The GNU Name System & NGI

Christian Grothoff

Berner Fachhochschule
Technik und Informatik

10.12.2020

Context

Design Choices for a Civil Network!

Internet Design Goals (David Clark, 1988)

1. **Internet communication must continue despite loss of networks or gateways.**
2. The Internet must support multiple types of communications service.
3. The Internet architecture must accommodate a variety of networks.
4. The Internet architecture must permit *distributed management* of its resources.
5. The Internet architecture must be cost effective.
6. The Internet architecture must permit host attachment with a low level of effort.
7. **The resources used in the internet architecture must be accountable.**

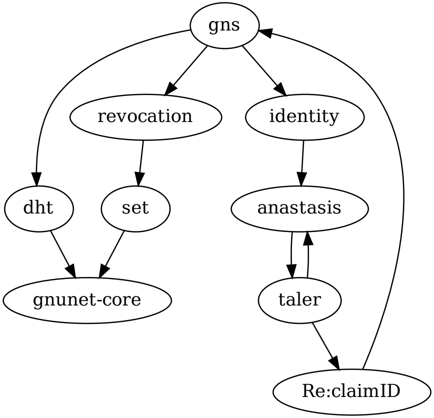
GNUnet Design Goals

1. GNUnet must be implemented as Free Software.
2. GNUnet must minimize the amount of personally identifiable information exposed.
3. The GNUnet must be fully distributed and resilient to external attacks and rogue participants.
4. GNUnet must be self-organizing and not depend on administrators or centralized infrastructure.
5. GNUnet must inform the user which other participants have to be trusted when establishing private communications.
6. GNUnet must be open and permit new peers to join.
7. GNUnet must support a diverse range of applications and devices.
8. GNUnet must use compartmentalization to protect sensitive information.
9. The GNUnet architecture must be resource efficient.
10. GNUnet must provide incentives for peers to contribute more resources than they consume.

Applications in GNUnet (under development)

- Anonymous and non-anonymous publishing
- IPv6–IPv4 protocol translation and tunnelling
- Conversation: secure, decentralized voice communication
- **GNU Name System**: censorship-resistant replacement for DNS (Martin Schanzenbach, Bernd Fix, **NGI DISCOVERY**)
  - Revocation: Key revocation
  - Ascension: Automatically migrate DNS zones to GNS (Patrick Gerber)
- Re:claimID: identity management (Martin Schanzenbach, et al)
- GNU Taler: privacy-friendly payments (Florian Dold, et al)
- Anastasis: key escrow and recovery (Vaishnavi Mohan, Dennis Neufeld, et al)

Software Architecture



System Architectures

GNU Taler Classical client-server

Anastasis Client-side secret splitting, untrusted multiple servers in Clouds

Re:claimID Self-sovereign identities with trusted authorities for attestation

GNUnet Fully decentralized, peer-to-peer

The GNU Name System

Back to the Internet: DNS troubles

- DNS remains a source of traffic amplification for DDoS
- DNS censorship (i.e. by China) causes collateral damage in other countries
- DNS is part of the mass surveillance apparatus (MCB)
- DNS is abused for the offensive cyber war (QUANTUMDNS)

Band aid solutions[1] will **not** fix this.

[1] DNS-over-TLS, DoH, DNSSEC, DPRIVE, ODNS, ...

The GNU name system

- Decentralized name system
- Supports globally unique (& secure) identification
- Achieves query and response privacy
- Provides public key infrastructure
- Virtually instant key revocation
- Interoperable with DNS

Applications for GNS

DNS Theoretical full replacement (⇒ Ascension)

SecuShare PKI for decentralized social networking applications (Carlo von Loesch, et al)

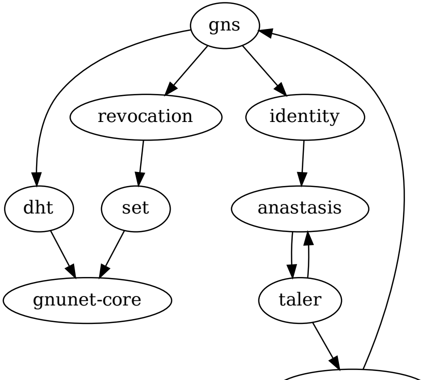
Re:claimID OIDC-compatible provider-less identity management / SSO platform

p≡p PKI for e-mail

Next Steps

Ongoing work within NGI

- NGI DISCOVERY **RFC-style protocol specification for GNS, 2nd implementation in Go**, GNUnet packages for major distributions (done)
- NGI TRUST Attribute attestation for Re:claimID, integrated demonstrator with Taler and WooCommerce to provide account-less form-less shopping experience; usability study (WiP)
- NGI ZERO Security audit of GNU Taler and Taler auditor deployment preparations (WiP)
- ~~NGI LEDGER~~ Anastasis for backup of user core secrets (GNS keys, Taler cash) — FundingBox procedural failures ⇒ killed by EC
- ~~NGI POINTER~~ ~~Building a privacy-friendly decentralized Internet~~



Future work

set RFC-style protocol specification (with Elias Summermatter)

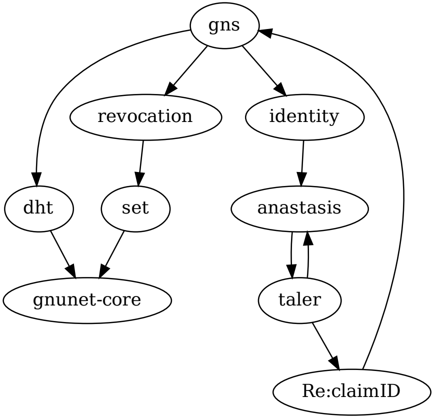
dht RFC-style protocol specification (~~POINTER~~)

gnunet-core Performance and usability issues (~~POINTER~~, ~~INNOSUISSE~~)

anastasis Deployment and use for various applications (~~LEDGER~~)

taler Digital Euro (ECB?)

Re:claimID The new SwissID / Electronic Patient Dossier / etc.



Questions?

Literature:

- Matthias Wachs, Martin Schanzenbach and Christian Grothoff. *A Censorship-Resistant, Privacy-Enhancing and Fully Decentralized Name System*. **13th International Conference on Cryptology and Network Security**, 2014.
- Martin Schanzenbach, Christian Grothoff, Bernd Fix. *The GNU Name System*. `https://datatracker.ietf.org/doc/draft-schanzen-gns/`
- Florian Dold, Christian Grothoff. *The 'payto' URI Scheme for Payments*. `https://tools.ietf.org/html/rfc8905`

More Information on the Web:

- `https://gnunet.org/`
- `https://taler.net/`
- `https://grothoff.org/christian/`