

Netzwerkdienste für sozial-liberale Gesellschaften

Christian Grothoff

• • • • Berner Fachhochschule
Technik und Informatik



29.9.2018

“All governments should be pressured to correct their abuses of human rights.” –Richard Stallman

No one shall be subjected to (...) interference with his privacy, family, home or correspondence (...) – Article 12

⇒ **Staat darf nicht in private Kommunikation eingreifen oder einsehen.**

“Everyone (...) has the right to social security and is entitled to realization (...) of the economic, social and cultural rights indispensable for his dignity and the free development of his personality.” – Article 22

“Everyone has the right to a standard of living adequate for the health and well-being of himself and of his family (...).” – Article 25a

⇒ **Staat muss in Wirtschaft zur Herstellung sozialer Grundrechte eingreifen.**

- ▶ Internetüberwachung durch den Tiefen Staat findet seine Schranken in der Technik, nicht im Gesetz.
⇒ **Technik muss Privatsphäre schützen.**
- ▶ Durch Internet globalisierte Wirtschaft erschwert staatliche Kontrolle.
⇒ **Technik muss Staat effektive Steuerungsmechanismen im Wirtschaftsbereich bereitstellen** *ohne* Privatsphäre zu verletzen.



(U) What is TREASUREMAP?



(U//FOUO) Capability for building a near real-time, interactive map of the global internet.

Map the entire Internet – Any device*, anywhere, all the time

(U//FOUO) We enable a wide range of missions:

- Cyber Situational Awareness – *your own network plus adversaries'*
- Common Operation Pictures (COP)
- Computer Attack/Exploit Planning / Preparation of the Environment
- Network Reconnaissance
- Measures of Effectiveness (MOE)

(* limited only by available data)



February 13, 2018

From a [decades-long strategy](#) of exploiting state sales tax loopholes to its [ongoing "HQ2" sweepstakes](#), Amazon's leaders have rarely turned down a chance to use the tax system as the source of their competitive advantage.

The online retail giant has built its business model on tax avoidance, and its [latest financial filing](#) makes it clear that Amazon continues to be insulated from the nation's tax system. [In 2017, Amazon reported \\$5.6 billion of U.S. profits and didn't pay a dime of federal income taxes on it.](#) The company's financial statement suggests that various tax credits and tax breaks for executive stock options are responsible for zeroing out the company's tax this year.

The company's zero percent rate in 2017 reflects a longer term trend.



Matthew Gardner
Senior Fellow

Share



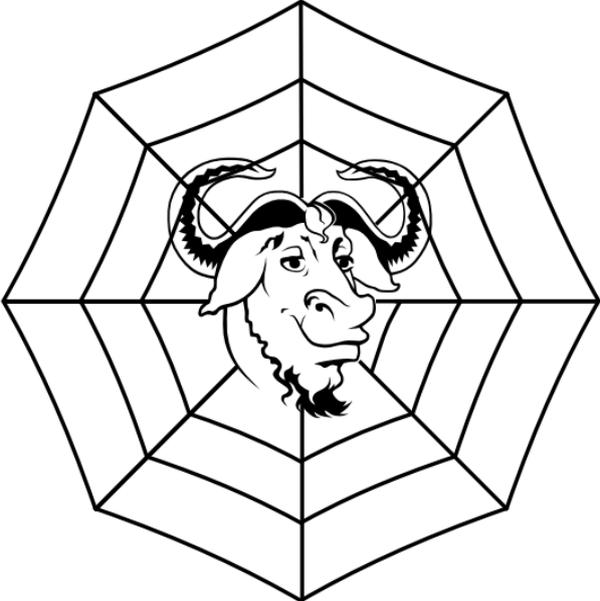
Blog Categories

[Corporate Taxes](#)

[Education Tax Breaks](#)

<https://itep.org/amazon-inc-paid-zero-in-federal-taxes-in-2017-gets-789-million-windfall-from-new-tax-law/>

Wir müssen etwas tun!



Designziele für zivile Netze

1. GNUet muss als Freie Software implementiert sein.
2. GNUet darf nur die minimal notwendigen personenbezogenen Daten preisgeben.
3. GNUet muss komplett verteilt und resistent gegen externe Angriffe als auch bössartige Teilnehmer sein.
4. GNUet muss selbstorganisierend sein und nicht von Administratoren oder zentraler Infrastruktur abhängig sein.
5. GNUet muss den Benutzer informieren wem vertraut werden muss wenn private Kommunikationskanäle etabliert werden.
6. GNUet muss ein offenes Netz sein dem neue Peers beitreten können.
7. GNUet muss ein breites Spektrum an Anwendungen und Geräten unterstützen.
8. GNUet muss sensitive Daten durch Kompartimentierung schützen.
9. Die GNUet Architektur muss Ressourcen effizient einsetzen.
10. GNUet muss Anreize schaffen, dass Peers mehr Ressourcen bereitstellen als sie selber verbrauchen.

Anwendungen für GNUet (in Arbeit)

- ▶ Anonymes und nicht-anonymes Publizieren
- ▶ IPv6-IPv4 Protokollübersetzer und Tunnel
- ▶ **GNU Name System**: zensurresistenter Ersatz für DNS
- ▶ Conversation: sicheres, dezentrales Telefonieren
- ▶ SecuShare: soziales Netzwerk
- ▶ **GNU Taler**: datenschutzfreundliches Bezahlen
- ▶ ...

The GNU Name System

Das GNU Name System¹

Eigenschaften vom GNS

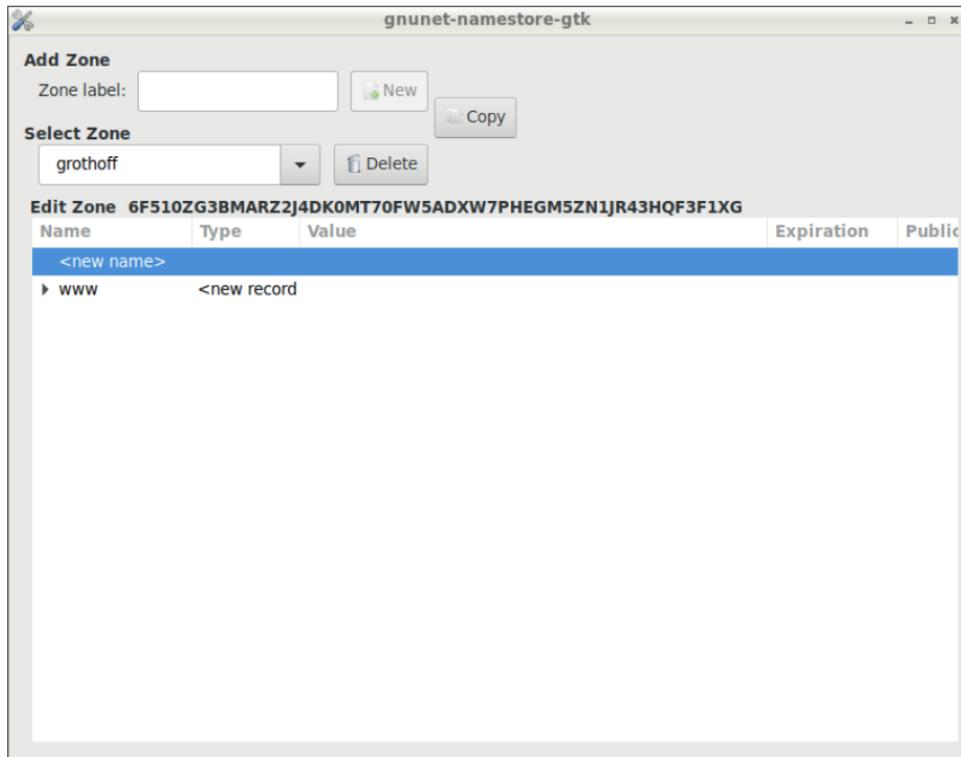
- ▶ Dezentralisiertes Namenssystem ⇒ Namen sind nicht global.
- ▶ Unterstützt global eindeutige (& sichere) Identifizierung
- ▶ Erreicht Datenschutz für Fragen und Antworten
- ▶ Funktioniert als PKI
- ▶ Interoperabel mit DNS

Anwendungen für GNS im GNUet

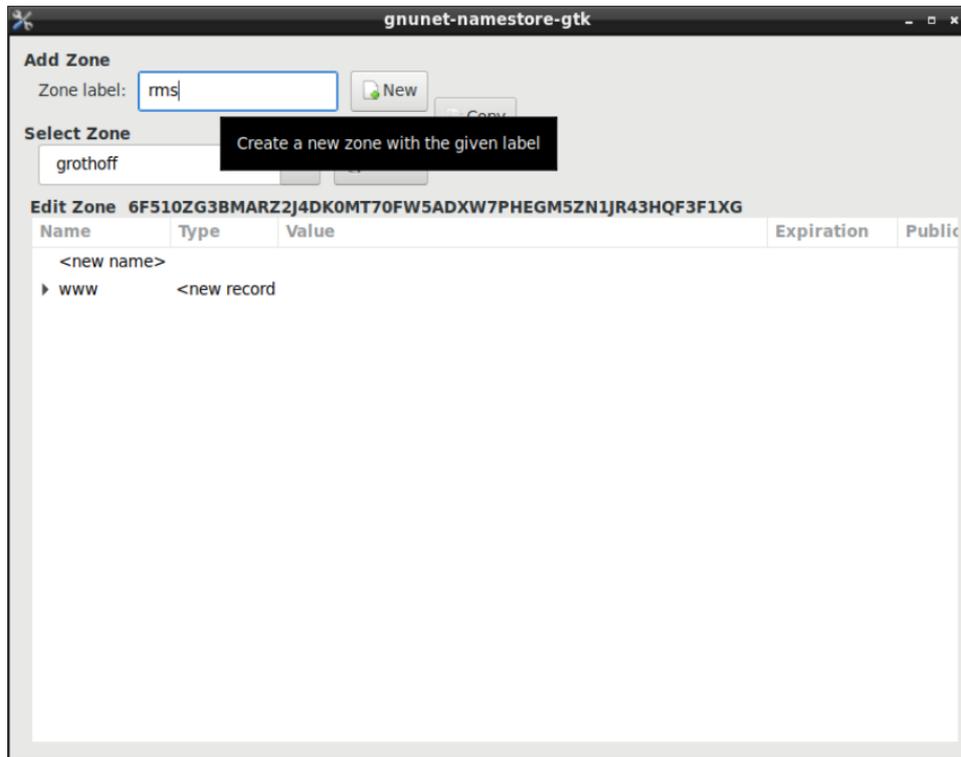
- ▶ Identifizierung von IP Diensten die im P2P-Netz gehostet werden
- ▶ Identitäten in sozialen Netzwerkanwendungen
- ▶ Adressbuch in der Telefonanwendung
- ▶ Ersatz für DNS
- ▶ ...

¹Joint work with Martin Schanzenbach and Matthias Wachs

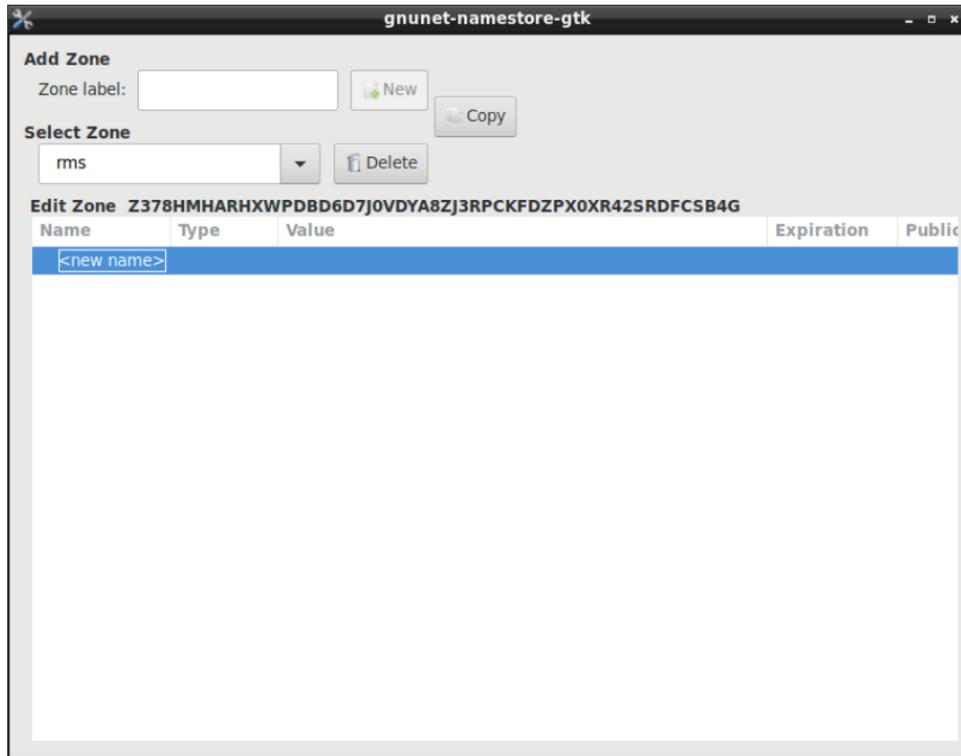
Zonenmanagement



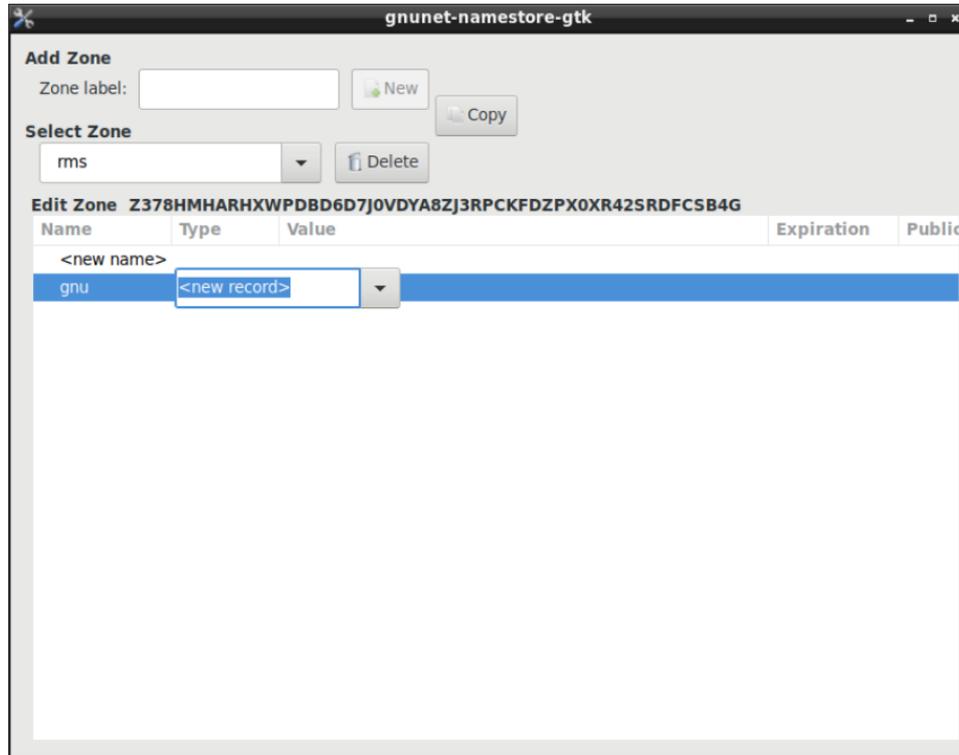
Zonenmanagement



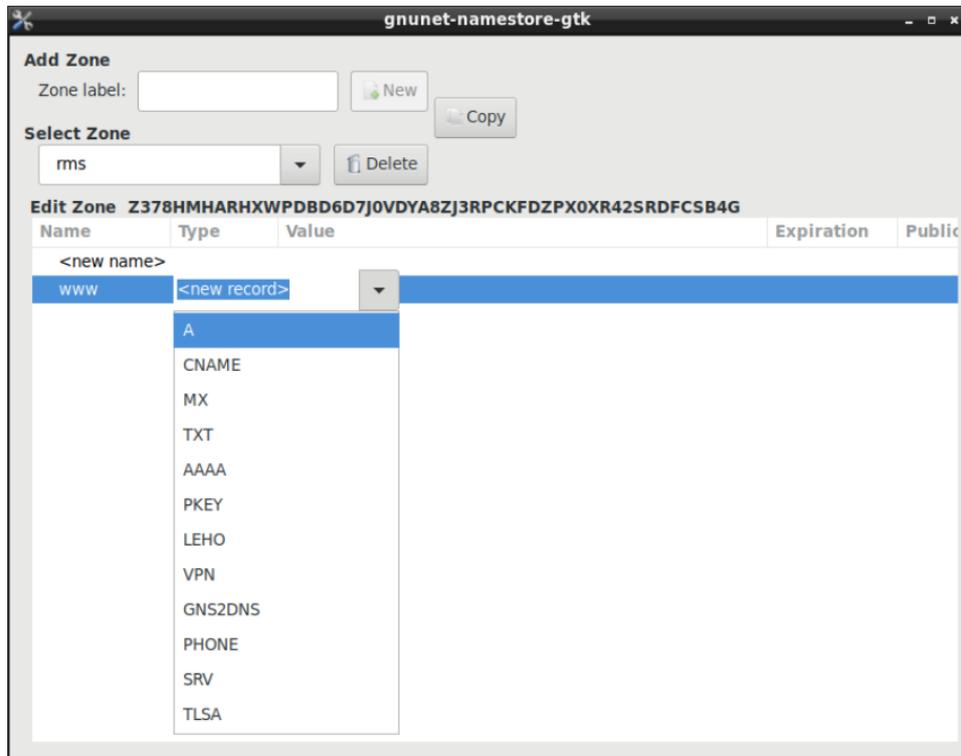
Zonenmanagement



Zonenmanagement



Zonenmanagement



Zonenmanagement

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

Zonenmanagement

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:' input field, 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 Z378HMHARHXWPDBD6D7J0VDYA8ZJ3RPFKFDZPX0XR42SRDFCSB4G' and contains a table with columns 'Name', 'Type', 'Value', 'Expiration', and 'Public'. A dropdown menu is open over the 'Type' column of the 'www' row, listing various DNS record types: A, CNAME, MX, TXT, AAAA, PKEY, LEHO, VPN, GNS2DNS, PHONE, SRV, and TLSA. The 'www' row is highlighted in blue, and the 'A' record type is also highlighted in blue in the dropdown menu.

Add Zone
Zone label:

Select Zone

Edit Zone Z378HMHARHXWPDBD6D7J0VDYA8ZJ3RPFKFDZPX0XR42SRDFCSB4G

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

- A
- CNAME
- MX
- TXT
- AAAA
- PKEY
- LEHO
- VPN
- GNS2DNS
- PHONE
- SRV
- TLSA

Zonenmanagement

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:

Import from: www.gnu.org Convert

Options
 Record is public (visible to other users) Import Certificate from external
 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: 57 - + Seconds: 50 - +

Cancel Save

Zonenmanagement

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:
2e1e12dacb350e69317a7f37d769f46f16f437cf8d392319279c93515e5600baed3d3acd5dc83b673e8c60cf7
fba0dce00a4d162a3b966a3ebf72487c376fca0

Certificate:

Import from: www.gnu.org

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

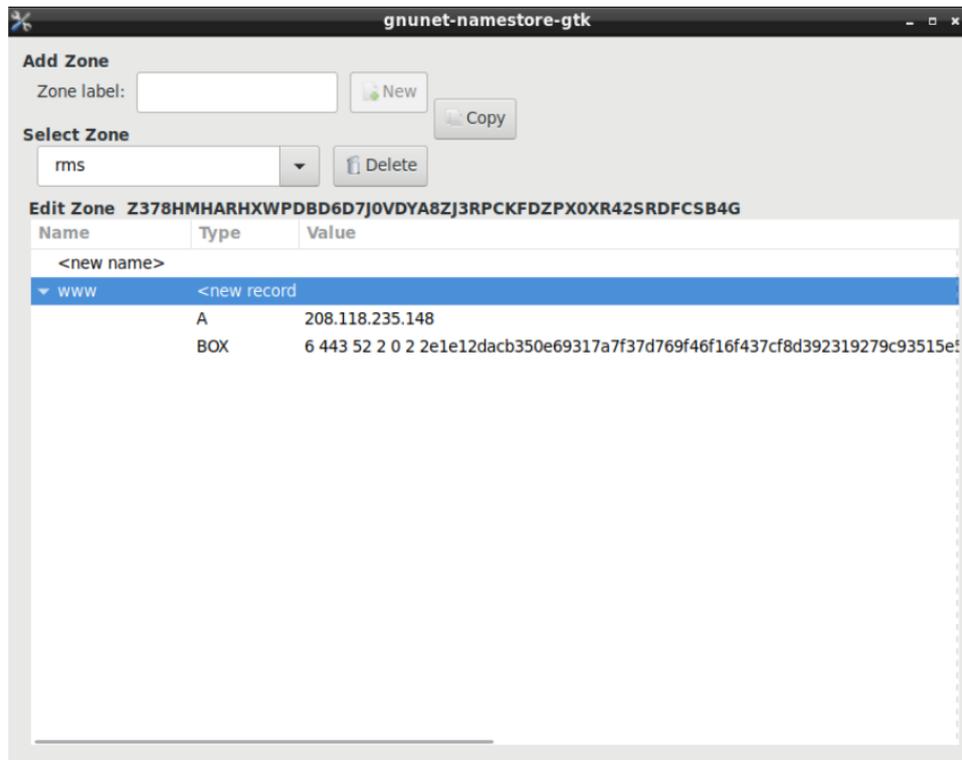
Expiration Time
 Relative Absolute Never

< 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 - +

Zonenmanagement



The screenshot shows the 'gnet-namestore-gtk' application window. It features three main sections: 'Add Zone', 'Select Zone', and 'Edit Zone'. The 'Add Zone' section has a 'Zone label:' input field, 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 '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 this is a row with 'BOX' and a long alphanumeric string.

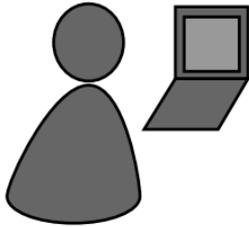
Add Zone
Zone label:

Select Zone

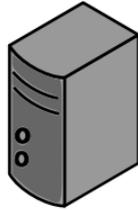
Edit Zone Z378HMHARHXWPDBD6D7J0VDYA8ZJ3RPCKFDZPX0XR42SRDFCSB4G

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

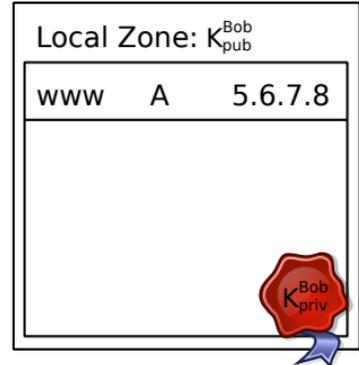
Namesauflösung im GNS



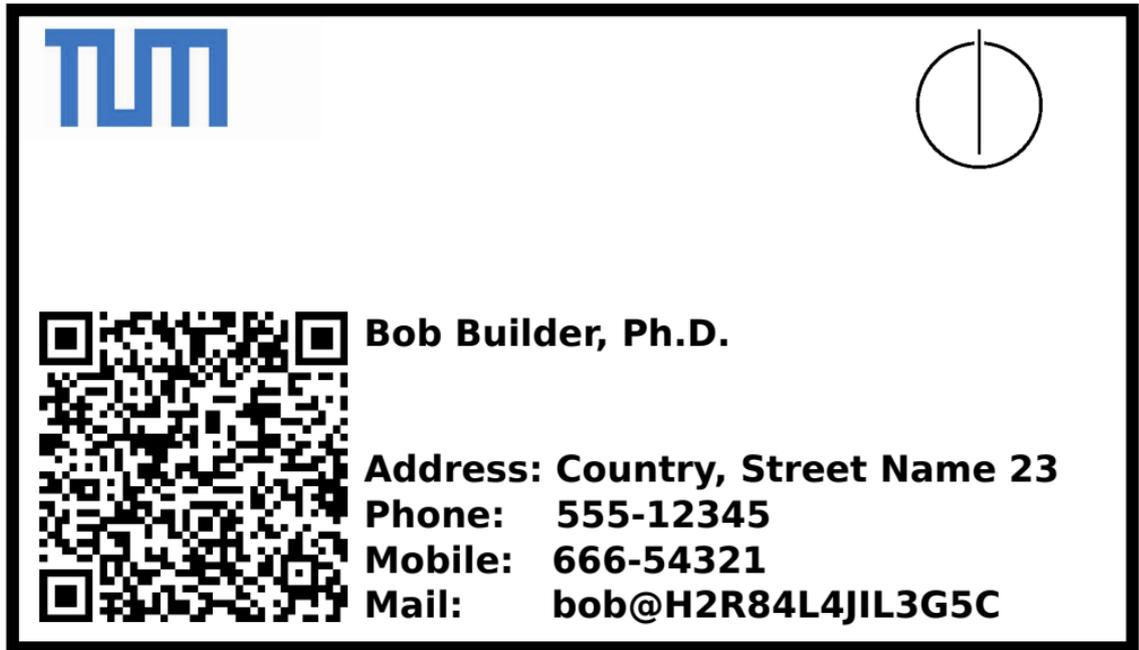
Bob



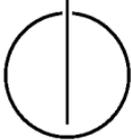
Bob's webserver



- ▶ Bob kann seinen Webserver unter **www.bob** erreichen



TUM



Bob Builder, Ph.D.

Address: Country, Street Name 23

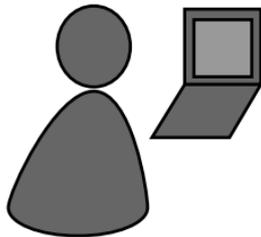
Phone: 555-12345

Mobile: 666-54321

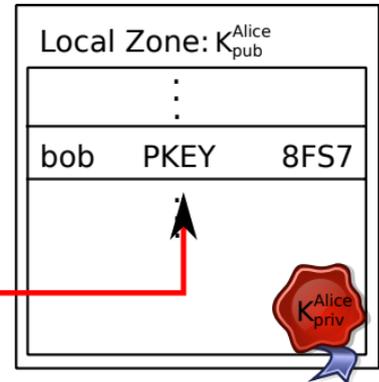
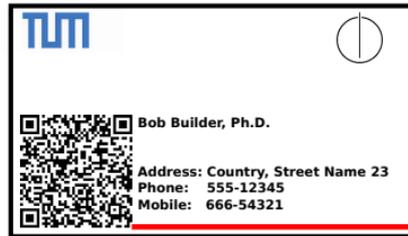
Mail: bob@H2R84L4JIL3G5C

- ▶ Bob gibt seinen öffentliche Schlüssel seinen **Freunden**, z.B. via QR Code

Delegation

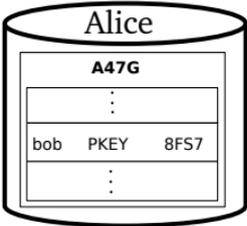
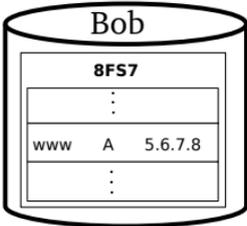
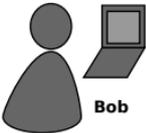


Alice

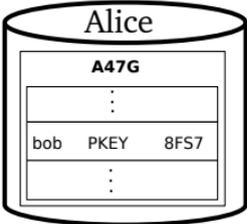
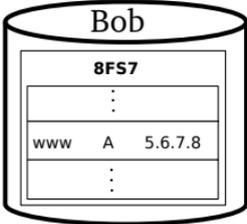


- ▶ Alice lernt Bob's "öffentlichen" Schlüssel
- ▶ Alice erzeugt Delegation an Zone K_{pub}^{Bob} unter Label **bob**
- ▶ Alice kann den Webserver von Bob unter **www.bob.alice** erreichen

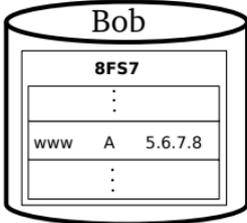
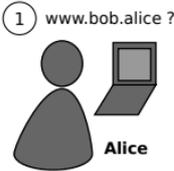
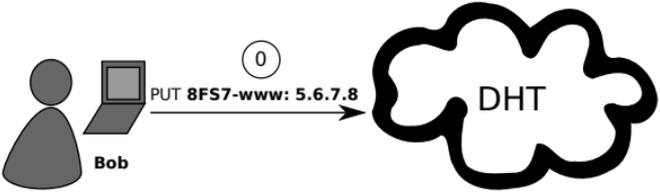
Namensauflösung



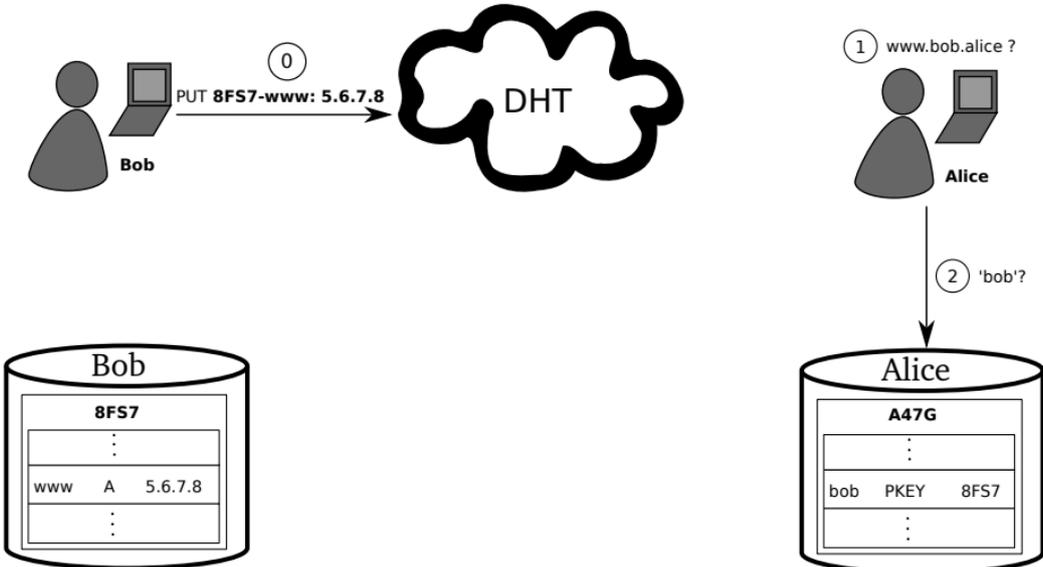
Namensauflösung



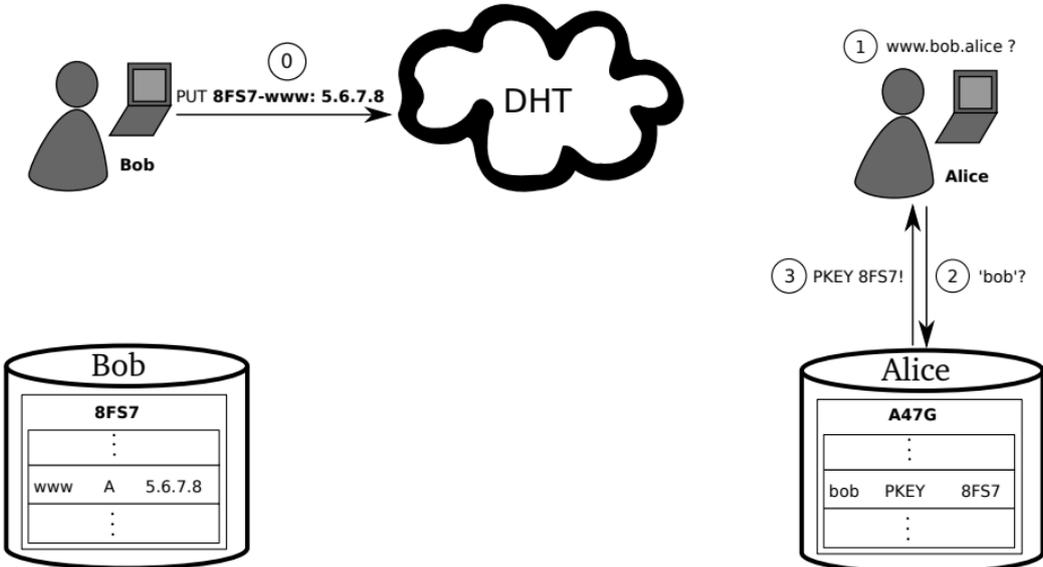
Namensauflösung



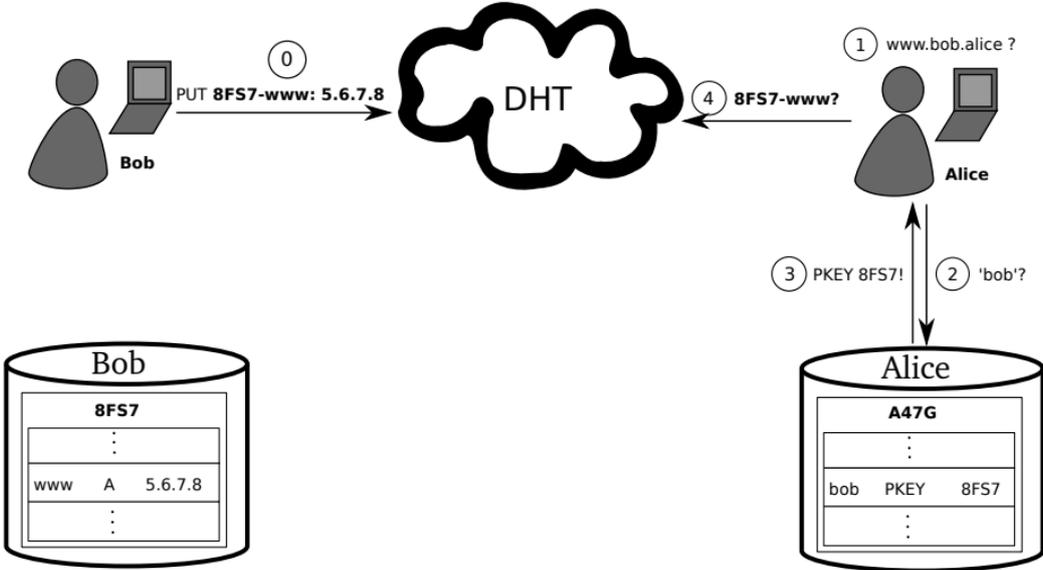
Namensauflösung



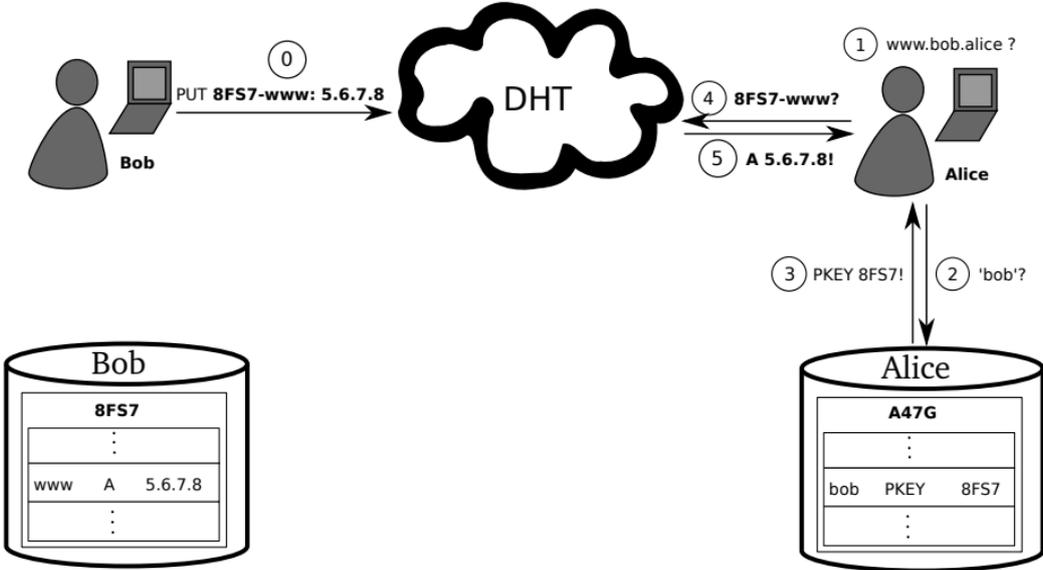
Namensauflösung



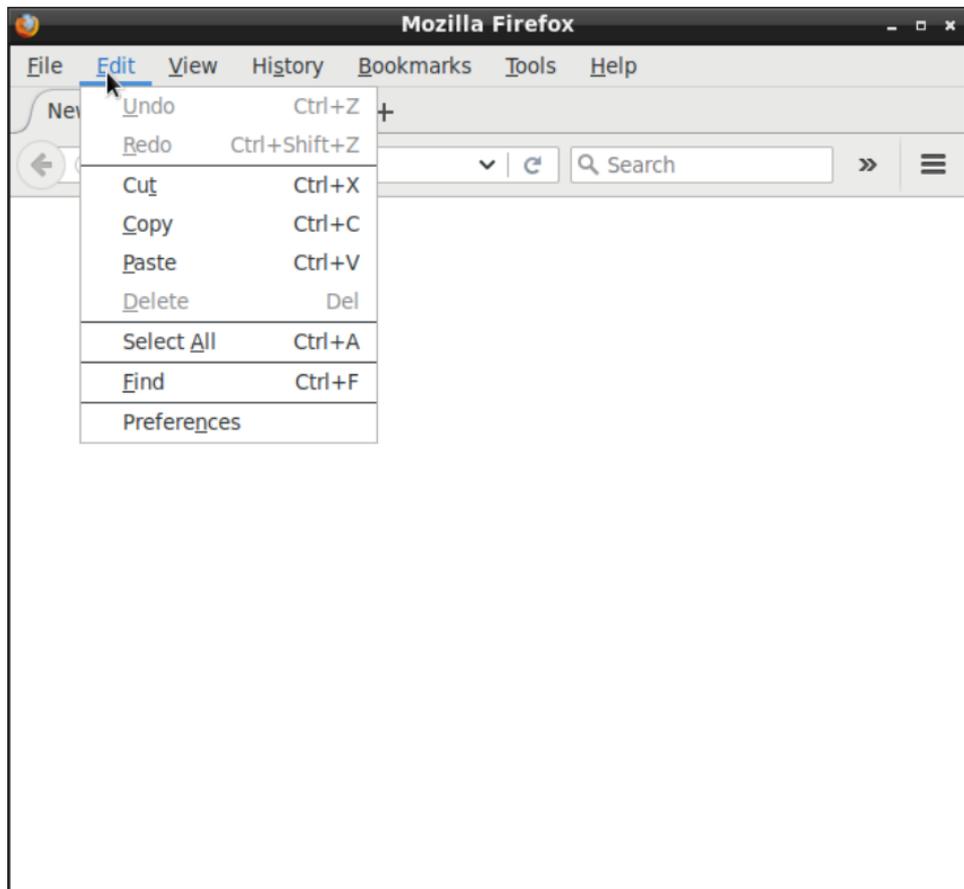
Namensauflösung



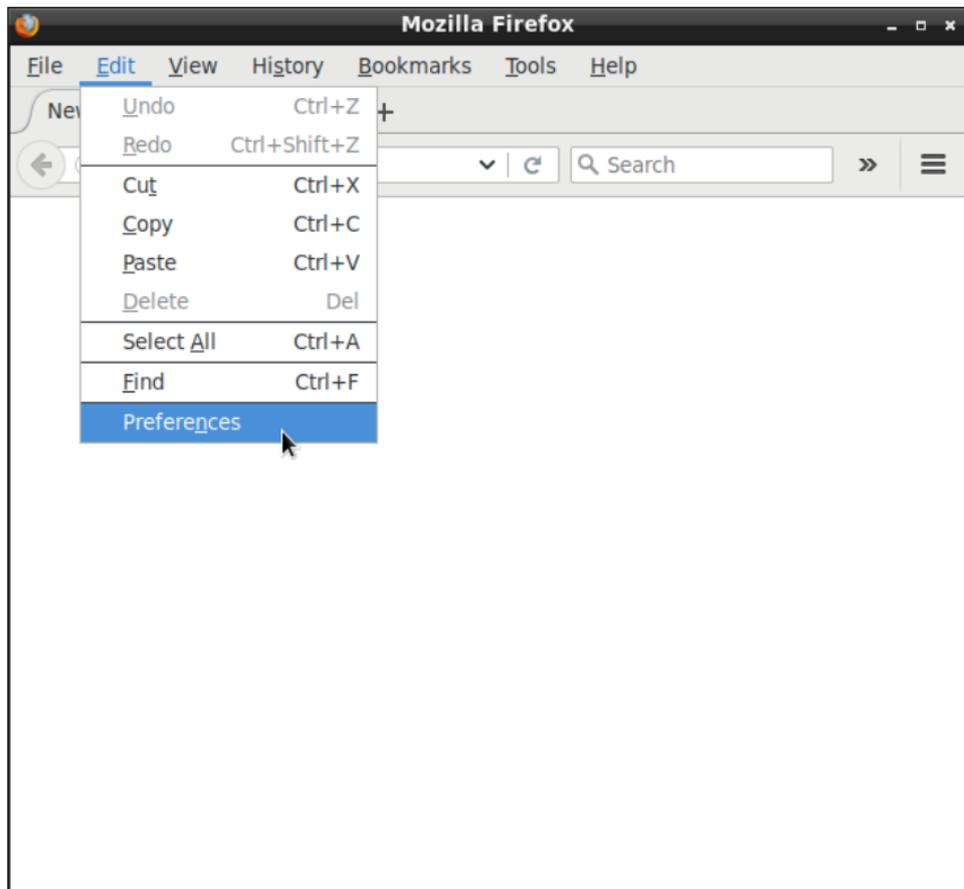
Namensauflösung



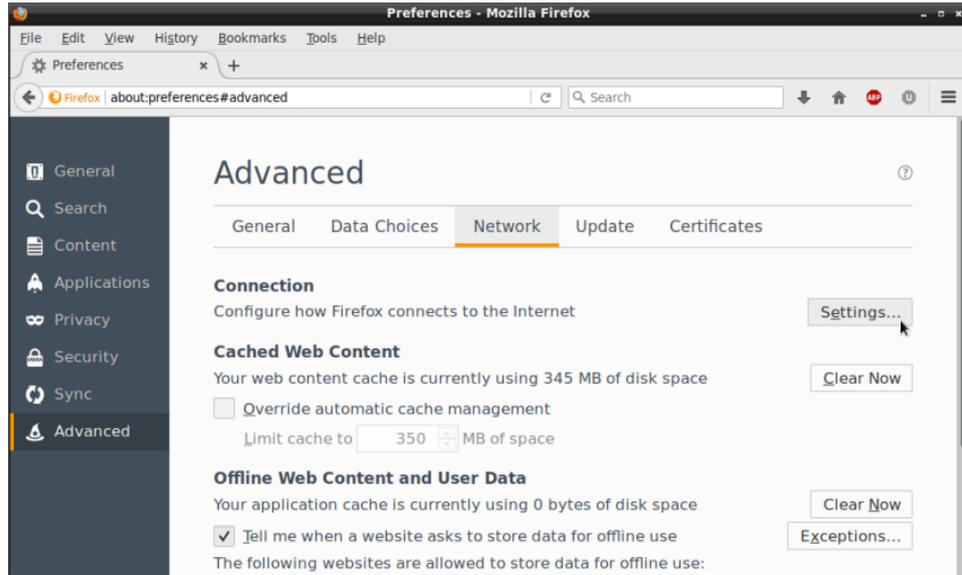
Browser Konfiguration



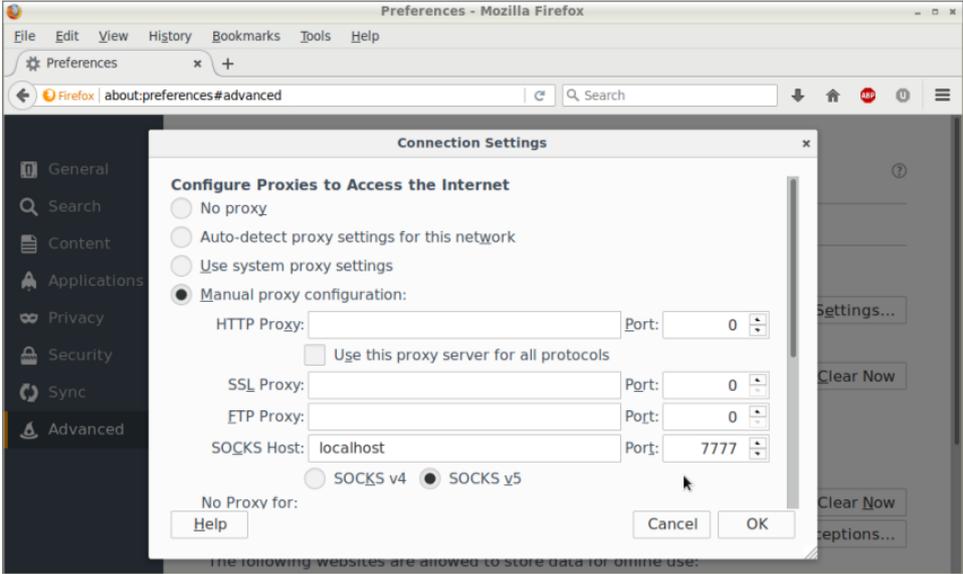
Browser Konfiguration



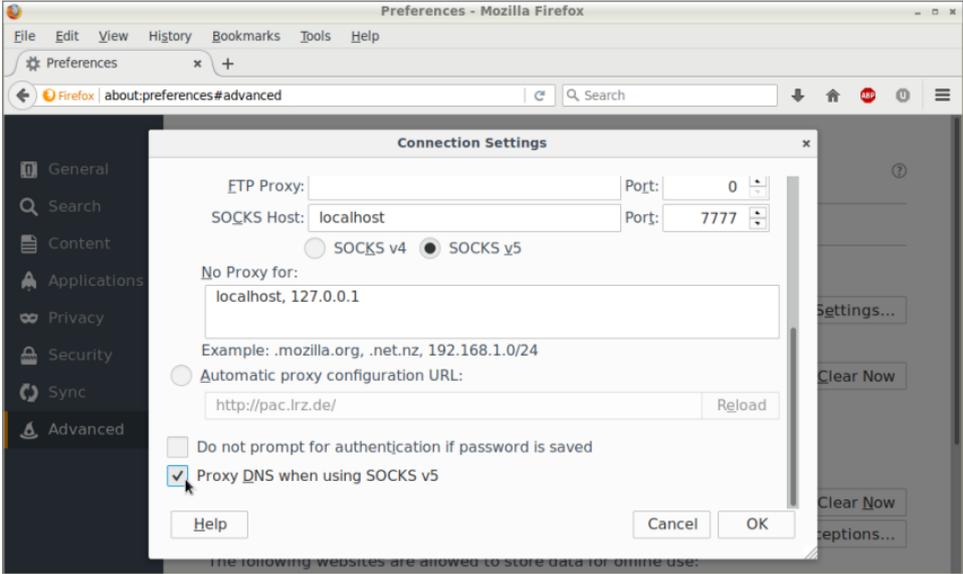
Browser Konfiguration



Browser Konfiguration



Browser Konfiguration



Browser Benutzung

The screenshot shows a Mozilla Firefox browser window with the title "The GNU Operating System and the Free Software Movement - Mozilla Firefox". The address bar displays "https://www.rms". The page content includes a navigation menu with links for "EDUCATION", "SOFTWARE", "DOCUMENTATION", and "HELP GNU". A prominent red button says "JOIN THE FSF". Below it, there is a "Free Software Supporter" section with an "email address" input field and a "Sign up" button. The main content area features a section titled "What is GNU?" with a paragraph explaining GNU as a free software system. To the right, there is a "Planet GNU" section with a link to "LibreJS 7.15 released".

The GNU Operating System and the Free Software Movement - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Preferences x The GNU Operating S... x +

https://www.rms Search

Why GNU/Linux? Search

العربية [ar] [es] فارسی [fa] français [fr] italiano [it] 日本語 [ja] 한국어 [ko] lietuvių [lt] [lv] Shqip [sq] українська [uk] 简体中文 [zh-cn] 繁體中文 [zh-tw]

JOIN THE FSF

Free Software Supporter

email address Sign up

EDUCATION SOFTWARE DOCUMENTATION HELP GNU

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...

GNU Taler

Motivation



Moderne Wirtschaft braucht Online-Bezahlsysteme.

Kreditkarten?



SWIFT/Mastercard/Visa sind zu transparent.

Wir können Bargeld **digital** und
sozialverträglich machen.

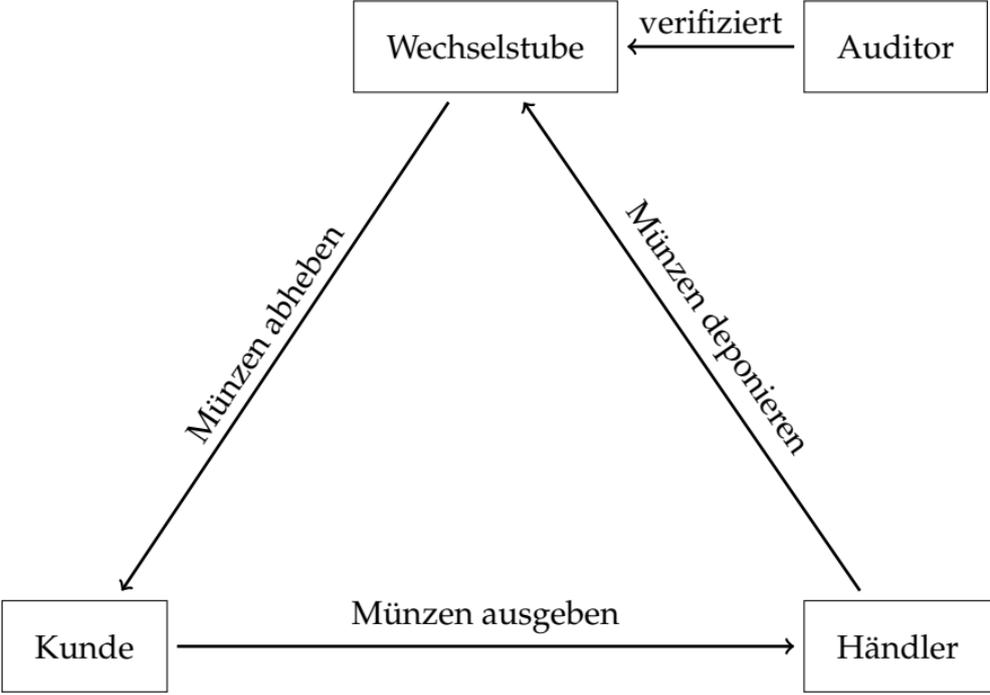
<Taler>

Taxierbare Anonyme Libre Elektronische Reserven

Designziele für GNU Taler

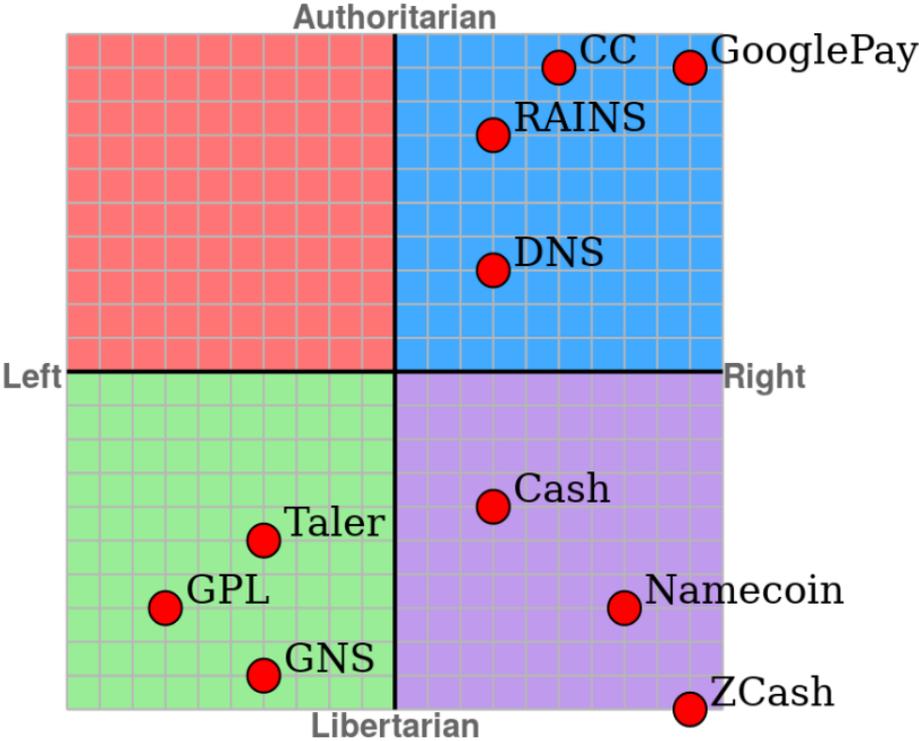
1. GNU Taler muss als Freie Software implementiert sein.
2. GNU Taler muss die Privatsphäre von Käufern schützen.
3. GNU Taler muss es dem Staat ermöglichen Einkommen zu besteuern und illegale Geschäftspraktiken zu verfolgen.
4. GNU Taler darf nur die minimal notwendigen Daten preisgeben.
5. GNU Taler muss finanziellen Betrug verhindern.
6. GNU Taler muss einfach zu benutzen sein.
7. GNU Taler muss effizient sein.

Architektur von GNU Taler



GNU Taler Demo!

Politisch-Technischer Kompass



Fragen?

Mehr Informationen im Interent:

▶ <https://gnunet.org/>

▶ Krypto-GNS:

<https://gnunet.org/video-30c3-talk-gnu-name-system>

▶ <https://taler.net/>

▶ Krypto-Taler:

<https://taler.net/videos/sha2017taler.webm>

▶ Folien werden auf

<https://grothoff.org/christian/> publiziert.

