Das Prüfen mit XGpgSig

Eine Nachricht wird über XGpgSig mit den Befehl **verify** wie folgt geprüft.
Falls die Prüfung fehlschlägt, also es zu keiner positiven Bestätigung kommt wird ein Fehler ausgegeben.
Dieser ist in der Datei „XpgpSig.err“ mit Datum und Uhrzeit festgehalten.

1. Beispiel

```
XGpgSig.exe verify -iC:\test\287.msg -oC:\test\287_2.msg
```

Hier wird die Nachricht (Datei) in „C:\test\287.msg“ geprüft. Falls kein Fehler auftritt wird die Datei „C:\test\287_2.msg“ erzeugt. In dieser Datei sieht man das Ergebnis der Prüfung.
Hier eine Beispielnachricht:

```
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
X-PGP-CHECK: Unterschrift vom 04/04/08 15:24:07 mittels RSA-Schlüssel ID
BD335EBA
X-PGP-CHECK: Korrekte Unterschrift von "Thomas Mustermann
<test@example.com>"

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

Das obige Fenster zeigt das Ergebnis einer geprüften Nachricht. Zusätzlich wurde hier der Header „X-PGP-CHECK“ mit Informationen aus der GPG.EXE gespeichert.

2. Beispiel

```
XGpgSig.exe verify -iC:\test\287.msg -oC:\test\287_2.msg -hSHA1
```

Hier wird die Nachricht (Datei) in `C:\test\287.msg` geprüft. Falls kein Fehler auftritt wird die Datei „C:\test\287_2.msg“ erzeugt. In dieser Datei sieht man das Ergebnis der Prüfung.
Durch den Parameter **-hSHA1** wird der Hash Algorithmus auf SHA1 gesetzt. Befindet sich in der Nachricht der
Header „X-PGP-Hash“ mit der Kennzeichnung des Hash Algorithmus, so wird dieser automatisch den Parameter **-h** zugeordnet.

Ab der Version 0.0.2.5 kann der Parameter „-h<Name>“ verwendet werden. Hinter den Parameter steht der
Hash Algorithmus, welches die GPG.EXE verwenden soll. Fragt man die GPG.EXE mit den Parameter „–help“ ab, so erfährt man welche Hash Algorithmen verwendet werden können.
Bei der Version 1.4.9 sind es zum Beispiel „MD5, SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224“.