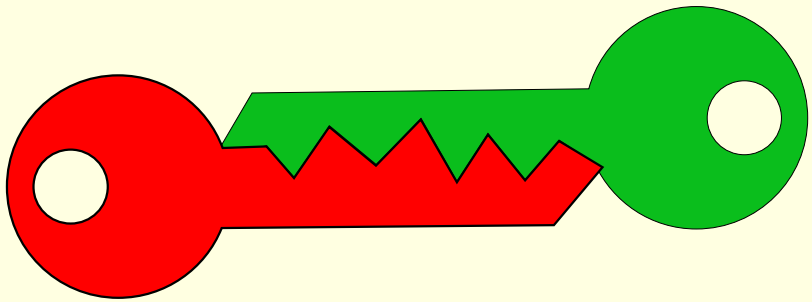
Digitale Unterschriften für Einsteiger

- Digitale Unterschriften sind ein cleverer Ansatz, komplexe Mathematik im täglichen Leben zu nutzen

- Mal sehen, wie das funktioniert…

Einrichtung Schritt 1 : Erzeugen des eigenen Schlüssels

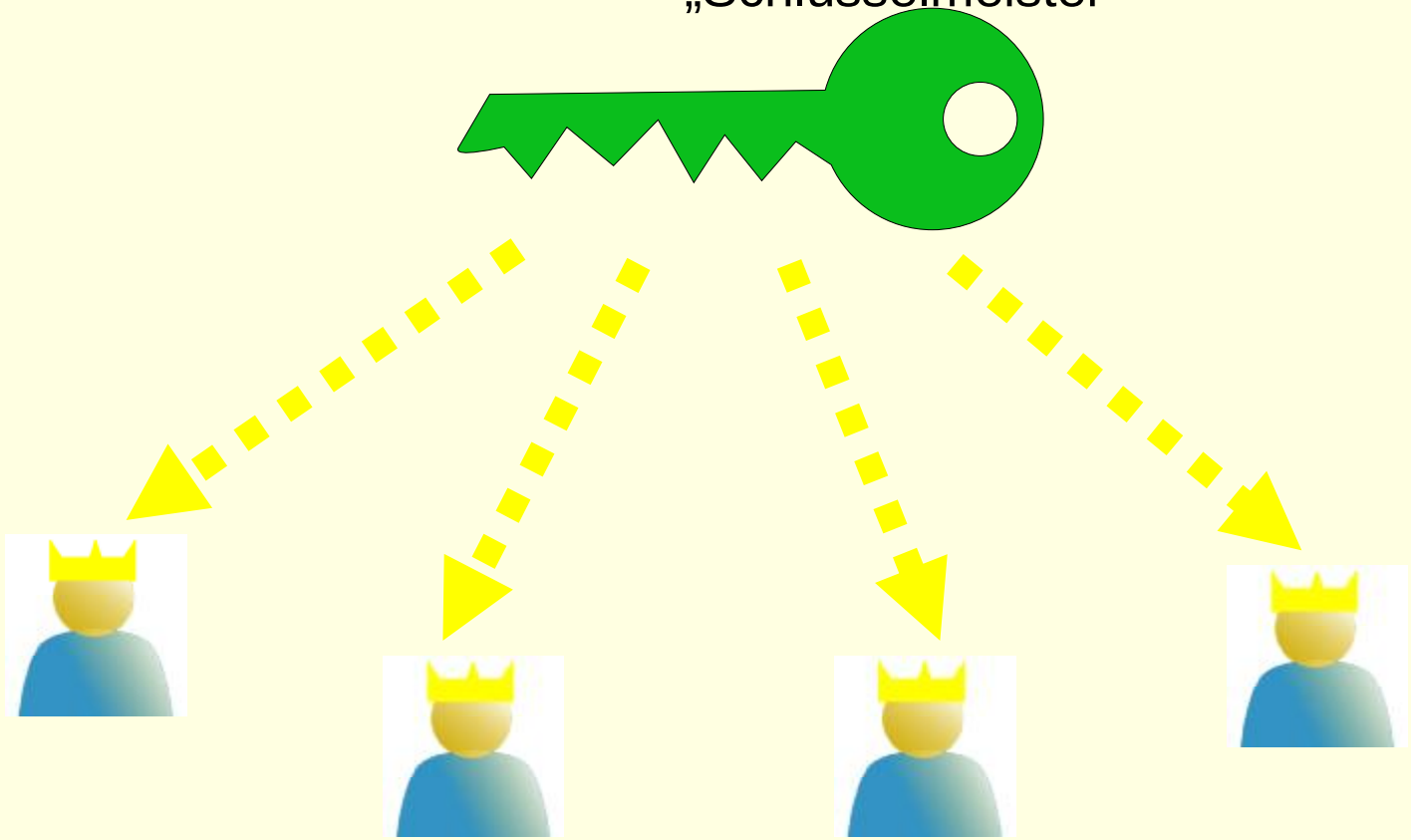
- Zuerst erzeugt man ein Schlüsselpaar bestehend aus einem öffentlichen und einem privaten Schlüssel (Public und Secret Key)



- Der Zugang zum privaten Schlüssel ist durch Passwort geschützt

Einrichtung Schritt 2 : Bekanntgeben des öffentlichen Schlüssels

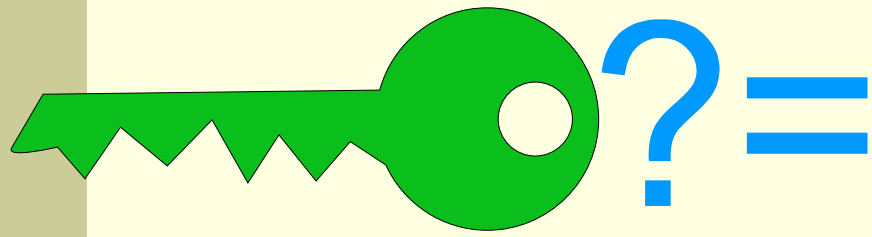
- Versenden des öffentlichen Schlüssels an die „Schlüsselmeister“



Digital Signatures with TheSign

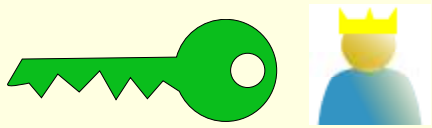
Einrichtung Schritt 3 : Überprüfen und Unterschreiben des neuen Schlüssels

- Die „Schlüsselmeister“ überprüfen den öffentlichen Schlüssel anhand des Schlüsselzertifikats (Key Certificate)



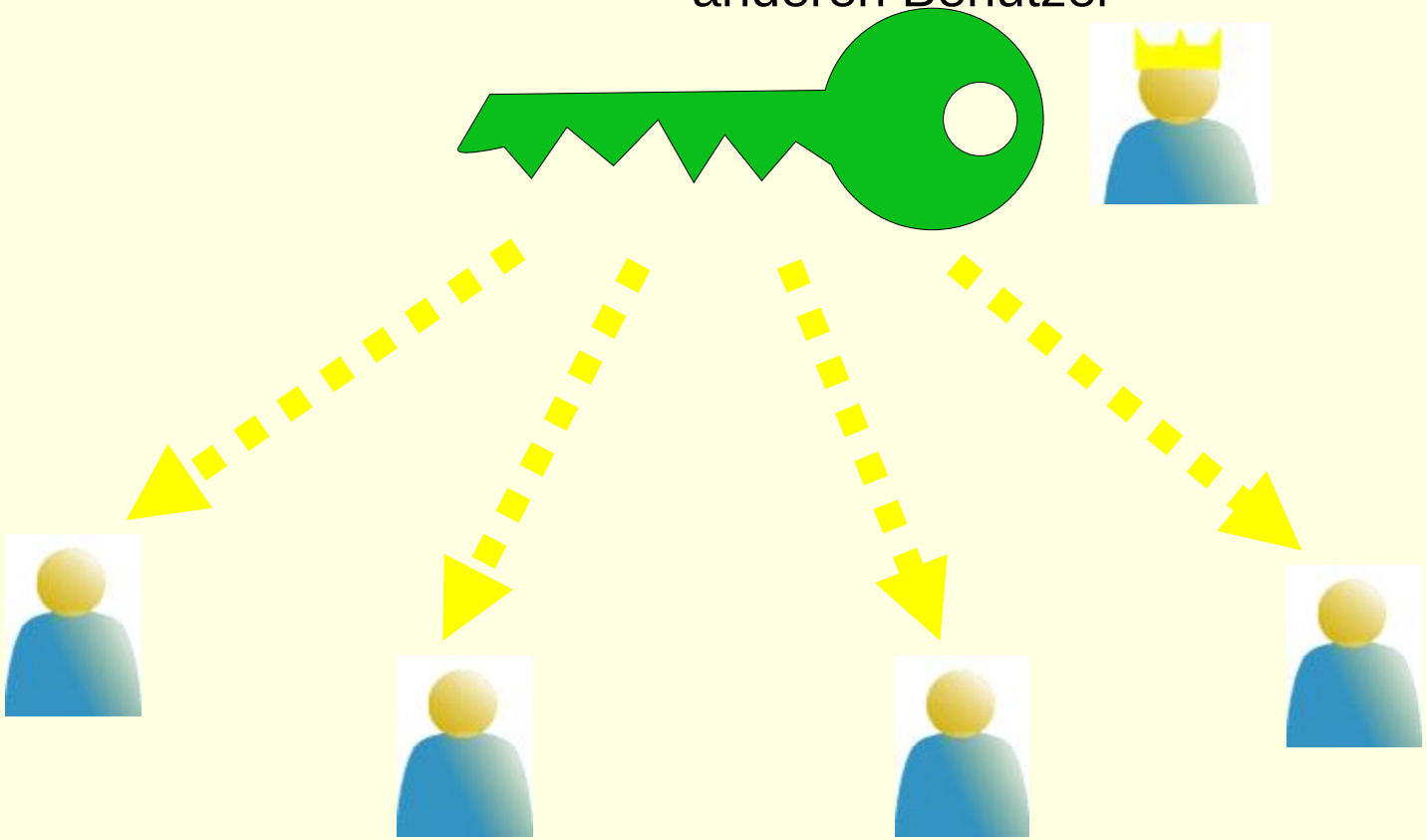
```
pub 1024D/6702661F 2003-05-04
Key fingerprint = A2E8 8737 3654 D5E2 031F 02B5 BCDE B096 6702 661F
uid Steffen Köehler (SY CS1 E)
uid Steffen Koehler
sub 1024g/FA8259DC 2003-05-04
```

- Wenn es zusammenpasst, unterschreiben sie den Schlüssel als gültig



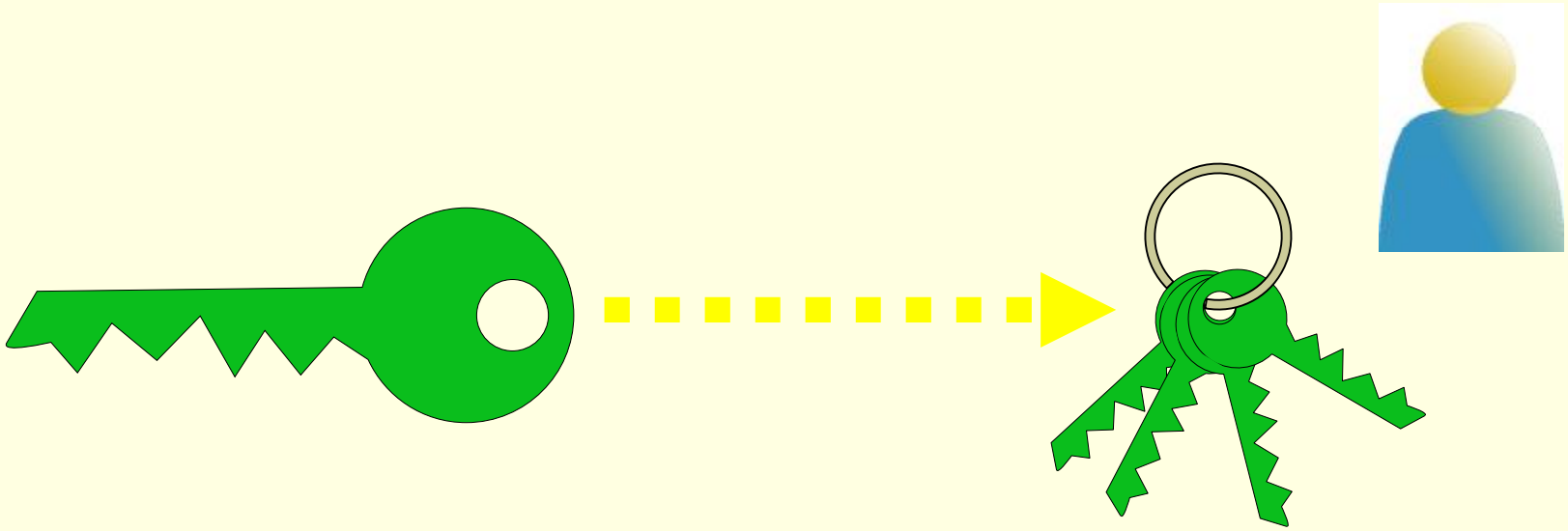
Einrichtung Schritt 4 : Verteilen des öffentlichen Schlüssels

- Die Schlüsselmeister verteilen den verifizierten Schlüssel an alle anderen Benutzer



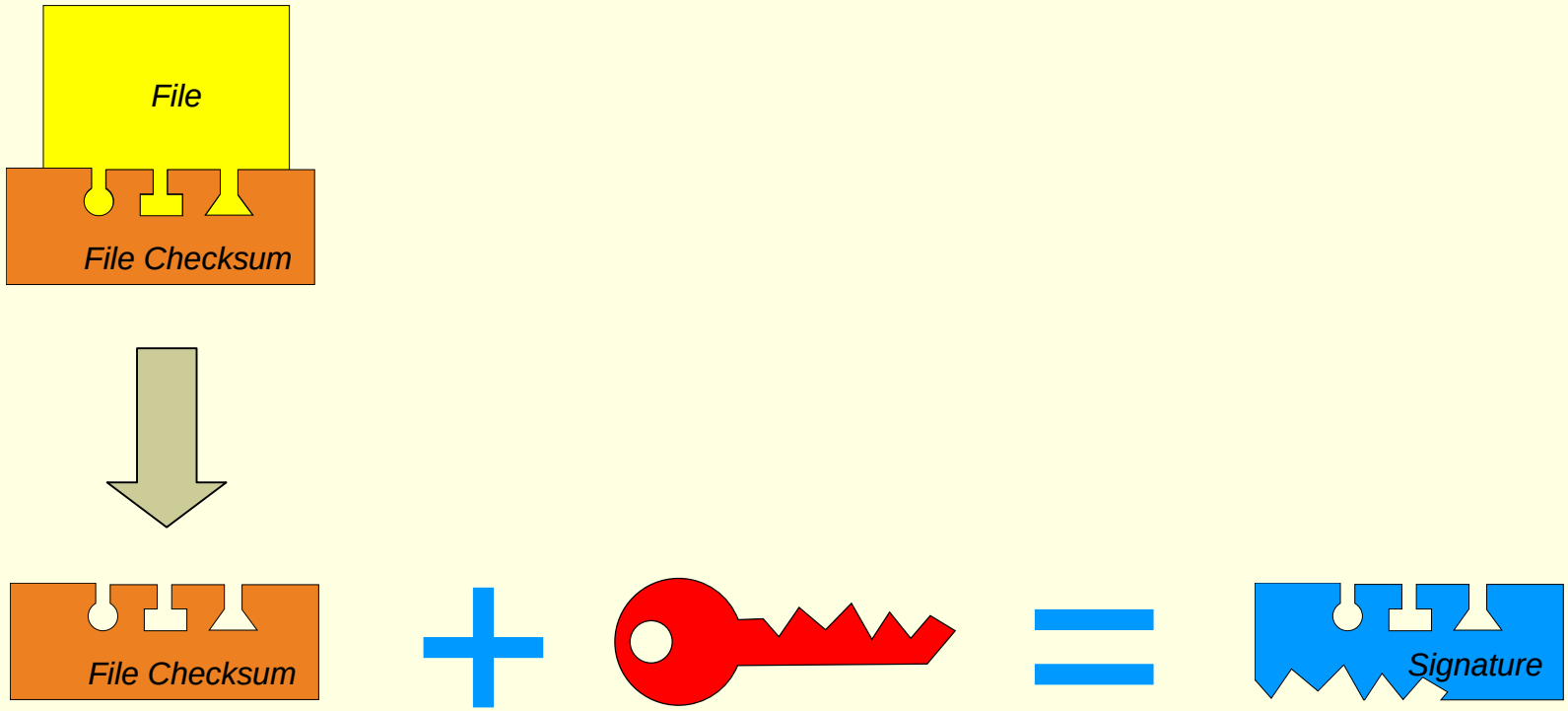
Einrichtung Schritt 5 : Speichern des empfangenen Schlüssels

- Die Benutzer ergänzen den empfangenen öffentlichen Schlüssel zu ihrem Schlüsselring (Public Key Ring)

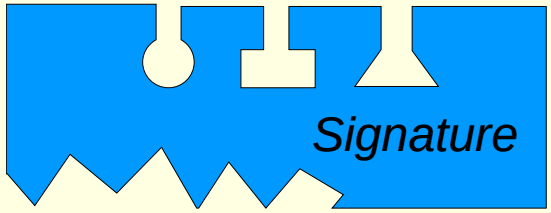


Erzeugen einer Digitalen Unterschrift

- Zum Unterschreiben einer Datei erzeugt man eine Unterschrift generiert aus dem eigenen privaten Schlüssel und der Prüfsumme der zu unterschreibenden Datei



Der Inhalt einer Digitalen Unterschrift



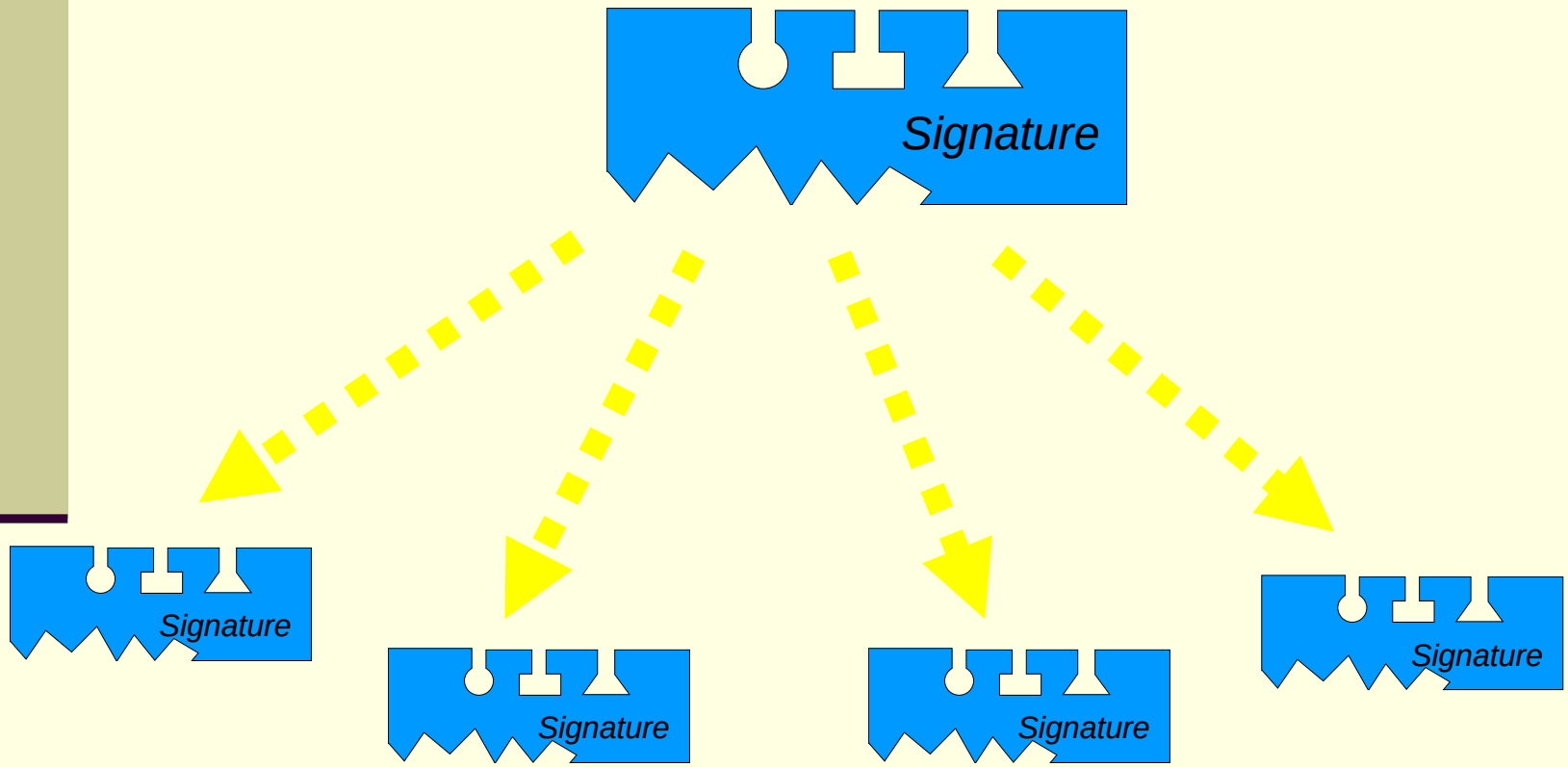
Eine digitale Unterschrift enthält die folgenden Daten:

- Eine Prüfsumme der Datei, zu der die Unterschrift gehört
- Die anonyme ID des Benutzers, der unterschrieben hat (nur wenn man selber dessen öffentlichen Schlüssel besitzt, kann man den Namen erkennen)
- Das lokale Datum und Uhrzeit, wann die Unterschrift gemacht wurde

```
Checking WSR4340.pdf.sig ...WSR4340.pdf.sig checked:
gpg: Signature made 07/14/08 13:46:47 using DSA key ID 5281A72F
gpg: Good signature from “xxxxxxxxx (xx CS1 E) <xxx.xxx@xxxtech-eu.com>"
gpg: Signature made 07/14/08 16:18:47 using DSA key ID F0F2F3EA
gpg: Good signature from yyyy yyyy (yy CS1 ME) <yyy.yyyy@sxxtech-eu.com>"
gpg: Signature made 07/15/08 12:44:15 using DSA key ID A6C128F6
gpg: Good signature from “zzzz zzzz (zzzz EESE) <zzzz@zzzzz.com>"
```

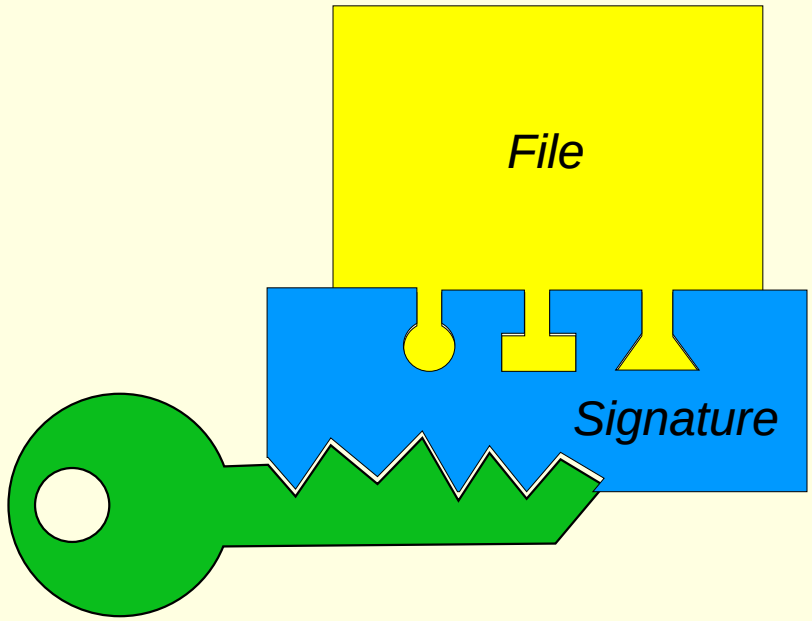
Verteilen einer Digitalen Unterschrift

- Die Unterschriftendatei wird an alle geschickt, die die Unterschrift benötigen



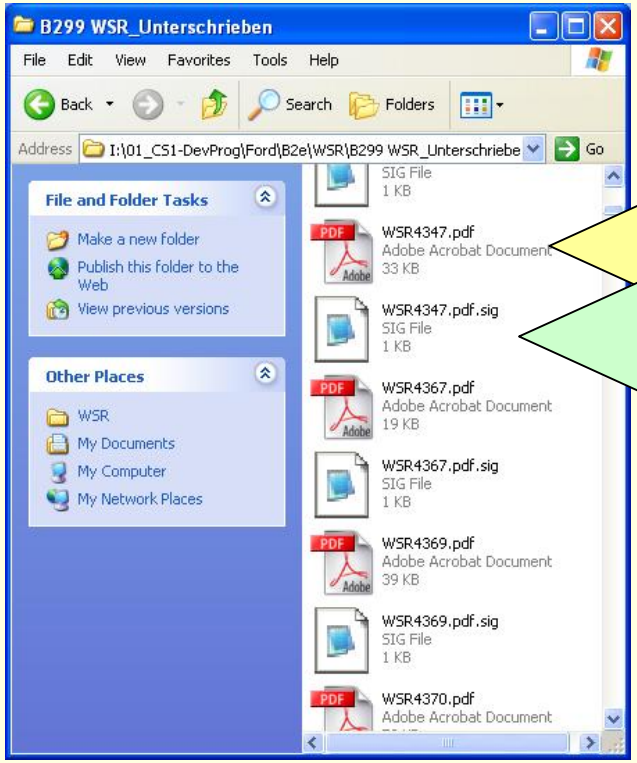
Überprüfen einer Digitalen Unterschrift

- Die anderen Benutzer überprüfen die Unterschrift durch Vergleichen der Prüfsumme mit ihrer eigenen lokalen Datei und der ID mit den in ihrem Schlüsselring gespeicherten Daten des öffentlichen Schlüssels



- Nur wenn beide Werte übereinstimmen, ist die Unterschrift gültig

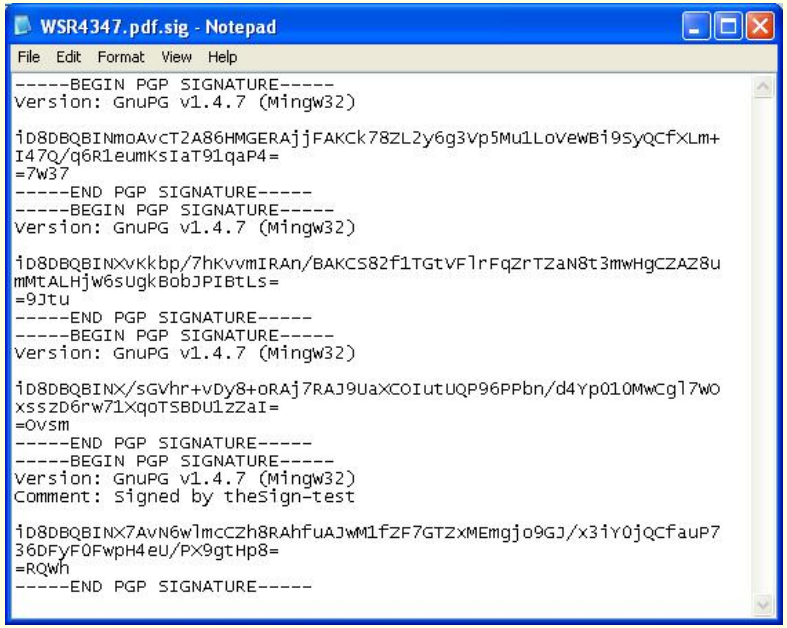
Speicherung der Unterschriften



Abgelegt werden dann die unveränderte Originaldatei und dazu die Unterschriften zusammengefasst in einer eigenen, gleichnamigen SIG- Datei

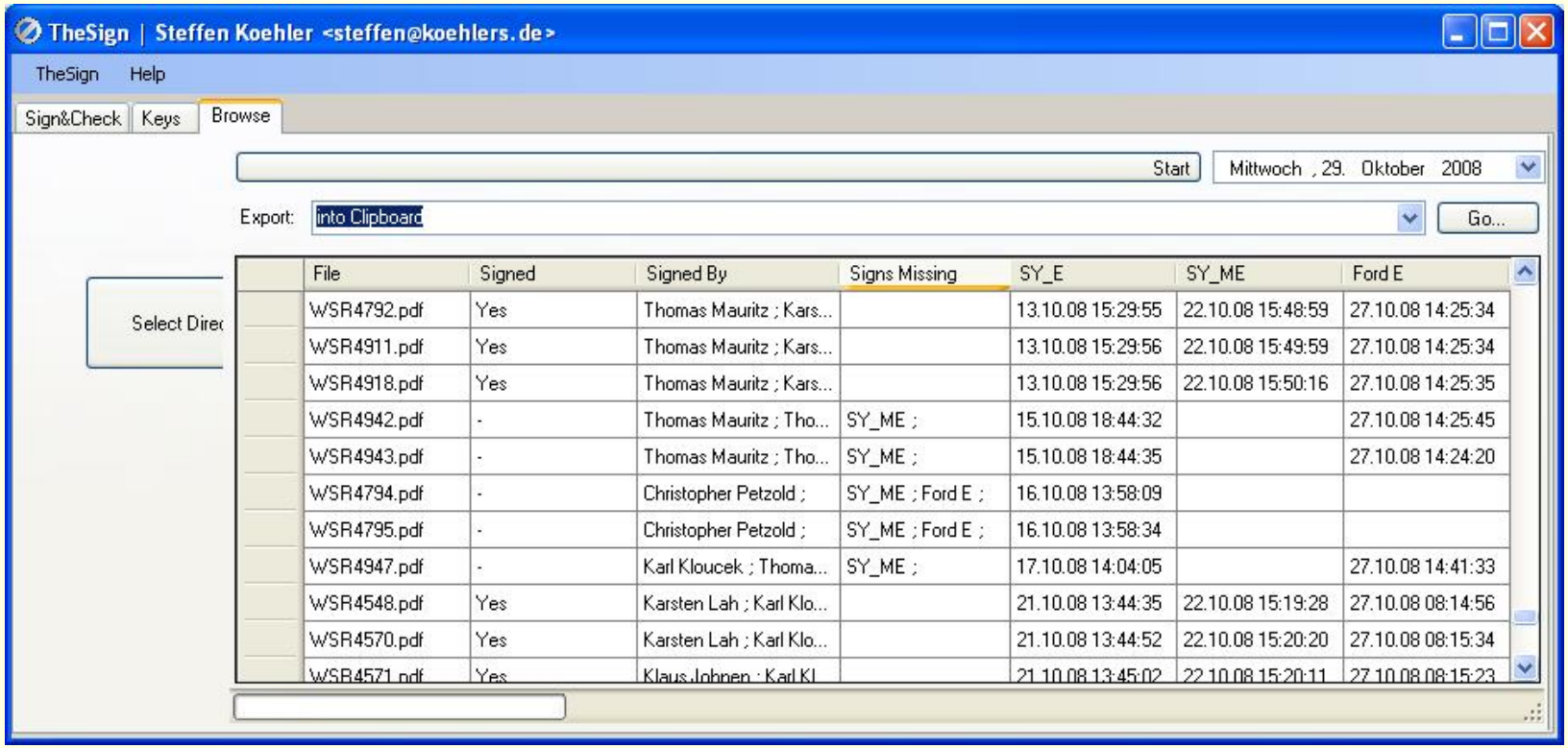
Original- Datei

Unterschriften- Datei



Überprüfung der Unterschriftensammlung

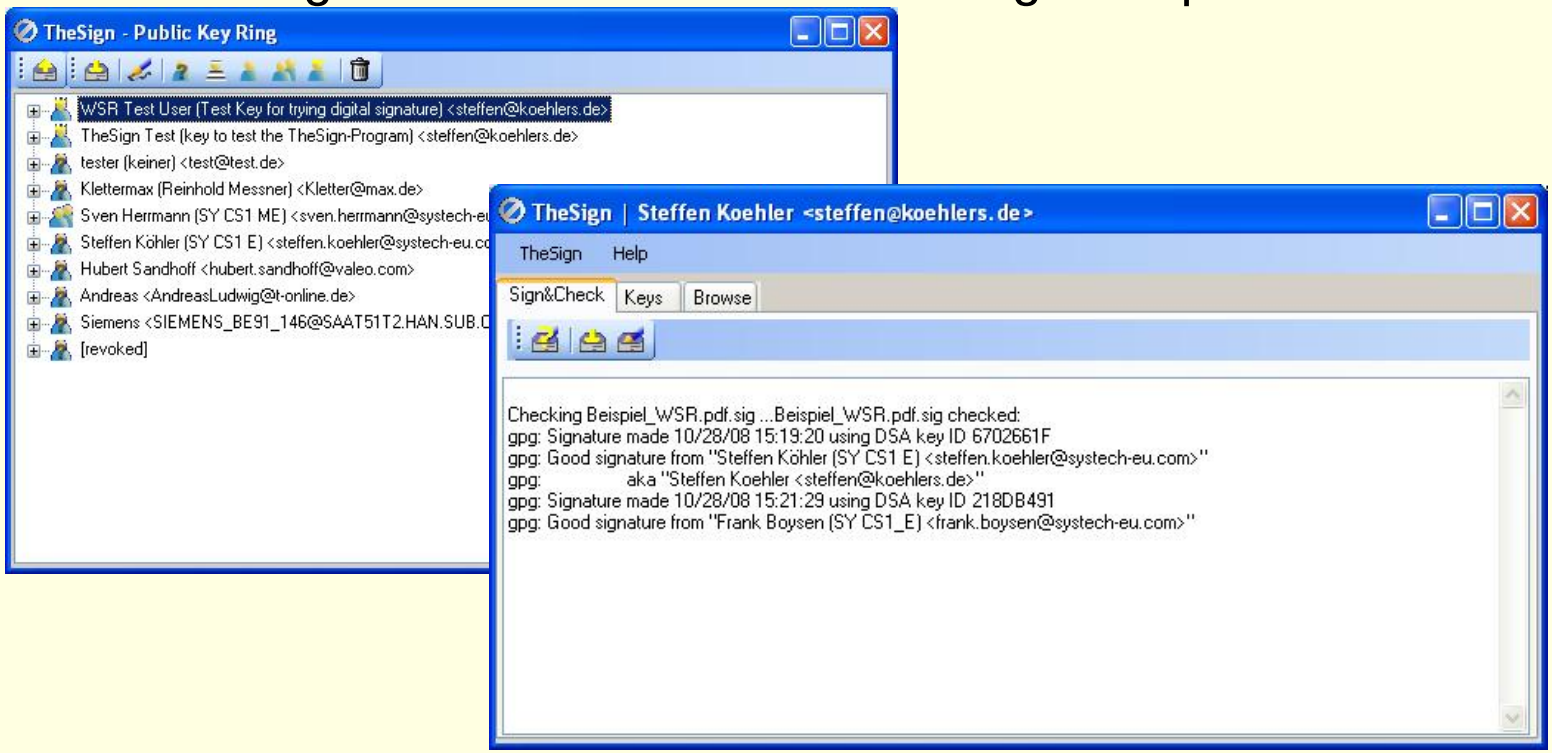
Die Software ermöglicht es, Unterschriftenregelungen zu definieren und diese dann auf Knopfdruck auf alle Dateien eines kompletten Verzeichnisses anzuwenden



File	Signed	Signed By	Signs Missing	SY_E	SY_ME	Ford E
WSR4792.pdf	Yes	Thomas Mauritz ; Kars...		13.10.08 15:29:55	22.10.08 15:48:59	27.10.08 14:25:34
WSR4911.pdf	Yes	Thomas Mauritz ; Kars...		13.10.08 15:29:56	22.10.08 15:49:59	27.10.08 14:25:34
WSR4918.pdf	Yes	Thomas Mauritz ; Kars...		13.10.08 15:29:56	22.10.08 15:50:16	27.10.08 14:25:35
WSR4942.pdf	-	Thomas Mauritz ; Tho...	SY_ME ;	15.10.08 18:44:32		27.10.08 14:25:45
WSR4943.pdf	-	Thomas Mauritz ; Tho...	SY_ME ;	15.10.08 18:44:35		27.10.08 14:24:20
WSR4794.pdf	-	Christopher Petzold ;	SY_ME ; Ford E ;	16.10.08 13:58:09		
WSR4795.pdf	-	Christopher Petzold ;	SY_ME ; Ford E ;	16.10.08 13:58:34		
WSR4947.pdf	-	Karl Kloucek ; Thoma...	SY_ME ;	17.10.08 14:04:05		27.10.08 14:41:33
WSR4548.pdf	Yes	Karsten Lah ; Karl Klo...		21.10.08 13:44:35	22.10.08 15:19:28	27.10.08 08:14:56
WSR4570.pdf	Yes	Karsten Lah ; Karl Klo...		21.10.08 13:44:52	22.10.08 15:20:20	27.10.08 08:15:34
WSR4571.pdf	Yes	Klaus Johnen ; Karl Kl...		21.10.08 13:45:02	22.10.08 15:20:11	27.10.08 08:15:23

TheSign – ein Programm für Alles

- Um all das Beschriebene auch machen zu können, wurde TheSign für eine einfache Bedienung konzipiert



- Weitere Informationen finden sich unter http://www.koehlers.de/wiki/doku.php?id=thesign:index