

# Cashless to e-Cash - Enabling withdrawal of digital cash through third parties in GNU Taler

Degree programme : BSc in Computer Science  
Thesis advisors : Prof. Dr. Benjamin Fehrensen, Prof. Dr. Christian Grothoff

This thesis realizes a framework to enable withdrawal of digital cash for GNU Taler through card payments. The integration addresses a report commissioned by the European Central Bank (ECB), which identified the easy onboarding as one of the most important aspects of a future Digital Euro. Our objective is to establish a user-experience which follows established patterns.

The new cashless-to-ecash (C2EC) components implement the technical protocols to issue digital cash to customers through card payments. The implemented terminal application built on top of the Paydroid platform shows how the protocol can be used by providers. Leveraging established patterns will lead to a better uptake of GNU Taler by enabling money to flow from existing payment systems into GNU Taler's digital cash.

From the perspective of the user the process looks like this:

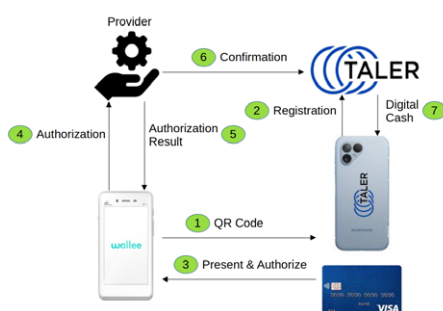
1. Bob wants to withdraw 10 CHF in digital cash. Luckily he is in a store which has one of the compatible Wallee terminals running the Taler integration.
2. The store owner Alice starts the withdrawal flow on the terminal and enters the amount of 10 CHF.
3. Bob now scans the QR code displayed on the terminal with his Taler wallet and authorizes the transaction using his credit card (and pin).
4. The digital cash is automatically withdrawn by his wallet. Bob can now spend his digital cash.

In a payment system, money must never be lost. Any step in the process can fail. We need to handle aborts. Abort handling was therefore an important aspect of the technical protocol. From step one to three the abortion is unequally easier, since no money was transferred and the withdrawal can simply be aborted. While the fourth step is automatic, it can still fail due to persistent power outage or lack of internet connectivity. When step four fails, the Taler operator should reverse the transaction at the provider's backend. The withdrawal, abort and transaction reversal cases were implemented during the thesis using Wallee as provider. The limitation of the process lies in the finality of the transaction on the side of the provider.

We expect BFH to operate C2EC as part of its Taler setup with real money in the future.



Joel Roman Häberli  
IT Security



Interacting Components - Wallee Terminal, Taler and Credit Card of the customer



Further reading: <https://taler.net/en/news/2024-08.html>