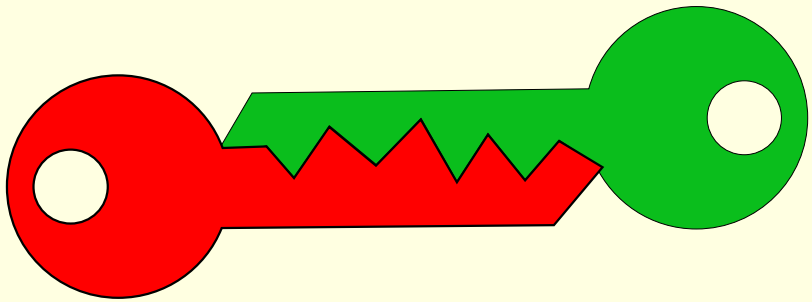
Digital Signatures for Newbies

- Digital Signatures are a clever approach of using complex mathematics in real life work
- Let‘s see how it works…

Setup Step 1 : Genererate your own key

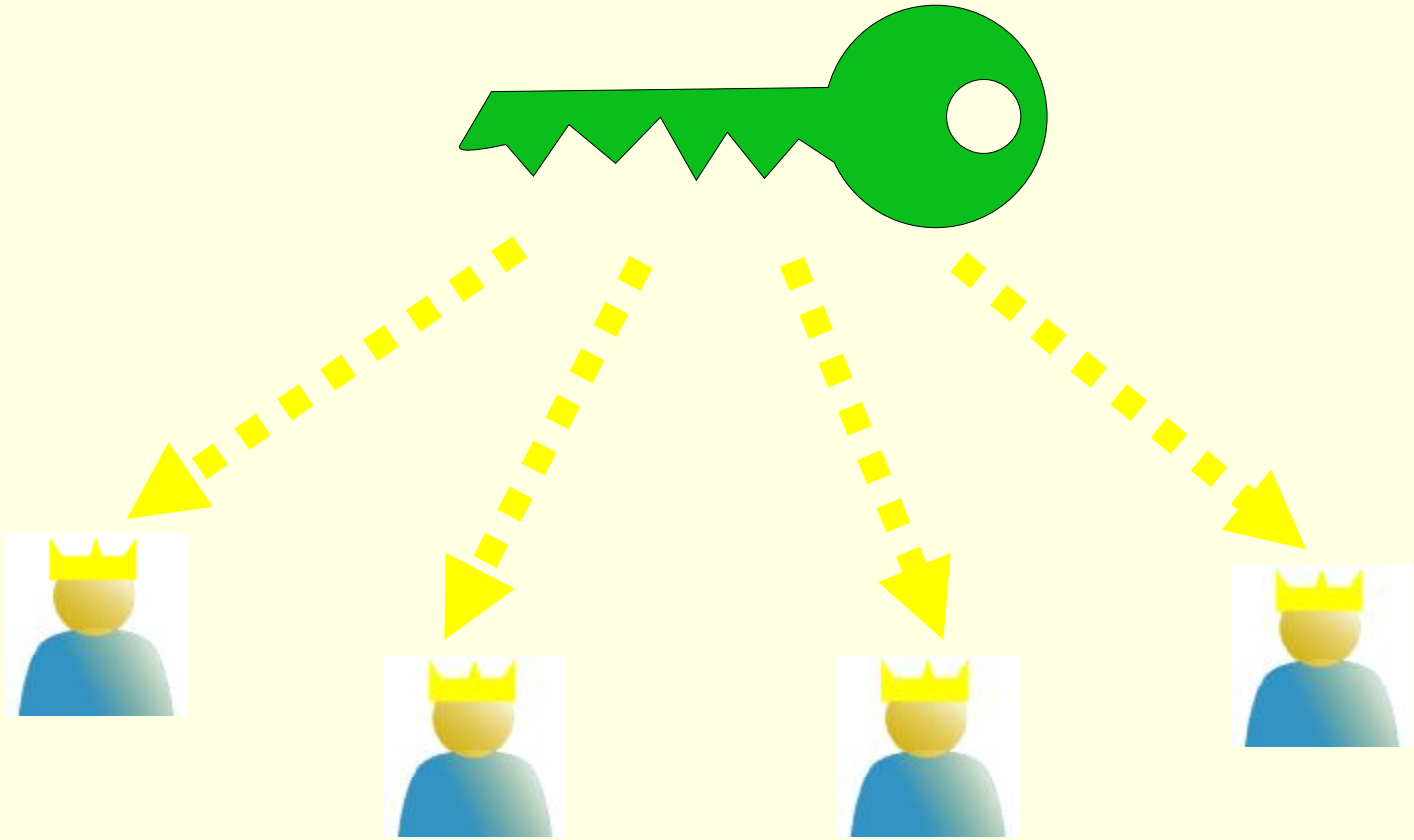
- First you create a Key pair containing a Public Key and a Secret Key.



- The access to your Secret Key is protected by a passphrase

Setup Step 2 : Publish the Public Key

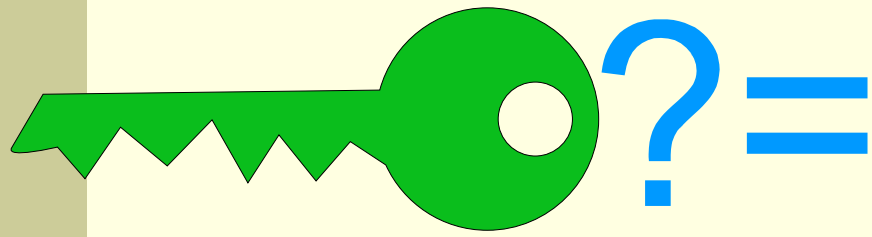
- Email the Public Key to the „Key Masters“



Digital Signatures with TheSign

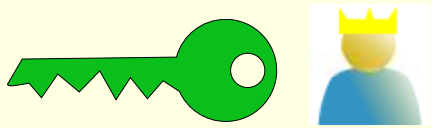
Setup Step 3 : Verify & Sign new Keys

- The „Key Masters“ verify your Public Key with your Key Certificate



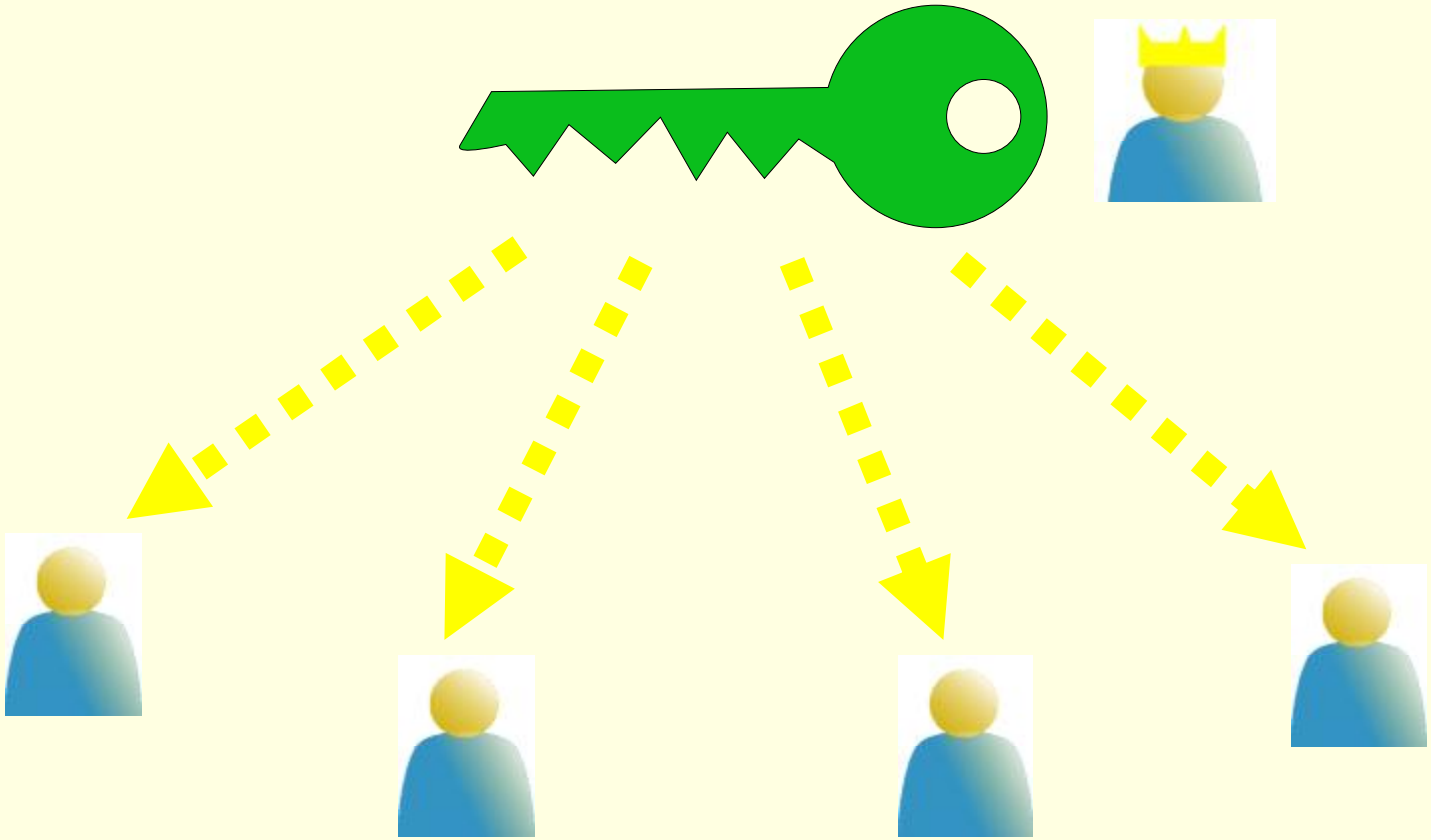
```
pub 1024D/6702661F 2003-05-04
Key fingerprint = A2E8 8737 3654 D5E2 031F 02B5 BCDE B096 6702 661F
uid Steffen Köehler (SY CS1 E)
uid Steffen Koehler
sub 1024g/FA8259DC 2003-05-04
```

- If it matches, they sign your key as valid



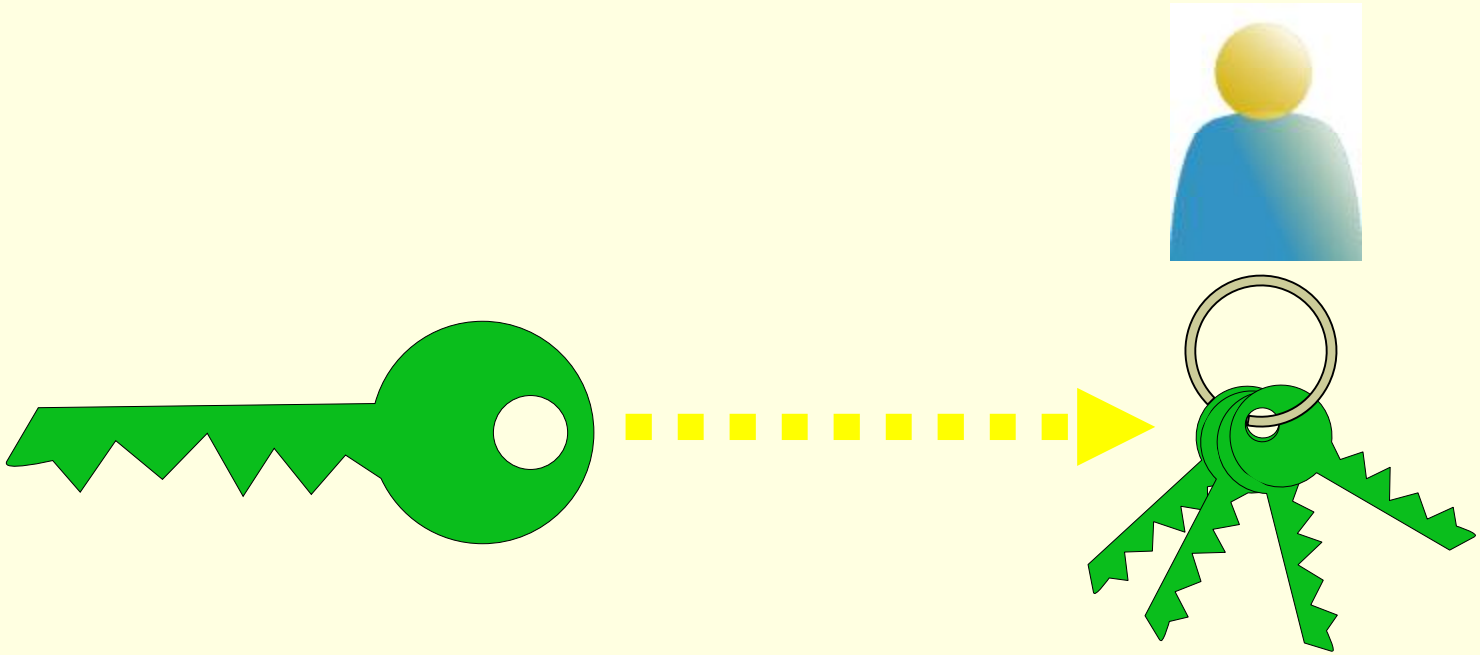
Setup Step 4 : Distribute the Public Key

- The Key Masters distribute the verified Key to all other users



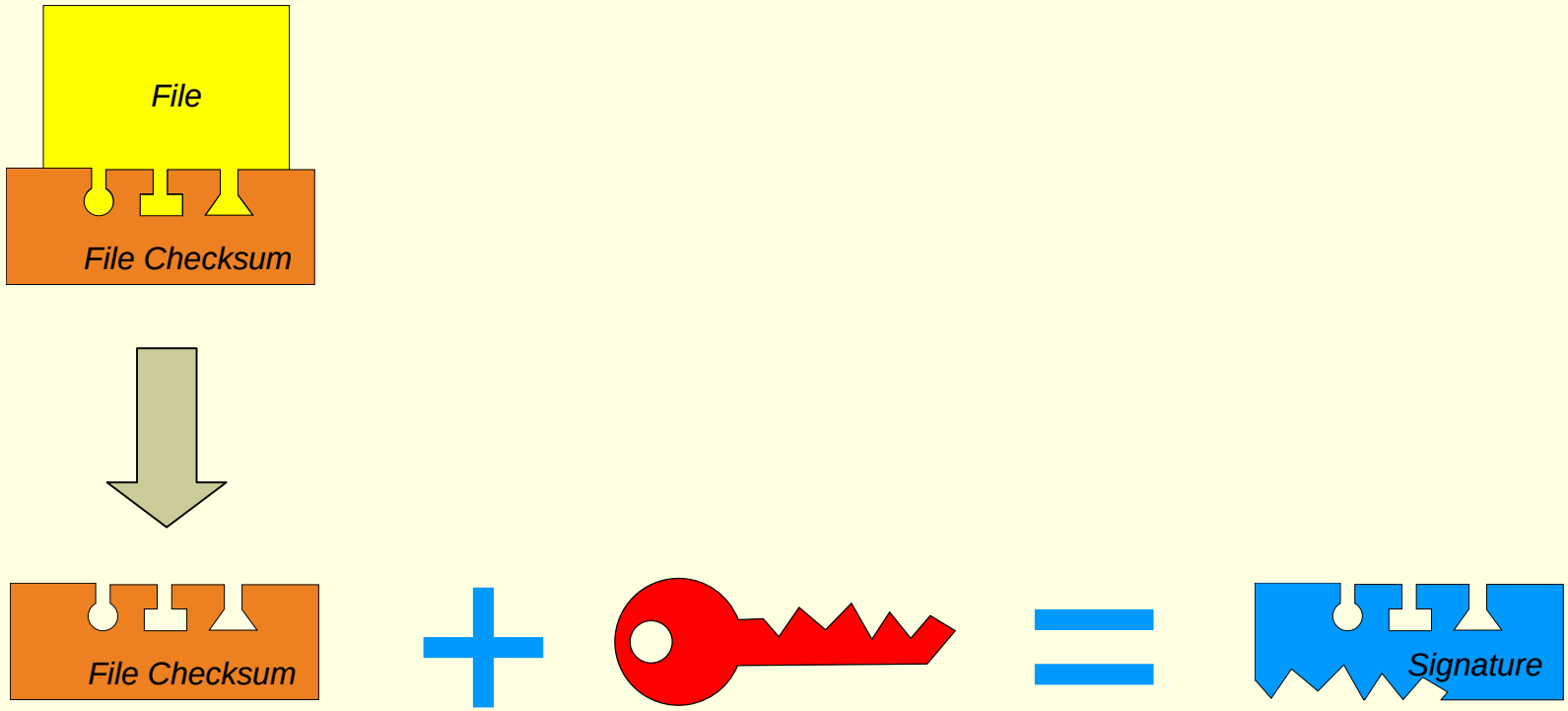
Setup Step 5 : Store received Keys

- The users add the received Public Keys to their Public Key Ring

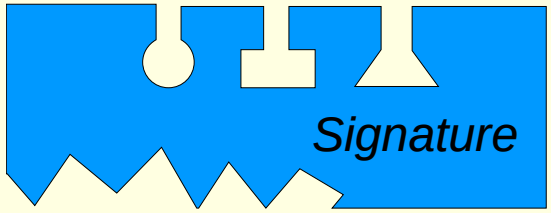


Creating a Digital Signature

- To sign a file, you create a Signature out of your Secret Key and the file checksum



Content of a Digital Signature



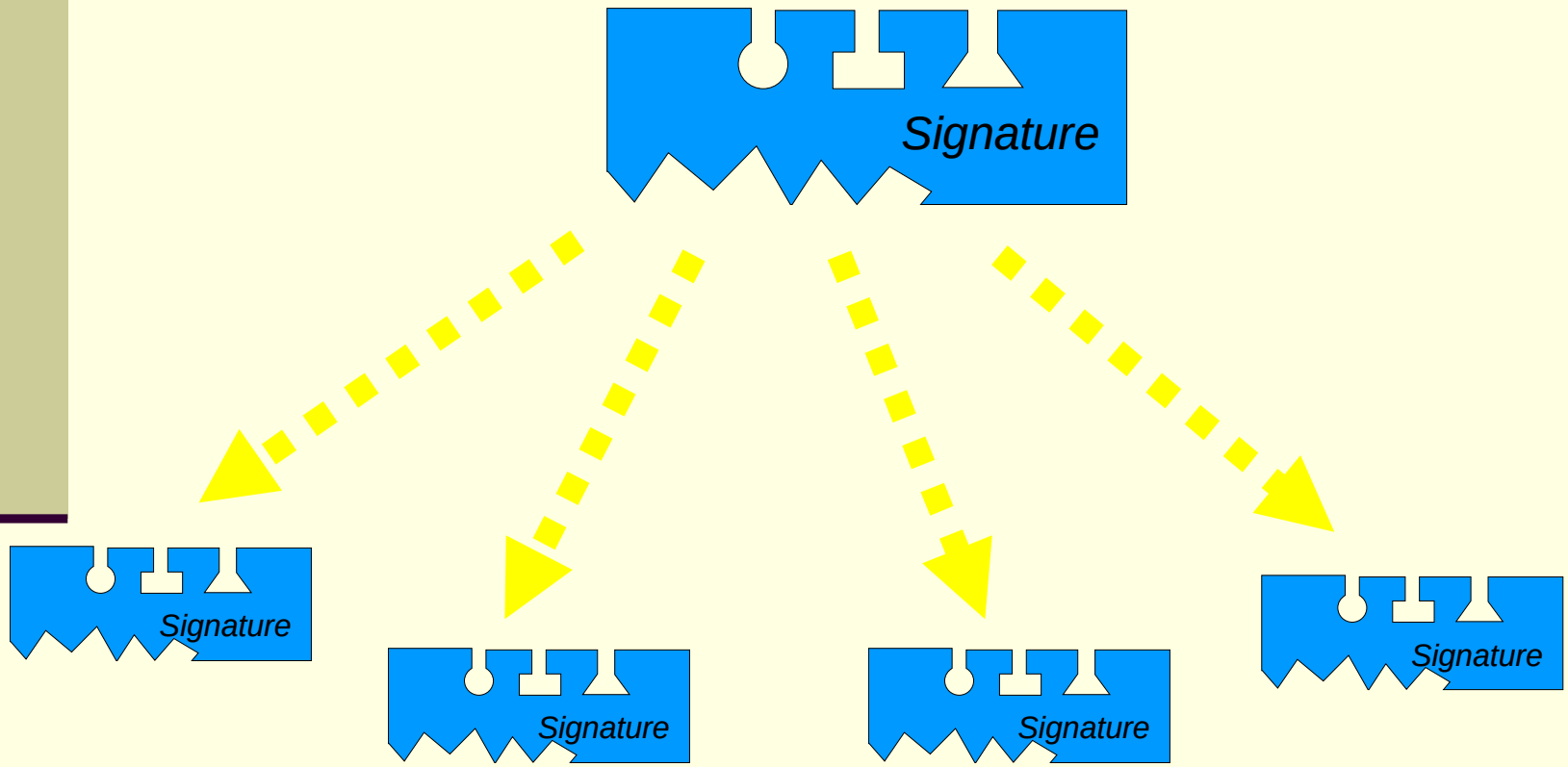
A digital signature contains the following data:

- A checksum of the file it belongs to
- The anonymus ID of the user, who signed the file (the users name can only found when having his public key)
- The local date and time when the signature was made

```
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>"
```

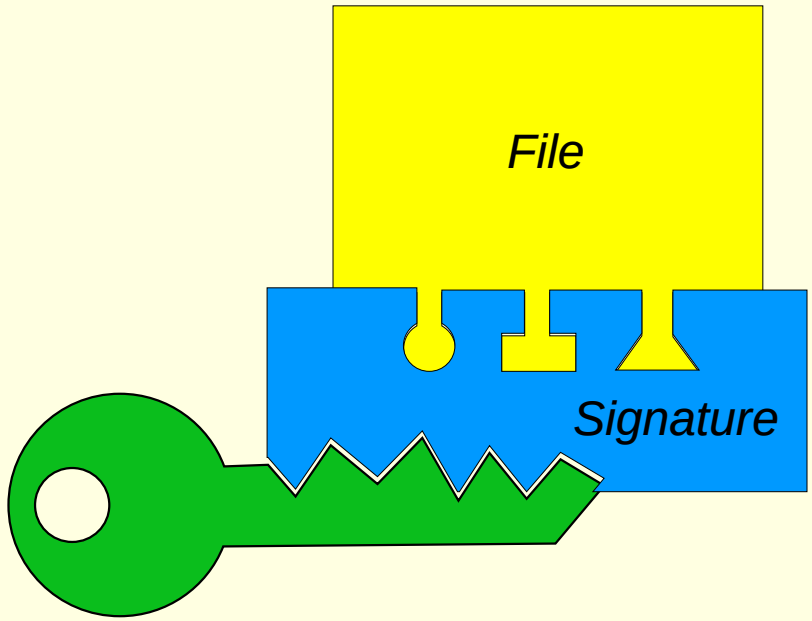
Distributing a Digital Signature

- Distribute the Signature to whoever needs it



Verifying a Digital Signature

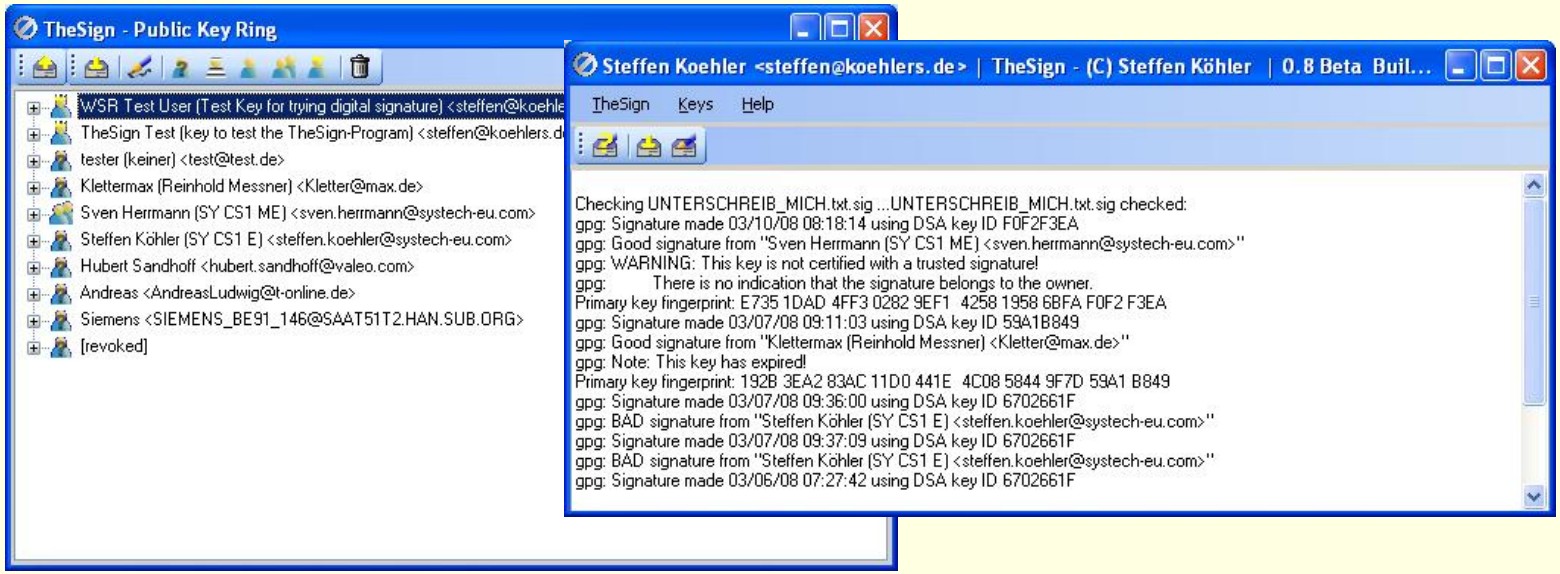
- The other users validate the Signature by compare it to the file checksum of their local file and the Public Key, stored in their Public Keyring



- Only if both matches, the Signature is valid

TheSign – the Tool to do all this

- To perform all these tasks, TheSign is been made to make it simple



- more information can be found at http://www.koehlers.de/wiki/doku.php?id=thesign:index