Cashless to e-Cash

Joel Häberli[*1]
Berner Fachhochschule, Departement Technik und Informatik, [*]Institute for Cybersecurity and Engineering ICE

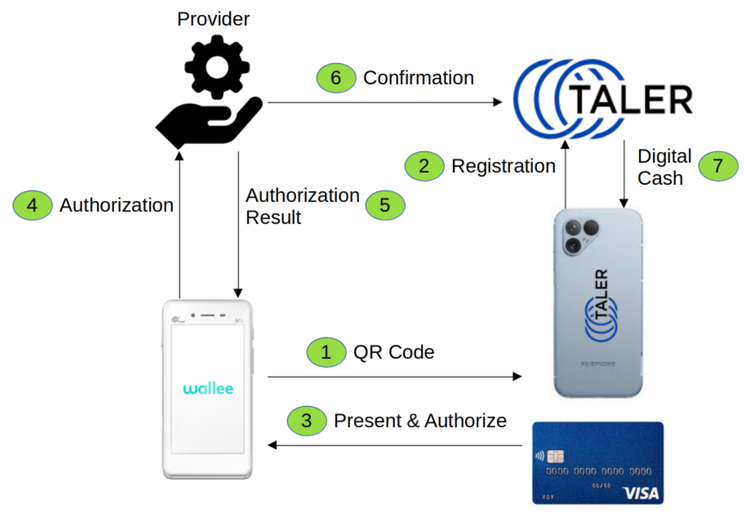
Motivation

This thesis realizes a framework to enable withdrawal of digital cash for GNU Taler through a established payment service provider. It addresses a report commissioned by the European Central Bank (ECB), which identified easy onboarding as one of the most important aspects of a Digital Euro. Our goal is to improve the uptake of GNU Taler.

Our key design objectives were:

1. Finality: Liability for the money is not on the side of the Taler operator
2. Convenience: The user-experience follows established patterns
3. Abort: Robust and secure payment flow allowing abort handling without loss of money

Additionally our design minimizes changes to the existing Taler system and works with a broad range of established payment methods such as credit cards, debit card, Paypal or Twint.



Bachelor thesis and further materials:

https://taler.net/en/news/2024-08.html

Terminals API design requirements

To allow the withdrawal of digital cash using Taler we designed the *Terminals API*.

It is responsible for:

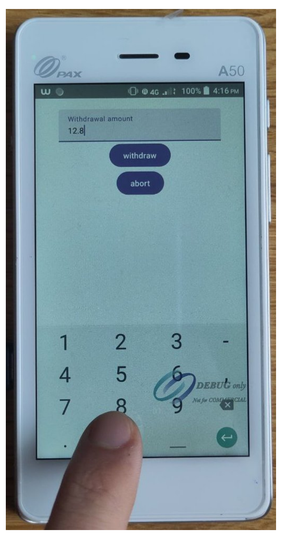
1. Associate Taler wallet with the financial transaction
2. Expose transaction confirmations to the Taler operator
3. Allow the Taler operator to reverse transactions if wallet fails to withdraw digital cash
4. Inform Taler wallet about transaction state

We implemented the Terminals API using Go under a Free Software license (GNU AGPLv3).

Paydroid POS Terminal App (Wallee A50)

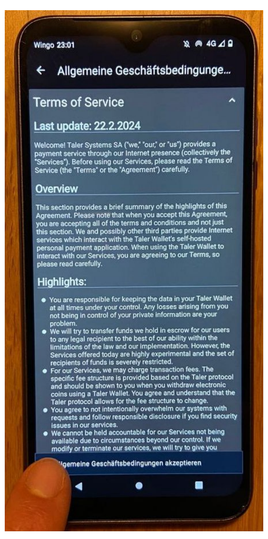
We implemented a payment service terminal on top of the Paydroid platform. Paydroid allows writing custom terminal applications with strong authentication of the customer. In combination with the Wallee payment provider this allows us to accept various payment instruments, including credit and debit cards. Our app asks the user to (1) enter the amount, (2) associate a wallet by scanning a QR code, (3) wait for the wallet to confirm, (4) to authorize the payment and (5) view a summary of the transaction.

(1) Enter Amount



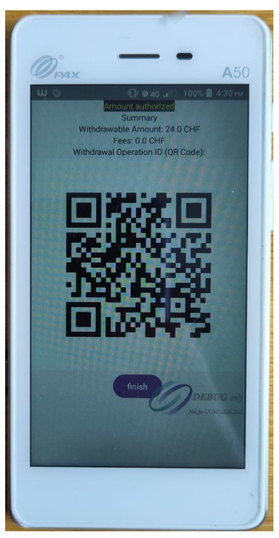
(2) Associate wallet

(3) Confirm withdrawal



(4) Authorize Payment

(5) View Summary



C2EC is extensible

The Wallee integration in the C2EC backend is an example. In principle it should be easy to integrate other acquirers. The architecture also supports other use cases, such as cash to e-cash.

The key limitation is that the provider must guarantee finality of the transaction. The Taler operator cannot efficiently recoup digital cash it issued to a Taler wallet.

The established payment service provider must ensure the customer has irrevokably authorized the transaction. This is typically done using two factor authentication, issued by the bank. The Taler operator is ensured in realtime, that they will receive the wire transfer.

Help us to support more payment providers and add an additional integration!

[1] joel.haeberli@taler.net