Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Cashless to e-Cash

Bachelor Thesis, Joel Häberli

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Intro – What?

- Cashless withdrawal of digital cash
- Implementation of...
  - Taler Exchange component C2EC
  - Payment Terminal App for the Paydroid platform

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Intro – Why?

- ECB plans a Digital Euro
- Easy onboarding is important
- Will improve acceptance
- Uptake of GNU Taler

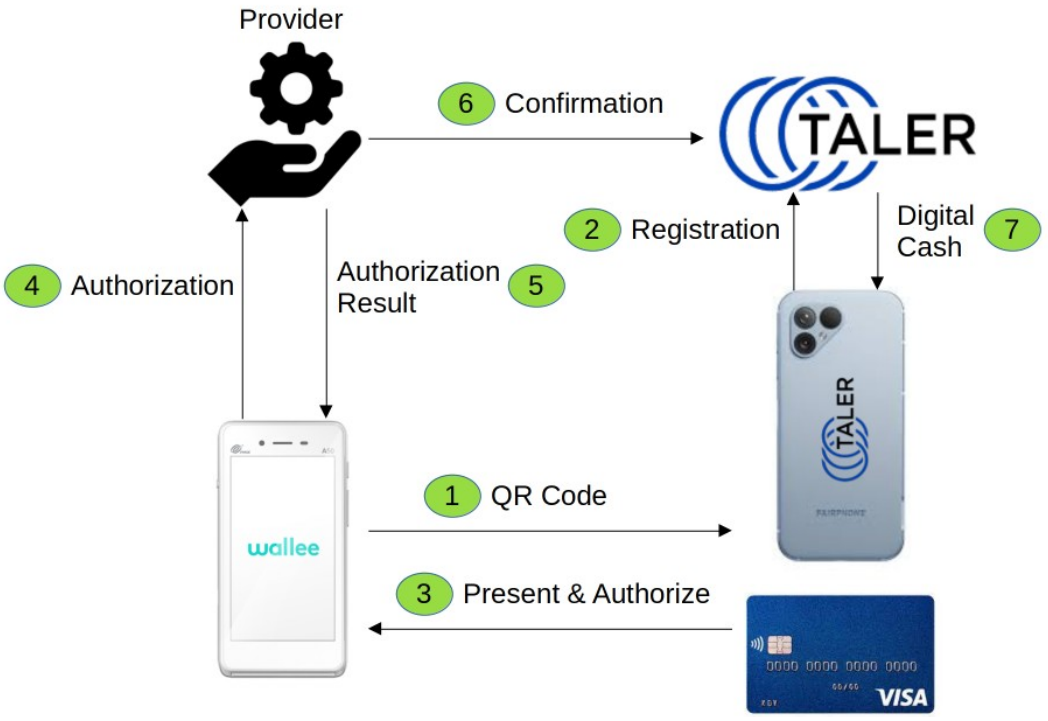
Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

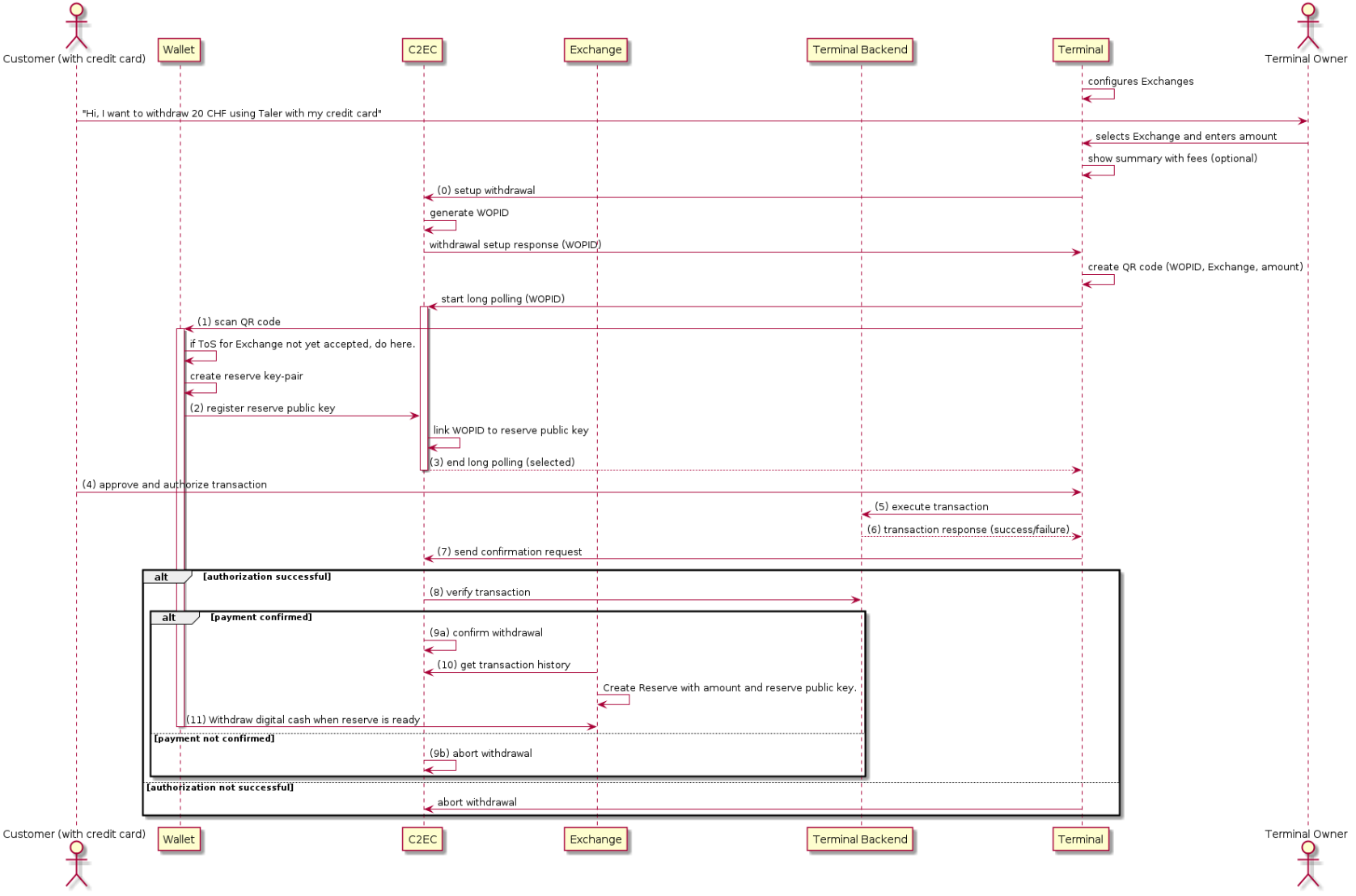
Content

- How does it work?
- Objectives & Fees
- Demo
- Architecture & Security considerations
- Conclusion

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

How does it work?




Customer (with credit card)
Wallet
C2EC
Exchange
Terminal Backend
Terminal
Terminal Owner
configures Exchanges
"Hi, I want to withdraw 20 CHF using Taler with my credit card"
selects Exchange and enters amount
show summary with fees (optional)
(0) setup withdrawal
generate WOPID
withdrawal setup response (WOPID)
create QR code (WOPID, Exchange, amount)
start long polling (WOPID)
(1) scan QR code
if ToS for Exchange not yet accepted, do here.
create reserve key-pair
(2) register reserve public key
link WOPID to reserve public key
(3) end long polling (selected)
(4) approve and authorize transaction
(5) execute transaction
(6) transaction response (success/failure)
(7) send confirmation request
alt
[authorization successful]
(8) verify transaction
alt
[payment confirmed]
(9a) confirm withdrawal
(10) get transaction history
Create Reserve with amount and reserve public key.
(11) Withdraw digital cash when reserve is ready
[payment not confirmed]
(9b) abort withdrawal
[authorization not successful]
abort withdrawal
Customer (with credit card)
Wallet
C2EC
Exchange
Terminal Backend
Terminal
Terminal Owner

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Objectives

- Finality
- User-Experience
- Security

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

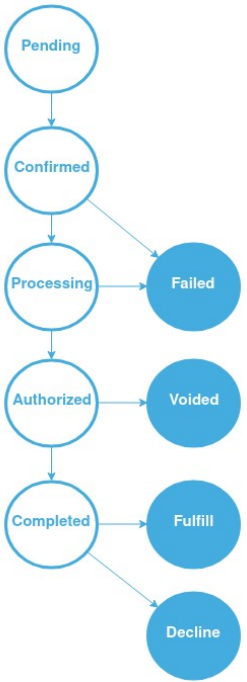
Finality

- When shall the money be available?
- The Exchange must be given the guarantee for the money

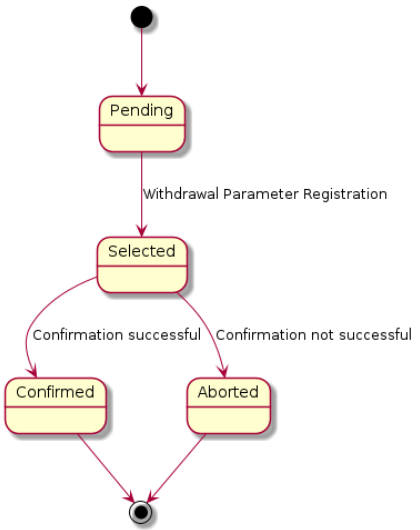
Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Finality

Wallee states



map



Taler states

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

User-Experience

- How does the withdrawal process looks from the perspective of the customer?
- Follow established patterns

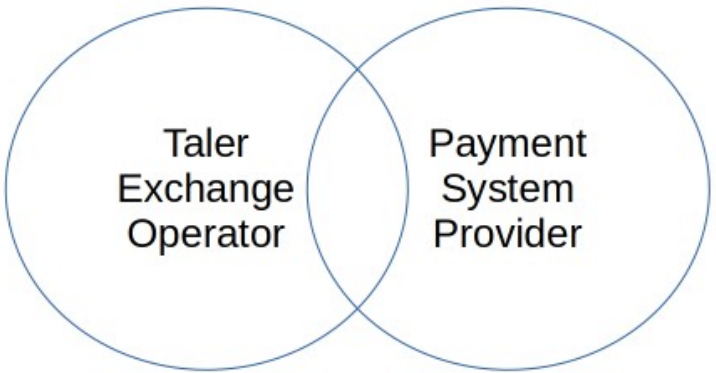
Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

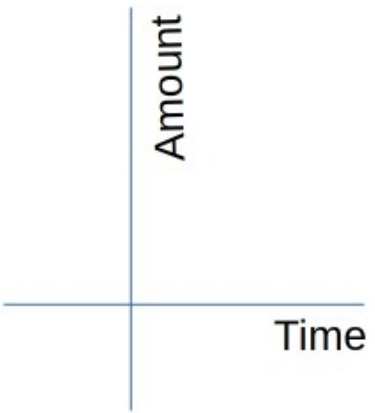
Security

- Money must never be lost
- Abort withdrawal
- Refund money, when not withdrawn

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Fees – It’s a mess





Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Fees – Model 1

- **Taler Exchange Operator** charges fees
- Terminal loads fees from C2EC config
- Terminal sends fees on check
- C2EC checks fees during confirmation

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Fees – Model 2

- **Payment Service Provider** charges fees
- Terminal sends fee amount on check
- C2EC checks fees during confirmation

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Fees – Model 3

- **Taler Exchange Operator** charges fees
- **Payment Service Provider** charges fees
- Terminal sends entire amount on check
- C2EC needs to check both fees in confirmation

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Fees – Model 4

- **Payment Service Provider** charges fees *late*
- Fees can only be known at the time of confirmation
- Fees need to be removed from the withdrawal amount by C2EC
- Customer will not be payed out the amount which was entered in the beginning

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Fees – Current Situation

- Currently Model 1 is implemented
- Supported by Wallee
- Fees are approximated by the C2EC operator

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Demo

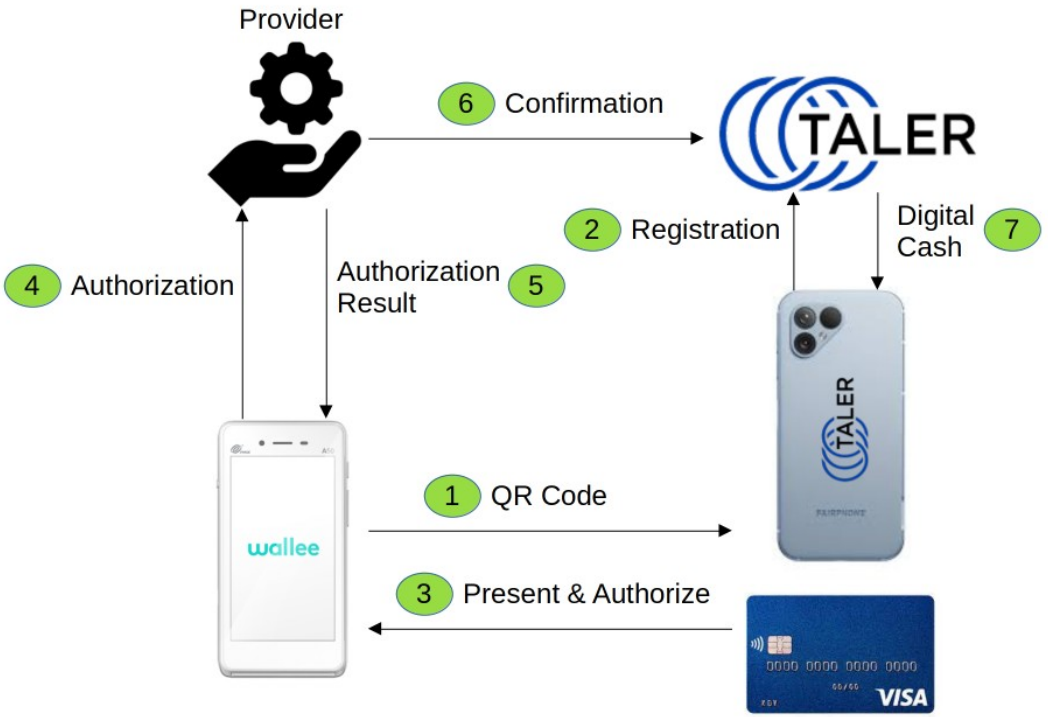
- Demonstrate withdrawal using the Terminal
- Demonstrate transaction reversal

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Install the Taler wallet ;)

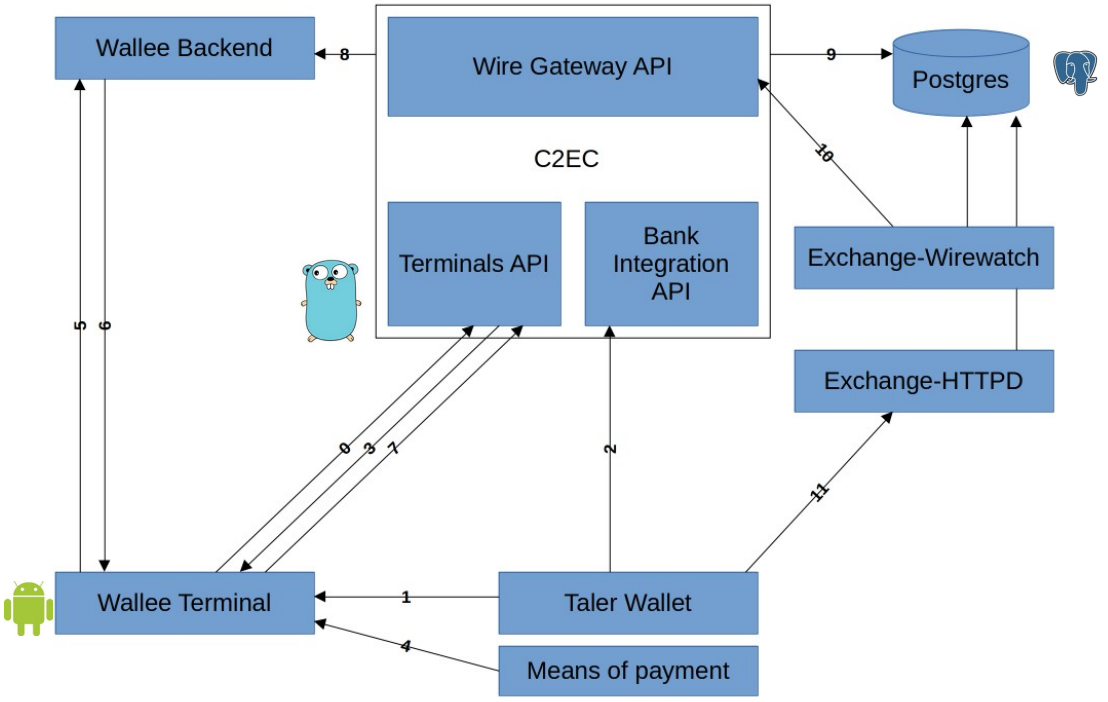
Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Architecture



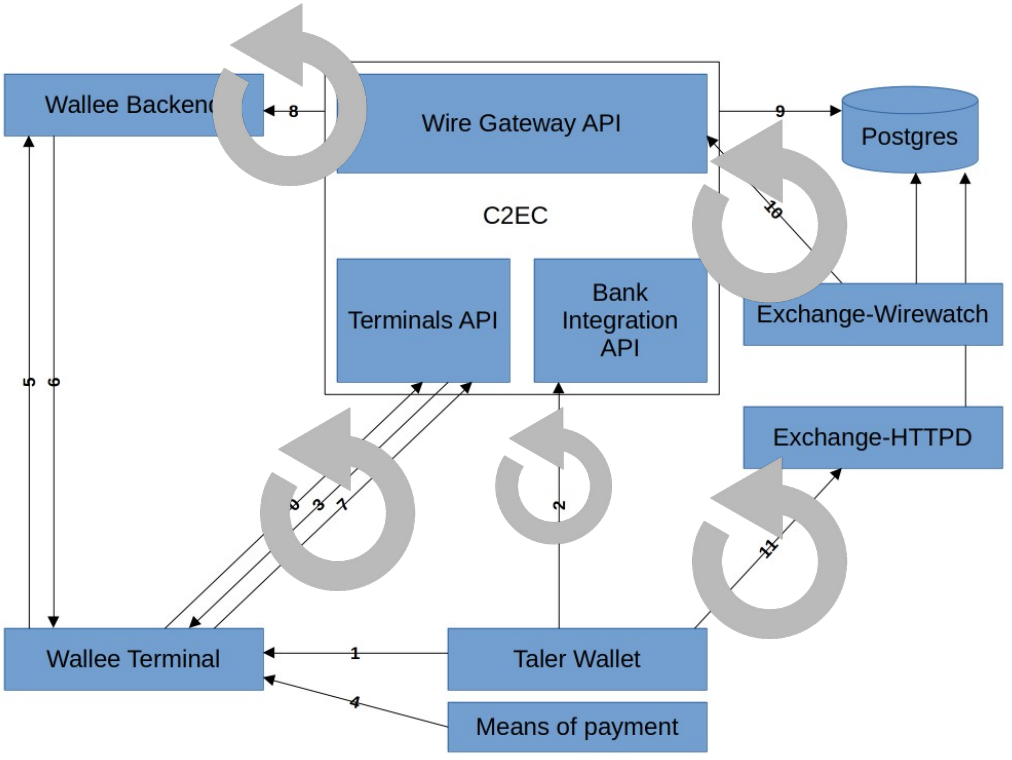
Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Architecture - Overview



Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Architecture – Retries



Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Architecture - Extensibility

- Implement specific provider client

```
type ProviderClient interface {
    SetupClient(provider *Provider) error
    GetTransaction(transactionId string) (ProviderTransaction, error)
    Refund(transactionId string) error
    FormatPayto(w *Withdrawal) string
}
```

- Register client in *SetupClient*

```
PROVIDER_CLIENTS["PROVIDER-NAME"] = clientInstance
```

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Architecture - Extensibility

- Implement specific provider transaction

```
type ProviderTransaction interface {
    AllowWithdrawal() bool
    AbortWithdrawal() bool
    Confirm(w *Withdrawal) error
    Bytes() []byte
}
```

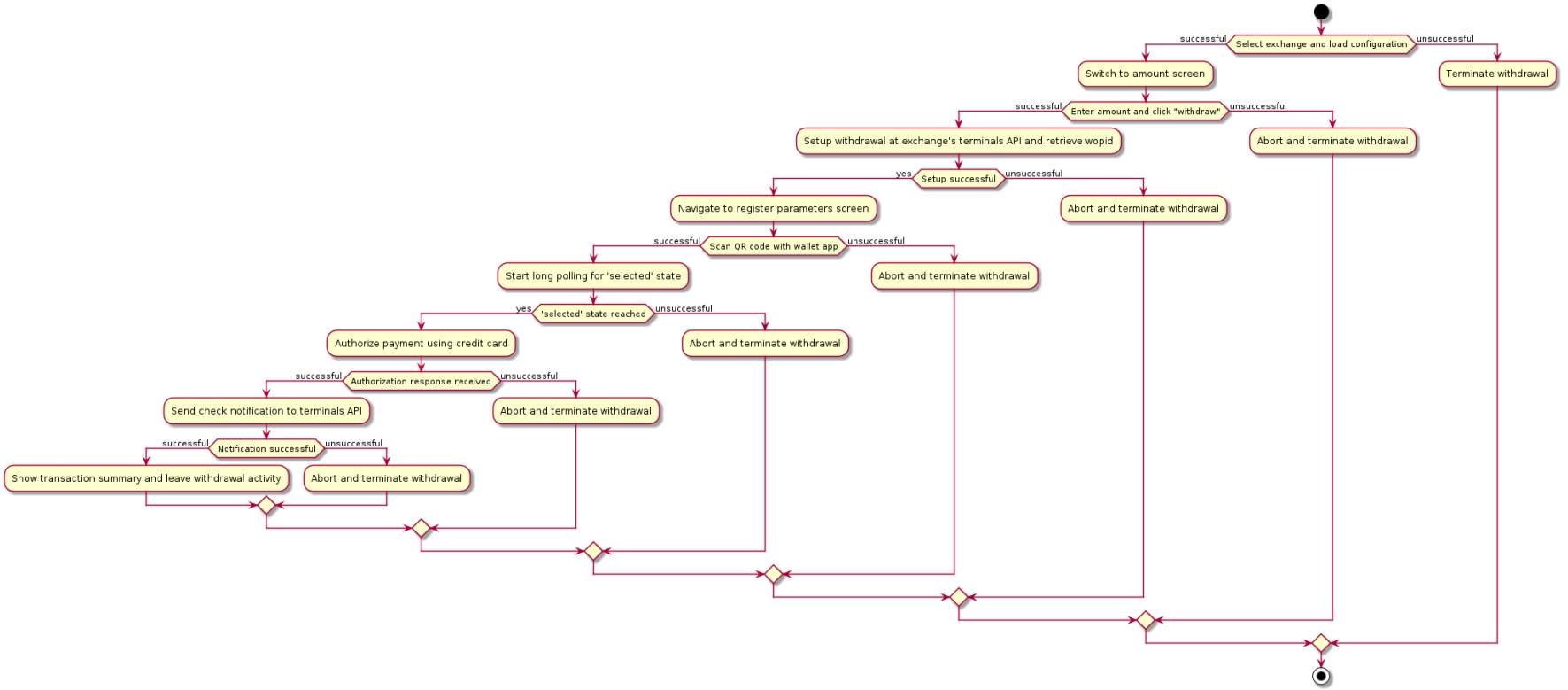
Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Architecture - Extensibility

- Configure new Provider
  - Setup Provider in Database
  - Configure Provider in Config
- Add Provider to *setupProviderClients* in main.go

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University

Architecture - Terminal



Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Security Considerations

- WOPID (Nonce)
- Terminal (PCI-DSS Certified)
- Confirmation (based on TLS)
- Credentials (stored using Argon2)

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Results

- Objectives: Finality, UX and Security
- C2EC with the new Terminals API
- Wallee Payment Terminal App
- Extensibility

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Reflection

- The UX can be enhanced
- Structure of the Go code in C2EC can be enhanced
- I set the right priorities
- I learned a lot about Taler, Go and Android

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Future Work

- Run the Wallee terminal at the BFH
- Integrate other providers
- Implement other Fee models
- Relative fees
- C2EC Terminal management
- ...

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Thanks for listening

NGI TALER

TALER

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