

Decentralized Public Key Infrastructures

Christian Grothoff

Berner Fachhochschule

11.6.2021

Learning Objectives

The GNU Name System

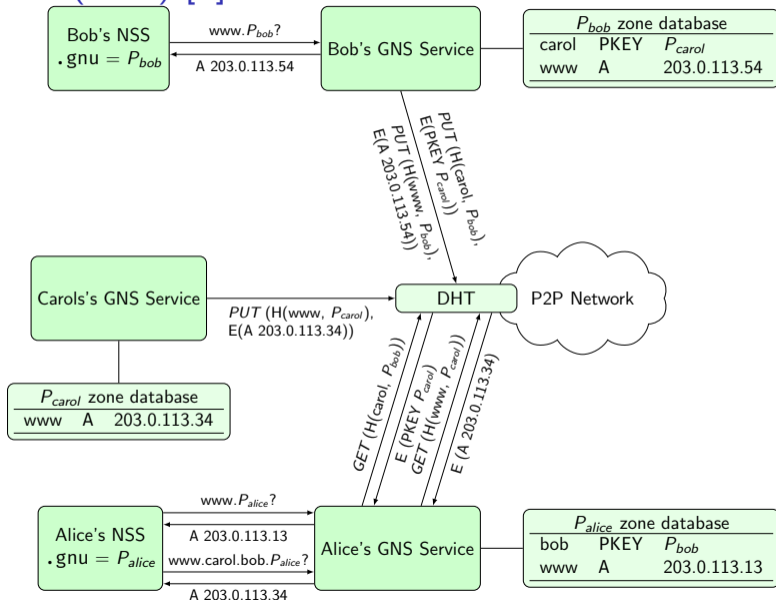
Private Information Retrieval

Comparisson of Name Systems

Introduction to GNUnet

References

The GNU Name System (GNS) [?]



The GNU Name System¹

Properties of GNS

- ▶ Decentralized name system with secure memorable names
- ▶ Delegation used to achieve transitivity
- ▶ Also supports globally unique, secure identifiers
- ▶ Achieves query and response privacy
- ▶ Provides alternative public key infrastructure
- ▶ Interoperable with DNS

¹Joint work with Martin Schanzenbach and Matthias Wachs

Zone Management: like in DNS

The screenshot shows the 'gnunet-setup' application window. The 'GNS' tab is active, displaying the configuration for editing a zone named 'API5QDP7A126P06VV60535PDT50B9L12NK6QP64IE8KNC6E807G0'. The preferred zone name is 'schanzen'. The 'Master Zone' radio button is selected. A table lists DNS records for the zone, including MX, PKEY, LEHO, AAAA, and A records. A QR code and a 'Save As' button are also visible.


gnunet-setup

General Network Transports File Sharing Namestore **GNS**

Editing zone API5QDP7A126P06VV60535PDT50B9L12NK6QP64IE8KNC6E807G0 Copy

Preferred zone name (PSEU):

Master Zone Private Zone Shorten Zone

 Save As

Name	Type	Value	Expiration	Public
<new name>				
+ +	<new record>			
	MX	5,mail.+	end of time	<input checked="" type="checkbox"/>
priv	<new record>			
	PKEY	3IQT1G601GUBVOS5C0JO87OEFB8N3DBJQ4L9SBI8PFLR8UKCVGHG	end of time	<input type="checkbox"/>
heise	<new record>			
	LEHO	heise.de	end of time	<input checked="" type="checkbox"/>
	AAAA	2a02:2e0:3fe:100::8	end of time	<input checked="" type="checkbox"/>
	A	193.99.144.80	end of time	<input checked="" type="checkbox"/>
home	<new record>			
大学	<new record>			
short	<new record>			
mail	<new record>			
homepage	<new record>			
fdfs	<new record>			
www	<new record>			

[Welcome to gnunet-setup.](#)



Bob Builder, Ph.D.

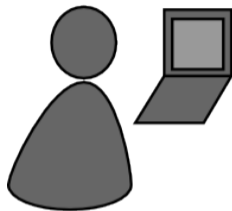
Address: Country, Street Name 23

Phone: 555-12345

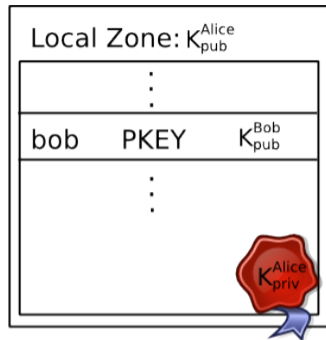
Mobile: 666-54321

Mail: bob@H2R84L4JIL3G5C.zkey

Delegation

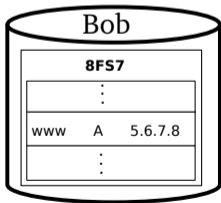
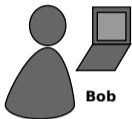


Alice

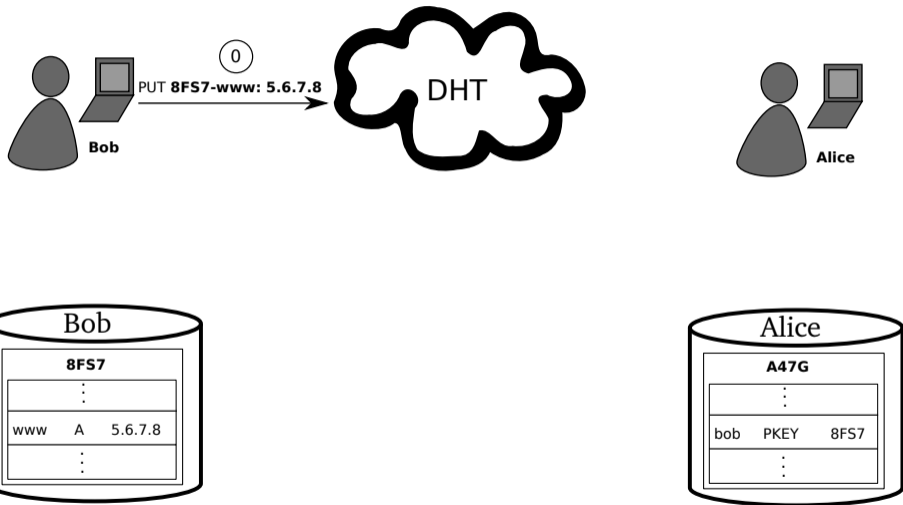


- ▶ Alice learns Bob's public key
- ▶ Alice creates delegation to zone K_{pub}^{Bob} under label **bob**
- ▶ Alice can reach Bob's webserver via **www.bob.gnu**

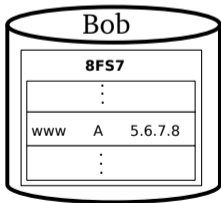
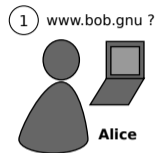
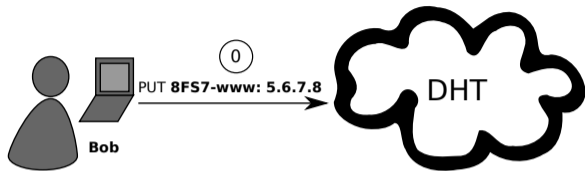
Name Resolution



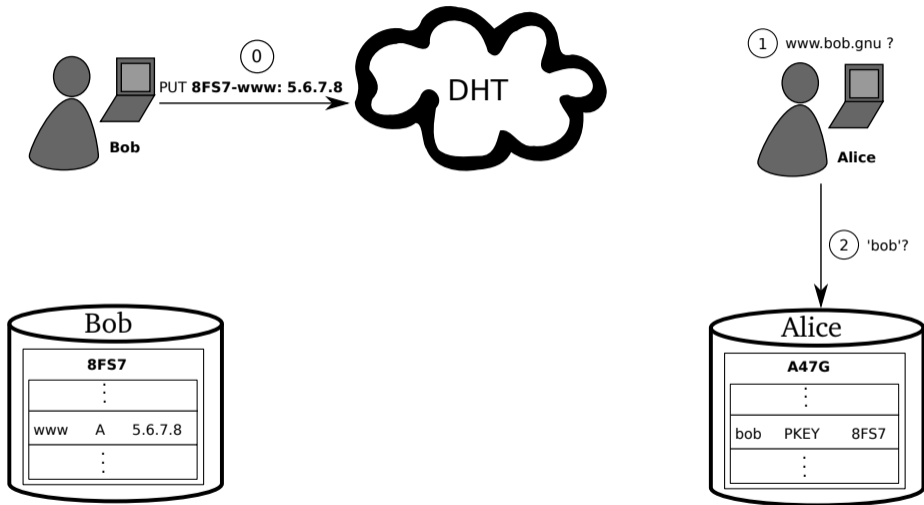
Name Resolution



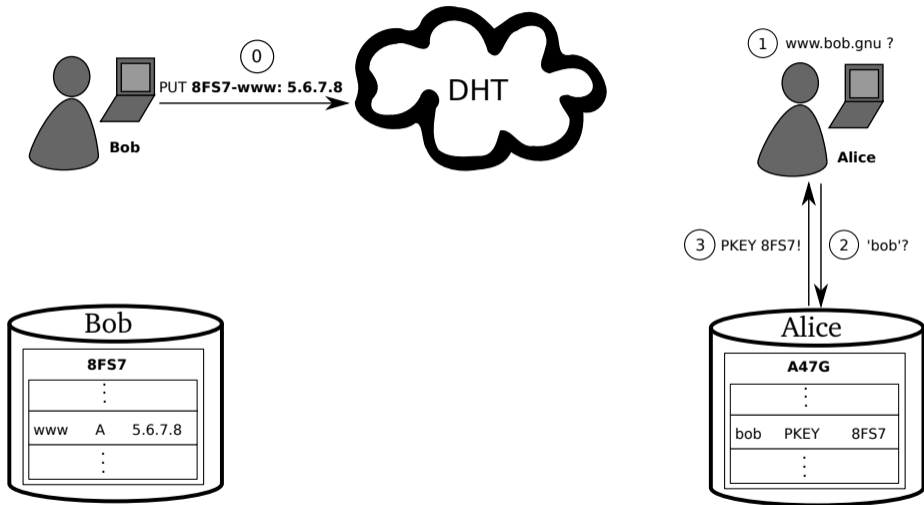
Name Resolution



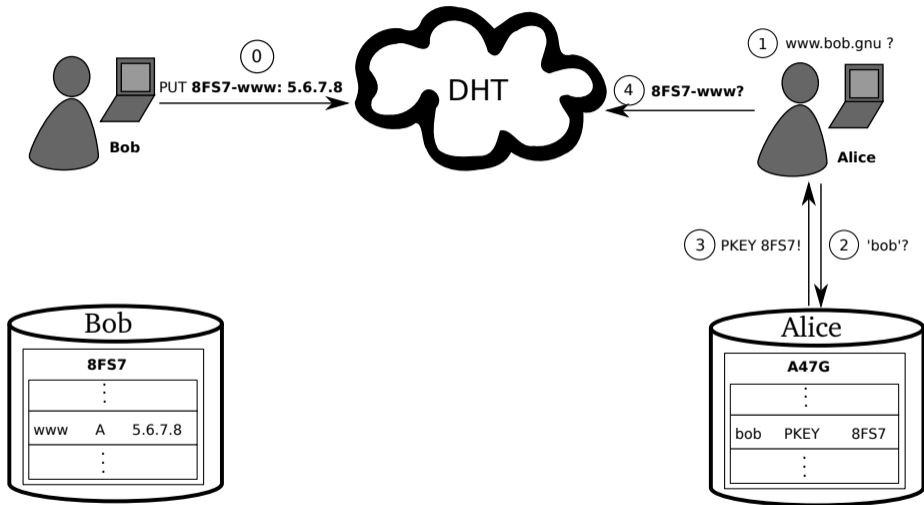
Name Resolution



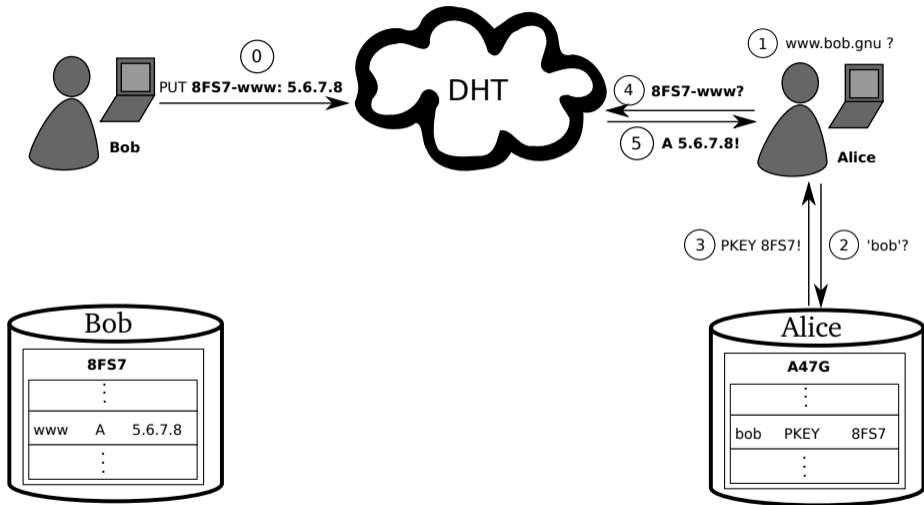
Name Resolution



Name Resolution



Name Resolution



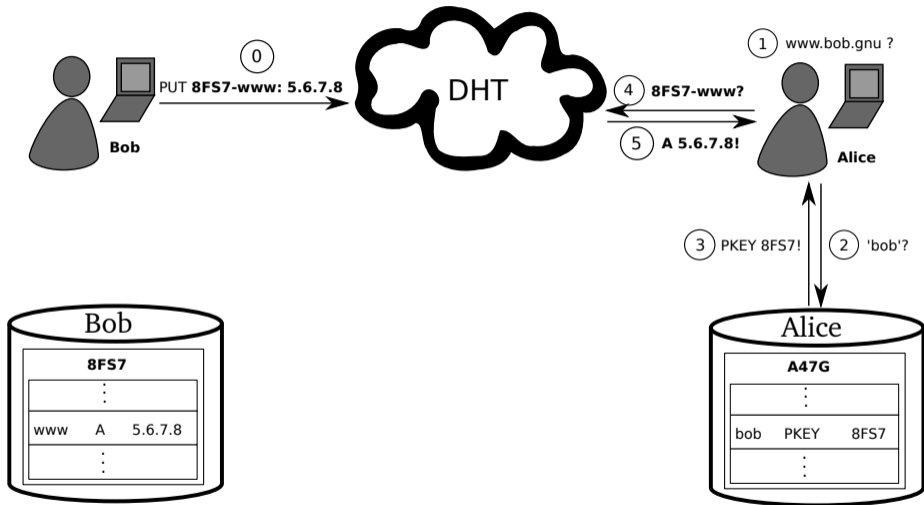
GNS as PKI (via DANE/TLSA)

The screenshot shows a web browser window with the address bar displaying <https://freedom.gnu>. A security warning dialog box is open, titled "freedom.gnu" with a sub-header "Identity verified". The dialog has two tabs: "Permissions" and "Connection". The "Connection" tab is active, showing a green lock icon and the text: "The identity of this website has been verified by GNS CA." Below this is a link for "Certificate Information". Another section shows a green lock icon and text: "Your connection to freedom.gnu is encrypted with 256-bit encryption." Below this, it states "The connection uses TLS 1.2." and "The connection is encrypted using AES_256_CBC, with SHA1 for message authentication and ECDHE_RSA as the key exchange mechanism." A third section, "Site information", includes an information icon and the text "You have never visited this site before today." At the bottom of the dialog is a link "What do these mean?". The background website has a red navigation bar with links for "Why", "Licenses", "Education", "Software", "Documentation", and "Help". A blue header reads "What is GNU?". Below the header, text says "Operating system that is [free software](#)—it respects your freedom." and "of GNU (more precisely, GNU/Linux systems) which are [what we provide](#)." A small inset image shows a document titled "What is free software? The Free Software Definition" with a cartoon ram logo.

The [GNU Project](#) was launched in 1984 to develop the GNU system. The name "GNU" is a recursive acronym for "GNU's Not Unix!". ["GNU" is pronounced g'noo](#), as one syllable, like saying "grew" but replacing the *r* with *n*.

A Unix-like operating system is a [software collection](#) of applications, libraries, and developer tools, plus a program to allocate resources and talk to the hardware, known

Privacy Issue: DHT



Query Privacy: Terminology

G generator in ECC curve, a point

o size of ECC group, $o := |G|$, o prime

x private ECC key of zone ($x \in \mathbb{Z}_o$)

P public key of zone, a point $P := xG$

l label for record in a zone ($l \in \mathbb{Z}_o$)

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

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

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

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

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

Query Privacy: Cryptography

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

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

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

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

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

Searching for records under label I in zone P

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

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

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

Using cryptographic identifiers

- ▶ Zone are identified by a public key
 - ▶ “alice.bob.*PUBLIC-KEY*” is perfectly legal in GNS!
- ⇒ Globally unique identifiers

GNS Summary

- ▶ Interoperable with DNS
- ▶ Globally unique identifiers with “.PUBLIC-KEY”
- ▶ Delegation allows using zones of other users
- ▶ Trust paths explicit, trust agility
- ▶ Simplified key exchange compared to Web-of-Trust
- ▶ Privacy-enhanced queries, censorship-resistant
- ▶ Reliable revocation using flooding with proof-of-work

Privacy summary

Method	Defense against MiTM	Zone privacy	Privacy vs. network	Privacy vs. operator	Traffic amplification resistance	Censorship resistance	Ease of migration
DNS	✗	✓	✗	✗	✗	✗	✓
DNSSEC	✓	✗	✗	✗	✗	✗	✗*
DNSCurve	✓	✓	✓	✗	✓	✗	✗
DNS-over-TLS	✓	n/a	✓	✗	✓	✗	✗
Namecoin	✓	✗	✓	✓	✓	✓	✗
RAINS	✓	✗	✓	✗	✓	✗	✗
GNS	✓	✓	✓	✓	✓	✓	✗

*EDNS0

Key management summary

	Suitable for personal use	Memorable	Decentralised	Modern cryptography	Understandable	Exposes metadata	Transitive
DNS	✗	✓	✗	✗	✗	✗	✓
DNSSEC	✗	✓	✗	✗	✗	✗	✓
DNSCurve	✗	✓	✗	✓	✗	✗	✓
DNS-over-TLS	✗	✓	✗	✗	✗	✗	✓
TLS-X.509	✗	✓	✗	✗	✗	✗	✓
Web of Trust	✓	✗	✓	✗	✗	✗	✓
TOFU	✓	✗	✓		✓	✓	✗
Namecoin	✗	✓	✗	✓	✓	✗	✓
RAINS	✗	✓	✗	✓	✓	✗	✓
GNS	✓	✓	✓	✓	✓	✓	✓

Possible Future Work (Project 2, BS thesis)

- ▶ Implement Fog-of-Trust (ideally in Rust)

Case study: GNS

DNS is known to suffer from a lack of end-to-end integrity protections. As a result, Chinese "great firewall" DNS manipulation has been shown to impact name resolution even in Europe.

"The GNU Name System (GNS) establishes a new name system using cryptography where zone data, queries and replies are private. The use of a distributed hash table (DHT) implies that resolution costs are comparable to those of DNS. However, states and ISPs cannot monitor or block queries, limiting their ability to protect the public from malicious Web sites. Names are not globally unique, allowing multiple anonymous users to lay claim to the same name. However, the system includes some well-known mappings by default, which users are unlikely to change. Trademarks, copyrights anti-fraud or anti-terrorism judgements can only be enforced against those well-known mappings, which users are able to bypass."

Discuss virtues and vices affected.

Conclusion

DNS	globalist
DNSSEC	authoritarian
Namecoin	libertarian (US)
RAINS	nationalist
GNS	anarchist

In which world do you want to live?

Exercise

```
# apt-get install git autoconf automake autopoint gettext
# apt-get install libunistring-dev libgnutls28-dev
# apt-get install openssl gnutls-bin libtool libltdl
# apt-get install libcurl-gnutls-dev libidn11-dev
# apt-get install libsqlite3-dev
$ git clone git://gnunet.org/libmicrohttpd
$ git clone git://gnunet.org/gnunet
$ git clone git://gnunet.org/gnunet-gtk
$ for n in libmicrohttpd gnunet gnunet-gtk do;
    cd $n ; ./bootstrap ; ./configure --prefix=$HOME ...
    make install
    cd ..
done
```

Exercise

```
$ gnunet-setup # enable TCP transport only
$ gnunet-arm -s # launch peer
$ gnunet-namestore-gtk # configure your GNS zone
$ gnunet-gns # command-line resolution
$ gnunet-gns-proxy # launch SOCKS proxy
$ firefox # configure browser to use proxy
```

References