Inhaltsverzeichnis

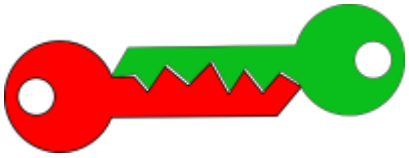
How do Digital Signatures work?

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

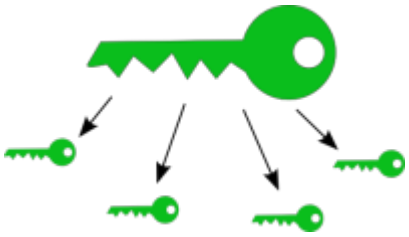
First you create a Key pair containing a Public Key and a Secret Key.



The access to your Secret Key is protected by a passphrase

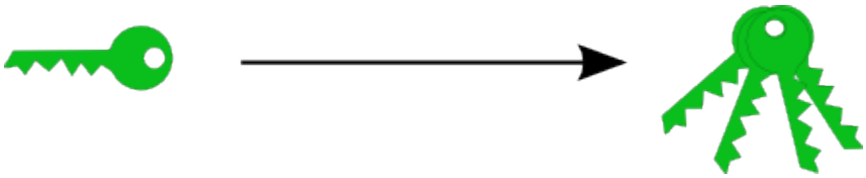
Setup Step 2 : Distribute your Public Key

Distribute your Public Key to other users



Maintenance: Store received keys

The users add received Public Keys to their Public Key Ring



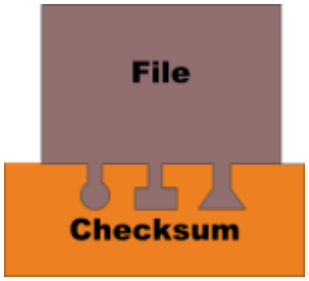
Maintenance: Verify received Keys

The other users verify your Public Key with your Key Certificate

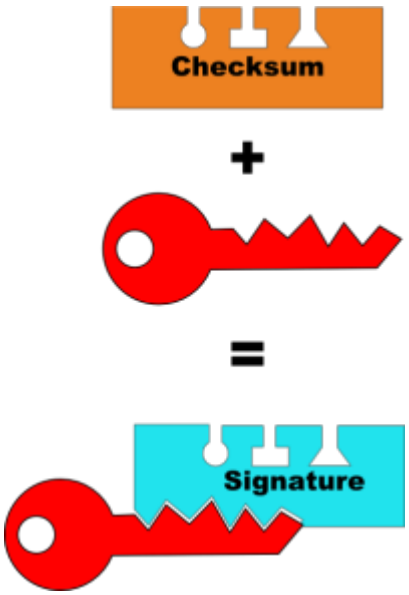
If it matches, they sign your key as valid

Creating a Digital Signature

To sign a file, first the checksum of the file is calculated

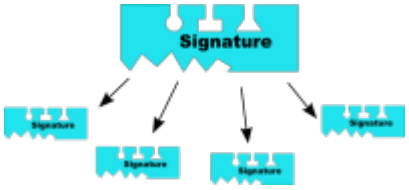


Then you create a Signature out of your Secret Key and the file checksum



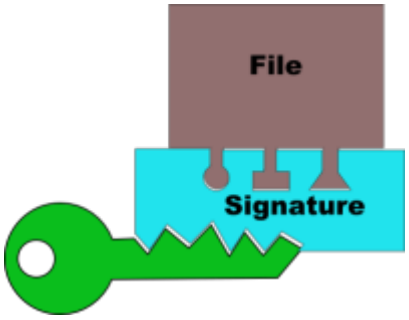
Distributing a Digital Signature

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 your Public Key stored in their Public Keyring



Only if both matches, the Signature is valid