GNU Name System: 2019 Edition

Christian Grothoff

Berner Fachhochschule
Technik und Informatik

IETF 104

"Developers of new name resolution systems that must work in existing contexts actually have no choice: they must use a Special-Use Domain Name to segregate a portion of the namespace for use with their system." –RFC 8244

Context

Applications in GNUnet (under development)

- Anonymous and non-anonymous publishing
- IPv6–IPv4 protocol translation and tunnelling
- **GNU Name System**: censorship-resistant replacement for DNS
- Conversation: secure, decentralized voice communication
- SecuShare: social networking
- GNU Taler: privacy-friendly payments
- ...

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.

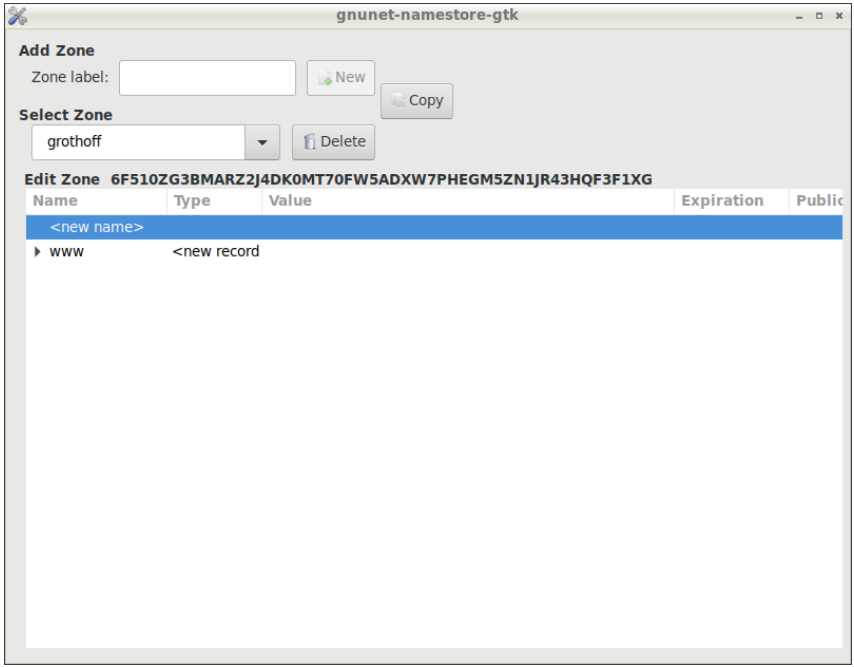
[1] DNS-over-TLS, DoH, DNSSEC, DPRIVE, ...

The GNU name system[2]

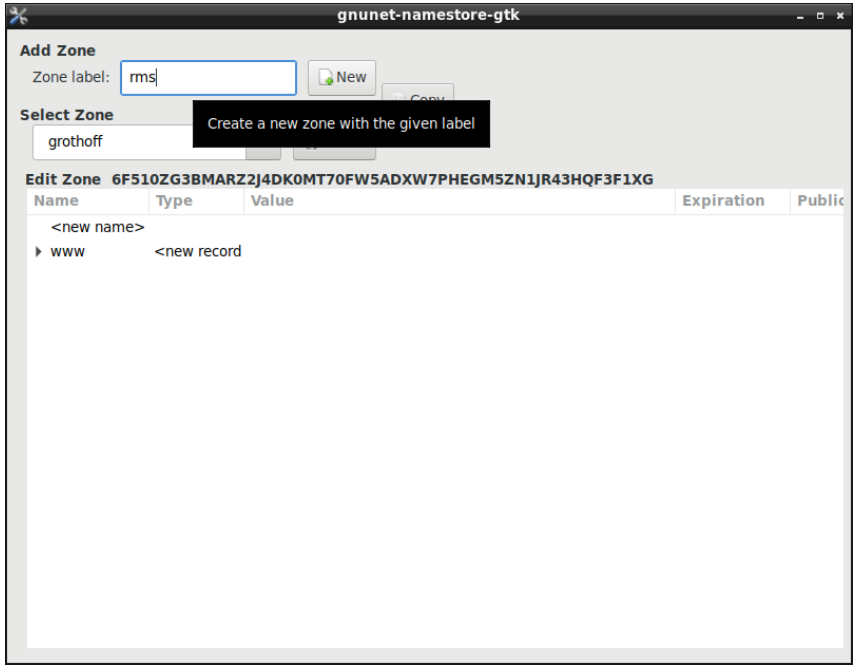
- Decentralized name system ⇒ Names are not global
- Supports globally unique (& secure) identification
- Achieves query and response privacy
- Provides public key infrastructure
- Interoperable with DNS

[2] Joint work with Martin Schanzenbach, Matthias Wachs and Patrick Gerber

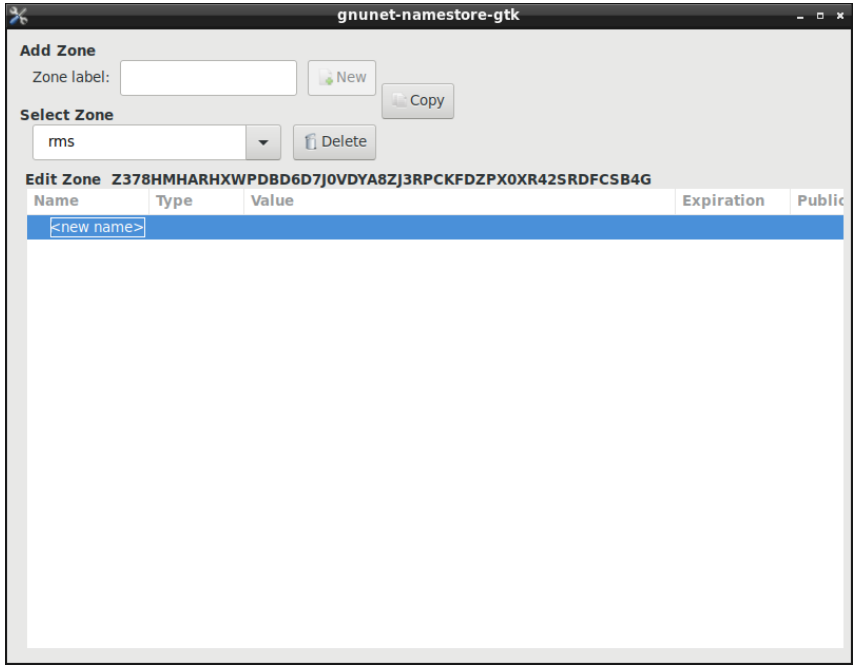
Zone management



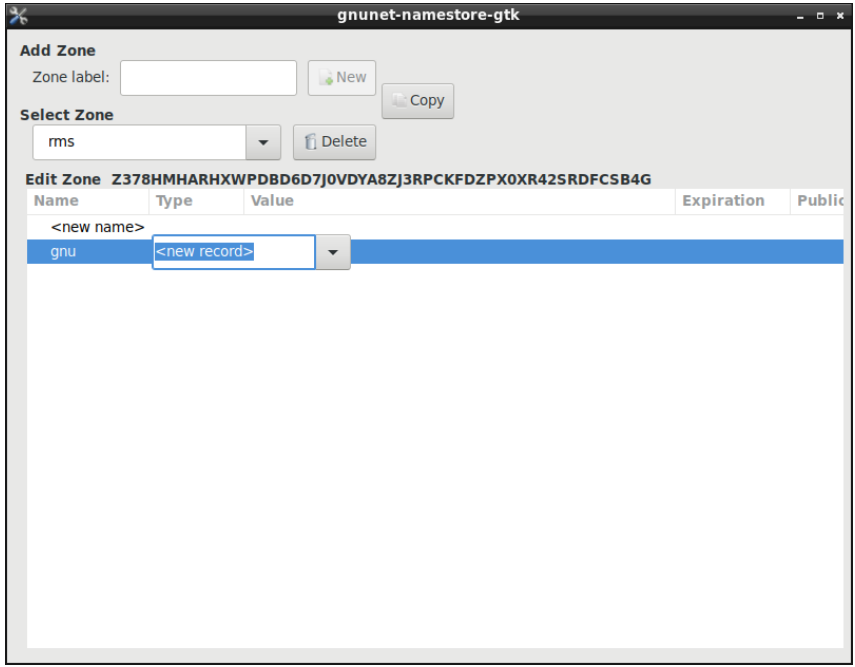
Zone management



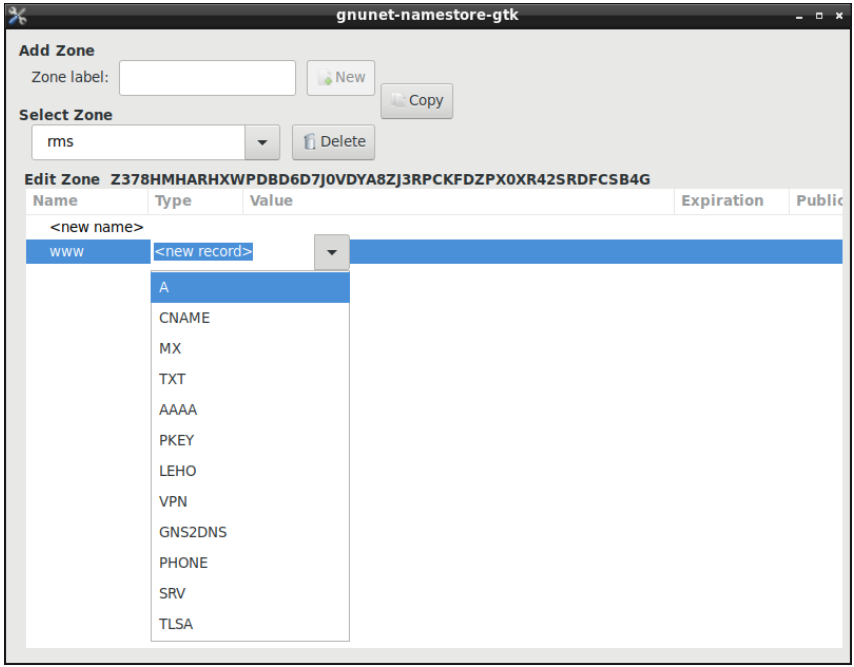
Zone management



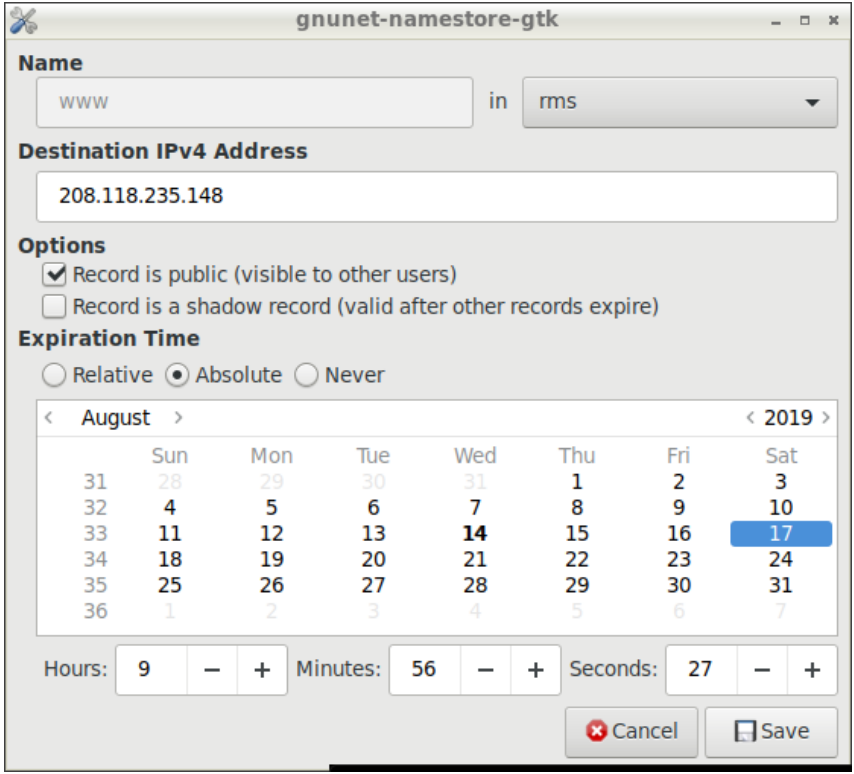
Zone management



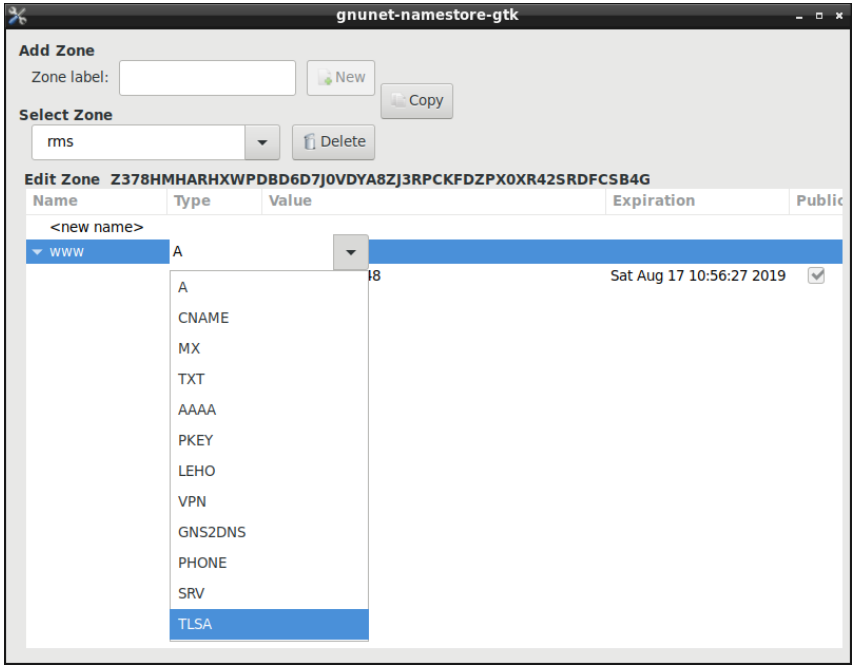
Zone management



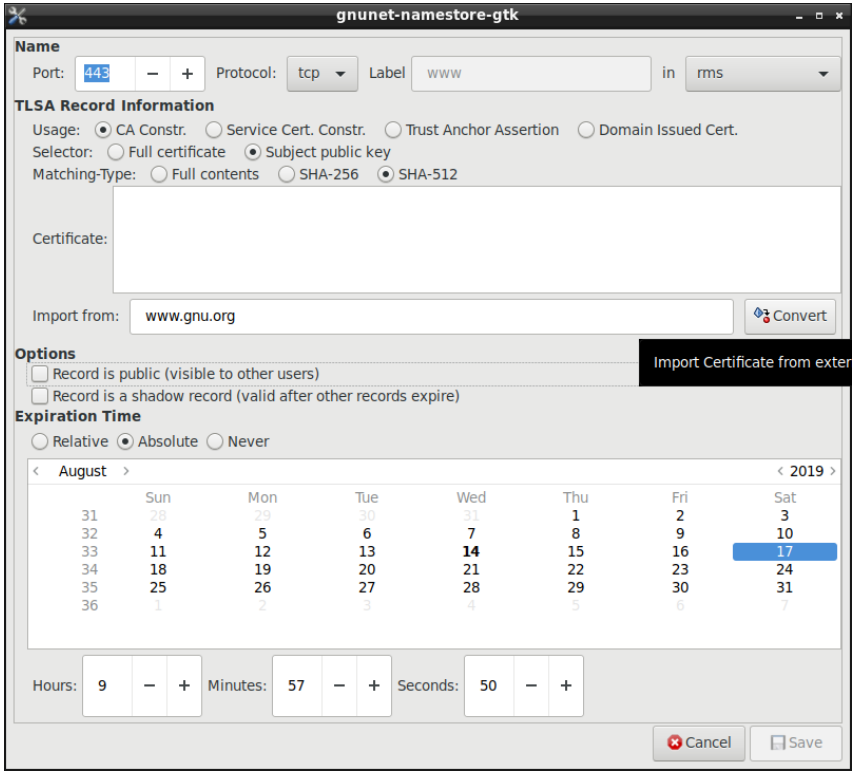
Zone management



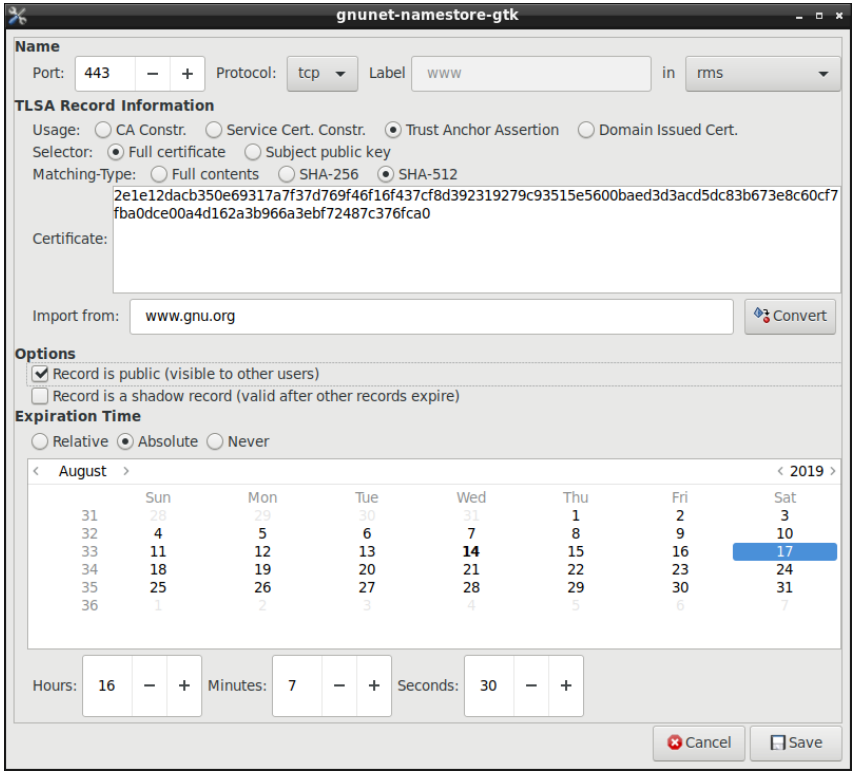
Zone management



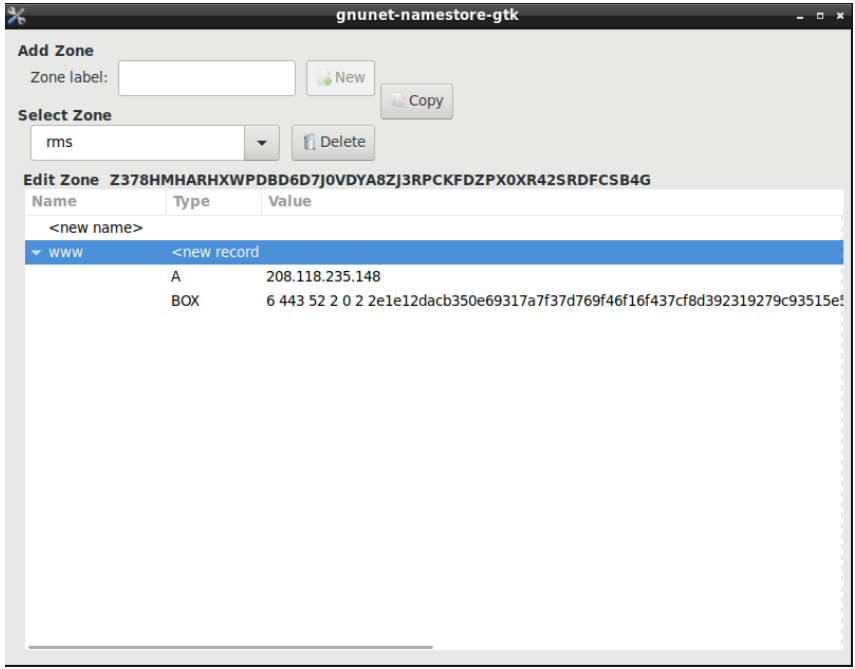
Zonenmanagement



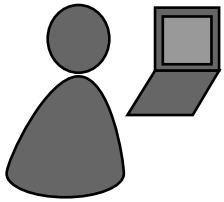
Zone management



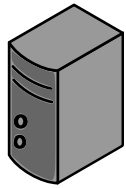
Zone management



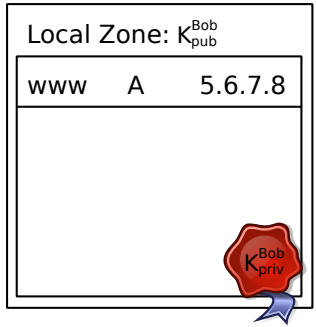
Name resolution in GNS



Bob

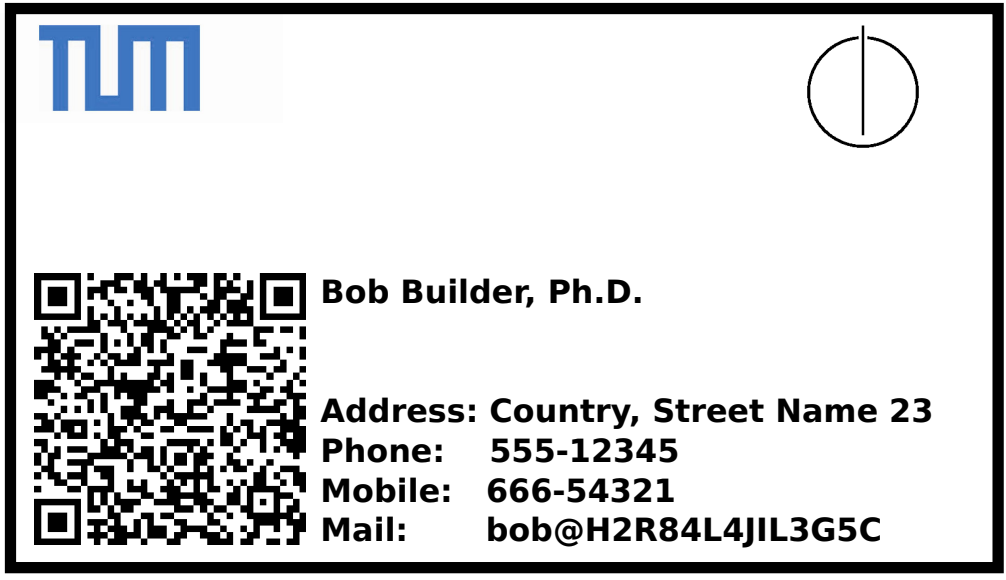


Bob's webserver



- Bob can now reach his Web server under **www.bob**

Secure Introduction

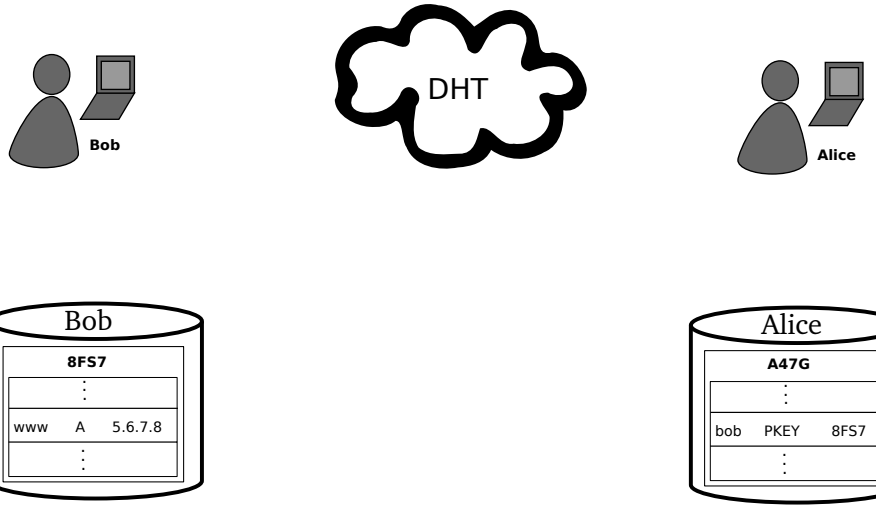


- Bob provides his public key to his **friends**, i.e. via QR code

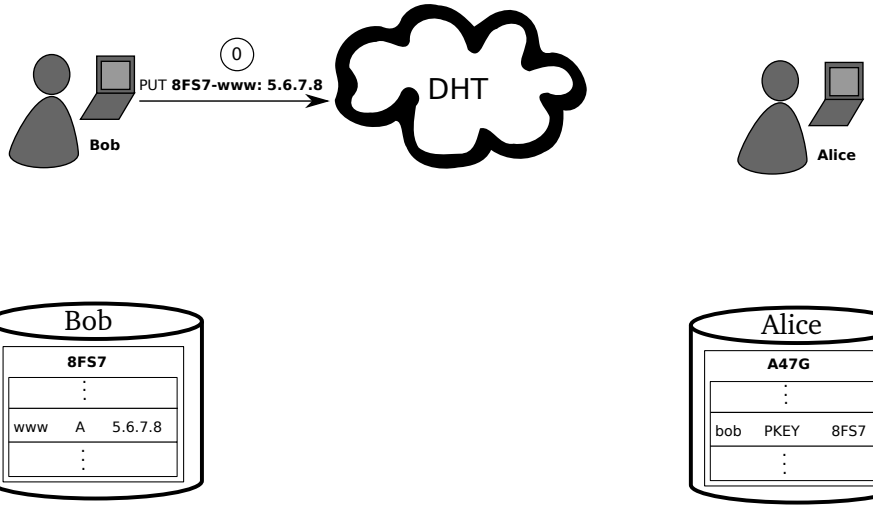
Delegation

- Alice learns Bob's "public" key
- Alice creates a delegation to zone K^{Bob}_{pub} under the label **bob**
- Alice can then reach Bob's Web server under **www.bob.alice**

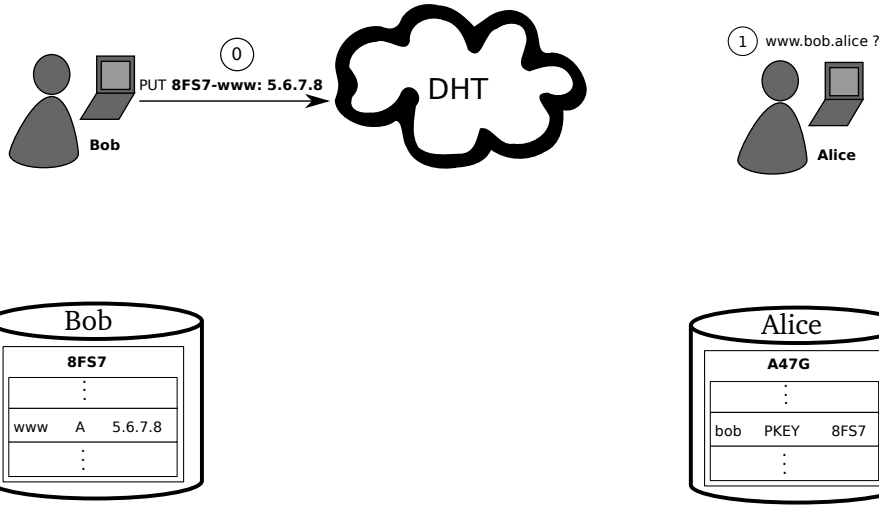
Name resolution



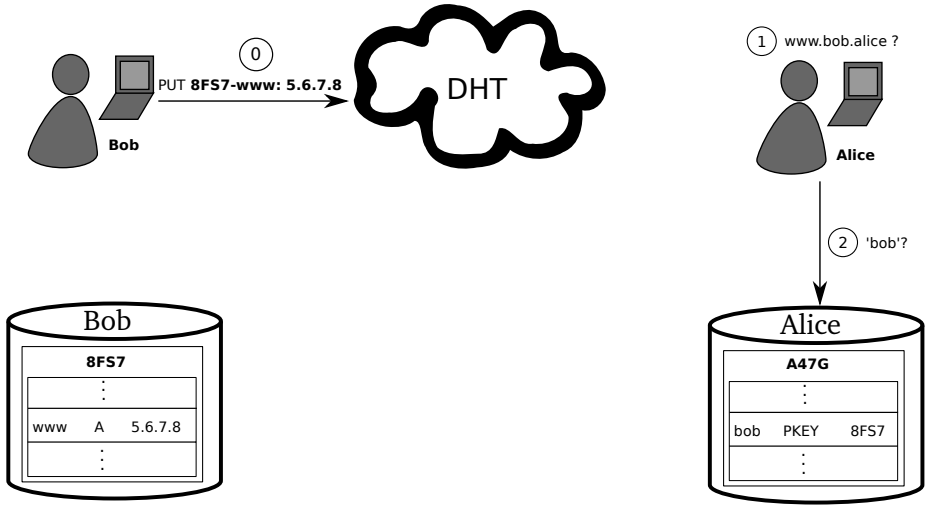
Name resolution



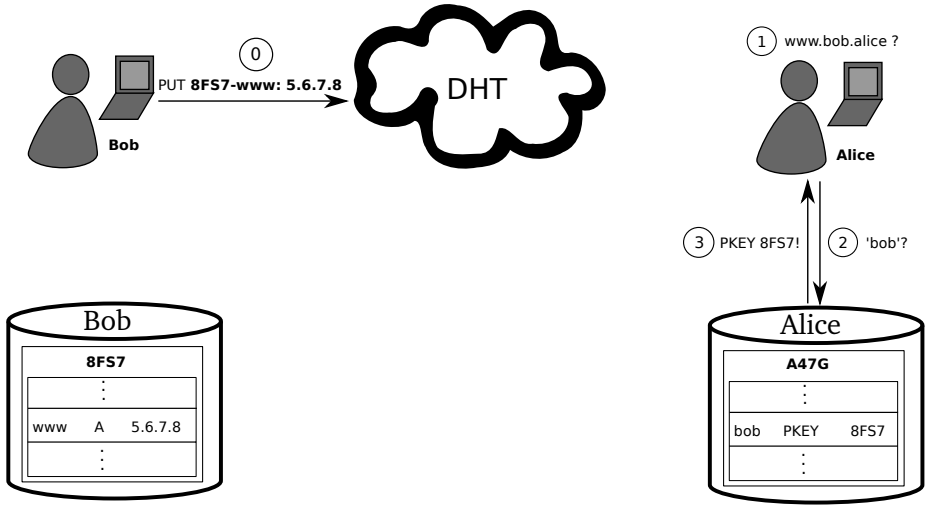
Name resolution



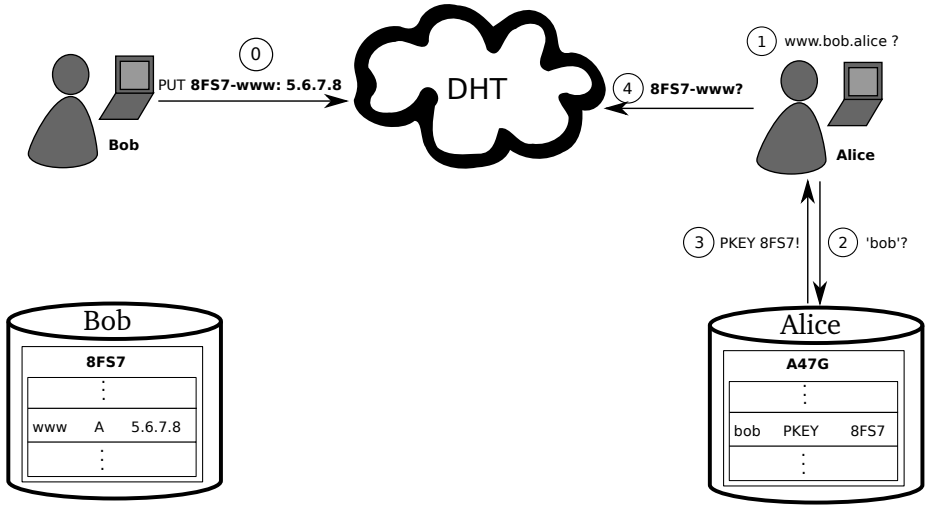
Name resolution



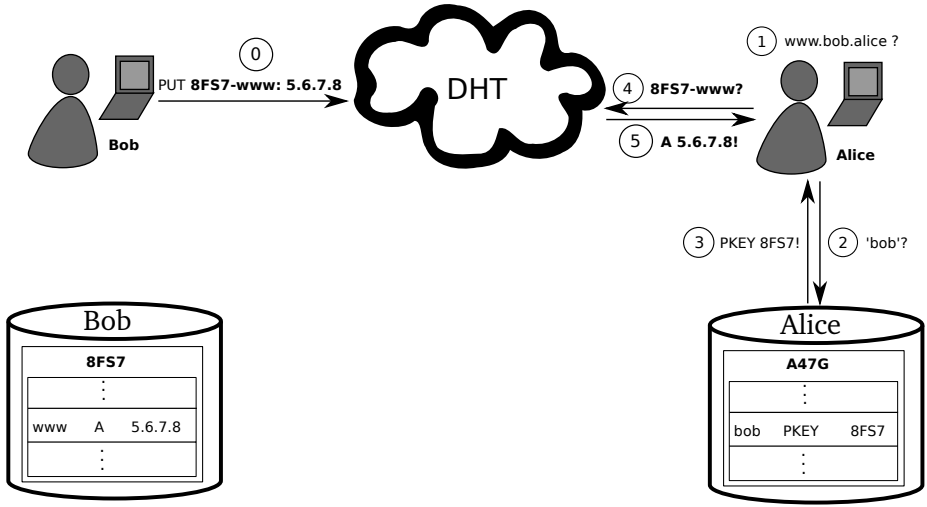
Name resolution



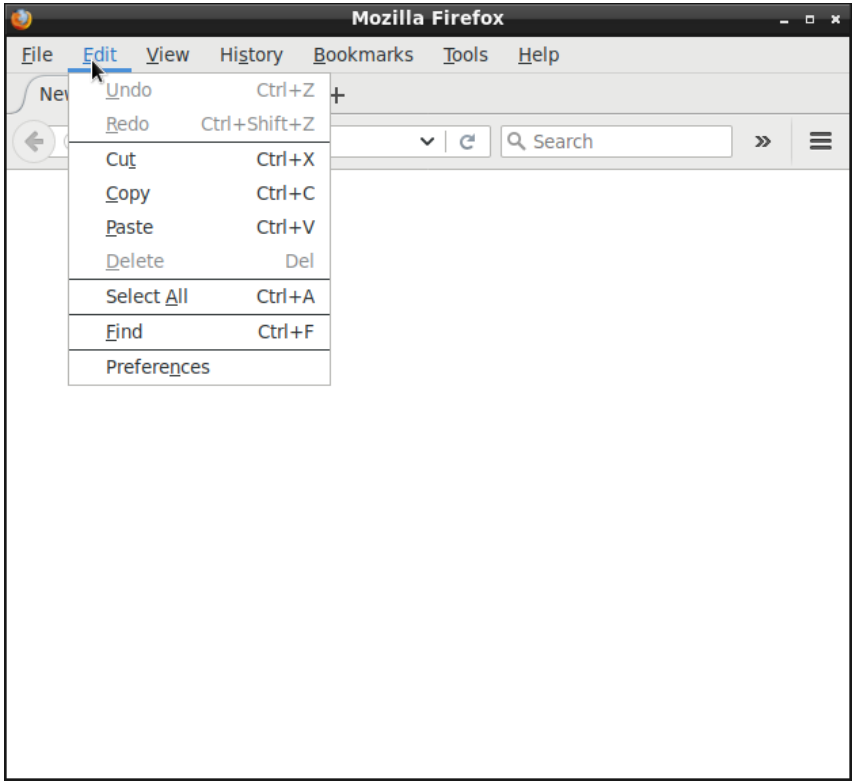
Name resolution



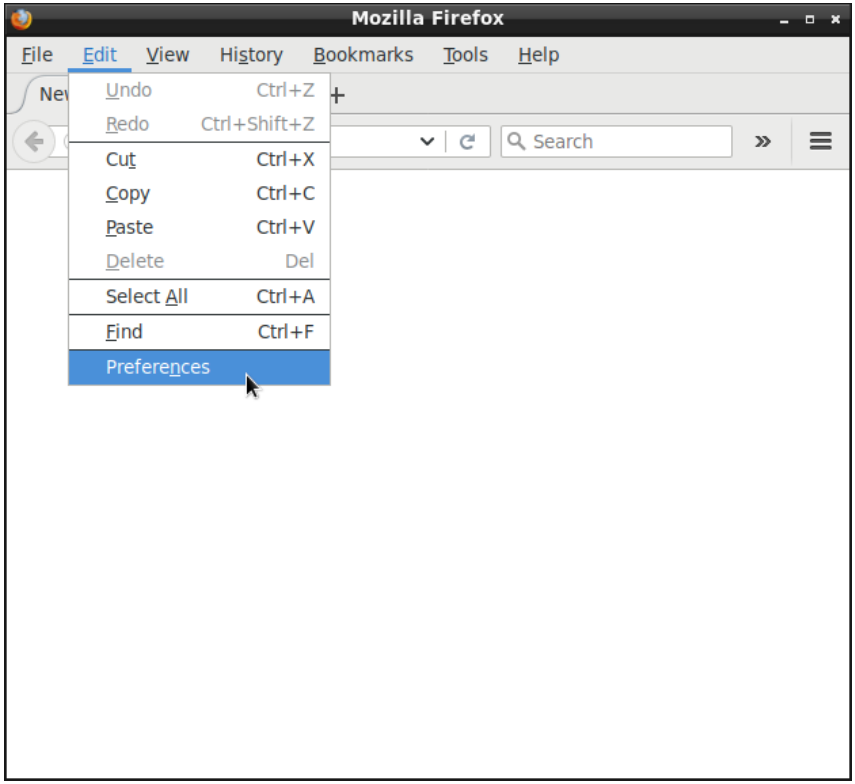
Name resolution



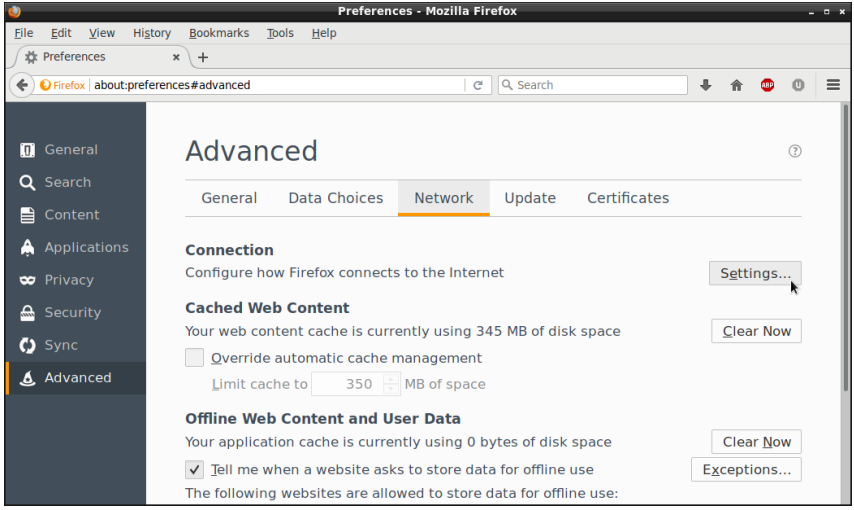
Browser Configuration



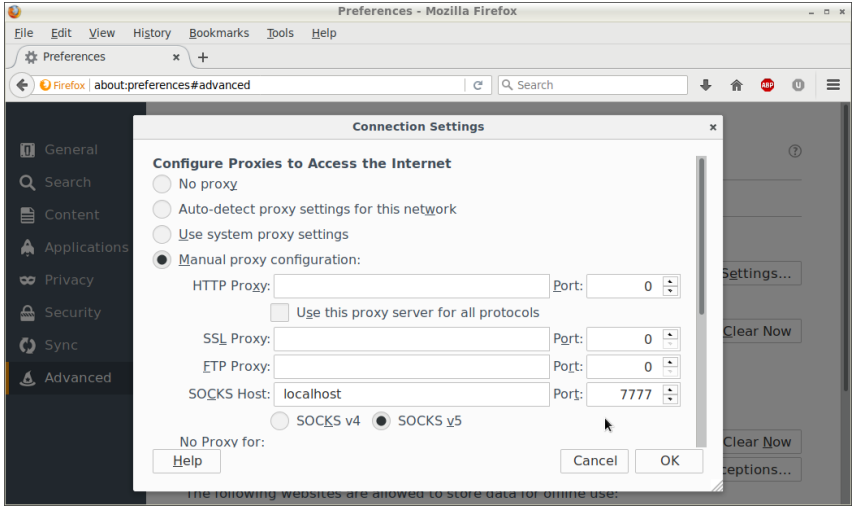
Browser Configuration



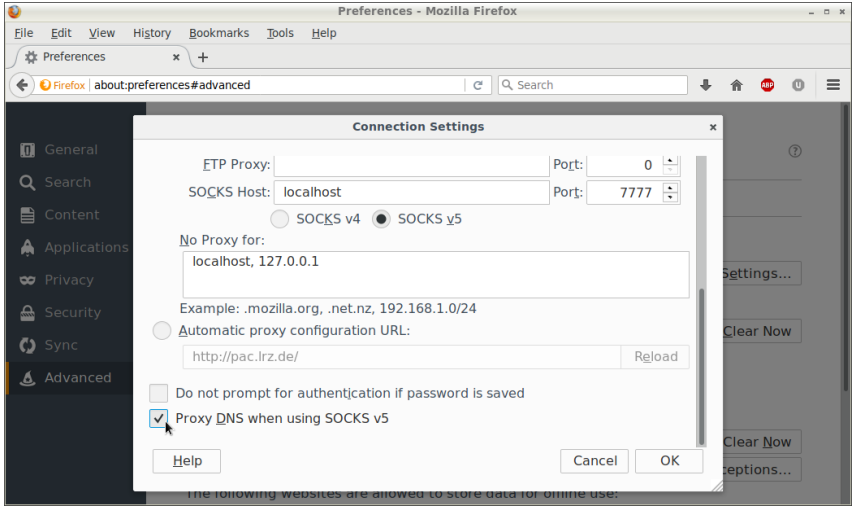
Browser Configuration



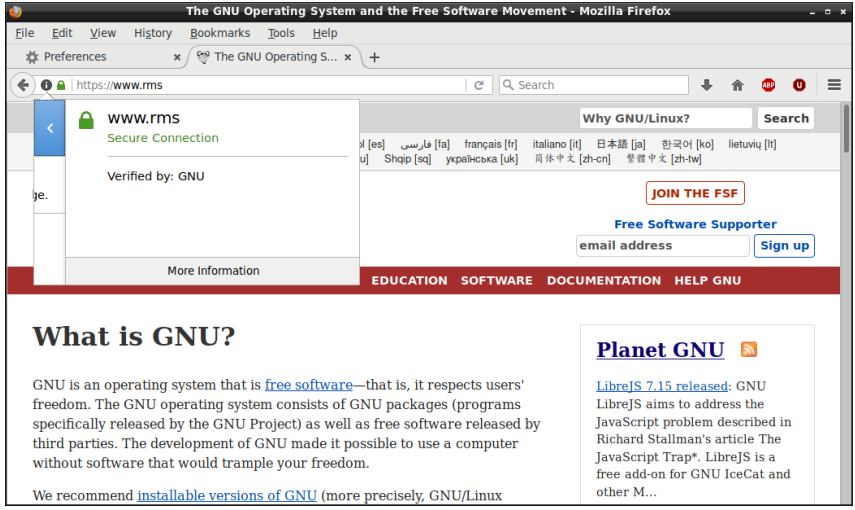
Browser Configuration



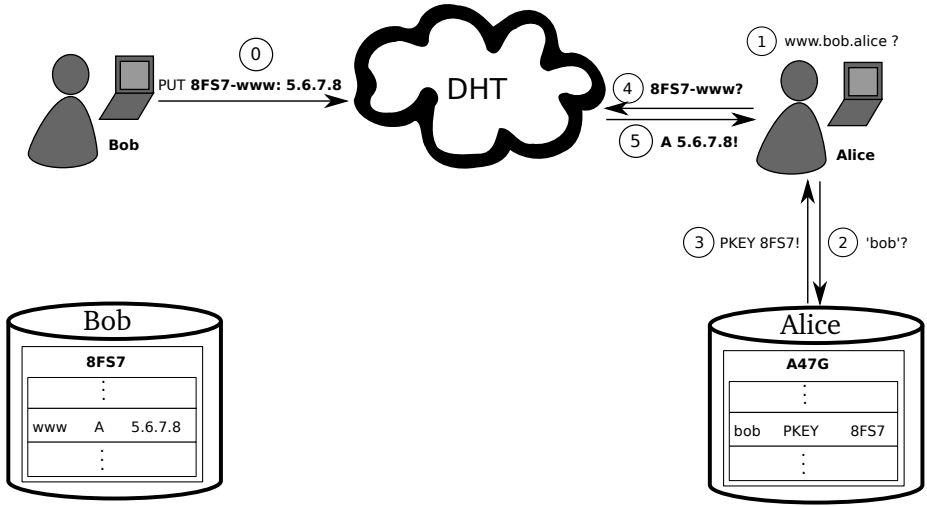
Browser Configuration



Browser Usage



Privacy issue: DHT



Query privacy: terminology

G	generator in ECC curve, a point
n	size of ECC group, $n := \|G\|$, n prime
x	private ECC key of zone ($x \in \mathbb{Z}_n$)
P	public key of zone, a point $P := xG$
l	label for record in a zone ($l \in \mathbb{Z}_n$)
$R_{P,l}$	set of records for label l in zone P
$q_{P,l}$	query hash (hash code for DHT lookup)
$B_{P,l}$	block with encrypted information for label l in zone P published in the DHT under $q_{P,l}$

Query privacy: cryptography

Publishing records $R_{P,l}$ as $B_{P,l}$ under key $q_{P,l}$

$$h := H(l, P) \tag{1}$$
$$d := h \cdot x \mod n \tag{2}$$
$$B_{P,l} := S_d(E_{HKDF(l,P)}(R_{P,l})), dG \tag{3}$$
$$q_{P,l} := H(dG) \tag{4}$$

Query privacy: cryptography

Publishing records $R_{P,l}$ as $B_{P,l}$ under key $q_{P,l}$

$$h := H(l, P) \tag{1}$$
$$d := h \cdot x \mod n \tag{2}$$
$$B_{P,l} := S_d(E_{HKDF(l,P)}(R_{P,l})), dG \tag{3}$$
$$q_{P,l} := H(dG) \tag{4}$$

Searching for records under label l in zone P

$$h := H(l, P) \tag{5}$$
$$q_{P,l} := H(hP) = H(hxG) = H(dG) \Rightarrow \texttt{obtain}\ \ B_{P,l} \tag{6}$$
$$R_{P,l} = D_{HKDF(l,P)}(B_{P,l}) \tag{7}$$

Globally unique identifiers

- Public keys are globally unique
- Users can use any public key (in a base32 encoding) as a TLD
- "alice.bob.*KEY*" is a valid, globally unique identifier

Key revocation

- Revocation message signed with private key (ECDSA)
- Flooded on all links in P2P overlay, stored forever
- Efficient set reconciliation used when peers connect
- Expensive proof-of-work used to limit DoS-potential
- Proof-of-work can be calculated ahead of time
- Revocation messages can be stored off-line if desired

Latest political developments

Originally, GNS used pTLD ".gnu" as protocol switch.
`draft-grothoff-iesg-special-use-p2p-names` tried to make this official following RFC 6761.

- IETF's `dnsop` refused to follow RFC 6761 for us, only Apple and Facebook have political power to get "free" TLDs (".local", ".onion")
- But, RFC 8244 (quote from slide 1) is wrong:

  Our latest release allows users to override *any* domain name
- Can override "ietf.org", or ".fr", or ".bob" by simply specifying a GNS public key for that domain in configuration:
  - Usability greatly improved (thank you, IETF)
  - Transparency reduced for users: usability study showed users cannot tell DNS vs. GNS
- `gnunet-dns2gns` is DNS proxy speaking DNS resolving some names via GNS

Latest techncial developments

- Demonstrated scaling of DHT implementation to deal with millions of records
- Implemented `gnunet-zoneimport` to import DNS records by single query (given list of names)
- Implemented Ascension to import DNS records via AXFR
- Imported ".fr" into GNS zone based on public name list and brute force zone transfer
- Imported ".se" and "bfh.ch" using AXFR

Conclusion and outlook

- The DNS monopoly is over.
- GNS is simpler than DNS: no glue, no NSEC3, no RRSIG
- GNS provides private name resolution and censorship resistance
- GNS does not require ICANN or a root zone or IANA special-use TLDs
- Operators should no longer be advised about ".gnu", but about name resolution protocol diversity *without* any signalling
- GNUnet will include *domain* $\rightarrow$ *public key* map in default configuration

  $\Rightarrow$ Donate just 130,000 EUR to GNUnet e.V. today to get yours![3]

[3] This is a special discount for `dnsop` members.

Questions?

More Information on the Web:

- `https://gnunet.org/gns`
- Slides will be published at `https://grothoff.org/christian/`.

> *"When governments fear the people, there is liberty. When the people fear the government, there is tyranny. The strongest reason for the people to retain the right to keep and bear arms is, as a last resort, to protect themselves against tyranny in government."*
>
> —*Thomas Jefferson*