

Tuesday, December 23. 2014

OpenPGP Key Transition Statement for Hanno 'Rince' Wagner

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1,SHA512

OpenPGP Key Transition Statement for Hanno 'Rince' Wagner

I have created a new OpenPGP key and will be transitioning away from my old key. The old key has not been compromised and will continue to be valid for some time, but I prefer all future correspondence to be encrypted to the new key, and will be making signatures with the new key going forward.

I would like this new key to be re-integrated into the web of trust. This message is signed by both keys to certify the transition. My new and old keys are signed by each other. If you have signed my old key, I would appreciate signatures on my new key as well, provided that your signing policy permits that without re-authenticating me.

The old key, which I am transitioning away from, is:

```
pub 1024D/9B7E8785 2012-02-13 [expires: 2017-02-11]
  Key fingerprint = 9B29 43C1 E851 EB1F 5EE1 399E 002E CB48 9B7E 8785
```

The new key, to which I am transitioning, is:

```
pub 3744R/4CF2D85A 2014-12-19 [expires: 2024-12-16]
  Key fingerprint = A757 23A1 76CD E346 0449 956A 7C31 92F1 4CF2 D85A
```

The entire key may be downloaded from: <https://blog.rince.de/4cf2d85a.txt>

To fetch the full new key from a public key server using GnuPG, run:

```
gpg --keyserver keys.gnupg.net --recv-key 4cf2d85a
```

If you already know my old key, you can now verify that the new key is signed by the old one:

```
gpg --check-sigs 4cf2d85a
```

If you are satisfied that you've got the right key, and the User IDs match what you expect, I would appreciate it if you would sign my key:

```
gpg --sign-key 4cf2d85a
```

You can upload your signatures to a public keyserver directly:

```
gpg --keyserver keys.gnupg.net --send-key 4cf2d85a
```

Or email wagner@rince.de (possibly encrypted) the output from:

```
gpg --armor --export 4cf2d85a
```

If you'd like any further verification or have any questions about the transition please contact me directly.

To verify the integrity of this statement:

```
wget -q -O- http://blog.rince.de/download/key-transition-2014-12-23.txt|gpg --verify
```

Hanno

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.12 (GNU/Linux)

```
iEYEARECAAYFAISZs9UACgkQAC7LSJt+h4UyLgCePN5kQs8/YD+M7sbBUhcmk8m2
y0IAAn0J3xLuTjM11H/Ahj8NnoKEKJyC7iQHwBAEBCgAGBQJUmbPVAAoJEHwxkvFM
8thalm8OnjPO0as/SbbEN19On/mhXtyqDGsIWR3G4QU2nOz3PCZ0ko9+2Ukwxd4y
p/vBxSVAHj2mw2nYbNO4Z26Wzd0xs/wG7sy1AXgzxj7mlRapzNuyuiVngVK8PwnJ
Uzbucu2IK/um1qpaOe40xDCsThN6K+KBRF7QBm84VCjvzpTwO23Kmlh3wde94u1f
O0wZwm+n5jO5XXunVx/fSBjMyKylPt5mTLakf9yEqpH/5quL2occG3eQfN3mvEOA
0h3M/XDOjJCY/B4mHkwBpEmpmbZhQ6eewTONzj6u+Qwb4tUmlwyZZQnrSLKFu33S
VskWvhtTUOqxOg8PkRRQo/67bld+q9whm8AjTZDvznnkDHnGI4Y3cvPVAeBfXAX2
kyGfxWt+TI6EpGJb0KR0nTITyY6BZ+UyHMEskhvfJ1I4mvNkTXrtQ04VDH1V83Vo
z5Dai0MgPf+m1oOmt04vnjRYU6JtGzDPTVv8oAjMmSZvxuZ/ry/ANhwbMcs0DIdJ
ue0xAdenxMqLNgzA6pcCSOK/AxJ85U8KswNIZIJ7zmxoWIFjrtf+CkzpNp69yd4Z
tSWU/s6/L2Dq0uquzgbptqej4pybkrsixteFuralWhpovyhH9ritqK2aTg==
```

=5nn0

-----END PGP SIGNATURE-----

Posted by rince at 19:28

Friday, December 5, 2014

Wie ich Daten von einem Handy aufs andere bekomme: Threema und TextSecure

Gestern abend ist mein Handy, ein nexus 4 heruntergefallen.

Es ist so blödd gefallen dass links unten das Display ordentlich aufgeratscht ist - mit dem Effekt dass man bei der Bildschirmstatur nur noch wenig tippen kann und die Menütasten gar nicht tun.

Nun war natürlich die Frage, wie komme ich an die Daten dran?

Ich habe mich an den Blogeintrag von Kris Kintopp erinnert, wo er darüber geflucht hat dass die Daten so schlecht von Handy zu Handy migriert werden können und befürchtete schlimmes - aber so schlimm wurde es dann gar nicht.

Mein Glück waren folgende Umstände:

- Ich hatte bereits ein neues Handy
- Im Gegensatz zu vielen Freunden und Bekannten habe ich nicht alles bei Google synchronisiert, nur meine Apps (das sehe ich als Vorteil an), da ich diese über den Play store gekauft habe
- Ich habe aber Dropbox + Boxcryptor zum Datentransfer. Boxcryptor verschlüsselt die Daten auf dem Handy, so dass bei Dropbox dann nur verschlüsselte Daten ankommen und nicht geschaut werden kann was in der Datei steckt.

Erstes Problem: Wie kann ich überhaupt das Handy ansprechen wenn das Display kaputt ist?

Es hat ein wenig gedauert, aber ich konnte über den Google Playstore Teamviewer Quick Support installieren. Dies brachte mich in die Lage, mit Hilfe von Teamviewer auf meinem PC das Display anzusteuern.

Da ich aber möglichst nichts über die Cloud machen wollte habe ich dann einen VNC-Server auf dem Handy installiert und mit TightVNC auf dem PC weitergearbeitet.

Nun hatte ich vollständigen Zugriff auf das Handy, auch mit Touch-Gesten. Super!

Nächstes Problem: Daten von Threema und TextSecure zu migrieren.

Beides ging relativ einfach, auch wenn ich unterschiedliche Wege gehen musste:

- Threema bietet ein verschlüsseltes Backup an. Dies konnte ich anlegen und dann teilen - und über den Teil-Mechanismus konnte ich die Datei Boxcryptor übergeben.

Auf dem neuen Handy konnte ich diese Datei in den Ordner Threema\Backups legen, Threema starten und das Backup einspielen

Ergebnis: Alle Kontakte mit ihren Stati (verifiziert oder nicht) waren wieder da, die Gespräche ebenfalls.

Textsecure bietet aktuell kein verschlüsseltes Backup an. Daher bin ich dort einen anderen Weg gegangen.

Ich habe mit Titanium Backup Pro ein Backup dieser Anwendung inklusive der Daten gemacht.

Dieses habe ich dann wieder via Teilen auf Boxcryptor gelegt (damit war es verschlüsselt) und dann auf dem neuen Handy wieder mit Titanium Backup wieder hergestellt.

Jetzt musste ich einmal den Dienst de-registrieren und wieder registrieren und danach tat alles wieder.

Das einzige was noch fehlt mangels Zeit ist das Synchronisieren meiner Kontakte und Kalender-Daten, daran arbeite ich nachher weiter.

Und für meine Musiksammlung fehlt mir was zum sinnvollen Synchronisieren ohne Google-Mechanismen.

Mal schauen was ich da noch finde

Posted by rince at 11:25