Donau: Donation authority

Tax-deductable Privacy-Preserving Donations

Johannes Casaburi Lukas Matyja

Advisor: Prof. Dr. Christian Grothoff
Advisor: Prof. Dr. Emmanuel Benoist
Expert: Daniel Voisard

June 13, 2024

Abstract

This project describes the design of a privacy-preserving donation system. The central entity in the design is the donation authority (Donau) which was implemented in free software in the context of the GNU Taler project. While implemented primarily for GNU Taler, the system could in principle work with other payment systems.

Providing evidence of charitable donations for tax deductions often requires sensitive personal information, raising privacy concerns. Donors may wish to anonymize receipts while still being able to make legitimate donations to recognized charities. On the other side tax authorities may wish to better prevent donation fraud with verifiable signatures. Deductions for unrecognized charities or failure to deduct valid foreign donations also occur. A system allowing anonymous yet verifiable donation receipts would address these issues. The Donau would be operated by a tax authority. The Donau backend implements a REST API used primarily by charities and donors. It maintains a list of recognized charities, enabling tax authorities to audit the total amount of donation receipts each charity is issuing. Upon making a donation to one of the charities the donor receives a *donation receipt* which will be stored locally on the donor's device. Throughout this process neither the charity nor the Donau obtains any identifiable information about the donor, thus enabling anonymous donations. To simplify the verification for the tax authority, the donor needs to submit their donation receipts to the Donau at the end of the year. At that time, the Donau can combine the individual donation receipts in one final annual *donation statement*. Upon request of the tax authority, the donor can provide this donation statement to the tax authority which can check its validity and can then approve the tax deduction.

Contents

Acknowledgements

First and foremost, we would like to thank Christian Grothoff and Emmanuel Benoist for their continued support and feedback throughout the project. A special thank to Michiel Leenaars from the NLnet foundation who had the initial idea for the project. We would also like to thank our expert Daniel Voisard for his feedback during the project. Further we would like to thank Christian Blättler for his contributions to GNUnet, on which our project relies on. A big thank to the tax authority Zürich who agreed to an interview, which has provided us with valuable insight in how donations are verified and important aspects that a system like the Donau should fulfill. We would like to mention that we have used DeepL for word translations and `https://app.diagrams.net/` for some of the figures in this thesis.

Chapter 1

Introduction

1.1 Motivation

To be able to donate to a charity and deduct that donation from taxes, it is often required to provide evidence. The donor would have to present said evidence in form of a donation receipt which would include information about both the donor and the charity. The donor may want to keep this information private and only provide a receipt that proves that a certain amount was indeed donated to a recognized charity.

There are many reasons why such information can be sensitive and should be hidden from third parties. Both personally and politically this information could be harmful to individuals if not handled responsibly. To remain anonymous donors would have to keep their donation receipts, which would not allow them to deduct the donation from taxes. It is best to reduce and anonymize this information as much as possible, while still having all the necessary information to verify donations and prevent illegal practices.

Tax authorities may have to verify donations manually which can be time consuming and involves a disproportionate amount of effort for the tax authority. The donor on the other hand has to keep track of the donation receipts. It is not unheard of, that these receipts get lost or forgotten by the time the tax declaration is submitted.

For every donation the donor wants the donation to be tax deductible, the addressed charity has to be recognized by the local tax authority. However, it can happen that donations to unrecognized charities are mistakenly deducted or that donations to recognized charities abroad are not deducted. This misconduct has found attention by Michiel Leenaars from the NLnet Foundation[1]. He has noticed that donations to their organization from other countries are sometimes not deducted from the taxes

[1] see `https://nlnet.nl/`

of their donors, although this should be the case in the European Union according to the article 63 of [1].

1.2 Goals

The goal of this thesis is to assess how donations currently work, and to develop and implement a protocol, that aims to improve and standardize how donations are verified and conducted. The Donau system should be implemented as free software.

One of the main goals of the Donau is to protect the privacy of donors, while they should still be able to deduct their donations from taxes. The donor should be able to do so without revealing more information than needed to the tax authority.

The tax authority should be able to easily verify all donations from a donor by scanning a QR-Code. This QR-Code is generated by the donor and should contain all the proof needed to deduct all donations of the year from taxes. Because the receipts are centralized in one place, in the donor's wallet, the donor does not have to worry about storing or loosing the receipts. In addition, by submitting the donation receipts to the Donau the donation receipts will be stored by the Donau. This should be a significant improvement in user convenience for both the donor and tax authority.

The Donau should prevent donation fraud with fake, expired or third-party donations. As it should maintain a list of recognized charities, in order to prevent donations from non charitable organizations. The Donau should keep track of the total amount of the donation receipts issued for each charity, to enforce donation limits according to local law and to prevent donation fraud.

The goals described above boil down to the following:

- Protect the donors privacy and still be able to deduct the amount from the taxes.
- Make donations verifiable by simply scanning a QR-Code.
- Improve the user convenience for both the donor and tax authorities.
- Prevent donation fraud with fake, expired or third-party donations.

1.3 Scope

At the start of the project the REST API specifications together with the database schema and Donau protocol was written. While implementing, the Donau API and DB tests were written to ensure that the endpoints and database work correctly. During the project the code was documented and various other documents like presentations and project summaries were created. This included a short video, presenting the Donau.

An interview was held with the tax authority Zürich, which has provided valuable insight in how donations are verified and important aspects that a system like the Donau should fulfill.

Out of scope was the charity implementation which would have been integrated into the Taler merchant and the donor client implementation which would have been integrated into the Taler wallet. Unlike the charity integration, the donor part of the Taler wallet is payment system dependent. In other words, since the Taler wallet can only make donations with the Taler payment system, it could only receive donation receipts for this. The administrator interface was also not realized, which would have provided a user-friendly interface to manage the charities. The Android verification application was also out of scope, as it could only be partially implemented.

Chapter 2

Background

This chapter captures how donations are currently verified and describes the crucial cryptographic elements used by the Donau. The project is based on existing cryptography.

2.1 How Donations Are Currently Verified

In order to find out how the tax authorities nowadays verify donations for donation deduction an interview with the tax authority Zürich was held. The interview transcript can be found in the appendix section 6.3. Currently the tax authority Zürich verifies donations by hand. The verification process is intentionally kept simple as donation fraud does not seem to be a big problem. Other ways to conduct fraud, are more likely and profitable with less legal risk attached. There is no known data that contains how much money the state has lost with donation fraud.

If the amount donated is unusually high further proof is needed. The tax authority will check if the donor is financially capable of donating this amount. Bank transaction receipts may be requested as proof. In extreme cases it is brought to court, in which case the donor needs to proof that the donation is indeed valid and was made by them.

2.2 Hash Functions

Hash functions are used to compress input values to a fixed output size. They are deterministic. The same input leads to the same output. The Donau uses hash functions to compress data in order to record less data in the database or to send less data over the network.

An important property of a hash functions is preimage and second preimage resistance. Second preimage resistance prevents an attacker from finding a different

input that produces the same hash value as a given input, which is crucial for maintaining data integrity and security in applications like digital signatures and file verification which are used in the Donau.

With second-preimage resistance no equivalent hash for any input x' to a given hash $h(x)$ with $x \neq x'$ can be found in a reasonable time. Collision resistance is the stronger assumption and even prevents to find $h(x) = h(x')$ with $x \neq x'$. A further important assumption is the Avalanche Criterion. The property defines that a small change in the hash input message leads to a substantial change in the output hash. This criteria makes it hard to guess the input even if a part of the input is known.[2] To protect the donor, their identity is represented as a salted hash of the tax identification number. The salt is a small high entropy value, to make it more difficult to guess the hashed value.

The Donau uses the SHA-512 hash function. SHA-512 is part of the SHA-2 family and provides a 256 bit security level for collision resistance. The security of the hash function is mathematically approved.[3]

2.3 EdDSA Signatures

With signatures, authenticity and non-repudiation want to be achieved. In this context hashes and public key cryptography are used.[2] For this purpose the Donau uses EdDSA signatures. The Edwards-curve Digital Signature Algorithm or for short EdDSA is a scheme for digital signatures based on the twisted Edwards elliptic curves and the Schnorr signature scheme. EdDSA signatures using the curve Curve25519 are also called Ed25519. The Donau only uses Ed25519. Whether Curve25519 or the Edwards-curve, the scheme is very efficient and secure.[4]

2.4 Blind Signatures

One important cryptographic scheme used by the Donau is the blind signature scheme. It is an extension of digital signatures which provides, besides authenticity and non-repudiation, privacy by allowing a user to obtain a signature for a message, without revealing the contents of the message to the signer. All cryptographic elements used by the Donau where provided by the GNU Taler libraries. Blind signatures are slightly slower than the normal signatures, this does not result in a performance issue as this project on GNU Taler shows: [5].

This section only provides an overview of blinded signatures. Detailed information about blinded signatures can be found at `https://taler.net/papers/cs-thesis.pdf`. Blinded signatures are the key elements to reach privacy for the donor (see section 3.1). With blinded signatures a blinded unrecognizable message was signed. Only the creator of the blinded message is able to unblind the signature and therefore to receive a valid signature for the unblinded message. The Donau system uses

blinded signatures to bind the identity to a donation receipt while hiding the identity of the donor. As a result of the property of blindness, the blind signer (in this case the Donau) is not able to link the clear-text message with the made blind signature or the blind signature with the unblind signature [6, p.12].

There are multiple blind signature schemes. The Donau distinguishes the following two equivalent blind signature schemes:

2.4.1 RSA

Concrete the RSA-FDH blind signatures are used. Before blinding, to eliminate certain attacks, a Full-Domain Hash (FDH) is applied on the message. Full-Domain means the hash has the same size as the RSA modulus. The blind signature scheme is similar to the normal RSA signature scheme. In addition to the normal scheme, the message is blinded with a private and random value. Practically the length of the modulus and therefore for the key size, signature size and the security level is variable. The scheme only has one round trip.[7]

2.4.2 Clause Schnorr (CS)

The Clause Schnorr Signature Scheme differs from the RSA scheme. Initially the blinder needs two random values from the signer party. One random value from the signer and two random private values are required to blind the message once. This process is repeated and the two blinded messages are sent to the signer, who randomly selects a blinded message for blinding. Two blinded messages are needed to prevent an certain type of attack. In comparison to the RSA scheme, the Clause Schnorr Scheme needs an additional round trip to get the initial nonces from the signer. However, the individual crypto operations are so much faster than the operations from the RSA scheme that the additional round trip is no longer significant.[8]

Because Clause Schnorr signatures are based on elliptic curves, smaller keys can be used. GNU Taler supports one fixed 256 bit key size, which provides an security level of 128 bits. The exact processes of this signature scheme do not need to be understood in order to understand this thesis.

2.5 GNU Taler

GNU Taler is an open protocol for electronic payment system using blind signatures to protect the privacy of the customer. One key component of the GNU Taler payment system is the exchange which is responsible for exchanging existing money into electronic money. Customers can retrieve funds from the exchange to make anonymous payments. The merchant is not anonymous and thus can not hide the income. This helps to avoid tax evasion and money laundering [9].

GNU Taler uses denominations to represent the values of a coins. A denomination contains the unit of currency and the face value of a given coin. Each denomination

contains a cryptographic public key used by the exchange to verify the denomination. The Donau is based on the exchange and requires some of its parts to work. The concept of the denomination was adapted into the donation units, which are used to represent the value of a donation.

Chapter 3

Approach

The Donau environment includes three stakeholders. Donors, charities and the tax authority (See figure 3.1). The Donau itself is operated by the tax authority while maintaining a list of verified charities. Each charity maintains a backend solution that allows it to communicate with the Donau and the donors.

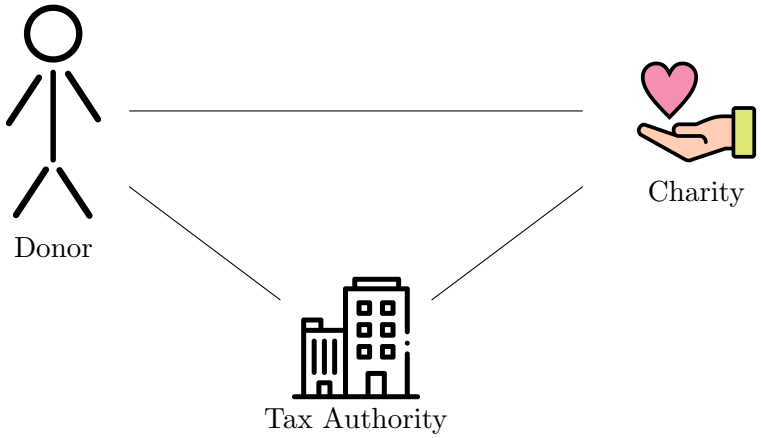


Figure 3.1: Stakeholders present in the Donau system.

3.1 Issuing Donation Receipts

When donating to a charity the donor sends the payment together with a receipt request to the charity. In order to link the donation to the donor so that the donation receipt cannot be used by someone else, the donor's unique tax identification number is part of the receipt request. This tax ID does not cause a problem for anonymity as the whole receipt including the tax ID is blinded (See section 2.4).

In figure 3.2 the blinded receipt is illustrated as an envelope. The charity must

verify if the payment was successful and if the amount written in the receipt request is lower or equal the amount donated.

Next, if the charity approves the receipt request, it signs the unmodified request and forwards the request to the Donau. The Donau accepts only issued requests from recognized charities. For a charity to be recognized, it must first be registered in the relevant Donau. When the Donau receives an issue receipt request from a charity, it checks the validity of the charity signature before the Donau issues the actual donation receipt by signing the request.

This is different from current systems where the charity usually issues the receipt. By shifting this task to the Donau, the receipts can easily be verified and unlink the donor from the charity. Because the Donau does only know the amount and the charity it is signing for, this first step of issuing receipts anonymizes the data and provides privacy for the donor. If the payment process also provides anonymity (as is the case with GNU Taler) the donations are fully anonymous.

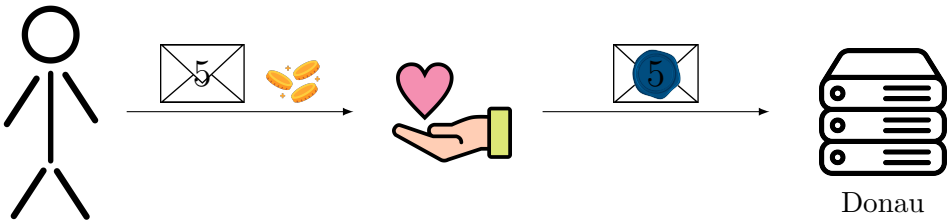


Figure 3.2: Donor donates to a charity, sending a issue receipt request to the Donau

Upon receiving the signed issue request from the charity, the Donau must verify the charity signature and check that the yearly donation limit of the charity is not exceeded. After successful verification the Donau blind signs the donation receipt which is then sent via the charity back to the Donor (See figure 3.3). The donor now unblinds the signature from the Donau to make it valid for the unblinded receipt (for more information on blind signatures see section 2.4). The unblinded receipt gets saved locally on the donors device for later. This process repeats for every donation. At the end of the year the donor may have accumulated any number of these donation receipts.

3.2 Summarize the Receipts

When it is time for the tax declaration (usually at the beginning of the next year) the donor has to request a final donation statement signature from the Donau, summarizing all the donation receipts of a year (see figure 3.4). This step combines the amounts of the donation receipts in a single total amount. This further protects the privacy of the donor as the individual donations could be enough information

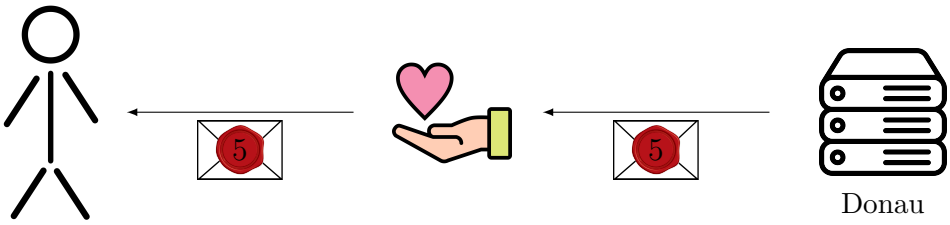


Figure 3.3: Donor receives the signed receipts from the Donau

to link up the specific donations to their corresponding charity and donor. Merging donation receipts also reduces the time and effort for the manual verification of the tax authority as the donor generates a single QR-Code containing the donation statement. This statement contains the total amount donated, year, tax ID and the signature over all of these values. This signature is used to verify the donation statement by the tax authority. The donation statement can be requested multiple times during the year for save keeping. The latest donation statement will always contain all the receipts of a year - the old receipts (from previous statements of the year) and the new donation receipts.

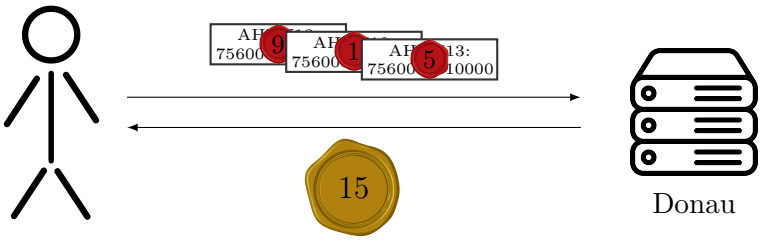


Figure 3.4: The Donau summarizes the donation receipts and sends the statement back

3.3 Validation

Once the donor has received the donation statement signature, he can summarize them in a QR code. The donor must submit the QR-Code with his tax documents, in order to claim the tax reduction (see figure 3.5). The final check is made by the tax authority, by checking the donation statement signature. If the signature is valid, this is the proof that the specified donor indeed has donated the claimed amount in the indicated year.

The tax authority will not have any information to which charity the donor has donated money. The tax authority only knows the total donated amount and that

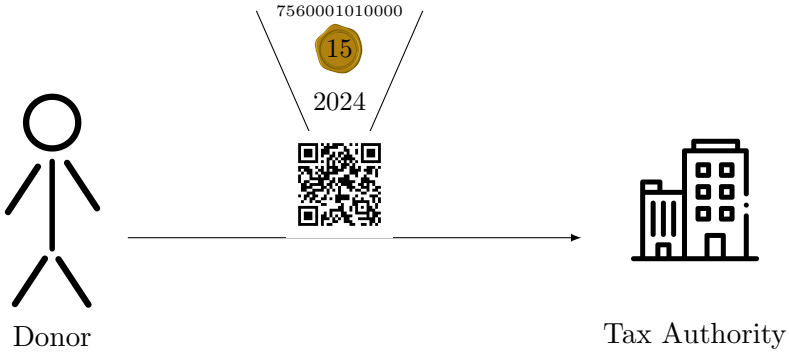


Figure 3.5: The tax authority verifies the statement previously created by the Donau

every donation was made to one of the recognized charities in the specified year. This way the donor could make an anonymous donation and still have enough proof to deduct the amount from taxes. The Donau will keep track of the total amount of the donation receipts issued for each charity, to enforce donation limits according to local law and to prevent donation fraud.

3.4 Incorporating the Donau

Every donor is delegated to only one specific Donau of his location where he is able to issue and submit donation receipts for deducting taxes. If a charity wants to be accepted in multiple tax areas, it has to be registered by all the corresponding donation authorities. To do so, the charities has to apply to the tax authorities. The region for which a Donau is responsible depends on the tax area of the tax authority and their reglementation of what is charitable. One Donau could be responsible for a geographical area like a canton, a country or even a confederation of states.

Chapter 4

Protocol

This chapter describes the Donau protocol. In the first section notations and definitions are established which are then used in the later section where the protocol details are described. To fully comprehend the cryptographic concepts discussed in this chapter, the reader may need prior knowledge or background in this field.

4.1 Notation & Definitions

4.1.1 Notation

The following are notations used in the following pages of this chapter.

- $\langle a, b, ... \rangle$ is used to represent a Pair or tuple

4.1.2 Definitions

- **Cryptographic Hash Function**

  $$h := H(m)$$

  where m is a message and h the resulting hash.

- **Blinding Function**

  $$\overline{u} := blind(u, b, K_x^{pub})$$

  where u is the value to blind, b the blinding factor to apply and K_x^{pub} the public key of the Donation Unit that will be used for signing.

  The blinding can be done with either the **RSA** blind signature scheme or the Blinded **Clause-Schnorr** signature scheme.

- **Unblinding Function**

  $$\beta := unblind(\overline{\beta}, b, K_x^{pub})$$

where $\overline{\beta}$ is the value to unblind, b the blinding factor to apply and K_x^{pub} the public key of the Donation Unit that was used for signing.

The unblinding must be carried out using the **same** signature scheme that has already been used for the blinding.

- **Donation Unit Key generation**

$$\langle K_x^{pub}, K_x^{priv} \rangle := Keygen^B(\omega)$$

where ω is a source of entropy. The resulting key pair represents a **Donation Unit**. The result is a public key K_x^{pub} and private key K_x^{priv}. The equivalent used in Taler system is a `Denomination`.

- **Donau Key generation**

$$\langle D^{pub}, D^{priv} \rangle := Keygen^D(\omega)$$

where D^{pub} and D^{priv} are the respective public and private Donau keys.

- **Charity Key generation**

$$\langle C^{pub}, C^{priv} \rangle := Keygen^C(\omega)$$

where C^{pub} and C^{priv} are the respective public and private Charity keys.

- **Donation Unit (DU)**

$$\langle K_x^{pub}, K_x^{priv} \rangle$$

A Donation Unit consists of a public and private key where x is the associated value (e.g. 2 EUR).

- **Donor Identifier (DI)**

$$i := H(\texttt{TAXID}, S)$$

where S is a random salt with sufficient entropy to prevent guessing attacks to invert the hash function.

- **Unique Donor Identifier (UDI)**

$$u := \langle i, N \rangle$$

where N is a high-entropy nonce to make the resulting hash **unique** per donation.

- **Blinded Unique Donor Identifier (BUDI)**

$$\overline{u} := blind(u, b, K_x^{pub})$$

A **BUDI** is the result of blinding a Unique Donor Identifier u where b is the blinding factor and K_x^{pub} the associated Key. The blinding is done to protect the privacy of the donor.

- **Blinded Unique Donor Identifier Key Pair (BKP)**

$$p := \langle \overline{u}, H(K_x^{pub}) \rangle$$

A **Blinded Unique Donor Identifier Key Pair** is the result of adding the corresponding hash of the **Donation Unit** public key to the **Blinded Unique Donor Identifier** $\overline{u}$ where $H(K_x^{pub})$ is the hash of the **Donation Unit** public key.

- **Signing**
  - **Normal signing (e.g. EdDSA):**

$$\boxed{s := sign(m, k^{priv})} \tag{4.1}$$

where m is a message and k^{priv} is the private key used to sign the message, for example the Donau private key D^{priv} or the Charity private key C^{priv}.

Applications:

* Signatures over a **Blinded Unique Donor Identifier Key Pair**:

$$\boxed{\vec{\mu}_s := sign(\vec{p}, C^{priv})} \tag{4.2}$$

where $H(K_x^{pub})$ indicates which **Donation Unit** key should be used by the Donau to sign the resulting **Donation Receipt**. Thus, this hash carries the information about the exact value, the final Donation Receipt should carry.

A charity signs a collection of **Blinded Unique Donor Identifier Key Pairs** before transfering them to the Donau to issue the **Donation Receipts**

* Generation of the **Donation Statement**

  - **Blind signing(e.g. RSA/CS):**

$$\boxed{\overline{\beta} := blind\_sign(\overline{u}, K_x^{priv})} \tag{4.3}$$

where $\overline{u}$ is a blinded value and K_x^{priv} is the private key used to blind sign the message.

Application:

* The Donau blind signs **Blinded Unique Donor Identifiers** received from the Charity with the private key matching the public key in the received **Blinded Unique Donor Identifier Key Pair**

- **Verify Functions**

  To verify the signatures m corresponds to the message and s to the signature:

  - **normal verify**

    $$verify(m, s, P^{pub})$$

    where P^{pub} can be the Donau public key D^{pub} or Charity public key C^{pub}.

  - **blind verify**

    $$verify\_blind(m, s, K_x^{pub})$$

    verify a signature that was made blind and made with a Donation Unit private key K_x^{priv}.

- **Donation Receipt**

  $$r := \langle u, \beta, H(K_x^{pub}) \rangle$$

  where β is the unblinded signature sent to the Donau to get the **Donation Statement**.

- **Donation Statement Signature**

  $$\sigma := sign(\langle i, \Sigma\vec{r}, \texttt{Year} \rangle, D^{priv})$$

  The **Donation Statement Signature** is the signature over the sum (amount donated) of all the **Donation Receitps** $\Sigma\vec{r}$, that a donor has received from donating throughout the year where i is the **Donor Identifier**. The **Donation Statement** itself includes all sign values and the signature itself.

  These **Donation Statement Signatures** attest the amount donated in a particular year by a specific donor.

4.2 Protocol Details

4.2.1 Key generation and initial setup

Donau key generation

1. The Donau generates a Donau public key D^{pub} and private key D^{priv} for EdDSA signing.
2. The Donau generates the **Donation Units** consisting of a public key K_x^{pub} and private key K_x^{priv} where x is the associated value.

Charity key generation

1. The Charity generates a charity public key (C^{pub} and private key C^{priv}) and fetches the **Donation Unit** public keys from the Donau.

2. The Charity transmits its public key C^{pub} and the requested yearly donation limit to the party controlling the Donau (e.g the local tax authority) using a **secure channel**.
3. The party in charge of Donau administration ensures that the applying charity is authentic and publicly recognized as a charitable organisation. Furthermore, it ensures that all eventual restrictions by law are followed. After the verification was successful the Charity public key C^{pub} together with its requested yearly donation limit are registered in the Donau database.

4.2.2 Donating to a charity

In order to make a donation the donor has to first download the **Donation Unit** public keys K_x^{pub} from the Donau for the current year. After that the donor generates his **Donor Identifier** which is a salted hash of his tax number. As each **Donation Unit** holds a specific value the donor has to split the donation amount into **Donation Units** offered by the Donau.

Donor Identifier i:

$$i := H(\texttt{TAXID, S})$$

Example: With ***Donation units*** $\{1, 2, 4\}$ *beeing available, and a donation of* 7*, the donation amount is split into the valus* 4*,* 2 *and* 1*.*

For every **Donation Unit** the donor generates a **Unique Donor Identifier** by adding a nonce to his **Donor Identifier** i. If a **Donation Unit** of the same value has to be present more than once to represent the target sum, multiple **Unique Donor Identifiers** of same **Donation Unit** has to be generated.

In our example, there are 3 ***Unique Donor Identifiers*** *needed to represent the value of* 7*.*

Unique Donor Identifiers u_1, u_2, u_3:

$$u_1 := \langle i, \texttt{N}_1 \rangle$$
$$u_2 := \langle i, \texttt{N}_2 \rangle$$
$$u_3 := \langle i, \texttt{N}_3 \rangle$$

where S is the salt and N a Nonce.

In a next step the donor needs to blind the **Unique Donor Identifiers** using a *different* blinding factor b for every **Unique Donor Identifier**. This ensures that no identifiable information is leaked to a third party including the Donau and charity. This results in a **Blinded Unique Donor Identifier**.

Blinded Unique Donor Identifiers $\overline{u}_1, \overline{u}_2, \overline{u}_3$

$$\overline{u}_1 := blind(u_1, b_1, K_1^{pub})$$
$$\overline{u}_2 := blind(u_2, b_2, K_2^{pub})$$
$$\overline{u}_3 := blind(u_3, b_3, K_4^{pub})$$

So far, the **Blinded Unique Donor Identifiers** do not carry information about their value. The *intended effective value is now indicated* by grouping each **Unique Donor Identifier** with the according hash of the **Donation Unit** public key K_x^{pub}. Resulting in a **Blinded Unique Donor Identifier Key Pair** (**BKP**)

It is only the *intended effective* value because the value will only be attributed later on with the signature of the Donau.

*Note: The public key is not in relation with the sequential index of the **BKP**, it only relates to the value of the pair!*

Blinded Unique Donor Identifier Key Pairs $\overline{m}u_1, \overline{m}u_2, \overline{m}u_3$

$$\overline{\mu}_1 := \langle \overline{u}_1, h(K_1^{pub}) \rangle$$
$$\overline{\mu}_2 := \langle \overline{u}_2, h(K_2^{pub}) \rangle$$
$$\overline{\mu}_3 := \langle \overline{u}_3, h(K_4^{pub}) \rangle$$

These individual **BKP**'s are then put in an array of **BKP**'s $\vec{\mu}$

$$\vec{\mu} := \langle \overline{\mu}_1, \overline{\mu}_2, \overline{\mu}_3 \rangle$$

The donor sends the array of **BKP**'s $\vec{\mu}$ as well as the corresponding **payment** to the charity.

4.2.3 Charity receives donation

Upon receiving the **BKP**'s $\vec{\mu}$ with the corresponding payment the charity has to verify that the amount requested (based on the **Donation Unit** public key hash $h(K_x^{pub})$) is **lower or equal** to the effective amount of the donation.

If the payment was successful with the correct amount present, the charity signs (using EdDSA) a structure containing all unsigned **BKP**'s $\vec{\mu}$ coming from the donor.

Signing the array of BKP's:

$$\sigma_c = sign(\vec{\mu}, C^{priv})$$

The charity sends the **BKP**'s $\vec{\mu}$ and the signature σ_c to the Donau.

4.2.4 Donau creates donation receipt material

The Donau now has received the **BKP**'s $\vec{\mu}$ previously sent by the charity. The Donau must ensure that the charity signature is valid.

Verifing the charity signature σ_c:

$$verify(\vec{\mu}, \sigma_c, C^{pub})$$

Once verified the Donau has to check for any legal restrictions such as the yearly donation limit per charity. Then the Donau increments the current amount of the donations received per year of the charity. This value is increased by the total amount of the **Blinded Unique Donor Identifier (BUDI)**'s, if the increment does not exceed the annual limit.

After that the Donau blind signs all the **BUDI**'s using the **Donation Unit** private keys K_x^{priv} matching the public keys used in the hash $h(K^{pub})$ which was inturn used in the **BKP**'s.

Donau blind signing Blinded Unique Donor Identifiers $\overline{u}_1, \overline{u}_2, \overline{u}_3$:

$$\overline{\beta_1} = blind\_sign(\overline{u}_1, K_1^{priv})$$
$$\overline{\beta_2} = blind\_sign(\overline{u}_2, K_2^{priv})$$
$$\overline{\beta_3} = blind\_sign(\overline{u}_3, K_4^{priv})$$

The signatures $\overline{\beta_1}, \overline{\beta_2}, \overline{\beta_3}$ are then sent back to the charity which in turn forwards them to the donor. This is done out of simplicity as the charity has already a secure channel open with the donor, eliminating the need to open another channel.

4.2.5 Donor receives donation receipt material

Upon receiving the Donau signatures $\overline{\beta_1}, \overline{\beta_2}, \overline{\beta_3}$ via the charity, the Donor checks if the blind signatures over the **Blinded Unique Donor Identifiers** $\overline{u}_1, \overline{u}_2, \overline{u}_3$ are valid:

$$verify\_blind(u_1, \overline{\beta_1}, K_1^{pub})$$
$$verify\_blind(u_2, \overline{\beta_2}, K_2^{pub})$$
$$verify\_blind(u_3, \overline{\beta_3}, K_4^{pub})$$

Once verified the donor unblinds the signatures of the **BUDI**'s to get the signatures over the **Unique Donor Identifier (UDI)**'s. This results in a collection of **Donation Receipt (DR)**'s each consisting of the **UDI**, the signature β and the hash of the **Donation Unit** public key $h(K_x^{pub})$.

Donor unblinds Donau signatures $\overline{\beta_1}, \overline{\beta_2}, \overline{\beta_3}$:

$$\beta_1 = unblind(\overline{\beta_1}, b_1, K_1^{pub})$$
$$\beta_2 = unblind(\overline{\beta_2}, b_2, K_2^{pub})$$
$$\beta_3 = unblind(\overline{\beta_3}, b_3, K_4^{pub})$$

Donor creates the final Donation Receipts r_1, r_2, r_3

$$r_1 = \langle UDI_1, \beta_1, h(K_1^{pub}) \rangle$$
$$r_2 = \langle UDI_2, \beta_2, h(K_2^{pub}) \rangle$$
$$r_3 = \langle UDI_3, \beta_3, h(K_4^{pub}) \rangle$$

These **Donation Receipt (DR)** are then stored on the donors device.

4.2.6 Donor requests a donation statement from the Donau

To make the donations tax deductable the donor needs to have a final **Donation Statement** which can be sent to the tax authority. To get the **Donation Statement** the donor sends the **Donation Receipts** $\{r_1, r_2, r_3\}$ accumulated throughout the year to the Donau. This can be done multiple times during the year. It is not done automatically as to obtain *unlinkability* between the *issuance* of the **Donation Receipts** (which happens upon donation) and their *submission* for the **Donation Statement**.

Once the Donau receives the **Donation Receipts** $\{r_1, r_2, r_3\}$ it has to check that for each **Donation Receipt**:

- the public key K_x^{pub} is known.
- the signature β is correct using the corresponding public key K_x^{pub}.
- the **Donor Identifier** is the same as in other **Donation Receipts**. (With multiple wallets each wallet must simply obtain a separate **Donation Statement**)
- the `nonce` is unique and was not used before by the donor for the corresponding year.

The Donau then signs over the total `amount` donated by the donor, the current `year` and the **Donor Identifier**. This results in a final signature called the **Donation Statement** which is then sent back to the donor.

Donau creates Donation Statement σ_s:

$$\sigma_s = sign(\langle i, \texttt{amount}_{Total}, \texttt{year} \rangle, D^{priv})$$

4.2.7 Donor sends final statement to a validator

The Donor uses the **Donation Statement** to create a QR-Code which then can be included in the tax declaration.

Donor generates a `QR` code which contains the **Donation Statement**:

$$\texttt{QR} = \langle \texttt{taxid}, \texttt{salt}, \texttt{year}, \texttt{amount}, \sigma_s \rangle$$

The validator at the tax office then scans the QR code and verifies the **Donation Statement Signature** σ_s.

$$verify(\langle i, \texttt{amount}_{Total}, \texttt{year}) \rangle, \sigma_s, D^{pub})$$

Chapter 5

Implementation

5.1 System Architecture

As the charity backend and donor wallet implementation are not yet developed the following architecture is reduced to the Donau backend.

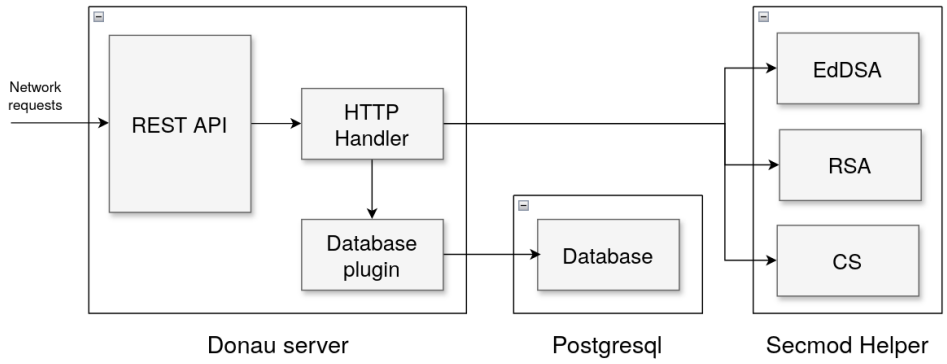


Figure 5.1: Donau system architecture

The Donau backend implements the REST API and HTTP handler which communicates with the database plugin. The postgresql database is further described in section 5.2.3 of the thesis. The HTTP handler includes a key handler that interacts with the three secmod processes. The secmod processes generate the keys. Only they have access to the private keys.

5.2 Donau

The Donau is written in C as it reuses parts of the codebase from the exchange of GNU Taler (see section 2.5 for more information about GNU Taler). The Donau

has a similar architecture and uses crypographic blinded signatures in a similar way as the exchange does.

5.2.1 REST API

The detailed REST API specification of the Donau backend is publicly available under the following URL: `https://docs.taler.net/core/api-donau.html`. The following are the main API endpoints:

`/keys`

The `GET /keys` request returns all valid donation unit public keys offered by the Donau, as well as the Donau's current EdDSA public signing key. Donation unit keys are used by the Donau to sign blinded messages for an issue receipt request. The signing key is primarily used to create the donation statement signature for the donor (see section 4.2.6).

The following is an example response of a `curl 127.0.0.1:8080/keys` command. Some parts of the following example responses are truncated (denoted by the three dots '...') to make them more readable.

```
{
  "version": "0:0:0",
  "base_url": "http://localhost:8080/",
  "currency": "EUR",
  "signkeys": [
    {
      "stamp_start": {
        "t_s": 1717069556
      },
      "stamp_expire": {
        "t_s": 1718279156
      },
      "key": "CFV2PY8164E231XZSQK30K8R6CBQ..."
    },
    {
    ...
    }
    ],
    "donation_units": [
    {
      "donation_unit_pub": {
        "cipher": "RSA",
        "rsa_public_key": "020000YC7XK99S..."
      },
      "year": 2024,
      "lost": false,
```

```
      "value": "EUR:5"
    },
    {
      "donation_unit_pub": {
        "cipher": "CS",
        "cs_public_key": "7SKRQGBSEPBG24..."
      },
      "year": 2024,
      "lost": false,
      "value": "EUR:1"
    },
    {
    ...
    }
    ]
}
```

`/charities`

In order for a charity to be able to issue receipts by a specific Donau it must be registered by this Donau. To do so the Donau provides an API to manage charities. It is expected that only the Donau administrator can manage the registered charities. The charity itself should be able to request their issued donation receipt to keep track of the set donation limit. The response includes the maximum donation amount and the current donated amount for the charity of the current year.

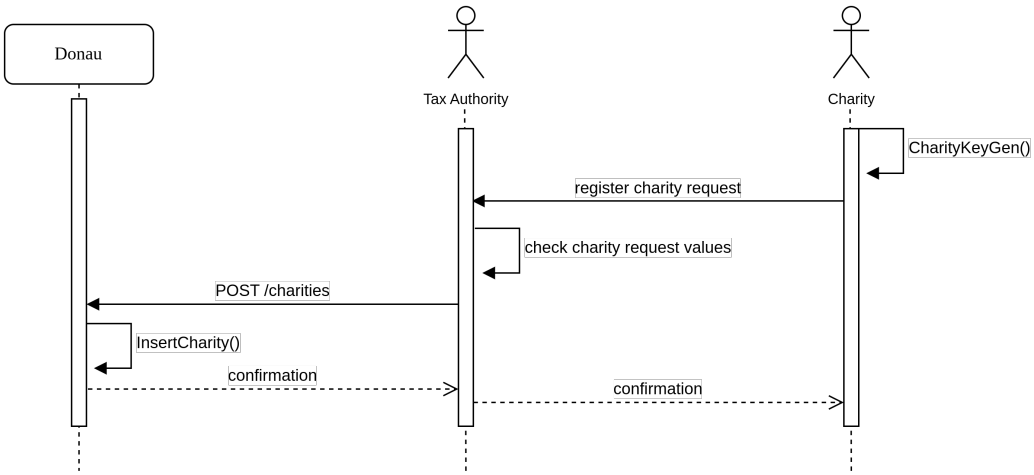


Figure 5.2: The tax authority registers a new charity in the Donau

The following is an example response of a `curl 127.0.0.1:8080/charities` com-

mand. There is only one charity named `example` registered with a donation limit of 10 euros.

```
{
  "charities": [
    {
      "charity_pub": "ABETNXT9ZF606FRF3WD5...",
      "url": "example.com",
      "name": "example",
      "max_per_year": "EUR:10",
      "receipts_to_date": "EUR:0",
      "current_year": 2024
    }
  ]
}
```

To insert a charity a `POST` request can be sent using `curl -d @charity.json -X POST http://127.0.0.1:8080/charities`.

```
{
  "charity_pub": "ABETNXT9ZF606FRF3WD5...",
  "charity_name": "mycharity",
  "charity_url": "mycharity.example.com",
  "max_per_year": "EUR:1000",
  "receipts_to_date": "EUR:0",
  "current_year": 2024
}
```

charity.json

The response consists of the charity ID generated by the database.

```
{
  "charity-id": 1
}
```

`/batch-issue`

Only recognized charities are allowed to issue receipts for their donors (see section 3.1). A `POST` issue receipt request includes an array of `BKP`s. A `BKP` consists of a `BUDI` and a hash of a public donation unit key (see section 4.1). The charity signs the request with its own EdDSA private key. The corresponding public key was given to the Donau in the registration process of the charity. After the Donau checked the signature from the charity it signs the `BUDI`s with the corresponding donation unit private key. Before the signatures are returned to the charity the Donau saves a hash of the request and all donation unit signatures to make the request idempotent (see section 5.2.3).

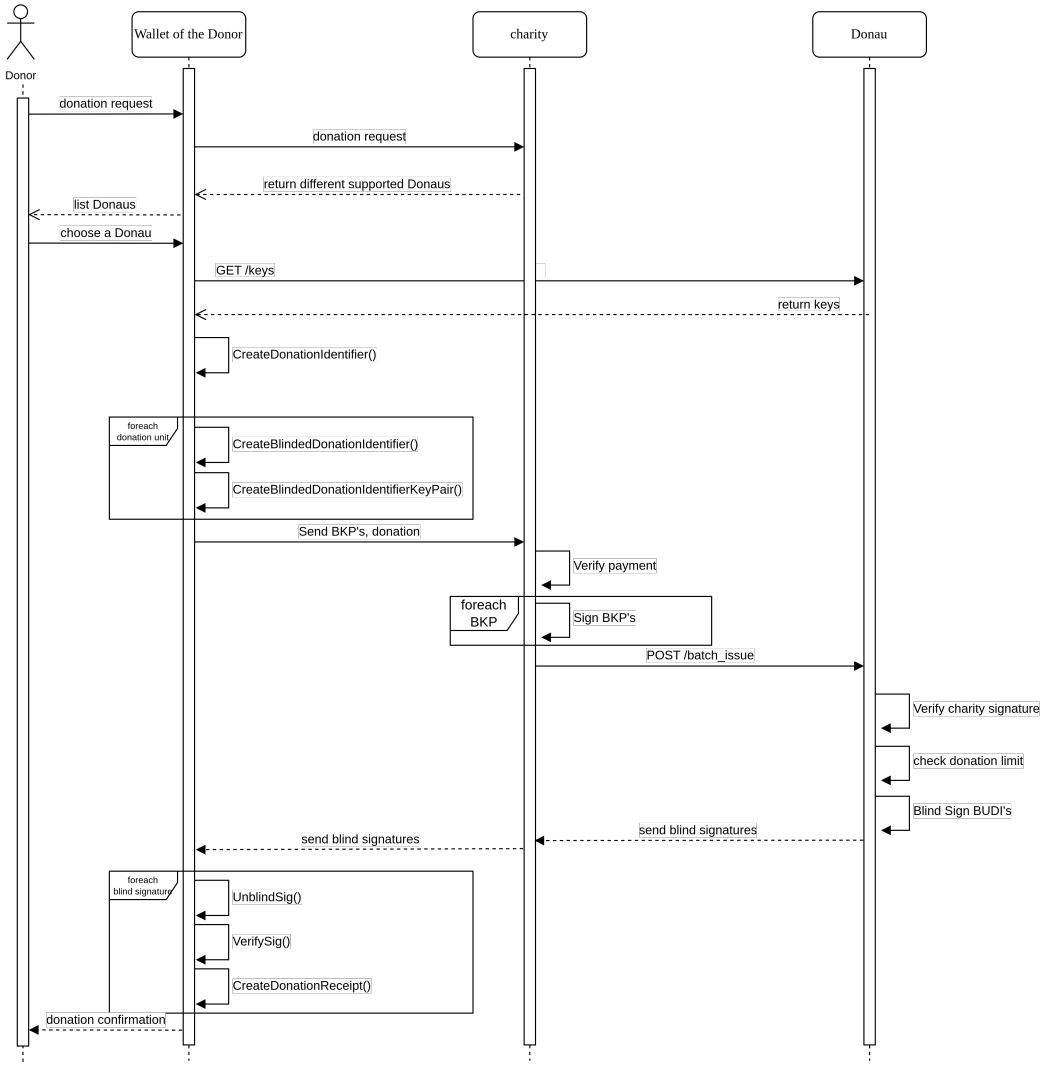


Figure 5.3: Flow of the issue receipt process

The following is an example response of a
`curl -d @issue.json -X POST http://127.0.0.1:8080/batch-issue/1` request. The number at the end of the URL is the charity ID.

```
{
  "budikeypairs": [
  {
    "h_donaton_unit_pub": "130C2KDHTAFDQFB8XED...",
    "blinded_udi": {
    "cipher": "RSA",
    "rsa_blinded_identifier": "AXPTEE24W28S9XN..."
    }
  }
  ],
    "charity_sig": "JEJ0QMDXD416XKSK1SG0DETJEH...",
  "year": 2024
}
```

issue.json

```
{
   "blind_signatures": [
     {
      "blinded_signature": {
      "cipher": "RSA",
      "blinded_rsa_signature": "16XHNWSCDRVKHF..."
       }
     }
   ],
   "issued_amount: "EUR:15"
}
```

`/batch-submit`

The batch-submit route is used by the donor to summarize their donation receipts into one donation statement EdDSA signature. The request is composed of the donation receipt (see section 4.1), the corresponding year and the hash of the salted tax ID. When processing the request the Donau checks the validity of the donation receipts and searches after more saved donation receipts made in the requested year. The EdDSA signature over the total amount of the value of the donation units of all donation receipts of the year, the hash of the salted tax ID and the year forms

the donation statement. The donation statement and the receipts are stored in the Donau database (see section 5.2.3).

`/donation-statement`

The donation statement will not be returned after a submit request, a donation statement get request can be made for a specified year and tax ID.

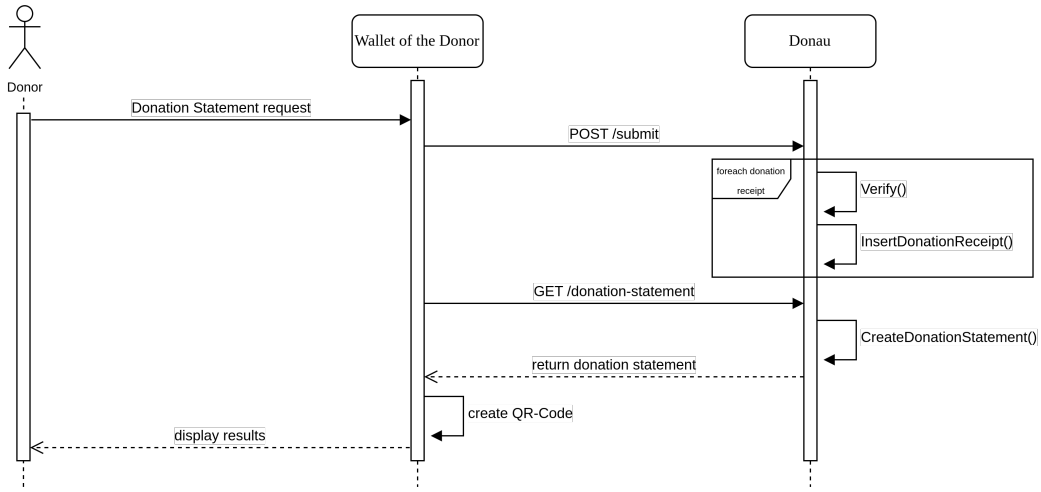


Figure 5.4: Donor requests a donation statement from the Donau

The following is an example of a
`curl -d @submit.json -X POST http://127.0.0.1:8080/batch-submit` request. If successful, the Donau returns the `HTTP 201` status code with an empty response.

```
{
  "h_donor_tax_id": "N2NYR2SFNGZSS388R2SB0VK...",
  "donation_year": 2024,
  "donation_receipts": [
  {
    "h_donaton_unit_pub": "130C2KDHTAFDQFB8X...",
    "nonce": "JEQC39G",
    "donation_unit_sig":
    {
    "cipher": "RSA",
    "rsa_signature":  "GQBXPNE4JT5W53T3CVP6E..."
    }
  }
  ]
}
```

submit.json

The following is an example response of a
`curl http://127.0.0.1:8080/donation-statement/2024/N2NYR2SFNGZSS388R2SB...`
request.

The last parameter of the URL is the salted hash of the donor tax ID.

```
{
  "total": "EUR:15",
  "donation_statement": "C1JVDP25AR001W5AHMAZ...",
  "donau_pub": "63f62b7901311c2187bfcde6304d1..."
}
```

5.2.2 Donau client

The REST client removes some of the complexity of sending requests to the Donau Server. It converts request parameters into JSON and parses JSON responses into a usable C format. What the exact queries are and how they look like is already described in chapter .

5.2.3 Donau database

The Donau database contains five tables as shown in figure 5.5. The `donation_units` and `donau_sign_keys` table store the keys necessary for signing and creating donation receipts. Donation receipts that are issued to be signed by the donau are stored in the `receipts_issued` table while the receipts that are already signed are stored in the `receipts_submitted` table. The `history` table keeps the donation records of the past years.

charities

Each registered charity has an entry in this table. There may be a donation limit imposed by local law which prevents further donations if the limit is reached.

- `charity_id`: Unique ID generated by the database.
- `charity_pub`: Charity EdDSA public key
- `charity_name`: Name of the charity
- `charity_url`: Charity URL
- `max_per_year`: The annual donation limit according to local law.
- `receipts_to_date`: The current amount of donations in the current year. Reset to 0 when incrementing the `current_year`.

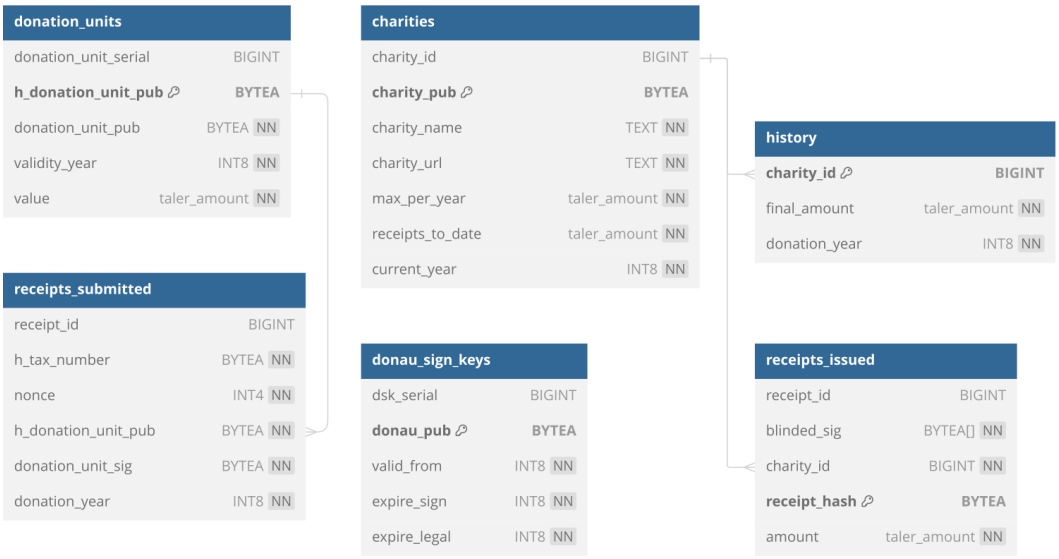


Figure 5.5: Donau database model (generated by `https://dbdiagram.io/`)

- `current_year`: Current year

donation_units

Table containing all the valid donation units the Donau knows about.

- `donation_unit_serial`: Unique ID generated by the database.
- `h_donation_unit_pub`: Hash value of the donation unit public key `donation_unit_pub`
- `donation_unit_pub`: The donation unit public key. Is either an RSA or CS public key.
- `validity_year`: The year, for which the donation unit is valid.
- `value`: The amount and currency that this donation unit represents.

donau_sign_keys

Contains all Donau EdDSA signing keys.

- `dsk_serial`: Unique ID generated by the database.
- `donau_pub`: Donau EdDSA public key.
- `valid_from`: Year the signing key becomes valid.
- `expire_sign`: Year the signing key becomes invalid.
- `expire_legal`: Year the signing key legally expires.

receipts_issued

Contains all issued donation receipts sent to the Donau.

- `receipt_id:` Unique ID generated by the database.
- `blinded_sig:` Array of blinded signatures. These are the `BKP`'s the Donau blind signed.
- `charity_id:` The ID of the charity that received the donation.
- `receipt_hash:` Hash value over all the blinded donation receipt received plus the hash of the donation units public key.
- `amount:` The amount and currency this donation receipt contains.

receipts_submitted

Contains all submitted donation receipts sent to the Donor. By storing the signature `donation_unit_sig`, the idempotentcy of the API is kept in case the private key is replaced.

- `receipt_id:` Unique ID generated by the database.
- `h_tax_number:` The hash of the tax number and salt.
- `nonce:` The nonce used in the `Unique Donor Identifier`
- `donation_unit_pub:` Reference to public key used to sign.
- `donation_unit_sig:` The unblinded signature the Donau made.
- `donation_year:` The year the donation was made.

history

History of the yearly donations for each charity. This data provides a record of donations each year. It could also provide valuable information that could be used in statistics to analyze general donations over the year.

- `charity_id:` Unique ID generated by the database.
- `final_amount:` The final amount that was donated to the charity
- `donation_year:` The year in which the donations where made.

5.3 Android Verification App

The Android app is part of the verification process used by the tax authority to check the donation statement (see 4.2.7).

The app decodes the received QR code from the donor, parse the signing values and the signature and use them to verify the signature. At the end, the values and the status of whether the signature is valid are displayed. The arguments of the QR code are defined in chapter 4.2.7 which have to be separated with a delimiter. The delimiter depends on the encoding method for the binary values. Since the QR code should be kept as small as possible, base64 would be a good choice. With base64 a colon, for example, can be used as a delimiter. Colons are not available in the base64 alphabet. The base64 encoding allows the QR code to be alphanumeric encoded[1]. This enables to use more characters in a single QR code.[10]
A possible QR code string specification with colons as delimiter could look like this:

$$YEAR : TOTALAMOUNT : TAXID : TAXIDSALT : ED25519SIGNATURE$$

In order to correctly verify the signature everything have to be in form and order. As the tax ID and the tax ID salt were used hashed for the signing, this have to be repeated. Every signature in the Taler ecosystem uses unique signature codes to to avoid misuse.

[1] alphanumeric encoded QR codes have a capacity of up to 4296 characters and support only a few special characters

Chapter 6

Results and Future work

6.1 Results

Currently the Donau REST API is fully implemented. The Donau can manage any number of charities using the `/charities` endpoint. All the keys used for signing and blind signing are managed by the Donau together with the Secmod helpers.

Overall the Donau is able to issue donation receipts and provide the necessary donation statement to the donor, all while keeping the data anonymized and protecting the privacy of the donor. It is also worth mentioning that the unusual cryptography of blinded signatures does not effect the performance. With the binding of the tax number to the donation receipts and the signature of the tax authority with year-dependent keys, the receipts are absolutely bound to a donor and to a year and cannot be falsified or imitated without falsifying the signature. Therefore donation fraud can be prevented. By summarizing the receipts into one single QR-Code, the user convenience for the tax authority and for the donor could be improved.

Important components that are needed to operate the Donau are not yet implemented. This includes the charity side and donor client side. The Android verification app is only partially implemented. Although test where written to ensure that the Donau endpoints operate as expected, there are still some other bugs and most likely also unknown bugs, not yet found.

The tax authority emphasizes user convenience and simplicity in a system like the Donau. The tax authority also mentioned the challenges that arise when operating such a system in the federalism. Each party often has different requirements that a system like the Donau should fulfill. Although the Donau is in its early stages and the prototype has not yet been deployed, the tax authority Zürich definitely sees potential in the user convenience side of the Donau.

6.2 Future work

6.2.1 Client implementation

The donor client implementation needs to be implemented in the Taler wallet. This is a necessary step to be able to use the Donau together with the Taler payment system. Then donations could be made fully anonymous. The necessary functionality must be implemented in the `taler-wallet-core`. This includes the option to make donations and request for the final donation statement. If the donor wants to be able to deduct the donations from taxes, the user is asked to input his tax number. Hidden from the user are the generation of the various elements such as `DI`, `UDI`, `BUDI` and `BKP`. The blinding and unblinding implementation must also be present.

6.2.2 Charity backend

Each registered charity needs to communicate with the donors and the Donau. The Taler merchant backend needs to be modified to incorporate the charity backend logic. To do this it is necessary to add a charity information table to the merchant database. This table should contain information like the charity public key, domain, base URL, currency and instance. The instance being a number as there could be different instances running. The merchant backend needs to be extended to incorporate the charity logic. Meaning the signing of BKP's sent to the charity and also the communication with the donor. The charity should return a list of Donaus where the charity is registered, so that the donor can choose the appropriate Donau for tax deduction. A system similar to the one described in the thesis of Christian Blättler is to be implemented [11].

6.2.3 Donau SPA

For the administrator a single page application is needed to comfortably manage the charities. This would include functionality to add, remove and modify charities. This setup could include a reverse proxy, which authenticates the Donau admin. Once the identity has been confirmed the proxy can access the Donau endpoint to manage a charity. The proxy would hold a bearer token, in order to authenticate itself.

6.3 Conclusion

Tax transparency is a crucial aspect of a well-functioning society, as it fosters trust, accountability, and fairness in the relationship between the state and its citizens. Transparency allows for public scrutiny, which can help identify inefficiencies, loopholes, or instances of corruption within the tax system, ultimately leading to necessary reforms and improvements.

Unfortunately, it occurred to us that some tax departments still rely on outdated, paper-based systems or legacy software, hindering their ability to operate efficiently and transparently. The lack of digitization not only slows down processes but also increases the risk of errors, data inconsistencies, and potential mishandling of sensitive information.

The adoption of free and open-source software (FOSS) presents a compelling solution. FOSS solutions offer several advantages, including cost-effectiveness, customizability, and the ability to scrutinize the underlying code for security and transparency purposes. By embracing FOSS, tax departments can modernize their systems, streamline processes, and enhance data integrity, ultimately fostering greater transparency and trust with the public.

The Donau system supports tax justice. The Donau not only manages to anonymize user data, so that everyone is treated equally, but also helps the donor to make use of their right to deduct donations from taxes. Because the donation receipts are stored in a central location and can even be deposited in the Donau, the likelihood of losing or forgetting to submit the receipts is reduced.

Of course, bureaucracy and federalism can hinder the introduction of such a system. Especially when it comes to the recognition of charities. But the Donau could provide a first step into a more standardized system that handles donations in a secure and privacy preserving way.

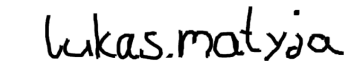
Declaration of Authorship

I hereby declare that I have written this thesis independently and have not used any sources or aids other than those acknowledged.

All statements taken from other writings, either literally or in essence, have been marked as such.

I hereby agree that the present work may be reviewed in electronic form using appropriate software.

June 13, 2024



Lukas Matyja

Johannes Casaburi

Bibliography

[1] The Parliament of Australia. Consolidated version of the treaty on the functioning of the european union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT, 2012.

[2] Rajeev Sobti and Geetha Ganesan. Cryptographic hash functions: A review. *International Journal of Computer Science Issues, ISSN (Online): 1694-0814*, Vol 9:461 – 479, 03 2012.

[3] NIST. Hash functions. https://csrc.nist.gov/projects/hash-functions#approved-algorithms.

[4] Niels Duif Daniel J. Bernstein. High-speed high-security signatures. https://ed25519.cr.yp.to/ed25519-20110926.pdf, 2011.

[5] Gian Demarmels, Lucien Heuzeveldt. Adding schnorr's blind signature in taler. https://taler.net/papers/cs-thesis.pdf, 2022.

[6] Georg Fuchsbauer, Antoine Plouviez, and Yannick Seurin. Blind schnorr signatures and signed elgamal encryption in the algebraic group model. https://eprint.iacr.org/2019/877, 2019.

[7] Nigel P. Smart and Nigel Paul Smart. *Cryptography made simple*. Information security and cryptography. Springer, 2016.

[8] Lucien Heuzeveld Gian Demarmels. Adding schnorr's blind signature in taler. https://taler.net/papers/cs-thesis.pdf, 2022.

[9] Gnu taler: Features. https://taler.net/en/features.html.

[10] DENSO WAVE. Information capacity and versions of the qr code. https://www.qrcode.com/en/about/version.html.

[11] Christian Blättler. Privacy-preserving subscriptions and discounts. https://taler.net/papers/subscription-discounts-thesis.pdf, 2024.

List of Figures

Glossary

Donau	Short for donation authority. Donau is used as project name. The hole system is called Donau system and the Server of the tax authority is also called Donau.
charity	If donations to an organization or a part of it are tax deductible for a donor, then this organization or this part is a charity for this Donau.
Taler	The GNU Taler payment system.
nonce	Number used once, a high-entropy value which must not be reused.
salt	A high-entropy value added to the hash function input to prevent brute-force attacks .
ID	Unique identifier.
DU	Donation unit, used to represent the value and currency of coins.
DI	Donor identifier, a salted hash of the donor tax number.
UDI	Unique donor identifier, donor identifier combined with a unique nonce.
BUDI	Blinded unique donor identifier, result of blinding a UDI.
BKP	Blinded unique donor identifier key pair, a tuple of the corresponding hash of the DU public key and the BUDI.

Appendix

Interview transcript

Date: 18. April 2024
Tax Authority Zürich (interviewees): I1, I2, I3, I4
BFH (interviewers):

- Lukas Matyja (LM)
- Johannes Casaburi (JC)
- Christian Grothoff (CG)
- Emmanuel Benoist (EB)

(The following transcript has been slightly adapted for readability.)

LM: (...) Wir würden gerne erfahren, wie überhaupt so die momentane Situation aussieht punkto Spendenbelege, wie ihr die Spendenbelege prüft und ob es da Unterschiede bei der Höhe der Spendenbeträge gibt und wie diese dann geprüft werden?

I1: I2, willst du etwas dazu sagen?

I2: Ja, also konkrete Zahlen haben wir nicht, oder habe ich zumindest gerade keine. Also man kann sagen, dass wir grundsätzlich Kleinspenden nur bei Verdacht überprüfen.

CG: Ja gut. Aber wie wird das überprüft? Das kann ich mir gar nicht vorstellen.

I2: Indem man überprüft, was auf der Quittung steht. Es wird ja eine Quittung ausgestellt.

CG: Aber das ist ja nur auf Papier. Da kann ich ja auch eine 0 dranhängen.

I2: Ja, kann man. Solche Betrugsfälle sind wirklich selten. Also es kommt so gut wie nie vor, weil die Konsequenzen entsprechend hoch sind. Und die Steuerersparnis, die man da rausholt ist eher klein. Also das ist ein Phänomen, dass wir in der Praxis so gut wie nie sehen.

CG: Sie sehen es nicht, oder können Sie es gar nicht erkennen? Wie würden Sie es denn erkennen?

I2: Ja, wenn es ungewöhnlich ist. Ist jetzt schwer zum Beantworten, aber mir sind von den wenigen Betrugsfällen, die ich in den 15 Jahren, seit ich bei der Steuerverwaltung arbeite, mitbekommen habe, waren Spenden kein Thema. Es ist mir kein einziger Fall bekannt.

I1: Aber theoretisch haben Sie natürlich recht, Herr Professor, das kann gemacht werden. Es kann jemand dieses Dokument verfälschen, das wäre dann nicht nur Steuerbetrug.

CG: Aber auch Dokumentenfälschung, dass das kriminell ist, ist nicht die Frage.

I1: Und und die die Realität ist natürlich so, dass wenn Sie jemanden haben, der ein gewisses Einkommen hat, dann gibt es einen prozentualen Maximalbetrag, den er ja überhaupt als Spende spenden kann. Und wenn Sie dort jemanden haben, der immer an der Obergrenze ist, wird denke ich einmal in 5 Jahren möglicherweise bei grossen Beträgen eine kurze Prüfung gemacht, nämlich die, dass man sagt, schick mir doch schnell den Bankbeleg, wo du das eingezahlt hast. Und wenn das dann auffliegt, dann greifen wir mittels Nachsteuer und Strafsteuerverfahren eh Bussenverfahren, dann greifen wir die Jahre zurück auf, also auch die definitiv erfolgte Steuerveranlagung. Dies kann dann nochmal zur Strafsteuerthematik überprüft werden und dann gehen wir in der Regel nochmal die ganze Steuererklärung durch, weil möglicherweise gibt es auch andere Elemente, die nicht korrekt deklariert wurden. Und da tatsächlich, also da ist uns jetzt nichts so in dem Sinn bekannt, aber theoretisch, wenn sie das natürlich jetzt so wie in ihrer Idee digital verifizieren, beziehungsweise uns würde es dann schon helfen, wenn die gemeinnützige Organisation natürlich dort ein Qualitätssiegel, wie sie es jetzt eigentlich auch ausgedacht haben, übermittelt und das dann direkt an uns übermittelt wird oder noch schöner wäre es, wenn das in einem QR Code zusammengefasst ist, dann müssen wir das nur einmal anschauen. Es würde aber auch der Betrag reichen. Weil wie schon gesagt, im Spendenbereich macht es einfach wenig Sinn, dort wirklich umgangssprachlich zu bescheissen. Wenn Sie das wirklich machen wollen, machen Sie das an anderen Orten, wo es sich dann steuerlich lohnt.

CG: Okay ich bin da vielleicht nicht kreativ genug im Bezug auf Steuerbetrügereien.

I1: Das ist auch gut so.

(...)

CG: Genau. Aber das, was ich primäre höre, ist sozusagen, was Sie sagen, bei der Überprüfung würde der Bankbeleg überprüft, das war das Stichwort, was ich mir aufgeschrieben habe, das heisst, wenn ich dann sage, ich habe bar gespendet, was machen Sie dann?

I1: Dann sind Sie nachweispflichtig, also bei Abzügen grundsätzlich. Das ist ein

Grundsatz im Steuerrecht, Sie sind nachweispflichtig. Sie sind Beweispflichtig. Das heisst, wenn ich Sie frage, wie haben Sie das gezahlt und Sie sagen bar. Der Klassiker ist der Heilsarmee Topf. Ich habe da 100'000 Franken reingelegt und kann das nicht belegen. Dann können wir in der Regel dann sagen, gut, dann können wir den Abzug so nicht anerkennen.

CG: Aber wenn ich die Quittung über die hunderttausend habe, dann habe ich ja einen Beleg.

I1: Wenn wir dann aber die Höhe der Spende anzeifeln, dann werden wir den Zahlungsfluss überprüfen. Das macht man üblicherweise mit dem Einverlangen eines Bankbeleges und wenn Sie den nicht nachweisen können und jetzt ehrlich gesagt oder wenn Sie jedes Jahr 20 Franken an Greenpeace spenden und das weiter so machen, dann ist es wahrscheinlich OK. Da wird niemand überprüfen. Aber wenn Sie 10 Jahre lang 20 Franken und nachher 20 000 spenden, dann werden wir nachfragen. Und dann werden wir möglicherweise schauen, ist das überhaupt möglich, wieviel verdienen Sie, wie zeigt sich das in ihrer Bilanz oder, und da kann man dann schon nachgreifen und wenn Sie es uns nicht schlüssig beweisen können, werden wir das ablehnen. Und wenn Sie das nicht akzeptieren wollen, können Sie Einsprache machen und dann geht es dann über die Rechtsmittel weiter bis ganz nach oben bis zum Bundesgericht. Das wird dann sicherlich nichts mehr.

CG: Ich habe jetzt noch eine zweite Sache, das ist die Bilanzprüfung, das heisst Sie prüfen die Plausibilität. Dass ich sozusagen so viel Geld entweder weniger auf dem Konto habe ist am Ende ja dann die Antwort, auch wenn ich bar gespendet habe, muss das Geld ja das Bargeld hergekommen sein.

I1: Ja, genau.

CG: Genau. Also ich denke das sind die beiden Stichworte was bisher eben passiert ist. Einmal der Bankbeleg als Beweis. Bargeld wahrscheinlich gibt es da eine Plausibilitätsgrenze. Ich habe eine Millionen bar gespendet, glaubt mir dann keiner. Beziehungsweise da muss ich eben nachweisen, dass ich die Million vorher vom Konto abgeholt habe.

I1: Sie sagen es genau. Oder wenn Sie dann schlüssig nachweisen können, dass Sie zu diesem Datum auf die Bank und dann wieder zur Topfkollekte gegangen sind. Dann können wir es immer noch ablehnen, aber die Kausalität ist dann mindestens nicht ganz unwahrscheinlich, oder?

CG: Ja, genau, und die Strafbarkeit ist auf jeden Fall reduziert. Es muss ja dann vor Gericht geklärt werden, ob es plausibel war, dass ich eine Million an Bargeld abgeholt habe.

I1: Genau das können Sie dann in einem Einspracheverfahren im Rekursverfahren dann geltend machen und dann können die Richter, die unabhängigen Richter, können das natürlich dann beurteilen.

CG: Gut, aber ich denke sind dann für die Bachelorarbeit die beiden entscheidenden Stichworte bisher. Es findet eben eine Bankbelegprüfung statt, falls eine Banktransaktion da ist und eine Bilanzprüfung vom Cashflow her, ob die Spende plausibel ist und da reinpasst.

I1: Genau, da gibt es andere Sachverhalte, wo das auch noch notwendig ist. Aber das ist natürlich so. Die Plausibilität spielt schon eine Rolle.

CG: Gut.

LM: Dann eine weitere Frage unsererseits noch. Wissen Sie ungefähr wie viele Steuergelder dem Kanton Zürich durch Spendenbetrug entgehen? Also ich habe jetzt schon ein bisschen herausgehört, wahrscheinlich nicht, aber hätten Sie eine Schätzung?

I1: Wenn wir das wüssten, würden wir es Ihnen nicht sagen.

CG:[lacht]. Okay.

LM: Okay ja nein, kein Problem.

I1: Es gibt gewisse Daten. Gewisse Daten werden nicht veröffentlicht, aber solche Themen würden auftauchen oder tauchen auf, wenn eben ein Steuerstrafverfahren durchgeführt wird. Und meines Wissens führen wir da aber keine Statistik über die einzelnen Einkommen, oder Abzugsklassen, die hier Betragsmässig eine Rolle spielen. Aber das können Sie sicher verifizieren. Ich glaube einmal im Jahr vielleicht, nicht regelmässig, wird das der Presse zur Verfügung gestellt. In der Regel gibt es dann ab und zu einen kleinen Presseartikel, wenn Sie da etwas finden, allenfalls gibt es da Statistiken. Mir ist das nicht bekannt, dass wir das statistisch so auswerten.

CG: Gibt es eine andere Statistik, zum Beispiel wie viele Steuern aufgrund von Spenden erstattet werden, oder reduziert werden? Also nicht betrügerisch, sondern einfach regulär.

I1: Nein, auch das. Da ist mir auch nicht bekannt, aber das wäre dann allenfalls etwas. Eine Motion, ein Postulat, ein politischer Vorstoss, der dort Auskunft haben wollte, das können Sie gut über das Internet recherchieren(...)

CG: War nur die Frage, ob die Daten vorliegen.

I1: Nein, bei uns liegen sie nicht vor, aber ich kann nicht ausschliessen, dass vor Jahren irgendwo mal ein Postulat diese Frage behandelt hat. Und dann würde man das aber auch in der Antwort der Regierung dann ablesen, was sie da haben. Es ist mir aber nichts bekannt, also ich will Sie da nicht auf Umwege schicken. Das sind Themen, die wir eigentlich nicht auswerten, weil wir steuerlich ein anderes Ziel haben. Oder, das ist einfach zulässig, dass sie solche Organisationen unterstützen, das ist der Wille des Gesetzgebers. Aber für uns natürlich im Sinn nur solange relevant, bis wir überprüft haben, ob die Spende so nach unseren Kriterien erfolgt ist, aber weitere Auswertungen sind kein Auftrag der Steuerverwaltung.

CG: Okay ja.

LM: Danke. Ja, uns würde auch noch interessieren. Jetzt, nachdem wir das System vorgestellt haben, was Sie davon halten. Oder, rein theoretisch, wenn man das bei Zürich anwenden würde. Was würden Sie sich noch von so einem System wünschen?

I3: Da kann ich vielleicht von meiner Seite etwas dazu sagen. Ich fände es wichtig, wenn dieser Beleg einen Auslesebarcode hat. So dass die Information komplett auslesbar ist. Und dass sich der Barcode an den ECH Standard hält. Kennen Sie diesen?

CG: Nein. Ich nicht.

I3: Das sind Datenstandards der Schweizer Verwaltung. Diese findet man im Internet unter ech.ch. Da werden Standards publiziert. Im Moment ist noch ein genereller Standard für 2D Barcodes in Arbeit, der sollte aber bald publiziert werden. Damit können generell PDF oder gescannte Belege in die Steuerapplikationen eingelesen werden.

LM: OK, interessant, ja.

I3: Und dann hätte ich noch eine Frage. Dieser Barcode dient ja zur Validierung. Wie funktioniert die Validierung? Also muss da noch auf den Server eine Abfrage gestartet werden oder kann der Barcode über eine Prüfziffer eigenständig validiert werden?

CG: Ein Barcode kann eigenständig validiert werden, er hat eine digitale Signatur und steht eigentlich für sich selber, da sind auch alle notwendigen Informationen: Spendernummer, Betrag, Spendenjahr sind alle codiert.

LM: Genau. Also die Signatur kann automatisch überprüft werden. Aber ja, das macht wahrscheinlich Sinn, wenn dem Steuerprüfer die Informationen angezeigt werden und er dann natürlich selber auch noch einen Plausibilitätscheck macht.

I3: Also wichtig wäre in dem Moment einfach, dass nicht auch noch der Spender anonym ist.

CG: Nein, an der Stelle nicht mehr. Die Spendenquittung waren von Anfang an an den Spender gebunden, der kann sie auch nicht jemandem einfach übertragen. Ja, also zum Zeitpunkt der Spende muss der Spender sozusagen seine Steuernummer schon festgelegt haben. Ja, und all die Spendenquittungen, die dann ausgestellt wurden sind sozusagen an diese Steuernummer geknüpft.

I3: Gut, danke.

LM: Ja, genau, und vielleicht noch zum Schluss. Rein theoretisch, wenn man so ein System umsetzen oder einführen möchte. Uns würde natürlich jetzt interessieren, was die ersten Schritte wären, die man machen müsste? Oder ich weiss nicht, haben Sie vielleicht mal ähnliche Systeme eingeführt? Wie sieht das so aus?

I4: Vielleicht noch 3 Gedanken von meiner Seite dazu. Also ich, ich muss sagen, ich hab das das erste Mal gesehen, sind einfach 3 Gedanken. Das erste: Ich finde es interessant, da muss ich ein bisschen darüber nachdenken, dass man am Anfang relativ viel Aufwand treibt, um die Bindung des Spenders als Person mit dem Beleg zu anonymisieren und zu signieren. Und wir dann im Prüfverfahren genau diesen Sachverhalt natürlich erhärten wollen und damit das anerkannt wird. Und deswegen ist das rein vom Business Prozess her, wie viel Aufwand man betreibt, etwas zu verstecken, was nachher eigentlich materiell zwingend ist, um es anzuerkennen. Den Aufwand, so treibt das, das ist einfach etwas, wo ich ein bisschen darüber nachdenken. Das zweite, was ich vielleicht so bemerken dürfte, was eben sehr interessant ist, weniger aus der Sicherheitsperspektive als aus der Benutzerperspektive, das eigentlich zum Zeitpunkt, wo ich die Spende tätige, ich etwas tue und registriere. Und wir haben natürlich gerade bei der Steuererklärung den Fall, dass ich typischerweise das Problem habe aus Benutzersicht, dass ich Ende Jahr an alles denken muss, was ich das ganze Jahr gemacht habe und deswegen sich die Synergien vielleicht weniger bei der Anonymisierung als bei der, ich sag's mal bei der User Convenience finden liessen. Und der dritte Gedanke, was auch nicht zu vernachlässigend wäre vielleicht. Es gibt ja nicht nur die Steuerverwaltung Zürich. Es gibt verschiedene in der Schweiz, die Spendenorganisationen sind natürlich in der ganzen Schweiz oder auch international tätig und die Personen sind auch in verschiedenen Zuständigkeiten, das heisst, wenn man so einfach sagt, die Steuerbehörde betreibt so ein System, stellt sich dann sofort die Frage, muss dann eine Spendenorganisation mit 25 kantonalen Steuerämtern und Sie haben gesagt, vielleicht haben wir verschiedenen IDs, je nachdem das so handhaben und das schlägt vielleicht jetzt auch ein bisschen die Brücke zu einer Einführung. Was das angeht.

CG: Also wir haben gesagt, wenn sage ich mal in der Schweiz jeder Kanton einzeln entscheidet, ob das Rote Kreuz gemeinnützig ist oder nicht. Oder andere Organisationen. Dann muss natürlich für jeden Kanton auch eine eigene Donau die Gemeinnützigkeit anerkennen und die Gemeindesituation muss dann für Steuerpflichtige im jeweiligen Kanton dann natürlich da auch bei der entsprechenden Donau sich gemeldet haben, um die entsprechenden Spendenquittungen, die in dem Kanton anerkannt werden, auszustellen. Auf der europäischen Ebene sieht es etwas anders aus. Da ist es noch etwas spassiger, da müssten nämlich die Steuerbehörden, die gemeinnützigen Organisationen aus anderen Ländern anerkennen. Laut Recht und Gesetz nach unserem Verständnis, aber gleichzeitig tun sie es nicht. Also wir hatten eben gerade das Beispiel von der NLnet Stiftung, die sagte, wir sind aus den Niederlanden, wir sind gemeinnützig und die deutschen Finanzämter machen Ärger, wir haben Spender die dann vom Pferd des deutschen Finanzamt nicht anerkannt werden, dabei müssten sie das eigentlich. Also wenn das einheitlich geregelt ist, könnte man natürlich eben auch sagen, es gibt dann eine Donau für die EU oder eine Donau für die Schweiz. Aber wenn man natürlich sagen kann: ja, aber in einem Kanton ist das eine gemeinnützige Organisation, im anderen ist es kein, da muss man natürlich auch andere Autoritäten deployen. Aber sicherlich, also es ist möglich technisch,

es ist ein bisschen natürlich auch eine rechtliche Frage, inwieweit Gemeinnützigkeit regional unterschiedlich bewertet wird. Beantwortet das die Frage so ein bisschen? Also den Kommentar? Fragen weiss ich nicht.

I4: Ja. Es war ja auch nicht wirklich eine Frage. Es war mir ein Gedanke, wo ich zum jetzigen Zeitpunkt nicht mal die Frage präzis gestellt habe, sondern es geht mehr darum, ich glaube, es sind Aspekte, die natürlich eine Rolle spielen. Der eine Aspekt ist eher, dass man, bevor wir über eine Einführung eines IT Systems sprechen, der Businessprozess, wenn ich das so sagen darf, aus Benutzersicht und von allen Beteiligten harmonisiert sein sollte. Und auf der anderen Seite, dass es eben auch die Frage gibt der Zuständigkeiten, die dann entsprechend zu harmonisieren sind. Und ich entnehme jetzt Ihren Kommentaren, dass Sie sich dem Problem oder der Herausforderung bewusst sind.

CG: Ja, das schon.

LM: Ja, also wir wissen, das ist ein langer Weg und es ist noch viel zu früh, um von einer Umsetzung zu sprechen. Aber nichtsdestotrotz wollte ich das mal ansprechen.

CG: Weil ich denke, was ich heraushöre ist, wir müssen natürlich jetzt erstmal den ersten Prototypen fertigstellen, dass es überhaupt erst mal theoretisch läuft, das ist noch Forschung und dann kann man eben gucken, ob man sagt, OK, das passt von den Prozessen her, das könnte man machen, aber es klingt jetzt erst mal, als ob Sie sagen von der User Convenience her - vereinfachen der Steuererklärung, Vereinfachung der Prüfungsvorgänge und so weiter, wäre es nicht komplett uninteressant für Sie. Höre ich jetzt mal so raus.

I1: Auf jeden Fall. Neue Ideen sind immer grundsätzlich immer mal prüfenswert und da hat es sicher einige interessante Ansätze drin. Eben, ich denke, es braucht noch einiges an Arbeit. Und aus Sicht Verwaltung natürlich dann auch eben die die Frage 26 Mal machen oder einmal machen. Und der Kanton Zürich hat natürlich gemeinnützige Organisationen, die nur im Kanton Zürich tätig sind. Die haben möglicherweise auch keine Anerkennung im Kanton Genf. Und dann haben Sie sofort aus der aus der Grossen EU die Probleme auch in der kleinen Schweiz in ähnliche Thematik, die hier auch versteckt sind, natürlich. Aber das ist der Preis eines föderalen Systemes. Das löst man dann eben technisch.

CG: Vielleicht. Vielleicht. Manchmal macht man es auch 26 mal.[lacht]

I1: Jaja genau. Auch das ist eine technische Lösung, wenn man es 26 Mal macht, verdient vielleicht jemand auch viel besser.

(...)

EB: Entschuldigung, ich hab mich ein bisschen auf ECH umgeschaut und auf der Website von ECH ist es ein bisschen leer oder gibt ein leeres Zeichen für Barcodegenerierung für Steuerbelege. Haben Sie ein Verweis, wo wir mehr finden können?

I3: Nein, wie ich gesagt habe, der Standort ist in Arbeit und sollte noch dieses Jahr publiziert werden. Der allgemeine Standard für Barcodes, Steuerbelegbarcodes, der ist noch in Arbeit, aber der kommt, man kann sich aber andere Standards anschauen, die teilweise schon den gleichen Barcode beinhalten, das wäre zum Beispiel der 196 für E Steuerauszüge Steuerdepots.

(...)