Flows in the GNU Taler System

Christian Grothoff

March 17, 2025

Contents

1 Interactions **2**
- 1.1 Withdraw . . . 4
- 1.2 Deposit . . . 5
- 1.3 Pay . . . 6
- 1.4 Refund . . . 8
- 1.5 Push payment . . . 9
- 1.6 Pull payment (aka invoicing) . . . 10
- 1.7 Shutdown . . . 11

2 Regulatory Triggers **12**
- 2.1 KYC: Withdraw . . . 13
- 2.2 KYC: Deposit . . . 15
- 2.3 KYC/AML: Push Payment . . . 17
- 2.4 KYC/AML: Pull Payment . . . 19

3 Regulatory Processes **21**
- 3.1 Domestic wallet check . . . 22
- 3.2 KYC process . . . 24
- 3.3 KYB process . . . 26
- 3.4 AML process . . . 28

4 Fees **29**
- 4.1 Fees per wire . . . 30
- 4.2 Fees per coin . . . 31

Chapter 1

Interactions

This chapter introduces the main payment interactions in the GNU Taler payment system. For each interaction, we introduce the parties involved and in which order they interact and how. In each interaction it is possible that the Taler exchange needs to trigger a compliance process. These regulatory riggers are described in more detail in Chapter 2.

The main interactions of the system are:

withdraw a customer withdraws digital cash to their wallet

deposit a customer returns digital cash into their bank account

pay a customer pays into bank account of a merchant

refund a merchant decides to return funds to a customer

push a customer sends a payment to another wallet

pull a customer requests a payment from another wallet (effectively sending an invoice)

shutdown the Taler payment system operator informs the customers that the system is being shut down for good

In the analysis of the legal requirements, it is important to differentiate between transactions between wallets (customer-to-customer) and transactions where money flows from a wallet into a bank account (customer-to-merchant) as these have different limits: When digital coins are used to pay at a business in Taler, the business never actually receives usable digital coins but instead the amount is always directly credited to their bank account. Depending on the transacted amounts, the business will nevertheless be subject to KYB (Section 3.3) and AML checks.

Customers begin their business relationship with us when they withdraw digital cash. Taler has no accounts (this is digital cash) and thus there is no "opening" or "closing" of accounts for consumers. Given digital cash, the customers can either (1) deposit the funds explicitly into a bank account (see Section 1.2), (2) pay a merchant (see Section 1.3), (3) pay another customer using a peer-to-peer transfer (see Sections 1.5 and 1.6), or (4) the coins will expire if the wallet was lost (including offline for a long time or uninstalled).

Finally, if a wallet remains (occasionally) online but a user does simply not spend the coins will (5) diminish in value from the change fees (see Section 4.2) that apply to prevent the coins from expiring outright.

For customers, we will categorically limit of digital cash withdrawn per month to less than CHF 5'000 per month and less than CHF 15'000 per year, thus ensuring that consumers remain below the thresholds where most regulatory processes become applicable. Payments between users will be limited to receiving less than CHF 2'500 per month and less than CHF 15'000 per year. We will ensure that customers are Swiss (see Section 3.1) by requiring them to have a Swiss bank account and/or a Swiss phone number (+41-prefix).

For **merchants**, the Taler equivalent of "opening" an account and thus establishing an ongoing business relationship is for a business to receive payments (see Section 1.3) exceeding CHF 5'000/month or CHF 15'000/year. We will consider the account "open" (and require up-to-date KYB information and check sanction lists) as long as the business has made any transactions within the last 24 months.

As we will only transfer money into the existing bank accounts of the merchants to compensate them for sales made using the Taler payment system, we do not need to check the origin of funds for those merchants as they will only receive funds from us.[1]

For individual **transactions**, we will impose a limit of CHF 1'000/transaction (even though our reading of the regulations would permit individual transactions up to CHF 15'000).

The following sections describe the respective processes for each of these interactions.

[1]Should businesses want to use Taler for expenditures, they will need to withdraw digital coins from their bank account just like customers, and the limits for customers will continue to apply.

1.1 Withdraw

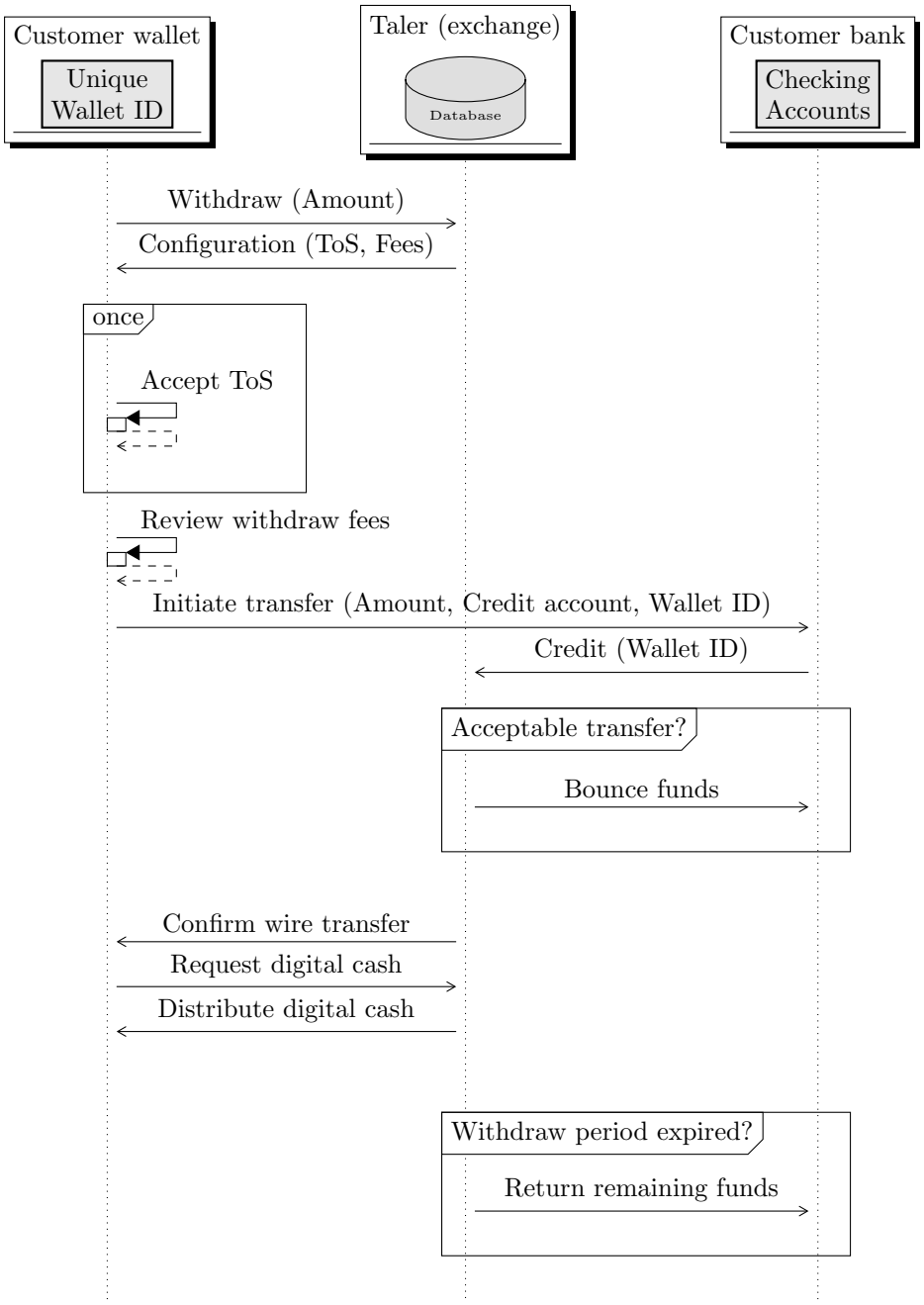

Figure 1.1: Withdraw interactions between customer, Taler exchange (payment service provider) and bank. The amount of digital cash distributed is subject to limits per origin account (see Section 2.1).

1.2 Deposit

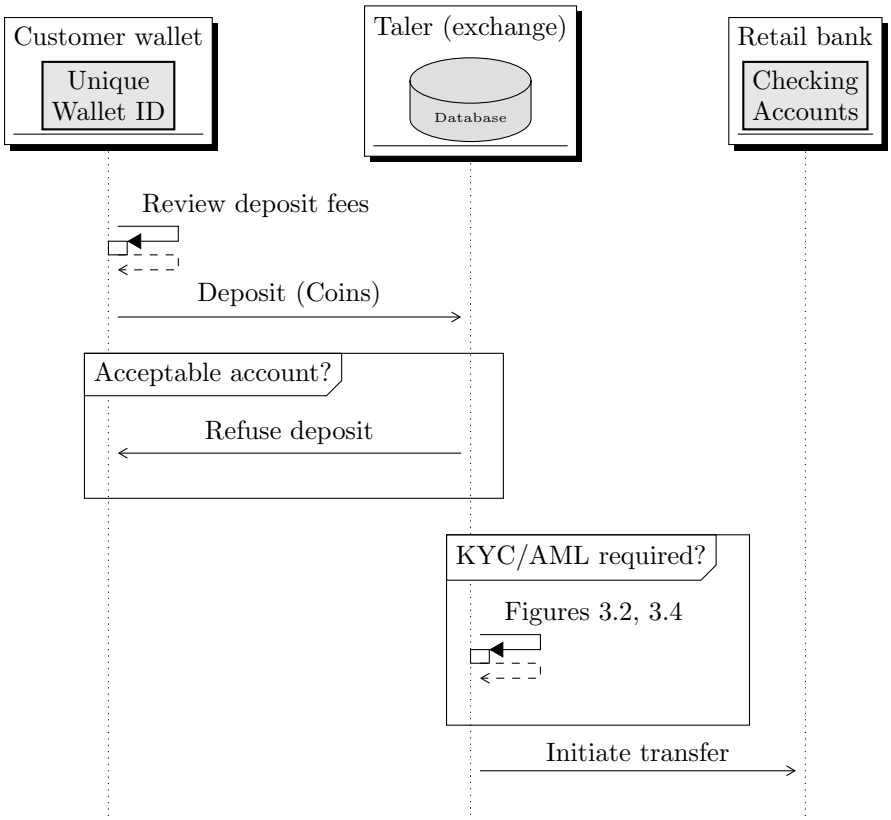

Figure 1.2: A customer deposits the coins issued by a Taler exchange (payment service provider) into a bank account. Even if the bank account is owned by the same customer, the KYC checks from Section 2.2 apply.

We do **not** permit the customer to regain control over their funds *unless* they pass the KYC/AML checks. The technical reason is simply that the KYC/AML checks happen *after* the aggregation logic and at this point refunds are no longer permitted. From a compliance perspective, this also prevents malicious customers from risk-free probing of the system.

1.3 Pay

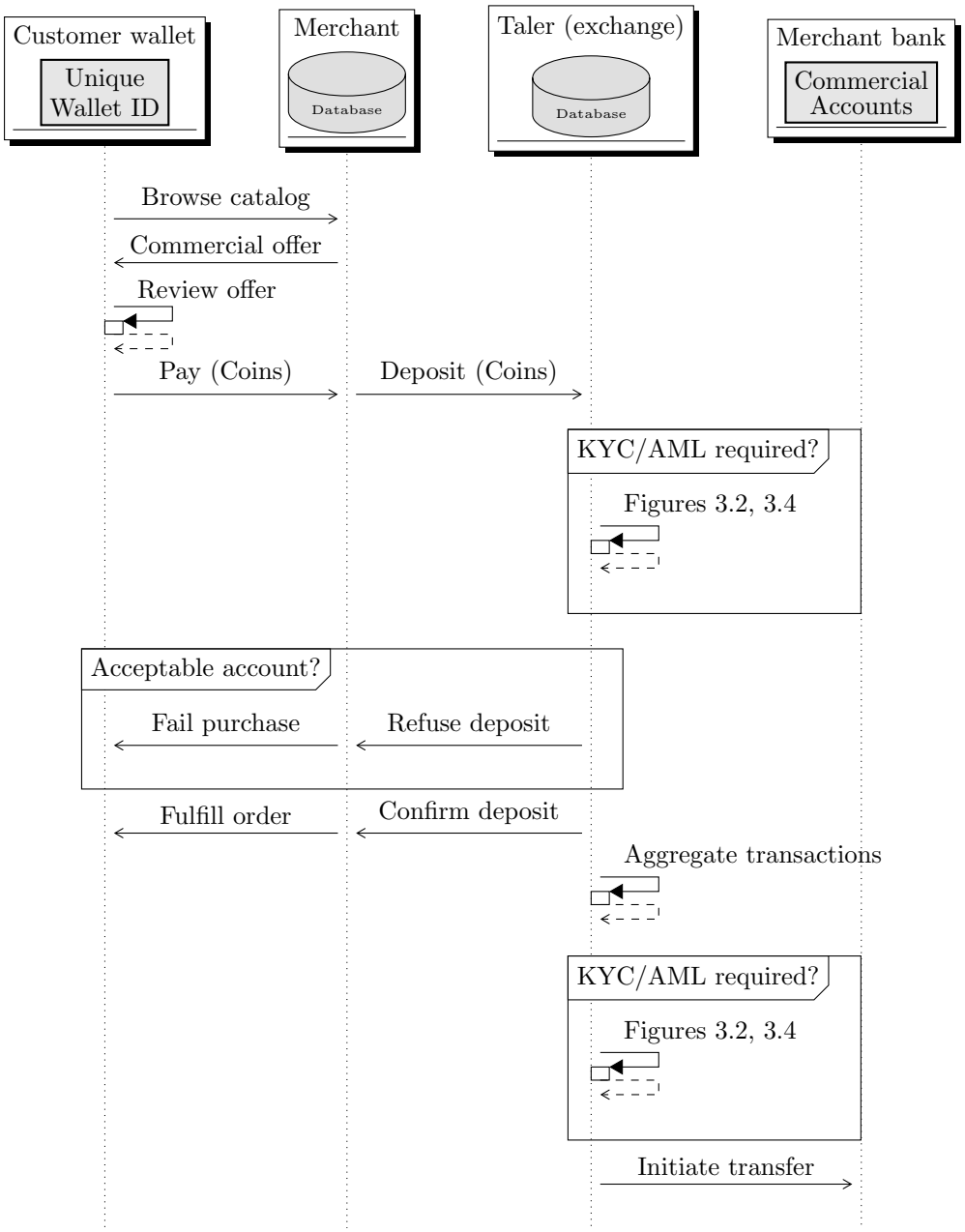

Figure 1.3: Payments from a customer to merchant result in depositing coins at the Taler exchange (payment service provider) which then credits the merchant's bank account. The KYC/AML checks are described in Section 2.2

Internal note: The exchange refusing a deposit immediately based on unaccaptable merchant accounts can depend both on the target account (e.g. wire

method not supported) or on the legitimization state of the merchant's target account (including lack of KYC authorization wire transfer, failure to accept terms of service, failure to provide KYC data, or some kind of AML/KYC rule being violated). However, in general the merchant backend will know if it has performed some mandatory sign-up process and can thus avoid the entire situation by only offering exchanges where the merchant is in good standing in its contracts. The central bug for supporting this in the merchant is #9052.

1.4 Refund

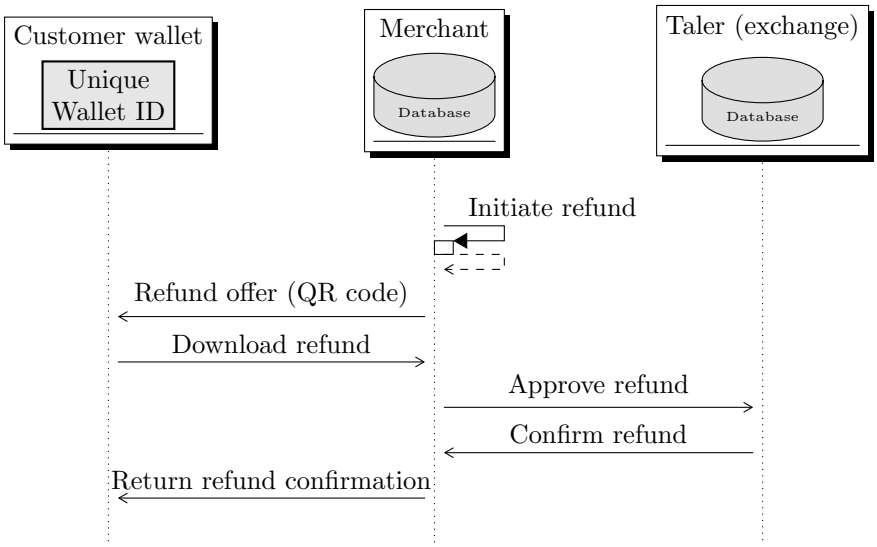

Figure 1.4: Refund processing when a merchant is unable to fulfill a contract. Refunds must happen *before* the exchange has aggregated the original transaction for a bank transfer to the merchant. Furthermore, refunds can only go to the customer who made the original payment and the refund cannot exceed the amount of the original payment.

1.5 Push payment

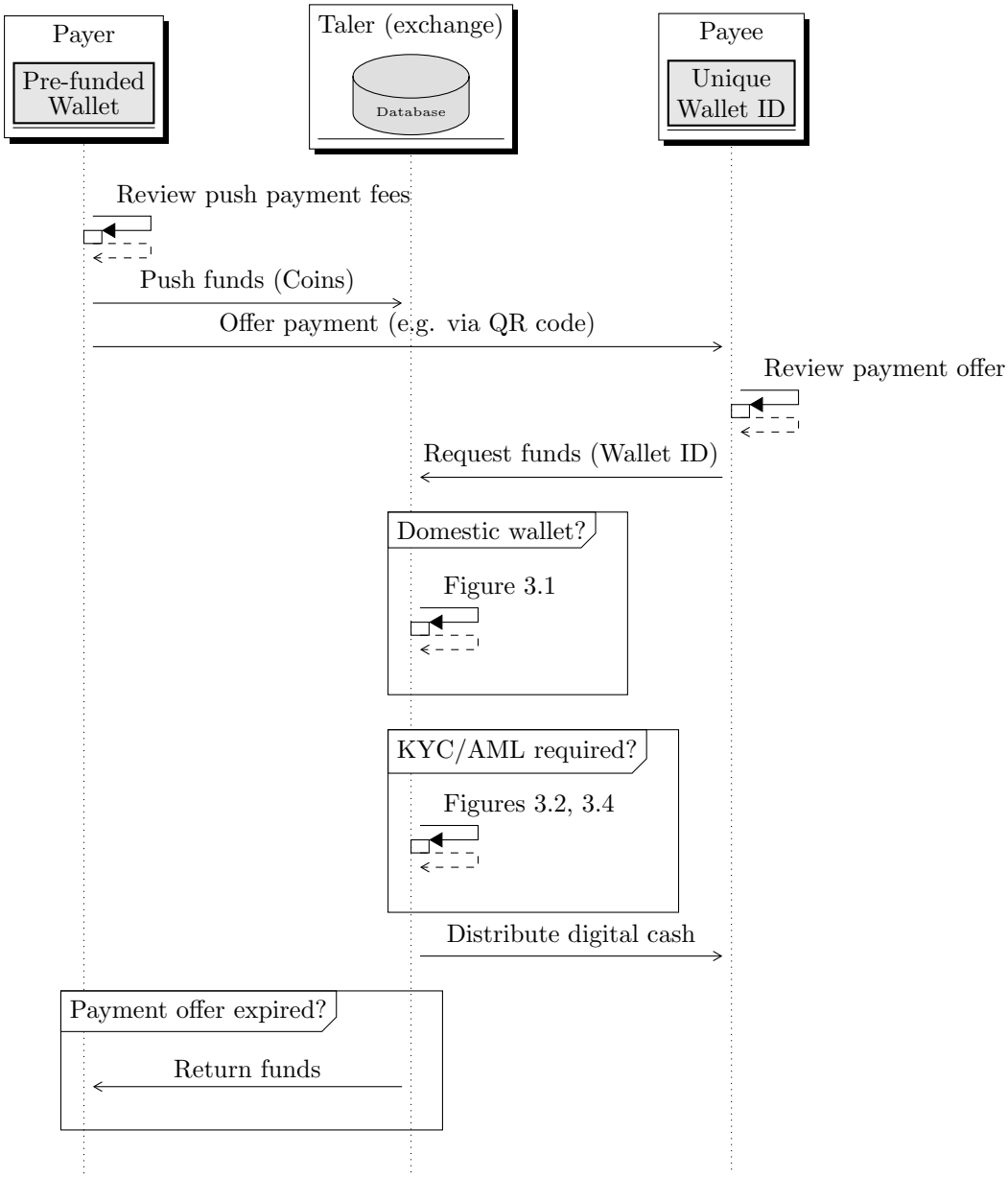

Figure 1.5: Interactions between wallets and Taler exchange in a push payment. KYC/AML checks are described in Section 2.3.

1.6 Pull payment (aka invoicing)

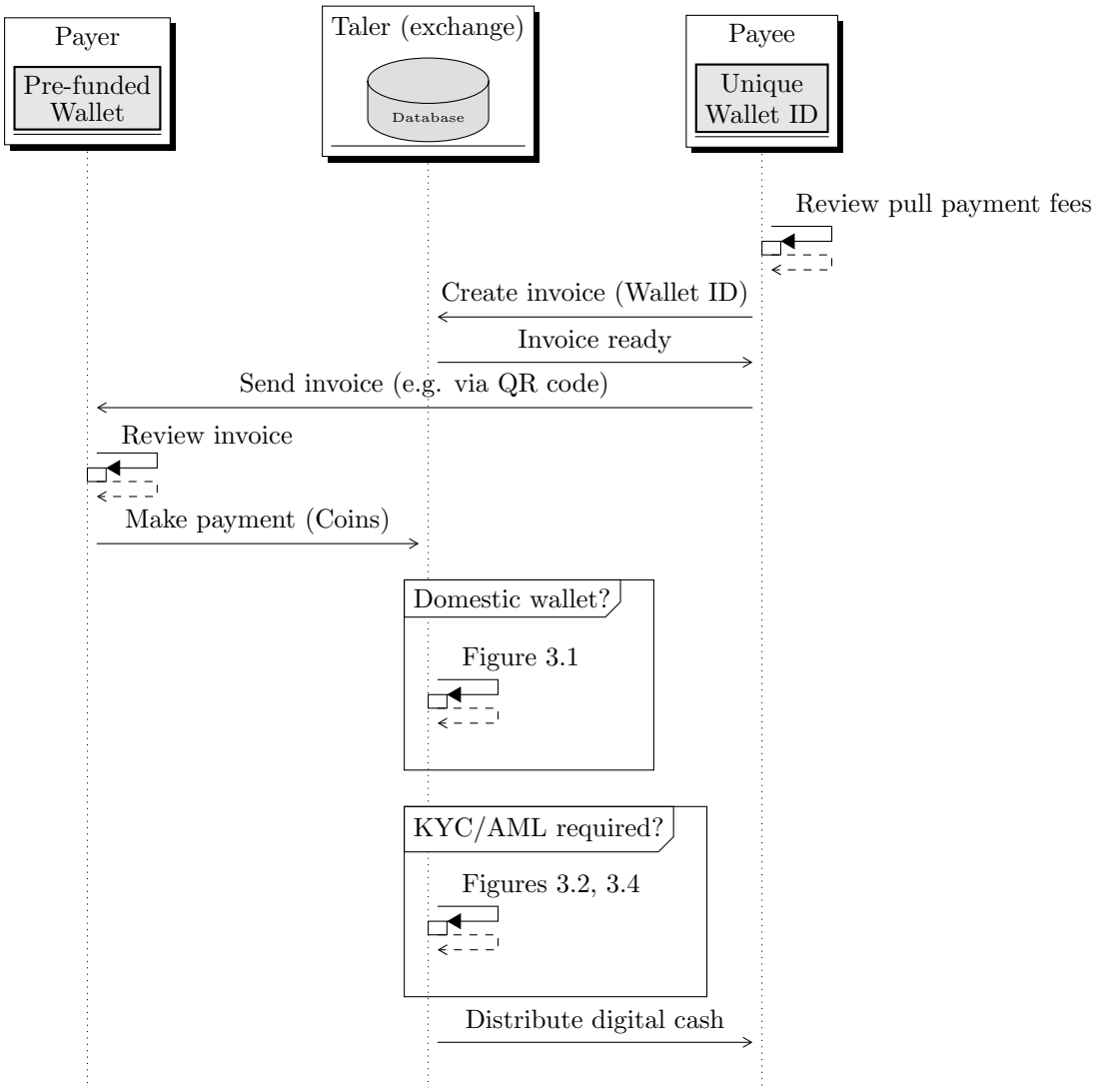

Figure 1.6: Interactions between wallets and Taler exchange in a pull payment. KYC/AML checks are described in Section 2.4.

We do **not** permit the payer to regain control over their funds, once the payment was made they are locked *until* the payee passes the KYC/AML checks. We only do the AML/KYC process once the funds are locked at the exchange. This ensures we know the actual transacted amounts (which may be lower than the total amounts requested) and prevents risk-free probing attacks.

1.7 Shutdown

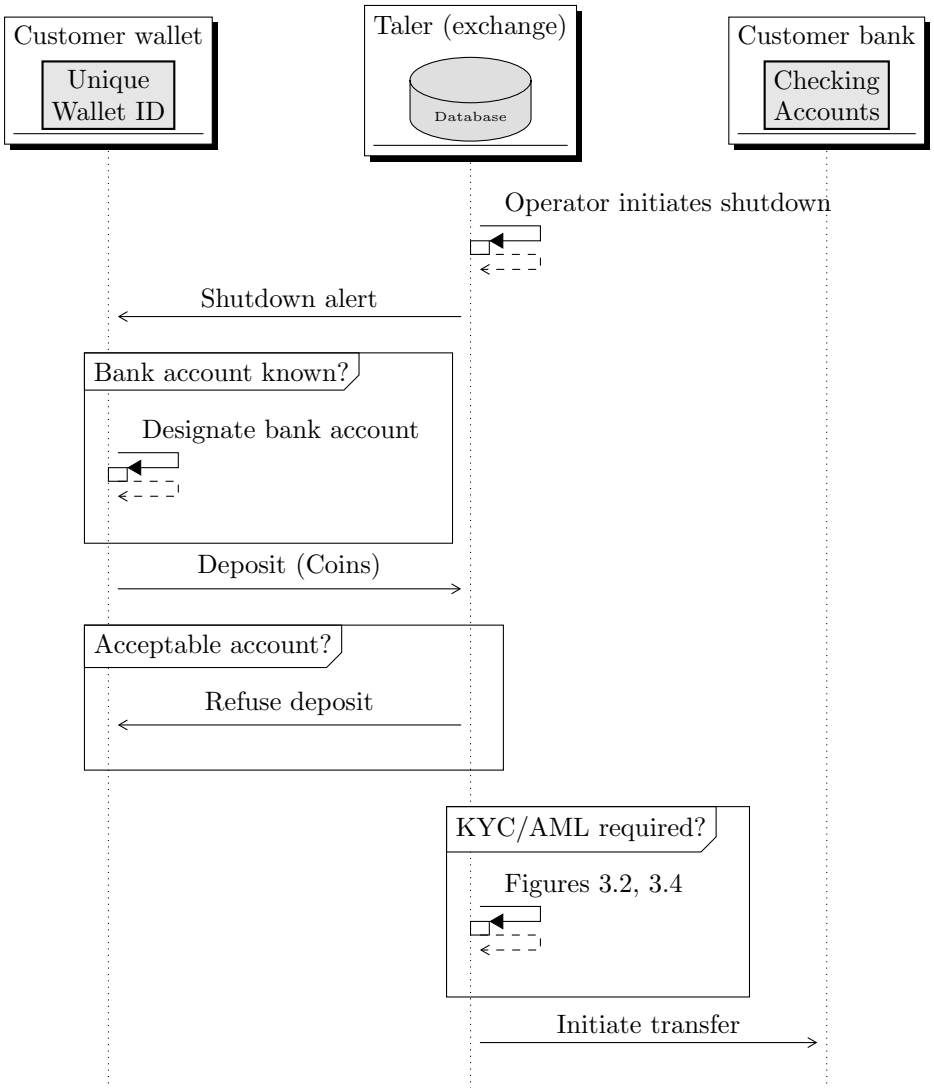

Figure 1.7: Shutdown interactions between customer, Taler exchange (payment service provider) and bank.

KYC/AML requirements are relaxed in cases where the customer is able to cryptographically demonstrate that they previously withdrew these coins from the designated checking account. Thus, KYC/AML checks here primarily still apply if the customer received the funds via P2P transfers from other wallets.

Chapter 2

Regulatory Triggers

In this chapter we show decision diagrams for regulatory processes of the various core operations of the GNU Taler payment system. In each case, the **start** state refers to one of the interactions described in the previous chapter. The payment system will then use the process to arrive at an **allow** decision which permits the transaction to go through, or at a **deny** decision which ensures that the funds are not moved.

The specific *decisions* (in green) depend on the risk profile and the regulatory environment. The tables in each section list the specific values that are to be configured.

There are five types if interactions that can trigger regulatory processes:

withdraw a customer withdraws digital cash from their **bank account**

deposit a customer or merchant's **bank account** is designated to receive a payment due someone paying with or depositing digital cash

push a **wallet** accepts a payment from another wallet

pull a **wallet** requests a payment from another wallet

We note in bold the **anchor** for the regulator process. The anchor is used to link the interaction to an identity. Once an identity has been established for a particular anchor, that link is considered established for all types of activities involving that anchor. A wallet is uniquely identified in the system by its unique cryptographic key. A bank account is uniquely identified in the system by its (RFC 8905) bank routing data (usually including BIC, IBAN and account owner name).

The KYC and AML processes themselves are described in Chapter 3.

2.1 KYC: Withdraw

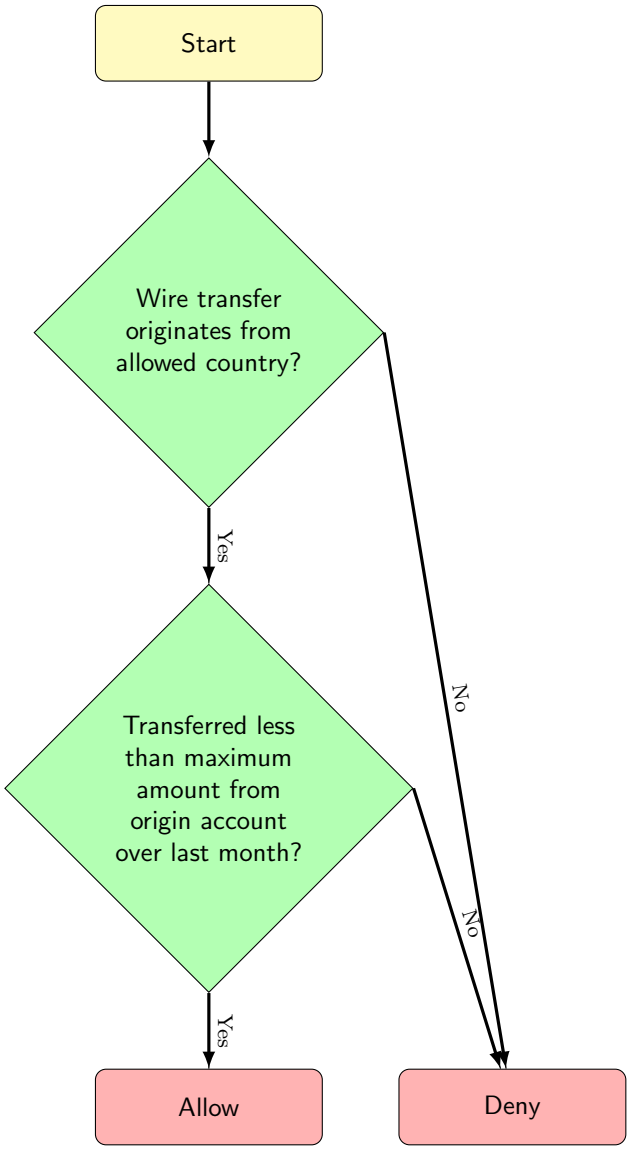

Figure 2.1: Regulatory process when withdrawing digital cash from a bank account. If the transfer is denied or the user fails to withdraw the funds for any other reason, the money is automatically returned after the bounce period (see Table 2.1) to the originating bank account.

SMS-Identification is done by in-house software. Withdraw limits are hard and cannot be raised even if the customer is known.

Table 2.1: Settings for the withdraw trigger. Note that the operation must satisfy all of the given rules.

Setting	**Type**	**Value**
Allowed bank accounts	RFC 8905 RegEx	*CH**
SMS-Identification	Amount/month	*200 CHF*
Withdraw limit	Amount/month	*5000 CHF*
Withdraw limit	Amount/year	*15000 CHF*
Bounce period	Delay	1 month

2.2 KYC: Deposit

Table 2.2: Settings for the deposit trigger. Note that the operation must satisfy all of the given rules.

Setting	**Type**	**Value**
Allowed bank accounts	RFC 8905 RegEx	*CH**
KYB deposit threshold	Amount/month	*5000 CHF*
KYB deposit threshold	Amount/year	*15000 CHF*
Default AML deposit threshold	Amount/month	*5000 CHF*

Additionally, our terms of service will prohibit businesses to receive amounts exceeding 1'000 CHF per transaction.

SMS-Identification is done by in-house software. KYB data is initially obtained and vetted by one of several external KYB providers before being passed for manual validation by our own staff who can then determine appropriate AML thresholds and set review criteria.

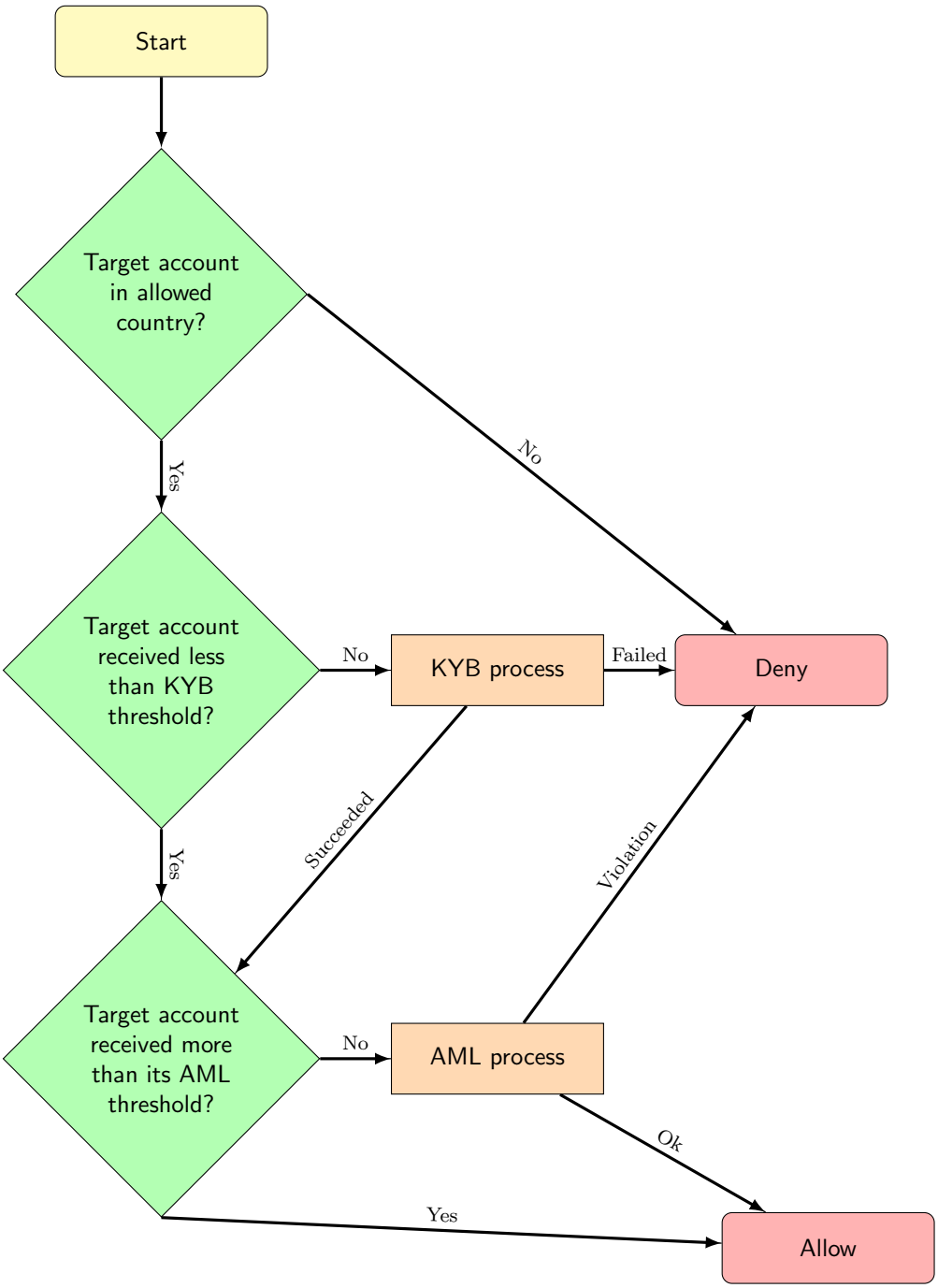

Figure 2.2: Regulatory process when depositing digital cash into a bank account. When the transfer is denied, the money is held in escrow until authorities authorize the transfer.

2.3 KYC/AML: Push Payment

Table 2.3: Settings for the push payment trigger. Note that the operation must satisfy all of the given rules.

Setting	**Type**	**Value**
Permitted phone numbers	Dialing prefix	*+41*
SMS-Identification	Amount/month	*0 CHF*
P2P KYC threshold	Amount/month	*5000 CHF*
P2P KYC threshold	Amount/year	*15000 CHF*
Default P2P AML threshold	Amount/month	*5000 CHF*

SMS-Identification is done by in-house software. KYC data is initially obtained and vetted by one of several external KYC providers before being passed for manual validation by our own staff who can then determine appropriate AML thresholds and set review criteria.

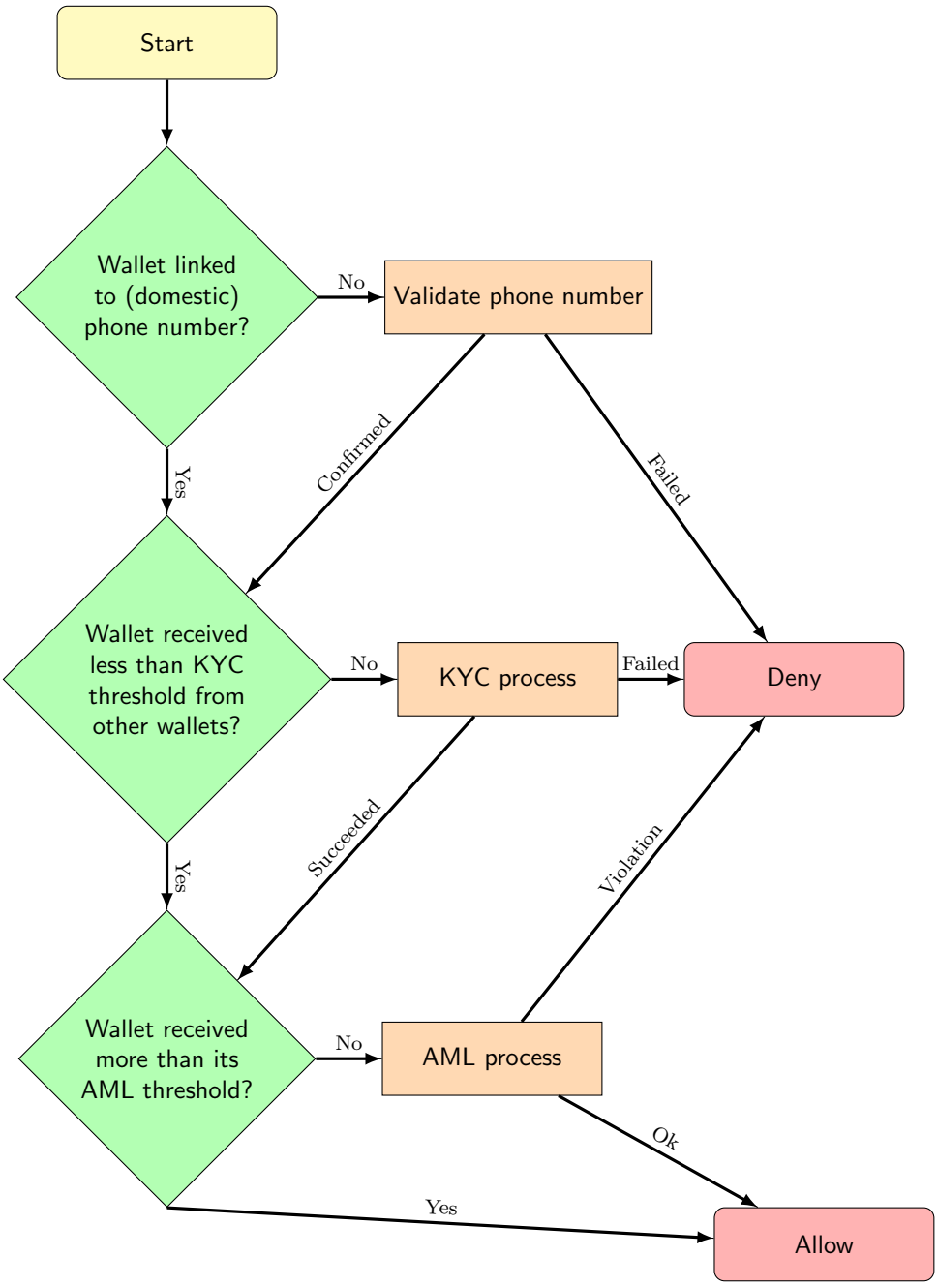

Figure 2.3: Regulatory process when receiving payments from another wallet. The threshold depends on the risk profile from the KYC process. When the transfer is denied, the money is held in escrow until authorities authorize the transfer.

2.4 KYC/AML: Pull Payment

Table 2.4: Settings for the pull payment trigger. Note that the operation must satisfy all of the given rules.

Setting	**Type**	**Value**
Permitted phone numbers	Dialing prefix	*+41*
SMS-Identification	Amount/month	*0 CHF*
P2P KYC threshold	Amount/month	*5000 CHF*
P2P KYC threshold	Amount/year	*15000 CHF*
Default P2P AML threshold	Amount/month	*5000 CHF*

SMS-Identification is done by in-house software. KYC data is initially obtained and vetted by one of several external KYC providers before being passed for manual validation by our own staff who can then determine appropriate AML thresholds and set review criteria.

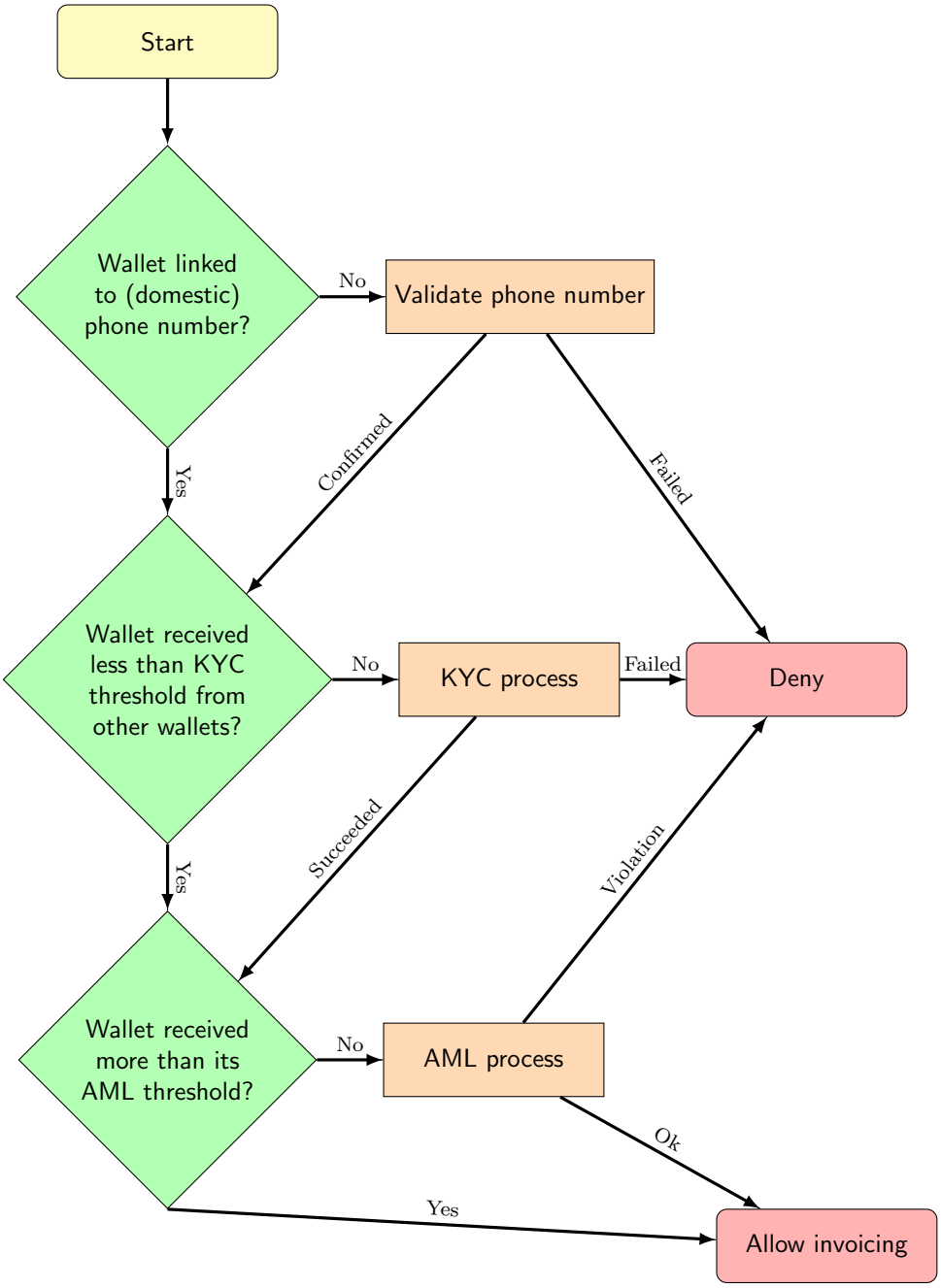

Figure 2.4: Regulatory process when receiving payments from another wallet. The threshold depends on the risk profile from the KYC process. When KYC thresholds would be passed, the receiving wallet cannot generate a valid invoice until it has provided the KYC data. When a transfer is denied by AML staff, the money is held in escrow until authorities authorize the transfer.

Chapter 3

Regulatory Processes

This chapter describes the interactions between the customer, exchange and organizations or staff assisting with regulatory processes designed to ensure that customers are residents in the area of operation of the payment service provider, are properly identified, and do not engage in money laundering.

The three main regulatory processes are:

domestic check This process establishes that a user is generally eligible to use the payment system. The process checks that the user has an eligible address, but stops short of establishing the user's identity.

kyc This process establishes a user's legal identity, possibly using external providers to review documents and check against blacklists.

aml The AML process reviews suspicious payment activities for money laundering. Here AML staff reviews all collected information.

3.1 Domestic wallet check

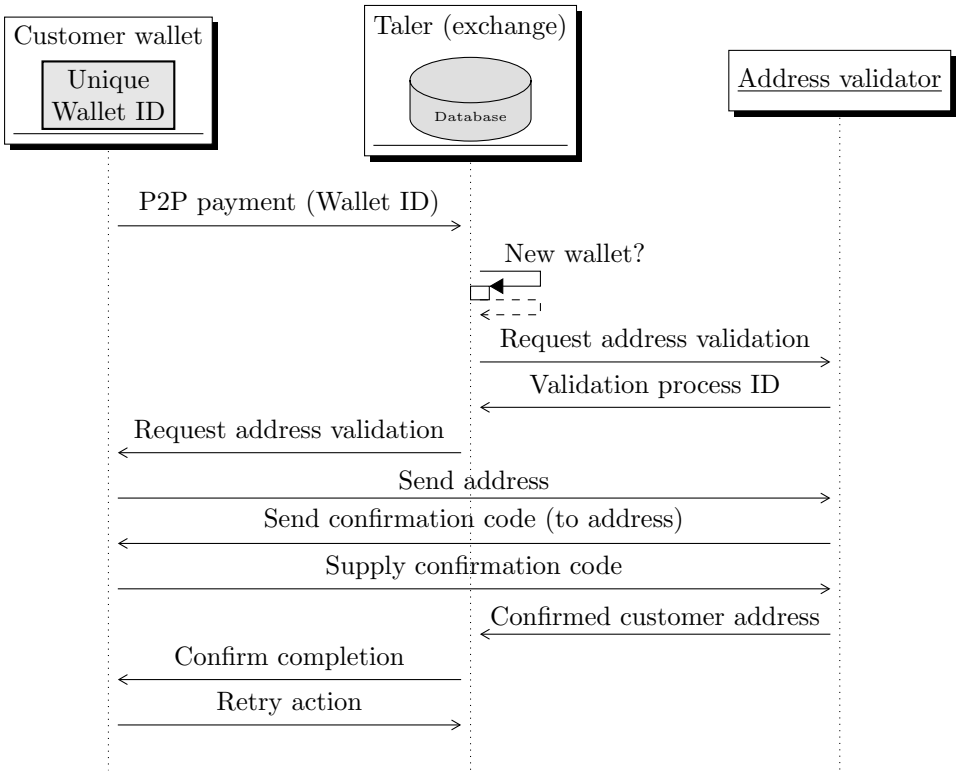

Figure 3.1: Deposit interactions between customer, Taler exchange (payment service provider) and external address validation service. The process can be triggered by wallet-to-wallet (P2P) payments described in Chapter 2.

Our users have to accept the terms of service which restrict the use of the service to domestic customers. For interactions with the core banking system, this simply means that we only accept payments from or to domestic bank accounts. For P2P payments between wallets, we require that the wallets are controlled by a domestic entity. We define domestic entities as those that are able to receive messages at a domestic address. Two types of addresses are supported:

- Control over a domestic **mobile phone number** is established by sending an SMS message with a confirmation code to the MSIN.
- Control over a domestic **postal address** is established by sending a letter with a confirmation code to the address.

Depending on the type of address, a validation has a limited validity period, as shown in Table 3.1. When the validity period is over, a wallet has to re-do the address validation before they can receive any further funds through the service.

Table 3.1: Restrictions on address validations

Type	**Validity period**	**Restricted to**
Mobile phone number	12 months	*+41*
Postal address	36 months	*Switzerland*

3.2 KYC process

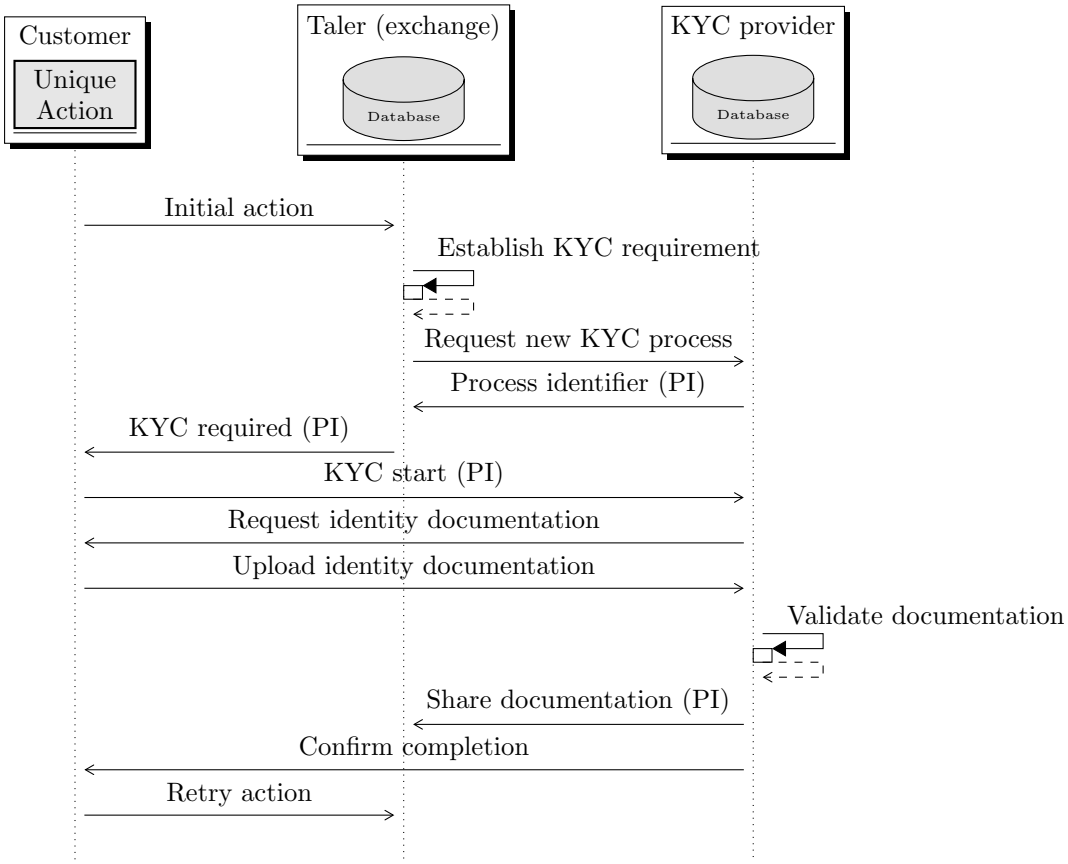

Figure 3.2: Deposit interactions between customer, Taler exchange (payment service provider) and external KYC provider. The process can be triggered by various *actions* described in Chapter 2.

At the beginning of the KYC process, the user needs to specify whether they are an **individual** or a **business**.[1] This then determines which types of attributes are collected in the KYC process (Table 3.2 vs. Table 3.3).

[1]In practice, we expect most wallet-users to be individuals, but in principle a wallet could be owned by a business.

Table 3.2: Information collected for individuals

Type	**Required**	**Example**
Surname	yes	Mustermann
First name(s)	yes	Max
Date of birth	yes	1.1.1980
Nationality	yes	Swiss
Actual address of domicile	yes	Seestrasse 3, 8008 Zuerich
Phone number	no	+41-123456789
E-mail	no	me@example.com
Identification document	yes	JPG image

Table 3.3: Information collected for businesses

Type	**Required**	**Example**
Company name	yes	Mega AG
Registered office	yes	Seestrasse 4, 8008 Zuerich
Company identification document	yes	PDF file
Contact person name	yes	Max Mustermann
Phone number	no	+41-123456789
E-mail	yes	me@example.com
Identification document	yes	JPG image
Date of birth	yes	1.1.1980
Nationality	yes	Swiss
Power of attorney arrangement	yes	PDF file

3.3 KYB process

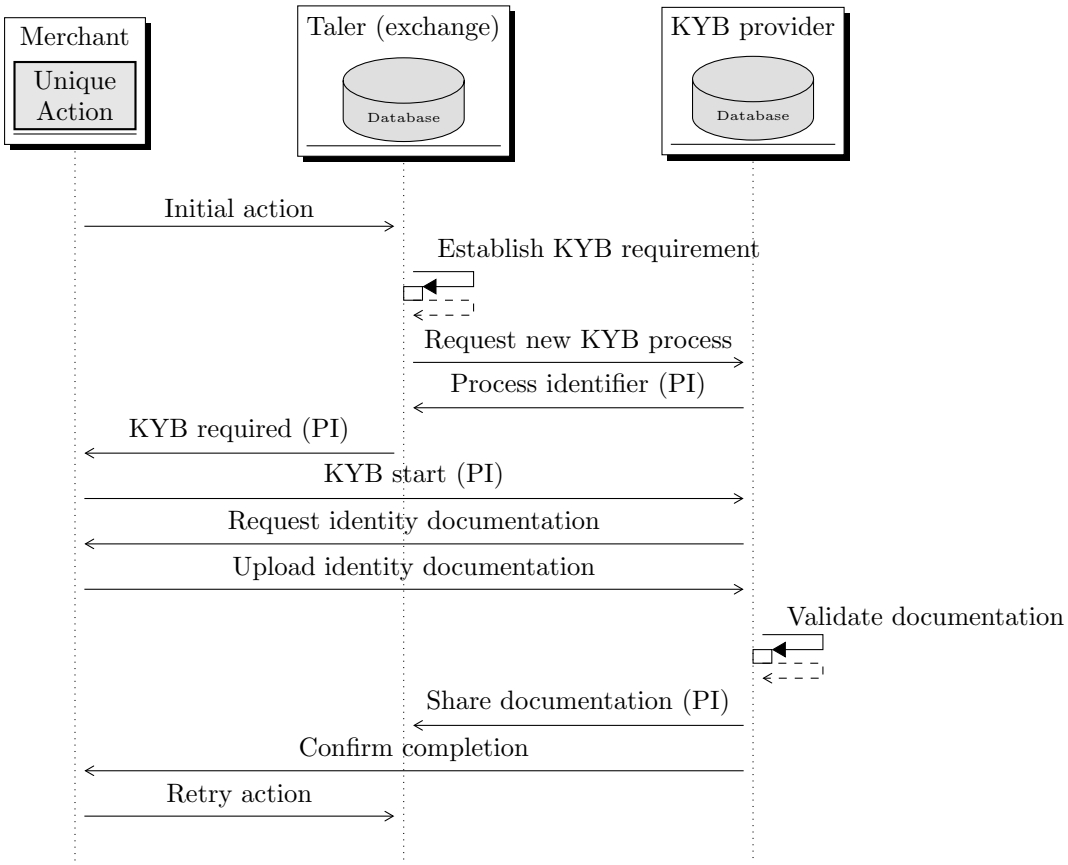

Figure 3.3: Deposit interactions between customer, Taler exchange (payment service provider) and external KYB provider. The process can be triggered by various *actions* described in Chapter 2.

At the beginning of the KYB process, the user needs to specify whether they are an **individual** (not incorporated) or a **business**.[2] This then determines which types of attributes are collected in the KYB process (Table 3.4 vs. Table 3.5).

[2]In practice, we expect most owners of bank accounts crossing the KYB threshold to be businesses, but in principle such a bank account could be owned by an individual operating a business without a separate legal entity.

Table 3.4: Information collected for unincorporated individuals

Type	**Required**	**Example**
Surname	yes	Mustermann
First name(s)	yes	Max
Date of birth	yes	1.1.1980
Nationality	yes	Swiss
Actual address of domicile	yes	Seestrasse 3, 8008 Zuerich
Phone number	no	+41-123456789
E-mail	no	me@example.com
Identification document	yes	JPG image
Taxpayer identification	yes	ZPV Nr. 253'123'456

Table 3.5: Information collected for businesses. Information on individals is collected for owners with more than 25% ownership and for those with signature authority for the business.

Type	**Required**	**Example**
Company name	yes	Mega AG
Registered office	yes	Seestrasse 4, 8008 Zuerich
Company identification document	yes	PDF file
Power of attorney arrangement	yes	PDF file
Business registration number	yes	
Business registration document	yes	PDF file
Registration authority	yes	
Authorized person name	yes	Max Mustermann
Share/authorization certification	yes	PDF file
Identification document	yes	JPG image
Date of birth	yes	1.1.1980
Nationality	yes	Swiss
E-mail	yes	me@example.com
Phone number	no	+41-123456789

3.4 AML process

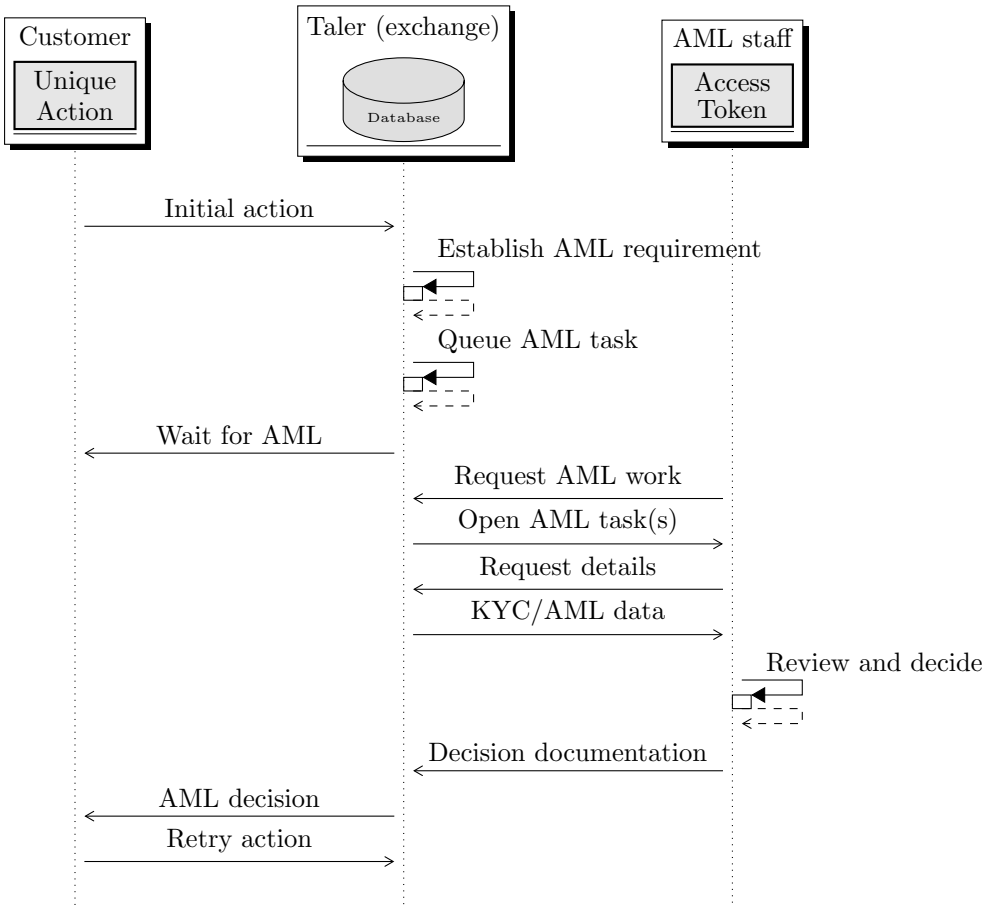

Figure 3.4: Deposit interactions between customer, Taler exchange (payment service provider) and the AML staff. The process can be triggered by various *actions* described in Chapter 2. AML staff interactions are cryptographically secured and decisions and the provided reasoning are archived by the exchange. AML staff may interact with the customer (out-of-band) in its decision process.

Chapter 4

Fees

The business model for operating a Taler exchange is to charge transaction fees. Fees are charged on certain operations by the exchange. There are two types of fees, **wire fees** and **coin fees**. This chapter describes the fee structure.

Fixed, amount-independent **wire fees** are charged on wire transfers using the core banking system. Details on wire fees are described in Section 4.1.

Coin fees are more complex, as they do not exactly follow neither the usual percentage of volume model of other payment systems. Instead, coin fees are applied per coin, resulting in a *logarithmic* fee structure. As a result, the effective fee *percentage* for tiny transactions is high (for example 50% for transactions of 0.0025 CHF) while the effective fee percentage for large transactions is nominal (for example $\approx 0.05\%$ for transactions of ≈ 40 CHF). Details on coin fees are described in Section 4.2.

Fees are configurable (and that fee types beyond those described here are supported by the software). Thus, the specific fees may be adjusted in the future based on business decisions. However, changes to the fees are never retroactively applied to coins already in circulation. Wire fees that have been publicly announced for a particular time period also cannot be changed. Finally, any change to the terms of service must also be explicitly accepted by the users before they withdraw additional funds.

4.1 Fees per wire

Wire fees apply whenever an exchange needs to initiate a wire transfer to another bank account. Wire fees do not apply to every individual payment to a merchant, as merchants can choose to *aggregate* multiple micropayments into one large payment on the wire. Wire fees also do not apply to wallet-to-wallet payments within the Taler system.

A **wire** fee is applied when a merchant receives an aggregated payment into their bank account.

A **closing** fee is applied when a wallet fails to withdraw coins and money has to be sent back to the originating bank account.

Table 4.1: Table with wire fees. Wire fees are set annually.

Year	**Fee type**	**Amount**
2023	wire	*CHF 0.05*
2023	closing	*CHF 0.10*
2024	wire	*CHF 0.05*
2024	closing	*CHF 0.10*
2025	wire	*CHF 0.05*
2025	closing	*CHF 0.10*

4.2 Fees per coin

Payments with Taler are always made using coins. Each coin has a specific denomination, and an exchange will issue coins in different denominations (in the same currency). The fees per coin depend on the operation and the denomination.

The primary fee to be paid is a **deposit** fee that is charged whenever a coin is fully or partially deposited into a bank account or another wallet.

A secondary fee to be paid is a **change** fee that is charged whenever a coin partially spent and change must be rendered.

Coins also have an **expiration** date of approximately **one year**. After the expiration date, coins become worthless. Wallets that are online **three months** *before* a coin expires will automatically trade any such coins for one or more fresh coins with a later expiration date. This process is also subject to the **change** fee.

Table 4.2: Fees per coin. Coin denomination values are given in units of CHF 0.01.

Denomination	**Fee type**	**Amount**
$2^{-4} - 2^{0}$	deposit	*CHF 0.00125*
$2^{-4} - 2^{0}$	change	*CHF 0.00125*
$2^{0} - 2^{3}$	deposit	*CHF 0.00250*
$2^{0} - 2^{3}$	change	*CHF 0.00125*
$2^{4} - 2^{8}$	deposit	*CHF 0.005*
$2^{4} - 2^{8}$	change	*CHF 0.00125*
$2^{8} - 2^{12}$	deposit	*CHF 0.01*
$2^{8} - 2^{12}$	change	*CHF 0.00125*