Das Signieren

Eine Nachricht wird mit den Befehl **sign** wie folgt signiert. Natürlich müssen Sie auch den privaten Schlüssel
und das erforderliche Kennwort haben. Mit den Parameter **-s** gibt man die Schlüssel-ID an, mit welcher die
Nachricht signiert werden soll. Ansonsten wird der Standardschlüssel verwendet.

1.Beispiel

```
XGpgSig.exe sign -iC:\test\287.msg -oC:\test\287_1.msg -s0x1772C8D8 -
pE:\porg\gnupg\
```

Hier wird eine Nachricht (Datei) in „C:\test\287.msg“ mit einen Schlüssel (ID: **0x1772C8D8**) unterschrieben.
Falls kein Fehler auftritt wird die signierte Nachricht als Datei „287_1.msg“ ausgegeben.
Zusätzlich wird hier über den Parameter **-p** der vollständige Pfad zur GPG.EXE angegeben.
Falls ein Fehler auftritt wird dieser in der Datei „XpgpSig.err“ mit Datum und Uhrzeit festgehalten.



Die Datei „XpgpSig.err“ wird im Programmverzeichnis erstellt.

2.Beispiel

```
XGpgSig.exe sign -iC:\test\287.msg -oC:\test\287_1.msg -s0x1772C8D8
```

Hier wird eine Nachricht (Datei) in „C:\test\287.msg“ mit einen Schlüssel (ID: **0x1772C8D8**) unterschrieben.
Falls kein Fehler auftritt wird die signierte Nachricht als Datei „287_1.msg“ ausgegeben.
Der vollständige Pfad zur GPG.EXE wird aus der INI-Datei „XGpgSig.ini“ gelesen.
Falls ein Fehler auftritt wird dieser in der Datei „XpgpSig.err“ mit Datum und Uhrzeit festgehalten.

Ab der Version 0.0.2.4 kann mittels Parameter -k<Passwort> das Passwort bei der Signierung automatisch übergeben werden. Die Zeit zwischen den Erscheinen des Fensters (GPG.EXE) mit der Aufforderung das Kennwort einzugeben und der automatischen Übergabe des Kennworts kann in einen
neuen Eintrag in der INI-Datei eingestellt werden. Zusätzlich kann man das Fenster unsichtbar machen.

3.Beispiel

```
XGpgSig.exe sign -iC:\test\287.msg -oC:\test\287_1.msg -s0x1772C8D8 -hSHA1
```

Hier wird eine Nachricht (Datei) in „C:\test\287.msg“ mit einen Schlüssel (ID: **0x1772C8D8**) unterschrieben.
Durch den Parameter -h wird der Hash Algorithmus auf SHA1 gesetzt.
Falls kein Fehler auftritt wird die signierte Nachricht als Datei „287_1.msg“ ausgegeben. In dieser Datei ist
nun auch der zusätzliche Header „X-PGP-Hash“ mit der Angabe des Hash Algorithmus vorhanden.
Der vollständige Pfad zur GPG.EXE wird aus der INI-Datei „XGpgSig.ini“ gelesen.
Falls ein Fehler auftritt wird dieser in der Datei „XpgpSig.err“ mit Datum und Uhrzeit festgehalten.

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“.

From:
https://remo-web.de/ - **remo-web.de**

Permanent link:
https://remo-web.de/doku.php?id=entwicklung:xgpgsig:signieren

Last update: **2015/07/25 21:00**