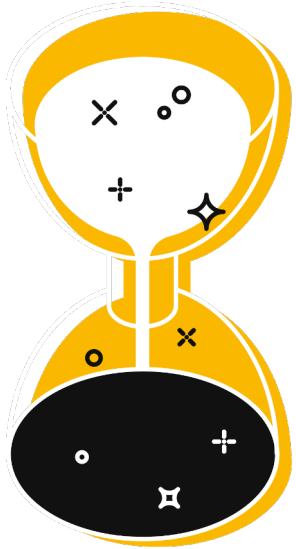
Around the World with NTS

deployment and usage

Christer Weinigel, Netnod 2023-03-15

Start with NTP

- Network Time Protocol
- The protocol for distribution of time over the internet
- Has been around for a long time
  - Created by David Mills in 1980, RFC 958 in 1985
  - Latest version is NTP version 4, RFC 5905, from 2010
- Very good timing accuracy
- Multiple implementations



Netnod and NTP

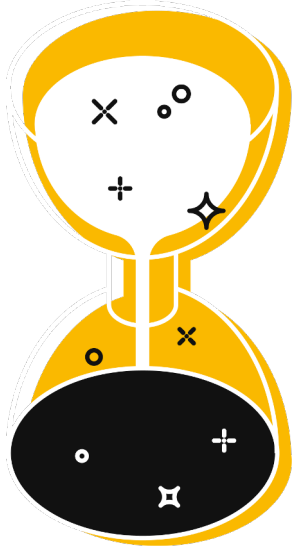
- Netnod have been doing NTP since 2013
- Multiple nodes with redundant hardware
  - 2x caesium clocks
  - 2x time distribution
  - NTP in a FPGA, multiple 10Gbit/s ports at wire speed
  - Battery backup for everything
  - Traceable to UTC(SP) and UTC

Netnod's NTP nodes

- Six nodes throughout Sweden
  - Luleå
  - Sundsvall
  - Stockholm x2
  - Gothenburg
  - Malmö/Copenhagen

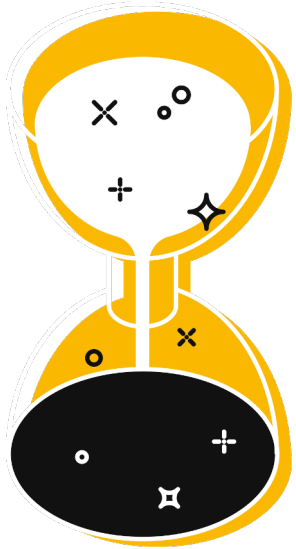
Issues with NTP

- No security
  - Plain text, vulnerable to man in the middle attacks
  - Time is important
    - TLS, HTTPS, SMTPS, IMAPS, POP3S
    - DNSSEC
- Actually: no scalable security
  - Authentication using a shared secret and MD5/SHA1
    - Limited number of shared keys (16 bits)
    - Key distribution is hard
  - Autokey never caught on



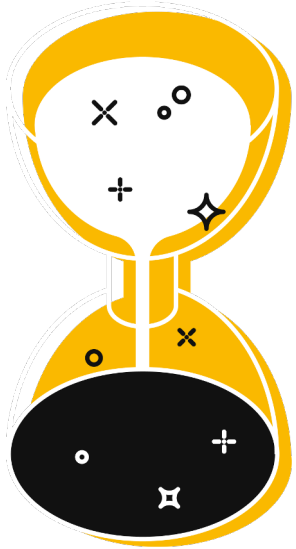
What is NTS?

- NTP with security
  - Adds authentication and encryption to NTP
  - Scales to an unlimited number of clients
  - Netnod got involved in IETF draft process during 2018
  - Published as RFC 8915 in September 2020



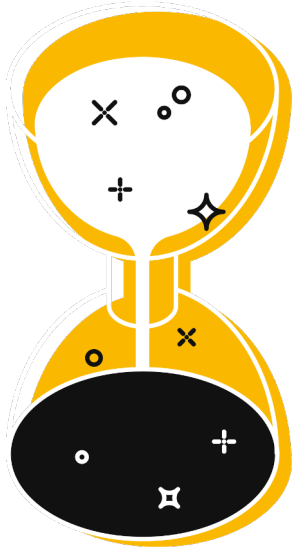
NTS phases

- Key establishment, NTS-KE
  - TLS using same infrastructure as HTTPS
  - Server creates cookies which are stored on the client
- Timestamping, NTS-TS (not an official abbreviation)
  - NTP with extension fields
  - Stateless server using cookies from client



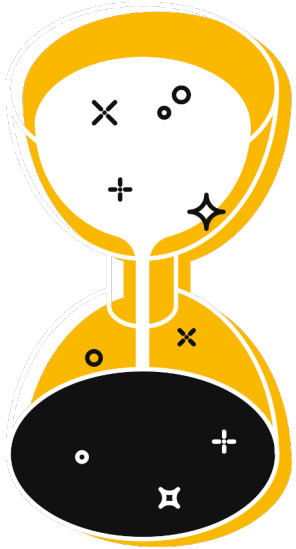
NTS implementations

- Implementations in C, C++, Go, Python, Rust
- NTPsec
- Chrony
- Netnod does NTS
  - Custom NTS-KE server
  - Custom NTS-TS in an FPGA
    - 10Gbit/s port at wire speed



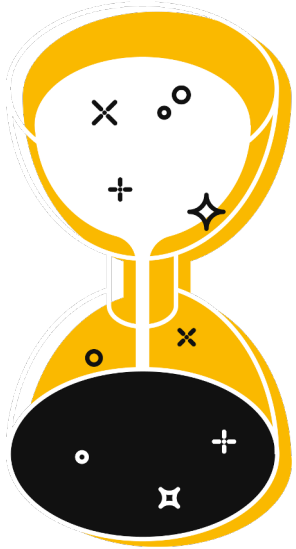
NTP and NTS References

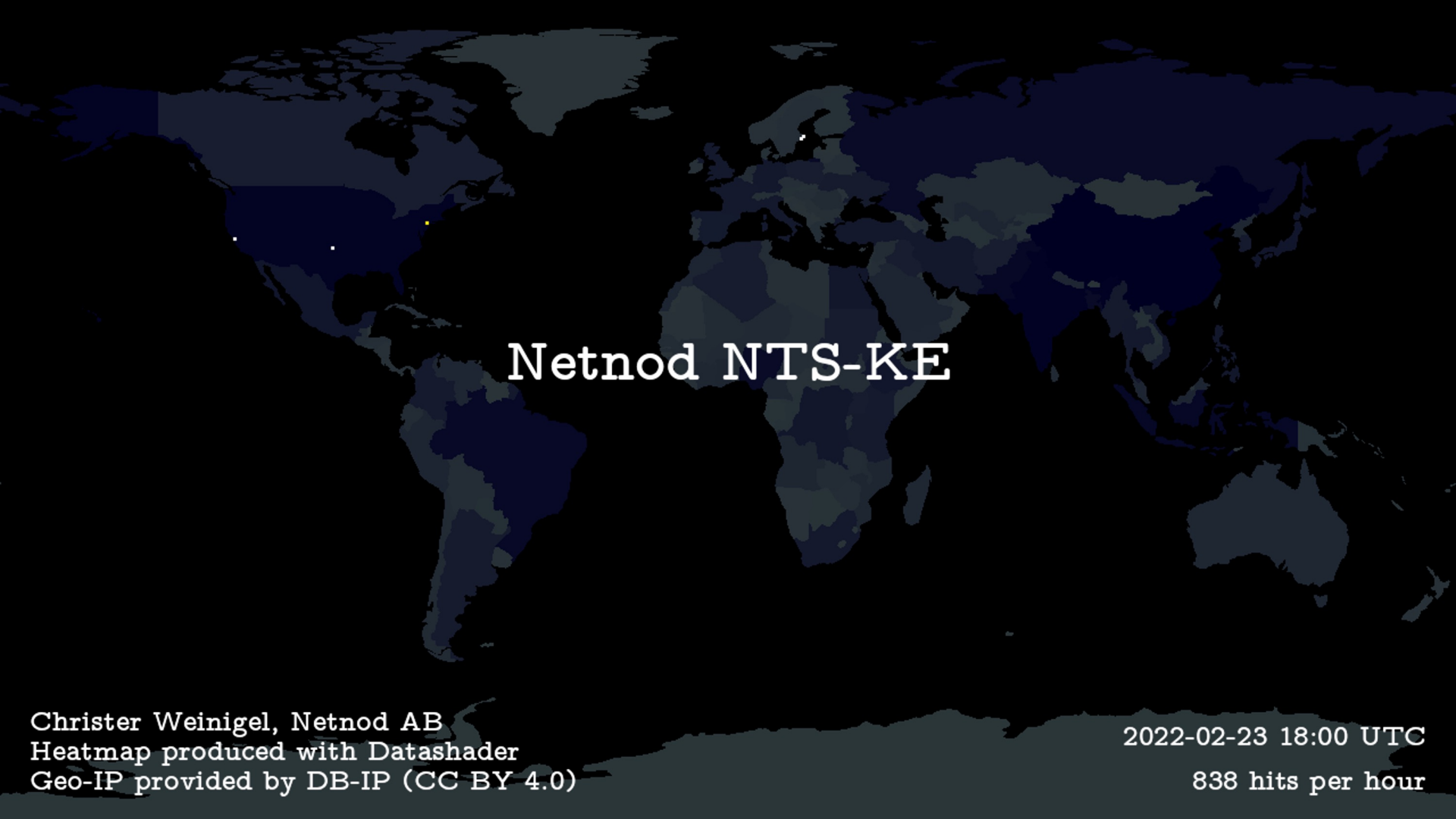
- NTS white papers
  - How does NTS work and why is it important?
  - How we developed the world's first hardware implementation of Network Time Security
- NTS proposed standard (RFC 8915)
- Best practice for connecting to NTP servers
- How to set up an NTS client
- List of Netnod time services



Movie about NTS usage

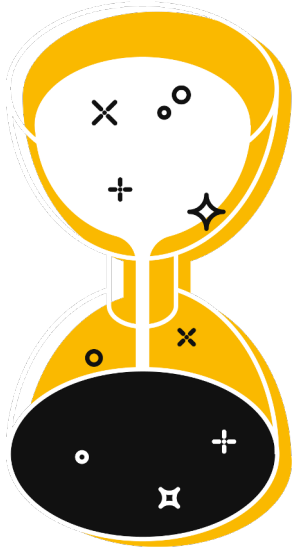
- Movie showing NTS-KE usage
  - Netnod's NTS servers are in Stockholm
  - Coloured dots show clients
  - Netnod turned on new servers in february 2022




Netnod NTS-KE
Christer Weinigel, Netnod AB
Heatmap produced with Datashader
Geo-IP provided by DB-IP (CC BY 4.0)
2022-02-23 18:00 UTC
838 hits per hour

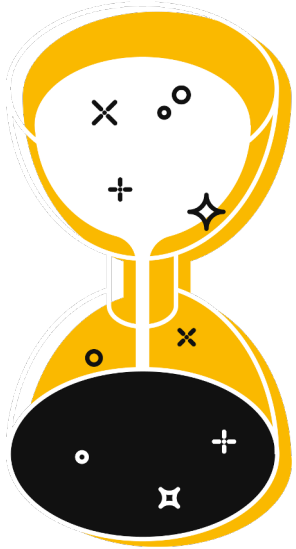
Actions

- Increase NTS-KE server performance
  - Throw more hardware at the problem
    - Add more CPU and memory
  - Shorter timeouts, less logging, better threading
  - Kernel optimisation, interrupts, buffers
- Load balancing within a node
- More nodes
  - Added Gothenburg, Malmö, Sundsvall earlier than planned
  - Luleå will soon be up too



Conclusion

- Had to eat my own words
  - "Load won't be a problem, only enthusiasts will use NTS for some time"
- I'm personally very happy
  - NTS is actually being used
  - Increases security and robustness of the internet
- Feel free to contact me if you have any questions
  - Christer Weinigel <wingel@netnod.se>



Thanks for listening!

Visit ut at netnod.se