PGP web of trust

Web of trust

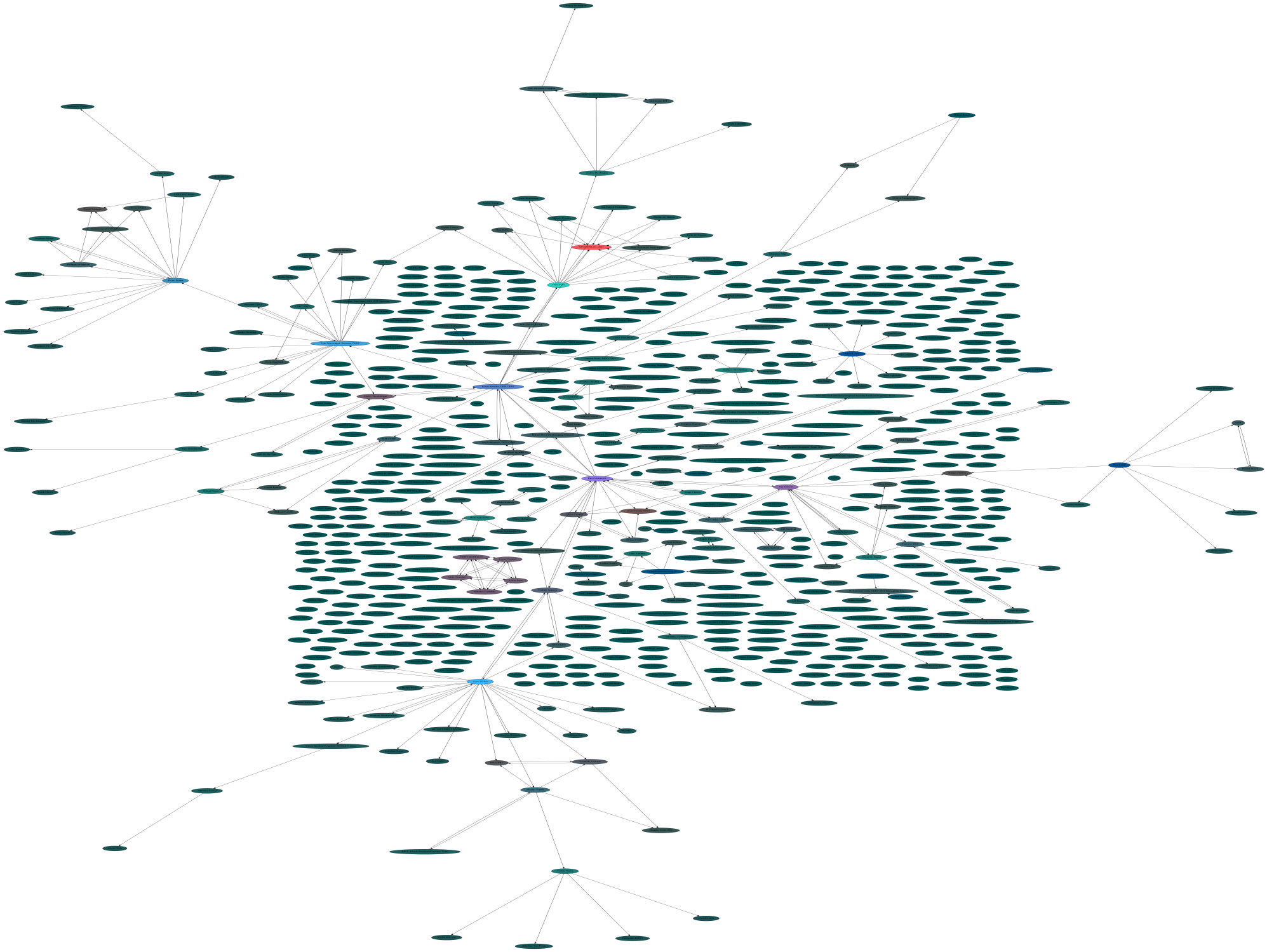
- From: http://pgp.cs.uu.nl/plot/

- The PGP **web of trust** can be viewed as a directed graph where the **points** are the PGP keys, and the **arrows** (directed lines) are the signatures.
- If there is a path from key *A* to key *B*, the **distance** from *A* to *B* is the length of the **shortest** path from *A* to *B*.
- The **strong set** is the largest set of keys such that for any two keys in the set, there is a path from one to the other.
- The **mean shortest distance** (MSD) of a key is the average distance to that key.
- The **avarage mean shortest distance** (AMSD) is the average of the MSD's of all keys.

FIRST Keyring

gpg: Total number processed: 676
gpg: w/o user IDs: 1
gpg: imported: 671 (RSA: 287)
gpg: unchanged: 3
gpg: new signatures: 5

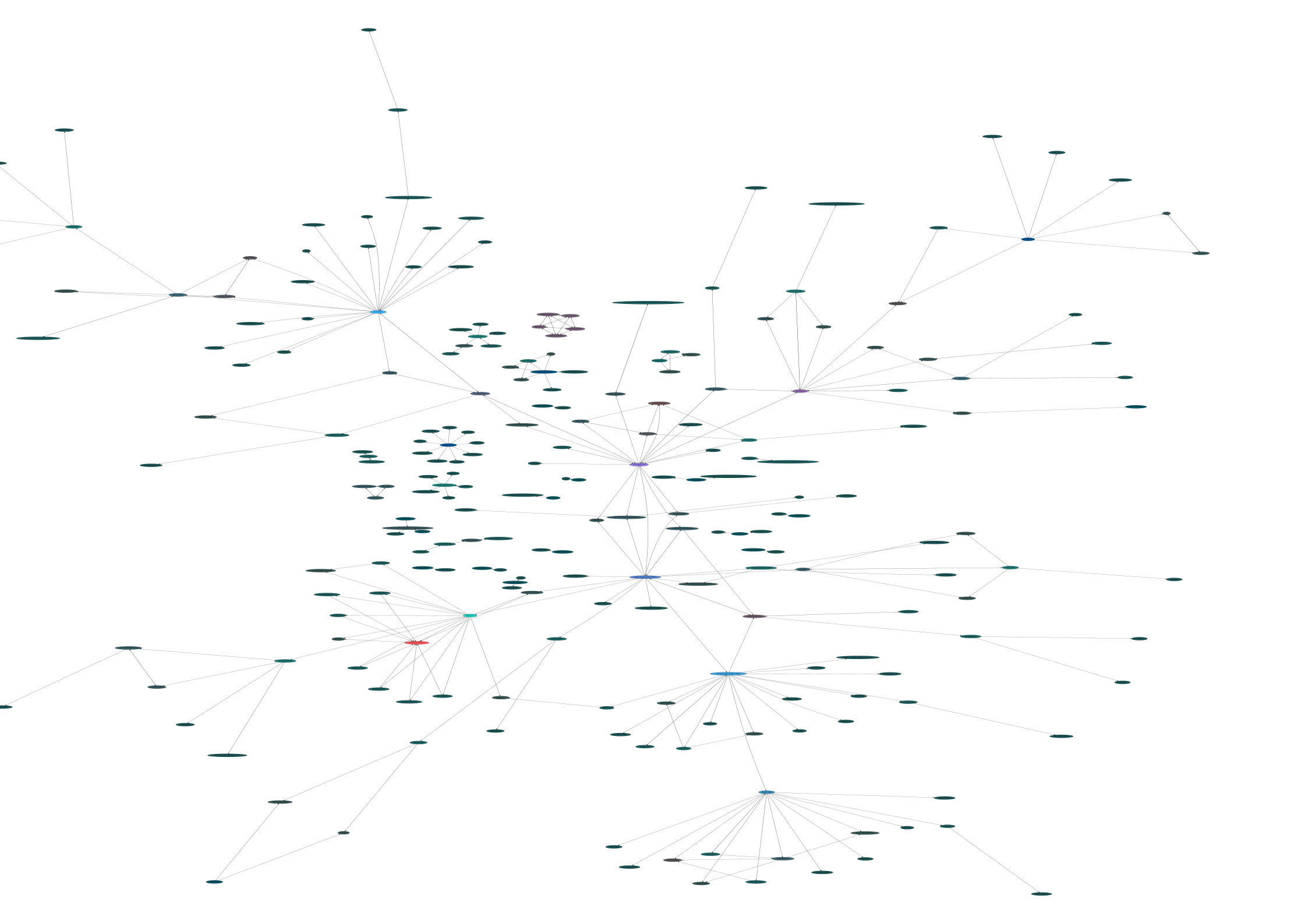
OpenSource tool: sig2dot.pl (google for it ;-)



Not so good

- 236 FIRST teams
- 676 keys , not so much

ONLY 116 are part of the Web of TRUST !!!!



Keysigning Party

In cryptography, a key signing party is an event at which people present their PGP-compatible keys to others in person, who, if they are confident the key actually belongs to the person who claims it, digitally sign the PGP certificate containing that public key and the person's name, etc. This is one way to strengthen the web of trust

Wikipedia.

FIRST 23 Keyring : http://biglumber.com/x/web?keyring=3593

Send your PGP key to the server

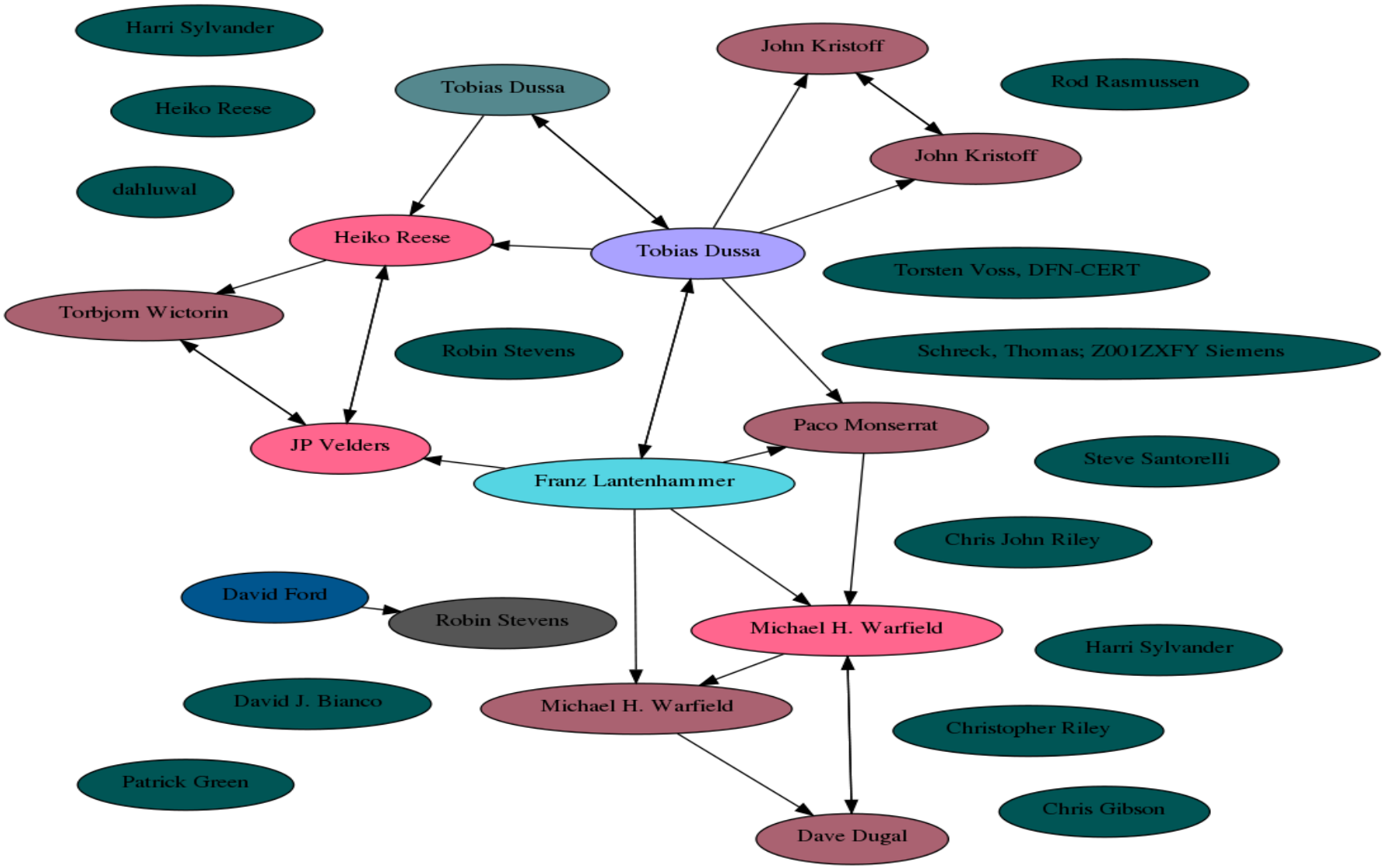
Bring you your ID card/ passport tomorrrow

Keysigning Party status

http://biglumber.com/x/web?keyring=3593

- Today: 17Keys in the MSD out 29
  - 9 in the < 10K line group
  - Not perfect, but quite good

Today


Harri Sylvander
John Kristoff
Tobias Dussa
Rod Rasmussen
Heiko Reese
John Kristoff
dahluwal
Heiko Reese
Tobias Dussa
Torsten Voss, DFN-CERT
Torbjorn Wictorin
Robin Stevens
Schreck, Thomas; Z001ZXFY Siemens
Paco Monserrat
JP Velders
Steve Santorelli
Franz Lantenhammer
Chris John Riley
David Ford
Robin Stevens
Michael H. Warfield
Harri Sylvander
David J. Bianco
Michael H. Warfield
Christopher Riley
Patrick Green
Chris Gibson
Dave Dugal

Remember

FIRST member: Submit & update your keys

All: attend the PGP keysigning party tomorrow