

GNU Name System: 2019 Edition

Christian Grothoff



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 solutions¹ will **not** fix this.

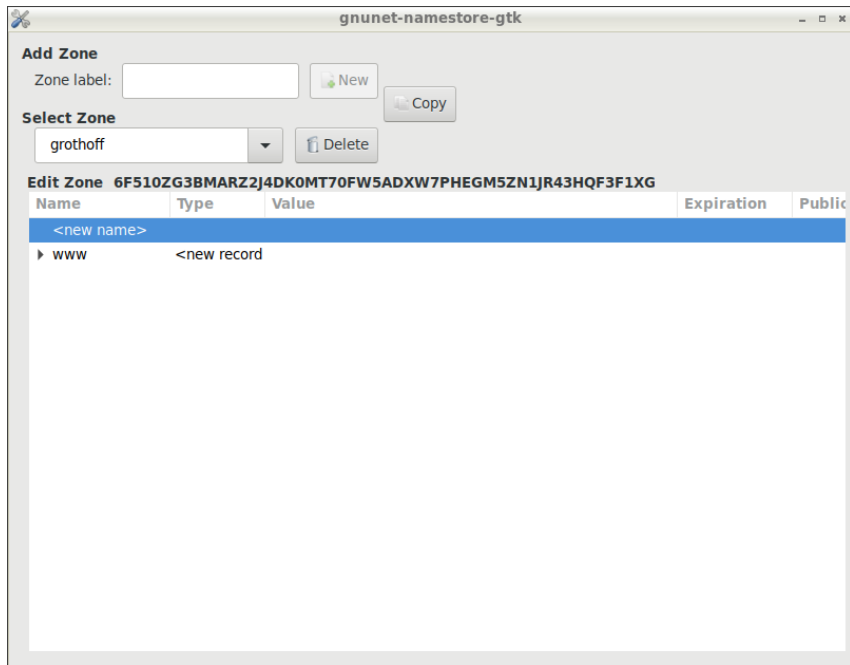
¹DNS-over-TLS, DoH, DNSSEC, DPRIVE, ...

The GNU name system²

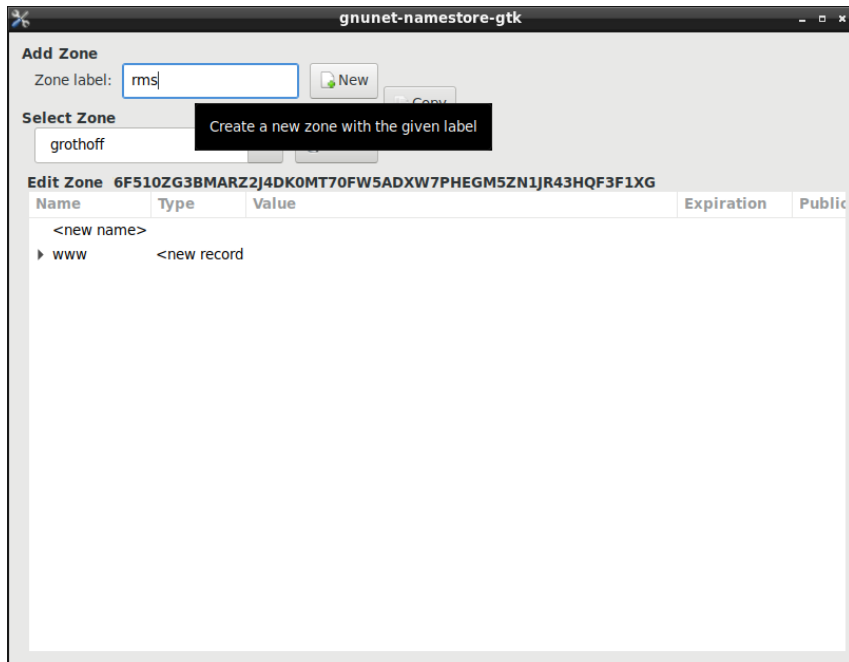
- ▶ Decentralized name system \Rightarrow Names are not global
- ▶ Supports globally unique (& secure) identification
- ▶ Achieves query and response privacy
- ▶ Provides public key infrastructure
- ▶ Interoperable with DNS

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

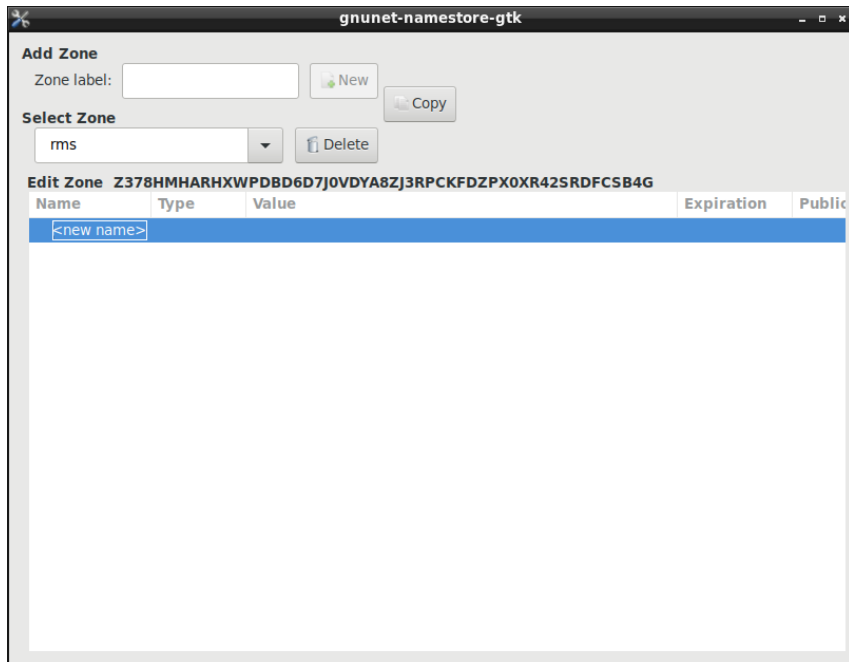
Zone management



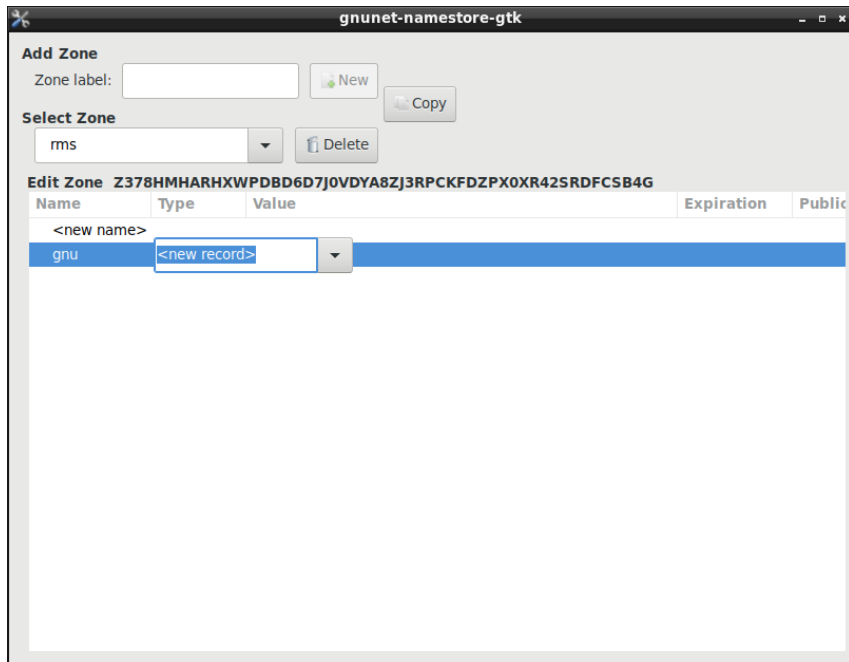
Zone management



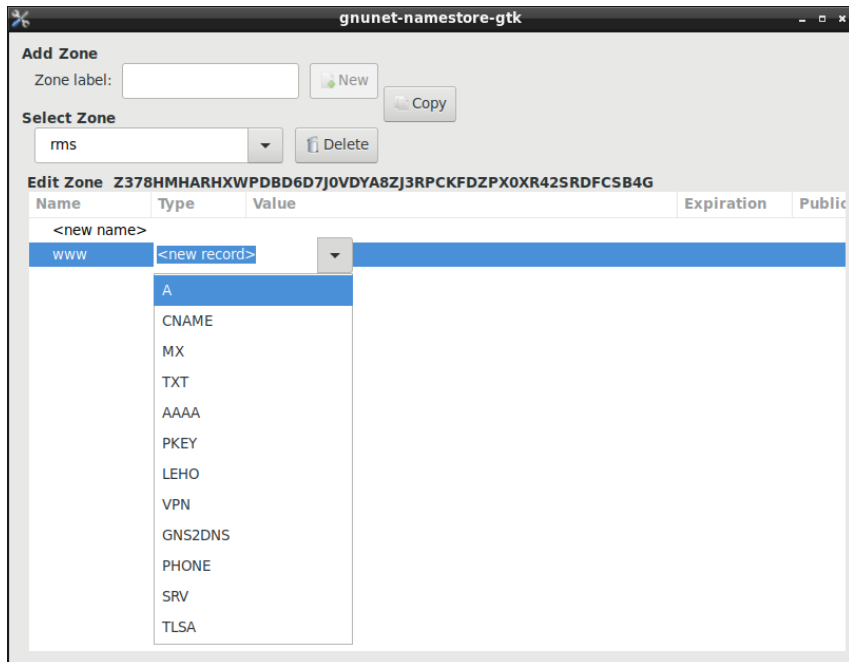
Zone management



Zone management



Zone management



Zone management

gnunet-namestore-gtk

Name

www in rms

Destination IPv4 Address

208.118.235.148

Options

Record is public (visible to other users)

Record is a shadow record (valid after other records expire)

Expiration Time

Relative Absolute Never

< August > < 2019 >

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	28	29	30	31	1	2	3
32	4	5	6	7	8	9	10
33	11	12	13	14	15	16	17
34	18	19	20	21	22	23	24
35	25	26	27	28	29	30	31
36	1	2	3	4	5	6	7

Hours: 9 - + Minutes: 56 - + Seconds: 27 - +

Cancel Save

Zone management

The screenshot shows the 'gnunet-namestore-gtk' application window. It has three main sections: 'Add Zone', 'Select Zone', and 'Edit Zone'.
1. 'Add Zone': A text input field for 'Zone label' is empty. To its right are 'New' and 'Copy' buttons.
2. 'Select Zone': A dropdown menu shows 'rms'. To its right is a 'Delete' button.
3. 'Edit Zone': The title is 'Edit Zone Z378HMHARHXWPDBD6D7J0VDYA8ZJ3RPCKFDZPX0XR42SRDFCSB4G'. Below it is a table with columns: Name, Type, Value, Expiration, and Public. The first row is expanded, showing a dropdown menu for the 'Name' column with the following options: <new name>, www, A, CNAME, MX, TXT, AAAA, PKEY, LEHO, VPN, GNS2DNS, PHONE, SRV, and TLSA. The 'www' row is highlighted in blue. The 'A' type is selected, and the 'Expiration' column shows 'Sat Aug 17 10:56:27 2019' with a checkmark in the 'Public' column.

Name	Type	Value	Expiration	Public
<new name>				
www	A		Sat Aug 17 10:56:27 2019	<input checked="" type="checkbox"/>

Zonenmanagement

gnunet-namestore-gtk

Name

Port: - + Protocol: tcp Label in

TLSA Record Information

Usage: CA Constr. Service Cert. Constr. Trust Anchor Assertion Domain Issued Cert.

Selector: Full certificate Subject public key

Matching-Type: Full contents SHA-256 SHA-512

Certificate:

Import from:

Options

Record is public (visible to other users)

Record is a shadow record (valid after other records expire)

Expiration Time

Relative Absolute Never

< August > < 2019 >

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	28	29	30	31	1	2	3
32	4	5	6	7	8	9	10
33	11	12	13	14	15	16	17
34	18	19	20	21	22	23	24
35	25	26	27	28	29	30	31
36	1	2	3	4	5	6	7

Hours: - + Minutes: - + Seconds: - +

Zone management

gnunet-namestore-gtk

Name
Port: 443 - + Protocol: tcp Label: www in rms

TLSA Record Information
Usage: CA Constr. Service Cert. Constr. Trust Anchor Assertion Domain Issued Cert.
Selector: Full certificate Subject public key
Matching-Type: Full contents SHA-256 SHA-512
Certificate:
2e1e12dacb350e69317a7f37d769f46f16f437cf8d392319279c93515e5600baed3d3acd5dc83b673e8c60cf7fba0dce00a4d162a3b966a3ebf72487c376fca0

Certificate:

Import from: www.gnu.org

Options
 Record is public (visible to other users)
 Record is a shadow record (valid after other records expire)

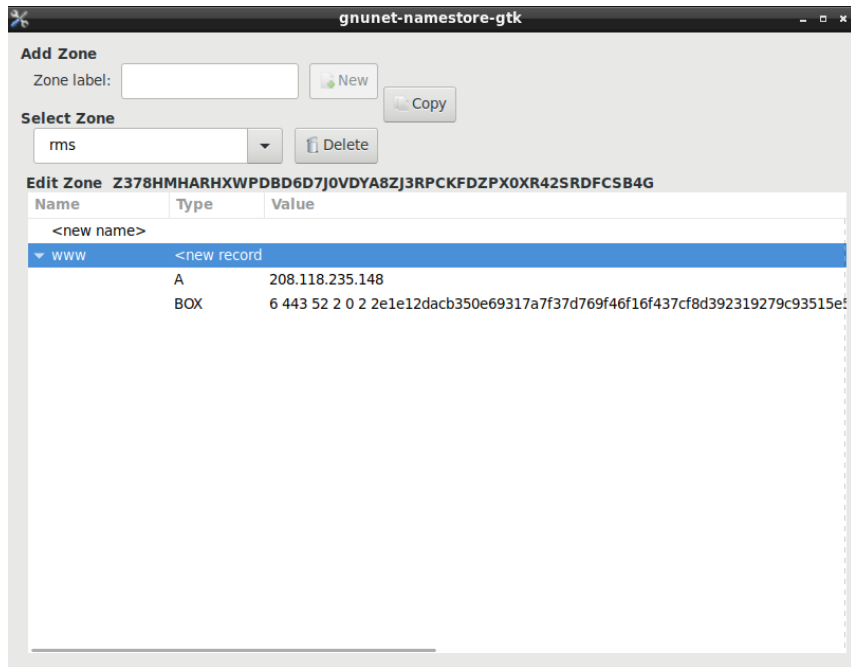
Expiration Time
 Relative Absolute Never

< August > < 2019 >

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	28	29	30	31	1	2	3
32	4	5	6	7	8	9	10
33	11	12	13	14	15	16	17
34	18	19	20	21	22	23	24
35	25	26	27	28	29	30	31
36	1	2	3	4	5	6	7

Hours: 16 - + Minutes: 7 - + Seconds: 30 - +

Zone management



The screenshot shows the 'gnunet-namestore-gtk' application window. It has three main sections: 'Add Zone', 'Select Zone', and 'Edit Zone'. The 'Add Zone' section has a 'Zone label:' text box, a 'New' button, and a 'Copy' button. The 'Select Zone' section has a dropdown menu showing 'rms' and a 'Delete' button. The 'Edit Zone' section is titled 'Edit Zone Z378HMHARHXWPDBD6D7J0VDYA8ZJ3RPCKFDZPX0XR42SRDFCSB4G' and contains a table with columns 'Name', 'Type', and 'Value'. The table has three rows: a header row with '<new name>', a row with 'www' (expanded) and '<new record>', and a row with 'A' and '208.118.235.148'. Below that is a row with 'BOX' and a long alphanumeric string.

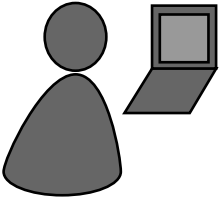
Add Zone
Zone label:

Select Zone

Edit Zone Z378HMHARHXWPDBD6D7J0VDYA8ZJ3RPCKFDZPX0XR42SRDFCSB4G

Name	Type	Value
<new name>		
▼ www	<new record>	
	A	208.118.235.148
	BOX	6 443 52 2 0 2 2e1e12dacb350e69317a7f37d769f46f16f437cf8d392319279c93515e5

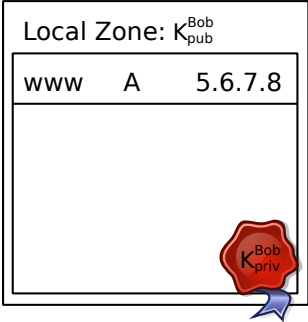
Name resolution in GNS



Bob



Bob's webserver



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



TUM



Bob Builder, Ph.D.

Address: Country, Street Name 23

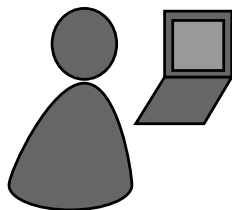
Phone: 555-12345

Mobile: 666-54321

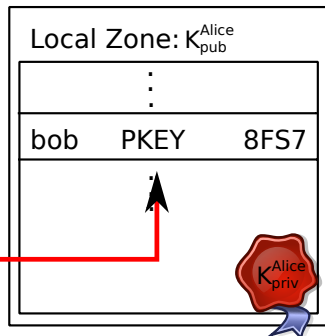
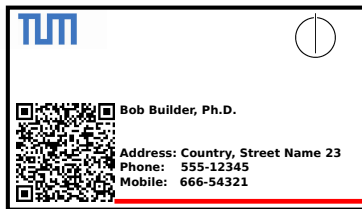
Mail: bob@H2R84L4JIL3G5C

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

Delegation

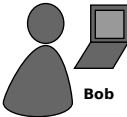


Alice



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

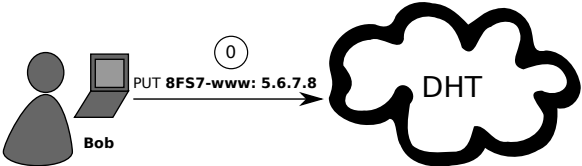
Name resolution



Bob			
8FS7			
⋮			
www	A	5.6.7.8	
⋮			

Alice		
A47G		
⋮		
bob	PKEY	8FS7
⋮		

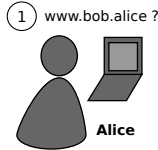
Name resolution



Bob		
8F57		
⋮		
www	A	5.6.7.8
⋮		

Alice		
A47G		
⋮		
bob	PKEY	8F57
⋮		

Name resolution



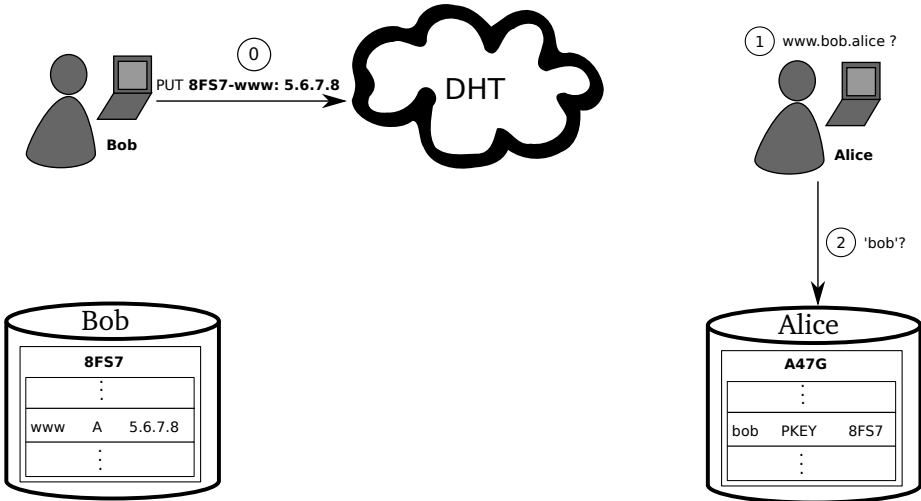
Bob

8F57		
⋮		
www	A	5.6.7.8
⋮		

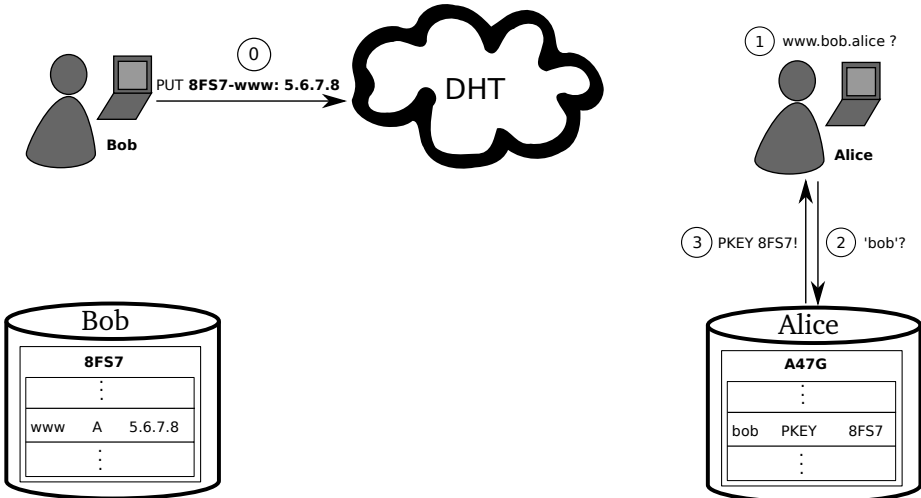
Alice

A47G		
⋮		
bob	PKEY	8F57
⋮		

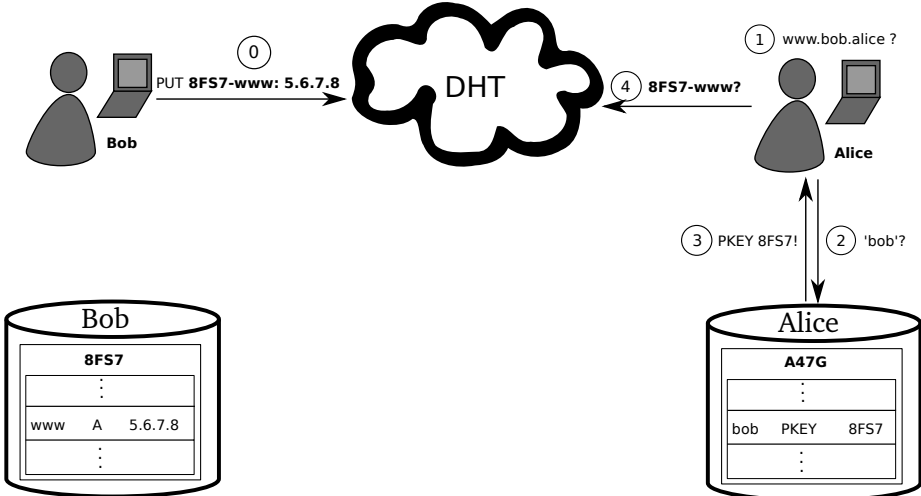
Name resolution



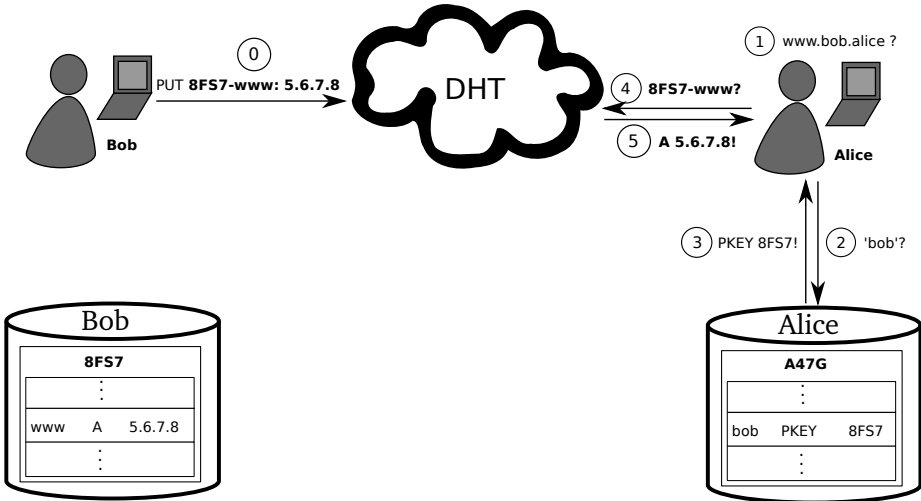
Name resolution



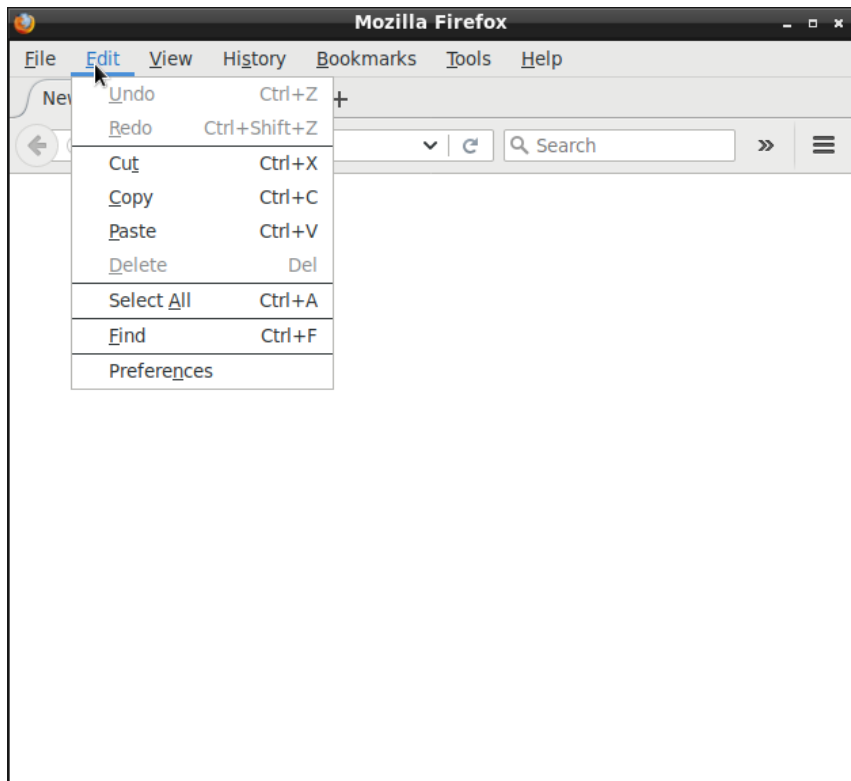
Name resolution



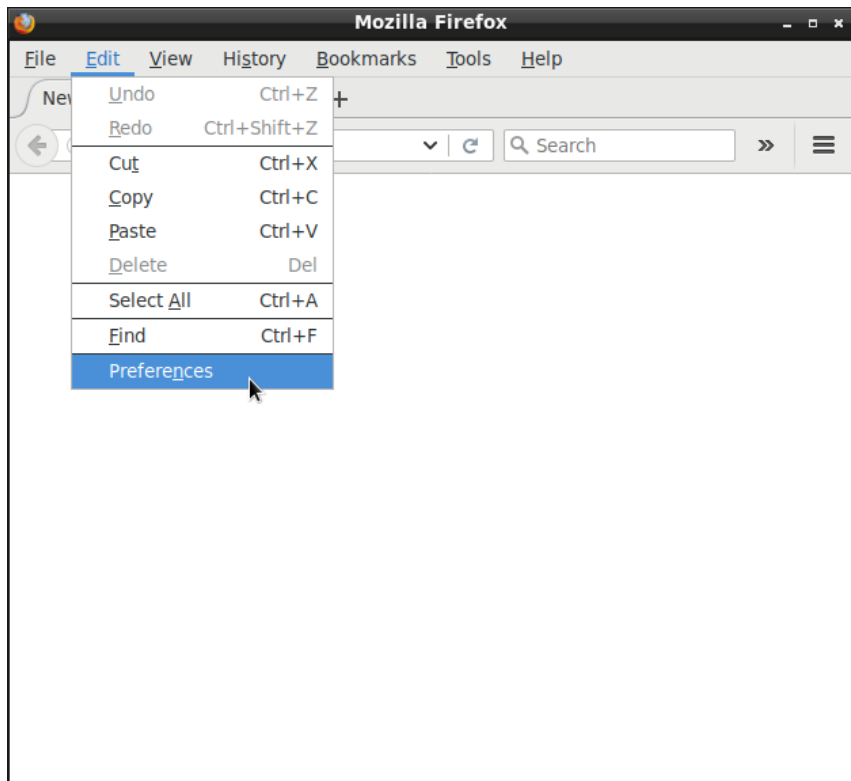
Name resolution



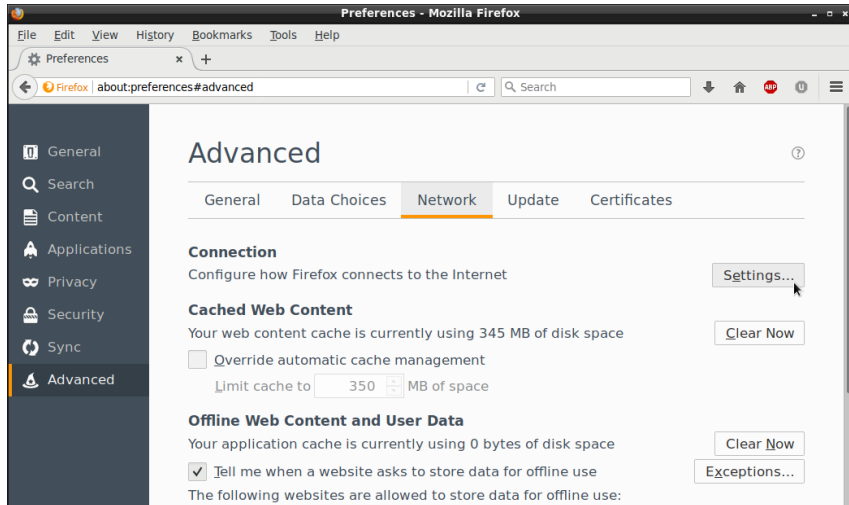
Browser Configuration



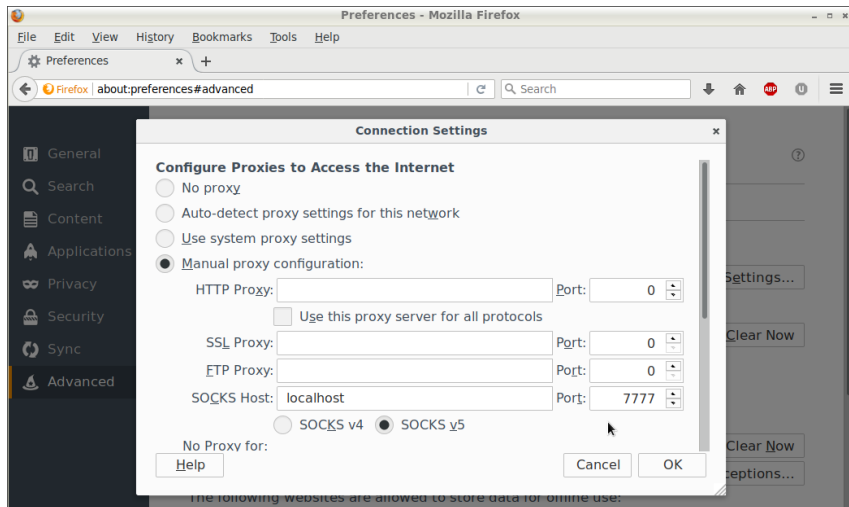
Browser Configuration



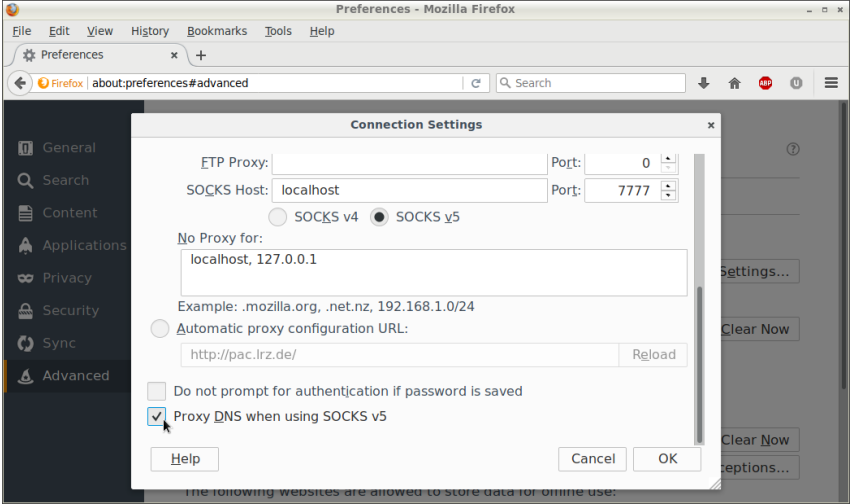
Browser Configuration



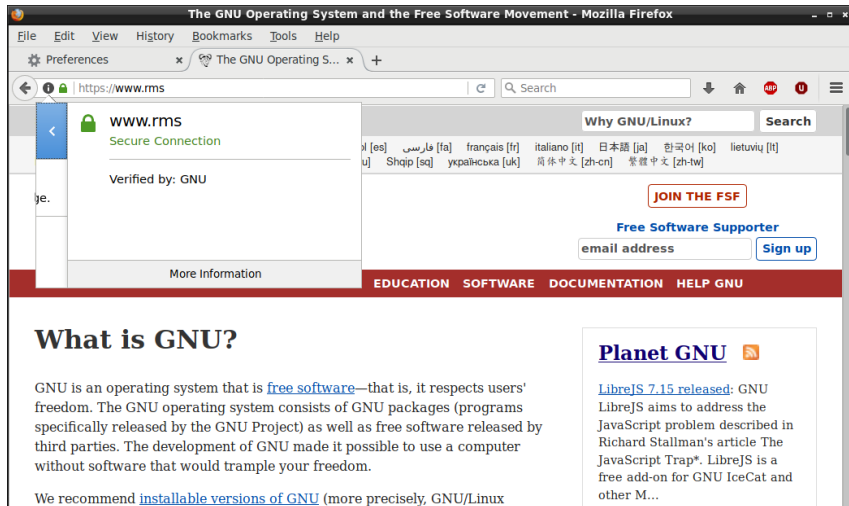
Browser Configuration



Browser Configuration



Browser Usage



The screenshot shows a Mozilla Firefox browser window titled "The GNU Operating System and the Free Software Movement - Mozilla Firefox". The address bar shows "https://www.rms". A security warning overlay is visible on the left side of the page, indicating a "Secure Connection" and "Verified by: GNU". The main content area features a search bar with the text "Why GNU/Linux?", a "JOIN THE FSF" button, and a "Free Software Supporter" section with an "email address" input field and a "Sign up" button. A navigation bar at the bottom contains links for "EDUCATION", "SOFTWARE", "DOCUMENTATION", and "HELP GNU". The main heading is "What is GNU?" followed by a paragraph explaining GNU as a free software operating system. A sidebar on the right contains a "Planet GNU" section with a link to "LibreJS 7.15 released: GNU LibreJS aims to address the JavaScript problem described in Richard Stallman's article The JavaScript Trap".

What is GNU?

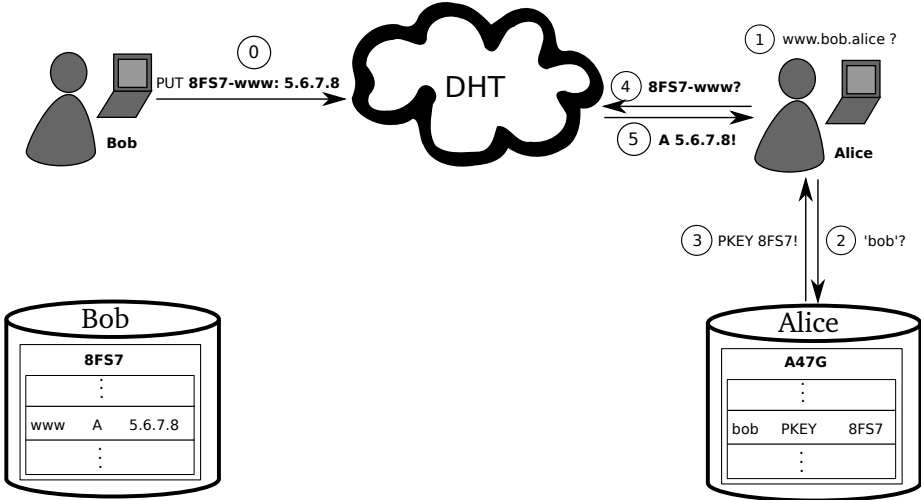
GNU is an operating system that is [free software](#)—that is, it respects users' freedom. The GNU operating system consists of GNU packages (programs specifically released by the GNU Project) as well as free software released by third parties. The development of GNU made it possible to use a computer without software that would trample your freedom.

We recommend [installable versions of GNU](#) (more precisely, GNU/Linux

Planet GNU

[LibreJS 7.15 released](#): GNU LibreJS aims to address the JavaScript problem described in Richard Stallman's article The JavaScript Trap*. LibreJS is a free add-on for GNU IceCat and other M...

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 $q_{P,l}$

$$h := H(l, P) \tag{1}$$

$$d := h \cdot x \pmod n \tag{2}$$

$$B_{P,l} := S_d(E_{HKDF(l,P)}(R_{P,l})), dG \tag{3}$$

$$q_{P,l} := H(dG) \tag{4}$$

Query privacy: cryptography

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

$$h := H(l, P) \tag{1}$$

$$d := h \cdot x \pmod n \tag{2}$$

$$B_{P,l} := S_d(E_{HKDF(l,P)}(R_{P,l})), dG \tag{3}$$

$$q_{P,l} := H(dG) \tag{4}$$

Searching for records under label l in zone P

$$h := H(l, P) \tag{5}$$

$$q_{P,l} := H(hP) = H(hxG) = H(dG) \Rightarrow \text{obtain } B_{P,l} \tag{6}$$

$$R_{P,l} = D_{HKDF(l,P)}(B_{P,l}) \tag{7}$$

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 technical 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* → *public key* map in default configuration
⇒ Donate just 130,000 EUR to GNUnet e.V. today to get yours!³

³This 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