TALER

Taxable Anonymous Libre Electronic Reserves

Project number: Horizon Europe 101135475

D3.4

Design for Donations

Due date of deliverable: 30 November 2024
Actual submission date: 30. November 2024

WP contributing to the deliverable: WP3

Start date of project: 1. December 2023 Duration: 3 years

Coordinator:
Eindhoven University of Technology
`www.taler.net/eurotaler`

Revision 1.0

Project co-funded by the European Commission within Horizon Europe		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission services)	
RE	Restricted to a group specified by the consortium (including the Commission services)	
CO	Confidential, only for members of the consortium (including the Commission services)	

HISTORY OF CHANGES		
VERSION	PUBLICATION DATE	CHANGE
0.1	31 July 2024	Donau design completed and implemented
0.2	29 November 2024	Complete version with requirements and capabilities
1.0	30 November 2024	Minor edits following intnernal review

Design for Donations

Bob Goudriaan, Christian Grothoff, Tanja Lange, Michiel Leenaars, Jonathan Levin

30. November 2024
Revision 1.0

The work described in this report has been funded (in part) by the European Union and by the Swiss State Secretariat for Education, Research and Innovation in the HORIZON-CL4-2023-HUMAN-01-CNECT call in project 101135475 TALER. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Abstract

This report provides an overview of functional requirements for privacy-preserving donations, keeping in mind the need for tax authorities to verify the proper source of donations prior to granting tax benefits. As a second contribution it provides a technical design to realize privacy-preserving and yet tax-deductable donations in GNU Taler, for which it presents the protocol specification and implementation details for the Donation Authority (Donau).

Keywords: GNU Taler, Tax-deductible Donations. Donau, Donation Authority, Privacy-Preserving Payments

Chapter 1

Introduction

The scope of this document is to provide an overview of potential technical requirements and desiderata for donation systems that wish to offer a technical solution in which donors can make donations to registered charities and then receive a tax benefit from the tax authorities when filing their tax statement. The document also provides a detailed technical design and implementation for privacy-preserving donations, developed in the thesis [4] by Johannes Casaba and Lukas Matyja supervised by Emmanuel Benoist and Christian Grothoff. The design provides a solution for a relevant subset of the requirements. We also discuss extensions and adaptations for covering other requirements.

This document is written in the context of the NGI TALER project, which is based around the electronic payment system GNU Taler. As may be obvious from the underlying acronym "Taxable Anonymous Libre Electronic Resources", GNU TALER bridges two seemingly opposite requirements: providing privacy to citizens with regards to how they spend their money in the digital realm, while at the same time creating a system for organizations which handle financial transactions that is transparent and auditable. The latter prevents fraud and keeps taxation as a basic mechanism to take action in the common interest and fund public services. To the citizens it offers the same privacy properties we are used to with traditional cash payments.

GNU Taler is a *digital commons*, based on free software and advanced cryptography. This means that – unlike proprietary products – the software can be adjusted by all stakeholders to carry the properties it should have.

1.1 Donations in a human rights perspective

Donating is an important way for people to empower causes they believe in, and facilitate collective action. In many countries, there is explicit recognition of the public benefit of such generosity: a friendly tax treatment of donations. It makes sense: money you immediately give away to a recognized good cause is not income that will be converted by you into private consumption. So conceptually it deserves a different tax treatment.

Donations have many causes, but quite often they are an obvious expression of the human right towards the freedom of thought, conscience and religion. Individual spending can be very intimate and personal, and even aggregate spending habits can reveal a great deal about people. This holds even more so for donating.

Protecting donation confidentiality is therefore important to protect those freedoms. We

have to recognize that in some situations the mere fact hat someone has – in private – donated to some cause at some point in their life, can put them at risk in another context. The right to privacy is another critical aspect of donating. International human rights law provides a non-ambiguous responsibility to promote and protect the right to privacy.

Both these rights—towards freedom of thought and to privacy—are anchored in key international treaties and covenants such as the Universal Declaration on Human Rights (Article 12), the European Convention for the Protection of Human Rights and Fundamental Freedoms (Article 8) and many more.

1.2 Protection towards all sides

Privacy threats not only exist on the outside. Not many people are aware that while the causes they support may be worthwhile, not all philanthropies play as nice as one would expect them to towards donors. This happens in particular when such organizations employ third party (often commercial) agencies to help "yield" more donations on a commission basis or as "fund raisers". Especially for-profit fund raising agencies tend to resort to questionable social engineering approaches. One common scenario is that after a first donation, such bad actors start to aggressively pressure a particular donor for more – with personalized emails, letters, phone calls and even in person visits. This may happen beyond a single good cause: people that donate are known to be susceptible to a certain proposition, resulting in an avalanche of follow up demanding requests.

In the era of data driven donations and corporate social media surveillance, this kind of behavior has unfortunately become so easy that there are not just pro bono but even paid services (source in the Netherlands: Stichting Donateursbelangen) to de-register and exercise the "right to be forgotten" after donating.

Even without such excesses, there are many circumstances when people like to donate something to their preferred causes without revealing their identity. Some people just prefer to stay anonymous because of personal beliefs or even religious requirements, or simply do not want to have publicity which might lead to a cascade of efforts from fund raisers.

1.3 Donation confidentiality

Making a financial donation is a deeply personal choice to share part of one's wealth in order to benefit a cause one cares about. Some traditional ways of donating (for instance passing around baskets or even plates in a religious gathering) are vulnerable to group pressure, and door to door fundraising is also confrontational and puts people on the spot.

When donations are devoid of such pressures and there is no need for, e.g., virtue signaling, donation confidentiality comes into play. Historically, people wanting to make an anonymous donation might have an envelope with cash or a box of goods delivered. Obviously, this was never compatible with providing tax benefits. Alternatively, they might arrange for an expensive intermediary like a notary (although that would not be fully anonymous, and depend on the discretion of the notary).

Technically guaranteed donation confidentiality is certainly non-trivial to implement in the digital payment era. What you donate to and why may be strictly personal, but due to the nature of the banking system along the financial pipeline there is an uncomfortable number of actors handling sensitive data that allows for profiling and targeted discrimination

on grounds. And there are even more that later on may have access to it. Digital payments are logged and made accessible to many different actors, and reporting donations to tax authorities adds yet (at least) one more actor to the pipeline. It is the scope of this document to try and solve this issue and finally introduce donation confidentiality which adheres to "privacy by design".

1.4 Overview of the requirements analysis

There are two types of donations we will consider. The first is *ad hoc* or *informal donations*, which are made from individual to individual as *one time gifts* typically in appreciation of the work being done by an individual or collective. The second category is *regulated donations* involving at least one *recognized* philanthropic organization or charity. Both involve voluntary transferal of some financial assets for which no products or services are rendered in return.

In the design requirements we will mostly cover donations to charities that offer a tax benefit as that triggers the most complex requirements.

As part of their regular operations as well as their recognition as public benefit organizations, registered charities are already subject to a variety of audits as well as strict regulatory and fiscal scrutiny. Good causes that do not adhere to these rules are stripped from any fiscal benefits. At least donations to recognized public benefit organizations may therefore be confidential: donors should be able to freely choose whichever of the approved philanthropies they donate to, without disclosing which.

In cases where donation confidentiality is not (yet) feasible, we will try and provide fallbacks that best serve the interest of donors, give them choice and respect their privacy as least as well as the current system in place.

1.5 Overview of the technical solution and implementation

On the technical side, this report presents the Donau protocol [4] for making privacy-preserving donations.

In the current way that donations are handled, the charities are in charge of issuing donation receipts to the donor and thus must know the donor's identity and address. The donor has to include the donation receipts in their tax declaration; this means the tax authority not only learns the amount that the tax payer donated to charitable organizations but also how much they gave to which.

The Donau protocol makes it possible for the donor to give an unforgeable proof of the combined amount they donated to registered charities, without the charities or the tax authorities learning who donated to whom. The privacy features obviously require that there is more than one charity and more than one donor. The Donau protocol is oblivious to how the donation payment happens. If the donor chooses to donate by credit card or bank transfer then their identity becomes known to the charity through the payment. However, a relevant feature of the protocol is that the charity does not need to learn the identity of the donor. Hence, payments can be made with GNU Taler keeping full anonymity of the donor.

The design requires the creation of a Donation Authority (Donau), an additional service separate from the charities and the payment system. The Donau is responsible for recognizing charitable organizations and tracking the total amount of donation receipts each charity is issuing for the charitable contributions the charity is receiving. It is typically be expected

that the tax authority would operate it. We note that the Donau does not receive sensitive private information about donors: privacy is achieved using cryptography to unlink proofs of donations from the actual donation process.

1.6 Structure of this report

The next chapter reflects on the requirements that donations need to satisfy. There are many aspects to donations and for the technical design and implementation we chose to focus on a design that provides privacy for donations. Chapter 3 shows the technical details of the design including the cryptographic building blocks used in the system. The following chapter reports on the implementation. Finally we consider various extensions of the presented approach that could be added to satisfy requirements currently not met by the core design. Many of these extensions are simply a matter of proper integration and user interface design, while a few presume the existence of a widely available digital identity system providing a single unlinkable pseudonym for each citizen per charity.

1.7 What this document is not

This document is not in any way an overview of current legal requirements across the world on how taxation on donations work. Taxation is predictably unpopular despite its clear essential function in how modern societies work, and therefore a very political topic that is subject to frequent change. Whether it is taxation on labor and profits, on property, on inheritance, on income from investment or gambling, or on consumption of products or services – there is no global universally agreed standard on whether these should be taxed and how that is to be done. Ad hoc regulation as part of political shifts makes taxation very context-specific and temporal. We are unaware of any attempt at creating such an overview as a public resource, and the cost of creating and subsequently maintaining such an effort would be prohibitive.

Instead the focus of this document is on providing an overview of generic requirements that could be made to a donation flow in order to comply with regulation.

One should note that, in many jurisdictions, recipients of donations do not necessarily have the same protections. Donations should be given without return consideration, but of course there are many financial transactions (such as gifts or donations from business or lobby groups to political parties) that are not as clean in this respect.

Chapter 2

Requirements Analysis

The starting point of this document is to create an initial overview of requirements to provide donors with donation privacy and tax authorities with adequate proof that a donation was indeed clean and made according to the rules for donations in their region of operation.

Tax authorities are creative, and taxation is an ever evolving area of complexity. We will therefore not claim to provide the definitive overview, but to provide a good start for bootstrapping a donation ecosystem in the full knowledge that this will need to be updated.

Subsequent deliverables (D3.5 and D3.6) may prioritize different properties and features or add further requirements on the design.

2.1 Assumptions

The basic assumptions when defining requirements for a donation flow are as follows:

- A donor donates from their *own assets*, and is willing to go on record (by means of a self-declaration) as acting on their own accord. Violation of this principle would then constitute fraud at their end.
- A tax authority wants to assert that a donation comes from the legitimate donor, and is not made by some third party on their behalf.
- There is no inverse relationship between the donor and donee, where the donor stands to receive money back from the donee in some concrete (in)direct way as result of the donation.
- Donors are willing and able to provide privacy-preserving attestation of some unique and non-falsifiable personal or organizational property (such as a tax identification number) *at the time of donation* in order to be able to add up multiple donations within a single tax reporting period and validate that these do not extend beyond a threshold set by the tax authority or other regulators
- The philanthropies or charities are subject to *regulatory oversight*, *proper governance* and *regular audits*, so that money laundering is not relevant
- It is acceptable for some third party to be involved, but only based on Free/Libre Open Source software (FLOSS) and on a zero knowledge basis

- All parties involved own and can operate digital devices so that they can store digital identifiers, cryptographic keys, and donation receipts or records
- Donors are expected to have a device that can hold a wallet for permanent storage of donation receipts.
- Charities and tax authorities are willing and able to run basic infrastructure.

2.2 Design goals

The following design goals hold:

- Accommodate a donor's wish to remain fully anonymous, also towards the organization(s) donated to.
- The donor should be able to claim the tax benefits they are entitled to without having to disclose any of the organization(s) donated to to the tax authority.
- The donor may accumulate any number of smaller or larger donations towards different eligible organizations (ideally even cross-border, in the presence of suitable fiscal arrangements such as within the European Union).
- Since donations are cumulative and often spontaneous, a donor should not have to decide upfront whether they will request tax benefits for their donations later on. Hence, all donations to suitable registered charities should result in a form of donation receipt.
- At the same time, the wallet of a donor should offer plausible deniability of any specific donations.

2.3 Optional Features

The following list of optional features of a donation system would allow for a maximum fit with as many fiscal regimes as possible for both informal and regulated donations, while at the same time serving the interest of the donors in question in the best possible manner. Specific realizations may weigh these differently based on local regulations and capabilities, but most need to be be provided in some form.

- Provide fiscal statement
- Proof of registration
- Providing a configurable self-testimony from the donor that they comply with specific legislation or regulation related to donations
- Cumulative donation counter from same donor to same cause
- Providing a notarized affidavit asserting uniqueness
- Unique ID for voting/Donor Advised Choices
- Making a compound weighted donation

- Cost transparency
- Staged donation
- Bandwidth donations
- Codes of conduct
- Restricted access mechanism
- Donation matching with a reference
- Anonymous donation matching by employer

We will elaborate on each of these features below.

2.3.1 Feature: Provide fiscal statement

The ability to provide a fiscal statement from the receiving charity linked to the donation is the starting point for most regulated donations, in order to comply to current practices. For example, with a time-stamped and printable fiscal statement of the amount, digitally signed by the charity, a donor can prove their donations in person to a tax authority.

It should be possible to obtain this statement at the time of donation, and ideally within a reasonable period afterwards – in both cases without having to expose any additional information to anyone (such as an IP address which is typically visible when downloading a document via the web).

There might be a need to include personal data/attributes in the attestation (e.g. a name, password ID, etc). There is no need for the charity itself to have any knowledge about such information, so it may be included encrypted with a key accessible exclusively to the donor/the tax authority/an auditor or other suitable independent third party.

The information should be configurable, and it should be clear which information is somehow independently validated.

2.3.2 Feature: Proof of registration

In some countries (e.g. Belgium) donors are required to register themselves with the tax authority before making a donation. While we believe that to be an anti-feature, it should be possible to include a checksummed code provided by the tax authority or a charity that makes sure that only registered donors can donate.

2.3.3 Feature: Configurable pledge

It may be necessary for the donor to testify (prior to the donation) that they comply with some legislative or regulatory requirement, or agree with a policy set by the charity in question.

As a generic requirement, this translates to a configurable pledge by the donor (e.g. "I am not an employee or grantee of the organization I am donating to, and am acting on my own accord. I stand to make no direct financial gains from making this donation").

The potential for abuse of donations to regulated charities is very limited. Such a self-testimony will allow the default to be to treat donations in a "good faith" manner rather than with a top-heavy and restrictive one-size-fits-all method.

2.3.4 Feature: Cumulative donation counter from same donor to same cause

One way to bypass restrictions in terms of allowed donation sizes before possible "Know Your Donor" requirements kick in, is to split up donations. If limits per donor are in place it becomes necessary to be able to assert that cumulative donations from a donor stay below a set threshold, where the threshold might have a temporal aspect (per year, per quarter, per two years).

2.3.5 Feature: Notarized affidavit

More generically—for instance when there is a minimum age for donations to certain class of causes—a privacy-preserving solution might be to have a notarized affidavit independently asserting the requirements have been met to be included in the metadata of the payment.

Such a privacy-preserving affidavit would not be traceable back to any underlying private information of the donor or to the charity in question. It might contain a counter or append-only record, and a date stamp with an accuracy no more precise than a calendar week (to avoid correlation attacks).

It is better for this affidavit not to be provided by individual charities but by trusted third parties otherwise ignorant of the transactions in questions: it involves an isolated task which can easily be outsourced to an independent service. That independent service only needs to perform this singular task based on having access to the proof/attribute(s) in question and does not need to have any further knowledge of any of the actors. The latter assumes that any unique identifier in the affidavit is uniquely linked to the donor so that they cannot circumvent limits by going via different third parties.

As long as the affidavit is non-falsifiable and irrevocable, it should suffice to assert uniqueness and allow to prove that the required conditions were met.

2.3.6 Feature: Unique ID for donor advised decisions

Also from the side of a donor, there might be a need for having a unique ID for voting. In the same vein as Donor Advised Funds, a crowd-sourced version could be Donor Advised Choices where donors can vote on specific options ("Shall we prioritize stretch goal A or B", or "We see a new opportunity, is it okay to replace some stated work with something else") – either on a weighted variant (larger donation gives more weight) or on a one person, one vote (all unique donors get the same one vote each).

Alternatively, a preference vote encoded inside the payment (based on e.g. Condorcet voting) could provide a one-time donor advised voting mechanism.

2.3.7 Feature: Compound weighted donation

The general idea is that donors can make a single donation, but this consists of multiple payments to multiple recipients. This is particularly relevant for informal donations to the developers of free and open source projects that do not make use of a fiscal host. In such a situation, the donations may be divided across the individual developers with a certain weight. Each of the recipients receives a direct donation from the donor, which typically will be far below the threshold for taxation.

There can be a suggested/default weight, but the donor should be able to tweak the relative weights and/or block specific recipients.

2.3.8 Feature: Cost transparency

It should be transparent to the donor what percentage of their donation is actually used for the effort for which funds are being raised. In particular it should be possible for the *cost for fundraising* to be made explicit, especially if this involves third parties. It should be possible to choose to donate without paying for fundraising.

(This might use the features from compound weighted donation)

2.3.9 Feature: Staged donation

This is a feature that works along the lines of so-called smart contracts. As goals are incrementally met by the project, donated funds are released. If the goals are not met according to the preset stages, the part of the money that is concerned with work that is not delivered is not paid and may ultimately be restored to its rightful owner, the donor.

2.3.10 Feature: Bandwidth donations

When people are pooling together resources to make some goal possible, in order to stimulate the broadest possible donations, the amount donated can be made flexible (within a certain *donation bandwidth*). Instead of stretching goals (which donors might not agree with) and promoting freeloading, the size of individual donations could shrink as well. This would stimulate to share the collective load.

2.3.11 Feature: Code of conduct

Donors transfer part of their (sometimes scarce) earthly possessions to support the good work of a cause they believe in, and it is only logical that this altruism comes with certain expectations in terms of how the organization receiving that money will subsequently spend it.

A *Code of Conduct* is the equivalent of the product warranty, where charities declare themselves accountable and promise to uphold certain best practices and adhere to public scrutiny – and are subsequently held to their promise by stakeholder organizations like Donateursbelangen.

An example of such a Code of Conduct public benefit organizations can subscribe to is the Donor Pledge ("Donateursbelofte" in Dutch). It should be possible for a charity to adhere to multiple such Code of Conducts and offer them as part of their donation portal.

Similarly, there are certification schemes for charities qualifying as public benefit organizations. These offer a reverse link from the certifying organization to the charity. It should be possible to include the certification conditions and this reverse link alongside the payment.

2.3.12 Feature: Restricted access mechanism

In order to engage donors with the work being done, philanthropies might want to give "behind the scenes" access to ongoing work to their donors. In order for that to happen, it should be possible to provide (limited) access to restricted materials for donors only. On a

technical level, this could be handing out *One Time Passwords* or other forms of proof of donation that will allow donors to get access to restricted areas.

2.3.13 Feature: Unlock thank you artwork

Making a donation is not just a clinical financial transaction where money is transferred from A to B, but something that also has emotional weight: the donor has taken a step they may have pondered about for a long time. Celebrating this altruistic win is part of the donation experience. "Thank you" artwork consists of images, video and/or audio used to enliven the financial transaction.

In some cases artists or other creatives might donate a work to the charity in question for this purpose, in other cases a charity might use photos of their day to day work or other personal tokens.

For transferring physical objects, the donor would need to be identifiable as such. At the same time, it should be possible for a donor to decline receiving such gifts and retain their anonymity, to the extent that this does not conflict with other regulations.

2.3.14 Feature: Donation matching with a reference

In some cases, a benefactor will want to incentivize others contemplating a donation to a specific good cause to go ahead. That is not necessarily something that needs privacy: some people and organizations use donations to publicly profile themselves. A common mechanism to incentivize others is to promise to match their donations to the organization in question, which is frequently done by announcing a period in which other people's donations will be "matched" (as in: donor A promises to donate as much as all other donations in that time period combined).

However, this is obviously a very crude mechanism, only suitable for benefactors with very deep pockets. It also does not give much opportunity for the benefactor to explain why they do this (and, let us be realistic, get some PR out of it as well).

By allowing the donor to include a reference to e.g. a social media post or blog post announcing the matching and requesting other donors to include that reference when making their donations, the donor providing the matching can 'see' that they are being heard/are getting PR mileage out of their donation.

2.3.15 Feature: Anonymous donation matching by employer

Quite a few large employers do donation matching as part of their corporate responsibility or human resource management (HRM) efforts. This is typically not tied to a single cause. Many larger employers sponsor such matching gift programs, either by themselves (such as the U.S. Office of Personnel Management's Give CFC) or via (currently expensive) third party organizations such as Benevity, Submittable, WeSpire, Goodera, etc.

In many cases, this practice is rather privacy-invasive. If you donate to, e.g., a reproductive rights organization, an NGO promoting climate justice, or a digital rights organization, an employer might want to find out from whom that donation originated. This makes it attractive for the donor to have a chance to stay anonymous while nevertheless ensuring that their donation is matched as one done by an employee of the company. This would require a mechanism where charities could prove to an employer that some eligible person (typically

an employee or retiree) has donated money which needs to be matched – obviously, without disclosing anything else.

2.4 General background information

This section contains general background information pertaining donations.

2.4.1 General Regulatory Framework

European Union (EU) member states regulate donations through a blend of EU-wide directives and country-specific laws. While there is no uniform regulation that applies to all donations in Europe, certain EU directives and principles affect donation practices, particularly those related to transparency, anti-money laundering (AML), tax compliance, and donor data protection.

2.4.2 Transparency and Accountability

Transparency in charitable donations is crucial to maintain public trust and deter financial misuse. European countries typically require organizations that receive donations to adhere to transparency measures, including:

- **Public Financial Reporting:** Most European countries mandate that charities, nonprofits, and similar organizations publish annual financial reports. These reports generally include detailed breakdowns of income sources, donation amounts, and expenditures.
- **Disclosures for Large Donations:** In some countries, large donations must be reported to regulatory authorities. This threshold and the specific requirements vary by country. For example, Germany requires registration for organizations receiving public donations, while the UK mandates certain reporting for donations above a particular threshold.
- **Third-Party Audit Requirements:** To verify the financial integrity of charitable organizations, many countries mandate independent audits for organizations surpassing specific revenue thresholds.

2.4.3 Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF)

Given the potential for abuse of charitable donations for money laundering and financing illegal activities, EU-wide Anti-Money Laundering Directives (such as the AMLD5) require organizations to implement stringent controls.

- **Know Your Donor (KYD):** Similar to the Know Your Customer (KYC) practices in the financial sector, some countries require organizations to verify the identity of donors making significant contributions. This requirement is typically tied to AML laws.

- **Transaction Monitoring and Reporting:** Charitable organizations must monitor donation transactions and report any suspicious activities to relevant national authorities.
- **Registration with Financial Intelligence Units (FIUs):** Nonprofits are encouraged, and sometimes required, to register with FIUs in certain EU countries to facilitate AML compliance.

2.4.4 Taxation and Deductibility

The tax treatment of donations varies across Europe, but many countries provide tax incentives to encourage charitable giving. Donations to qualifying nonprofit organizations are often tax-deductible, either partially or fully, depending on local laws.

- **Eligibility of Donors and Organizations:** Both the donor and the recipient organization usually need to meet specific criteria. For instance, only donations to accredited charities registered with national authorities are often eligible for tax relief.
- **Limits on Deductions:** Most countries place caps on deductible donations, typically as a percentage of the donor's income. For example, France allows deductions up to 20% of taxable income, whereas Germany permits deductions up to 20% of annual income or corporate profits.
- **Cross-Border Donations and Tax Relief:** The EU's "Stauffer doctrine" principle requires member states to treat cross-border donations similarly to domestic donations if the recipient organization meets equivalent standards, which facilitates cross-border charitable giving across the EU.

2.4.5 Data Protection and Privacy (GDPR)

The General Data Protection Regulation (GDPR) is a significant EU law that affects how personal data is collected, stored, and managed, including for donations.

- **Consent for Data Collection:** Donors must be informed of how their personal data will be used, and organizations must obtain explicit consent if data will be used for purposes beyond the donation transaction itself, such as marketing.
- **Data Minimization and Retention:** Organizations are expected to collect only the data necessary for processing the donation, retain it only as long as necessary, and ensure proper data deletion practices.
- **Right to Access and Erasure:** Donors have the right to request access to their personal data held by an organization and can request deletion or correction of their data under specific circumstances.

2.4.6 Corporate Donations and Sponsorships

Corporate donations are also regulated, particularly when related to tax deductibility, disclosures, and compliance requirements.

- **Transparency in Corporate Sponsorships:** European countries may require public disclosure of corporate donations or sponsorship arrangements, especially when public funds are involved. Many countries also enforce rules against donations that may appear to be intended for influencing legislation or government actions.
- **Limits on Corporate Donations:** Some countries impose caps on corporate donations eligible for tax relief to prevent excessive deductions and potential misuse.

2.4.7 Cross-Border Giving and EU Philanthropy Initiatives

The European Union encourages philanthropy across borders within Europe, but the process is still complex due to varying national tax and legal frameworks.

- **European Foundation Statute and the European Philanthropy Manifesto:** These initiatives aim to harmonize cross-border philanthropy regulations. The proposed European Foundation Statute, for instance, would create a legal form of a foundation operating across the EU.
- **Transnational Requirements for Nonprofits:** Nonprofits must navigate both the tax and regulatory requirements of each country in which they operate or fundraise, including any special registrations, tax filings, or documentation for cross-border transactions.

2.4.8 Ethical Standards and Codes of Conduct

Some European countries have established or encouraged adoption of ethical standards or codes of conduct for fundraising activities. Examples include:

- **Code of Conduct for Fundraising:** Many countries have adopted codes of conduct, which may govern methods for soliciting donations, advertising practices, and donor interaction protocols. There are also private initiatives such as the Donor Pledge from the Dutch foundation Donateursbelangen ("Donor Interest Foundation").
- **Charity Commissions and Regulatory Bodies:** Several European countries have independent regulatory bodies that oversee charitable organizations, such as the Charity Commission in the UK, to ensure compliance and ethical conduct in donations.

2.5 Country-Specific Considerations

While EU-wide directives provide a framework, each country has unique laws. Here are a few examples:

- **Germany:** Nonprofit organizations must register with local authorities to receive tax exemptions, and donations exceeding 10 000 EUR must be reported.
- **France:** Nonprofits must adhere to the "Loi de 1901" and comply with annual reporting requirements to remain eligible for public donations.
- **Italy:** Nonprofits are eligible for tax incentives if they register as ONLUS (Organizzazione Non Lucrativa di Utilità Sociale) or a similar designation under Italian law.

2.6 Conclusion

Navigating donation regulations in Europe involves adhering to EU directives on transparency, AML, tax compliance, and data protection while also meeting specific requirements in individual countries. Compliance ensures trust in the philanthropic sector, promoting ethical giving practices and cross-border donations within the EU's regulatory landscape.

Chapter 3

Protocol Description

The previous chapter identified several requirements and desired features that a donation system must or should satisfy. The technically most challenging part is to permit donors to stay anonymous towards the charity they are donating to and to keep private from the tax authorities which charities they donated to. The protocol presented in this chapter addresses this challenge and all of the design goals from Section 2.2. In Section 5.1 we discuss how the various optional capabilities could be achieved on top of this core protocol design.

The Donau protocol, developed for this project by Johannes Casaba and Lukas Matyja under the supervision of Emmanuel Benoist and Christian Grothoff, provides a solution for both of these challenges. This chapter follows closely and often is a verbatim reproduction of the thesis [4] by Casaba and Matyja. We thank them for their significant contributions.

This chapter provides a technical overview of the Donau protocol, starting with some cryptographic background followed by the setup and usage.

3.1 Background & Terminology

This section gives an informal introduction to some concepts from cryptography which are used later in the report.

- **Cryptographic Hash Function** A cryptographic hash function H is a function that takes as input an arbitrarily long bit string and returns a fixed-length output string, which satisfies some security requirements. In formulas

$$H : \{0,1\}^* \to \{0,1\}^n, m \mapsto h = H(m).$$

  The function H should provide preimage resistance, that means that it should be infeasible to find an input that hashes to a given output. It should also provide second-preimage resistance, that means that it should be infeasible to find a second input that maps to the same output as a given input. Even more restricting, it should provide collision resistance, meaning that it should be infeasible to find two inputs that hash to the same output (without any other restriction).

  Sometimes a hash function gets used in a scenario where the natural input values come from a small, easily guessable set, like passwords or PINs. In this scenario an attacker could break preimage resistance by just iterating through all possible inputs to find the matching one and, worse, could even store all resulting hash values in a big table for

instant preimage lookups for all users. One partial fix is to **salt** the hash, i.e., to add a random suffix or prefix to the input before hashing it. Applications then need to store the salt as well. If the salt can be kept private this stops the simple preimage attacks, otherwise it at least requires the attacker to try all inputs *per targeted hash*. We write a **salted hash** as $h = H(m, s)$, where s is the salt value.

- **Digital Signatures**

  A digital signature is a cryptographic scheme for authenticating a message or document, analogous to a handwritten signature. A signer creates a public/private keypair. The private signing key is used to generate a signature on a message. The public key is distributed, and can be used by anybody to verify the authenticity of the signature. A signature scheme is secure if, among other things, the private key cannot be computed from the public key and if nobody can generate a signature that verifies for some message under a public key if they do not have access to the matching private key.

- **Blind Signature**

  A **blind signature** is a type of digital signature where the signing party signs a so-called blinded message. The party requesting the signature hides the true message with a **blinding factor**, which only they know. Signature schemes that support blind signatures are constructed in such a way that one can compute a signature that is valid on the original (not blinded) message from the blind signature and the blinding factor. Requirements on the blind signature scheme are that the signer does not learn anything about the message they are signing and cannot link the unblinded signature to the blind one they signed.

  The **blinding** operation requires the message m to blind, the blinding factor b and the public key K_x^{pub} of the party issuing the blind signature, written as $\overline{m} = \mathsf{blind}(m, b, K_x^{\mathsf{pub}})$. We write the **unblinding** operation as $\beta = \mathsf{unblind}(\overline{\beta}, b, K_x^{\mathsf{pub}})$, where $\overline{\beta}$ is the value to unblind, b the blinding factor to apply and K_x^{pub} the public key that was used for signing.

3.2 Key generation and initial setup

Taler makes heavy use of blind signatures to issue coins; in the context of donations, blind signatures are issued by the donation authority Donau.

3.2.1 Donau key generation

1. The Donau generates an Ed25519 [1] keypair (D^{pub}, D^{priv}), called the **Donau Key**, for digital signatures.

2. The Donau also generates a set of **Donation Unit** keypairs ($K_x^{\mathsf{pub}}, K_x^{\mathsf{priv}}$) for blind signatures, corresponding to different currency denominations x that a donation can be composed of. The blind signature scheme used is either blind RSA [2] or blind Schnorr [3].

3.2.2 Charity key generation

1. Each charity generates its own Ed25519 charity key ($C^{\mathsf{pub}}, C^{\mathsf{priv}}$).

2. The charity also fetches the Donation Unit public keys from the Donau.

3. The charity transmits its public key C^{pub} and its requested yearly donation limit (if any) to the party controlling the Donau (e.g the local tax authority) using a authenticated channel.

4. The party in charge of Donau administration (usually the relevant tax authority) ensures that the charity is authentic and a legally recognized charitable organization. After successful verification, the charity public key C^{pub} together with its requested yearly donation limit (if any) are registered in the Donau database.

3.2.3 Donor Identifier generation

Each donor generates a personal **Donor Identifier** by computing a salted hash of their taxpayer ID. They use this Donor Identifier value for each donation they make and later to receive a donation receipt from the Donau.

The donor computes their Donor Identifier DI as

$$\mathsf{DI} = H(\texttt{TAXID}, S)$$

where S is a random salt and `TAXID` is their taxpayer ID. The donor stores the salt S along with their DI. They need to use the salt to link the Donation Identifier to their tax ID and claim the tax benefits for their donation. The use of the salt means the DI cannot be linked to the donor by anybody without S, even if they know `TAXID`.

3.3 Donating to a charity

When a donor wishes to donate to a charity, they first retrieve the Donau's Donation Unit public keys K_x^{pub} for the current year. The donor then represents their donation as a sum of the Donation Units offered by the Donau.

Example: Assuming the Donau publishes the Donation units $\{1, 2, 4, 8\}$*, a donation of* 7 *would be split into 1 unit each of the values* 4, 2 *and* 1*.*

For each necessary Donation Unit the donor generates a **Unique Donor Identifier (UDI)** by appending a random nonce to the value DI. If multiple instances of the same Donation Unit are needed to represent the target sum, the donor creates a different nonce for each instance of that Donation Unit. The donor must remember all UDIs.

In our example, there are 3 *Unique Donor Identifiers needed to represent the donated value of* 7*. We can write them as:*

$$u_1 = (\mathsf{DI}, N_1)$$
$$u_2 = (\mathsf{DI}, N_2)$$
$$u_3 = (\mathsf{DI}, N_3)$$

where DI *is the Donor Identifier from above, and the* N_i*s are nonces.*

Next the donor blinds the Unique Donor Identifiers using a unique blinding factor for each one. This hides the information in the UDIs from third parties, including the Donau and charity, and protects against linkability. The result is a set of **Blinded Unique Donor Identifiers (BUDIs)**.

In our example, the Blinded Unique Donor Identifiers would be

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

with random blinding factors b_1, b_2, and b_3.

So far, the **Blinded Unique Donor Identifiers** do not carry information about their monetary values. The *intended effective value is indicated* by grouping each Unique Donor Identifier with the hash of its respective Donation Unit public key K_x^{pub}. We call this pair a **Blinded Unique Donor Identifier Key Pair** (**BKP**). It is only the *intended effective* value because their value is zero until they are signed by the Donau. Note that they must be signed with the matching Donation Unit key as the blinding and unblinding operations rely strongly on the public key.

The BKPs for our example are:

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

These individual BKPs are then put in an array $\vec{\mu}$ of BKPs.
Here

$$\vec{\mu} = (\overline{\mu}_1, \overline{\mu}_2, \overline{\mu}_3)$$

The donor sends this array to the charity along with the corresponding payment. As stated in the introduction, the payment mechanism is irrelevant for the donation protocol.

3.4 Charity receives donation

Upon receiving the array $\vec{\mu}$ of BKPs and the corresponding payment from the donor, the charity verifies that the total amount claimed in the BKPs (based on the Donation Unit public key hashes $h(K_x^{\mathsf{pub}})$) is less than or equal to the amount they received in the payment. The charity then signs the array of BKPs with its Ed25519 Charity Key. That is, it computes

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

The charity sends the array $\vec{\mu}$ of BKPs and their signature σ_c to the Donau to generate a receipt.

3.5 Donau generates donation receipt

When the Donau receives a signed set of BKPs from a charity, it verifies the charity's signature. It then checks that no legal restrictions, such as a possible yearly donation limit for the charity, is being violated. If not, the Donau increments its record of the charity's total receipts by the total amount of the donation, i.e., the sum of the denominations used in the BKPs.

The Donau then blindly signs all BUDIs using the Donation Unit private keys K_x^{priv} that correspond to the public keys hashed in the BKPs.

In our example, the Donau blindly signs the three BUDIs submitted by the charity

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

These signatures constitute a blinded donation receipt from the Donau, and the Donau sends these back to the charity, which in turn forwards them to the donor.

3.6 Donor receives donation receipt

Upon receiving the blinded donation receipt from the Donau via the charity, the donor verifies the blind signatures over the BUDIs. If they verify, the donor then unblinds them to obtain signatures over the original UDIs. These UDIs, their unblinded signatures, and their respective hashed Donation Unit public keys constitute a collection of donation receipts. These donation receipts are stored on the donor's device.

In our example: the donor unblinds the Donau signatures $\overline{\beta_1}, \overline{\beta_2}, \overline{\beta_3}$, obtaining:

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

The donor then creates the final Donation Receipts:

$$r_1 = (\mathsf{UDI}_1, \beta_1, h(K_1^{\mathsf{pub}}))$$
$$r_2 = (\mathsf{UDI}_2, \beta_2, h(K_2^{\mathsf{pub}}))$$
$$r_3 = (\mathsf{UDI}_3, \beta_3, h(K_4^{\mathsf{pub}}))$$

3.7 Donor requests an annual donation statement from Donau

In order for the donor to claim a tax deduction, the donor needs to obtain a final **Donation Statement** which can be sent to the tax authority. The donor sends their saved donation receipts $\{r_1, \ldots, r_k\}$, accumulated throughout the year, to the Donau. This can be done multiple times during the year, but the receipts are not automatically in order to achieve *unlinkability* between the *issuance* of the receipts (which happens at the time of donation) and their *submission* for the Donation Statement.

Remember that each UDI is the concatenation of the donor identifier DI and a random nonce, i.e., they all start with the same DI.

Once the Donau receives the donor's donation receipts, it checks that for each 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 DI is the same in all receipts.
- the nonces are unique and were not submitted before by the same donor, identified as DI.

Importantly, the Donau does not see signatures of the charities the donor donated to, so it does not know where the donor spent money. They also only see a collection of common denominations, so they are unable to correlate total donation amounts per charity. Finally, the receipts are unblinded, so the Donau has never seen these signatures before. This makes the receipts unlinkable from when they were originally signed by the Donau.

The Donau then generates a signature over the total `amount` of all receipts, the current `year` and the Donor Identifier. This results in a final signature called the **Donation Statement**, which the Donau returns to the donor:

$$\sigma_s = \mathsf{sign}((\mathsf{DI}, \mathsf{amount}_{\mathsf{Total}}, \mathsf{year})), D^{\mathsf{priv}})$$

3.8 Donor sends final statement to a validator

Finally, to claim their deduction, the donor includes their donation statement in their tax declaration. The implementation detailed in the next chapter chooses to represent this information as a QR-Code

$$\mathtt{QR} = (\mathtt{TAXID}, S, \mathsf{year}, \mathsf{amount}_{\mathsf{Total}}, \sigma_s).$$

Other representations and integration into software for filing tax returns are possible. It is relevant that `TAXID` and salt S are included to recompute the donation identifier DI while linking the donation receipt to the tax ID.

The validator at the tax office verifies the **Donation Statement Signature** σ_s.

$$\mathsf{verify}((H(\mathtt{TAXID}, S), \mathsf{amount}_{\mathsf{Total}}, \mathsf{year})), \sigma_s, D^{\mathsf{pub}})$$

Chapter 4

Implementation

This chapter is also heavily based on (and often a verbatim reproduction of) the thesis [4] by Johannes Casaba and Lukas Matyja supervised by Emmanuel Benoist and Christian Grothoff. We thank Johannes Casaba and Lukas Matyja for their significant contributions.

This chapter describes the current implementation of the Donau, which consists of a REST API, an Android verification app, and the Donau database. The Donau is written in C, as it reuses parts of the codebase from the exchange of GNU Taler. The Donau has a similar architecture and uses cryptographic blinded signatures in a similar way as the exchange does.

On the user side, donation receipts are collected in a wallet; the wallet takes the users taxpayer ID and picks its own salt to create the Donor Identifier DI.

4.1 REST API

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

4.1.1 /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. 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"
    },
    {
    ...
    }
    ]
}
```

4.1.2 `/charities`

In order for a charity to be able to issue receipts by a specific Donau it must be registered by this Donau. The Donau provides an API to manage charities. By default only the Donau administrator can change the list of registered charities. The charity itself is able to request a donation report to keep track of their total donations in the current year. The response includes the maximum donation amount and the current donated amount for the charity of the current year.

The following is an example response of a `curl 127.0.0.1:8080/charities` command. There is only one charity named `example` registered with a donation limit of 10 euros.

```
{
  "charities": [
    {
      "charity_pub": "ABETNXT9ZF606FRF3WD5...",
```

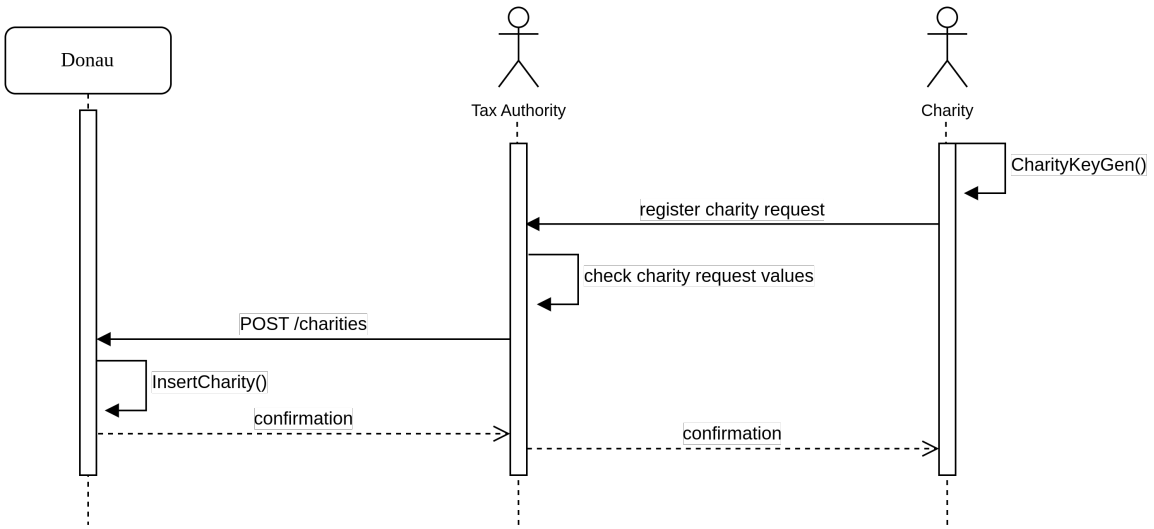

Figure 4.1.1: The tax authority registers a new charity in the Donau. A charity first requests to be added to the Donau, including its Charity EdDSA public key in its request. The tax authority them adds the charity by sending a POST request to the `/charities` endpoint with the relevant data on the charity

```
      "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`.

The following is an example of a `charity.json` entry

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

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

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

4.1.3 `/batch-issue`

Only recognized charities are allowed to issue receipts for their donors. 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 3.1). 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 checks 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 detect replays (see section 4.3).

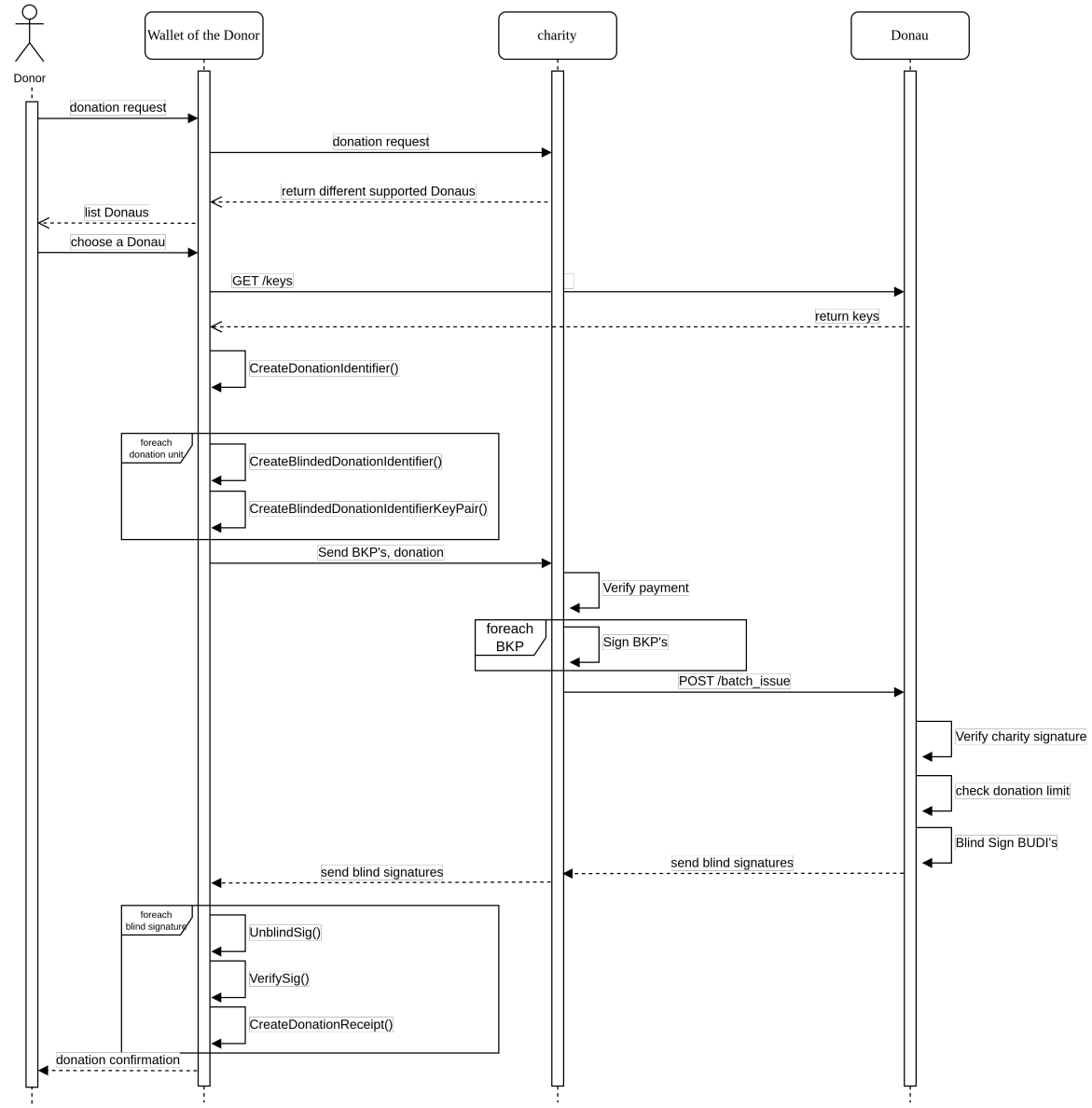

Figure 4.1.2: Flow of the issue receipt process

The following is an example response of a
`curl -d @issue.json -X POST http://127.0.0.1:8080/batch-issue/1` request showing a `issue.json` entry. 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
}

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

4.1.4 `/batch-submit`

The batch-submit route is used by the donor to summarize their donation receipts into one donation statement, which then gets signed by the Donau with their EdDSA signature. The request is composed of the donation receipts (see section 3.5), the corresponding year and the Donor Identification DI, which is the salted hash of the donor's taxpayer ID. When processing the request, the Donau checks the validity of the donation receipts and searches its database for other saved donation receipts made in the requested year. The Donau computes a donation statement, consisting of a signature over the total value of the donation units of all donation receipts of the year, the salted hash of the taxpayer ID, and the current year, and stores this in its database along with the submitted receipts (see section 4.3).

In our implementation the Donau does not return this donation statement under this call but under the `donation-statement` request, see below.

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. The following record would be stored.

```
{
  "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..."
    }
  }
  ]
}
```


4.1.5 /donation-statement

To obtain the donation statement, the donor submits a GET request for a specified year and taxpayer ID.

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 DI.


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


4.2 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 format.

4.3 Donau database

The Donau database contains five tables as shown in figure 4.3.1. 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.

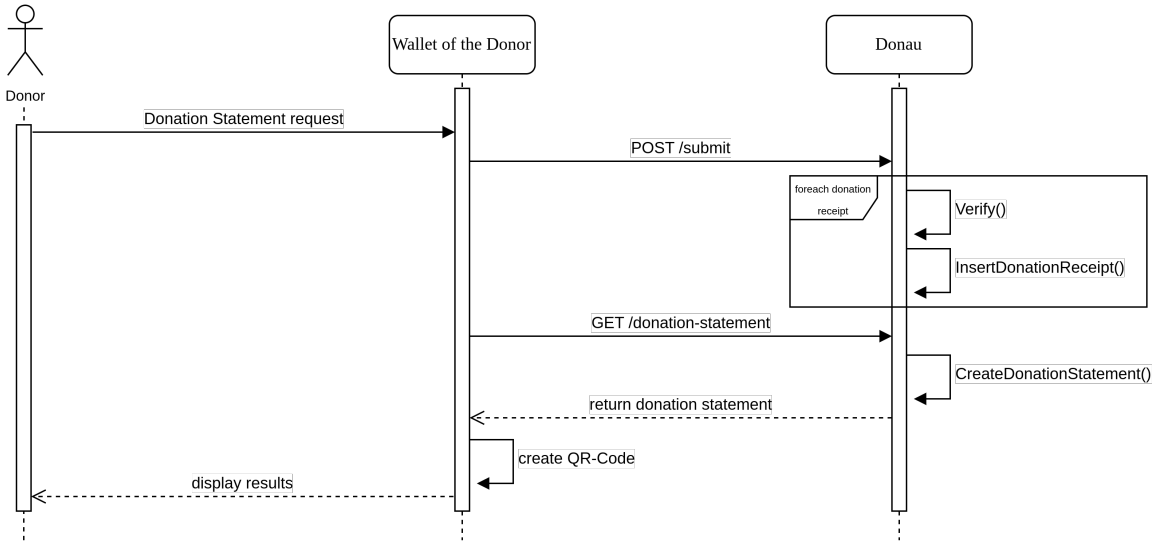

Figure 4.1.3: Donor requests a donation statement from the Donau

4.3.1 `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`.
- `current_year`: Current year

4.3.2 `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 Schnorr public key.
- `validity_year`: The year, for which the donation unit is valid.
- `value`: The amount and currency that this donation unit represents.

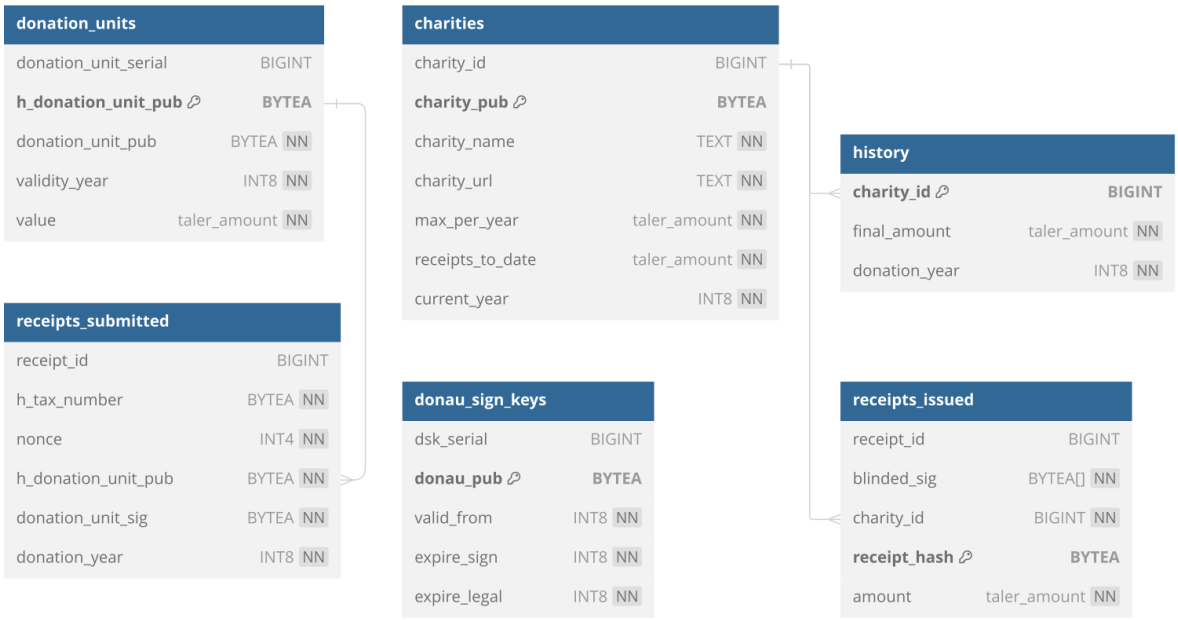

Figure 4.3.1: Donau database model (generated by https://dbdiagram.io/)

4.3.3 `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.

4.3.4 `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.

4.3.5 `receipts_submitted`

Contains all submitted donation receipts sent to the Donor. By storing the signature `donation_unit_sig`, the idempotence 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 (called DI in Chapter 3).
- `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.

4.3.6 `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.

4.4 Android Verification App

The Android app is part of the verification process used by the tax authority to check the donation statement (see section 3.8). The app decodes the submitted QR code from the donor, parses the signed values and the signature, and uses them to verify the signature. The arguments of the QR code are defined in section 3.8 and encoded as colon-delimited base64 values:

```
YEAR:TOTALAMOUNT:TAXID:TAXIDSALT:ED25519SIGNATURE
```

Finally, the values and the verification result are displayed.

Chapter 5

Discussion

This chapter compares the Donau design with the requirements and desired optional features and discusses threat models.

5.1 Optional features and the Donau design

Chapters 3 and 4 presented a complete design and implementation of a donation system that achieves confidentiality of donations while permitting donors to prove how much they donated to registered charities.

In this section we first show how the presented design and implementation could be made to fit the other features discussed in section 2.3 and which ones it addresses already.

5.1.1 Feature: Provide fiscal statement

Both the individual donation receipts and the annual donation statement provided by Donau satisfy the requirement of providing a fiscal statement. In general, the annual donation statement is more user-friendly and more privacy-friendly as it only contains the total amount and is more compact.

5.1.2 Feature: Proof of registration

In the Donau protocol, the donor is identified using a unique donor identifier. The format of the identifier is not fixed by the protocol, and could easily be replaced by the (hash over) donor registration data. While in this case the charity and Donau cannot check the validity of the donor's registration due to blinding, the tax authority would be assured that only donors who properly registered prior to their donation get a donation receipt that is valid for them. This enforces registration for tax deductible donations.

If the purpose of the registration is to limit charities to only accept money from registered donors, additional components need to be included. The cryptographic concept of attribute-based credentials can be used to build a suitable functionality. When a donor registers, they are provided a credential to prove that they are registered. When donating to a charity, the donor uses their credential to sign their donation. The charity checks that the signature is valid and it thus obtains proof that they are interacting with a registered donor as nobody else could make a valid signature. There are different approaches to attribute-based credentials

and features differ between them. To keep the privacy guarantees of the Donau protocol and only add donor registration, the system should be unlinkable and anonymous.

We acknowledge that this design does not provide a link between the donor identifier DI used in the BKP and the donor registration as that is incompatible with the property of providing anonymity to the donor. A registered donor with a valid credential may choose to submit BKPs that include invalid DIs or somebody else's DI. However, the design gives a proof to the charity that the payment they receive comes from a registered donor. See section 5.2 later for a discussion of threats.

Given that only few countries require donor registration and we consider this a requirement that hampers charities, we chose not to include this feature in our design.

5.1.3 Feature: Configurable pledge

The Donau protocol is expected to be integrated with a payment process, such as the GNU Taler payment protocol. Here, the actual payment would sign over contract terms between the donor and the charity. The pledge can be easily integrated into these contract terms.

5.1.4 Feature: Cumulative donation counter from same donor to same cause

Limiting donations per donor is difficult when donations are supposed to be anonymous and adding this feature to the Donau protocol requires additional components.

Donors could be issued some credentials, to be used in an attribute-based credential scheme which is anonymous but linkable. This could be set up to have one credential per charity and requiring a signature under a valid credential for each donation. This would mean that donations to the same charity by the same donor are linked, and the charity would be required to check the signature and to keep all donations and signatures, in order to decline further donation attempts by donors who have reached their limit.

As a practical instantiation it is conceivable to combine the Donau protocol with an EID solution that provides some unlinkable pseudonym derived from the donor's main identity. The unlinkable pseudonym could be unique to the donor, charity and time period. By signing the donation process with such an unlinkable pseudonym it is possible to prevent smurfing donations, alas at the expense of reducing anonymity to pseudonymity.

As discussed above in section 5.1.2, the signature on the donation does not guarantee that the DI hidden in the BKPs matches that of the signer.

5.1.5 Feature: Notarized affidavit

GNU Taler already supports privacy-preserving age-restrictions on payments, thus it would be trivial to prove that the donor is of legal age as part of the payment process (without disclosing any further information). In general, including other attestations may be possible, but is likely to be highly problematic from a privacy point of view. Not to mention that birth dates are commonly recorded and thus age can be easily attested by the payment service provider, other types of attestations would require building the corresponding certification infrastructure.

5.1.6 Feature: Unique ID for donor advised decisions

Issuing tokens to advise decisions would be part of the donation contract. The donation process could return such a token in addition to the donation receipt to enable the donor to vote, similar to the discount and subscription tokens already proposed for GNU Taler.

An inherent feature of the Donau protocol is that the donor has the private keys of the coins used to make a donation, and thus inherently a feature that could be used to advise decisions.

Limiting decisions to one per donor instead of proportional to the amount donated is more complex, as it would require a solution similarly to enforcing cumulative limits per donor as discussed in section 5.1.4.

The main challenge in both scenarios would be to find a way to inform the anonymous donors when their input is solicited.

5.1.7 Feature: Compound weighted donation

In general, the simplest way to do a compound weighted donation would be to break up the donation into multiple donations at the time when the donation is made. Given GNU Taler's ability to handle micropayments, doing multiple smaller payments is generally not an issue. Alternatively, the payment system could be enhanced with escrow functionalities that would allow the donation to be split up according to a given set of weights which is only provided after the donation was made.

5.1.8 Feature: Cost transparency

Fees in the GNU Taler system are given as part of the protocol and always shown to the payer, ensuring cost transparency. The design does not require the use of additional parties beyond the payment system, donor and charity. If fundraising parties are involved as well, their cuts could be easily made transparent in the GNU Taler contract terms used in the donation payment.

5.1.9 Feature: Staged donation

Staged donations would require the payment service to hold funds in escrow until certain conditions are met (or refund them). GNU Taler can already do refunds, and escrow of funds is a feature planned for the future.

The blinded donation receipts could similarly be held in escrow, released only when the next stage of funding is reached and the donation is released. A problem, however, is that the donor is anonymous and thus cannot be reached at the time that later goals are met.

A solution is for the charity to further blind or encrypt the Donau signatures and to publicly post the keys when the next stage of funding is reached and the donation becomes effective. In the following we assume that the donation is split up by funding stage and that the donor submitted an array of BKPs per funding stage, so $\vec{\mu}_j = (\bar{\mu}_{j1}, \bar{\mu}_{j2}, \ldots)$ is the array of BKPs for funding stage j. To make the multitude of keys manageable, the charity uses a random string t_j per funding stage and *encrypts* the Donau response $(\beta_{j1}, \beta_{j2}, \ldots)$ for the stage j payments with $H(t_j, \vec{\mu}_j)$. The encrypted Donau responses (one per stage) are returned to the donor at the time of donation instead of the plaintext Donau responses.

When work progresses to reach stage j and the donation payments are collected, the charity posts t_j publicly. Every donor can then compute their key $H(t_j, \vec{\mu}_j)$ and decrypt their donation receipts for stage j. This requires the donor to store the BKPs along with the encrypted donation receipts until stage j is reached and t_j is released. It requires the charity to have a bulletin board for posting t_j. We consider the latter a given as charities soliciting staged donations typically post extensive progress reports online, in particular when they move to the next stage and need to justify them declaring success on the previous stage. This report should then link to the key t_j.

5.1.10 Feature: Bandwidth donations

If the donated amount is to shrink based on certain conditions the design discussed in section 5.1.9 can be adopted. Here is a simple example where the final contribution of each donor is proportional to their maximum pledge: Each donation is composed of some fixed number N of equal shares. During the period that the charity is soliciting funding, all donations are held in escrow. Donors receive N encrypted Donau responses (one per share). Once the funding period ends, the total sum of pledges is known. Let the fraction a/N of the total suffice for the funding goal of the charity. The charity then posts the first a keys $t_1, t_2, \ldots, t_a$, unlocking the Donau responses for the effectively donated part, and receives the share of a/N of the pledged donations from escrow. The remaining $(N-a)/N$ shares of the donations are returned to the donors, e.g., by voiding the contracts that spent them. Since the would-be donors do not know $t_{a+1}, \ldots, t_N$, they cannot decrypt more Donau responses than their effective donation corresponds to. Finally, the charity needs to update the Donau to reduce the received amount on record.

5.1.11 Feature: Code of conduct

A code of conduct could easily be integrated into the contract terms of the payment process.

5.1.12 Feature: Restricted access mechanism

The envisioned discount token and subscription extensions of the GNU Taler protocol could be used to return to the donor a token that would grant them access to additional information.

5.1.13 Feature: Unlock thank you artwork

The GNU Taler protocol can already be used to buy digital goods. While we are usually thinking about newspaper articles or videos, this can of course also include images or audio resources. Thus, this can easily be done by using the payment process to authorize bypassing what in a commercial setting would be called a paywall.

Sending physical gifts requires having an address of the donor and thus is not compatible with the anonymity feature. However, there is nothing in the design that stops the charity and donor from exchanging address information during the donation process.

5.1.14 Feature: Donation matching with a reference

Donation matching is an agreement between the charity and a matching donor. The charity can show proof of the payments received; if these are done using GNU Taler then the charity

can show the deposit confirmations issued by the GNU Taler exchange to the charity. This way, the charity can prove to the match funder that they received a certain amount of donations, and they can even include the contract terms to show that the donors intended to participate in the match funding project. This requires that the match funder is not active in the considered donation period or that they subtract their own donations from the total.

Permitting the charity to verify that the match funder is actually complying requires the match funder to give up their anonymity towards the charity. This can be done at the stage of the donation contract during the payment. In the typical scenario that the match funder wants to publicly announce their matching, the charity and the world will know of the link. However, there is no technical reason that their matching donation is linkable to them and the Donau and tax authority will not see a link to the donations reported by the charity.

Both donor and match funder can in principle share their donation receipts publicly to advertise their good deed. They can also ask the charity to confirm that matching amounts arrived, but these actions would be outside the Donau protocol and of course void their anonymity.

5.1.15 Feature: Anonymous donation matching by employer

Technical solutions can be similar to what is discussed in section 5.1.2.

A simple solution if the match funder is a company with a taxpayer ID known to their employees and the match funder knows the donors' taxpayer IDs (as is common in an employment scenario) is to use that donations in the Donau system do not prove that the donation is made by the taxpayer with `TAXID`, and works as follows: The donor donates the full amount (their contribution as well as the match funding) to the charities of their choice, where they include their own DI in the proportion of the amount that should be their own donation and one derived from the `TAXID` of their employer in the other part. Then they show the donation receipts for both halves to the match funder. The match funder can verify validity of both receipts and that the proportion of their match is correct. They then refund the amount that was donated on their behalf to the employee and use the donation receipt for their `TAXID` when filing their tax statement.

5.2 Threats

The presented protocol is using similar cryptographic constructions as the GNU Taler payment system itself, primarily blind signatures and regular signatures. However, it does not use the "refresh" protocol of GNU Taler, as there is no need to render change. As a result, the Donau protocol suffers from a subset of the threats from quantum computing detailed in deliverable D5.3 [5], which analyzes the impact of quantum computers on GNU Taler.

A new Donau-specific threat is that donations could be used for laundering criminal assets. This does not mean that we expect charities themselves to play foul, but tax benefits that could be transferred to someone else would indirectly represent actual value (even commercially tradeable): donations from someone paying lower tax rates could be used to artificially lower the income of a person paying a higher rate. The money going to the charity would essentially be used to trigger a laundered partial payout in the legitimate world. The Donau protocol does not prove that the donor identification DI used in the UDIs inside the BKPs is that of the actual donor, as that is incompatible with the anonymity and confidentiality

guarantees of the system. In practice, we expect this threat to be largely theoretical: the hypothetical money launderer would need to take a significant loss (depending on the tax rate, but generally probably more than half, given that common effective tax rates are rarely above 50%). Thus, the costs of laundering money with this method would most likely substantially exceed the cost of other methods to launder criminal assets.

Bibliography

[1] Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. High-speed high-security signatures. *J. Cryptogr. Eng.*, 2(2):77–89, 2012.

[2] David Chaum. Blind signatures for untraceable payments. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *Advances in Cryptology: Proceedings of CRYPTO '82, Santa Barbara, California, USA, August 23-25, 1982*, pages 199–203. Plenum Press, New York, 1982.

[3] Georg Fuchsbauer, Antoine Plouviez, and Yannick Seurin. Blind Schnorr signatures and signed ElGamal encryption in the algebraic group model. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part II*, volume 12106 of *Lecture Notes in Computer Science*, pages 63–95. Springer, 2020.

[4] Lukas Matyja Johannes Casaburi. Donau: Donation Authority. Tax-deductible Privacy-Preserving Donations. Bachelor Thesis, 2024. https://taler.net/papers/donau-thesis.pdf.

[5] Tanja Lange and Jonathan Levin. Impact of quantum computers on GNU Taler. Technical report, NGI TALER, December 2024.