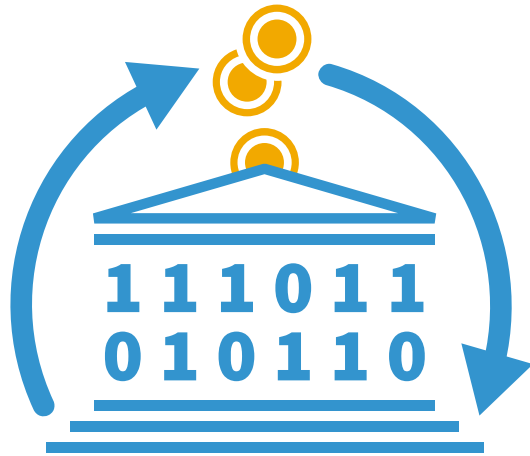




Public Money

Public Code

publiccode.eu

Did you vote already?

[Matrix]

*“Een open netwerk voor beveiligde
gedecentraliseerde communication”*

Peter Scholtens



Linux
User Group
Nijmegen



Wat is Matrix?

Een beveiligd netwerk:

- communicatie van client tot server is beveiligd, maar op de server niet?
- optie voor end-to-end encryptie van clients (niet default)

En gedecentraliseerd netwerk:

- iedereen kan een server opzetten en meedoen.
 - Een server binnen Nederland? Geen probleem
-
- Je adres op matrix is bewust anders dan je e-mail adres:

@username:servername.domain



.compare(,)

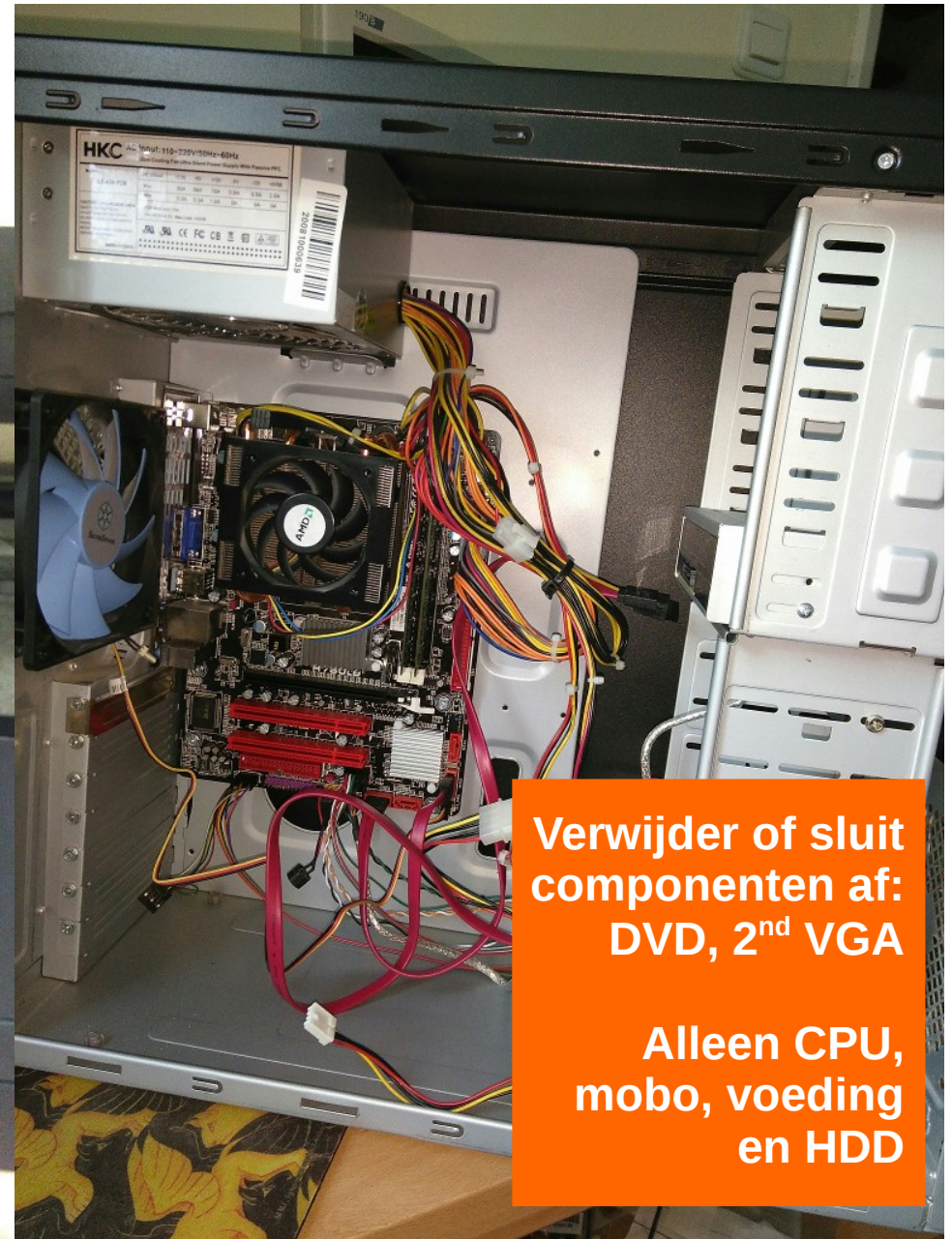
	Matrix	Tox.chat	Retroshare	Wire.com
Open Source	Yes	Yes	Yes	Closed
End-to-End encryption	Not yet / but possible	Default	?	
Simple Human readable ID to distribute to friends	Yes, @peter.scholten: matrix4me.nl	Not really, DHT: 56A1ADE4B65B86BCD51CC73E 2CD4E542179F47959FE3E0E21B 4B0ACDADE51855D34D34D37C B5	Not really, DHT, certificates etc.	
Really peer2peer	No ,each user can add own server	Yes, but sometimes server needed to start communication to look up sites.	Yes, only connect via friend of friend server (recursively?)	
IP protection	Your IP is visible.	Possible with Tor	Possible with Tor	
Services	Voice, Chat, Video	Voice, Chat, Video	Voice, Chat, Video	
Conversation history	Yes	No?	?	
OS support	Most including Ubuntu Touch!	Only one client on Andriod, iOS		



My [Matrix] server

Gebruikte Desktop PC als server

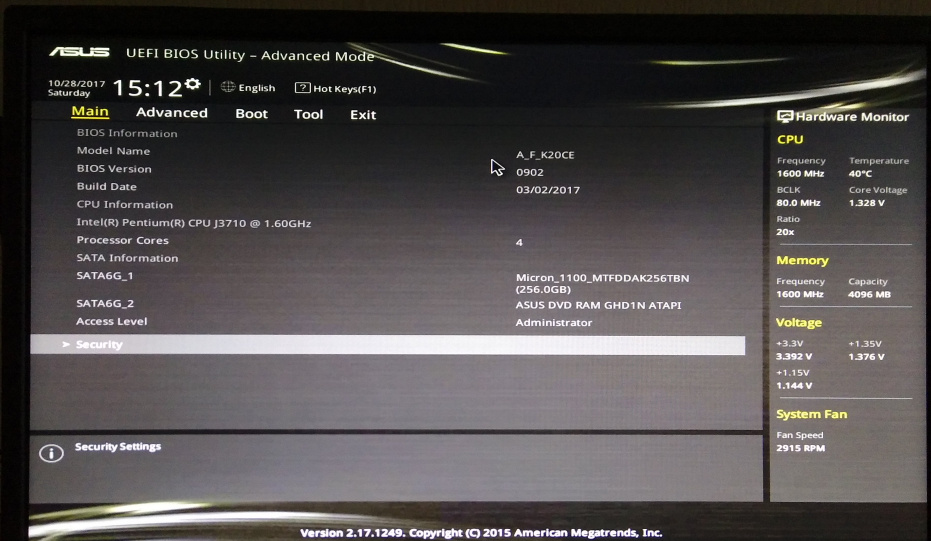
Debian 9.2 amd64
AMD Phenom II X4 925
8GB RAM
32GB swap space
640GB Disk



Verwijder of sluit componenten af:
DVD, 2nd VGA

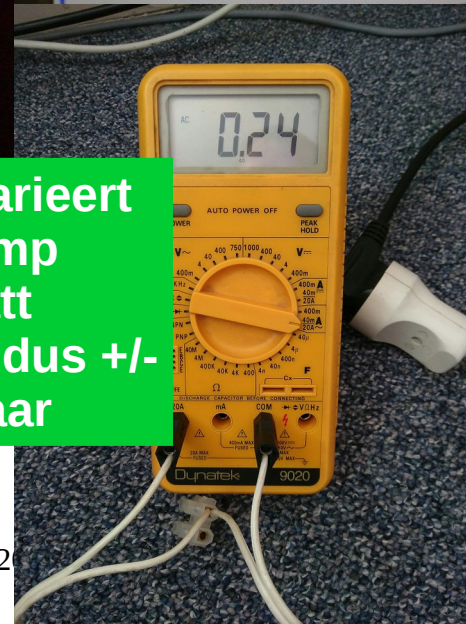
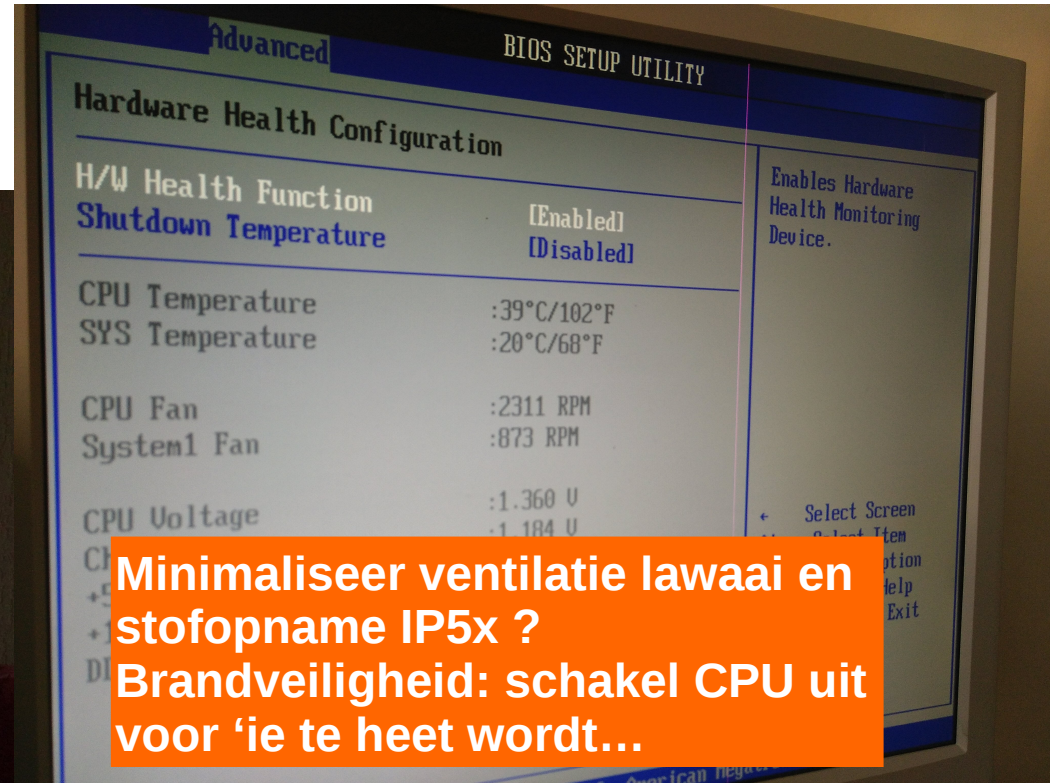
Alleen CPU,
mobo, voeding
en HDD

My [Matrix] server



Update naar recentste BIOS helaas geen libreboot support :-)

**Stroom gebruik varieert
van 0.25 ... 0.36 Amp
Dat is 55 ... 80 Watt
Met € 0,1932/Kwh dus +/-
€ 100 ... 134 per jaar**



Synapse

- Matrix protocol is opgebouwd uit bekende HTTP request commando's: GET, PUT, POST, DELETE, en data uitwisseling via JSON
 - Zie <https://matrix.org/docs/spec/>
 - Poorten 8008 en 8448 worden gebruikt
- Server geschreven in Python als Proof-of-Concept
 - Deze is ook het meest uitontwikkeld
- Andere servers in Golang (dendrite, pallium) Rust (Ruma) maar nog niet voorbij alpha status
- Reference implementaties met als doel spec' te controleren...



Synapse from Source

<https://github.com/matrix-org/synapse>

Bibliotheken van bestaande bronnen:

```
sudo apt-get install build-essential python2.7-dev libffi-dev \  
python-pip python-setuptools sqlite3 \  
libssl-dev python-virtualenv libjpeg-dev libxslt1-dev
```

En Synapse van github:

```
virtualenv -p python2.7 ~/.synapse  
source ~/.synapse/bin/activate  
pip install --upgrade pip  
pip install --upgrade setuptools  
pip install https://github.com/matrix-org/synapse/tarball/master
```



YAML

Configuration:

```
$ cd ~/.synapse
$ python -m synapse.app.homeserver \
    --server-name my.domain.name \
    --config-path homeserver.yaml \
    --generate-config \
    --report-stats=[yes|no]
```

En aanmaken van eerste gebruiker:

```
$ source ~/.synapse/bin/activate
$ synctl start # if not already running
$ register_new_matrix_user -c homeserver.yaml
https://localhost:8448
New user localpart: erikj
Password:
Confirm password:
Make admin [no]:
Success!
```

Andere acties (reset wachtwoord) gaan nog via DB.



DNS instellingen voor federation

Let op: Het wijzigen van je DNS, zonder dat je weet wat je doet, kan leiden dat je webpagina's niet meer werken! Voor meer info over DNS zie onze help pagina.

Deze domeinnaam is beveiligd met DNSSEC

DNS regels

Rij	Type	Subdomein	Domeinnaam	Inhoud	Prioriteit	Actie
1	A		matrix4me.nl	80.101.41.222		 
2	A	*	matrix4me.nl	80.101.41.222		 
3	A	www	matrix4me.nl	80.101.41.222		 
4	SRV	_matrix._tcp	matrix4me.nl	0 443 matrix4me. nl	10	 
5	TXT		matrix4me.nl	"v=spf1 a mx inclu de:spf.mijndomein hosting.nl ~all"		 

Controleer met DNS test utility:



```
dig -t srv _matrix._tcp.matrix4me.nl
```

Modem / Router instellingen

Sharing

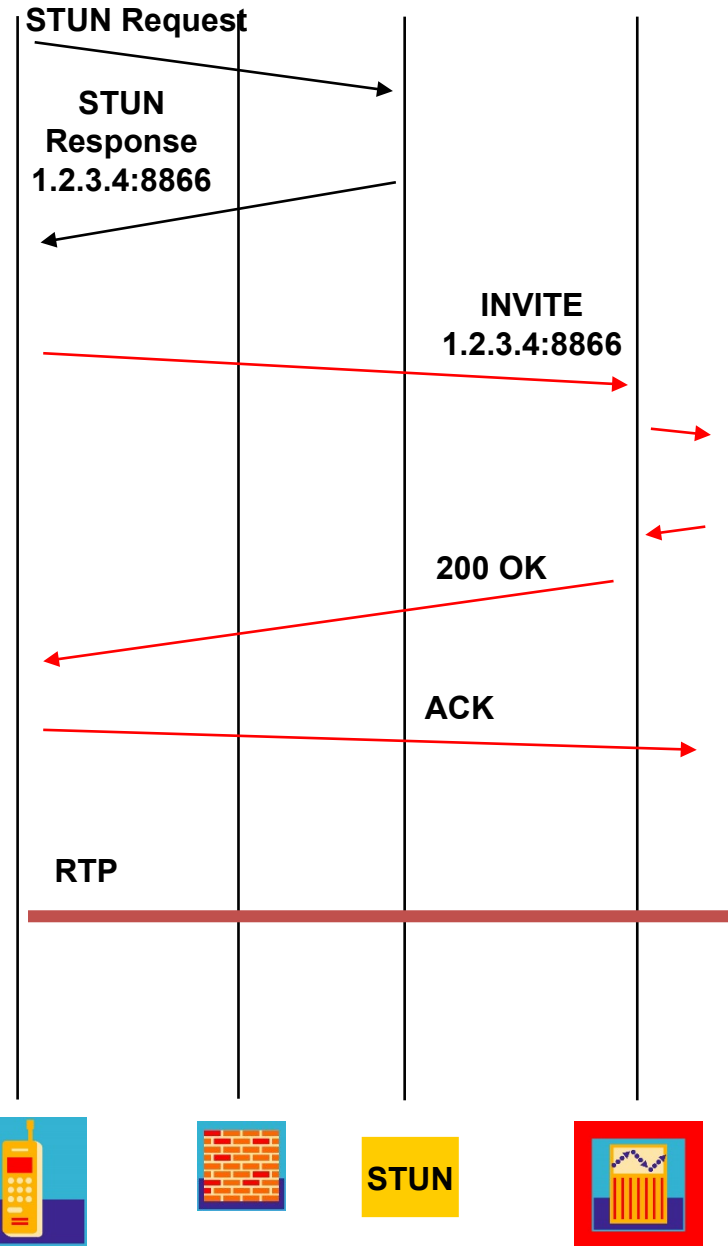
Status	Name	Protocol	IP address in the Internet	Port assigned externally
●	Matrix IPv4	TCP	80.101.41.222	443
●	TURN	UDP	80.101.41.222	3478 - 3479

Let op: TCP voor HTTPS, maar UDP voor TURN



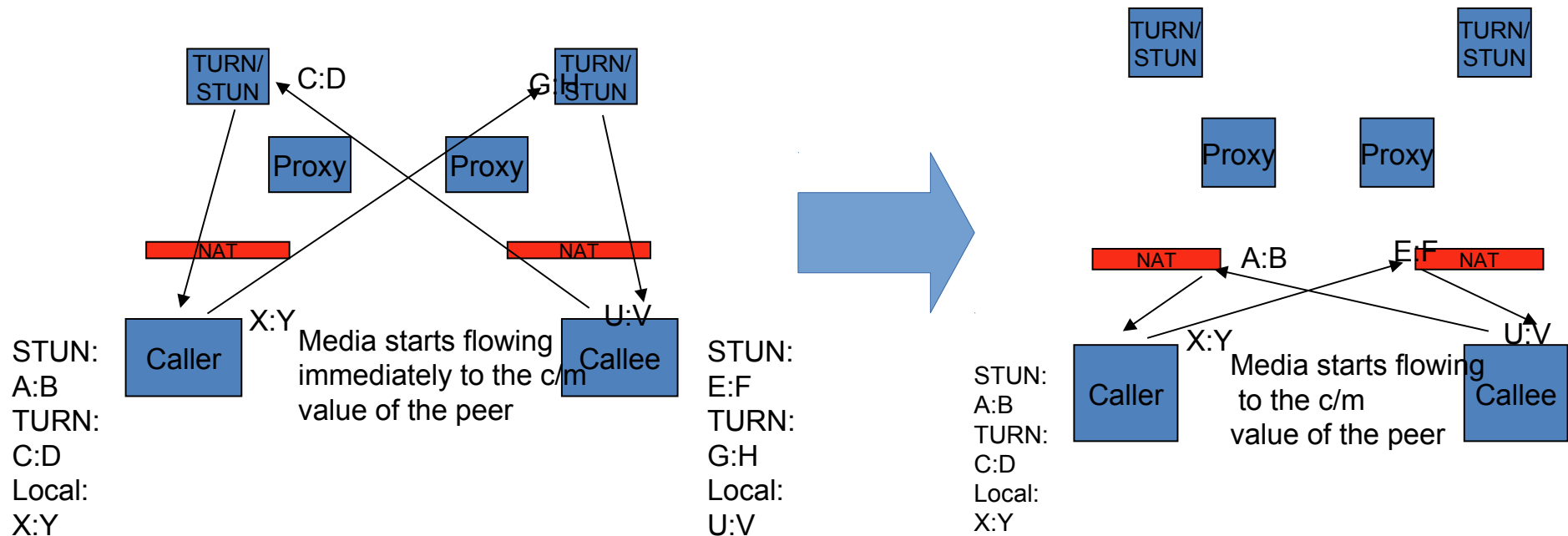
TURN, STUN, ICE ?

Nodig om om de NAT heen te werken
(Met IPv6 hoeft dit niet meer?)



- <https://en.wikipedia.org/wiki/STUN>
- <http://www.jdrosen.net/uploads/1/5/0/0/15008848/stun-turn-ice.pptx>
- https://en.wikipedia.org/wiki/Traversal_Using_Relays_around_NAT

Protocol voor opbouwen verbinding



- Succesvolle verbinding betekent *geen belasting* voor de TURN / STUN server

Federation tester

Test verbinding:

```
turnutils_natdiscovery -m 80.101.41.222    #zit in package coturn
```

Test of de federation server zichtbaar is vanuit andere matrix servers:

https://matrix.org/federationtester/api/report?server_name=matrix4me.nl

Lijst met (public) servers:

<https://www.hello-matrix.net>



Database

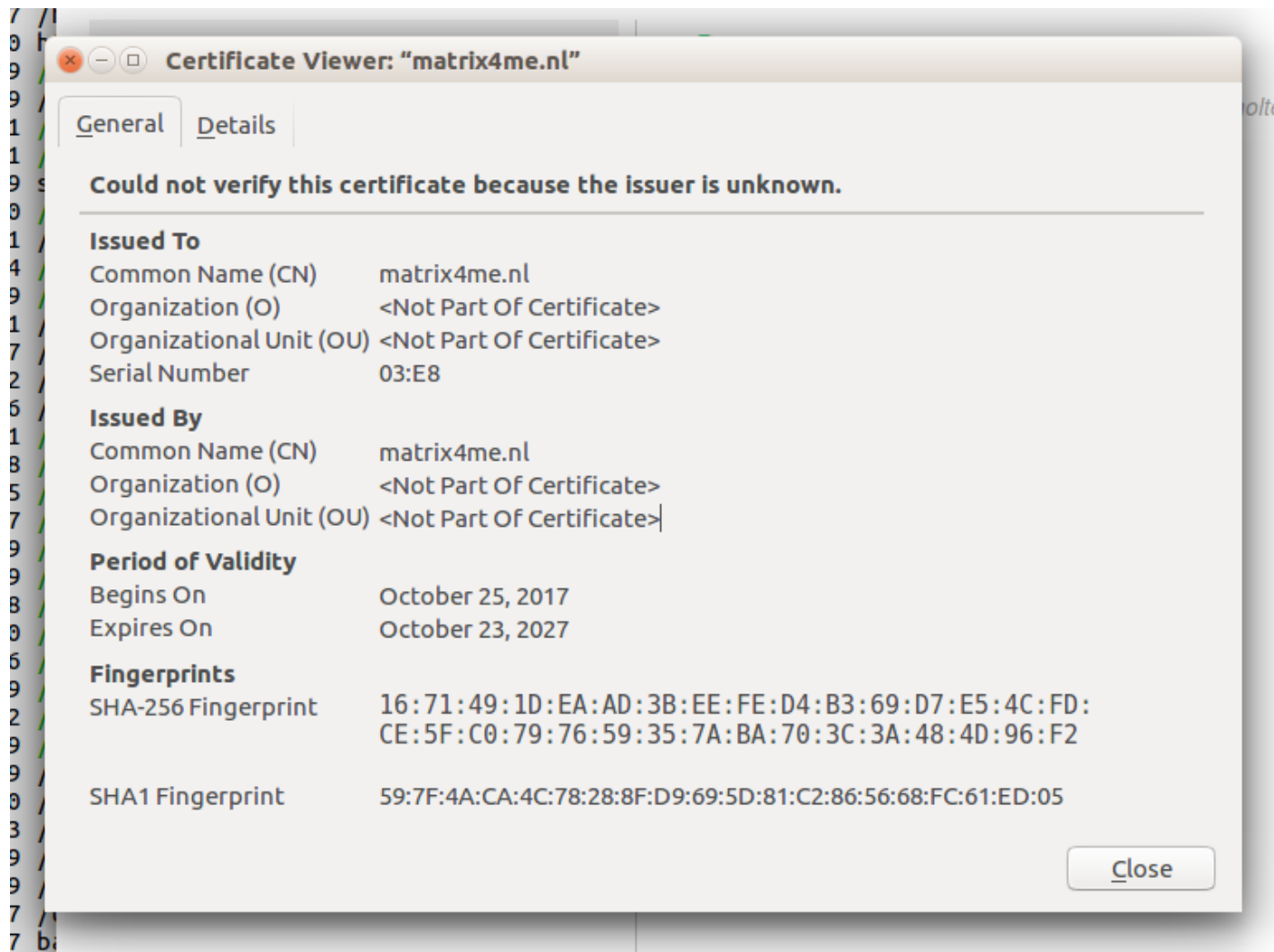
- SQLite is default geïnstalleerd met synapse server
 - <https://www.sqlite.org/whentouse.html> *“Generally speaking, any site that gets fewer than 100K hits/day should work fine with SQLite. The 100K hits/day figure is a conservative estimate, not a hard upper bound. SQLite has been demonstrated to work with 10 times that amount of traffic.”*
 - Gemakkelijk te installeren en te gebruiken,
 - maar 100K hits/dag = 1.15hit/seconde...
- PostgreSQL kan ook in synapse
 - Meer parallel verdeling, tegelijkertijd lezen en schrijven
 - Conversie tool nodig zie:
<https://github.com/matrix-org/synapse/blob/master/docs/postgres.rst>
 - Let op, master versie is geheel foutloos op dit moment (synapse 0.24.1):
<https://github.com/matrix-org/synapse/issues/2565>
- Dit zou veeeeel meer gebruikers aan moeten kunnen...



[Matrix] Clients



Self-signed certificaat <https://matrix4me.nl>





Skype, Facebook,
Twitter???
No, Matrix4Me!

Web applicatie
AngularJS wordt
geleverd met
synapse server.

Effectieve manier om
set-up lokaal te
testen,

Maar wordt niet meer
onderhouden...

Log in using:

☐ Email address

☒ Matrix ID (e.g. @bob:matrix.org or bob)

Login

Home Server:

Your home server stores all your conversation and account data.

Identity

Server:

*Matrix provides identity servers to track which emails etc. belong to which Matrix IDs.
Only https://matrix.org currently exists.*

[Create account](#)

[Forgotten password?](#)



Riot.im is zowel een webapp als verkrijgbaar op F-Droid, Google Play en Appstore

Inloggen

Inloggen met

matrix4me.nl Matrix-ID ▼

@peter.scholtens:matrix4me.nl

.....

[Wachtwoord vergeten?](#)

Inloggen



Standaardserver



Aangepaste server

Thuisserver-URL

https://matrix4me.nl

Identiteitserver-URL

https://vector.im

[Wat betekent dit?](#)

[Open een account](#)

[Als gast inloggen](#)

Nederlands ▼

UBports en Aquaris BQ4.5

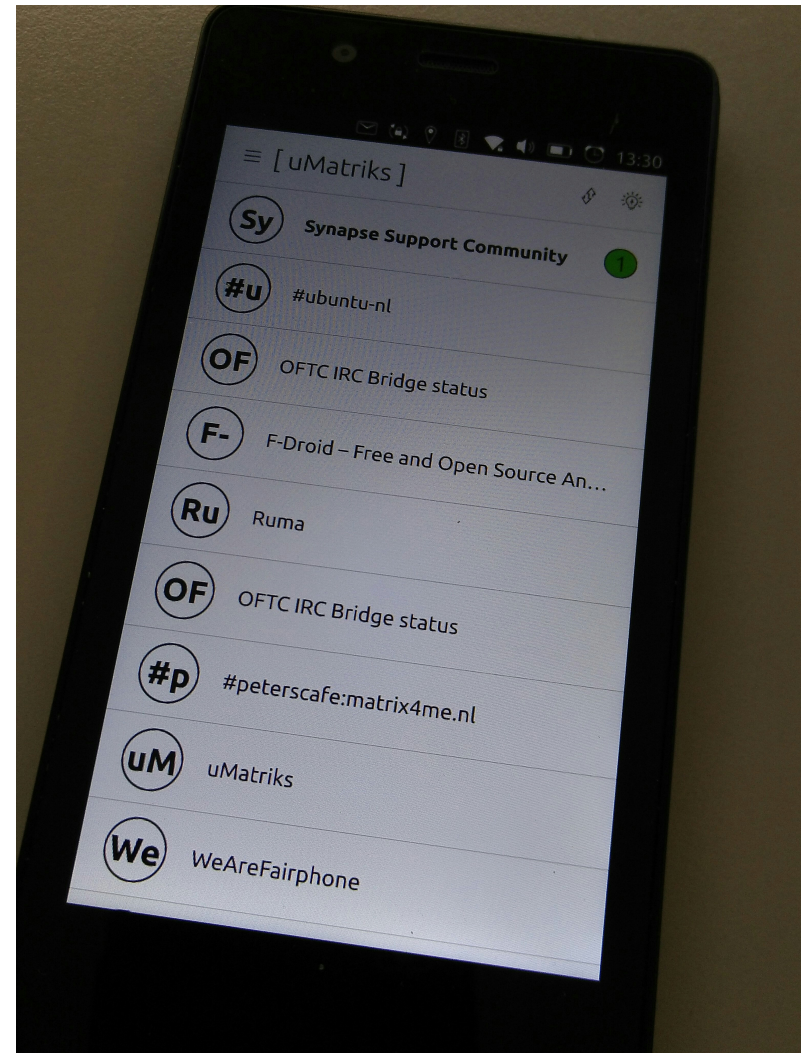
Volg de handleiding op:

<https://devices.ubports.com/#/krillin>

Zie ook:

<https://www.patreon.com/ubports>

Installeer uMatriks via de Open Store:



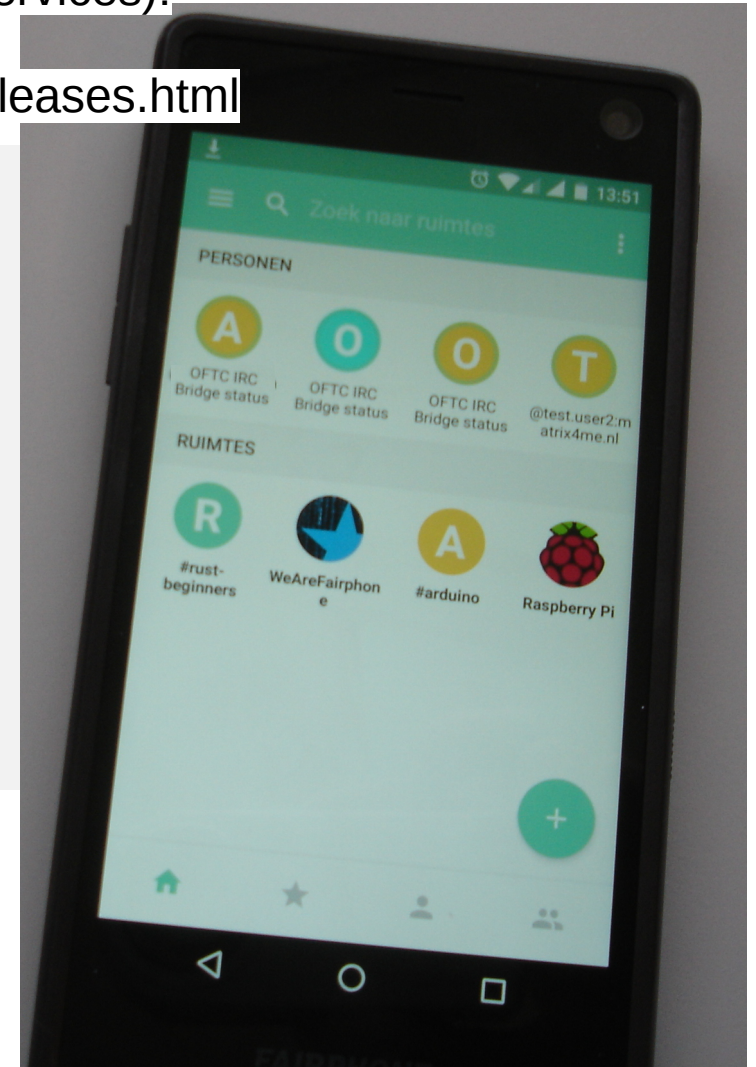
F-Driod en Fairphone 2

Installeer Fairphone Open OS (zonder Google Mobiles Services):
(KRACK al op 24 oktober gerepareerd!)

<https://code.fairphone.com/projects/fairphone-2-official-releases.html>

Android™ 6.0 Marshmallow

Operating system	Build number	Release date	Extra information
Fairphone Open 17.06.4	fp2-sibon-17.06.4	June 2017	Checkup
Fairphone Open 17.07.6	fp2-sibon-17.07.6	July 2017	Checkup
Fairphone Open 17.08.1.1	fp2-sibon-17.08.1.1	August 2017	Checkup
Fairphone Open 17.09.3	fp2-sibon-17.09.3	September 2017	Checkup
Fairphone Open 17.10.1	fp2-sibon-17.10.1	October 2017	Checkup
Fairphone Open 17.10.2	fp2-sibon-17.10.2	October 2017	Checkup
Fairphone Open 17.11.2	fp2-sibon-17.11.2	November 2017	Checkup



En vervolgens via F-Driod de Riot.im app



F-Droid



Riot.im

Open team collaboration

[Matrix] and more



!roBOTs

Je kunt robots maken en installeren. Bijvoorbeeld de hello-bot van <https://gitlab.com/argit/hello-matrix-bot>

Je nodigt deze robot uit: **@hello-matrix:matrix.org**

En kunt nu het weer opvragen door:

!help

!dice

!weather nijmegen

!calculate 2*pi

!whois matrix4me.nl



Bridges

IRC is beschikbaar via **matrix-appservice-irc**

Syntax voor deze IRC kanalen:

`#freenode_#somewhere:matrix.org` (for freenode)

`#mozilla_#somewhere:matrix.org` (for moznet)

Bijvoorbeeld:

`#freenode_#linuxnijmegen:matrix.org`

(Nog niet door mij geprobeerd...:)

Voor het Verto protocol: **matrix-appservice-verta**

Een brug naar Slack: **matrix-appservice-slack**

Skype, Lync, XMPP, etc via libpurple: **node-purple**

