

# The GNU Name System

ICANN66

---

Martin Schanzenbach

11/5/2019



# The GNU Name System In a Nutshell

---

- DNS remains a source of traffic amplification 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 offensive cyber war (QUANTUMDNS).
- DoT/DoH, DNSSEC, DPRIVE unfortunately do **NOT** fix this.

# What is the GNU Name System?<sup>2</sup>

- Fully decentralized name system  $\Rightarrow$  Names are not global.
- Supports globally unique and secure identification.
- Features query and response privacy.
- Provides a public key infrastructure
  - Each zone is associated with a cryptographic key pair.
  - Delegation between zones establishes trust relationship.
- Interoperable with DNS.
- Usable.<sup>1</sup>

---

<sup>1</sup>User studies conducted in “Decentralized Authentication for Self-Sovereign Identities using Name Systems” (DASEIN) project.

<sup>2</sup>Joint work with Christian Grothoff and Matthias Wachs

- Identity management: **re:claimID** (<https://reclaim-identity.io>)
- Social Networks: **SecuShare** (<https://secushare.org>)
- Healthcare: **Accident insurance and private health data**.<sup>3</sup>
- Others: **Chat, Host addressing, ...**

---

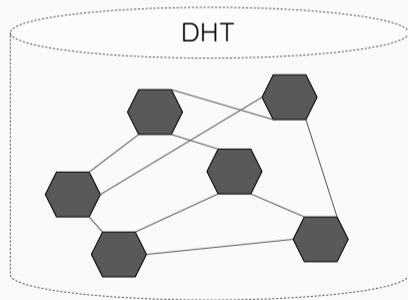
<sup>3</sup>Joint work with FH Bern, “Decentralized Authentication for Self-Sovereign Identities using Name Systems” (DASEIN)

# Technical Overview

---

## Record Storage / Retrieval

- GNS stores records in a **Distributed Hash Table** (DHT).
- DHTs allow us to map keys to values.
- Naive approach: Map domain names to records.  
e.g.: example.com  $\Rightarrow$  A: 1.2.3.4



- **Query privacy**
  - GNS implements a **Private Information Retrieval** (PIR) scheme:  
“a protocol that allows a user to retrieve an item from a server in possession of a database without revealing which item is retrieved.”<sup>4</sup>
  - Queries do not reveal domain name.
- **Record confidentiality**: Values in DHT are signed and encrypted by zone owner.
- **Zone privacy**: Zones cannot be enumerated.
- **Censorship and DDoS resistance**: Decentralized, resilient directory.

---

<sup>4</sup>[https://en.wikipedia.org/wiki/Private\\_information\\_retrieval](https://en.wikipedia.org/wiki/Private_information_retrieval)



## Zone Delegation

- The “NS” equivalent in GNS is called “PKEY” .
- A “PKEY” record contains public zone keys.
- The combination of a “PKEY” record value and a name allows users to query records in a delegated zone.

“.com” zone: 5G0Z

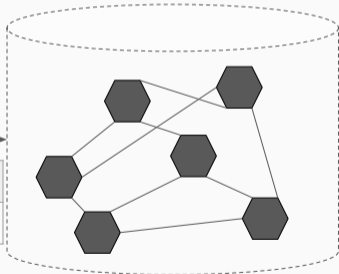
Bob's zone: 7F5T



www.bob.com = 1.2.3.4

PUT *bob* in 5G0Z

PUT *www* in 7F5T



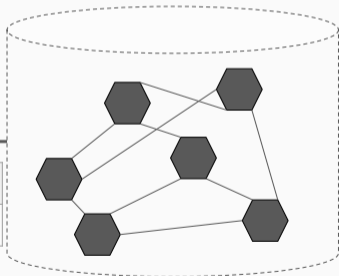
Label	Type	Value
bob	PKEY	7F5T

Label	Type	Value
www	A	1.2.3.4

*www.bob.com?*



GET *bob* in 5G0Z



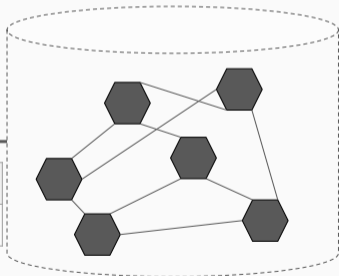
Label	Type	Value
bob	PKEY	7F5T

[www.bob.com](http://www.bob.com)?



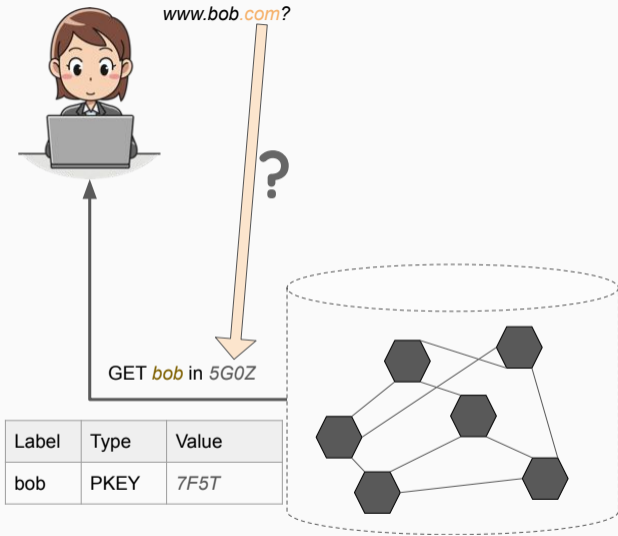
GET [www](http://www) in 7F5T

Label	Type	Value
www	A	1.2.3.4



**How do we bootstrap the top-level zones?**

---



# The GNU Name System Root

“Hyper-hyper local root” concept:

- Resolver ships with initial root zone configuration.
- Root zone configurable *locally* at *each* endpoint.
- User override/extension of root at top-level or subdomain-level for:
  - Circumvent censorship if necessary.
  - Private networks.

# Envisioned Governance Model

- Non-profit organization.
- Multi-stakeholder model: Board, supporting organizations, ...
- Examples for possible stakeholders:
  - Software and OS Distributors
  - Browser vendors
  - Governments
- Funding options:
  - Applications for new top-level domains.
  - Registrations of new top-level domains.
  - ...



**Quo Vadis?**

---

- In progress:
  - 2019-2020: Technical specification of GNS protocol, packaging and alternative implementations.<sup>5</sup>
  - Continuous development and integration into applications.
- 2020–: Establishment of governing body.

---

<sup>5</sup>Funded by NLnet under EU Next Generation Internet program (<https://nlnet.nl/project/GNS/>).

# The GNU Name System

`https://gnunet.org`

`schanzen@gnunet.org`

`3D11 063C 10F9 8D14 BD24 D147 0B09 98EF 86F5 9B6A`

## References

1. 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.
2. Martin Schanzenbach, Georg Bramm, Julian Schütte. *reclaimID: Secure, Self-Sovereign Identities Using Name Systems and Attribute-Based Encryption*. **17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom)**, 2018
3. Christian Grothoff, Martin Schanzenbach, Annett Laube, Emmanuel Benoist, Pascal Mainini. *Decentralized Authentication for Self-Sovereign Identities using Name Systems (DASEIN)*. <https://git.gnunet.org/bibliography.git/plain/docs/dasein10.pdf>, 2018.