Nach der Keysigningparty

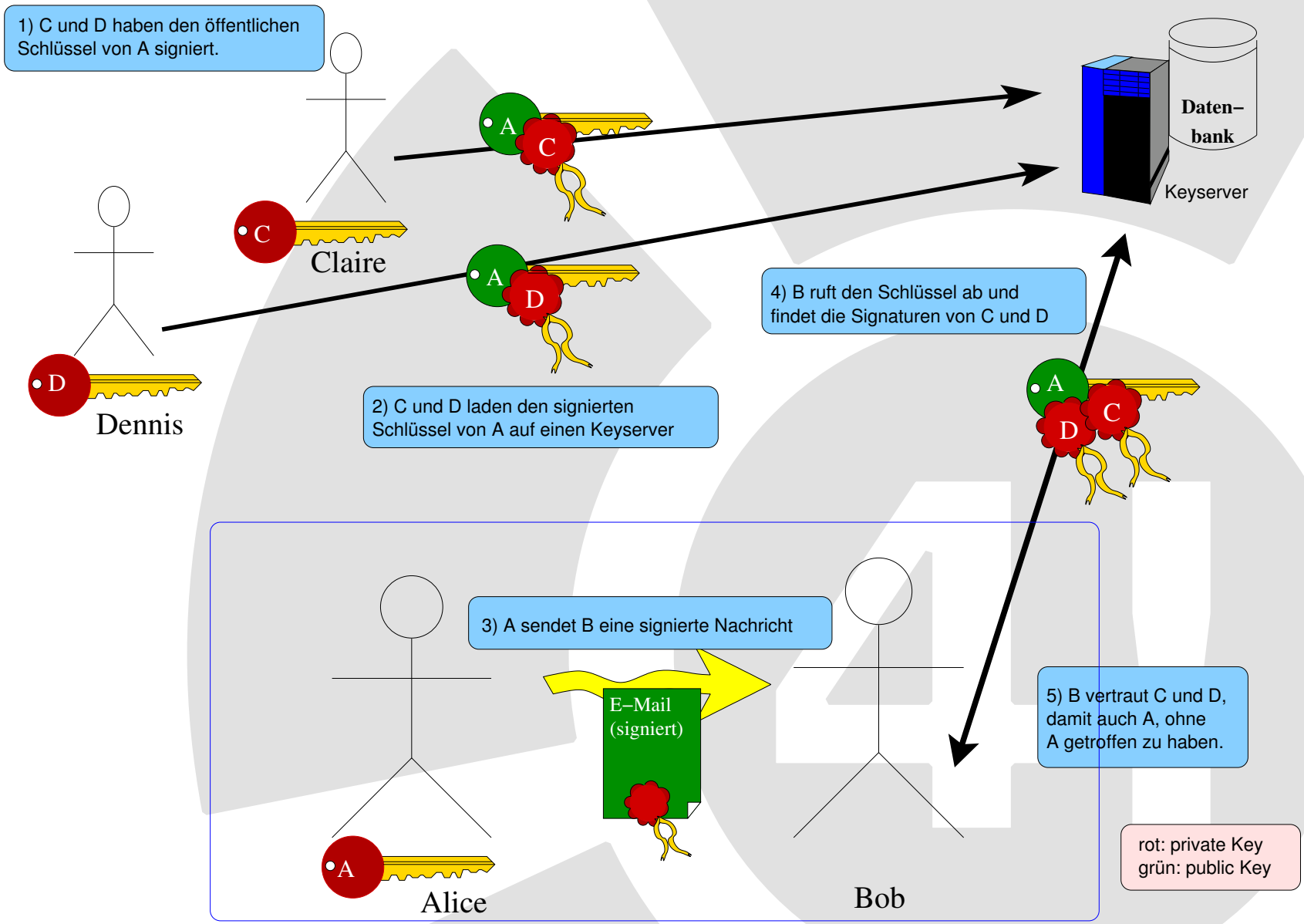
Keysigning mit caff

Theresa Enghardt

<theresa@freitagsrunde.org>

12. Juli 2012

Wiederholung: Schema Web of Trust



Keysigning - Theorie

- Beim Keysigning überprüft man:
  - die Korrektheit des Schlüssels (anhand des Fingerprints)
  - die Identität (anhand des Ausweises)
  - **NICHT:** Die Korrektheit der einzelnen User IDs (UIDs)

  $\Rightarrow$ Falsch angegebene E-mail-Adresse wird nicht erkannt
- Danach signiert man den Schlüssel des anderen lokal auf dem eigenen Rechner
- Idealerweise signiert man jede BenutzerID (UID) auf dem Schlüssel einzeln
- Nun schickt man den signierten Schlüssel verschlüsselt an die angegebenen Emailadresse(n)
- Damit sind nun auch die Emailadressen verifiziert!
- das Web of Trust lebt, wie der Name sagt, vom Vertrauen:

$\Rightarrow$ bitte niemals blind signieren!

Keysigning - Praxis

- Liste von mehr als 20 Schlüsseln, jeweils mehrere UIDs (zB E-mail-Adressen)
- Ideal: An jede E-mail-Adresse, die als UID in einem Schlüssel steht, eine Mail schreiben
  - Mail enthält die Unterschrift für nur diese UID
  - Mail ist verschlüsselt mit diesem öffentlichen Schlüssel
  - nur, wenn Mailadresse existiert und Person, die sie abruft, den privaten Schlüssel zum Entschlüsseln hat, kann die Unterschrift danach auf einen Keyserver hochgeladen werden
- **Problem:** 20 Schlüssel * 3 E-mail-Adressen/Schlüssel = eine Menge Arbeit
- Lösung: `caff`

Caff

- **caff - CA F**ire and **F**orget
- Skript, das das Unterschreiben von Schlüsseln erleichtert
- Auf der Kommandozeile aufrufen, z.B. `caff 0x82F61240`
  1. Importiert Schlüssel aus lokal gespeicherten oder lädt ihn von einem Keyserver
  2. Fragt: Sollen alle UIDs unterschrieben werden? ("Nein": einzelne Auswählen möglich)
  3. Fragt: Soll der Schlüssel wirklich unterschrieben werden? (Danach: Passphrase eingeben)
  4. Ruft gpg auf, um zu unterschreiben
  5. Liefert dann eine gpg-Kommandozeile
  6. `save` - Fragt für jede Mailadresse nach, ob die Unterschrift dorthin geschickt werden soll
  7. Schickt an jede Mailadresse den unterschriebenen Schlüssel der passenden UID

Caff: Installieren

- caff selbst
  - Ist ein Perlskript, das in einigen Paketen enthalten ist
  - **Achtung:** Ich gehe im Folgenden von Linux aus. Jemand Erfahrungen mit anderen Betriebssystemen? Input erwünscht!
  - Debian/Ubuntu: `apt-get install signing-party`
  - Gentoo: `emerge -av signing-party`
  - Fedora: `yum install pgp-tools`
  - Andere Distributionen: Selbst runterladen - `http://anonscm.debian.org/viewvc/pgp-tools/trunk/`
- Zusätzlich benötigt: lokaler Mail Transfer Agent (MTA) zum Senden von E-mails
- Zum Beispiel **S**imple**SMTP** = `ssmtp`
- Oder **D**ragon **M**ail **A**gent = `dma`

Caff: Konfigurieren

- Im Home-Verzeichnis Datei .caffrc erstellen oder bereits existierende .caffrc editieren

```
$CONFIG{'owner'} = 'Theresa Enghardt';
$CONFIG{'email'} = 'theri@mailbox.tu-berlin.de';
$CONFIG{'bcc'} = 'theri@mailbox.tu-berlin.de';

$CONFIG{'keyid'} = [ qw{833D34EF1C76A0F7} ];

$CONFIG{'keyserver'} = 'subkeys.pgp.net';

# Additionally encrypt messages for these keyids
$CONFIG{'also-encrypt-to'} = [ qw{833D34EF1C76A0F7} ];
```

- Eigener Name, E-mail, (lange) KeyID
- Bcc: Sendet unterschriebenen Schlüssel auch an mich
- Muss dann auch an mich verschlüsselt werden, sonst nicht lesbar
- Keyserver, von dem zu unterschreibende Keys geholt werden
- Außerdem kann der Standard-Mailtext geändert werden... Der wird sonst schnell langweilig.

Mailagent: Installieren

- Simple SMTP: SSMTP
  - Debian/Ubuntu: `apt-get install ssmtp`
  - Gentoo: `emerge -av mail-mta/ssmtp`
- Dragon Mail Agent: DMA
  - Debian/Ubuntu: `apt-get install dma`
- Ansonsten: Das Internet weiß mehr...

SSMTP konfigurieren: mailaliases

In `/etc/ssmtp/revaliases`:

```
root:theri@mailbox.tu-berlin.de:mail.tu-berlin.de:465
theresa:theri@mailbox.tu-berlin.de:mail.tu-berlin.de:465
```

- Zuerst Username auf dem aktuellen System: `theresa`, bzw `root`
- Dann Mailadresse: `theri@mailbox.tu-berlin.de`
- Dann Mailhost: `mail.tu-berlin.de` - meistens `mail.`<Provider-Domain>
- Mailhost ist das, wo dein Mailclient auch seine Mails hinschickt (meist unter SMTP Settings zu finden).
- Dann Port (hier: SMTP über SSL): 465 - default ist 25 (unverschlüsselt!)

SSMTP konfigurieren: ssmtp.conf

Beispielconfig `/etc/ssmtp/ssmtp.conf` (Teil 1):

```
# Config file for sSMTP sendmail
#
# The person who gets all mail for userids < 1000
# Make this empty to disable rewriting.
root=theri@mailbox.tu-berlin.de

# The place where the mail goes. The actual machine name is required no
# MX records are consulted. Commonly mailhosts are named mail.domain.com
mailhub=mail.tu-berlin.de:465

AuthUser=theri
AuthPass=__ZENSIERT__
```

- Zuerst `root` - eigene Mailadresse erhält alles
- Dann Mailhub (= Mailhost) - wie in der anderen Configdatei
- Dann Username - Manchmal muss die Domain dazu, hier reicht der Name
- Dann Passwort - Ja, das wird im Klartext gespeichert.

Weiter geht's auf der nächsten Seite...

SSMTP konfigurieren: ssmtp.conf

Beispielconfig `/etc/ssmtp/ssmtp.conf` (Teil 2):

```
# Where will the mail seem to come from?
rewriteDomain=mailbox.tu-berlin.de

# The full hostname
hostname=mailbox.tu-berlin.de

# Are users allowed to set their own From: address?
# YES - Allow the user to specify their own From: address
# NO - Use the system generated From: address
FromLineOverride=YES

UseTLS=YES
```

- rewriteDomain und hostname - sonst steht da, die Mail kommt von anghammarad (Name meines Rechners).flauschig.org ...
- FromLineOverride - Mailprogramme können anderen Absender angeben
- UseTLS - Verschlüsselte Verbindung aufbauen. Ihr wollt das.

Mailsetup testen

- Mailsetup kann etwas komplex/tricky sein
- Deswegen: Nicht sofort caff anschmeißen, erst testen.
- Wie? Mails von der Kommandozeile schicken!

```
theresa@anghammarad:~$ mail -s "SMTP-Test" theresa@freitagsrunde.org
Ohai, ich teste grade mein sSMTP-Setup. Wer das liest, ist doof.

.
Cc:
```

- `mail` sollte schon installiert sein
- -s steht für Subject (Betreff) der Mail
- weiteres Argument ist der Empfänger
- Danach: Text der Mail eintippen, Beenden durch Leerzeile, Punkt und Enter (oder Strg+D)
- Optional: Cc (Kopie) an eine bestimmte E-mail-Adresse

Mailsetup testen

- Probleme beim Senden?
  1. Füge in /etc/ssmtp/ssmtp.conf die Zeile `Debug=YES` hinzu
  2. Probiere noch einmal zu senden
  3. Lies dann den Log (z.B. `tail /var/log/mail.log -n 30`). Oft steht dort eine Fehlermeldung, die einen Hinweis auf das Problem gibt.
- Mail angekommen?
  - $\Rightarrow$ Mailheader okay? (zB in Thunderbird: Strg+U drücken)
  - Hinter "From: "(Absender) sollte das Richtige stehen
  - Das "Date: "(Datum) sollte in etwa stimmen
  - Sonst könnte die Mail im Spamordner landen
  - Manche Mailserver fügen Header hinzu, in denen Spamkriterien stehen

Und nun endlich: caff

```
theresa@anghammarad:~$ caff 0x82F61240

[INFO] Importing key 833D34EF1C76A0F7 from your normal GnuPGHome.
[INFO] fetching keys, this will take a while...
[INFO] Sign the following keys according to your policy, then exit gpg with 'save'
 after signing each key
gpg --homedir=/home/theresa/.caff/gnupghome --secret-keyring /home/theresa/.gnupg/
secring.gpg --no-auto-check-trustdb --trust-model=always --edit 5BE7F0088B83935711
08984A3B8EA41F82F61240 sign save
gpg (GnuPG) 1.4.12; Copyright (C) 2012 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.

pub  1024D/82F61240  erzeugt: 2004-10-22  verfällt: 2012-08-17  Aufruf: SC
[...]
[  unbek.] (9)  Florian Streibelt [...] <Florian.Streibelt@TU-Berlin.DE>
[  unbek.] (10)  Florian Streibelt [...] <florian@freitagsrunde.org>

Wirklich alle User-IDs beglaubigen? (j/N) j
```

- Importiere zuerst eigenen Schlüssel
- Hole dann fremde Schlüssel vom Keyserver
- Skript ruft gpg mit einigen Optionen, die es auch ausgibt
- Einzelne IDs beglaubigen: mit 'Nein' antworten, dann Nummern eingeben

caff in Aktion

```
pub   1024D/82F61240 2004-10-22 [verfällt: 2012-08-17]
  Schl.-Fingerabdruck = 5BE7 F008 8B83 9357 1108  984A 3B8E A41F 82F6 1240
[...]
[  unbek.] (9)  Florian Streibelt [...] <Florian.Streibelt@TU-Berlin.DE>
[  unbek.] (10)  Florian Streibelt [...] <florian@freitagsrunde.org>

Sind Sie wirklich sicher, daß Sie vorstehenden Schlüssel mit Ihrem
Schlüssel "Theresa Enghardt <theresa@someserver.de>" (1C76A0F7) beglaubigen wollen

Wirklich unterschreiben? (j/N) j

Sie benötigen eine Passphrase, um den geheimen Schlüssel zu entsperren.
Benutzer: "Theresa Enghardt <theresa@someserver.de>"
2048-Bit RSA Schlüssel, ID 1C76A0F7, erzeugt 2011-04-12
```

- Zeige nochmals alle UIDs und den Fingerprint des Schlüssels
- Abfrage, ob unterschrieben werden soll - Default ist "Nein", um versehentliches Unterschreiben zu verhindern
- Passphrase eingeben (entfällt ggf. ab dem 2. Mal, wenn gpg-agent benutzt wird)

caff in Aktion

```
gpg> save
[...]
[INFO] 3B8EA41F82F61240 (9) Florian Streibelt <Florian.Streibelt@TU-Berlin.DE> done.
[INFO] 3B8EA41F82F61240 (10) Florian Streibelt <florian@freitagsrunde.org> done.
[INFO] key 5BE7F0088B8393571108984A3B8EA41F82F61240 done.
Mail signature for Florian Streibelt (general purpose key) <Florian.Streibelt@
TU-Berlin.DE> to 'Florian.Streibelt@TU-Berlin.DE'? [Y/n] Y
Mail signature for Florian Streibelt (Freitagsrunde der TU-Berlin) <florian@
freitagsrunde.org> to 'florian@freitagsrunde.org'? [Y/n] Y
```

- GPG-Kommando zeile gpg> erscheint
- Eingabe von save speichert den unterschriebenen Schlüssel
- Wenn alle Schlüssel unterschrieben wurden: Abfrage, ob Mails verschickt werden sollen, für jede einzelne UID
- $\Rightarrow$ Jabber-IDs, Foto-IDs und weitere Nicht-E-mail-Adressen direkt ausnehmen (und ggf. später über anderen Weg verschicken)
- Default ist "Ja", Enter Spammen also möglich

Aufnahme des GPG-Vortrags:

http://wiki.freitagsrunde.org/TechTalks/2012-07_GnuPG-Verschluesselung

Folien:

http://docs.freitagsrunde.org/Veranstaltungen/keysigning/2012/

caff:

http://frank.uvena.de/de/Keysigning/Caff/index.php

GG, Art.10, Abs1:
Das Briefgeheimnis
sowie das Post- und
Fernmeldegeheimnis
sind unverletztlich...