DONAU

Tax-deductable Donations

Johannes Casaburi Lukas Matyja

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

May 8, 2024

Abstract

This bachelor thesis describes and implements a theoretical concept of a donation authority system. The donation authority (Donau) is free software with a focus on privacy and anonymity and part of the GNU Taler project. It depends on the code of the GNU Taler environment, but is completely independent of the Taler payment system. An interview with a local tax authority was held to determine the current state of how donations are verified as well as the usability and possible adoption of a system like the Donau.

The Donau is operated by the tax authority and maintains a list of verified non-profit charities. The charities as well as the donors must be able to communicate with each other for the system to work. Upon making a donation to one of the charities the donor receives a so called "Donation receipt" which will be stored locally on the donor's device. Throughout this process neither the charity nor the Donau will optain any identifiable information thus making it anonymous. To make the donations tax deductable the donor needs to submit ther receipts to the Donau. Which in turn will combine the receipts in one final receipt called the "Donation statement". Upon request this will be sent to the donor in form of a QR-Code. This QR-Code can then be sent to the tax authority which verifies its validity and is then able to deduct the amount from the taxes.

Contents

Chapter 1

Introduction

1.1 Motivation

To anonymously donate to a charity and have that donation be deducted from taxes is often not possible. Large enough donations done anonymously using cash may need to be verified (if requested) when attempting to deduct the donation from taxes. The donor would then have to present some sort of evidence in form of a receipt which would deanonymize his donation to the charity. Furthermore, this process can be time consuming, involving a disproportionate amount of effort for the tax authorities.

1.2 Goals

The aim of this bachelor thesis is to assess the current situation in the area of donation deduction and to formulate and implement a solution for the problems described above. The main goals are the following:

- The Donau should enable donors to donate anonymously and still be able to deduct the amount from the taxes.
- These donations should be verfiable by simply scanning a QR-Code
- Great usability for both the donor and tax authorities to make the process as easy as possible.
- Eliminate tax fraud with donations that where not actually made

Chapter 2

Overview

2.1 The Concept

The Donau[1] environment includes three stakeholders. Donors, charities and the tax authority. The Donau server 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. See Figure 2.1 3

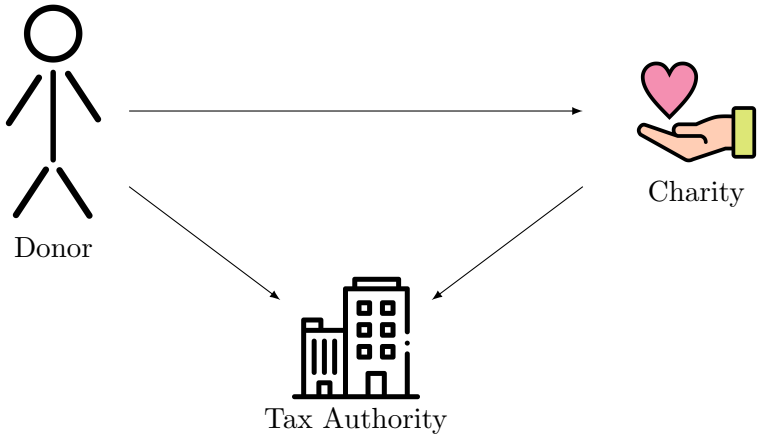

Figure 2.1: stakeholders

2.1.1 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

[1] short for donation authority

is part of the receipt request. The tax id number does not cause a problem for anonymity as the hole receipt with the id number is blinded (see section 2.x). In the picture 2.2 4 the blinded receipt is illustrated as 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 untouched request and forwards the request to the Donau. The Donau accepts only issue requests from verified charities. If this is the case, the Donau issues the actual donation receipt by signing the request. This is different from the current model where the charity issues the receipt. By shifting this task to the Donau the receipts can easily be verified and unlinks the donor from the charity which in turn provides anonymity for the donor opposite the Donau in this first step of issuing receipts.

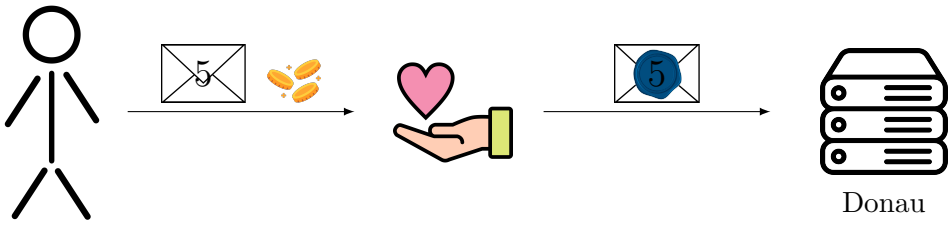

Figure 2.2: issue receipt request

Upon receiving the signed issue request from the charity, the Donau must verify the charity signature and check for any legal restrictions, such as a yearly donation limit **source!**. After successful verification the Donau creates a blinded donation receipt which is sent via charity to the Donor (see figure: 2.3 4). The donor now unblinds the signature from the Donau to make it valid for the unblinded receipt (see section 2.x). The unblinded receipt gets saved on the donors device for later. This process repeats for every donation. At the end of the year the donor may have accumulated a bunch of these donation receipts.

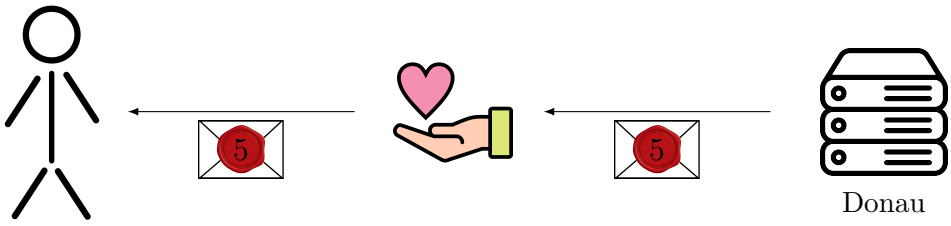

Figure 2.3: issue receipt response

2.1.2 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: 2.4 5). This step combines the amounts of the donation receipts in a single total amount. This protects the privacy of the donor because the individual donation amounts could be enough information to link with specific donations. The combination of the donation receipts makes it also easier for the manual verification besides the tax auditors. The statement signature is made besides the total amount, over the year and the tax id. The donation statement can be requested multiple times during the year for save keeping the donation receipts. The latest donation statement will always contain all the receipts of a year - the old receipts (from a previous statement) and the new donation receipts.

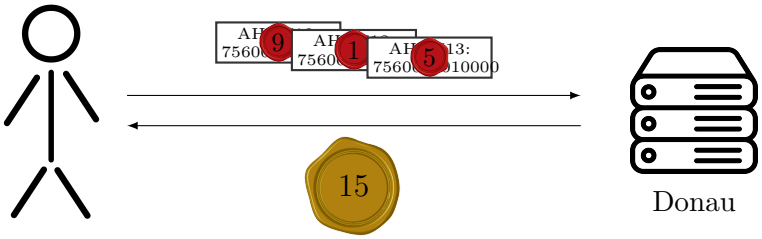

Figure 2.4: summarize receipts

2.1.3 Validation

Once the donor has received the values, he can summarize them in a QR code. The donor must submit the QR-Code with their tax return in order to claim the donation reduction (see figure:2.5 6). The final check is made by the tax auditors, 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 auditors will not have any information to what charity the donor has donated money. Everything the tax auditors know is that every donation was made to one of the approved charites in the specified year and the total amount. This way the donor could make an anonymous donation and still have enough proof to deduct the amount from taxes. By keeping track of how much money a charity has received in donations per year and how much a donor has donated throughout the year, tax fraud is essentially eliminated.

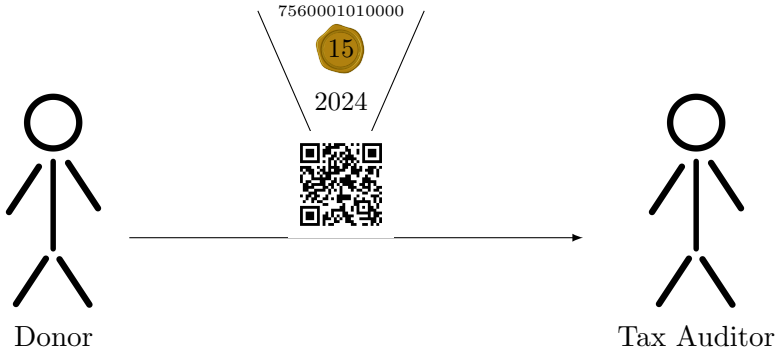

Figure 2.5: validation

2.1.4 Incorporating the Donau

Every donor is related 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 the multiple tax areas, it has to be registered by all the corresponding Donaus. To do so, the charities has to apply to the tax authority. The region for which a Donau responsible depends on the tax area of the tax authority and their reglementation of what is charitable. A Donau is maybe responsible for a geographical area like a canton, a country or even a confederation of states. Different Donaus must also be kept for different currencies, but this should not be a problem as most countries have a single currency.

Chapter 3

Cryptographic Preliminaries

3.1 blinded signatures

Chapter 4

Protocol

4.1 Notation & Definitions

4.1.1 Notation

- $\langle a, b, ... \rangle$: Pair/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**

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

  The **Donation Statement** 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**.

  These 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 splits the donation amount into a sum of **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 one **Donation Unit** of the same value is present more than once, then there needs to be a **Unique Donor Identifier** for each of the **Donation Units**.

In our example, there are 3 ***Unique Donor Identifiers****: one per* ***Donation Unit****.*

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 $h(K_x^{pub})$) for signing 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. 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 inturn forwards them to the donor. This is done out of simplicity as the charity has already a secure channel open with the donor, elmination 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** $\overline{u}_1, \overline{u}_2, \overline{u}_3$ is 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** σ_s to create a QR-Code which then can be included in the tax declaration.

Donor generates a `QR` code which contains the following:

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

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

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

Chapter 5

Implementation

5.1 Architecture

Chapter 6

Results and Outlook