuPG"

| | |
|---|---|
| Wert: | Der vollständige Pfad zur EXE-Datei „GPG.EXE“ |
| Standardwert: | N/A [1)] |

:bu04: Bei Programmversion 0.1.x und höher ist hier der vollständige Pfad zur „GPG2.EXE“ anzugeben.
Siehe: Parameter der GPG.EXE , Parameter der GPG2.EXE

### 1.3.2 Sektion "XGpgSig" - Eintrag "RunGPG"

| | |
|---|---|
| Wert: | Parameter die zur Signierung verwendet werden. |
| Standardwert: | **–pgp2 –no-comments –clearsign** |

:bu04: Bei Programmversion 0.1.x und höher hat sich der Standardwert geändert.
Dieser Eintrag sollte nicht verändert, sonder nur ergänzt werden. (Anfügen von Parametern)

| | |
|---|---|
| Wert: | Parameter die zur Signierung verwendet werden. |
| Standardwert: | **–batch –no-comments** |

### 1.3.3 Sektion "XGpgSig" - Eintrag "SigHeader"

| | |
|---|---|
| Wert: | Folgende Header werden zur Signierung verwendet. |
| Standardwert: | **:Subject:Control:Message-ID:Date:From:Sender:Newsgroups:Approved:Followup-To:Supersedes:** |

Das allgemeine Format ist „Format: “:HEADER:HEADER:HEADER:“.
Hierbei werden die Header durch den Doppelpunkt getrennt.

### 1.3.4 Sektion "XGpgSig" - Eintrag "KillTmp"

| | |
|---|---|
| Wert: | 0 oder 1 |
| Standardwert: | **1** |

Der Eintrag „KillTmp“ (Sektion: XgpgSig) ist in der Version 0.0.2.2 in der INI-Datei hinzugekommen.
Der Wert 0 steht für den boolescher Ausdruck FALSE und der Wert 0 für TRUE.

Mit den Wert 0 werden die erzeugten temporären Dateien die in Betrieb des Programms verwendet werden
nicht gelöscht. Ist jedoch der Wert 1, so werden diese Dateien kurz vorm Beenden des Programms gelöscht.
Es wird empfohlen den Wert auf 1 zu setzen, da es zu Problemen innerhalb des Programms kommen kann
wenn diese temporären Dateien noch vor der Benutzung von XgpgSig vorhanden sind.
Bei der Signierung werden die temporären Dateien „XpgpSig.$$i“ und die Datei „XpgpSig.$$i.asc“ erstellt.
Die Datei „XpgpSig.$$i“ wird durch die internen Prozedur ConvertMsgToSign erzeugt.

Hier werden die ausgewählten Header und der Nachrichtentext für die Signierung ausgewählt und in dieser
temporären Datei abgespeichert. Die Datei „XPgpSig.$$i.asc“ ist die Datei, welche nach der Signierung mit
der GPG.EXE entsteht. Diese Datei wird später weiterverarbeitet um dann die Ausgabedatei zu erzeugen.

Bei der Prüfung werden die temporären gleichen Dateien wie bei der Signierung erzeugt.
Dabei wird die Datei „XPgpSig.$$i“ durch die interne Prozedur ConvertXPgpSigToPgp erzeugt.

Nun wird noch der PGP-Block noch hinzugefügt und die Datei „XPgpSig.$$i.asc“ erzeugt.
Dann wird mittels GPG.EXE geprüft. Das Prüfergebnis wird in die Ausgabedatei geschrieben.

### 1.3.5 Sektion "XGpgSig" - Eintrag "PWait"

| Wert: | Integer Wert in Millisekunden, z.B. 300 |
|---|---|
| Standardwert: | **300** |

Dieser Eintrag wird erst ab der Version 0.0.2.4 genutzt. Hier wird ein Integerwert angegeben.
Dies ist die Wartezeit (in Millisekunde) zwischen den Erscheinen des Fensters zur Signierung (GPG.EXE)
`[Die Passphrase wird abgefragt]` und der automatischen Übergabe des Passworts.

### 1.3.6 Sektion "XGpgSig" - Eintrag "ShowGPG"

| Wert: | 0 oder 1 |
|---|---|
| Standardwert: | **1** |

Beim Wert `1` wird das das Fenster (Kommandozeile) bei der Parameterübergabe angezeigt. Beim Wert `0` nicht.<br>

### 1.3.7 Sektion "XGpgSig" - Eintrag "SigHash"

| Wert: | Kennzeichnung des Hash Algorithmus |
|---|---|
| Standardwert: | **MD5** |

Die möglichen Hash Alogrithem sind von der Version von GnuPG anbhängig.
Bei der Version 1.4.9 sind es: „**MD5, SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224**“.
Genauer Informationen entnehmen Sie bitte der Dokumenation von GnuPG für Windows.

### 1.3.8 Sektion "Log" - Eintrag "LogBadSig"

| Wert: | 0 oder 1 |
|---|---|
| Standardwert: | **1** |

Der Wert „1“ steht für das Anlegen einer Logdatei.
Hierbei werden Fehlermeldungen in einer Datei gesammelt gespeichert.

### 1.3.9 Sektion "Log" - Eintrag "LogGoodSig"

| Wert: | 0 oder 1 |
|---|---|
| Standardwert: | **1** |

Der Wert „1“ steht für das Anlegen einer Logdatei.
Hierbei werden Meldungen in einer Datei gesammelt gespeichert.

### 1.3.10 Sektion "PW" - Eintrag "Passwort"

| Wert: | Ihr Kennwort |
|---|---|
| Standardwert: | **XGpgSig** |

Hier können Sie ihr benötiges Kennwort bei der Signierung mit Ihren GnuPG-Schlüssel angeben.
Dies erfolgt im Klartext. Sie können auch das Kennwort im Kommandozeilenfenster von GnuPG selbst eingeben.
Hierbei sollte der Wert „ShowGPG“ in Sektion „XGpgSig“ auf „1“ stehen.

### 1.3.11 Sektion "PW" - Eintrag "KeyID"

| Wert: | KeyID |
|---|---|
| Standardwert: | N/A [2)] |

Hier sollte nun Ihre GnuPG-Schlüssel ID stehen in Form „0x.....“.
Mit dieser KeyID wird die Nachricht signiert. Alternativ kann es über den Parameter „-s`<ID>`“ erfolgen.

## 2. Tipps

Weitere Informationen können Sie den deutschsprachigen Handbuch im PDF-Format entnehmen.
Dies ist im Downloadbereich zu finden.

[1)] , [2)]
Englisch für „not available“ / nicht verfügbar