

# **Das Taler-Bezahlungssystem**

Stefan Kügel      Christian Grothoff

19. Juni 2020

# 1 Das System im Überblick

## Systembestandteile

Taler ist ein elektronisches Bezahlssystem mit besonderer Betonung von Datenschutz und Transaktionssicherheit. Es besteht aus offenen Netzwerkprotokollen, Programmierschnittstellen in verschiedenen Sprachen und einer Hardware-Ausstattung zum Berechnen und Speichern von Daten. Das System weist fünf notwendige Systembestandteile auf:

1. Zentrale Steuerungslogik (Exchange) zum Verwalten sämtlicher Geldtransfers zum und vom Exchange-Treuhandkonto
2. Elektronische Geldbörsen (Wallet) zum Verwalten der Coins (digitale Repräsentanten von Bargeld)
3. Schnittstellen (LibEuFin-Komponente Nexus) zur Anbindung des Exchange-Treuhandkontos an das bestehende EBICS/FinTS-System
4. Anwendung für Verkäufer (Merchant Backend) zum Einfordern und Verwalten von Umsätzen
5. Auditor-Anwendung zur laufenden Kontrolle der Funktionsweise aller Systembestandteile mit automatisch erstellten Prüfberichten

Das System erklären neben diesem Dokument auch die Taler-Homepage<sup>1</sup> und die englischsprachige Dokumentation. Diskussionen werden auf der englischsprachigen Mailingliste geführt.

Taler wird entwickelt von der Firma Taler Systems SA mit Sitz in Luxembourg, deren Entwickler zumeist in Deutschland leben und arbeiten. Informationen zum Geschäftsmodell befinden sich auf Seite 54.

Die Prüfung der Codebasis, der eingesetzten Signaturverfahren, der Transaktionen und der Sicherheitsmaßnahmen im laufenden Betrieb soll durch die Sicherheitsexperten von Code Blau (Berlin) erfolgen, welche als unabhängige Auditoren das System kontrollieren<sup>2</sup>.

Taler verwendet keine Blockchain- oder Distributed-Ledger-Technologie und ist keine virtuelle Währung oder Kryptowährung. Die Werte der elektronischen Münzen in den Geldbörsen der Kunden sind in Euro nominiert.

## Funktionsweise

Taler stellt eine Steuerungslogik bereit, die im weiteren Text Exchange genannt wird. Ein Exchange verwaltet einerseits die Buchungen von und zu Girokonten der Geschäftsbanken

---

1 [taler.net](http://taler.net), siehe auch die Wikipedia-Seite von Taler in englischer Sprache

2 Siehe Webseite von Code Blau ([codeblau.de](http://codeblau.de))

## 1 Das System im Überblick

mithilfe seines Treuhandkontos, andererseits die Buchungen der Transaktionen von und zu den elektronischen Geldbörsen, den Wallets. Die beiden jeweiligen Buchungsströme werden koordiniert vom Exchange. Euro-Gelder bleiben stets im SEPA-Bereich und fließen nur vom Girokonto der Zahlenden über das Treuhandkonto des Exchange-Betreibers auf die Girokonten der Verkäufer.

Ein Wallet kann man sich vorstellen als eine Debit- oder Prepaid-Geldbörse: Ein digitales Pendant zu einer Brieftasche, die statt Scheinen und Geldmünzen kryptografisch signierte Münzen, die „Coins“, enthält, welche wie Bargeld ebenfalls keinen identifizierenden Rückschluss auf ihre Eigentümer gestatten. Ein Coin stellt einen elektronischen Repräsentanten der Zahlungsmittel dar, die auf Basis ihrer Ursprungswährung in die Reserve des Treuhandkontos des Exchange-Betreibers gebucht wurden. Taler ist somit ein Prepaid-System, eine Kreditvergabe hierüber ist ausgeschlossen.

Externe Auditoren werden im laufenden Betrieb automatisch über die Transaktionen des Exchange informiert und können im Fall von Unstimmigkeiten zeitnah reagieren.

Die Nutzer des Taler-Bezahlsystems sollten ihre Coins wie Bargeld behandeln, das heißt: sie dem entsprechend auch sichern. Die Daten eines Wallets mit seinen Coins können auf beliebig vielen digitalen Endgeräten und Speichermedien abgelegt und gesichert werden. Die Wallets verfügen weiterhin über ein eingebautes Backup-Verfahren, mit dem sie die Wallet-Daten bei einem Dienstleister sicher abspeichern. Die Nutzer können mit den Coins bezahlen bzw. diese durch eine Rückbuchung auf ihr Girokonto wieder zurückgeben. Falls sie kein Backup ihrer Wallet-Daten angelegt haben, können sie die Coins auch verlieren.

Die elektronischen Münzen in einem Wallet entsprechen rechtlich einem Eigentumswert im Zugriffsbereich der Wallet-Besitzer, während der Exchange-Betreiber deren Gegenwert in der Ursprungswährung treuhänderisch verwahrt. Der Exchange-Betreiber hat ein Zahlungsverprechen den Wallet-Besitzern gegenüber, wenn diese als Käufer ihre Coins einsetzen, und verantwortet die Weitergabe der realen Geldwerte an die (Giro-)Zielkonten der Verkäufer bei deren Geschäftsbanken.

Die Nutzung des Wallet für den Zahlvorgang in Euro-Währung gestaltet sich folgendermaßen: Der Wallet-Besitzer wählt den Exchange, der Euro anbietet, und löst einen Abhebevorgang aus, der das Girokonto des Wallet-Besitzers mit einer Soll-Buchung belastet und das Treuhandkonto des Exchange-Betreibers mit einer Haben-Buchung beaufschlagt. Der Exchange erlaubt dann dem empfangenden Wallet das Abheben des entsprechenden Betrags an elektronischen Münzen in Euro. Bezahlt werden kann mit diesen Coins in Webshops, an Automaten und bei allen Verkaufsstellen, die am Point of Sale (POS) den Vertragsschluss mit Taler erlauben. Die Verkäufer müssen dabei kein Wallet installiert haben, um in dem Empfang der Zahlungen auf ihren Girokonten zu gelangen.

Der kryptografisch signierte Vertrag enthält die genauen Vertragsbedingungen zwischen Käufer und Verkäufer und ist für eventuelle Streitfälle auch vor Gericht verwendbar als Beleg über den Kauf der Waren zum gegebenen Kaufpreis.

Die Coins annehmenden Verkäufer müssen davon ausgehen, dass ihre Umsätze schon allein durch die Buchung ihrer Einnahmen aus dem Taler-Bezahlsystem auf ihre Girokonten bei Geschäftsbanken als Einkommen leicht nachvollziehbar sind. Zusätzlich dazu sind sie sich der Rolle des externen Auditors bewusst, welcher Unregelmäßigkeiten den Finanzbehörden meldet. Darüber hinaus veranlasst das Bezahlssystem in einem automatisierten Verfahren, dass die

## *1 Das System im Überblick*

Verkäufer bestimmte Vorgänge beim Auditor melden, um diesen in seiner Kontrollfunktion oder in einer spezifischen Aufsichtsfunktion zu unterstützen.

Dadurch bewirkt dieses Bezahlssystem zum einen, dass der Identitätsschutz der Käufer gewahrt bleibt, und zum anderen erschafft es eine Bemessungsgrundlage für die Steuererhebung und verhindert praktisch den Einsatz für illegale Geschäfte. Aufgrund dieser unterschiedlichen, doch konsequent durchzuhaltenden Behandlung der Geldströme auf Käufer- bzw. Verkäuferseite erfüllt Taler sowohl die Anforderungen der Gesetze zur Verhinderung der Geldwäsche (Anti Money Laundering) und der Terrorismusfinanzierung (Know Your Customer) als auch die Gesetze zum Schutz privater Daten einschließlich der Datenschutzgrundverordnung (DSGVO). Gleichzeitig erhalten die Finanzbehörden eine elektronische Datenbasis zur vereinfachten Steuererhebung für die Finanzierung unseres staatlichen und kommunalen Gemeinwesens.

## 2 Geschäftsvorgänge

Dieses Kapitel widmet sich den Geschäftsvorgängen des Bezahlsystems. Beschrieben werden hier die grundlegenden Verfahren (Abhebevorgang und Ausgabe- bzw. Bezahlvorgang, Rückerstattungen und Marktaustritt von Exchange-Betreibern sowie Einkommensnachweis von Verkäufern).

In Kapitel 10 veranschaulichen Screenshots die einzelnen Schritte des Abhebe- und Ausgabevorgangs mit einem Android-Smartphone einschließlich des Abhebevorgangs auf das Smartphone-basierte Wallet mit „Taler-Cashier“ als Automated Teller Machine (ATM), gefolgt von Screenshots des Bezahlvorgangs mit der POS-Anwendung „Merchant“.

### 2.1 Abhebevorgang

Mit dem Abhebevorgang beginnt die „Inwertsetzung“ von Coins in einem Wallet. Dieser Vorgang besteht aus der Soll-Buchung eines (Giro-)Kontos in Fiatwährung, der entsprechenden Haben-Buchung des Treuhandkontos eines Exchange-Betreibers und der Bildung einer Reserve im Exchange mit signierten Coins, welche das Ziel-Wallet schließlich abrufen.

Taler ermöglicht technisch zum gegenwärtigen Zeitpunkt den Abhebevorgang auf der Webseite einer Geschäftsbank oder an einem Bankschalter sowie die webbasierte Buchung mithilfe einer Browser-Erweiterung. Weitere Implementierungen (z.B. Abheben an einem Geldautomaten) sind angedacht oder bereits in Entwicklung. Einen speziellen Abhebevorgang stellt das sogenannte „Tipping“ durch Webseiten dar.

- A1 Integrierter Abhebevorgang vom Girokonto
- A2 Manuelle Überweisung
- A3 Tipping von Webseiten als geringwertige Aufwandsentschädigung

#### 2.1.1 Integrierter Abhebevorgang (A1)

Geschäftsbanken, die ihren Kunden das Abheben in Taler-Wallets erlauben wollen, müssen an ihren Kundenschnittstellen Taler als Aufladeverfahren anbieten. Die anderen Abhebevorgänge (A2, A3) setzen im Gegensatz dazu bei keiner der Kunden-Banken Schnittstellen zu Taler voraus.

Der integrierte Abhebevorgang umfasst folgende Verfahrensschritte:

1. Der Abhebevorgang beginnt immer mit der Anmeldung eines Wallet-Besitzers bei seiner Geschäftsbank mittels Zwei-Faktor-Authentifizierung (Eingabe von Kennung bzw. Einführen von Karte und PIN-Eingabe), bei ATM-Terminals erfolgt die PIN-Eingabe später (Punkt 6).

## 2 Geschäftsvorgänge

2. Zum gegenwärtigen Stand der Entwicklung können Nutzer folgende Abhebeverfahren auswählen:
  - a) Smartphone-Scan des QR-Codes auf der Bank-Webseite  
→ Die Bank erzeugt einen QR-Code, den der Nutzer mit einem Smartphone einliest (zurzeit Android, später auch andere Betriebssysteme)
  - b) Abheben in das Taler-Wallet als Browser-Erweiterung in Firefox, Opera oder Chrome/Chromium  
→ Das Wallet in der Browser-Erweiterung zeigt den abzuhebenden Betrag an, den der Nutzer mit dem Klick auf einen Button bestätigt
  - c) NFC-Read oder Smartphone-Scan an Bankschaltern bzw. Geldautomaten  
→ Die NFC-Schnittstelle zeigt den Betrag an bzw. der QR-Code wird mit dem Smartphone eingelesen
  - d) Smartphone-Scan mit Bargeldeinzahlung an einer Kasse mittels App „Taler-Cashier“  
→ Die Cashier-App auf dem Gerät des Kassierers erzeugt einen QR-Code, den der Nutzer mit seinem Android-Smartphone einliest

Der Nutzer wählt das Verfahren und gibt die Geldmenge ein, die später vom persönlichen Wallet als Coins abgehoben werden soll.

3. Mit der so erhaltenen Information stellt das Wallet eine Anfrage bei der Bank und erfährt damit von der Verfügbarkeit des vom Kunden gewünschten Betrags in der gegebenen Währung auf dessen Girokonto. Daraufhin öffnet das Wallet einen Dialog, um dem Nutzer die Auswahl des Exchange-Betreibers zu ermöglichen.
4. Der Nutzer wählt den Exchange. Falls der Nutzer neu ist, einen neuen Exchange wählen will oder sich die Allgemeinen Geschäftsbedingungen (AGB) des bisherigen Exchange-Betreibers geändert haben, werden dem Nutzer die AGB angezeigt, die er bestätigen muss. Gleichfalls werden die allgemeine Gebührenordnung des Taler-Bezahlsystems sowie die spezifischen Gebühren für den aktuellen Abhebevorgang angezeigt.
5. Wenn der Nutzer den Vorgang bestätigt, erzeugt das Wallet mit dem EdDSA-Kryptoverfahren frische Credentials (Zugangsberechtigung) für den Abhebevorgang und teilt der Bank den sogenannten Public key mit. Der Nutzer wird auf die Benutzerführung der Bank-Webseite bzw. des ATM-Terminals zurückverwiesen.
6. Dem Nutzer werden dort nochmals der Betrag und der gewählte Exchange angezeigt. Er muss gegenüber der Bank endgültig bestätigen, dass der Abhebevorgang nun ausgelöst werden soll. Dieser Abhebevorgang kann mit und ohne Authentifizierung erfolgen:
  - a) Ohne TAN-Eingabe im Fall von Beträgen unterhalb eines von der Bank festgelegten Limits: Gemäß *Payment Services Directive 2* (PSD2) kann die Obergrenze des Transaktionsbetrags pro Vorgang ohne TAN-Autorisierung 50 Euro betragen, allerdings nur fünfmal hintereinander oder bis ein weiteres Kann-Limit von 150 Euro Umsatz in Summe erreicht wird<sup>1</sup>.

---

<sup>1</sup> Siehe BaFin-Fachartikel Starke Kundenauthentifizierung

## 2 Geschäftsvorgänge

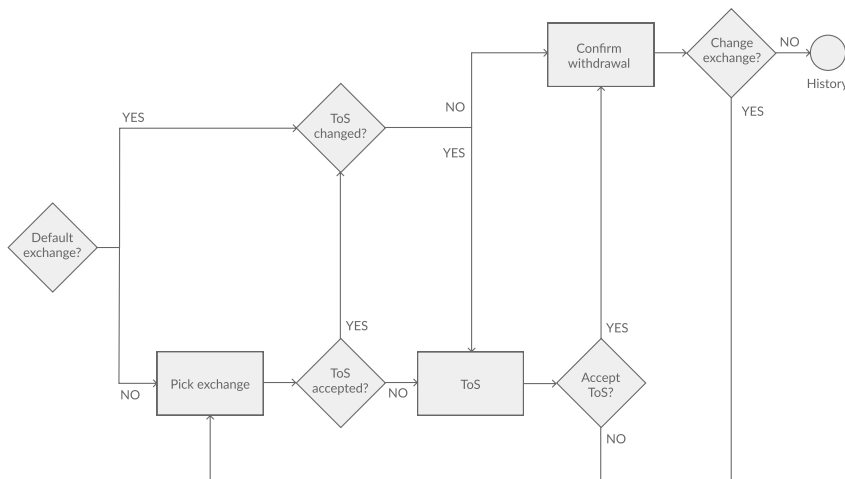
- b) Mit einer Zwei-Faktor-Authentifizierung (mTAN, photoTAN, Karten-PIN bei ATM-Terminals o.ä.): Die Bank verlangt vom Kunden die finale Autorisierung der Buchung, die sie damit ausführt.

Die Bank überweist den Betrag vom Girokonto an den gewählten Exchange unter Angabe des vom Wallet erzeugten Public key. Die Credentials erscheinen als Buchungsvermerk im Girokontoauszug der Nutzer. Damit ist jeder Aufladevorgang mit den betreffenden Geldwerten und Zeitpunkten eindeutig zuzuordnen und nachvollziehbar.

7. Der Public key dient zum Prüfen der korrekten Verbindung zwischen Wallet und Exchange. Damit wird in der Datenbank des gewählten Exchange eine Reserve über den Betrag der Girokontoüberweisung erzeugt, aus welcher das empfangende Wallet dann Coins abheben kann.
8. Mit dem Verfahren SEPA Instant Credit Transfer (SCT Inst) kann das Wallet die Coins in Echtzeit abheben, andernfalls mit normaler SEPA-Überweisung innerhalb eines Banktags. Dafür benötigt das Wallet die Credentials, die es vorher erzeugt hat. Sollte das Wallet dazu nicht in der Lage sein (z.B. weil der Nutzer es versäumt, das Wallet online gehen zu lassen), schließt der Exchange die Reserve automatisch wieder und überweist den Betrag (abzüglich einer Gebühr) auf das ursprüngliche Konto zurück. Das Zeitfenster für den Abhebevorgang wird als *Closing Time* bezeichnet und beträgt 14 Tage. Dieser Zeitraum sollte für Nutzer normalerweise ausreichen, um den Abhebevorgang abschließen zu können. Er sollte auch nicht zu lang sein, damit die Kunden bei eventuellen Problemen nicht zu lange auf ihre Rücküberweisungen warten müssen.

Die nachfolgende Grafik zeigt die Benutzerführung bei der Auswahl des Exchange und der Anzeige dessen AGB vor dem Abhebevorgang (Verfahrensschritt 4):

WITHDRAWAL PROCESS FLOW



### 2.1.2 Manuelle Überweisung (A2)

Die manuelle Überweisung besteht für den Fall, dass Taler-Nutzer von Girokonten abheben wollen, deren kontoführende Geschäftsbank Taler (noch) nicht unterstützt. Sie müssen hierfür den gewünschten Betrag mittels konventioneller Girobuchung an einen Exchange überweisen, von dem ihre Wallets dann den Betrag automatisch abheben. Die Wallet-Software liefert ihnen dazu die Überweisungsdaten, die sie einfach und schnell in ein Überweisungsformular von Hand oder mit dem vom Wallet erzeugten QR-Code übertragen:

1. Der Nutzer gibt den gewünschten Aufladebetrag im Wallet ein und wählt den Exchange.
2. Das Wallet erzeugt die Credentials und zeigt sie zusammen mit der Bankverbindung des gewählten Exchange an.
3. Diese Daten werden in die Felder des Überweisungsformulars für eine SEPA-Überweisung vom Girokonto auf den Exchange übertragen (manuell oder mit dem QR-Code als `payto://-URI` für Banking-Anwendungen).
4. Sobald die Überweisung beim Exchange angekommen ist, hebt das Wallet die Coins des Aufladebetrags gemäß Punkt 8 des integrierten Abhebevorgangs ab.

### 2.1.3 Tipping (A3)

Tipping ist eine geringfügige Aufwandsentschädigung von Webseiten an ihre Besucher. Webseiten können dies nutzen, um Besucher für das Betrachten von Werbung oder die Preisgabe von Daten zu belohnen z.B. bei Kundenrezensionen oder Bewertungen gekaufter Artikel. Den Nutzern bietet man damit einen Anreiz in Form eines Kleinstbetrags, der auf ihre Taler-Wallets gebucht wird. Dazu erzeugt die Webseite für das Wallet ein Token, durch welches das Wallet einen auf den Geldwert begrenzten Zugriff auf eine Reserve bekommt, die der Webseiten-Betreiber an einem Exchange seiner Wahl angelegt hat. Der Vorgang verlangt dann noch eine einfache Bestätigung durch die Webseiten-Besucher, mit der ihre Wallets die Coins abheben können.

## 2.2 Ausgabevorgang

Genauso wie den Abhebevorgang steuert die Software des Exchange im Zusammenspiel mit der Wallet-Software auch den Ausgabevorgang, das Bezahlen mit Coins. Dreh- und Angelpunkt aller Ausgabevorgänge ist der Exchange.

Mit den Coins verfügen die Wallet-Besitzer über elektronische Repräsentanten der Geldwerte, die der jeweils beim Abhebevorgang gewählte Exchange auf seinem Treuhandkonto vorhält. Kommt es zur Zahlung mit Coins, werden die Geldwerte vom Treuhandkonto an die empfangenden Girokonten der Verkäufer weitergebucht.

Mit „Verkäufer“ gemeint sind alle Stellen, die das Bezahlsystem am Point of Sale akzeptieren und Taler-Coins annehmen (z.B. Webshops, Webseiten, Supermärkte, Ladengeschäfte,



## 2 Geschäftsvorgänge

Verkaufsautomaten, Kiosksysteme, POS-Kassen usw.). Die Verkäufer müssen kein Wallet installiert haben, um bezahlt zu werden. Falls das digitale Endgerät der Nutzer beim Ausgabevorgang einmal keinen Internetzugang haben sollte, können Wallets auch über Internet-Zugänge von Verkäufern am Point of Sale mit dem Exchange kommunizieren und die Bezahlung durchführen.

Der Exchange sammelt Zahlungen von verschiedenen Kunden, bündelt diese nach Empfängern sortiert zu Sammelbuchungen und überweist diese zugunsten der betreffenden (Verkäufer-)Girokonten. Die Sammelbuchung („Aggregation“) minimiert Transaktionskosten und erhöht die Effizienz der Buchungsverarbeitung zwischen den Banken. Die Verkäufer können die Frequenz der Sammelbuchung bestimmen und sind aufgrund der Tatsache, dass für jede aggregierte Buchung eine im Protokoll ausgewiesene Gebühr vom Exchange erhoben wird, auch geneigt, die Häufigkeit der Überweisungen ökonomisch zu halten (siehe Gebührenarten).

Sollte ein Exchange zu hohe Überweisungsgebühren verlangen, schlägt die Händlersoftware diese Gebühren ganz oder zum Teil dem zu zahlenden Betrag bei den Kunden dieses Exchange auf. Für die Sammelbuchung führt der Exchange zum entsprechenden Zeitpunkt eine Soll-Buchung auf das Treuhandkonto seiner Bank aus, die entsprechende Haben-Buchung erfolgt zugunsten des Empfängerkontos.

Wird ein Coin ausgegeben, ist das Coin entwertet. Wer es zuerst ausgibt, verfügt über den bewegten Geldwert. Der Exchange bestätigt mit einer elektronischen Signatur dem Verkäufer beim Empfang eines Coin, dass der Verkäufer der Erstempfänger ist.

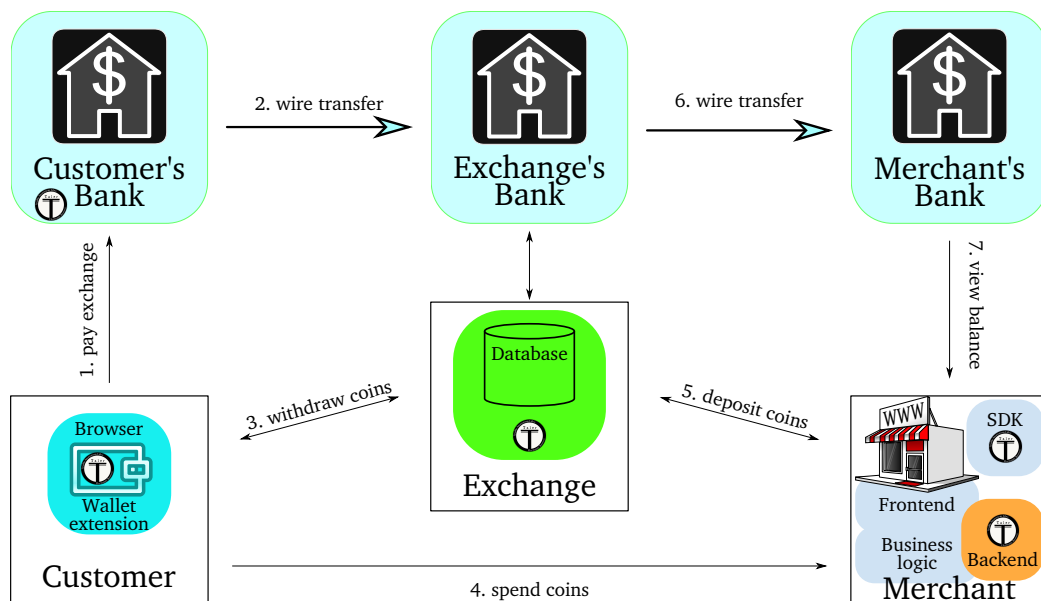
Ein Kopieren der Coins (was zwangsläufig aus deren redundanter Speicherung an verschiedenen Orten resultiert) erzeugt identische Coins von gleichem Wert. Wer die Verfügungsgewalt über diese identischen Coins besitzt, kann mit ihnen Zahlungen auslösen und so ihren Geldwert in Fiatwährung weiterbuchen lassen - jedoch nur exakt einmal pro Coin.

Ein regulärer Ausgabevorgang kommt z.B. zum Einsatz bei:

- B1 Gewöhnlicher Vertragsschluss zum Erwerb von Gütern im Internet (kein Point of Sale)
- B2 Point of Sale/Verkaufsautomaten (einschließlich der Möglichkeit der automatischen Rückerstattung beim Abbruch des Verkaufsvorgangs durch den Automaten, falls bei diesem ein technisches Problem auftritt)
- B3 Spenden

Die nachfolgende Illustration veranschaulicht die Abhebe- und Ausgabevorgänge:

## 2 Geschäftsvorgänge



### 2.3 Wechselgeld und zeitliche Gültigkeit von Coins

Bei Bezahlvorgängen kann es aufgrund der festen nominalen Stückelung der Coins notwendig sein, dass der Nutzer Wechselgeld erhält. Zur Ausgabe von Wechselgeld benutzt Taler das sogenannte *Refresh*-Protokoll, welches „frische“ Coins erzeugt.

Des Weiteren haben Coins ein Ablaufdatum. Bevor das Ablaufdatum eines Coin erreicht ist, sollten Taler-Nutzer das Refresh-Protokoll auslösen, um Coins mit einem neuen Ablaufdatum zu erhalten. Refresh-Operationen werden bei Bedarf vom Wallet automatisch ausgelöst, um die Gültigkeit der Coins zu verlängern (siehe auch Nicht-transaktionsbezogene Kosten: Wertverluste).

### 2.4 Rückerstattungen (Refund)

Solange ein Verkäufer noch keine Sammelbuchung mit einem bestimmten Ausgabevorgang eines Käufers erhalten hat, für den er nach Abschluss des Kaufvertrags einen Rabatt einräumen will oder von dem er zurücktreten möchte, kann er im Taler-System einen Teilbetrag bzw. den vollständigen Betrag des betreffenden Vorgangs an seinen Kunden zurückerstatten lassen. Dieses Rückerstattungsverfahren wird *Refund* genannt. Das Taler-Wallet des Käufers erhält den entsprechenden Betrag (gegebenenfalls abzüglich Gebühren) in Form von frischen Coins.

## 2.5 Marktaustritt eines Exchange (Recoup)

Im Fall eines Marktaustritts des Exchange-Betreibers oder in seinem Insolvenzfall erlaubt das Taler-Protokoll, dass alle Wallets automatisch über den Marktaustritt informiert werden. Dieser Geschäftsvorgang wird durch das *Recoup*-Unterprotokoll realisiert. Die Wallets senden automatisch alle Coins dieses Exchanges zurück und koppeln dies mit der Anweisung, den entsprechenden Betrag auf die Girokonten der jeweiligen Nutzer zurückzuerstatten. Dafür wird das Girokonto verwendet, von dem die Geldwerte für die Coins ursprünglich abgehoben wurden. Der Exchange veranlasst daraufhin die entsprechenden Soll-Buchungen des Treuhandkontos. Für den Recoup schließt das Taler-Protokoll Gebührenbelastung für die Coin-Eigentümer aus, obwohl dem Exchange-Betreiber Kosten für IBAN-Überweisungen entstehen (→ Gebührenarten).

Welche rechtlichen Rahmenbedingungen und Konsequenzen für Exchange-Betreiber im Fall eines Marktaustritts bzw. bei einer Insolvenz zu beachten sind, wird in einem Kapitel dieser Systembeschreibung explizit behandelt.

## 2.6 Einkommensnachweis von Verkäufern

Eine zuständige Behörde kann bei diesem Geschäftsvorgang Transaktionen nachvollziehbar machen, die auf Seite der Verkäufer zu Einkommen führen, und so eine Einkommensverfolgung anstrengen.

1. Voraussetzung ist, dass die Geschäftsbank des Verkäufers der Behörde Zugriff auf Buchungen erteilt hat, die auf dem Girokonto des Verkäufers eingehen.
2. Unter den Haben-Buchungen des Girokontos findet die Behörde möglicherweise Überweisungen eines Taler-Exchange. Diese Überweisungen haben im Feld Verwendungszweck die Web-Adresse des Exchange-Betreibers sowie eine eindeutige Identifikationsnummer für jede Sammelbuchung des Exchange.
3. Mithilfe dieser beiden Daten kann die Behörde automatisiert beim Exchange eine HTTP-Anfrage stellen, um die Liste der Mikrotransaktionen zu bekommen, die als Sammelbuchung aggregiert vom Treuhandkonto des Exchange auf das Girokonto des Verkäufers überwiesen wurden. Mit den Mikrotransaktionen erhält die Behörde den genauen Betrag des Kaufpreises und den kryptographischen Hash des Vertragstexts. Mit jedem Hash garantiert der Exchange, dass der dazugehörige Vertrag von einem Käufer-Wallet elektronisch unterzeichnet wurde.
4. Die Behörde kann gegebenenfalls von einem Verkäufer verlangen, den kompletten Vertragstext zu offenbaren, der zu diesem Hash verarbeitet wurde. Das Taler-Bezahlungssystem speichert automatisch für jede Transaktion alle kompletten Vertragstexte unter den dazugehörigen Hashes zusammen mit den kryptographischen Beweisen in einer Datenbank beim Verkäufer. Verkäufer können Behörden den direkten Zugriff auf diese Daten per HTTP freischalten.

## 3 Gebühren

Von den Nutzern des Bezahlsystems können Gebühren erhoben werden, um die zwangsläufig auftretenden betriebsnotwendigen Kosten von Exchange-Betreibern zu decken. Variable Kosten umfassen hauptsächlich Kosten für Strom sowie für IBAN-Buchungen zugunsten von Girokonten. Fixkosten fallen vor allem an für Personal, Hardware und Marketing. Eine normale Geschäftsbank wird die Kosten ihres Exchange, den sie in-house oder in einem Rechenzentrum betreibt, auf die Nutzer verteilen wollen. Das Taler-Protokoll stellt deshalb je eine Gebühr zur Wahl für die sechs Buchungsarten *Withdrawal*, *Deposit*, *Refresh*, *Refund*, *Wire fee* und *Closing*. Exchange-Betreiber bestimmen selbstständig die Kombination dieser Gebührenarten und deren Höhe, jedoch immer im Rahmen, den das Taler-Protokoll vorgibt.

Die Gebühren sollen zum einen die Käufer und Verkäufer, die das Bezahlsystem nutzen, zu einem ökonomischen Buchungsverhalten anleiten, zum anderen die Kosten der Bereitstellung des Bezahlsystems umschlagen bzw. bei gegebenem Bedarf verursachungsgerecht abbilden und auch den Verursachern direkt belasten. Exchange-Betreiber bestimmen die Höhe der jeweiligen Gebühr für jeden Coin-Nominalwert (fixer Nennwert, festgelegt mit dem Denomination key).

Der Audit-Report jedes Exchange sendet automatisch sowohl an die externen Auditoren als auch an den Exchange-Betreiber eine Aufstellung der laufenden Einnahmen aus jeder einzelnen Gebührenart.

### 3.1 Gebührenordnung

Während das Taler-Protokoll die verfügbaren Gebührenarten festlegt, legen Exchange-Betreiber mithilfe von Parametern Mindest- und Höchstwerte der Gebühren fest. Die Gebührenhöhe im Bezahlsystem wird damit von den Exchange-Betreibern bestimmt. Die pro Nennwert von Coins eingepflegten Gebührenhöhen erhebt die Exchange-Logik dann automatisch mit den auftretenden Buchungsarten.

Änderungen an der Gebührenordnung sind nur möglich konform mit der Genehmigung des Bezahlsystems durch Aufsichtsbehörden wie die BaFin. Rechtliche Grundlage für die Gebührenerhebung sind die Allgemeinen Geschäftsbedingungen der Exchange-Betreiber, bezüglich der auftretenden *IBAN-Buchungen* die AGB der Geschäftsbanken, die diese mit ihren Kunden hinsichtlich deren Girokonten vereinbaren.

#### 3.1.1 Verpflichtungen der Exchange-Betreiber

Exchange-Betreiber verpflichten sich, die Gebührenordnung einzuhalten. Andernfalls können sie ihren Schnittstellenzugang verlieren, ihre Zertifizierung aberkannt bekommen und darüber hinaus sogar schadenersatzpflichtig werden.

### 3 Gebühren

Für jede der auftretenden Buchungsarten gibt es eine Gebührenart, deren Höhe jeder Exchange-Betreiber festlegt. Ein Wert von 0 kommt damit der Abwahl von Gebühreneinkünften aus der betreffenden Buchungsart gleich. Das Bezahlsystem verfügt über sieben Buchungsarten, von denen drei (nämlich *Wire fee*, *Closing* und *Recoup*) den Exchange-Betreibern Kosten wegen IBAN-Buchungen verursachen. Das Unterprotokoll *Recoup* erlaubt dem Exchange-Betreiber keine Festlegung von Gebühren, da die Kosten der Rücküberweisung von Vermögenswerten bei einem Marktaustritt nicht den Coin-Eigentümern belastet werden dürfen, sondern vom Exchange allein getragen werden müssen.

Alle sechs Gebührenarten auf 0 zu setzen würde die Gebührenordnung für Taler-Nutzer vereinfachen und das Bezahlsystem attraktiver machen. Exchange-Betreiber müssen jedoch die Möglichkeit haben, einen eventuellen Missbrauch mit Buchungen, die besonders hohe Kosten verursachen, durch die Erhebung von Gebühren zu verhindern bzw. zu vermindern. Besonders dem anonym und unbegrenzt oft auslösbaren *Refresh* muss im Missbrauchsfall mit einer Gebühr begegnet werden können. Setzt der Exchange-Betreiber beispielsweise die Refresh-Gebühren auf Höhe der ihm konkret für diese Buchungsart anfallenden Kosten an, bereitet böswillige Kostentreiberei mit Refresh-Buchungen zumindest dem Exchange keinen Schaden, sondern belastet nur jene Nutzer, die besonders häufig einen Refresh ausführen lassen (dazu ausführlich weiter unten).

Exchange-Betreiber willigen ein, dass ihre Audit-Reports Einnahmen aus Gebühren an die Auditoren und dem entsprechend auch an Aufsichtsbehörden melden. Sie können Gebühren auf Coins nur zu deren Ausgabezeitpunkt festsetzen und nachträglich nicht mehr ändern. Gebühren auf Banküberweisungen sind gemäß des Taler-Protokolls immer nur jährlich anpassbar und vom Exchange-Betreiber mindestens für 2 Jahre in die Zukunft festzulegen. Durch diese Gebührenkonstanz können die Verkäufer ihre aufzuschlagenden Kosten besser planen und in ihre Verkaufspreise einkalkulieren.

Die AGB jedes Exchange müssen zudem die Nutzer unmissverständlich darauf hinweisen, dass es bei einem selbstverschuldeten Verzicht auf die Sicherung durch ein Backup-Tool (wie z.B. „Anastasis“) zum Totalverlust des Coin-Eigentums kommen kann (siehe Kapitel Nicht-transaktionsbezogene Kosten: Wertverluste).

Eine Privatkundenbank, die einen Exchange hostet und normalerweise bei ihren Kunden Gebühren für deren IBAN-Buchungen erhebt, hat die Möglichkeit zu bestimmen, ihren Kunden beim Abheben vom hauseigenen Girokonto in Taler-Wallets diese Gebühren zu erlassen.

#### 3.1.2 Verpflichtungen von Käufern

Die Nutzer haben vor dem ersten Abhebevorgang beim jeweiligen Exchange dessen AGB zu lesen und zu bestätigen. Dieser Schritt wird von Nutzern bei Änderungen der AGB ebenfalls zwingend verlangt. Sie akzeptieren mit ihrer Einwilligung in die AGB des Exchange, den sie aktiv auswählen, zum Beispiel eventuelle Wertverluste durch *Refresh*-Gebühren, die der Exchange-Betreiber erheben kann. Alle Gebührenarten und -höhen werden den Nutzern vor jedem Abhebevorgang angezeigt, einschließlich der *Wire fee*-Gebühr. Spezifische vorgangsbezogene Transaktionsgebühren, welche die Nutzer zu tragen hätten, werden vom Wallet immer im Rahmen der interaktiven Buchung angezeigt.

### 3 Gebühren

Die Nutzer verpflichten sich gemäß AGB, keinen Schadenersatzanspruch gegen das Bezahlungssystem oder den Exchange-Betreiber zu stellen wegen Verlusten, die ihnen durch Diebstahl oder selbstverschuldeten Verzicht auf Sicherung der Coins im persönlichen Wallet entstehen.

Des Weiteren müssen Nutzer gemäß AGB akzeptieren, dass die IBAN-Überweisung vom persönlichen Girokonto der Nutzer zum Exchange-Treuhandkonto je nach Vertrag mit der Hausbank Kosten verursachen kann, die unabhängig von Taler anfallen [bei deutschen Banken zurzeit um 9 Cent pro TAN für eine IBAN-Buchung]. Diese Kosten stehen mit dem Taler-Bezahlungssystem in keinerlei Bezug und können von ihm auch nicht beeinflusst werden.

#### 3.1.3 Verpflichtungen von Verkäufern

Die Sammelbuchung der Verkäuferumsätze, die eine Mehrzahl von Ausgabevorgängen der Käufer in einem Betrag an das empfangende Girokonto zusammenfasst und deren Frequenz die Verkäufer bestimmen, verursacht dem Exchange-Betreiber Kosten für jede IBAN-Buchung. Daher wird der Exchange-Betreiber angehalten sein, für diese Buchungsart die Gebühr *Wire fee* den Verkäufern zu belasten, denn diese sind die Verursacher der Sammelbuchung und nicht etwa die Käufer. Das Taler-Wallet zeigt den Käufern diese Gebühr an. Beim Abhebevorgang gibt das Wallet dem Käufer die komplette Übersicht über die Gebührenordnung an. Übernimmt ein Verkäufer jedoch die Gebühr anstelle seiner Kunden, zeigen die Wallets der Kunden bei diesem Verkäufer keine *Wire fee* mehr an. Diese Verkäufer machen so für ihre Kunden die Gebührenordnung übersichtlicher, verbergen allerdings die Gebühr einkalkuliert in ihren Verkaufspreisen. Sollten Exchange-Betreiber aus Sicht der Verkäufer eine zu hohe *Wire fee* verlangen, schlägt die Händlersoftware diese ganz oder zum Teil dem zu zahlenden Betrag bei den Kunden dieses Exchange auf (zur Umlage einer zu hohen *Wire fee* auf Kunden mithilfe eines Amortisationsfaktors, den Verkäufer bestimmen können, siehe Gebührenstrukturen).

Die AGB des Exchange [und nicht die AGB eines Exchange, mit dem die Verkäufer *keine* Vertragsbindung eingehen!] weisen unmissverständlich darauf hin, dass die Verkäufer, der indirekt den Käufer daran bindet, das Risiko eines Wertverlusts bis hin zum Totalausfall tragen, wenn sie für Überweisungen auf ihre Konten die IBAN zwar syntaktisch richtig, aber für ein falsches Zielkonto angeben. Sollten Verkäufer falsche Kontendaten einpflegen, haften sie selbst für daraus resultierende Schäden und nicht etwa ein Exchange-Betreiber. Ebenso tragen allein die Verkäufer weitere Gebühren aufgrund einer Fehlbuchung, die sie verursachen und für die ein manuelles Routing nötig wird (z.B. bei erloschenen Empfängerkonten).

#### 3.1.4 Technische Rahmenbedingungen der Gebührenerhebung

Gebühren werden erhoben pro Coin bzw. pro Banküberweisung. Die Anzahl an Coins wächst üblicherweise logarithmisch mit dem repräsentierten Betrag. Gebühren können anfallen sowohl auf Flussgrößen (z.B. auf bewegte Coins bei Abhebevorgängen und Ausgabevorgängen) als auch auf Bestandsgrößen (z.B. die aufbewahrten Coins in Wallets). Die Gebühren auf Coins können sich unterscheiden je nach Ausgabezeitpunkt eines Coin und je nach Wert eines Coin, sie sind für jedes Coin mit seinem Ausgabezeitpunkt festgelegt, können also nachträglich vom Exchange-Betreiber nicht geändert werden.

### 3 Gebühren

Jede Gebührenart wird selbst bei einer Höhe von 0 Einheiten immer als Variable in der Exchange-Schnittstelle geführt (siehe Dokumentation der Exchange RESTful JSON API). Während des gesamten Zeitraums der Gültigkeit aller Denomination keys (mögliche Nennwerte der Coins, die ein Exchange signiert) haben alle gewählten Gebührenarten ihre Gültigkeit beizubehalten.

## 3.2 Gebührenarten

Das Taler-Protokoll bietet folgende Gebührenarten:

1. ABHEBEN vom Girokonto (*Withdrawal*): Für jedes erfolgreiche Abheben vom Girokonto, pro Coin
2. AUSGEBEN / BEZAHLEN (*Deposit*): Für jeden Ausgabevorgang, pro Coin
3. WECHSELGELD (*Refresh*): Pro Coin bei
  - a) Wechselgeld-Buchungen
  - b) Ablauf des Gültigkeitszeitraums von Coins
  - c) Transaktionsabbruch infolge von Netzwerkfehlern sowie bei
  - d) *Refund*
4. RÜCKERSTATTUNGEN (*Refund*): Für Erstattungen oder bei Vertragsrücktritt durch Verkäufer, pro Coin
5. UMSATZVERBUCHUNG (*Wire fee*): Für die aggregierte Buchung von Umsätzen auf ein Zielkonto des Verkäufers, pro Überweisung
6. SCHLIESSEN DER RESERVE (*Closing*): Falls nach einer Überweisung an den Exchange das Wallet die Coins nicht abheben sollte, pro Rücküberweisung auf das Ursprungskonto

### 3 Gebühren

#### 3.2.1 Effekte der Gebührenarten auf Exchange-Betreiber, Käufer und Verkäufer

Jede der genannten Gebührenarten wird nun jeweils betrachtet aus Sicht der Käufer, der Exchange-Betreiber und der Verkäufer:

<b>Withdrawal aus Sicht der Käufer</b>
Wer Taler-Wallets mit Coins bestücken möchte, muss dazu eine IBAN-Buchung vom persönlichen Girokonto zugunsten des Exchange-Treuhandkontos auslösen, wofür je nach Vertrag mit der Hausbank Kosten anfallen. Dazu kommt die Withdrawal-Gebühr, die das Taler-Protokoll für jedes Coin, das ins Wallet abgehoben wird, verlangen kann. Auch wenn viele Bankkunden bereits an die Kostenpflicht von IBAN-Buchungen gewöhnt sind, wirkt die Withdrawal-Gebühr wie ein Kaufkraftverlust schon vor beabsichtigten Umsätzen, über den die Käufer durch die Anzeige aller Gebührenarten beim Abheben in Kenntnis gesetzt werden. Sobald sich die Käufer bewusst werden, dass sie die Kosten für jedes erzeugte Coin zu tragen haben, werden sie es vorziehen, möglichst wenige Coins mit hohen Nennwerten in ihre Wallets abheben zu lassen.
<b>Withdrawal aus Sicht der Exchange-Betreiber</b>
Eine Gebühr auf jedes erzeugte Coin würde tatsächlich alle geschaffenen elektronischen Münzen treffen und die Kosten ihrer Erzeugung verteilen, verhindert jedoch keinen Missbrauch mit anderen Buchungsarten und würde zudem jene Nutzer diskriminieren, die viele kleinere Nennwerte aufbuchen. Manche Nutzer könnten die Kosten des Exchange durch vermehrte Refresh-Buchungen mit Coins höherer Nennwerte steigern, die Kosten dafür sind jedoch marginal gering.
<b>Withdrawal aus Sicht der Verkäufer</b>
Withdrawal-Gebühren stellen zwar für Verkäufer keine Kosten dar, doch sind sie für ihre Kunden eine Hemmschwelle, Taler zu benutzen, wenn sie schon beim Abheben diese Gebühren angezeigt bekommen. Die Verkäufer würden es sogar vorziehen, die Kosten für die Erzeugung von Coins in ihre Verkaufspreise einzukalkulieren und vor den Kunden zu verbergen. Die <i>für Kunden</i> beim Abhebevorgang erzeugten Coins stehen allerdings mit den Verkäufern in keiner direkten Beziehung.
<b>Deposit aus Sicht der Käufer</b>
Obwohl die Kunden die Deposit-Buchung mit dem Kauf von Gütern auslösen, müssen die Verkäufer die Deposit-Gebühr pro Coin tragen, jedoch nur bis zu einem vom Verkäufer bestimmten Maximalwert. Der diesen Maximalwert übersteigende Rest der Deposit-Gebühr muss vom jeweiligen Käufer getragen werden. Mittels Deposit-Gebühren könnte man theoretisch alle Kosten des Exchange-Betriebs auf alle <i>eingesetzten</i> Coins verteilen. Die Käufer können in der Regel leicht nachvollziehen, dass eine Gebühr auf eingesetzte deponierte Coins erhoben wird.
<b>Deposit aus Sicht der Exchange-Betreiber</b>
Bei der Deposit-Buchung vergleicht die Exchange-Logik den Public key jedes Coin mit den in einem Array gespeicherten Schlüsseln der Postgres-Datenbank des Exchange und untersucht für jedes Coin, ob es erstmalig zur Bezahlung eingelöst wird. Dieser Vorgang verbraucht nur wenig Energie und bringt keine weiteren Kosten mit sich. Für Exchange-Betreiber können die marginal geringen Kosten erst bei einer exorbitanten Menge an Deposit-Buchungen bedeutend werden. Deposit-Gebühren stellen vor allem die wichtigste Einkommensquelle für den Exchange-Betreiber dar und können über alle eingesetzten Coins erhoben werden.
<b>Deposit aus Sicht der Verkäufer</b>



### 3 Gebühren

<p>Verkäufer werden darauf Wert legen, dass (1.) der vom Käufer gewählte Exchange die regulatorischen Auflagen der Aufsichtsbehörden und der Gesetze gegen Geldwäsche erfüllt, (2.) der Exchange im SEPA-Währungsraum operiert und (3.) die Gebühren des gewählten Exchange sich im Rahmen dessen befinden, was der Verkäufer mithilfe der seiner Maximalwerte für Deposit-Gebühren (und wie unten beschrieben auch für die Wire fee-Gebühr) festlegt.</p> <p>Wenn ein Exchange-Betreiber für Deposit-Buchungen verhältnismäßig hohe Gebühren verlangt, beeinflussen diese auch jede <i>Refund</i>-Buchung bei einer teilweisen Rabattierung, denn die hohen <i>Deposit</i>-Gebühren tragen die Käufer, wodurch die Rabattierung aus Sicht der Käufer schlechter wird. Nur bei einem kompletten Rücktritt vom Vertrag durch den Verkäufer befreit die <i>Refund</i>-Buchung die Käufer von <i>Deposit</i>-Gebühren, doch es entstehen durch die <i>Refund</i>-Buchung bei Vertragsrücktritt auch <i>Refresh</i>-Gebühren, die von den Käufern zu tragen wären.</p>
<p style="text-align: center;"><b>Refresh aus Sicht der Käufer</b></p>
<p>Refresh-Gebühren werden mehrheitlich verursacht durch die Erzeugung von frischen Coins als <i>Wechselgeld</i> (Beträge werden mit Coins von höherem Nennwert bezahlt) und durch die <i>Refund</i>-Buchung (nachträgliche Rabattierung oder Stornierung von Kaufverträgen). Seltener sind Refresh-Buchungen aufgrund des Ablaufs der Gültigkeit von Coins oder wegen Transaktionsabbrüchen durch Netzwerkfehler. Die Gebühr auf Refreshs wird pro Coin erhoben. Sie soll bei einer missbräuchlichen Anwendung entstehende Kosten vom Exchange abhalten und wird den Käufern belastet. Käufer werden diese Gebühr durch einen Missbrauch mit Refresh-Buchungen marginal nur als geringe persönliche Belastung betrachten, da deren absolute Höhe pro Coin niedrig ausfällt.</p>
<p style="text-align: center;"><b>Refresh aus Sicht der Exchange-Betreiber</b></p>
<p>Solange kein Missbrauch mit Refresh-Buchungen stattfindet, muss der Exchange-Betreiber abwägen, ob er die Kosten für Refreshs auf die Käufer direkt abwälzt oder mit einer anderen Gebührenart deckt. Die Refresh-Gebühr für den Missbrauchsfall heranzuziehen bedeutet, dass der Verursacher böswilliger Refreshs sämtliche Käufer eines Exchanges bei ihren regelmäßigen Refresh-Buchungen belasten. Dies verhindert zwar Missbrauch nicht, sondern macht nur die Buchungsart für diejenigen kostspielig, die oft Refreshs auslösen. Im akuten Missbrauchsfall werden Käufer mit Wire fee-Gebühren belastet. Die böswilligen Kostentreiber treffen damit wenigstens keinen konkreten Exchange, sondern alle Endverbraucher, die von ihm signierte Coins erhalten.</p>
<p style="text-align: center;"><b>Refresh aus Sicht der Verkäufer</b></p>
<p>Die Refresh-Buchung betrifft Verkäufer nicht direkt, jedoch die Refund-Buchung.</p>
<p style="text-align: center;"><b>Refund aus Sicht der Käufer</b></p>
<p>Im Gegensatz zur Gebührenart Refresh sind Verursacher der Refund-Buchung die Verkäufer - und nicht die Käufer. Bei einem teilweisen Refund infolge von Rabattierung nach dem Kaufvertragsschluss würden die bereits verbrauchten, deponierten Coins mit einer Refund-Gebühr belastet. Nur bei einem vollständigen Refund werden die Coins der Käufer von den <i>Deposit</i>-Gebühren entlastet, wohl aber mit den ungleich höheren Refresh-Gebühren belastet [stimmt das so?]. Auch bei einer teilweisen Rabattierung liegt im Regelfall die Ursache beim Verkäufer. Aus Sicht der Käufer sollten daher die Verkäufer diese Gebühr tragen.</p>
<p style="text-align: center;"><b>Refund aus Sicht der Exchange-Betreiber</b></p>

### 3 Gebühren

<p>Exchange-Betreiber können Refund-Buchungen nicht unterdrücken, da sie den Verkäufern die Möglichkeit zu Rabatten und Rücktritten von Kaufverträgen einzuräumen haben. Ein teilweiser Refund entlastet die Käufer teilweise von ihren Deposit-Gebühren, so dass diese mit der Zeit Verkäufer meiden, die nach Vertragsschluss oft rabattieren müssen. Verkäufer, die wiederholt mutwillig wiederholt komplette Refunds auslösen, befreien zwar die bereits beim Exchange deponierten Coins der Käufer von Deposit-Gebühren, belasten diese jedoch durch Refresh-Gebühren. Sollte ein Exchange-Betreiber dann auf die Refresh-Gebühr verzichten, würde er sich hohe Kosten aufbürden und evt. bankrottieren. Um dies zu vermeiden, muss der Exchange-Betreiber Refresh-Gebühren einführen bzw. erhöhen, wodurch er alle seine Kunden höher belastet. Sowohl die Kosten für den teilweisen als auch für den kompletten Refund müssten aus Sicht der Exchange-Betreiber die Verkäufer tragen, damit diese einen Anreiz verspüren, Rabattierungen oder Rücktritte möglichst zu vermeiden, die Vereinbarungen über Waren und Dienstleistungen den Kaufverträgen entsprechend zu erfüllen und ebenso ihre Käufer anzuhalten, seltener Rücksendungen und Vertragsrücktritte auszulösen (mit allen ökonomischen und ökologischen Effekten, die damit verbunden sind, z.B. durch häufige willkürliche Warenrücksendungen).</p>
<p style="text-align: center;"><b>Refund aus Sicht der Verkäufer</b></p>
<p>Zum heutigen Stand der Implementierung tragen bei einem Rücktritt vom Kaufvertrag die Käufer die Kosten der Refund-Buchung komplett, bei einer teilweisen Rabattierung tragen die Käufer die Deposit-Gebühr für ihre verbrauchten Coins. Verkäufern liegt es grundsätzlich daran, Rabatte und Rücktritte ökonomisch zu halten.</p>
<p style="text-align: center;"><b>Wire fee aus Sicht der Käufer</b></p>
<p>Diese Gebühr trifft die Käufer nur direkt in folgendem Fall: Das Protokoll erlaubt den Verkäufern, die Kosten der Gebühr teilweise auf die Käufer abzuwälzen, wenn der Exchange-Betreiber, der die Coins der Käufer signierte, die Wire fee-Gebühr über dem Wert einstellte, den jeder Verkäufer in seinem Merchant Backend mit der Variable <code>max_wire_fee</code> einpflegen kann (aber nicht muss). Die Kosten der Wire fee-Gebühr sind in die Preise der Verkäufer einkalkuliert. Die Verkäufer könnten die relativen Kostenvorteile des Taler-Bezahlsystems in Form von niedrigeren Endverbraucherpreisen an ihre Kunden weiterreichen, sind dazu aber nicht gezwungen.</p>
<p style="text-align: center;"><b>Wire fee aus Sicht der Exchange-Betreiber</b></p>
<p>Die Wire fee-Gebühr wälzt die Kosten für IBAN-Buchungen vom Treuhandkonto an die Verkäuferkonten ab - vom Exchange-Betreiber auf die Verkäufer. Die Käufer bekommen die Wire fee nur angezeigt, wenn der Verkäufer sie nicht übernimmt. Ansonsten merken die Kunden nicht, welche Gebühr von ihren verbrauchten Coins beim Exchange einbehalten wird. Für Exchange-Betreiber käme eine Abwahl der Wire fee gleich einem Freibrief an die Verkäufer, so oft wie möglich eine Sammelbuchung ihrer Umsatzeinkünfte auszulösen. Verlangt der Exchange-Betreiber hingegen die Wire fee per Überweisung an die Verkäuferkonten, führt diese Gebühr dazu, dass die Verkäufer die Häufigkeit der Sammelbuchung so einstellen, wie sie es für ihre Unternehmungen benötigen und sich die Gebühr dafür leisten möchten. Wenn die Frequenz dieser Buchungsart steigt, steigen auch die absoluten Kosten für die Verkäufer. Die Käufer erfahren von der Wire fee-Gebühr nur im Fall, dass ein Exchange-Betreiber diese höher setzt als der Wert, den ein Verkäufer in der Variable <code>max_wire_fee</code> eingepflegt hat.</p>
<p style="text-align: center;"><b>Wire fee aus Sicht der Verkäufer</b></p>
<p>Verkäufer wünschen möglichst schnell und oft ihre Umsätze zu verbuchen. Eine zeitnahe Umsatzverbuchung verbessert ihre Liquidität und bringt Zinsmitnahmen, wenn Umsatzeinkünfte früher als die Auszahlungen an Lieferanten eingehen. Sie sind daher gezwungen abzuwägen, ob sie lieber höhere absolute Kosten durch die Wire fee tragen oder auf Liquidität verzichten. Bei einigen Verkäufern entscheidet hingegen die Menge an Buchungen über die Häufigkeit der Sammelbuchung, um die Abteilungen für Accounting und Billing nicht zu überlasten. In jedem Fall sind die Kosten der Wire fee in die Endverbraucherpreise einkalkuliert.</p>

### 3 Gebühren

<b>Closing aus Sicht der Nutzer</b>
Die Closing-Buchung lösen Nutzer des Bezahlsystems aus, wenn sie nach einer erfolgreichen IBAN-Überweisung an das Treuhandkonto eines Exchange die Reserve nicht ins persönliche Wallet abheben lassen, weil sie das Wallet nicht innerhalb von 14 Tagen mit dem Taler-Exchange verbinden lassen. Da sie die Verursacher sind und dem Exchange für die Rücküberweisung Kosten bereiten, haben sie auch die Closing-Gebühr zu tragen. Dies erfolgt durch die Überweisung des ursprünglich überwiesenen Aufladebetrags abzüglich der Kosten für IBAN-Buchung und evt. manuelles Routing. Die Gebühr ist leicht durchzusetzen und stößt bei den meisten Nutzern auf Verständnis, denn im Regelfall werden sie von dieser Gebührenart nicht betroffen sein und können auch den AGB-Passus schnell nachvollziehen, dass die Verursacher die Kosten für selbstverschuldetes Nichtabheben tragen müssen.
<b>Closing aus Sicht der Exchange-Betreiber</b>
Die Kosten der Closing-Buchung entstehen dem Exchange-Betreiber aufgrund eines nicht regulären Nutzerverhaltens. Auf diesen Kosten darf er jedoch nicht sitzenbleiben, sondern muss sie dem verursachenden Nutzer belasten. Die Closing-Gebühr ist für Exchange-Betreiber unverzichtbar, um Missbrauch durch Kostentreiberei zu verhindern. Die Gebühr zu verlangen und einzubehalten gelingt stets reibungslos, da das Treuhandkonto des Exchange mit einer Überweisung bebucht wurde - und nicht mit einer SEPA-Lastschrift, die vom Nutzer in böswilliger Absicht storniert werden könnte.
<b>Closing aus Sicht der Verkäufer</b>
Die Closing-Buchung betrifft Verkäufer in keiner Weise.

### 3.2.2 Tabellarische Zusammenfassung

<b>Buchungsart</b>	<b>Withdrawal</b>	<b>Deposit</b>	<b>Refresh</b>	<b>Refund</b>	<b>Wire fee</b>	<b>Closing</b>
<b>Verursacher</b>	Käufer	Käufer	Käufer	Verkäufer	Verkäufer	Käufer
<b>Kostenträger</b>	Käufer	Verkäufer, Käufer bei hoher Exchange- Gebühr	Käufer	Käufer	Verkäufer, Käufer bei hoher Exchange- Gebühr	Käufer
<b>Kosten pro</b>	Coin	Coin	Coin	Coin	Überweisung	Überweisung
<b>IBAN-Kosten</b>	Ja, für Käufer	Nein	Nein	Nein	Für Exchange	Für Exchange
<b>Kosten für Nutzer</b>	?	Haupteinnahme- quelle für Exchange	?	Zuerst auf 0 lassen, nur bei Missbrauch anheben	?	Zuerst auf 0 lassen, nur bei Missbrauch anheben

### 3.2.3 Gebührenhöhen im Missbrauchsfall

Der Normalfall eines Buchungszyklus besteht aus *Withdrawal*, *Deposit* und *Wire fee* - wenn die zu zahlenden Beträge mit Coins von genau passenden Nennwerten beglichen werden. Für alle anderen Beträge, für die ein Coin von höherem Nennwert eingesetzt wird, muss die *Refresh*-Buchung Wechselgeld erzeugen, d.h. einen oder mehrere frische Coins ins Wallet buchen, bis der Differenzbetrag erreicht ist.

### 3 Gebühren

Refresh-Buchungen können jedoch anonym unbegrenzt oft mit schadhafte Absichten gegen Exchange-Betreiber ausgelöst werden. Jeder Exchange-Betreiber kann daher im Missbrauchsfall mit unterschiedlichen Gebührenhöhen gegen mutwillige oft ausgelöste Buchungsarten angehen.

- Missbrauch durch *Withdrawal*-Buchungen ist unwahrscheinlich, da die Kosten der IBAN-Überweisungen erst einmal von den Inhabern der Girokonten getragen werden.
- Missbrauch durch *Deposit*-Buchungen ist unwahrscheinlich, da der Exchange-Betreiber in der Regel Deposit-Gebühren erheben wird.
- Missbrauch durch *Refresh*-Buchungen ist möglich und bedarf einer differenzierten Behandlung: Im Normalfall wird ein Exchange-Betreiber keine Refresh-Gebühr erheben auf die Zahlung mit Coins unpassender Nennwerte (Wechselgeld), im Missbrauchsfall muss er diese Gebühr jedoch schon erheben. Ein Exchange setzt die Refresh-Gebühren dann auf einen hohen Wert, wenn seine Kunden massenhaft Refreshs auslösen (1.) mit Coins bei einem Transaktionsabbruch oder (2.) bei massenhaft wiederholtem *Refund*, den allerdings die Verkäufer auslösen und dessen Kosten fallweise tragen. Im extremen Missbrauchsfall - wenn ein Exchange unter mutwilligen Refresh-Buchungen leidet, muss er die Kosten dafür über die Refresh-Gebührenart auf alle Coin-Eigentümer, deren Coins von diesem Exchange signiert wurden, abwälzen.
- Missbrauch durch *Refund*-Buchungen ist theoretisch möglich und kann ebenfalls behandelt werden mit der Einführung oder Erhöhung von *Refund*-Gebühren.
- Verkäufer könnten das Einsparpotenzial von Sammelbuchungen verringern, indem sie eine zu hohe Frequenz der Aggregatsbuchungen auf ihre Girokonten einstellen. Eine Kostentreiberei durch zu hohe Frequenz der Sammelbuchungen ist möglich, da sie im Interesse der Verkäufer liegen. Exchange-Betreiber können dem massenhaften Auslösen der Sammelbuchungen mit hohen Frequenzen mit der *Wire fee*-Gebühr begegnen.
- Missbrauch durch Rücküberweisungen infolge von Nichtabheben ins Wallet belastet den Exchange mit Kosten für IBAN-Überweisungen, hier kann eine *Closing*-Gebühr zur Abwehr eingeführt werden, um das Problem abzustellen.

#### 3.2.4 Empfehlung der Höhen der Gebührenarten

Aus der vorangegangenen Diskussion der Gebührenarten ergibt sich eine Empfehlung für die Wahl der *Deposit*-Gebühr als wichtigster Gebührenart, da diese eine wesentliche Einnahmequelle des Exchange-Betreibers darstellt.

### 3 Gebühren

Gebührenart	Höhe
<b>Deposit</b>	Wesentliche Einnahmequelle des Exchange-Betreibers
<b>Wire fee</b>	Proportional kostendeckend für IBAN-Überweisungen; dient zur generellen Belastung der Verkäufer mit Kosten und Sammelbuchungskosten
<b>Closing</b>	Kostendeckend, nur zu erheben bei Verdacht auf Missbrauch, Vermeidung von Missbrauch durch Nichtabheben
<b>Refresh</b>	Kostendeckend, nur zu erheben bei Verdacht auf Missbrauch; wirkt gegen Missbrauch durch mutwillig ausgelöste Refreshs; als Negativzins
<b>Refund</b>	Kostendeckend, nur zu erheben bei Verdacht auf Missbrauch bei Refund, gegen mutwilliges Wiederholen von Refund-Spend-Refund-Spend...
<b>Withdrawal</b>	Missbrauch ist unwahrscheinlich; Missbrauch wäre theoretisch denkbar durch das Horten von Geld, um Negativzinsen zu vermeiden

Ebenso empfiehlt sich dem Exchange-Betreiber, im Missbrauchsfall folgende Gebührenhöhen festzulegen:

1. *Wire fee* als Gebührenart zum Decken der IBAN-Kosten, die zuerst nur die Verkäufer mit Kosten belastet und die letzten Endes deren Kunden in den Verkaufspreisen begleichen.
2. *Closing* als Gebührenart sollte jeder Exchange-Betreiber wählen in Höhe der Kosten für IBAN-Buchungen bei einem eventuellen Nichtabheben der Wallets seiner Nutzer.
3. *Refresh* hilft fallweise gegen Missbrauch, wenn Verkäufer massenhaft Refund auslösen sollten oder anonyme Wallets massenhaft Refreshs auslösen.
4. *Refund*-Gebühren sollten Exchange-Betreiber nur um einem eventuellen Missbrauch mit Refund-Buchungen zu begegnen kostendeckend festlegen.

## 4 Nicht-transaktionsbezogene Kosten: Wertverluste

Wertverluste sind nicht-transaktionsbezogene Kosten, die im Gegensatz zu den transaktionsbezogenen Gebühren, die im Normalfall der Nutzung auftreten, in Sonderfällen für die Nutzer entstehen können.

### 4.1 Wertverluste zu Lasten des Wallet-Guthabens

Drei Möglichkeiten bestehen, bei denen die Käufer Wertverluste ihres Coin-Guthabens tragen:

1. Verlust, Zerstörung oder Untergang eines Wallet, für das kein Backup angelegt wurde (Totalverlust des Guthabens)
2. Wertverlust in Höhe von Refresh-Gebühren auf das Wallet-Guthaben nach Ablauf der Gültigkeit der Coins (→ Parameter DURATION\_SPEND)
3. Kompletter Verfall der Coins nach Ablauf eines bestimmten Zeitraums ohne Refresh (z.B. 1 Jahr), weil so lange keine Internet-Verbindung des Wallet bestand

Zu 1.: Die AGB jedes Exchange müssen ihre Nutzer unmissverständlich darüber aufklären, dass sie für eine Sicherung ihrer Wallets verantwortlich sind und bei einem selbstverschuldeten Verzicht auf die Sicherung durch ein Backup-Tool wie z.B. „Anastasis“ den Totalverlust ihres Coin-Eigentums riskieren.

Zu 2.: Mit dem Refresh-Protokoll kann die Abzinsung von Coin-Guthaben gesteuert werden. Die Abzinsung ist laut Protokoll zurzeit so eingestellt, dass alle Coins bei einem Onlinegehen des Wallet geprüft werden, ob ihre Erzeugung länger als zwei Jahre zurückliegt. Die zeitliche Gültigkeit jedes Coin wird damit geprüft. Der Exchange-Betreiber legt dazu den Parameter DURATION\_SPEND (z.B. auf 2 Jahre) fest und bestimmt damit, wann die Refresh-Buchung *aufgrund des Alters eines Coin* greift und für alle betroffenen Coins frische Credentials erzeugt. Dieser Refresh ist gleichbedeutend mit einem Negativzins auf das betroffene Coin-Guthaben infolge von Refresh-Gebühren: Im gegebenen Beispiel mit DURATION\_SPEND = 2 Jahre wäre dies eine Abzinsung des Guthabens nach 2 Jahren in Höhe der Refresh-Gebühr, die der Exchange-Betreiber mit dem Parameter FEE\_REFRESH bestimmt.

Zu 3.: Der Zeitraum, in dem keine Wallet-Verbindung zur Exchange-Schnittstelle bestand und nach dessen Ablauf das Wallet einen Refresh-Vorgang mit komplettem Verfall der Coins anstößt, sollte vom Exchange-Betreiber lang genug eingestellt sein. Dieser Zeitraum muss

#### 4 Nicht-transaktionsbezogene Kosten: Wertverluste

so lang sein, dass ein Nutzer mit einer hohen Wahrscheinlichkeit ein digitales Endgerät mit seinem persönlichen Wallet darauf online gehen lässt. Für den Fall keiner Verbindung in diesem Zeitraum ist nach dessen Ablauf der Exchange-Betreiber neuer Eigentümer der Werte verfallener Coins.

An dieser Stelle sei noch einmal daran erinnert, dass Taler ein Bezahlsystem ist und kein Aufbewahrungsmittel zum Horten von Geldwerten. Im Normalfall verbinden Nutzer des Bezahlsystems ihre Wallets im gegebenen Zeitraum (hier 1 Jahr) und lösen mit jedem Verbinden einen Refresh aller Coins aus, der ihre Gültigkeitsdauer erneut um 2 Jahre verlängert.

Da für den initialen Betrieb des Taler-Exchange keine Refresh-Gebühren vorgesehen sind, werden die Nutzer auch nicht von Gebühren auf Refreshs ihrer Coins belastet.

Zu den rechtlichen Konsequenzen hinsichtlich Abzinsung, Verfall und Verjährung von Coin-Guthaben siehe 6.1.2 .

### 4.2 Wertverluste zu Lasten des Verkäuferumsatzes

Es bestehen folgende zwei Möglichkeiten, bei denen die Verkäufer Wertverluste ihrer Umsätze aus den deponierten Coins ihrer Kunden riskieren:

1. Bei einer Fehlbuchung aufgrund falsch angegebener IBAN-Kontonummer des Verkäufers bzw. erloschener Empfängerkonten und damit nötigem manuellem Routing (mit Gebühren nach Kostentabelle der Geschäftsbank des Verkäufers bzw. der GLS Bank).
2. Nach fehlerhaften Überweisungen (IBAN syntaktisch richtig, aber falsches Zielkonto). Wird dies zu spät vom Verkäufer bemerkt, um den Fehler noch durch ein manuelles Routing zu korrigieren, kann es auch hier zu einem Totalverlust kommen, insbesondere wenn der Betrag bereits auf das falsche Zielkonto gebucht wurde.

Das Bezahlsystem weist an geeigneter Stelle Verkäufer darauf hin, dass Verkäufer beim Einpflegen der IBAN ihres Geschäftsgirokontos Vorsicht walten lassen, damit sie Wertverluste durch Selbstverschulden vermeiden.

# 5 Gebührenstrukturen

## 5.1 Der initiale Exchange-Betrieb

Bei einer initialen Einführung des Betriebs schlagen wir eine einfache Gebührenstruktur vor. Es würden für die Buchungsarten *Refresh* und *Refund* zunächst keine Gebühren erhoben. Dies hat zur Folge, dass den Nutzern beim Auffrischen ihrer Coins durch die Refresh-Buchungen kein Nachteil entsteht und die Nennwerte der frischen Coins denen der „alten“ Coins entsprechen. Für den Fall, dass es zu einem eventuellen Missbrauch durch Refresh- oder Refund-Buchungen käme, sollte der Exchange-Betreiber Refresh- und Refund-Gebühren in Höhe von jeweils 0,25 Cent pro Coin durchgehend für alle Coin-Nennwerte einführen, um den Missbrauch für deren Verursacher kostspielig werden zu lassen.

Auch für den fiktiven Fall, dass ein negativer Zins auf Guthaben des Treuhandkontos erhoben würde und die Gebühreneinnahmen des Exchange signifikant hohe Negativzinsen nicht decken, könnte der Exchange-Betreiber *Refresh*-Gebühren in Höhe der Negativzinsen einführen. In jedem Fall würde diese Abzinsung von Coin-Werten jedoch erst für Coins gelten, die der Exchange nach der Umstellung auf die neue Gebührenordnung mit *Refresh*-Gebühren signiert.

Des weiteren würde der Exchange-Betreiber *Wire fee*-Gebühren in Höhe von beispielsweise 10 Cent pro IBAN-Buchung erheben, um die Kosten seiner IBAN-Buchungen zu decken. *Closing*-Gebühren für Rücküberweisungen auf Ursprungskonten würden zunächst nicht erhoben. Sollte der Exchange-Betreiber ein problematisches Transaktionsvolumen mit *Closing*-Buchungen feststellen, ist er gut beraten, auch für diese 10 Cent pro Buchung zu erheben.

Diese Tabelle veranschaulicht die Gebühren auf Coins und Buchungen beim initialen Exchange-Betrieb:

Coin-Nennwerte	Deposit-Gebühr pro Coin	Gültigkeitsdauer
0,25 bis 64 Cent	0,25 Cent	1 Jahr
128 bis 1024 Cent	0,50 Cent	1 Jahr
2048 bis 65536 Cent	1,00 Cent	1 Jahr
	Wire fee-Gebühr	
	10,00 Cent	

Aus der Tabelle ersichtlich sind unterschiedliche Höhen der Deposit-Gebühr auf die Coin-Nennwerte innerhalb der drei Bandbreiten von 0,25 bis 64 Cent, 128 bis 1024 sowie 2048

Tabelle 5.1: Gebührenstruktur



bis 65536 Cent. Die *Wire fee*-Gebühr beträgt 10 Cent pro IBAN-Überweisung auf Verkäufer-Empfängerkonten. *Refund*-, *Refresh*- und *Closing*-Gebühren bleiben auf Null gesetzt (per default). Die Gültigkeitsdauer ist mit `DURATION_SPEND` (Deposit lifetime) für die drei Bandbreiten auf 1 Jahr eingestellt, was bedeutet, dass alle Coins jedes Nennwerts innerhalb eines Jahres ausgegeben oder durch eine Refresh-Operation gegen neue Coins getauscht werden müssen, sonst verfallen sie.

### 5.2 Beispielrechnungen: Normalbetrieb

Alice hebt 5 Euro von ihrem Konto ab, lädt ihr persönliches Wallet mit Coins dieses Werts, zahlt damit 3,23 Euro für Brötchen und danach 30 Cent für einen Zeitungsartikel am Kiosk. Beim Abhebevorgang bekommt sie je eine Münze mit folgenden Nennwerten: 4, 16, 32, 64, 128, und 256 Cent. Für die Brötchen bezahlt sie mit Coins der Nennwerte 4 Cent, 64 Cent und 256 Cent und bekommt ein Coin mit dem Nennwert 1 Cent mittels der *Refresh*-Buchung als Wechselgeld. Für die drei eingesetzten Coins fallen  $1 \times 0,25$  Cent und  $2 \times 0,50$  Cent, also insgesamt 1,25 Cent, an *Deposit*-Gebühren an. Da der Verkäufer mit einem Parameter festgelegt hat, sich bis zu 0,5% seines Umsatzes an den *Refresh*-Gebühren seiner Kunden zu beteiligen, fallen für Alice keine Gebühren an<sup>1</sup>.

Der Verkäufer könnte nun manuell veranlassen, den Umsatz mit Alice vom Exchange auf sein Geschäftskonto zu überweisen, oder auf den Zeitpunkt zu warten, bis die Sammelbuchung seiner Umsätze automatisch erfolgt. Nehmen wir beispielsweise an, dass der Verkäufer zum Zeitpunkt der automatisch ausgelösten Sammelbuchung einen Umsatz erlöst hat, der das Vierfache von Alice's Umsatz beträgt. Der Verkäufer bekommt auf sein Girokonto dann insgesamt 12,77 Euro überwiesen: Bei einem Umsatz von  $4 \times 3,23$  Euro = 12,92 Euro trägt er Gebühren von insgesamt 15 Cent ( $4 \times 1,25$  Cent an *Deposit*-Gebühren plus  $1 \times 10$  Cent *Wire fee*-Gebühr).

Der Zeitungskiosk soll hingegen in dieser Beispielrechnung nicht bereit sein, sich an den Gebühren seiner Kunden zu beteiligen. Da der Kiosk nur wenige Artikel verkauft, setzt der Kioskbetreiber seinen Amortisationsfaktor `wire_fee_amortization` für die *Wire fee*-Gebühr auf 4. Diesem stimmen die Kunden durch Einwilligung in die AGB des Kioskbetreibers zu. Damit wird der Kaufpreis für Alice höher als die 30 Cent für die Zeitung. Sie zahlt insgesamt 33 Cent, denn sie trägt über die 30 Cent für die Zeitung noch 2,5 Cent an *Wire fee*-Gebühr (10 Cent für die *Wire fee*-Gebühr des Verkäufers geteilt durch seinen Amortisationsfaktor 4) plus die *Deposit*-Gebühr von 0,5 Cent für ein eingesetztes Coin, denn Alice zahlt mit ihrem Coin des Nennwerts 128 Cent. Sie erhält dafür Wechselgeld mit Coins der Nennwerte 1, 2, 4, 8, 16 und 64 Cent. Für das Wechselgeld fallen ihr keine *Refresh*-Gebühren an.

Sollte Alice in dieser Beispielrechnung nun noch einen weiteren Artikel des gleichen Kaufpreises kaufen, kann sie mit ihren Coins der Nennwerte 2 und 32 Cent bezahlen. Hier wäre die *Deposit*-Gebühr für die kleineren Coins zwar geringer (0,25 Cent pro Coin), aber dafür bräuchte sie zwei Coins und trägt somit ebenfalls eine *Deposit*-Gebühr von insgesamt

---

<sup>1</sup> Mit dem Parameter `default_max_deposit_fee` bestimmen Verkäufer prozentuale oder absolute Grenzwerte ihrer Gebührenübernahme.

## 5 Gebührenstrukturen

0,5 Cent. Der Preis bliebe damit bei 33 Cent für Zeitung mitsamt Gebühren, und in diesem Fall gibt es Wechselgeld mit einem Coin von 1 Cent Nennwert.

Gibt der Kioskbetreiber nur diese zwei Artikel zur Sammelbuchung an sein Girokonto, erhält er vom Exchange-Betreiber 55 Cent: 2 x 30 Cent Verkaufspreis plus 2 x 2,5 Cent *Wire fee*-Gebühr, die wegen des Amortisationsfaktors anteilig von Alice getragen werden, minus 10 Cent *Wire fee*-Gebühr an den Exchange-Betreiber für die Sammelbuchung.

Der Exchange-Betreiber erhält für alle genannten Buchungen 20 Cent an *Wire fee*-Gebühren (jeweils 10 Cent von Bäcker und vom Kioskbetreiber) sowie 6 Cent an *Deposit*-Gebühren von Alice, insgesamt also 26 Cent bei einem Gesamtumsatz von 3,83 Euro.

### 5.3 Beispielrechnungen: Mit Refresh-Gebühr

Alice hebt 5 EUR von ihrem Konto ab, und zahlt damit 3.23 EUR für Brötchen und danach 30 cent für einen Zeitungsartikel. Beim Abhebevorgang bekommt Sie je eine Münze mit den Nennwerten: 4, 16, 32, 64, 128, und 256 cents. Für die Brötchen bezahlt Sie mit den 4 cent, 64 cent und 256 cent Münzen, und bekommt eine 0.25 und eine 0.5 cent Münze (via refresh) für Wechselgeld (minus die 0.25 cent „refresh“ Gebühr). Für die Münzen fallen 1x0.25 und 2x0.50 cent, also insgesamt 1.25 cent an *Deposit* Gebühren an. Da der Bäcker bereit ist, sich bis zu 0.5% vom Umsatz an den Gebühren zu beteiligen, fallen für Alice nur die Refresh-Gebühren an. Sollte der Händler insgesamt 4x genau diese Einnahme machen, bekommt er weiterhin genau 12.77 EUR überwiesen, da er 4x 1.25 cent an *Deposit*-Fees plus 1x 10 cent *Wire*-Fees tragen müsste.

Die Zeitung ist geiziger, und ist nicht bereit, sich an Gebühren zu beteiligen. Da sie wenige Artikel verkauft, setzt die Zeitung einen Amortisationsfaktor von 4 für die *Wire*-Fees in ihrer AGB fest. Damit ist der Verkaufspreis für Alice bei 30 cent plus 2.5 cent für die *Wire*-Fees (10 cent geteilt durch den Amortisationsfaktor) plus alle *Deposit*-Fees. Alice zahlt dazu 33 cent mit ihrer 128 cent Münze, und erhält jeweils eine 0.25, 0.5, 2, 4, 8, 16 und 64 cent Münze an Wechselgeld. 0.25 cent an Wechselgebühren bleiben beim Exchange-Betreiber.

Sollte Sie noch einen Artikel kaufen, kann Sie mit den 2 und 2x16 cent Münzen zahlen. Hier ist jetzt die *Deposit*-Fee pro Münze kleiner, aber dafür braucht sie diesmal drei Münzen. Der Preis liegt dann bei 33.25 cent, und sie bekommt 0.5 cent an Wechselgeld (minus die 0.25 cent „refresh“ Gebühr). Hätte Sie mit der 32 cent Münze gezahlt, wäre der Preis zufällig genau gleich geblieben. Sollte der Verleger nur diese zwei Artikel in der (von ihm festgelegten) Abrechnungsperiode verkaufen, erhält er vom Exchange-Betreiber 55 cent: 2x30 cent Verkaufspreis, plus 2x 2.5 cent *Wire*-fees die von den Kunden getragen wurden, minus 10 cent *Wire* fees für den Exchange-Betreiber.

Der Exchange-Betreiber erhält insgesamt 20 cent an *wire*-Fees (jeweils 10 cent von Bäcker und Verleger), 6.25 cent and *Deposit*-Fees und 1.75 cent an *Refresh*-Fees.

Alice hat jetzt noch 0.25, 3x0.5, 4, 8, 32 und 64 cent in Münzen (also 109.75 cent) übrig. Sollte Sie diese nicht ausgeben, wird das Wallet sie ein paar Monate vor dem Ablaufdatum durch neue Münzen ersetzen. Dafür fallen dann grob im Jahresrhythmus *Refresh*-Gebühren an. Bei den 8 Münzen von Alice wären dies 2 cent.

# 6 Rechtliche Rahmenbedingungen und AGB

## 6.1 Fragen rechtlicher Art

Dieses Unterkapitel befasst sich mit rechtlichen Fragen, z.B. der Unterscheidung zwischen Eigentum und Besitz an Coins und den von ihnen repräsentierten Werten, Haftung für diese Werte sowie Verfall und Eigentumsübergang von Coins an Exchange-Betreiber.

### 6.1.1 Treuhandkonto und Insolvenzfall

Exchange-Betreiber sind verpflichtet, das Kapital auf dem Treuhandkonto von der Einzahlung bis zum Ausgabevorgang nur für das Taler-Bezahlsystem zu verwenden. Deshalb weist im Regelfall das Treuhandkonto einen Saldo in Höhe der summierten Coin-Werte auf. Von einem Exchange-Betreiber erwartet zudem das Zahlungsdiensteaufsichtsgesetz, Sicherungsmaßnahmen und Frühwarnmechanismen gegen Insolvenz einzurichten und Anfangskapital in bestimmter Höhe vorzuhalten<sup>1</sup>.

Solange kein Grund für eine Mitteilung drohender Insolvenz an das zuständige Amtsgericht vorliegt, ist ein Exchange zur Rücküberweisung des Treuhandkonto-Habensaldos an die ursprünglichen IBAN-Konten jederzeit berechtigt. Das Recoup-Protokoll kann er also zu seinem geordneten Marktaustritt nutzen. Im Insolvenzfall würden jedoch alle Coin-Werte in die Konkursmasse fallen und ihre Eigentümer zu Gläubigern werden. Der Exchange dürfte dann keinen Recoup ohne Beschluss eines Insolvenzgerichts durchführen.

Exchange-Betreiber sollten mit geeigneten Vorkehrungen sicherstellen, dass das Vermögen des Treuhandkontos nicht unter das Insolvenzrecht fällt, um zu vermeiden, dass im Konkursfall das dort verwahrte Guthaben dem Massevermögen zugeschlagen wird. Dieses Guthaben umfasst zum einen den Wert der Coins, die von diesem Exchange signiert wurden und sich rechtlich im Eigentum der Wallet-Besitzer befinden, zum anderen den Wert der *deponierten* Coins dieses Exchange, für die Verkäufer bislang noch keine Sammelbuchung zugunsten ihrer Girokonten ausgelöst bekamen. Die Vorkehrungen gegen Insolvenz schützen damit einerseits die Verbindlichkeiten von Exchange-Betreibern gegenüber den Coin-Eigentümern, andererseits die Forderungen der Verkäufer gegen Exchange-Betreiber auf Überweisung ihrer Umsatzeinkünfte.

---

1 Ein Exchange-Betreiber muss die Auflagen der BaFin erfüllen, in ihrem Register eingetragen sein und Anfangskapital vorhalten („hartes Kernkapital“, mindestens 20.000 Euro Anfangskapital für Finanztransfersgeschäfte, als Zahlungsauslösedienst 50.000 Euro, als E-Geld-Emittent 350.000 Euro, siehe §12 Zahlungsdiensteaufsichtsgesetz).

### 6.1.2 Verjährung von Coin-Werten

Die Verjährung erlaubt nur bei einer hohen Nutzerzahl des Bezahlsystems eine nennenswerte Einkommenserzielung. Wenn dieses Einkommen aus dem Verfall von Coin-Guthaben alle Kosten des Betriebs eines Exchange deckt, könnte man dessen Gebührenordnung wesentlich vereinfachen. Dieses Einkommen ist jedoch unstetig und unvorhersehbar, eignet sich von daher nicht für eine nachhaltige Finanzierung. Außerdem würden Exchange-Betreiber darauf verzichten, ihren Nutzern Anreize zu ökonomischem Buchungsverhalten zu geben<sup>2</sup>.

## 6.2 AGB-Formulierung

Die Formulierung der Allgemeinen Geschäftsbedingungen, die ein Exchange seinen Nutzern anzeigt und beim Abheben bzw. bei neuen Nutzungsbedingungen von diesen bestätigen lässt, ist noch in Entwicklung. Als Arbeitsvorlage zur Orientierung dienen die *Terms of Service* in englischer Sprache, die nur exemplarisch zu verstehen sind (siehe Kapitel 13 AGB/Nutzungsbedingungen oder Terms of Service in Git). Die später gebräuchlichen deutschen AGB für Taler-Nutzer sollten möglichst einfach, deutlich und freundlich formuliert sein und unmissverständlich auf die Pflichten der Nutzung und mögliche Risiken eines Wertverlusts hinweisen.

## 6.3 Datenschutzerklärung

Die englischsprachige *Privay Policy* dient ebenfalls als Arbeitsvorlage für die deutschsprachige DSGVO-konforme Datenschutzerklärung (siehe Kapitel 14 Datenschutzerklärung).

---

<sup>2</sup> Anbieter von Gutscheinkarten nutzen bereits als Geschäftsmodell die Einkommenserzielung aus der Verjährung von Gutscheinen. Zu beachten sind dabei §§ 195 und 199 BGB. Es gilt in der BRD eine gesetzliche Verjährungsfrist von 3 Jahren ab dem Ende des Jahres, in dem ein Gutschein erstellt wurde. Bei Taler-Coins handelt es sich jedoch nicht um Gutscheine, sondern um Eigentum, dessen Eigentümer allerdings dem Exchange-Betreiber namentlich nicht bekannt sind, da die Coins blind signiert werden.

## 7 Datensicherung für Wallets

Das Taler-Wallet verfügt über eine integrierte Backup-Lösung. Mit dieser können Nutzer ihre Coins und andere Wallet-Daten verschlüsseln und bei einem vom Nutzer bestimmten Backup-Betreiber hinterlegen. Taler Systems SA wird sicherstellen, dass mindestens ein Backup-Betreiber existiert. Die Software für den serverseitigen Betrieb der Backup-Lösung wird quelloffen der Allgemeinheit zur Verfügung gestellt, somit können qualifizierte Kunden ihre eigene Backup-Lösung betreiben bzw. andere Unternehmen eigene Speicherorte anbieten. Für die Nutzung des Backup-Angebots können die Backup-Betreiber Gebühren verlangen, welche auch über das Taler-Wallet direkt bezahlt werden. Die Sicherung der Backup-Daten kann je nach Betreiber über geheime Schlüssel oder auch über Multi-Faktor-Authentifizierung erfolgen.

## **8 Organisatorische Sicherheit**

Organisatorische Details zur sicheren Datenverarbeitung beim Exchange (Datenzentrum, Redundanz, Zugangskontrolle) wurden noch nicht bestimmt, da die geschäftliche Aufgabenteilung zwischen GLS Bank und Taler Systems SA in diesem Punkt noch nicht abschließend geklärt ist. In jedem Fall wird jedoch ein sicherer und bankenüblich zertifizierter Rechenzentrumsbetrieb bereitgestellt.

## 9 Regulatorische Compliance

1. Das Abhebevolumen pro Tag und pro Kunde soll begrenzt werden. Dies dient sowohl zum Selbstschutz der Kunden, zum Schutz vor einem „Bank Run“ und leistet ggf. einen Beitrag zur Durchsetzung von AML-Richtlinien. Wir gehen im Moment von einer Obergrenze von 1000 Euro pro Tag und Kunde aus, da diese Grenze z.B. auch für Bargeld üblich ist.
2. Händler können eine Obergrenze des Transaktionsbetrags pro Vorgang festlegen. Bestehende Obergrenzen z.B. für Kreditkarten ohne TAN-Autorisierung am Point of Sale gemäß PSD2 sind 50 Euro pro Buchung maximal fünfmal in Folge. Darüber hinaus gilt aktuell gemäß PSD2-Richtlinie die Kann-Option für Zahlungsdienstleister, welche Kundenbuchungen in der Summe von maximal 150 Euro ohne starke Authentifizierung erlaubt. Die genaue Anwendbarkeit dieser Richtlinien ist unklar, wobei wir bislang von Obergrenzen zwischen 50 und 1000 Euro pro Geschäftsvorgang ausgehen, ggf. auch in Abhängigkeit vom Geschäftsbereich des Händlers.
3. Die Identitätsfeststellung (KYC) erfolgt sowohl für Kunden als auch für Verkäufer stets bei den Geschäftsbanken. Für die Teilnahme am Bezahlsystem benötigen beide Seiten ein SEPA-Konto, das sie nur nach Klärung ihrer Identität bzw. der wirtschaftlich Berechtigten eröffnen können. Eine theoretische Ausnahme bei der Identitätsfeststellung wären Empfänger von Sozialleistungen, die z.B. von staatlichen Behörden ihre Sozialleistungen mithilfe des durch GNU Taler ermöglichten Tipping-Verfahrens auch ohne eigenes Girokonto empfangen könnten. In diesem Fall würde die Behörde die Identitätsfeststellung der Leistungsempfänger übernehmen müssen.
4. Die Verantwortung für AML bleibt bei den Geschäftsbanken der Verkäufer. Die Banken werden dazu von einer API des Exchange unterstützt, welche es erlaubt, die eingehenden SEPA-Buchungen mit den Vertragstexten jedes abgeschlossenen Geschäftsvorgangs zu verknüpfen. Diese API kann z.B. auch von Steuerbehörden genutzt werden, um die Geschäftsvorgänge der Verkäufer im Rahmen einer Steuerprüfung zu analysieren. Transaktionen an sanktionierte Empfänger werden - falls notwendig - von deren Geschäftsbank storniert bzw. eingefroren. Internationale Überweisungen auf Konten außerhalb des Euro-Währungsbereichs sind nicht erlaubt und werden nicht ausgeführt.
5. Die unabhängigen Auditoren (Code Blau GmbH) sind für unabhängige Prüfungen in folgenden Bereichen zuständig: Technisch (Quellcode), Exchange-Datenbank (Prüfung der gesammelten kryptografische Beweise), organisatorische Sicherheit, SEPA-Buchungen des Exchange (Credit und Debit) sowie die Bilanzprüfung. Die Code Blau GmbH würde ihre Berichte der Taler Systems SA, der GLS Bank und der BaFin regelmäßig zur Verfügung stellen bzw. bei Unregelmäßigkeiten auch sofort Meldung erstatten.

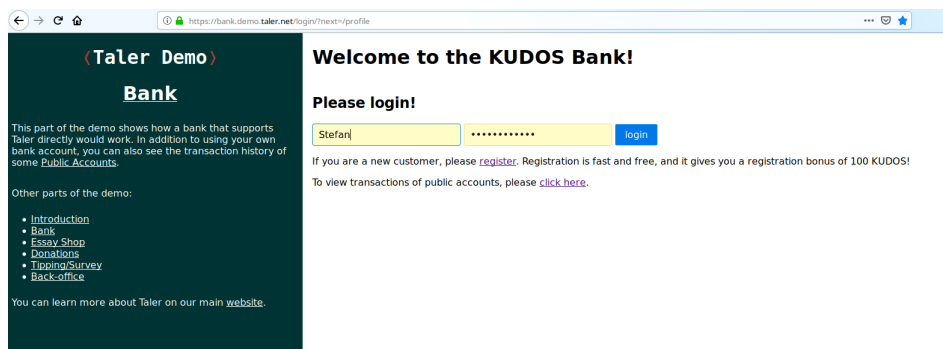
# 10 Screenshots der Geschäftsvorgänge

Die Screenshots zeigen die einzelnen Handlungsschritte aus Sicht der Nutzer des Taler-Bezahlsystems. Die Abschnitte 10.1 und 10.2 zeigen die Abhebe- und Ausgabevorgänge mit dem Wallet eines Smartphones mit Android-Betriebssystem (für weitere Smartphone-OS in Entwicklung), Abschnitt 10.3 veranschaulicht den Abhebevorgang auf das Smartphone-basierte Wallet mit der ATM-Anwendung „Taler-Cashier“. In Abschnitt 10.4 folgen Screenshots des Bezahlvorgangs mit der Point of Sale-Anwendung „Merchant“.

KUDOS stellen dabei eine Phantasiewährung des experimentellen Taler-Exchange dar, die KUDOS-Bank ist eine exemplarische Bank. Wenn ein Exchange Euro anbietet, stünde EURO als Währung anstelle der KUDOS.

## 10.1 Abhebevorgang vom Girokonto in das Wallet eines Android-Smartphones

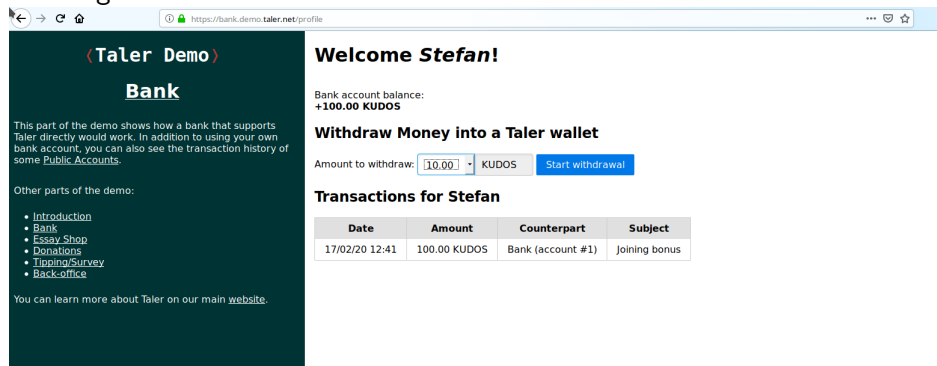
1. Der Kunde meldet sich an bei seiner Geschäftsbank an, die einen Taler-Exchange und damit Taler als Verfahren zum Abheben in Wallets anbietet:





## 10 Screenshots der Geschäftsvorgänge

2. Der Kunde wählt das Taler-Verfahren und gibt die Geldmenge ein, die auf das persönliche Wallet gebucht werden soll:



The screenshot shows a web browser window with the URL `https://bank.demo.taler.net/profile`. The page is titled "(Taler Demo) Bank". On the left, there is a navigation menu with links for Introduction, Bank, Essay Shop, Donations, Tipping/Survey, and Back-office. The main content area displays "Welcome Stefan!" and "Bank account balance: +100.00 KUDOS". Below this, there is a section titled "Withdraw Money into a Taler wallet" with a form to enter the withdrawal amount (currently 10.00 KUDOS) and a "Start withdrawal" button. A table titled "Transactions for Stefan" shows a single transaction on 17/02/20 at 12:41 for 100.00 KUDOS from Bank (account #1) with the subject "Joining bonus".

Date	Amount	Counterpart	Subject
17/02/20 12:41	100.00 KUDOS	Bank (account #1)	Joining bonus

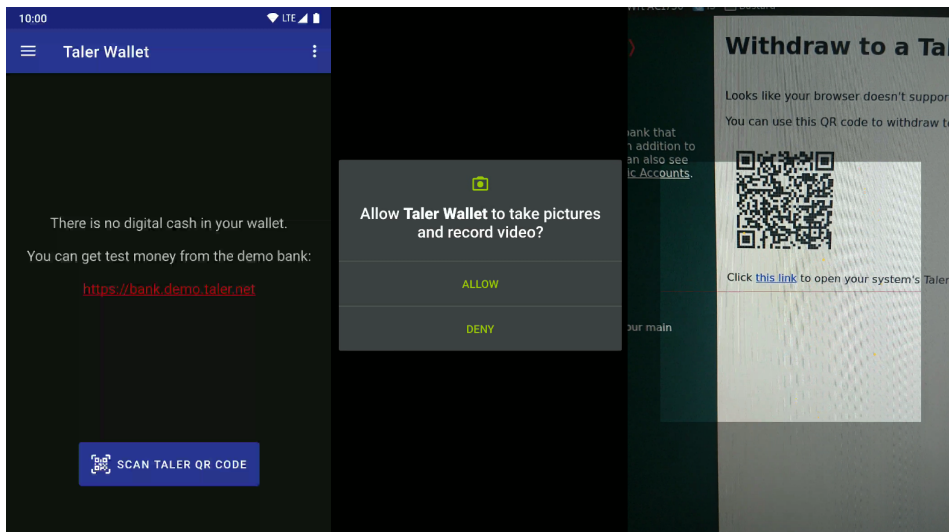
3. Die Bank-Webseite zeigt den QR-Code an, den die Bank-API erzeugt hat:



The screenshot shows a web browser window with the URL `https://bank.demo.taler.net/showwithdrawal/912f77b0-f804-4793-a34b-1c0bad481e88`. The page is titled "(Taler Demo) Bank". The main content area displays "Withdraw to a Taler Wallet" and a message: "Looks like your browser doesn't support GNU Taler payments. You can try installing a [wallet browser extension](#). You can use this QR code to withdraw to your mobile wallet:". A QR code is shown in the center. Below the QR code, there is a link: "Click [this link](#) to open your system's Taler wallet if it exists."

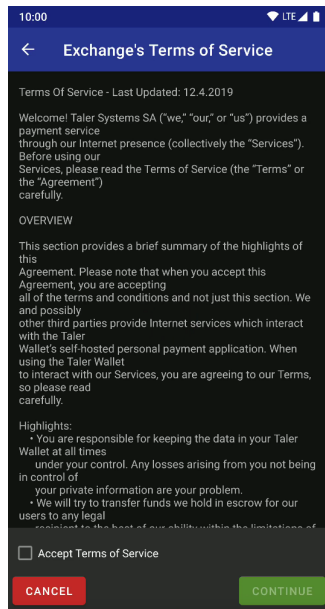
## 10 Screenshots der Geschäftsvorgänge

- Der Kunde öffnet die App des Taler-Wallet, sieht den aktuellen Coin-Bestand (Bild links), muss ggf. seinem Smartphone die Aufnahme von Fotos erlauben (Bild Mitte) und scannt mit dem Smartphone den QR-Code auf der Bank-Webseite (Bild rechts):

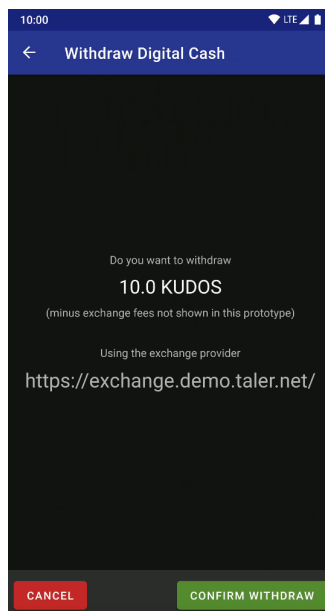


## 10 Screenshots der Geschäftsvorgänge

5. Der Kunde wählt den Exchange [hier noch nicht bildlich dargestellt], liest die allgemeine Gebührenstruktur und die Gebühren für den aktuellen Abhebevorgang [hier noch nicht bildlich dargestellt] sowie die Allgemeinen Geschäftsbedingungen des Taler-Bezahlsystems, welche er bestätigen muss:

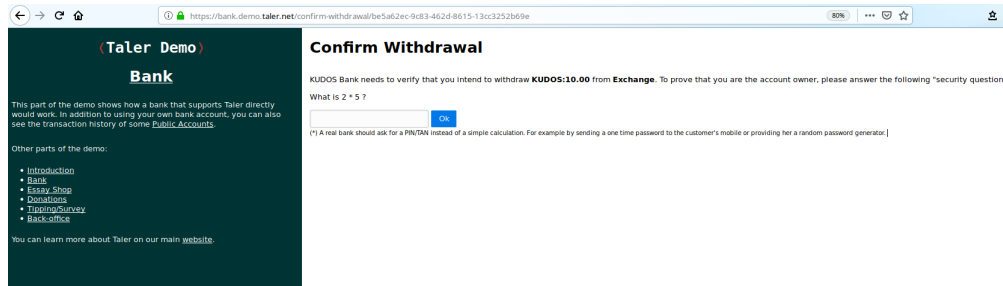


6. Der Kunde bestätigt den Abhebevorgang in der App:

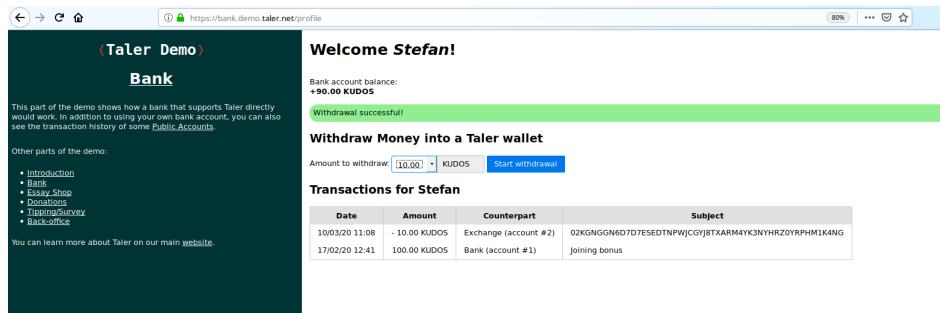


## 10 Screenshots der Geschäftsvorgänge

7. Der Kunde wird auf die Benutzerführung der Bank-Webseite bzw. des ATM-Terminals zurückverwiesen. Es werden ihm nochmals der abzuhebende Betrag und der gewählte Exchange angezeigt. Er muss gegenüber der Bank endgültig bestätigen, dass der Abhebevorgang nun ausgelöst werden soll. Bei einer Zwei-Faktor-Autorisierung verlangt die Bank vom Kunden eine TAN-Eingabe. Die TAN-Abfrage der Demo-Version wird hier in Form eines Captchas versinnbildlicht:

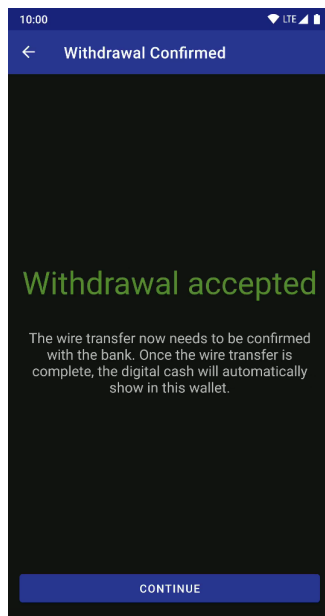


Die Bank führt die Buchung des Betrags an den gewählten Exchange damit aus:

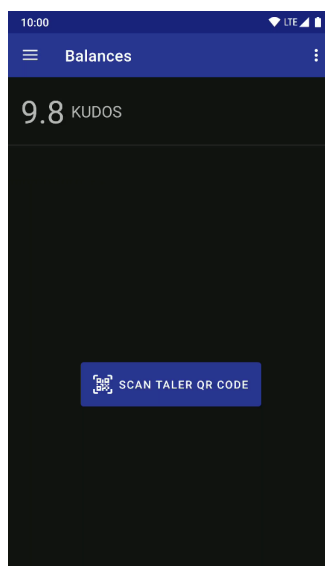


## 10 Screenshots der Geschäftsvorgänge

- Der gewählte Exchange bildet eine Reserve über den Betrag der Girokontoüberweisung, aus welcher das empfangende Wallet Coins abheben kann, die in der Summe dem angeforderten Betrag entsprechen:



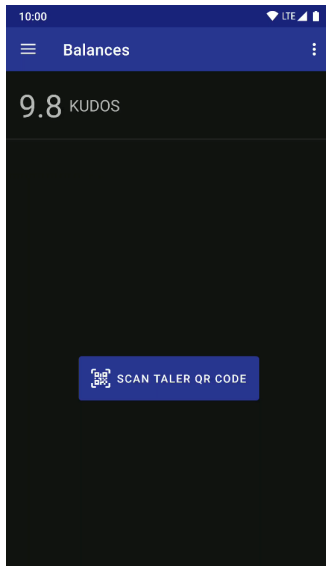
- Das Wallet des Kunden hat die Coins abzüglich der Überweisungsgebühr und der Transaktionsgebühr (für die Buchung vom Girokonto zum Exchange und die Transaktionen ins Wallet) empfangen:



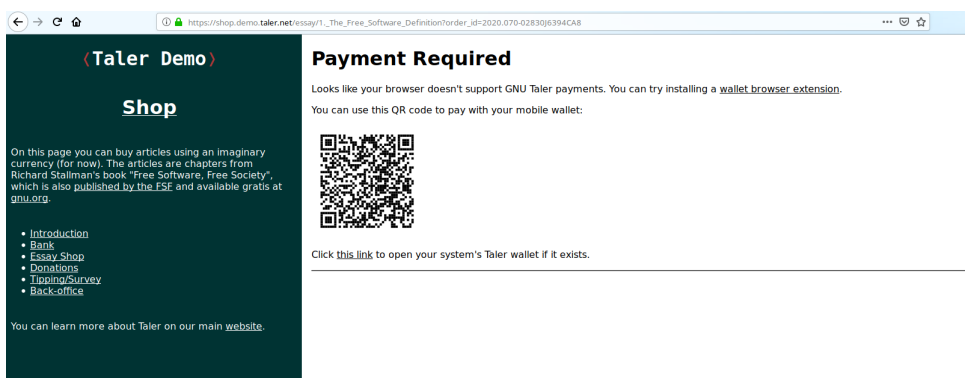
## 10.2 Ausgabevorgang mit dem Wallet eines Smartphones (Android-Betriebssystem)

Dieser Abschnitt veranschaulicht einen regulären Ausgabevorgang z.B. bei Vertragsschluss zum Erwerb von Gütern im Internet (den Bezahlvorgang am Point of Sale beschreibt Abschnitt 10.4).

1. Jeder Wallet-Besitzer wird vor einem Kauf den Bestand der verfügbaren Coins prüfen wollen und bekommt deren Summe in der Taler-App angezeigt:

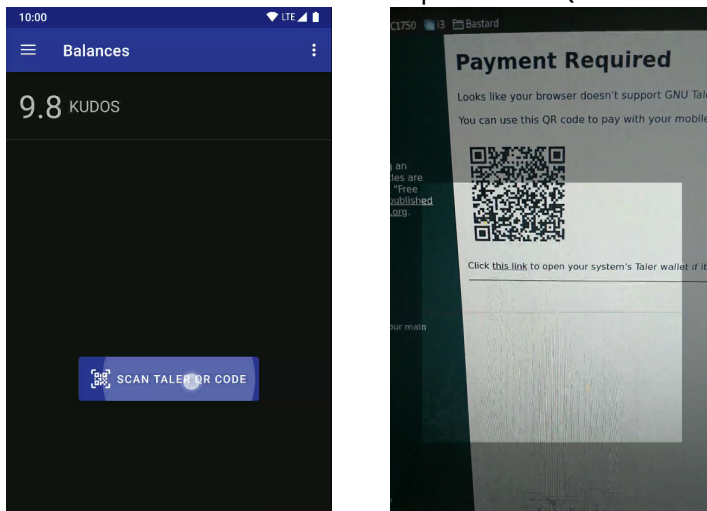


2. Der Verkäufer eines Guts, das der Kunde zu erwerben wünscht, betreibt die von Taler Systems SA zur Integration in Shops bereitgestellte Verkäufer-Software „Merchant“, welcher einen QR-Code über den Kauf erzeugt und dem Kunden auf der Webseite anzeigt:

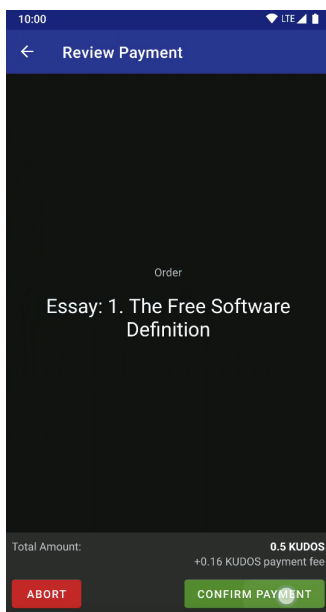


## 10 Screenshots der Geschäftsvorgänge

3. Der Kunde scannt mit dem Smartphone den QR-Code auf der Verkäufer-Webseite:

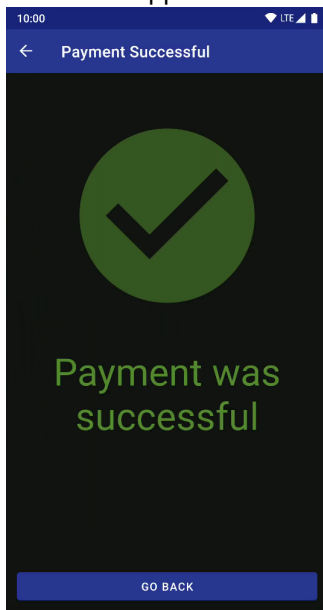


4. Der Kunde erhält Artikelbezeichnungen sowie den Gesamtbetrag über den Kaufpreis in der Taler-App angezeigt und wird um Bestätigung gebeten, um die Zahlung auszulösen:

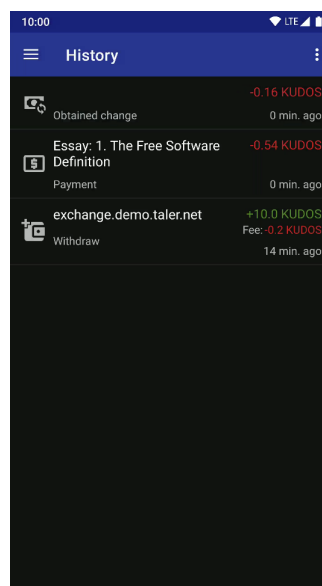
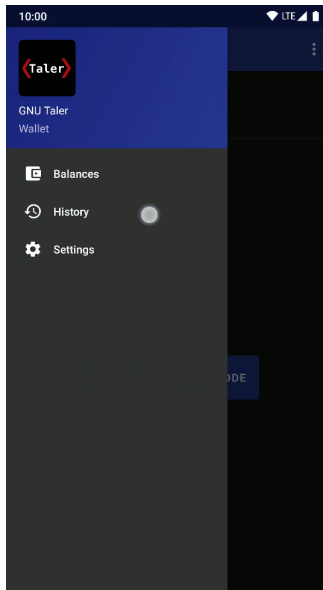


## 10 Screenshots der Geschäftsvorgänge

5. Die Taler-App meldet dem Kunden die erfolgte Bezahlung:



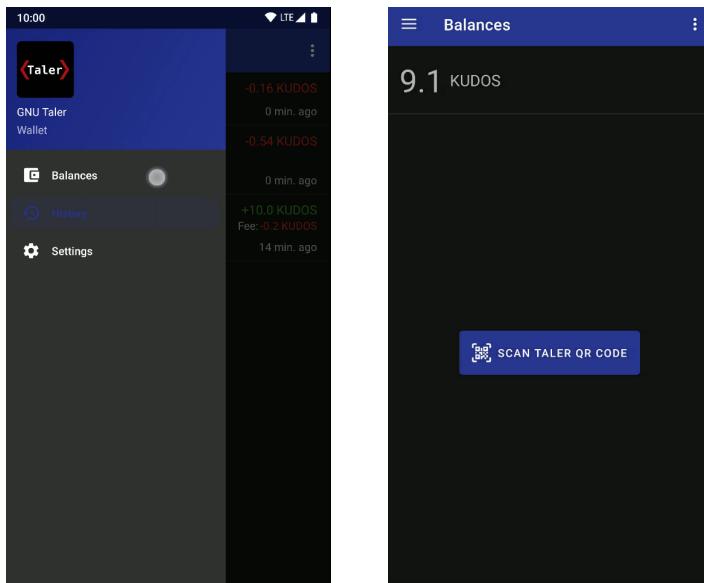
6. Der Kunde kann sich stets die Historie der Käufe anzeigen lassen:





## 10 Screenshots der Geschäftsvorgänge

7. Der Kunde kann sich stets den Bestand an Coins im Wallet anzeigen lassen:



### **10.3 Abhebevorgang auf ein Smartphone-basiertes Wallet mit „Taler-Cashier“ als Automated Teller Machine-Anwendung**

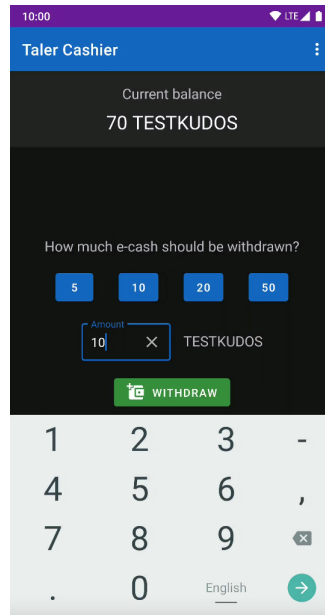
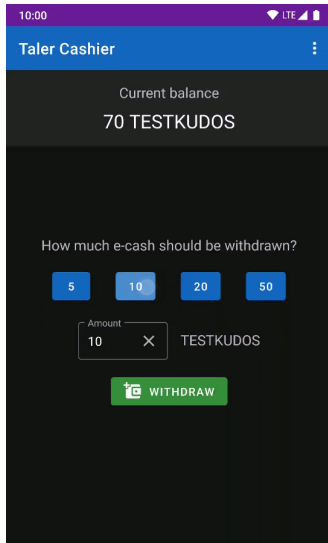
Ein Kassierer oder Kassenwart, der Taler-Cashier verwendet, hat die Möglichkeit, seinen Kunden das von ihnen erhaltene Geld in Form von Coins zu senden. Die Funktion entspricht einem ATM-Bankautomaten, der Bargeld annimmt und den Geldwert auf ein Wallet aufbucht. Als Kassenwart auftreten können Privatpersonen, meist wird es sich jedoch um Betreiber von Geschäften oder Kiosken handeln. Sowohl Kassenwart als auch Kunde müssen jeweils ein Smartphone besitzen. Der Kassenwart muss den Taler-Cashier, der Kunde das Taler-Wallet installiert haben. Die Anwendung wird zum heutigen Entwicklungsstand nur zu Demonstrationszwecken eingesetzt. Ihr großflächiger Einsatz im realen Geschäftsbereich ist noch nicht beabsichtigt. Sie lässt sich jedoch zukünftig implementieren als Möglichkeit der Bareinzahlung von Kunden, die noch nicht oder nicht mehr über ein Bankkonto verfügen.

Kassierer müssen das Geldwäschegesetz (GwG) und die Vorschriften gegen Geldwäsche (Know Your Customer, Anti Money Laundering) befolgen und daher bei der Annahme von Bargeldmengen ab der gesetzlich festgelegten Grenze von zurzeit 10.000 Euro die Identifizierung des Einzahlenden bzw. des wirtschaftlich Berechtigten verlangen.

Taler-Cashier verfügt über ein internes Limit an Coin-Beträgen. Dieses Limit hat die gleiche Wirkung wie ein begrenzter Bestand an Bargeld in einer Registrierkasse. Damit ist das Risiko eines Diebstahl von Werten aus der Cashier-App beschränkt, wenn beispielsweise der Kassenwart mit Gewalt zu einer Versendung von Coins gezwungen werden sollte.

1. Der Kassenwart öffnet die App Taler-Cashier und gibt dort den Betrag ein, den der Kunde ihm angegeben hat - entweder durch Tippen auf die voreingestellten Felder (Bild links) oder durch manuelle Eingabe (Bild rechts):

## 10 Screenshots der Geschäftsvorgänge

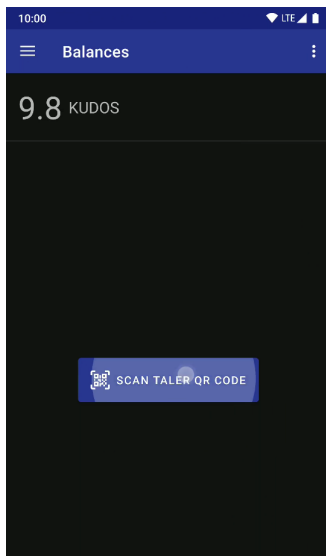


## 10 Screenshots der Geschäftsvorgänge

- Die Cashier-App erzeugt einen QR-Code auf dem Gerät des Kassenswarts:

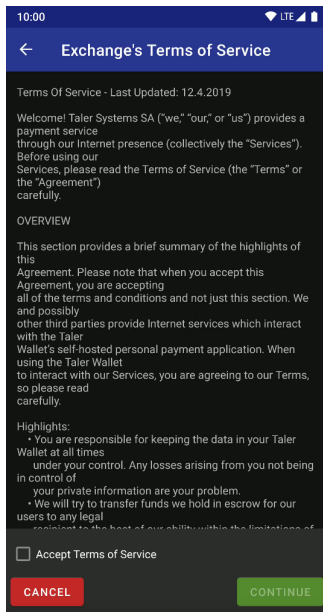


- Der Kunde scannt mit seinem Smartphone den QR-Code auf der Anzeige des Kassenswarts:

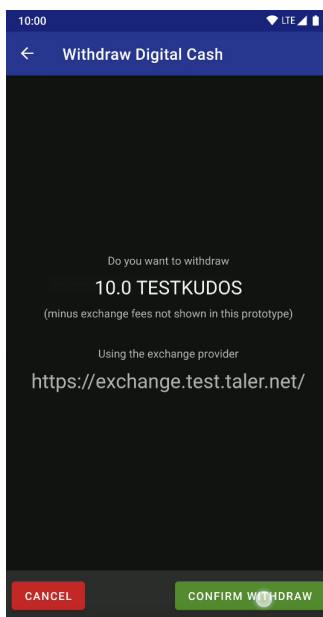


## 10 Screenshots der Geschäftsvorgänge

4. Der Kunde liest in seinem Gerät die Allgemeinen Geschäftsbedingungen des Taler-Bezahlsystems, welche er bestätigen muss:

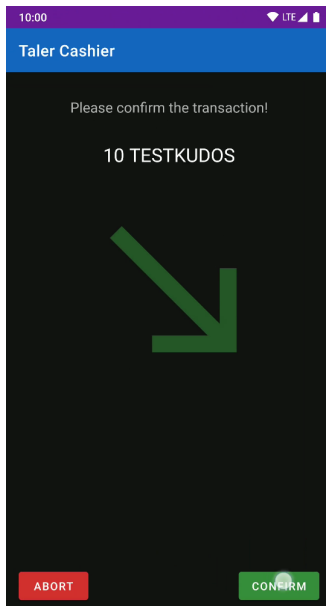


5. Der Kunde muss den Betrag bestätigen:

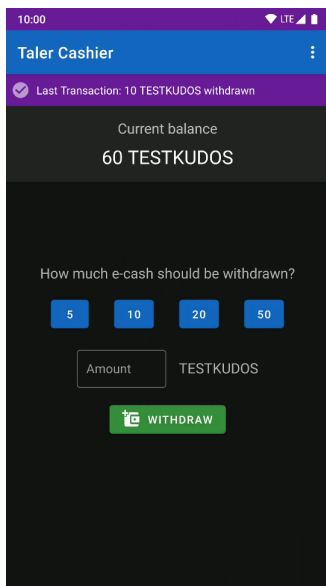


## 10 Screenshots der Geschäftsvorgänge

6. Die Cashier-App verlangt vom Kassenswart die Bestätigung, dass sein Wallet mithilfe der Cashier-Anwendung Coins an den Kunden senden darf:



7. Die Cashier-App meldet die erfolgte Abbuchung und zeigt den aktuellen Bestand an verbleibenden Coins an:



8. Das Wallet des Kunden erhält die Coins.

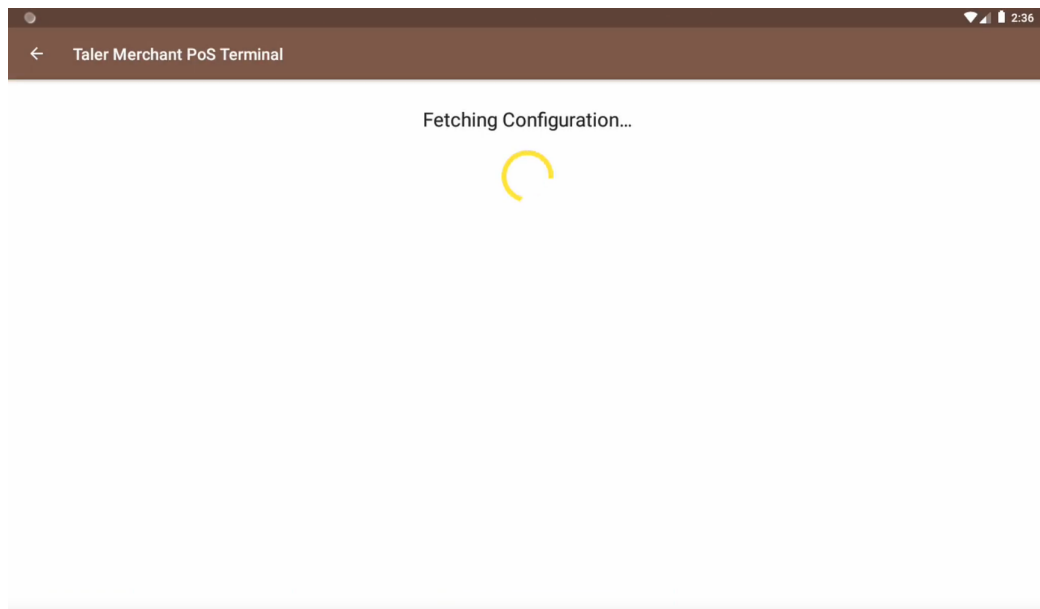
## 10.4 Bezahlvorgang mit der Point of Sale-Anwendung „Merchant“

„Merchant“ ist eine Beispielanwendung für das Bestellen und Bezahlen an Verkaufsstellen. Programmierer können den Code dieser Anwendung in bestehende Kassen- und Warenwirtschaftssysteme oder Webshops einbauen. Die einfache Integration des Codes trägt dazu bei, dass sich das Taler-Bezahlsystem in der Handelswelt schnell verbreiten wird.

Nachfolgend verdeutlichen die Screenshots die Benutzerführung auf Käuferseite und Verkäuferseite (Bestellung, Summierung, Bezahlung mit Coins aus dem persönlichen Wallet der Kunden, Verkaufshistorie).

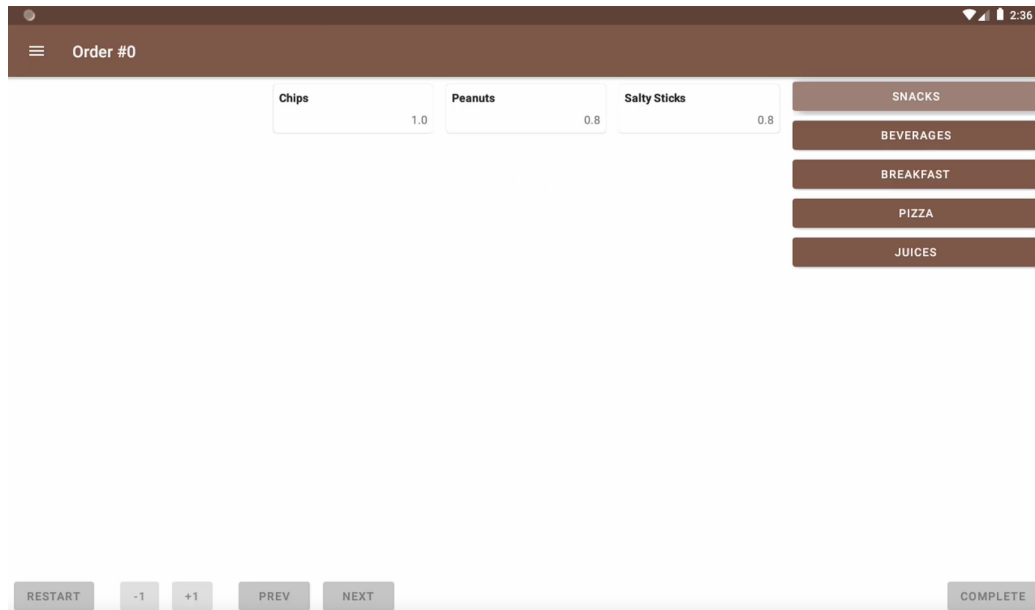
Der dargestellte Vorgang - hier am Beispiel einer Cafeteria - bezieht sich wie in den vorhergehenden Geschäftsvorgängen auch auf Wallets in Android-Smartphones. KUDOS sind wie gehabt der Platzhalter für EURO.

1. Das POS-Terminal wird gestartet:

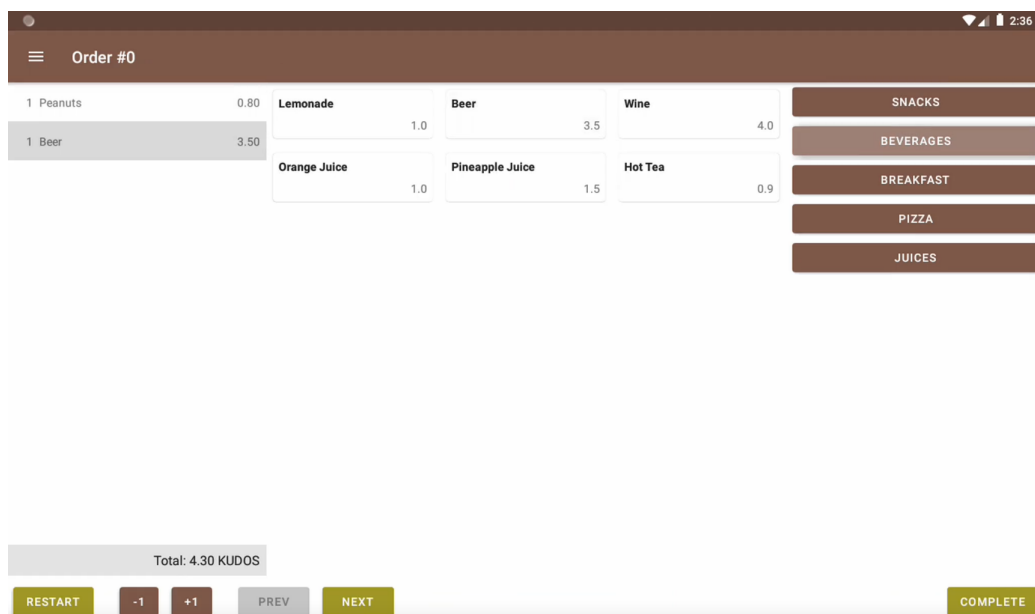


## 10 Screenshots der Geschäftsvorgänge

2. Im Auswahl-Menü werden die gewünschten Artikel gesammelt und ihre Beträge summiert:



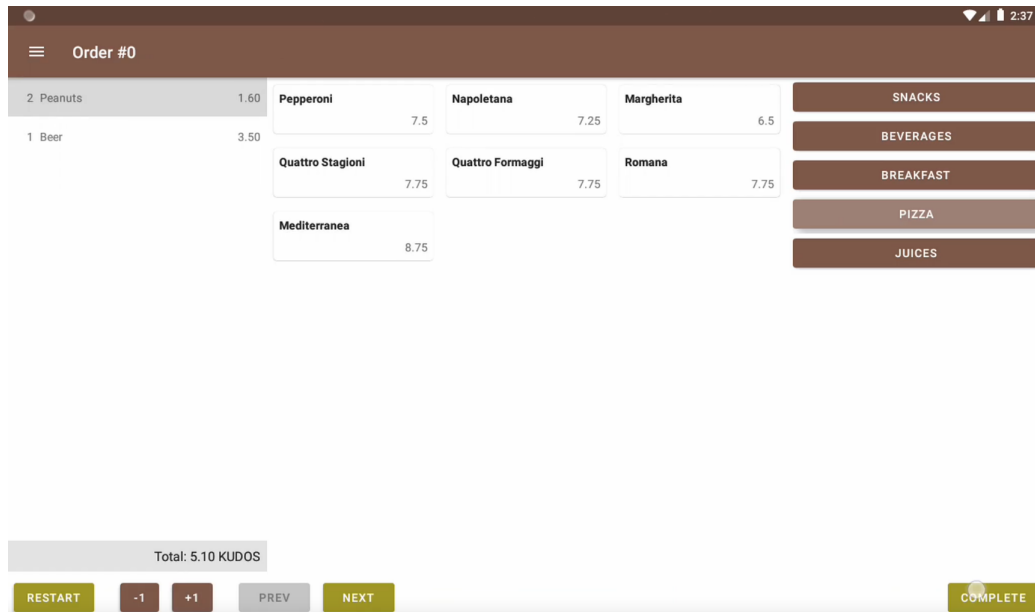
3. Dito. Der Kunde kann summieren lassen, soviel der Coin-Bestand auf dem Wallet erlaubt:



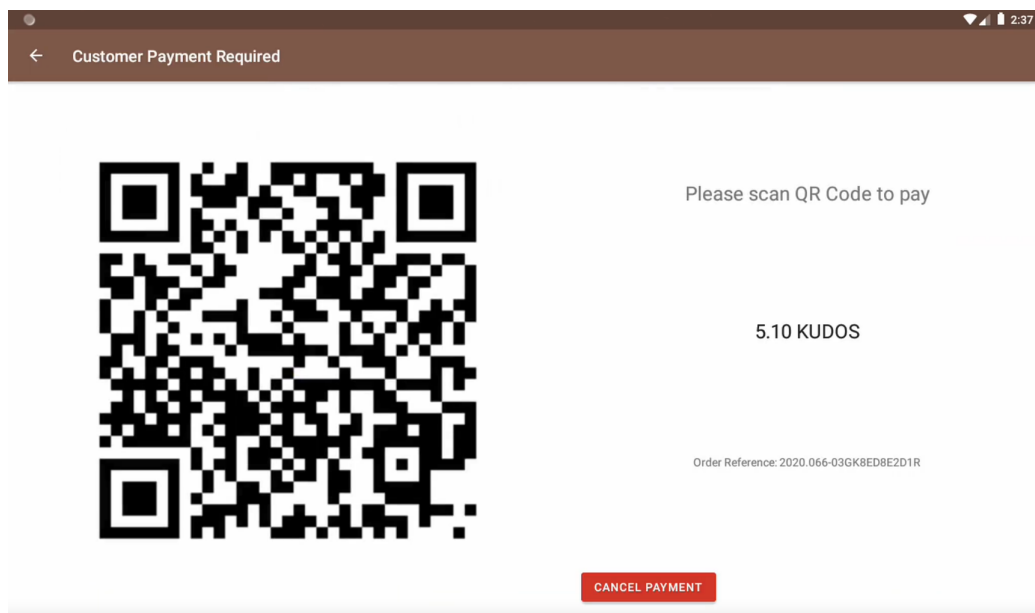


## 10 Screenshots der Geschäftsvorgänge

4. Ist die Bestellung vollendet, tippt der Terminal-Nutzer die Taste „Complete“, die Anwendung erzeugt dann einen QR-Code:

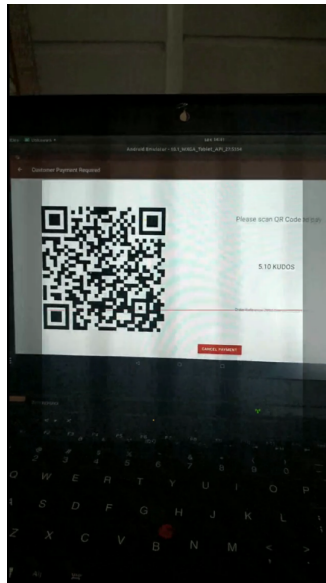
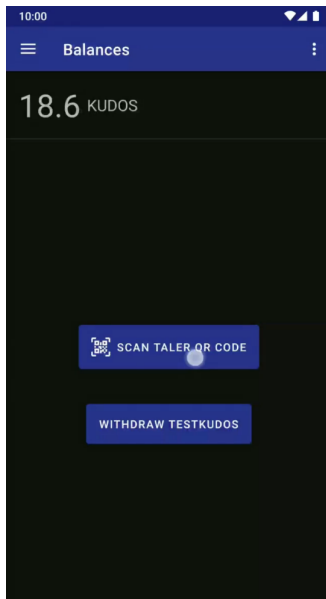


5. Dieser QR-Code wird dem Kunden zum Scannen angezeigt:

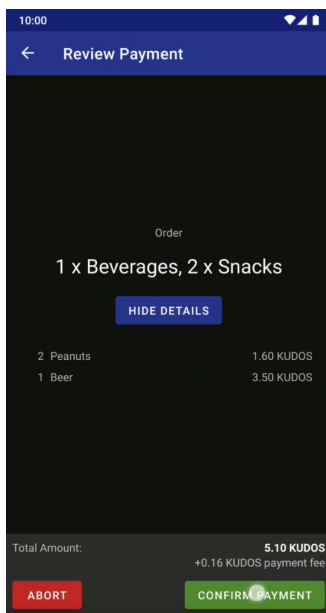
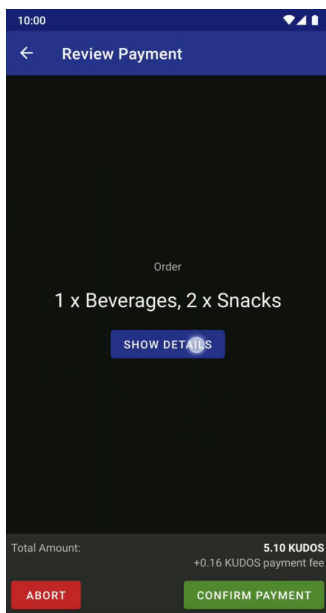


## 10 Screenshots der Geschäftsvorgänge

6. Der Kunde scannt den QR-Code mit seinem Smartphone:

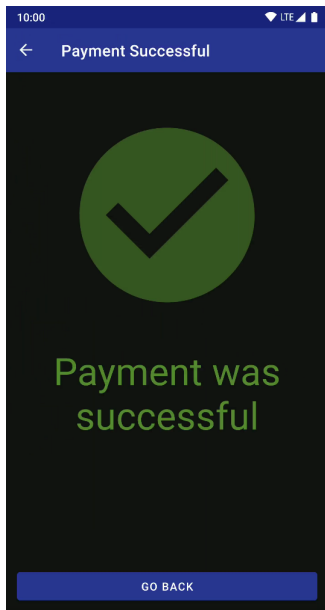


7. Der Kunde kann sich die Details des Kaufs anzeigen lassen und die Details auch wieder einklappen. Zum Kauf der Artikel muss er bestätigen:

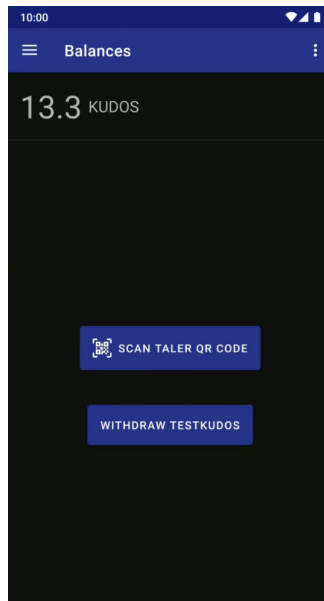
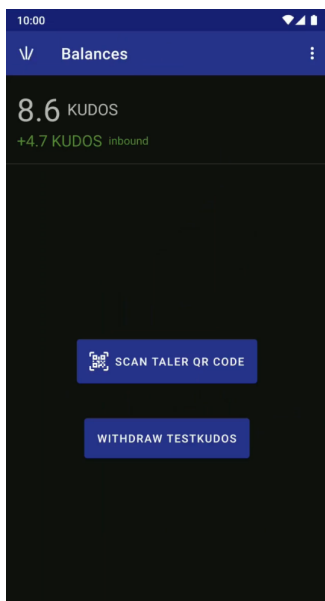


## 10 Screenshots der Geschäftsvorgänge

8. Es erscheint eine Bestätigung des erfolgten Kaufs:

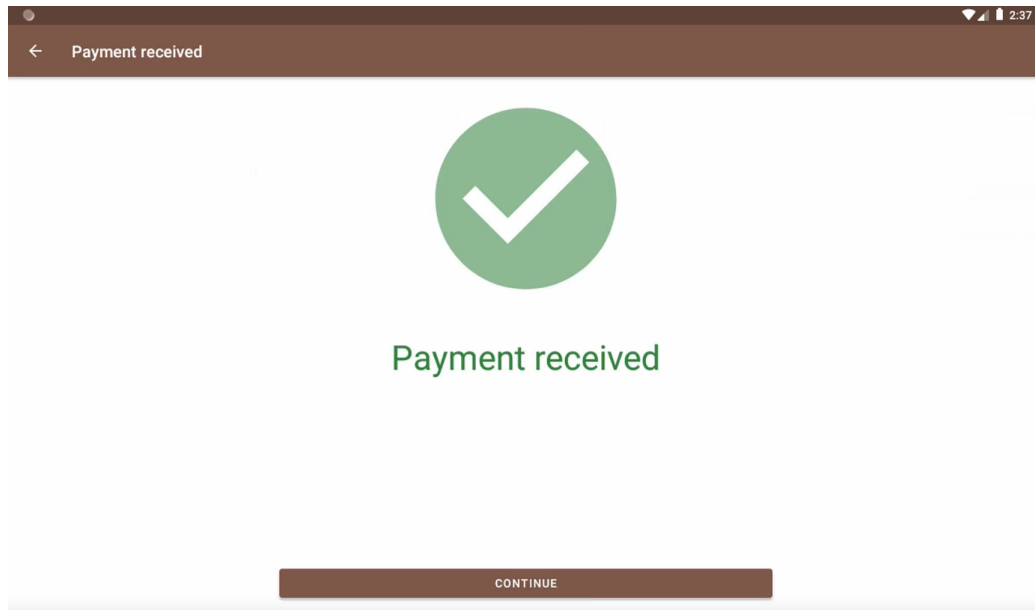


9. Hier wurde ein Coin über 10 KUDOS verbraucht, davon gehen 5,1 KUDOS zugunsten des Verkäufers, 0,2 KUDOS an den Exchange (als Einbehalt für Gebühren) und 4,7 KUDOS Wechselgeld an das Wallet zurück:

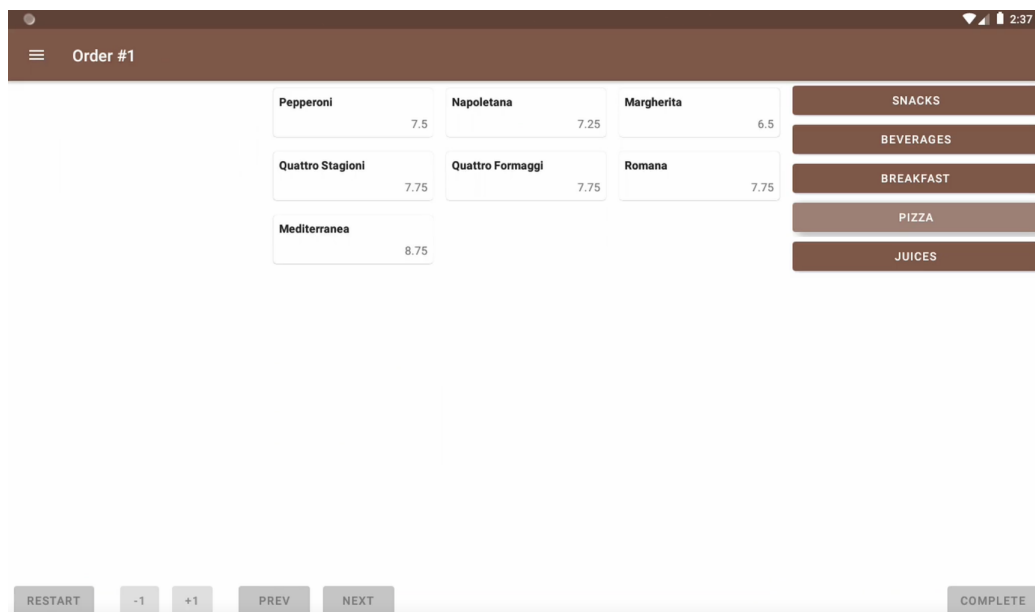


## 10 Screenshots der Geschäftsvorgänge

10. Das POS-Terminal zeigt nach Eingang der Coins die Bestätigung der erfolgten Zahlung:

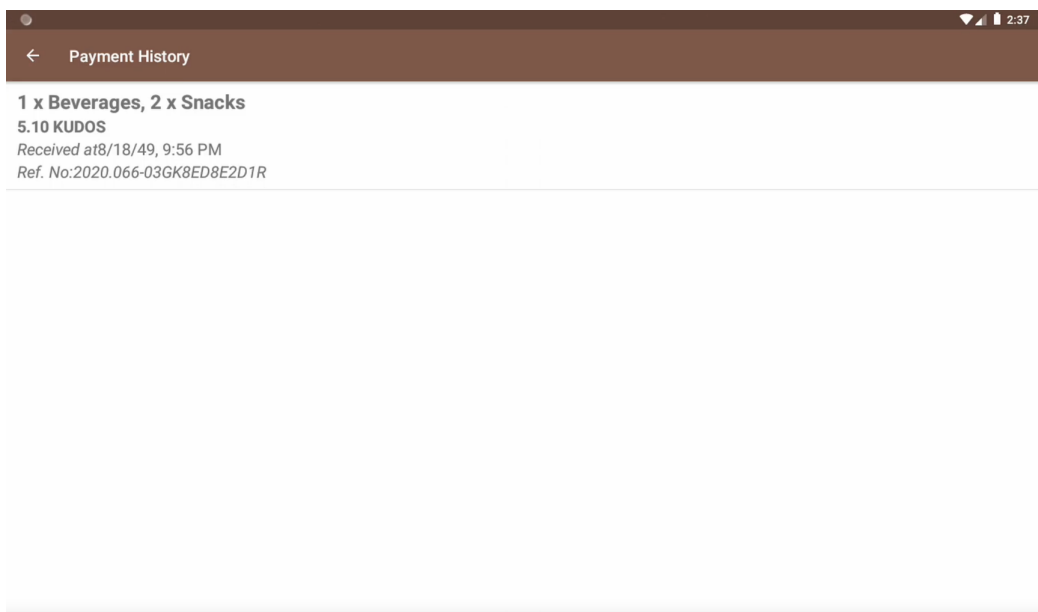
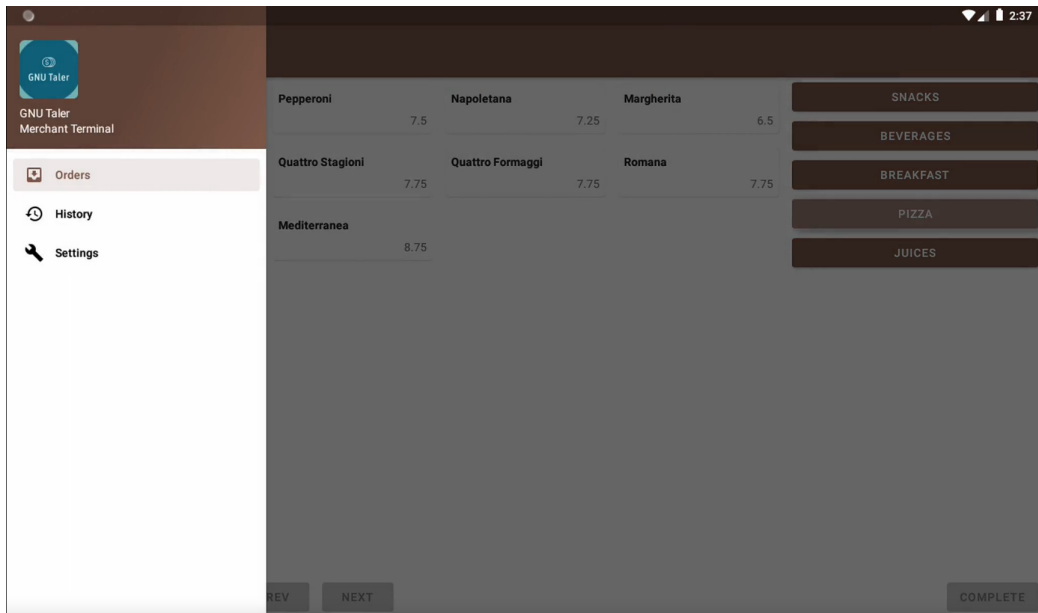


11. Das Terminal geht zum Auswahl-Menü zurück, die Bestellnummer hat sich erhöht:



## 10 Screenshots der Geschäftsvorgänge

12. Die POS-Anwendung kann jederzeit die Historie der Verkäufe anzeigen:



# 11 Taler Systems SA: Geschäftsmodell und Tragfähigkeit

## 11.1 Alleinstellungsmerkmale

Für ein langzeitiges Bestehen des Bezahlsystems und eine stetige Supportleistung ist es vorteilhaft, wenn Alleinstellungsmerkmale bestehen, die Taler vor allen anderen Systemen auszeichnen. Neben der schon angesprochenen unterschiedlichen Behandlung von Geldströmen auf Käufer- und Verkäuferseite sind dies der minimale Verbrauch von Energie für alle Buchungsvorgänge, ein niedriges Kostenniveau für Transaktionen, Internet-weite Verfügbarkeit und hohe Transaktionsgeschwindigkeit. Weiterhin sind auch die Integrationskosten und Betriebskosten bei den Händlern gering. Das Bezahlsystem weist dabei Alleinstellungsmerkmale auf, die durchaus disruptive Effekte entfalten können und Zahlungsgewohnheiten sowie die steuerliche Ehrlichkeit positiv beeinflussen.

## 11.2 Einnahmen

Auf der Einnahmenseite von Taler Systems SA stehen Einkünfte aus dem Support, den die Unternehmung gegenüber Exchange-Betreibern und Verkäufern leistet, insbesondere für das delegierte Aufsetzen und Inbetriebnehmen von Exchanges sowie für das Customizing von Point of Sale-Schnittstellen bei speziellen Wünschen oder Erfordernissen von Verkäufern.

Taler Systems SA erwartet neben den genannten Support-Einnahmen weiterhin auch Einkünfte aus Gebühren von Exchanges die, ggf. mit Kooperationspartnern, betrieben werden.

## 11.3 Ausgaben

Auf der Ausgabenseite trägt Taler Systems SA Personalkosten, Infrastrukturkosten (z.B. für Server und Arbeitsplatzrechner) und Kosten für den laufenden Betrieb der Unternehmung (Büromieten, Energie, Fahrtkosten, Marketing u.ä.). Hostet die Firma einen eigenen Exchange, würde sie dann auch dessen Betriebskosten tragen müssen.

## 11.4 Bibliografie

Vertiefende Literatur und Quellen finden Sie auf der Bibliografie-Webseite mit einer besonderen Empfehlung der Doktorarbeit über das Bezahlsystem von Florian Dold (PhD-Thesis 2019)<sup>1</sup>.

---

<sup>1</sup> [taler.net/en/bibliography.html](http://taler.net/en/bibliography.html) und [taler.net/papers/thesis-dold-phd-2019.pdf](http://taler.net/papers/thesis-dold-phd-2019.pdf)

## 12 Begriffsbestimmungen / Glossar

**ATM** Automated Teller Machine, Bankautomat mit Bargeld-Einzahlung

**Browser-Erweiterung** Add-on im Browser (Firefox, Chrome) eines → Wallet zum Abheben auch ohne QR-Scan/Smartphone

**Closing Time** Zeitfenster von 14 Tagen für den Abhebevorgang, in dem das empfangende Wallet die Coins vom gewählten Exchange abheben kann

**Coin** Kryptographisch gesicherte Repräsentation von Werten in Fiatwährung = Geldeinheit des E-Gelds im → Wallet (Nominalwert in Euro, Unique Identifier ist der EdDSA Public key)

**Credentials** Zugangsberechtigungen, welche das Wallet erzeugt, um einen Exchange aufzufordern, ihm die signierten Coins bereitzustellen

**Denomination key** Schlüsselvariable zum Festlegen der möglichen Coin-Nennwerte eines Exchange → Nominalwert

**Emergency Protokoll** Unterprotokoll zum Auslösen der → Recoup-Buchung im Fall eines geregelten Marktaustritts eines Exchange oder im Rahmen einer Abwicklung beim Insolvenzfall

**Exchange** Zentrale Steuerungslogik des Bezahlsystems mit der Datenbank zur Verwaltung aller SEPA-Buchungen und zum Abwickeln der Transaktionen von und zu Wallets

**Gebührenordnung** Im Taler-Protokoll fixierte Ordnung von Gebührenarten und Gebührenhöhen, siehe Gebühren

**IBAN-Buchung** Überweisungen mit Internationaler Bankkontonummer in Euro-Währung zwischen Girokonten und Exchange. Betrifft die Buchungsarten Withdrawal und Wire fee

**Lizenzen** Es gelten Affero GPLv3+ für den Exchange, LGPLv3+ für den Referenzcode der Integration in Händlerplattformen, GPLv3+ für Wallet-Code und Software für Kundenschnittstellen und die GNU Free Documentation License für dieses Dokument <sup>1</sup>

**Merchant** Von Taler Systems SA entwickeltes Bestell- und Bezahlsystem für → POS-Verkaufsstellen zum Bezahlen mit Taler-Wallets auf Android-Smartphones

**Merchant Backend** Anwendung zum Einfordern und Verwalten von Verkäuferumsätzen, die kein Wallet bei Verkäufern erfordert

<sup>1</sup> <https://www.gnu.org/licenses/fdl-1.3.html>

**Nennwert** = → Nominalwert eines Coin, z.B. 1, 2, 4, 8, 16, 32, 64, 128 Cent bis zu 65536 Cent (= 655,36 Euro)

**Nominalwert** Auf Euro-Währung lautender fester Nennwert eines Taler-Coin → Stückelung

**payto://-URI** Internet-Nomenklatur für Zahlungsziele zur Eingabe und Ausführung von Überweisungen (für IBAN-Girokonten, Zahlungsdienste, Kryptowährungen u.a.) <sup>2</sup>

**Point of Sale** Bestell- und Bezahlssystem an Verkaufsstellen wie z.B. Kiosken, Ladentheken, Supermarktkassen usw.

→ Bezahlvorgang mit der Point of Sale-Anwendung „Merchant“

**Public key** Identifier zum Prüfen der korrekten Verbindung zwischen Wallet und Exchange und als Buchungsvermerk im Girokontoauszug

**Recoup** Im Fall eines regulären Marktaustritts eines Exchange oder im Insolvenzfall des Betreibers wird der betroffene Exchange automatisch alle Wallets darüber informieren und sie veranlassen, die Geldwerte der noch nicht ausgegebenen Taler-Coins dieses Exchange an das ursprüngliche Girokonto zurückzugeben

**Refresh** Protokoll, das dafür sorgt, dass Coins in einem Wallet einen neuen Schlüssel erhalten wegen

1. Wechselgeld = Neuerzeugung von Coins bei Ausgaben mit Beträgen unterhalb des Nominalwerts eines verbrauchten Coin
2. Transaktionsabbruch infolge von Netzwerkfehlern, → Transaktionen
3. Verhindern des Ablaufs der Gültigkeit der Coins = Aktualisieren des Wallet, Auffrischen der Coins in ihm
4. Vertragsrücktritt oder Minderung (voller bzw. teilweiser Refund)

**Refund** Rückerstattung für den Fall, dass ein Verkäufer den Betrag seines Umsatzes mindert (= teilweise Refund) oder vom Vertrag zurücktritt (voller Refund); dies erzwingt immer einen → Refresh der betroffenen Coins im Wallet der Käufer

**Reserve** Eine Reserve entsteht im Exchange beim Abhebevorgang und umfasst signierte Coins, welche das empfangende Ziel-Wallet abrufen: Das Wallet erzeugt eine temporäre Zugangsberechtigung (→ Credentials), mit der das Wallet den Exchange auffordern kann, ihm Coins auszuhändigen, indem der Exchange diese signiert. Die Zugangsberechtigung wird in dem Augenblick angelegt, wenn ein Wallet-Besitzer von seinem Girokonto einen Betrag an den Exchange überweist mit dem betreffenden Credential als Buchungsvermerk im Girokontoauszug und einem eindeutigen Identifier (als öffentlichem Schlüssel), der den einmaligen Abhebevorgang betrifft

**Stückelung** Ein Coin kann stets nur den festen Nominalwert haben, den es bei seiner Erzeugung erhält, z.B. 1, 2, 4, 8, 16, 32, 64, 128 usw. bis zu 65536 Cent (655,36 €).

---

2 IETF-Webseite über den Uniform Resource Identifier 'payto'



Wird mit einem Coin ein Betrag bezahlt, der unterhalb seines Nominalwerts liegt, muss der Exchange den Unterschiedsbetrag an das ausgebende Wallet senden, indem es diesem frisch erzeugte Coins zubucht (das sogenannte → Wechselgeld)

**Taler-Cashier** Anwendung mit Mensch-Maschine-Interaktion zum Aufbuchen von Coins gegen Bargeld, welches eine Person wie ein Kassierer/Kassenwart entgegennimmt. Die Funktion entspricht einem ATM-Bankautomaten, der Bargeld annimmt und den Geldwert auf das Wallet aufbucht. Gegenwärtig müssen sowohl Kassenwart als auch Kunde jeweils ein Smartphone besitzen, der Kassenwart muss den Taler-Cashier, der Kunde ein Taler-Wallet installiert haben. Siehe Abschnitt 10.3

**Transaktionen** Kommunikation zwischen Exchange und Wallets für die jeweiligen Vorgänge des Abhebens, Ausgebens oder Auffrischen bzw. Rückerstattens von Coins (Withdrawal-, Deposit-, Refresh-, Refund-, Recoup-Buchungen)

**Wallet** Elektronische Geldbörse, Aufbewahrungsort der elektronischen Münzen → Coin

**Wechselgeld** Vom Exchange durch die Refresh-Buchung neu erzeugte Coins aufgrund eines Ausgabevorgangs, bei dem ein Coin verbraucht wird, dessen Nominalwert (Stückelung) über dem zu zahlenden Kaufpreis liegt, um den Unterschiedsbetrag auszugleichen

**Wertverluste** Nicht-transaktionsbezogene Kosten, die in Sonderfällen für Nutzer entstehen können (≠ Normalfall: transaktionsbezogene Gebühren)

**Wire fee** Gebühr für die aggregierte Buchung von Umsätzen auf ein Zielkonto von Verkäufern bei Geschäftsbanken, siehe → IBAN-Buchung

**Withdrawal** Abhebung vom (Giro)Konto = Aufbuchung von Beträgen aus (Fiat-)Währungen auf Coins in einem Wallet

Ein umfangreiches Glossar in englischer Sprache finden Sie auf der Taler-Webseite <https://docs.taler.net/developers-manual.html#developer-glossary> und wissenschaftliche Publikationen auf <https://taler.net/en/bibliography.html>.

# 13 AGB/Nutzungsbedingungen

Last Updated: 12.4.2019

Welcome! Taler Systems SA (“we,” “our,” or “us”) provides a payment service through our Internet presence (collectively the “Services”). Before using our Services, please read the Terms of Service (the “Terms” or the “Agreement”) carefully.

Overview -----

This section provides a brief summary of the highlights of this Agreement. Please note that when you accept this Agreement, you are accepting all of the terms and conditions and not just this section. We and possibly other third parties provide Internet services which interact with the Taler Wallet’s self-hosted personal payment application. When using the Taler Wallet to interact with our Services, you are agreeing to our Terms, so please read carefully.

Highlights: ~~~~~

- You are responsible for keeping the data in your Taler Wallet at all times under your control. Any losses arising from you not being in control of your private information are your problem.
- We will try to transfer funds we hold in escrow for our users to any legal recipient to the best of our ability within the limitations of the law and our implementation. However, the Services offered today are highly experimental and the set of recipients of funds is severely restricted.
- For our Services, we may charge transaction fees. The specific fee structure is provided based on the Taler protocol and should be shown to you when you withdraw electronic coins using a Taler Wallet. You agree and understand that the Taler protocol allows for the fee structure to change.
- You agree to not intentionally overwhelm our systems with requests and follow responsible disclosure if you find security issues in our services.
- We cannot be held accountable for our Services not being available due to circumstances beyond our control. If we modify or terminate our services, we will try to give you the opportunity to recover your funds. However, given the experimental state of the Services today, this may not be possible. You are strongly advised to limit your use of the Service to small-scale experiments expecting total loss of all funds.

These terms outline approved uses of our Services. The Services and these Terms are still at an experimental stage. If you have any questions or comments related to this Agreement, please send us a message to [legal@taler-systems.com](mailto:legal@taler-systems.com). If you do not agree to this Agreement, you must not use our Services.

How you accept this policy -----

By sending funds to us (to top-up your Taler Wallet), you acknowledge that you have read, understood, and agreed to these Terms. We reserve the right to change these Terms at any time. If you disagree with the change, we may in the future offer you with an easy option to recover your unspent funds. However, in the current experimental period you acknowledge that this feature is not yet available, resulting in your funds being lost unless you accept the new Terms. If you continue to use our Services other than to recover your unspent funds,

### 13 AGB/Nutzungsbedingungen

your continued use of our Services following any such change will signify your acceptance to be bound by the then current Terms. Please check the effective date above to determine if there have been any changes since you have last reviewed these Terms.

#### Services -----

We will try to transfer funds that we hold in escrow for our users to any legal recipient to the best of our ability and within the limitations of the law and our implementation. However, the Services offered today are highly experimental and the set of recipients of funds is severely restricted. The Taler Wallet can be loaded by exchanging fiat currencies against electronic coins. We are providing this exchange service. Once your Taler Wallet is loaded with electronic coins they can be spent for purchases if the seller is accepting Taler as a means of payment. We are not guaranteeing that any seller is accepting Taler at all or a particular seller. The seller or recipient of deposits of electronic coins must specify the target account, as per the design of the Taler protocol. They are responsible for following the protocol and specifying the correct bank account, and are solely liable for any losses that may arise from specifying the wrong account. We will allow the government to link wire transfers to the underlying contract hash. It is the responsibility of recipients to preserve the full contracts and to pay whatever taxes and charges may be applicable. Technical issues may lead to situations where we are unable to make transfers at all or lead to incorrect transfers that cannot be reversed. We will only refuse to execute transfers if the transfers are prohibited by a competent legal authority and we are ordered to do so.

#### Fees ----

You agree to pay the fees for exchanges and withdrawals completed via the Taler Wallet ("Fees") as defined by us, which we may change from time to time. With the exception of wire transfer fees, Taler transaction fees are set for any electronic coin at the time of withdrawal and fixed throughout the validity period of the respective electronic coin. Your wallet should obtain and display applicable fees when withdrawing funds. Fees for coins obtained as change may differ from the fees applicable to the original coin. Wire transfer fees that are independent from electronic coins may change annually. You authorize us to charge or deduct applicable fees owed in connection with deposits, exchanges and withdrawals following the rules of the Taler protocol. We reserve the right to provide different types of rewards to users either in the form of discount for our Services or in any other form at our discretion and without prior notice to you.

#### Eligibility -----

To be eligible to use our Services, you must be able to form legally binding contracts or have the permission of your legal guardian. By using our Services, you represent and warrant that you meet all eligibility requirements that we outline in these Terms.

#### Financial self-responsibility -----

You will be responsible for maintaining the availability, integrity and confidentiality of the data stored in your wallet. When you setup a Taler Wallet, you are strongly advised to follow the precautionary measures offered by the software to minimize the chances to lose access to or control over your Wallet data. We will not be liable for any loss or damage arising from your failure to comply with this paragraph.

#### Copyrights and trademarks -----

### 13 AGB/Nutzungsbedingungen

The Taler Wallet is released under the terms of the GNU General Public License (GNU GPL). You have the right to access, use, and share the Taler Wallet, in modified or unmodified form. However, the GPL is a strong copyleft license, which means that any derivative works must be distributed under the same license terms as the original software. If you have any questions, you should review the GNU GPL's full terms and conditions at <https://www.gnu.org/licenses/gpl-3.0.en.html>. "Taler" itself is a trademark of Taler Systems SA. You are welcome to use the name in relation to processing payments using the Taler protocol, assuming your use is compatible with an official release from the GNU Project that is not older than two years.

Your use of our services -----

When using our Services, you agree to not take any action that intentionally imposes an unreasonable load on our infrastructure. If you find security problems in our Services, you agree to first report them to [security@taler-systems.com](mailto:security@taler-systems.com) and grant us the right to publish your report. We warrant that we will ourselves publicly disclose any issues reported within 3 months, and that we will not prosecute anyone reporting security issues if they did not exploit the issue beyond a proof-of-concept, and followed the above responsible disclosure practice.

Limitation of liability & disclaimer of warranties -----

You understand and agree that we have no control over, and no duty to take any action regarding: Failures, disruptions, errors, or delays in processing that you may experience while using our Services; The risk of failure of hardware, software, and Internet connections; The risk of malicious software being introduced or found in the software underlying the Taler Wallet; The risk that third parties may obtain unauthorized access to information stored within your Taler Wallet, including, but not limited to your Taler Wallet coins or backup encryption keys. You release us from all liability related to any losses, damages, or claims arising from:

(a) user error such as forgotten passwords, incorrectly constructed transactions; (b) server failure or data loss; (c) unauthorized access to the Taler Wallet application; (d) bugs or other errors in the Taler Wallet software; and (e) any unauthorized third party activities, including, but not limited to, the use of viruses, phishing, brute forcing, or other means of attack against the Taler Wallet. We make no representations concerning any Third Party Content contained in or accessed through our Services.

Any other terms, conditions, warranties, or representations associated with such content, are solely between you and such organizations and/or individuals.

Limitation of liability -----

To the fullest extent permitted by applicable law, in no event will we or any of our officers, directors, representatives, agents, servants, counsel, employees, consultants, lawyers, and other personnel authorized to act, acting, or purporting to act on our behalf (collectively the "Taler Parties") be liable to you under contract, tort, strict liability, negligence, or any other legal or equitable theory, for:

(a) any lost profits, data loss, cost of procurement of substitute goods or services, or direct, indirect, incidental, special, punitive, compensatory, or consequential damages of any kind whatsoever resulting from:

(i) your use of, or conduct in connection with, our services; (ii) any unauthorized use of your wallet and/or private key due to your failure to maintain the confidentiality of your wallet; (iii) any interruption or cessation of transmission to or from the services; or (iv) any

### 13 AGB/Nutzungsbedingungen

bugs, viruses, trojan horses, or the like that are found in the Taler Wallet software or that may be transmitted to or through our services by any third party (regardless of the source of origination), or

(b) any direct damages.

These limitations apply regardless of legal theory, whether based on tort, strict liability, breach of contract, breach of warranty, or any other legal theory, and whether or not we were advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, so the above limitation may not apply to you.

Warranty disclaimer -----

Our services are provided "as is" and without warranty of any kind. To the maximum extent permitted by law, we disclaim all representations and warranties, express or implied, relating to the services and underlying software or any content on the services, whether provided or owned by us or by any third party, including without limitation, warranties of merchantability, fitness for a particular purpose, title, non-infringement, freedom from computer virus, and any implied warranties arising from course of dealing, course of performance, or usage in trade, all of which are expressly disclaimed. In addition, we do not represent or warrant that the content accessible via the services is accurate, complete, available, current, free of viruses or other harmful components, or that the results of using the services will meet your requirements. Some states do not allow the disclaimer of implied warranties, so the foregoing disclaimers may not apply to you. This paragraph gives you specific legal rights and you may also have other legal rights that vary from state to state.

Indemnity -----

To the extent permitted by applicable law, you agree to defend, indemnify, and hold harmless the Taler Parties from and against any and all claims, damages, obligations, losses, liabilities, costs or debt, and expenses (including, but not limited to, attorney's fees) arising from: (a) your use of and access to the Services; (b) any feedback or submissions you provide to us concerning the Taler Wallet; (c) your violation of any term of this Agreement; or (d) your violation of any law, rule, or regulation, or the rights of any third party.

Time limitation on claims -----

You agree that any claim you may have arising out of or related to your relationship with us must be filed within one year after such claim arises, otherwise, your claim is permanently barred.

Governing law -----

No matter where you're located, the laws of Switzerland will govern these Terms. If any provisions of these Terms are inconsistent with any applicable law, those provisions will be superseded or modified only to the extent such provisions are inconsistent. The parties agree to submit to the ordinary courts in Zurich, Switzerland for exclusive jurisdiction of any dispute arising out of or related to your use of the Services or your breach of these Terms.

Termination -----

In the event of termination concerning your use of our Services, your obligations under this Agreement will still continue.

Discontinuance of services -----

### 13 AGB/Nutzungsbedingungen

We may, in our sole discretion and without cost to you, with or without prior notice, and at any time, modify or discontinue, temporarily or permanently, any portion of our Services. We will use the Taler protocol's provisions to notify Wallets if our Services are to be discontinued. It is your responsibility to ensure that the Taler Wallet is online at least once every three months to observe these notifications. We shall not be held responsible or liable for any loss of funds in the event that we discontinue or depreciate the Services and your Taler Wallet fails to transfer out the coins within a three months notification period.

No waiver -----

Our failure to exercise or delay in exercising any right, power, or privilege under this Agreement shall not operate as a waiver; nor shall any single or partial exercise of any right, power, or privilege preclude any other or further exercise thereof.

Severability -----

If it turns out that any part of this Agreement is invalid, void, or for any reason unenforceable, that term will be deemed severable and limited or eliminated to the minimum extent necessary.

Force majeure -----

We shall not be held liable for any delays, failure in performance, or interruptions of service which result directly or indirectly from any cause or condition beyond our reasonable control, including but not limited to: any delay or failure due to any act of God, act of civil or military authorities, act of terrorism, civil disturbance, war, strike or other labor dispute, fire, interruption in telecommunications or Internet services or network provider services, failure of equipment and/or software, other catastrophe, or any other occurrence which is beyond our reasonable control and shall not affect the validity and enforceability of any remaining provisions.

Assignment -----

You agree that we may assign any of our rights and/or transfer, sub-contract, or delegate any of our obligations under these Terms.

Entire agreement -----

This Agreement sets forth the entire understanding and agreement as to the subject matter hereof and supersedes any and all prior discussions, agreements, and understandings of any kind (including, without limitation, any prior versions of this Agreement) and every nature between us. Except as provided for above, any modification to this Agreement must be in writing and must be signed by both parties.

Questions or comments -----

We welcome comments, questions, concerns, or suggestions. Please send us a message on our contact page at [legal@taler-systems.com](mailto:legal@taler-systems.com).

# 14 Datenschutzerklärung

Last Updated: 11.12.2019

This Privacy Policy describes the policies and procedures of Taler Systems SA (“we,” “our,” or “us”) pertaining to the collection, use, and disclosure of your information on our sites and related mobile applications and products we offer (the “Services” or “Taler Wallet”). This Privacy Statement applies to your personal data when you use our Services, and does not apply to online websites or services that we do not own or control.

Overview =====

Your privacy is important to us. We follow a few fundamental principles: We don’t ask you for personally identifiable information (defined below). That being said, your contact information, such as your phone number, social media handle, or email address (depending on how you contact us), may be collected when you communicate with us, for example to report a bug or other error related to the Taler Wallet. We don’t share your information with third parties except when strictly required to deliver you our Services and products, or to comply with the law. If you have any questions or concerns about this policy, please reach out to us at [privacy@taler-systems.net](mailto:privacy@taler-systems.net).

How you accept this policy =====

By using our Services or visiting our sites, you agree to the use, disclosure, and procedures outlined in this Privacy Policy.

What personal information do we collect from our users?

=====

The information we collect from you falls into two categories: (i) personally identifiable information (i.e., data that could potentially identify you as an individual) (“Personal Information”), and (ii) non- personally identifiable information (i.e., information that cannot be used to identify who you are) (“Non-Personal Information”). This Privacy Policy covers both categories and will tell you how we might collect and use each type.

We do our best to not collect any Personal Information from Taler Wallet users. We believe that the Taler Wallet never transmits personal information to our services without at least clear implied consent, and we only process and retain information with a strict business need. That being said, when using our Services, we inherently have to collect the following information:

- \* Bank account details necessary when receiving funds from you to top-up your wallet or to transfer funds to you when you are being paid via Taler. At the current experimental stage, only the pseudonym and password you entered in the bank demonstrator is stored.

- \* The amounts being withdrawn or deposited, with associated unique transaction identifiers and cryptographic signatures authorizing the transaction. Note that for purchases, we cannot identify the buyer from the collected data, so when you spend money, we only receive non-personal information.

14 Datenschutzerklärung

\* When you contact us. We may collect certain information if you choose to contact us, for example to report a bug or other error with the Taler Wallet. This may include contact information such as your name, email address or phone number depending on the method you choose to contact us.

How we collect and process information

=====

We may process your information for the following reasons:

- \* to transfer money as specified by our users (Taler transactions);
- \* to assist government entities in linking income to the underlying contract
- \* to support you using the Taler Wallet or to improve our Services

How we share and use the information we gather

=====

We may share your Personal Data or other information about you only if you are a merchant receiving income, with your bank, to the degree necessary to execute the payment.

We retain Personal Data to transfer funds to the accounts designated by our users. We may retain Personal Data only for as long as mandated by law and required for the wire transfers.

We primarily use the limited information we receive directly from you to enhance the Taler Wallet. Some ways we may use your Personal Information are to: Contact you when necessary to respond to your comments, answer your questions, or obtain additional information on issues related to bugs or errors with the Taler Wallet that you reported.

Agents or third party partners =====

We may provide your Personal Information to our employees, contractors, agents, service providers, and designees ("Agents") to enable them to perform certain services for us exclusively, including: improvement and maintenance of our software and Services. By accepting this Privacy Policy, as outlined above, you consent to any such transfer.

Protection of us and others =====

We reserve the right to access, read, preserve, and disclose any information that we reasonably believe is necessary to comply with the law or a court order.

What personal information can I access or change?

=====

You can request access to the information we have collected from you. You can do this by contacting us at [privacy@taler-systems.net](mailto:privacy@taler-systems.net). We will make sure to provide you with a copy of the data we process about you. To comply with your request, we may ask you to verify your identity. We will fulfill your request by sending your copy electronically. For any subsequent access request, we may charge you with an administrative fee. If you believe that the information we have collected is incorrect, you are welcome to contact us so we can update it and keep your data accurate. Any data that is no longer needed for purposes specified in the "How We Use the Information We Gather" section will be deleted after ninety (90) days.

Data retention =====

If you uninstall the Taler Wallet mobile applications from your device, or request that your information be deleted, we still may retain some information that you have provided to us to maintain the Taler Wallet or to comply with relevant laws.

Data security =====



14 Datenschutzerklärung

We are committed to making sure your information is protected. We employ several physical and electronic safeguards to keep your information safe, including encrypted user passwords, two factor verification and authentication on passwords where possible, and securing connections with industry standard transport layer security. You are also welcome to contact us using GnuPG encrypted e-mail. Even with all these precautions, we cannot fully guarantee against the access, disclosure, alteration, or deletion of data through events, including but not limited to hardware or software failure or unauthorized use. Any information that you provide to us is done so entirely at your own risk.

Changes and updates to privacy policy  
=====

We reserve the right to update and revise this privacy policy at any time. We occasionally review this Privacy Policy to make sure it complies with applicable laws and conforms to changes in our business. We may need to update this Privacy Policy, and we reserve the right to do so at any time. If we do revise this Privacy Policy, we will update the "Effective Date" at the bottom of this page so that you can tell if it has changed since your last visit. As we generally do not collect contact information and also do not track your visits, we will not be able to notify you directly. However, the Taler Wallet may inform you about a change in the privacy policy once it detects that the policy has changed. Please review this Privacy Policy regularly to ensure that you are aware of its terms. Any use of our Services after an amendment to our Privacy Policy constitutes your acceptance to the revised or amended agreement.

International users and visitors =====

Our Services are hosted in Switzerland. If you are a user accessing the Services from the European Union, Asia, US, or any other region with laws or regulations governing personal data collection, use, and disclosure that differ from Swiss laws, please be advised that through your continued use of the Services, which is governed by Swiss law, you are transferring your Personal Information to Switzerland and you consent to that transfer.

Questions =====

Please contact us at [privacy@taler-systems.net](mailto:privacy@taler-systems.net) if you have questions about our privacy practices that are not addressed in this Privacy Statement.