



“In der Praxis gibt es zwei Formen von Kryptographie: Mit der einen Form der Kryptographie können Sie Ihre Dateien vielleicht vor Ihrer kleinen Schwester schützen, mit der anderen Form vor dem Zugriff durch Organisationen der Regierung.”

Bruce Schneier, „Applied Cryptography“

- Was ist GnuPG?
- Wie funktioniert GnuPG?
 - Verschlüsselungskonzepte
 - Digitale Unterschriften
 - Digitale Zertifikate
- Demo

Was ist GnuPG?

- Verschlüsselung von Daten die nur vom Empfänger wieder entschlüsselt werden können
- Erzeugung einer Signatur über die versendeten Daten, um deren Authentizität und Integrität zu gewährleisten.
- GnuPG ist eine Weiterentwicklung aus PGP

Warum GnuPG?

Wie funktioniert GnuPG?

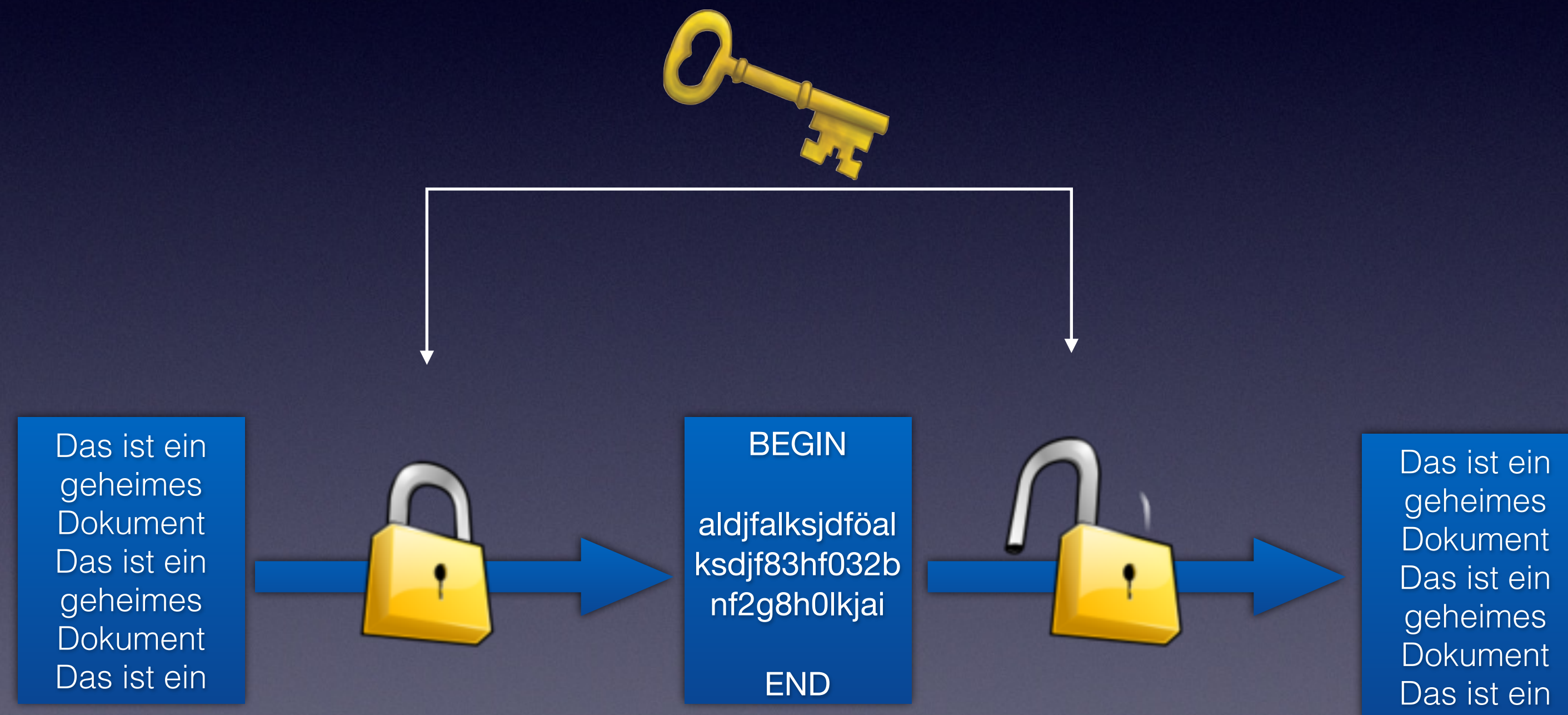
Wie funktioniert GnuPG?

Verschlüsselungskonzepte

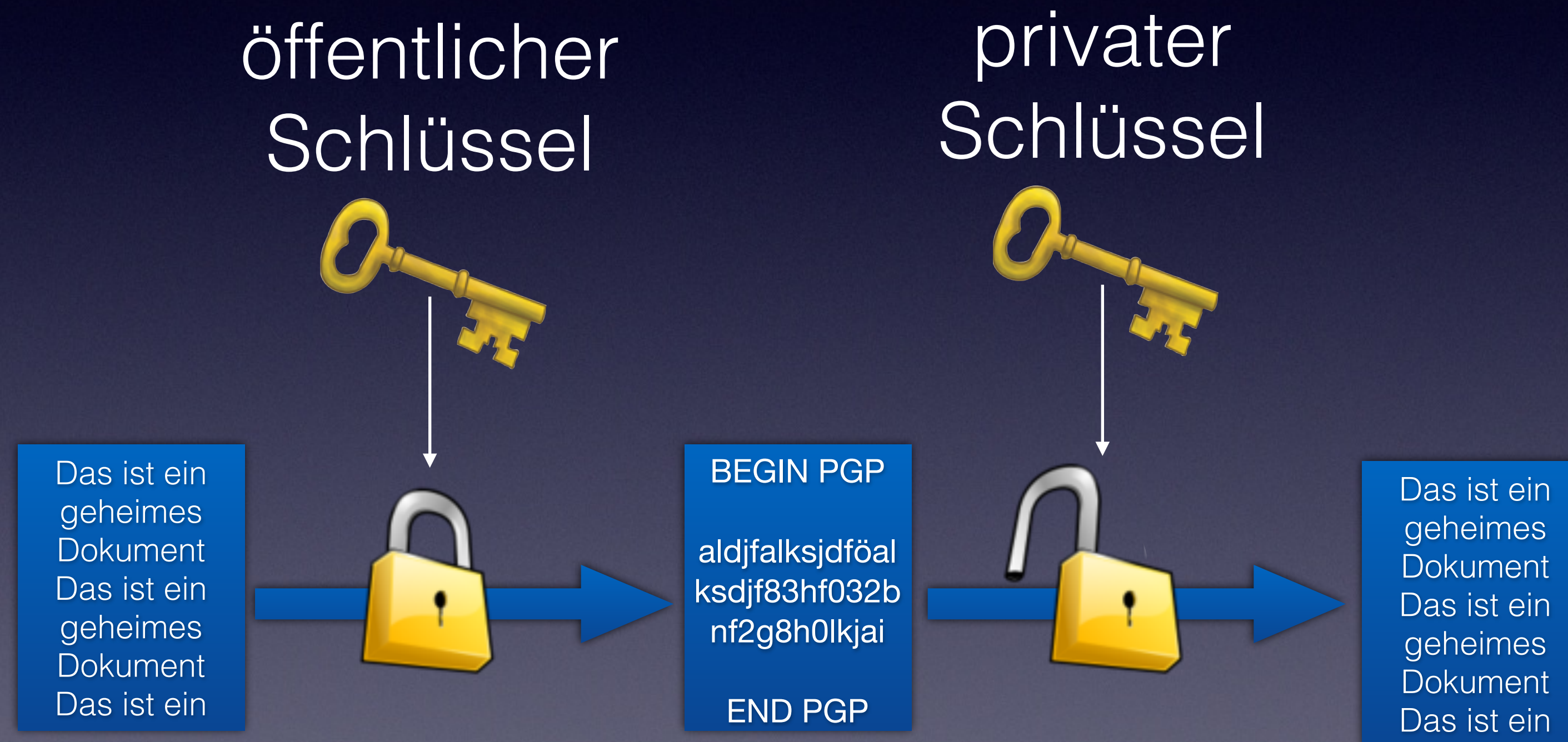
Verschlüsselungskonzepte

- Konventionelle Verschlüsselung (Symmetrisch)
- Public Key Verschlüsselung
- Hybride Verschlüsselung

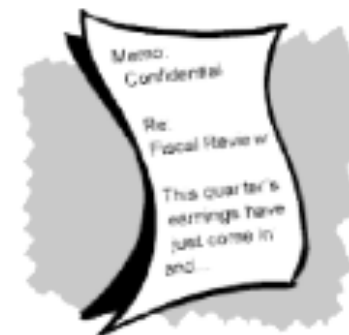
Konventionelle Verschlüsselung



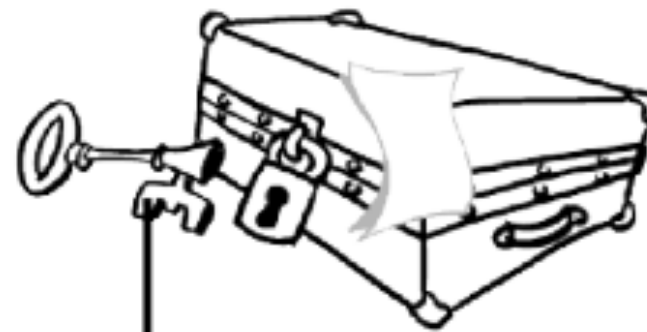
Public Key Verschlüsselung



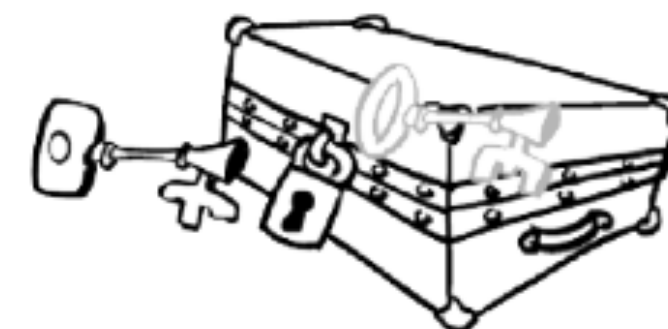
Hybride Verschlüsselung



**Klartext wird mit
Sitzungsschlüssel
verschlüsselt**



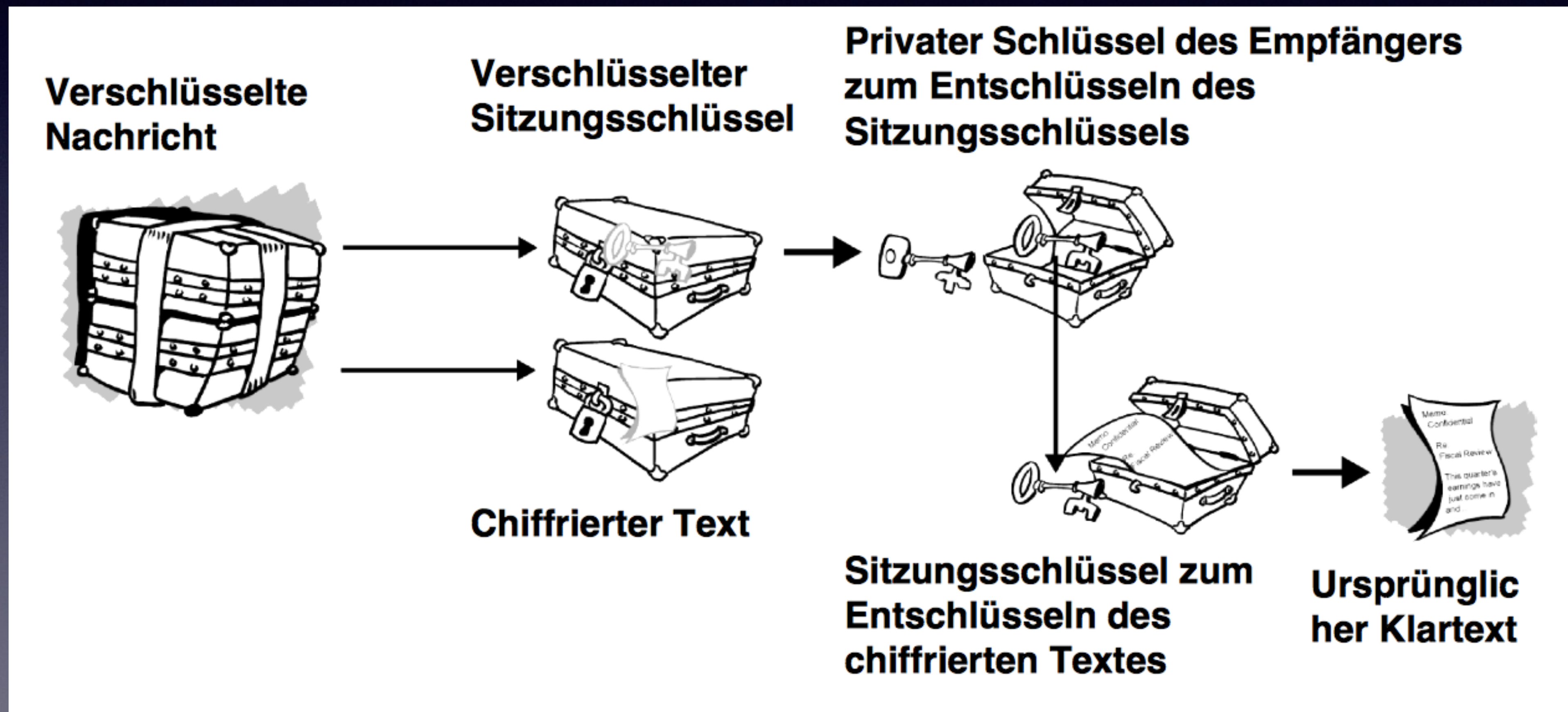
**Sitzungsschlüssel wird mit
öffentlichem Schlüssel verschlüsselt**



**Chiffrierter Text +
verschlüsselter Sitzungsschlüssel**



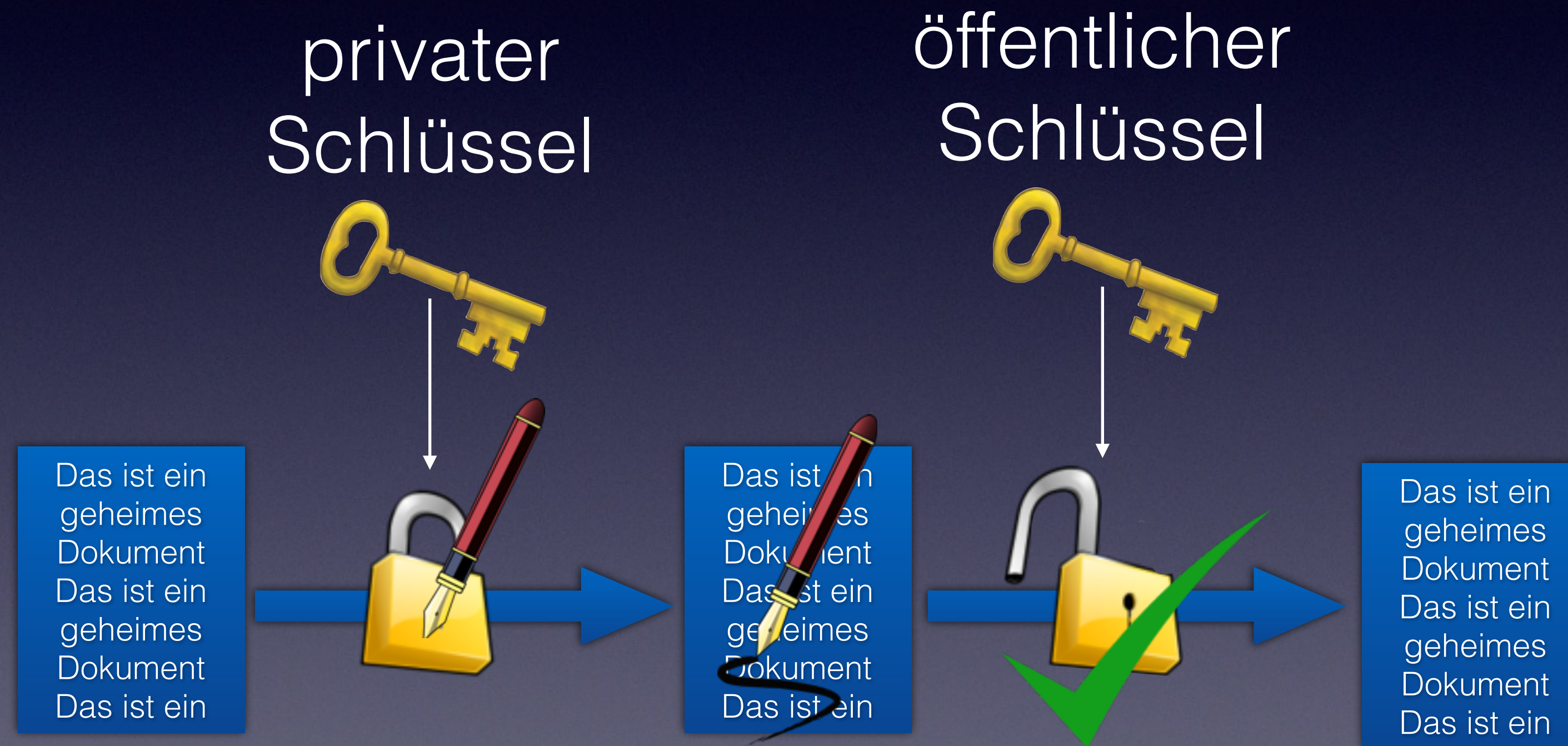
Hybride Verschlüsselung



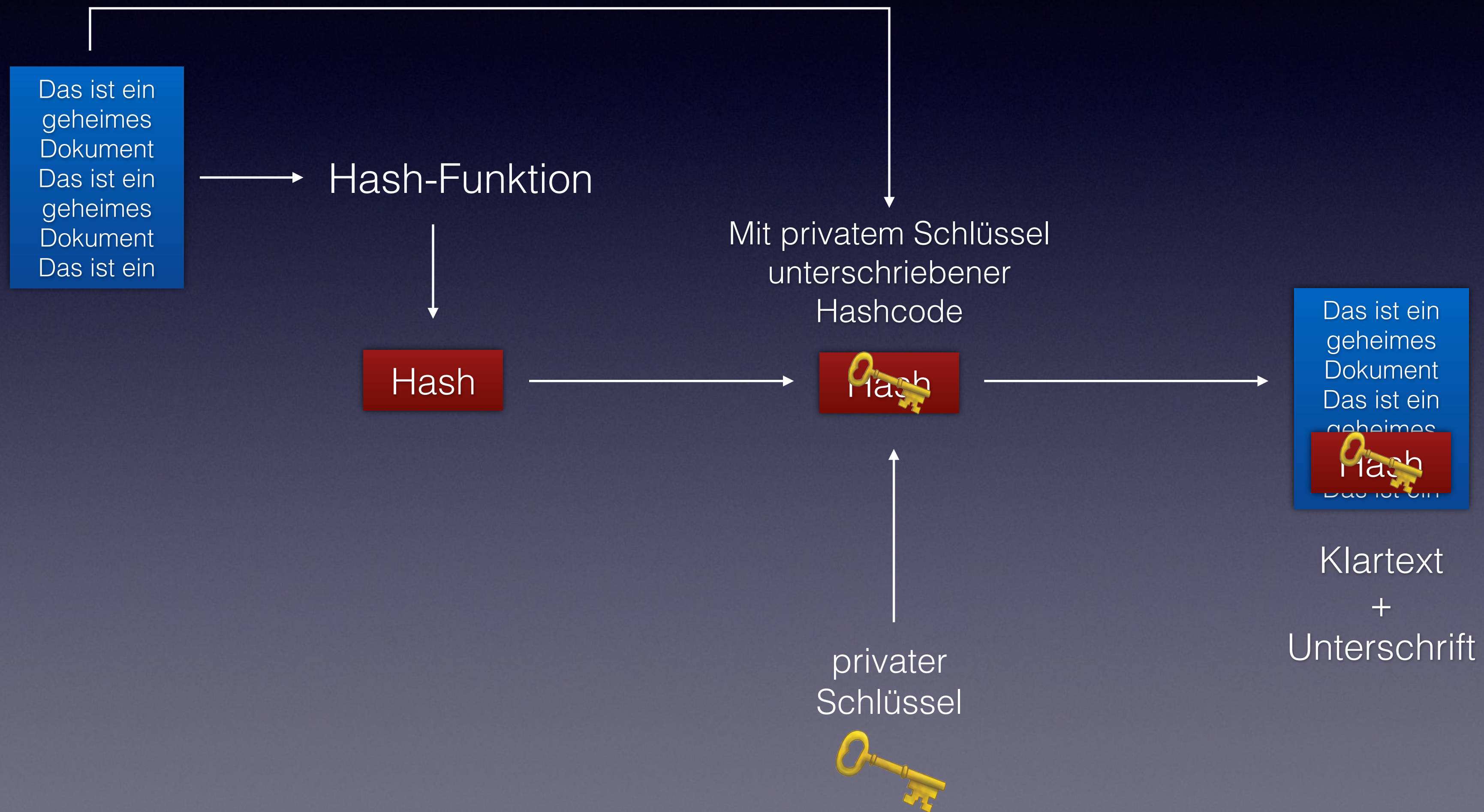
- Authentizität
- Integrität
- Nachweisbarkeit

Digitale Unterschriften

Digitale Unterschriften



Digitale Unterschriften



- Man kann nun Nachweisen, dass der Sender den Privatschlüssel zum öffentlichen Schlüssel hat
- die Echte Identität ist noch immer nicht bestätigt

Digitale Zertifikate

Digitale Zertifikate

- digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt
- Das digitale Zertifikat enthält insbesondere die zu seiner Prüfung erforderlichen Daten

Web of Trust

Demo

<http://www.gnupg.org>

```
SYSTEM-5:~ michaelnoppinger$ gpg --gen-key
```

gpg --gen-key

Schlüssel erzeugen


```
SYSTEM-5:~ michaelnoppinger$ gpg --gen-key
gpg (GnuPG/MacGPG2) 2.0.20; Copyright (C) 2013 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Bitte wählen Sie, welche Art von Schlüssel Sie möchten:
  (1) RSA und RSA (voreingestellt)
  (2) DSA und Elgamal
  (3) DSA (nur signieren/beglaubigen)
  (4) RSA (nur signieren/beglaubigen)
Ihre Auswahl? █
```

gpg --gen-key

Schlüssel erzeugen

```
SYSTEM-5:~ michaelnoppinger$ gpg --gen-key
gpg (GnuPG/MacGPG2) 2.0.20; Copyright (C) 2013 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Bitte wählen Sie, welche Art von Schlüssel Sie möchten:
  (1) RSA und RSA (voreingestellt)
  (2) DSA und Elgamal
  (3) DSA (nur signieren/beglaubigen)
  (4) RSA (nur signieren/beglaubigen)
Ihre Auswahl? 1
```

gpg --gen-key

Schlüssel erzeugen

```
SYSTEM-5:~ michaelnoppinger$ gpg --gen-key
gpg (GnuPG/MacGPG2) 2.0.20; Copyright (C) 2013 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Bitte wählen Sie, welche Art von Schlüssel Sie möchten:
  (1) RSA und RSA (voreingestellt)
  (2) DSA und Elgamal
  (3) DSA (nur signieren/beglaubigen)
  (4) RSA (nur signieren/beglaubigen)
Ihre Auswahl? 1
RSA-Schlüssel können zwischen 1024 und 8192 Bit lang sein.
Welche Schlüssellänge wünschen Sie? (2048) █
```

gpg --gen-key

Schlüssel erzeugen

```
SYSTEM-5:~ michaelnoppinger$ gpg --gen-key
gpg (GnuPG/MacGPG2) 2.0.20; Copyright (C) 2013 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Bitte wählen Sie, welche Art von Schlüssel Sie möchten:
  (1) RSA und RSA (voreingestellt)
  (2) DSA und Elgamal
  (3) DSA (nur signieren/beglaubigen)
  (4) RSA (nur signieren/beglaubigen)
Ihre Auswahl? 1
RSA-Schlüssel können zwischen 1024 und 8192 Bit lang sein.
Welche Schlüssellänge wünschen Sie? (2048) 1024
```

gpg --gen-key

Schlüssel erzeugen

Bitte wählen Sie, welche Art von Schlüssel Sie möchten:

- (1) RSA und RSA (voreingestellt)
- (2) DSA und Elgamal
- (3) DSA (nur signieren/beglaubigen)
- (4) RSA (nur signieren/beglaubigen)

Ihre Auswahl? 1

RSA-Schlüssel können zwischen 1024 und 8192 Bit lang sein.

Welche Schlüssellänge wünschen Sie? (2048) 1024

Die verlangte Schlüssellänge beträgt 1024 Bit

Bitte wählen Sie, wie lange der Schlüssel gültig bleiben soll.

- 0 = Schlüssel verfällt nie
- <n> = Schlüssel verfällt nach n Tagen
- <n>w = Schlüssel verfällt nach n Wochen
- <n>m = Schlüssel verfällt nach n Monaten
- <n>y = Schlüssel verfällt nach n Jahren

Wie lange bleibt der Schlüssel gültig? (0) █

gpg --gen-key

Schlüssel erzeugen

```
⓪ ⓪ ⓪ michaelnoppinger — gpg2 — 79x19
Bitte wählen Sie, welche Art von Schlüssel Sie möchten:
  (1) RSA und RSA (voreingestellt)
  (2) DSA und Elgamal
  (3) DSA (nur signieren/beglaubigen)
  (4) RSA (nur signieren/beglaubigen)
Ihre Auswahl? 1
RSA-Schlüssel können zwischen 1024 und 8192 Bit lang sein.
Welche Schlüssellänge wünschen Sie? (2048) 1024
Die verlangte Schlüssellänge beträgt 1024 Bit
Bitte wählen Sie, wie lange der Schlüssel gültig bleiben soll.
  0 = Schlüssel verfällt nie
  <n> = Schlüssel verfällt nach n Tagen
  <n>w = Schlüssel verfällt nach n Wochen
  <n>m = Schlüssel verfällt nach n Monaten
  <n>y = Schlüssel verfällt nach n Jahren
Wie lange bleibt der Schlüssel gültig? (0) 1y
```

gpg --gen-key

Schlüssel erzeugen

```
⓪ ⓪ ⓪ michaelnoppinger — gpg2 — 79x17
(1) RSA und RSA (voreingestellt)
(2) DSA und Elgamal
(3) DSA (nur signieren/beglaubigen)
(4) RSA (nur signieren/beglaubigen)
Ihre Auswahl? 1
RSA-Schlüssel können zwischen 1024 und 8192 Bit lang sein.
Welche Schlüssellänge wünschen Sie? (2048) 1024
Die verlangte Schlüssellänge beträgt 1024 Bit
Bitte wählen Sie, wie lange der Schlüssel gültig bleiben soll.
    0 = Schlüssel verfällt nie
    <n> = Schlüssel verfällt nach n Tagen
    <n>w = Schlüssel verfällt nach n Wochen
    <n>m = Schlüssel verfällt nach n Monaten
    <n>y = Schlüssel verfällt nach n Jahren
Wie lange bleibt der Schlüssel gültig? (0) 1y
Key verfällt am Sa 31 Jan 02:08:35 2015 CET
Ist dies richtig? (j/N) █
```

gpg --gen-key

Schlüssel erzeugen

```
⓪ ⓪ ⓪ michaelnoppinger — gpg2 — 79x17
(1) RSA und RSA (voreingestellt)
(2) DSA und Elgamal
(3) DSA (nur signieren/beglaubigen)
(4) RSA (nur signieren/beglaubigen)
Ihre Auswahl? 1
RSA-Schlüssel können zwischen 1024 und 8192 Bit lang sein.
Welche Schlüssellänge wünschen Sie? (2048) 1024
Die verlangte Schlüssellänge beträgt 1024 Bit
Bitte wählen Sie, wie lange der Schlüssel gültig bleiben soll.
    0 = Schlüssel verfällt nie
    <n> = Schlüssel verfällt nach n Tagen
    <n>w = Schlüssel verfällt nach n Wochen
    <n>m = Schlüssel verfällt nach n Monaten
    <n>y = Schlüssel verfällt nach n Jahren
Wie lange bleibt der Schlüssel gültig? (0) 1y
Key verfällt am Sa 31 Jan 02:08:35 2015 CET
Ist dies richtig? (j/N) j
```

gpg --gen-key

Schlüssel erzeugen


```
© ○ ○ michaelnoppinger — gpg2 — 79x17
Ihre Auswahl? 1
RSA-Schlüssel können zwischen 1024 und 8192 Bit lang sein.
Welche Schlüssellänge wünschen Sie? (2048) 1024
Die verlangte Schlüssellänge beträgt 1024 Bit
Bitte wählen Sie, wie lange der Schlüssel gültig bleiben soll.
    0 = Schlüssel verfällt nie
    <n> = Schlüssel verfällt nach n Tagen
    <n>w = Schlüssel verfällt nach n Wochen
    <n>m = Schlüssel verfällt nach n Monaten
    <n>y = Schlüssel verfällt nach n Jahren
Wie lange bleibt der Schlüssel gültig? (0) 1y
Key verfällt am Sa 31 Jan 02:08:35 2015 CET
Ist dies richtig? (j/N) j

GnuPG erstellt eine User-ID um Ihren Schlüssel identifizierbar zu machen.

Ihr Name ("Vorname Nachname"): █
```

gpg --gen-key

Schlüssel erzeugen

```
© ○ ○ michaelnoppinger — gpg2 — 79x17
Ihre Auswahl? 1
RSA-Schlüssel können zwischen 1024 und 8192 Bit lang sein.
Welche Schlüssellänge wünschen Sie? (2048) 1024
Die verlangte Schlüssellänge beträgt 1024 Bit
Bitte wählen Sie, wie lange der Schlüssel gültig bleiben soll.
    0 = Schlüssel verfällt nie
    <n> = Schlüssel verfällt nach n Tagen
    <n>w = Schlüssel verfällt nach n Wochen
    <n>m = Schlüssel verfällt nach n Monaten
    <n>y = Schlüssel verfällt nach n Jahren
Wie lange bleibt der Schlüssel gültig? (0) 1y
Key verfällt am Sa 31 Jan 02:08:35 2015 CET
Ist dies richtig? (j/N) j

GnuPG erstellt eine User-ID um Ihren Schlüssel identifizierbar zu machen.

Ihr Name ("Vorname Nachname"): Max Mustermann
```

gpg --gen-key

Schlüssel erzeugen

```
© ○ ○ michaelnoppinger — gpg2 — 79x17
RSA-Schlüssel können zwischen 1024 und 8192 Bit lang sein.
Welche Schlüssellänge wünschen Sie? (2048) 1024
Die verlangte Schlüssellänge beträgt 1024 Bit
Bitte wählen Sie, wie lange der Schlüssel gültig bleiben soll.
    0 = Schlüssel verfällt nie
    <n> = Schlüssel verfällt nach n Tagen
    <n>w = Schlüssel verfällt nach n Wochen
    <n>m = Schlüssel verfällt nach n Monaten
    <n>y = Schlüssel verfällt nach n Jahren
Wie lange bleibt der Schlüssel gültig? (0) 1y
Key verfällt am Sa 31 Jan 02:08:35 2015 CET
Ist dies richtig? (j/N) j

GnuPG erstellt eine User-ID um Ihren Schlüssel identifizierbar zu machen.

Ihr Name ("Vorname Nachname"): Max Mustermann
Email-Adresse: █
```

gpg --gen-key

Schlüssel erzeugen

```
© ○ ○ michaelnoppinger — gpg2 — 79x17
RSA-Schlüssel können zwischen 1024 und 8192 Bit lang sein.
Welche Schlüssellänge wünschen Sie? (2048) 1024
Die verlangte Schlüssellänge beträgt 1024 Bit
Bitte wählen Sie, wie lange der Schlüssel gültig bleiben soll.
    0 = Schlüssel verfällt nie
    <n> = Schlüssel verfällt nach n Tagen
    <n>w = Schlüssel verfällt nach n Wochen
    <n>m = Schlüssel verfällt nach n Monaten
    <n>y = Schlüssel verfällt nach n Jahren
Wie lange bleibt der Schlüssel gültig? (0) 1y
Key verfällt am Sa 31 Jan 02:08:35 2015 CET
Ist dies richtig? (j/N) j

GnuPG erstellt eine User-ID um Ihren Schlüssel identifizierbar zu machen.

Ihr Name ("Vorname Nachname"): Max Mustermann
Email-Adresse: max@mustermann.at
```

gpg --gen-key

Schlüssel erzeugen

```
© ○ ○ michaelnoppinger — gpg2 — 79x17
Welche Schlüssellänge wünschen Sie? (2048) 1024
Die verlangte Schlüssellänge beträgt 1024 Bit
Bitte wählen Sie, wie lange der Schlüssel gültig bleiben soll.
    0 = Schlüssel verfällt nie
    <n> = Schlüssel verfällt nach n Tagen
    <n>w = Schlüssel verfällt nach n Wochen
    <n>m = Schlüssel verfällt nach n Monaten
    <n>y = Schlüssel verfällt nach n Jahren
Wie lange bleibt der Schlüssel gültig? (0) 1y
Key verfällt am Sa 31 Jan 02:08:35 2015 CET
Ist dies richtig? (j/N) j

GnuPG erstellt eine User-ID um Ihren Schlüssel identifizierbar zu machen.

Ihr Name ("Vorname Nachname"): Max Mustermann
Email-Adresse: max@mustermann.at
Kommentar: █
```

gpg --gen-key

Schlüssel erzeugen

```
© ○ ○ michaelnoppinger — gpg2 — 79x17
Welche Schlüssellänge wünschen Sie? (2048) 1024
Die verlangte Schlüssellänge beträgt 1024 Bit
Bitte wählen Sie, wie lange der Schlüssel gültig bleiben soll.
    0 = Schlüssel verfällt nie
    <n> = Schlüssel verfällt nach n Tagen
    <n>w = Schlüssel verfällt nach n Wochen
    <n>m = Schlüssel verfällt nach n Monaten
    <n>y = Schlüssel verfällt nach n Jahren
Wie lange bleibt der Schlüssel gültig? (0) 1y
Key verfällt am Sa 31 Jan 02:08:35 2015 CET
Ist dies richtig? (j/N) j

GnuPG erstellt eine User-ID um Ihren Schlüssel identifizierbar zu machen.

Ihr Name ("Vorname Nachname"): Max Mustermann
Email-Adresse: max@mustermann.at
Kommentar: Das ist der Schluessel von Max Mustermann.█
```

gpg --gen-key

Schlüssel erzeugen

```
© ○ ○ michaelnoppinger — gpg2 — 79x17
  <n>w = Schlüssel verfällt nach n Wochen
  <n>m = Schlüssel verfällt nach n Monaten
  <n>y = Schlüssel verfällt nach n Jahren
Wie lange bleibt der Schlüssel gültig? (0) 1y
Key verfällt am Sa 31 Jan 02:08:35 2015 CET
Ist dies richtig? (j/N) j

GnuPG erstellt eine User-ID um Ihren Schlüssel identifizierbar zu machen.

Ihr Name ("Vorname Nachname"): Max Mustermann
Email-Adresse: max@mustermann.at
Kommentar: Das ist der Schluessel von Max Mustermann.
Sie haben diese User-ID gewählt:
  "Max Mustermann (Das ist der Schluessel von Max Mustermann.) <max@musterman
n.at>"

Ändern: (N)ame, (K)ommentar, (E)-Mail oder (F)ertig/(A)bbrechen? █
```

gpg --gen-key

Schlüssel erzeugen

```
© ○ ○ michaelnoppinger — gpg2 — 79x17
  <n>w = Schlüssel verfällt nach n Wochen
  <n>m = Schlüssel verfällt nach n Monaten
  <n>y = Schlüssel verfällt nach n Jahren
Wie lange bleibt der Schlüssel gültig? (0) 1y
Key verfällt am Sa 31 Jan 02:08:35 2015 CET
Ist dies richtig? (j/N) j

GnuPG erstellt eine User-ID um Ihren Schlüssel identifizierbar zu machen.

Ihr Name ("Vorname Nachname"): Max Mustermann
Email-Adresse: max@mustermann.at
Kommentar: Das ist der Schluessel von Max Mustermann.
Sie haben diese User-ID gewählt:
  "Max Mustermann (Das ist der Schluessel von Max Mustermann.) <max@musterman
n.at>"

Ändern: (N)ame, (K)ommentar, (E)-Mail oder (F)ertig/(A)bbrechen? F
```

gpg --gen-key

Schlüssel erzeugen


```
© ○ ○ michaelnoppinger — gpg2 — 79x17
Wie lange bleibt der Schlüssel gültig? (0) 1y
Key verfällt am Sa 31 Jan 02:08:35 2015 CET
Ist dies richtig? (j/N) j

GnuPG erstellt eine User-ID um Ihren Schlüssel identifizierbar zu machen.

Ihr Name ("Vorname Nachname"): Max Mustermann
Email-Adresse: max@mustermann.at
Kommentar: Das ist der Schluessel von Max Mustermann.
Sie haben diese User-ID gewählt:
    "Max Mustermann (Das ist der Schluessel von Max Mustermann.) <max@musterman
n.at>"

Ändern: (N)ame, (K)ommentar, (E)-Mail oder (F)ertig/(A)bbrechen? F
Sie benötigen eine Passphrase, um den geheimen Schlüssel zu schützen.

█
```

gpg --gen-key

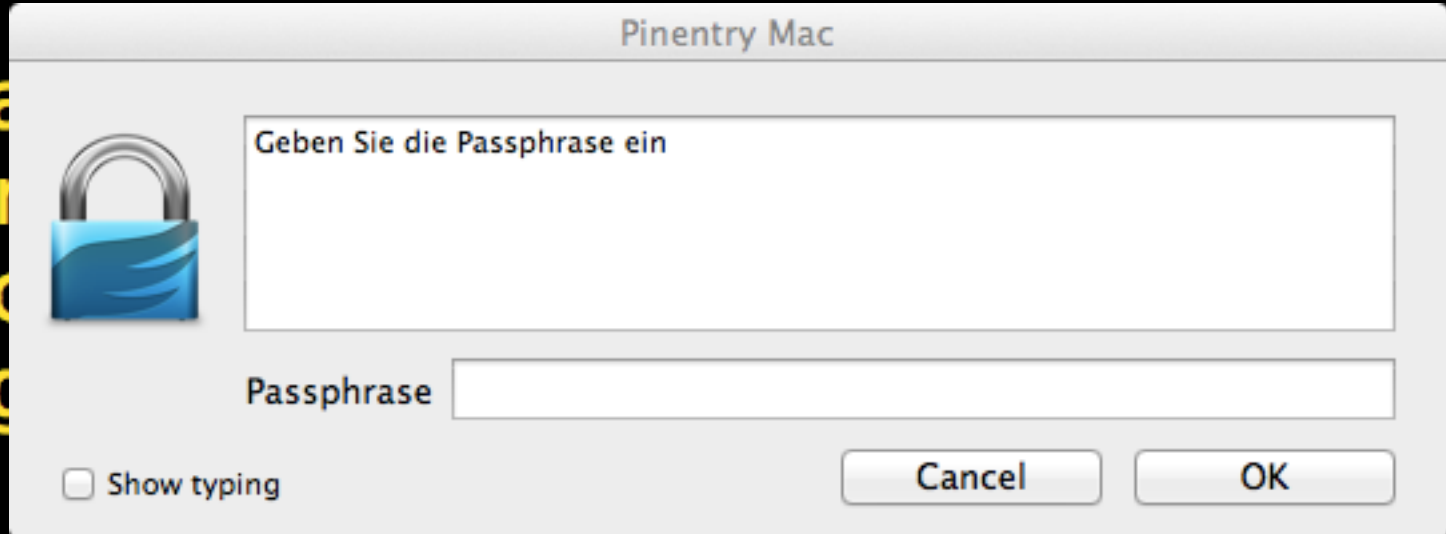
Schlüssel erzeugen

```
michaelnoppinger — gpg2 — 79x17
Wie lange bleibt der Schlüssel gültig? (0) 1y
Key verfällt am Sa 31 Jan 02:08:35 2015 CET
Ist dies richtig? (j/N) j

GnuPG erstellt eine User-ID um Ihren Schlüssel identifizierbar zu machen.

Ihr Name ("Vorname Nachname")
Email-Adresse: max@mustermann.at
Kommentar: Das ist der Schlüssel für mich
Sie haben diese User-ID gpg2:pubkey-1:
    "Max Mustermann (Das ist der Schlüssel für mich) <max@mustermann.at>"

Ändern: (N)ame, (K)ommentar, (E)-Mail oder (F)ertig/(A)bbrechen? F
Sie benötigen eine Passphrase, um den geheimen Schlüssel zu schützen.
```



gpg --gen-key

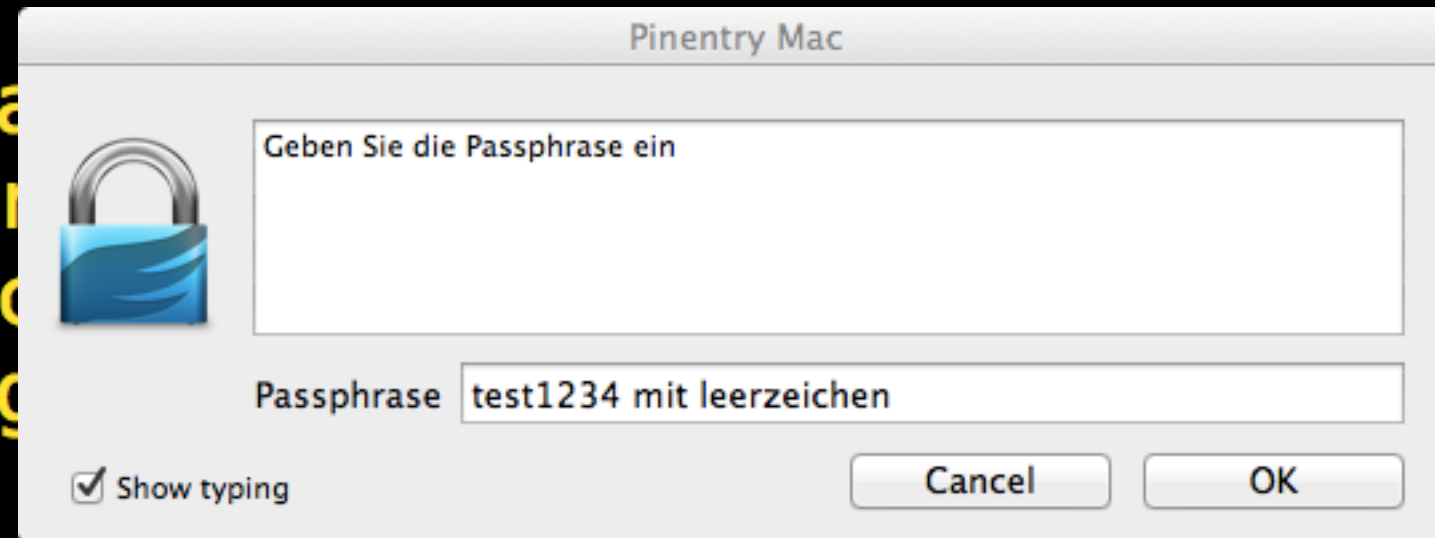
Schlüssel erzeugen

```
© ○ ○ michaelnoppinger — gpg2 — 79x17
Wie lange bleibt der Schlüssel gültig? (0) 1y
Key verfällt am Sa 31 Jan 02:08:35 2015 CET
Ist dies richtig? (j/N) j

GnuPG erstellt eine User-ID um Ihren Schlüssel identifizierbar zu machen.

Ihr Name ("Vorname Nachname")
Email-Adresse: max@mustermann.at
Kommentar: Das ist der Schlüssel für Max Mustermann.
Sie haben diese User-ID gpg2:pubkey-1:2015-01-31:1:Max Mustermann (Das ist der Schlüssel für Max Mustermann.) <max@mustermann.at>

Ändern: (N)ame, (K)ommentar, (E)-Mail oder (F)ertig/(A)bbrechen? F
Sie benötigen eine Passphrase, um den geheimen Schlüssel zu schützen.
```



gpg --gen-key

Schlüssel erzeugen

```
© ○ ○ michaelnoppinger — bash — 79x17
Wir müssen eine ganze Menge Zufallswerte erzeugen. Sie können dies
unterstützen, indem Sie z.B. in einem anderen Fenster/Konsole irgendetwas
tippen, die Maus verwenden oder irgendwelche anderen Programme benutzen.
gpg: Schlüssel 7C9B6E19 ist als uneingeschränkt vertrauenswürdig gekennzeichnet
Öffentlichen und geheimen Schlüssel erzeugt und signiert.

gpg: "Trust-DB" wird überprüft
gpg: 3 marginal-needed, 1 complete-needed, PGP Vertrauensmodell
gpg: Tiefe: 0 gültig: 4 signiert: 0 Vertrauen: 0-, 0q, 0n, 0m, 0f, 4u
gpg: nächste "Trust-DB"-Pflichtüberprüfung am 2015-01-31
pub 1024R/7C9B6E19 2014-01-31 [verfällt: 2015-01-31]
    Schl.-Fingerabdruck = 6894 B777 AA8D 9B8E 4847 2B47 6928 76FA 7C9B 6E19
uid                               Max Mustermann (Das ist der Schluessel von Max Mustermann.
) <max@mustermann.at>
sub 1024R/373BF2B2 2014-01-31 [verfällt: 2015-01-31]

SYSTEM-5:~ michaelnoppinger$ █
```

gpg --gen-key

Schlüssel erzeugen

```
SYSTEM-5:~ michaelnoppinger$ gpg --export -a
```

`gpg --export [uid]`

Schlüssel exportieren

```
SYSTEM-5:~ michaelnoppinger$ gpg --export -a Max Mustermann
```

gpg --export [uid]

Schlüssel exportieren

```
SYSTEM-5:~ michaelnoppinger$ gpg --export -a Max Mustermann
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG/MacGPG2 v2.0.20 (Darwin)
Comment: GPGTools - https://gpgtools.org

mI0EUur8AQEEA0zbzb7YDo3//LFSVPQkJQQ1ubYIssFg34eNKlFwR4IEEehppB9
2zk5tClN3lUbKoa/RfcKyV/m2LM4SylXh0sgnI929ke0o4yeYwEHjJcRaFrGdMpR
ukGwG5xLBfEUrnYcFdNC87c7s0bfeMm7SpYIHuUXTkpX02sYgJSym0MTABEBAAG0
T01heCBNdXN0ZXJtYW5uICChEYXMgaXN0IGRlciBTY2hsdWVzc2VsIHZvbiBhbnYXgg
TXVzdGVybWFubi4pIDxtYXhAbXVzdGVybWFubi5hdD6IvQQTaQoAJwUCUur8AQIb
AwUJAeEzgAULCQgHAwUVCgkICwUWAgMBAAIeAQIXgAAKCRBpKHb6fJtuGZdTbADD
aihahFtjuFwiCvD/31bITN6rq2ppXGlsd40rB+jzo+pxEj0ToQ1+4d+n70SfnYiF
CCSF7R+SLyJsMLLRsDk0ECC4t79I0QN7y0AV0RAfCG/TlvoVU2HT+HKPFgNXfr1I
YYEiCR/rLUUV9T64ESwgr1+pXiUb6/GEGtxlN3SaEriNBFLq/AEBBACpjU06Mpm8
XF0N9/6XZLm2gosmzUKub8lhKc1DlDXHVp1QWzGctrxLAv3HVdsevA1LRiD6mkeh
ev8dvP+4xA5b7+/Xq+8vLHpC28807TSzqo51xNCAYxhQGCDqxCR4Z3Eml80F2wHF
p86MBgY7ERV0MfIP9nzV5YY/xksX0Lv4yQARAQABiKUEGAEKAA8FA1Lq/AECGwwF
```

gpg --export [uid]

Schlüssel exportieren

```
michaelnoppinger — bash — 79x17
ukGwG5xLBfEUrnYcFdNC87c7s0bfeMm7SpYIHuUXTkpX02sYgJSym0MTABEBAAG0
T01heCBNdXN0ZXJtYW5uIChEYXMgaXN0IGRlciBTY2hsdWVzc2VsIHZvbiBvbnVz
TXVzdGVyYW50bWVudD50bWVudD50bWVudD50bWVudD50bWVudD50bWVudD50bWVudD
AwUJAeEzgAULCQgHAwUVCgkICwUWAgMBAAIeAQIXgAAKCRBpKHb6fJtuGZdTbADD
aihahFtjuFwiCvD/31bITN6rq2ppXG1Sd40rB+jzo+pxEj0ToQ1+4d+n70SfnYiF
CCSF7R+SLyJsMLLRsDk0ECC4t79I0QN7y0AV0RAfCG/TlvoVU2HT+HKPFgNXfr1I
YYEiCR/r1UUV9T64ESwgr1+pXiUb6/GEGtx1N3SaEriNBFLq/AEBBACpjU06Mpm8
XF0N9/6XZLm2gosmzUKub8lhKc1D1DXHvp1QWzGctrx1Av3HVdsevA1LRiD6mkeh
ev8dvP+4xA5b7+/Xq+8vLHpC28807TSzqo51xNCAYxhQGCDqxCR4Z3Em180F2wHF
p86MBgY7ERV0MfIP9nzV5YY/xksX0Lv4yQARAQABiKUEGAEKAA8FA1Lq/AECGwwF
CQHhM4AACgkQaSh2+nybbhmfDAP9H73AYGaCbdyHEujWS6ZieH8fWMjsapd1nD8b
+i2kUlpJ1xjfhGuKdJ/o58zYkZ/INu+R2X94HJXgD18dC52XKA70kf5GYrCY1X49
gC8hZtKAytjNjJBLHufL2S4Y1UGo988P7QL793HwI1BumQjo3mgCT0F3RUKQwUhb
HiQQKFQ=
=D/gJ
-----END PGP PUBLIC KEY BLOCK-----
SYSTEM-5:~ michaelnoppinger$
```

gpg -export [uid]

Schlüssel exportieren


```
SYSTEM-5:~ michaelnoppinger$ gpg --export -a Max Mustermann > key.gpg
SYSTEM-5:~ michaelnoppinger$ █
```

gpg --export [uid]

Schlüssel exportieren

```
SYSTEM-5:~ michaelnoppinger$ gpg --import key.gpg
```

`gpg --import [Datei]`

Schlüssel importieren

```
pgp -- mino@pictor:~/pgp -- bash -- 77x16
SYSTEM-5:pgp michaelnoppinger$ gpg -e geheim
```

gpg -e [Datei] Empfänger

Verschlüsseln

```
SYSTEM-5:pgp michaelnoppinger$ gpg -e geheim
Sie haben keine User-ID angegeben (Sie können die Option "-r" verwenden).

Derzeitige Empfänger:

Geben Sie die User-ID ein. Beenden mit einer leeren Zeile: █
```

`gpg -e [Datei] Empfänger`
Verschlüsseln

```
SYSTEM-5:pgp michaelnoppinger$ gpg -e geheim
Sie haben keine User-ID angegeben (Sie können die Option "-r" verwenden).

Derzeitige Empfänger:

Geben Sie die User-ID ein. Beenden mit einer leeren Zeile: Max Mustermann
```

`gpg -e [Datei] Empfänger`
Verschlüsseln

```
SYSTEM-5:pgp michaelnoppinger$ gpg -e geheim
Sie haben keine User-ID angegeben (Sie können die Option "-r" verwenden).

Derzeitige Empfänger:

Geben Sie die User-ID ein. Beenden mit einer leeren Zeile: Max Mustermann

Derzeitige Empfänger:
1024R/373BF2B2 2014-01-31 "Max Mustermann (Das ist der Schluessel von Max Mustermann.) <max@mustermann.at>"

Geben Sie die User-ID ein. Beenden mit einer leeren Zeile: █
```

`gpg -e [Datei] Empfänger`
Verschlüsseln

```
SYSTEM-5:pgp michaelnoppinger$ gpg -e geheim
Sie haben keine User-ID angegeben (Sie können die Option "-r" verwenden).

Derzeitige Empfänger:

Geben Sie die User-ID ein. Beenden mit einer leeren Zeile: Max Mustermann

Derzeitige Empfänger:
1024R/373BF2B2 2014-01-31 "Max Mustermann (Das ist der Schluessel von Max Mustermann.) <max@mustermann.at>"

Geben Sie die User-ID ein. Beenden mit einer leeren Zeile:
SYSTEM-5:pgp michaelnoppinger$ █
```

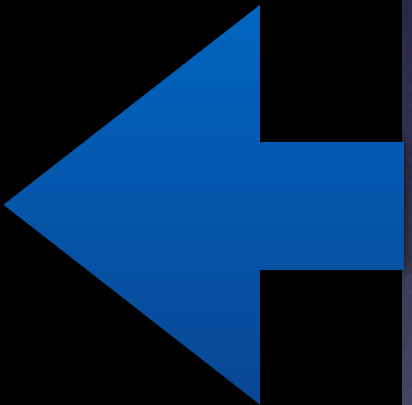
`gpg -e [Datei] Empfänger`
Verschlüsseln

```
pgp -- mino@pictor:~/pgp -- bash -- 77x16

Geben Sie die User-ID ein. Beenden mit einer leeren Zeile: Max Mustermann

Derzeitige Empfänger:
1024R/373BF2B2 2014-01-31 "Max Mustermann (Das ist der Schluessel von Max Mus
termann.) <max@mustermann.at>"

Geben Sie die User-ID ein. Beenden mit einer leeren Zeile:
SYSTEM-5:pgp michaelnoppinger$ ls -la
total 32
drwxr-xr-x    5 michaelnoppinger  staff   170 31 Jan 03:47 .
drwxr-xr-x+ 125 michaelnoppinger  staff  4250 31 Jan 02:45 ..
-rw-r--r--@   1 michaelnoppinger  staff  6148 31 Jan 01:06 .DS_Store
-rw-r--r--    1 michaelnoppinger  staff    28 31 Jan 03:35 geheim
-rw-r--r--    1 michaelnoppinger  staff   233 31 Jan 03:47 geheim.gpg
SYSTEM-5:pgp michaelnoppinger$ █
```



gpg -e Empfänger [Datei]

Verschlüsseln


```
pgp -- mino@pictor:~/pgp -- bash -- 77x16
SYSTEM-5:pgp michaelnoppinger$ gpg --clearsign geheim.gpg
```

`gpg --clearsign [Datei]`

Dateien unterschreiben

```
SYSTEM-5:pgp michaelnoppinger$ gpg --clearsign geheim.gpg

Sie benötigen eine Passphrase, um den geheimen Schlüssel zu entsperren.
Benutzer: "Max Mustermann (Das ist der Schluessel von Max Mustermann.) <max@m
ustermann.at>"
1024-Bit RSA Schlüssel, ID 7C9B6E19, erzeugt 2014-01-31

SYSTEM-5:pgp michaelnoppinger$ █
```

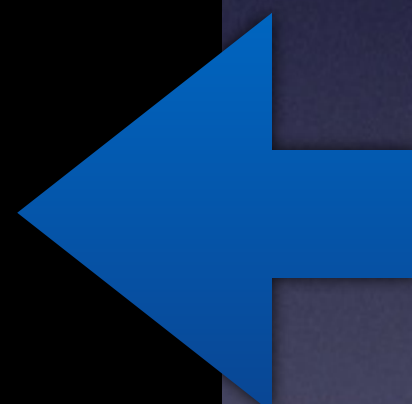
`gpg --clearsign [Datei]`

Dateien unterschreiben

```
SYSTEM-5:pgp michaelnoppinger$ gpg --clearsign geheim.gpg

Sie benötigen eine Passphrase, um den geheimen Schlüssel zu entsperren.
Benutzer: "Max Mustermann (Das ist der Schluessel von Max Mustermann.) <max@m
ustermann.at>"
1024-Bit RSA Schlüssel, ID 7C9B6E19, erzeugt 2014-01-31

SYSTEM-5:pgp michaelnoppinger$ ls -la
total 40
drwxr-xr-x    6 michaelnoppinger  staff    204 31 Jan 03:52 .
drwxr-xr-x+ 125 michaelnoppinger  staff   4250 31 Jan 02:45 ..
-rw-r--r--@   1 michaelnoppinger  staff   6148 31 Jan 01:06 .DS_Store
-rw-r--r--    1 michaelnoppinger  staff    28 31 Jan 03:35 geheim
-rw-r--r--    1 michaelnoppinger  staff   233 31 Jan 03:47 geheim.gpg
-rw-r--r--    1 michaelnoppinger  staff    644 31 Jan 03:52 geheim.gpg.asc
SYSTEM-5:pgp michaelnoppinger$ █
```



gpg --clearsign [Datei]

Dateien unterschreiben

```
pgp -- mino@pictor:~/pgp -- bash -- 77x16
SYSTEM-5:pgp michaelnoppinger$ gpg --verify geheim.gpg.asc
```

gpg [--verify] [Datei]

Unterschrift verifizieren

```
SYSTEM-5:pgp michaelnoppinger$ gpg --verify geheim.gpg.asc
gpg: Signature made Fr 31 Jan 03:52:57 2014 CET using RSA key ID 7C9B6E19
gpg: Good signature from "Max Mustermann (Das ist der Schluessel von Max Mustermann.) <max@mustermann.at>"
SYSTEM-5:pgp michaelnoppinger$ █
```

gpg [--verify] [Datei]

Unterschrift verifizieren

```
SYSTEM-5:pgp michaelnoppinger$ gpg -u "Michael Noppinger" -r "Max Mustermann"  
--armor --sign --encrypt geheim
```

```
gpg [-u Sender] [-r Empfänger] [--  
armor] --sign --encrypt [Datei]
```

Signieren und Verschlüsseln

```
SYSTEM-5:pgp michaelnoppinger$ gpg -u "Michael Noppinger" -r "Max Mustermann"
--armor --sign --encrypt geheim

Sie benötigen eine Passphrase, um den geheimen Schlüssel zu entsperren.
Benutzer: "Michael Noppinger <michael@noppinger.com>"
2048-Bit RSA Schlüssel, ID FB6276E6, erzeugt 2013-08-15 (Hauptschlüssel-ID A3
D5C68D)

SYSTEM-5:pgp michaelnoppinger$ █
```

gpg [-u Sender] [-r Empfänger] [--armor] --sign --encrypt [Datei]

Signieren und Verschlüsseln

```
pgp -- mino@pictor:~/pgp -- bash -- 77x16
SYSTEM-5:pgp michaelnoppinger$ gpg -u "Michael Noppinger" -r "Max Mustermann"
--armor --sign --encrypt geheim

Sie benötigen eine Passphrase, um den geheimen Schlüssel zu entsperren.
Benutzer: "Michael Noppinger <michael@noppinger.com>"
2048-Bit RSA Schlüssel, ID FB6276E6, erzeugt 2013-08-15 (Hauptschlüssel-ID A3
D5C68D)

SYSTEM-5:pgp michaelnoppinger$ ls -la
total 32
drwxr-xr-x    5 michaelnoppinger  staff   170 31 Jan 04:08 .
drwxr-xr-x+ 125 michaelnoppinger  staff  4250 31 Jan 02:45 ..
-rw-r--r--@   1 michaelnoppinger  staff  6148 31 Jan 01:06 .DS_Store
-rw-r--r--    1 michaelnoppinger  staff    28 31 Jan 03:35 geheim
-rw-r--r--    1 michaelnoppinger  staff   878 31 Jan 04:08 geheim.asc
SYSTEM-5:pgp michaelnoppinger$ █
```

gpg [-u Sender] [-r Empfänger] [--armor] --sign --encrypt [Datei]

Signieren und Verschlüsseln


```
SYSTEM-5:pgp michaelnoppinger$ more geheim
Das ist eine geheime Datei.
SYSTEM-5:pgp michaelnoppinger$ █
```

Inhalt von „geheim“

```
SYSTEM-5:pgp michaelnoppinger$ more geheim.asc
-----BEGIN PGP MESSAGE-----
Version: GnuPG/MacGPG2 v2.0.22 (Darwin)
Comment: GPGTools - https://gpgtools.org

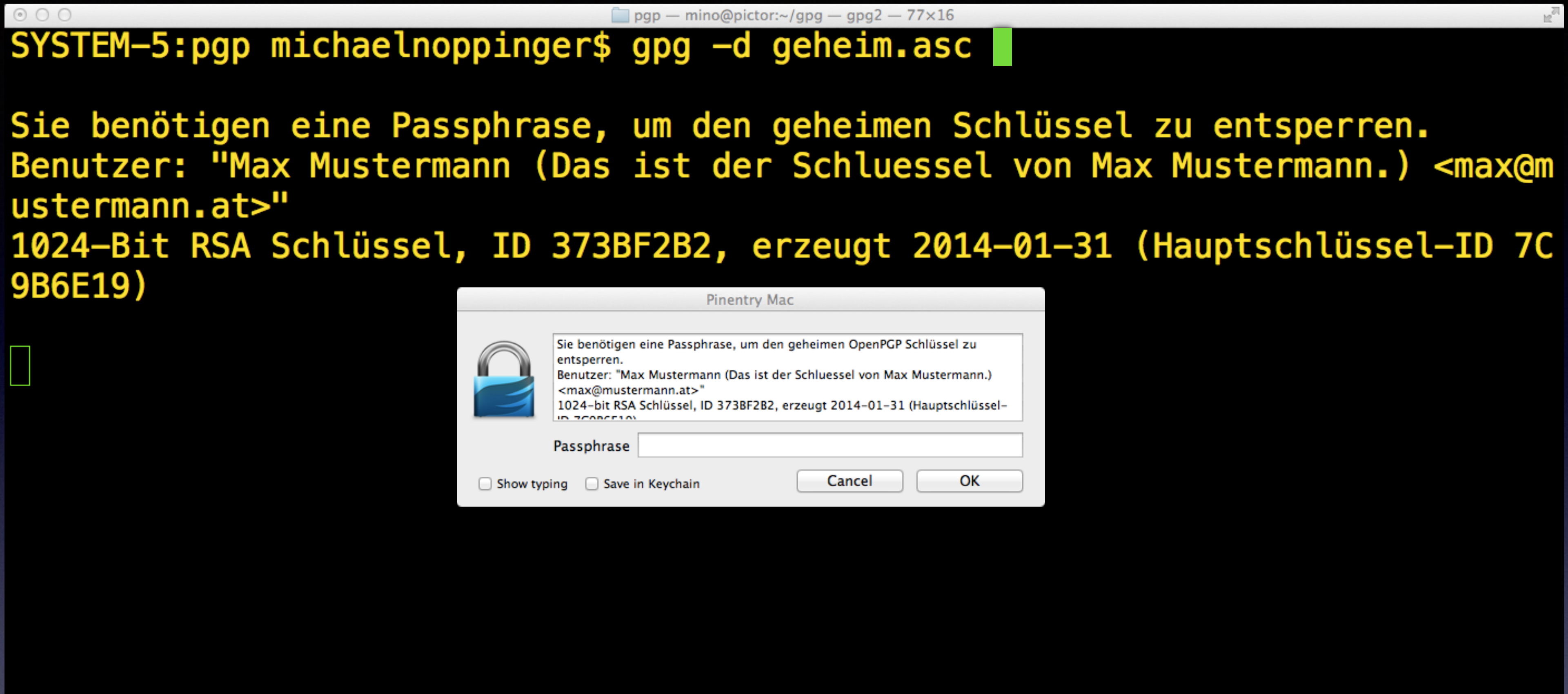
hIwDFNtR8zc78rIBA/9wcdcGLmTQvAQcFjo/vQnklq5tq0AJNutR1u1eCEUpj fWn
EY6ZXfBZna0nhkKsHB5A2eZfUMr7jxQfYHg67ELiCdY24gC9kqp8aMWfb2mJFJEi
tb2qyf2aVUH5aJ+ZNxxWu4bT34an7tqdTe5zic/bTYLSjvdAe0Z1nmNYv77aM9LA
zgFyg03Mgd7m6S8K1UYs6+ZK2m3i9gqNky9o0aQZ0t6g1RIqvXNSV4wTV7yzwBoK
S75i1Iv1ik0rNK8i6oeQUYH65o0wf8AeHf8NfdfJc2mNwJAYEHi98l1z88TW9Z6w
TcSoXj9wUh2C9qC4Ewwg9RPnPqVU/1ajC5aILSxrRALghFip2dFCN1J5Eu+Kc9XZ
DJk8ls2a6nXuHRFJ/SS4EaERPfFUHssYPqIQiDBCPLSI tT1cSk4SUvtdm+6MSrEG
7AjbGBFqv v/tExbjYwFBIWmdfcil2eXoHFM0qi/1vbiqqR0rphLVMMMBt0B50uqN
Sz20GJ5EdDCVDG0wYqN8FhHtR+8LUnCt30K2o+yzrQg9FLCt7MCP3o+eZPuqi//U
3PBAPFx1UQfjf+ze20BJL04XD6LqfbSJN0yS94xokvI5RSowRNm26ef6pmgh11WQ
tUARqhAs3iq+0V7zLX5V0oM9STFb loJBudQceXxGF5eUDp66BVMz8jAbmJKoS0UW
```

Inhalt von verschlüsseltem und signiertem „geheim“

```
SYSTEM-5:pgp michaelnoppinger$ gpg -d geheim.asc
```

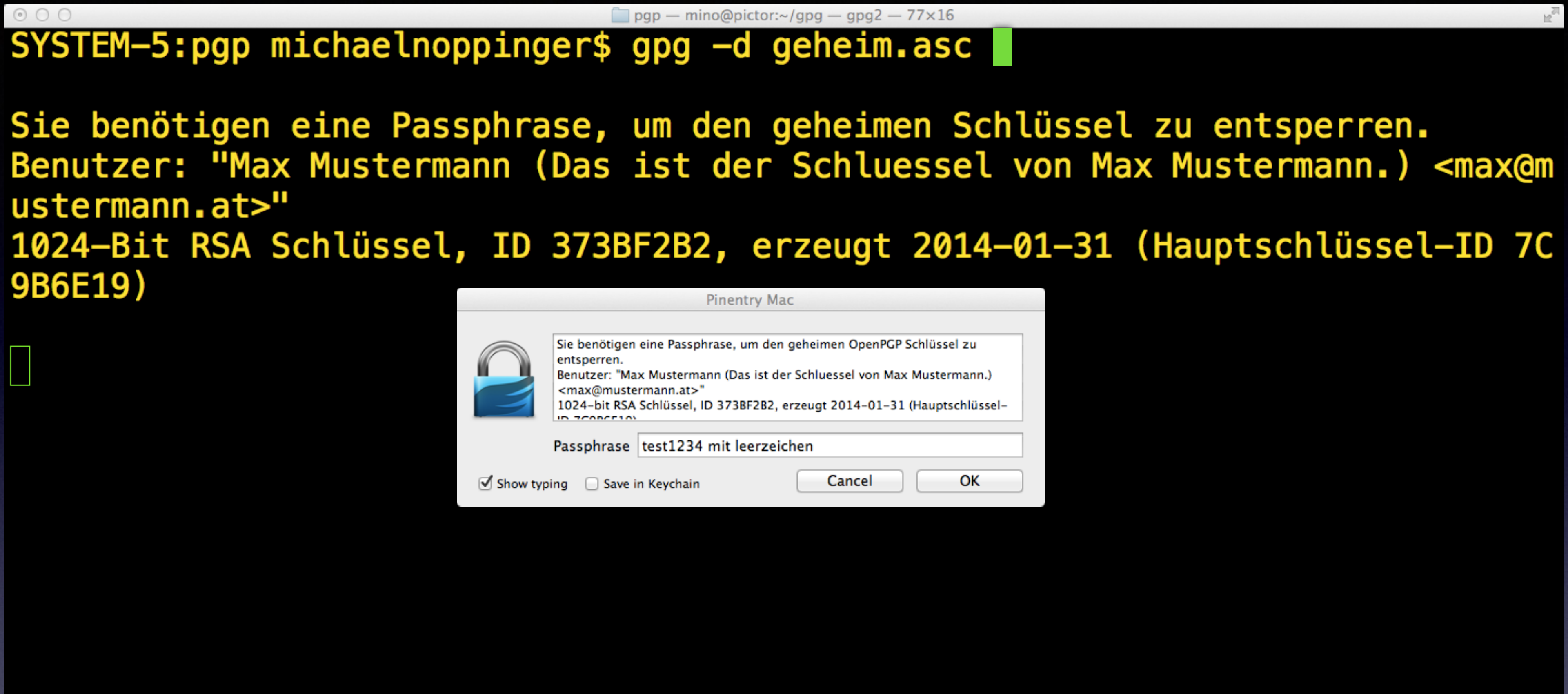
gpg [-d] [Datei]

Entschlüsseln und Signatur überprüfen



gpg [-d] [Datei]

Entschlüsseln und Signatur überprüfen



gpg [-d] [Datei]

Entschlüsseln und Signatur überprüfen

```
gpg -- mino@pictor:~/gpg -- bash -- 77x16

Sie benötigen eine Passphrase, um den geheimen Schlüssel zu entsperren.
Benutzer: "Max Mustermann (Das ist der Schluessel von Max Mustermann.) <max@m
ustermann.at>"
1024-Bit RSA Schlüssel, ID 373BF2B2, erzeugt 2014-01-31 (Hauptschlüssel-ID 7C
9B6E19)

gpg: verschlüsselt mit 1024-Bit RSA Schlüssel, ID 373BF2B2, erzeugt 2014-01-3
1
    "Max Mustermann (Das ist der Schluessel von Max Mustermann.) <max@muste
rmann.at>"
Das ist eine geheime Datei.
gpg: Signatur vom Fr 31 Jan 04:08:26 2014 CET mittels RSA-Schlüssel ID FB6276
E6
gpg: Korrekte Signatur von "Michael Noppinger <michael@noppinger.com>"
SYSTEM-5:gpg michaelnoppinger$ █
```

gpg [-d] [Datei]

Entschlüsseln und Signatur überprüfen

Wir wünschen viel Vergnügen
beim Ausprobieren von GnuPG!

- B. Schneier, “Applied Cryptography, Second Edition”, Wiley, 1996
Deutsche Ausgabe unter dem Titel “Angewandte Kryptographie”,
Addison-Wesley, 1996
- <http://en.wikipedia.org/wiki/Gnupg>