NEXT GENERATION INTERNET

The GNU Taler payment system

Christian Grothoff

40 Years Free Software Foundation

What is GNU Taler?

https://taler.net/en/features.html

Taler is

- a Free/Libre software *payment system* infrastructure project
- ... with a surrounding software ecosystem
- ... and a company (Taler Systems S.A.) and community that wants to deploy it as widely as possible.

However, Taler is

- *not* a currency or speculative asset
- *not* a long-term store of value
- *not* a network or instance of a system
- *not* decentralized
- *not* based on proof-of-work or proof-of-stake

Design principles

https://taler.net/en/principles.html

GNU Taler must ...

1. ... be implemented as **free software**.
2. ... protect the **privacy of buyers**.
3. ... enable the state to **tax income** and crack down on illegal business activities.
4. ... prevent payment fraud.
5. ... only **disclose the minimal amount of information necessary**.
6. ... be usable.
7. ... be efficient.
8. ... avoid single points of failure.
9. ... foster **competition**.

Origins

1996	Cryptography @ Wuppertal: Blind signatures for payment
2001	Cryptography @ Purdue: GNUnet package started
2007	GNU libmicrohttpd package started
2009	DFG funds Free Software Network Security Group
2011	Florian Dold joins Free Software Network Security Group
2013	P2P Course @ TUM: Florian solves giving change, first encounter with Leon Schumacher in Zürich
2016	Taler Systems SA founded in Luxembourg
2019	Florian defends PhD on the GNU Taler System
2022	Programmable money: cash with age restrictions
2023	Support for payments to offline merchants
2024	Donations, subscriptions and discount token design
2025	Post-quantum design of change protocol by TU/e & AS

Present: NGI TALER PILOT

https://taler.net/en/consortium.html

- EU Project started December 2023 to deploy GNU Taler
- 3 financial institutions (GLS Bank, Magnet Bank, Visual Vest), 2 academic institutions (Berner FH, TU Eindhoven), 3 SMEs (Taler Systems SA, Code Blau GmbH, Petit Singularites), 3 non-profits (NLnet Foundation, E-Seniors Association, Homo Digitalis)
- ≈ € 5M budget over 3 years
- Objective: **Deploy GNU Taler in Europe**

Launch Timeline

Q2’2022	Internal deployment at BFH
Q3’2024	Deployment of local currency Netzbon in Basel
Q2’2025	Public deployment of eCHF stablecoin in Switzerland, cleared by FINMA
Q3’2025	GLS bank launches in Eurozone
Q4’2025	Magnet bank launches in Hungary (?)

Operators

- `https://netzbon.ch/` is site of deployment in Basel (**NETZBON**)
- `https://exchange.e.netzbon-basel.ch/` hosts production REST API
- `https://taler-ops.ch/` is site of Taler Operations AG, Biel (**CHF**)
- `https://exchange.taler-ops.ch/` hosts production REST API
- `https://gls.de/taler/` main site for Taler at GLS Bank (**EUR**)

What software exists?

- libeufin-nexus: PostFinance (EBICS) integration
- libeufin-bank: regional currency bank
- merchant backend: REST API with inventory and order management
- payment plugins: Joomla!, Magento, WooCommerce
- challenger: address (postal, sms, e-mail) validation (OAuth2 API)
- exchange: Taler core system with AML/KYC processes for compliance
- wallets: for Android, Chromium/Chrome, Firefox, iOS – and command-line

Taler is licensed under LGPL (rarely), GPL (wallets) or AGPL (servers).

What can you do today?

- Add any Taler provider to your wallet
- Withdraw digital cash via SEPA transfer
- Deposit digital cash back into your bank account
- Make P2P payments
- Setup your own merchant / e-commerce site to receive payments
- Setup your regional / event currency ⇒ workshop!

What software is the community working on?

- Sync: backup service
- GNU Anastasis: distributed zero-knowledge key backup
- Mailbox: send payment messages to remote Taler wallets (instead of NFC/QR code)
- TalDir: map e-mail address or phone number to Taler wallet Mailbox address
- Donau: issue receipts for tax-deductable donations
- Adorsys-OBG: automate withdrawal via PSD2
- EKYC: Electronic KYC process for ID document uploading
- cashless2ecash: pay with card to withdraw Taler e-cash
- cash2ecash: pay with cash to withdraw Taler e-cash

What might we do tomorrow?

- Pay for online news, e-commerce, ...
- Integrated subscriptions, discount tokens
- Onboard large merchants (Galaxus, Migros, SBB, ...)
- Programmable payments (auctions, escrow, ...)
- M2M/IoT payments (no need for accounts, no 2-FA!)
- Pay recipient for messaging/e-mail (no more spam!)

What might we do tomorrow?

- Pay for online news, e-commerce, ...
- Integrated subscriptions, discount tokens
- Onboard large merchants (Galaxus, Migros, SBB, ...)
- Programmable payments (auctions, escrow, ...)
- M2M/IoT payments (no need for accounts, no 2-FA!)
- Pay recipient for messaging/e-mail (no more spam!)
- ...

`https://nlnet.nl/propose`

How to support?

Join: `https://lists.gnu.org/mailman/listinfo/taler`

Learn: `https://tutorials.taler.net/`

Discuss: `https://ich.taler.net/`

Report: `https://bugs.taler.net/`,

Develop: `https://git.taler.net/`

Apply: `https://nlnet.nl/taler`

Translate: `https://weblate.taler.net/`, `translation-volunteer@taler.net`

Integrate: `https://docs.taler.net/`

Do you have any questions?

References:

1. Özgür Kesim, Christian Grothoff, Florian Dold and Martin Schanzenbach. *Zero-Knowledge Age Restriction for GNU Taler*. **27th European Symposium on Research in Computer Security (ESORICS), 2022**.
2. David Chaum, Christian Grothoff and Thomas Moser. *How to issue a central bank digital currency*. **SNB Working Papers, 2021**.
3. Christian Grothoff, Bart Polot and Carlo von Loesch. *The Internet is broken: Idealistic Ideas for Building a GNU Network*. **W3C/IAB Workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT)**, 2014.
4. Jeffrey Burdges, Florian Dold, Christian Grothoff and Marcello Stanisci. *Enabling Secure Web Payments with GNU Taler*. **SPACE 2016**.
5. Florian Dold, Sree Harsha Totakura, Benedikt Müller, Jeffrey Burdges and Christian Grothoff. *Taler: Taxable Anonymous Libre Electronic Reserves*. Available upon request. 2016.
6. Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer and Madars Virza. *Zerocash: Decentralized Anonymous Payments from Bitcoin*. **IEEE Symposium on Security & Privacy, 2016**.
7. David Chaum, Amos Fiat and Moni Naor. *Untraceable electronic cash*. **Proceedings on Advances in Cryptology, 1990**.
8. Phillip Rogaway. *The Moral Character of Cryptographic Work*. **Asiacrypt**, 2015.

Acknowledgements

Funded by the European Union (Project 101135475).

Co-funded by
the European Union

Funded by SERI (HEU-Projekt 101135475-TALER).

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.