SECURE MOBILE NETWORKING

# DHL Hackstation

**Frederik Reiter**

TROOPERS

TECHNISCHE UNIVERSITÄT DARMSTADT


DHL

# Locker Types

## “FLAC” lockers

- Lots of hardware
  - Display
  - Scanner
  - Label printer
- Internet connectivity
- Usable without a smartphone

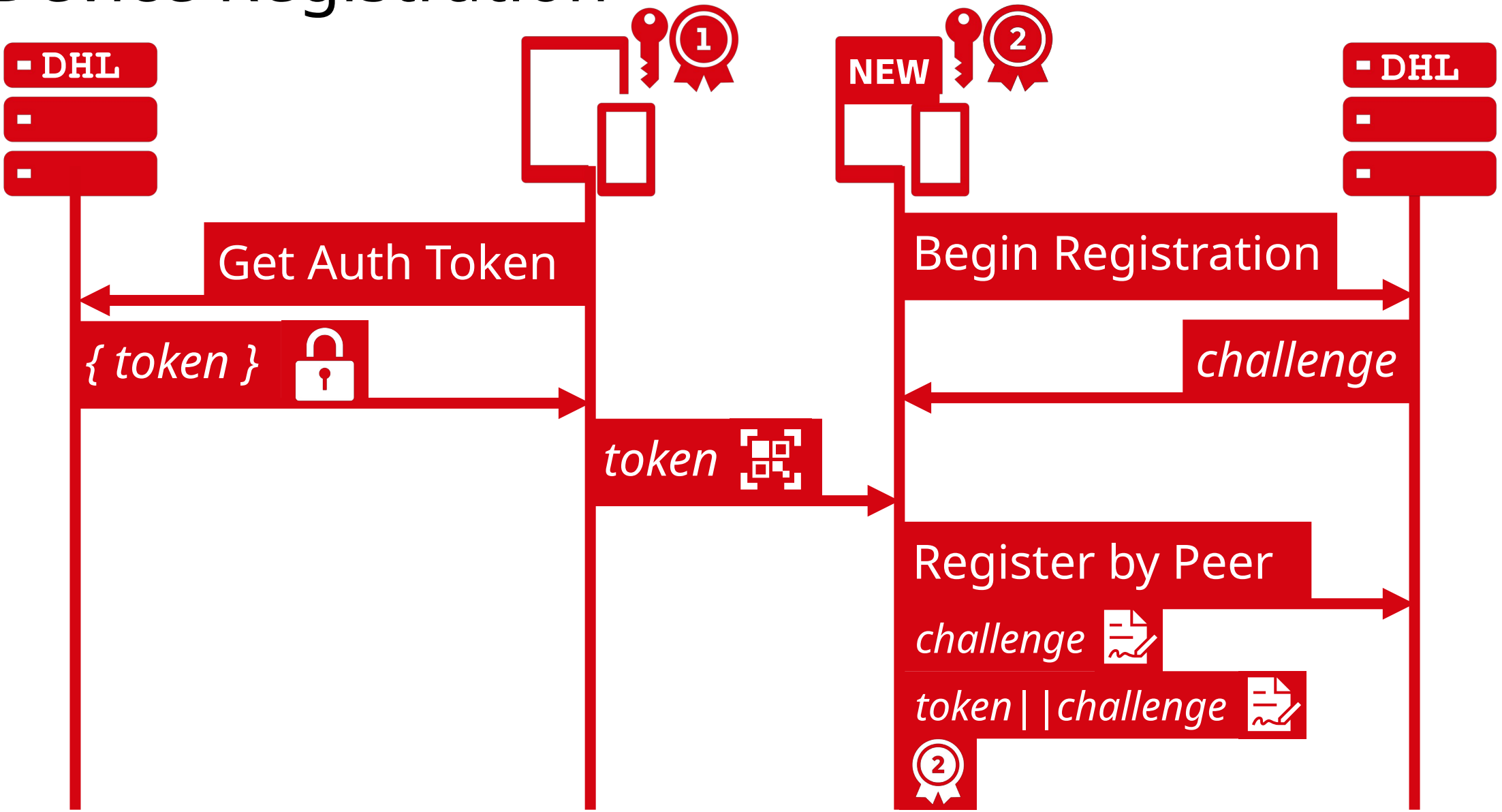
## “Lean” lockers

- No exposed hardware
- No internet connectivity
- Interact only with Bluetooth
- Requires Post & Paket app

# Prerequisites

- DHL account required to deliver directly to a parcel locker
- Only registered devices can interact with the locker
- Registered devices hold a private/public keypair
- First device is authenticated Out-Of-Band
  - Scan your DHL customer card
  - Receive a letter with a one-time activation code
- Further devices can be registered by any registered device

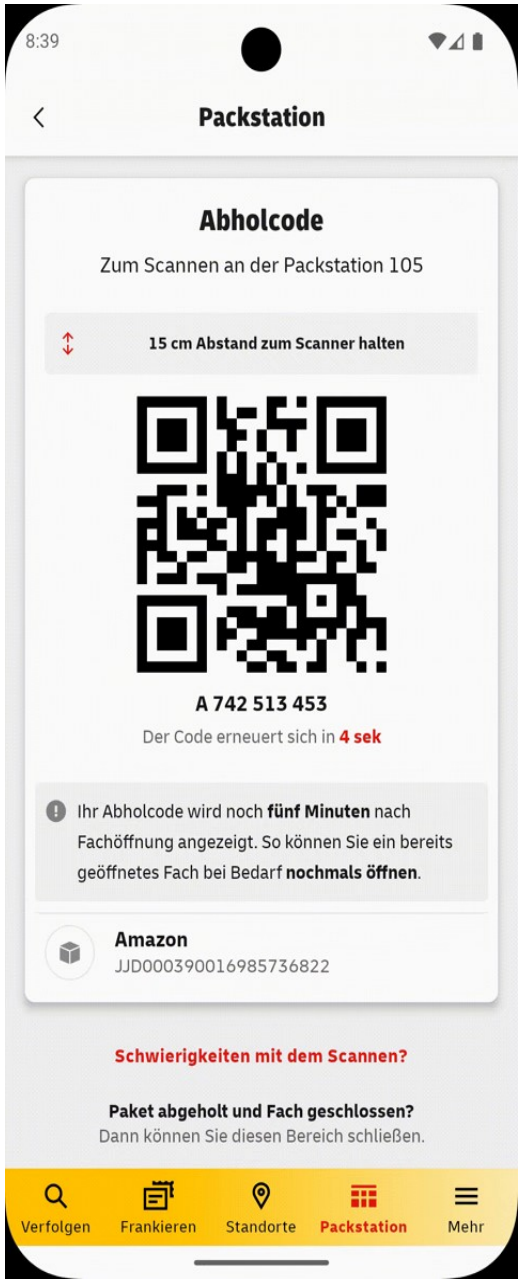
# Device Registration



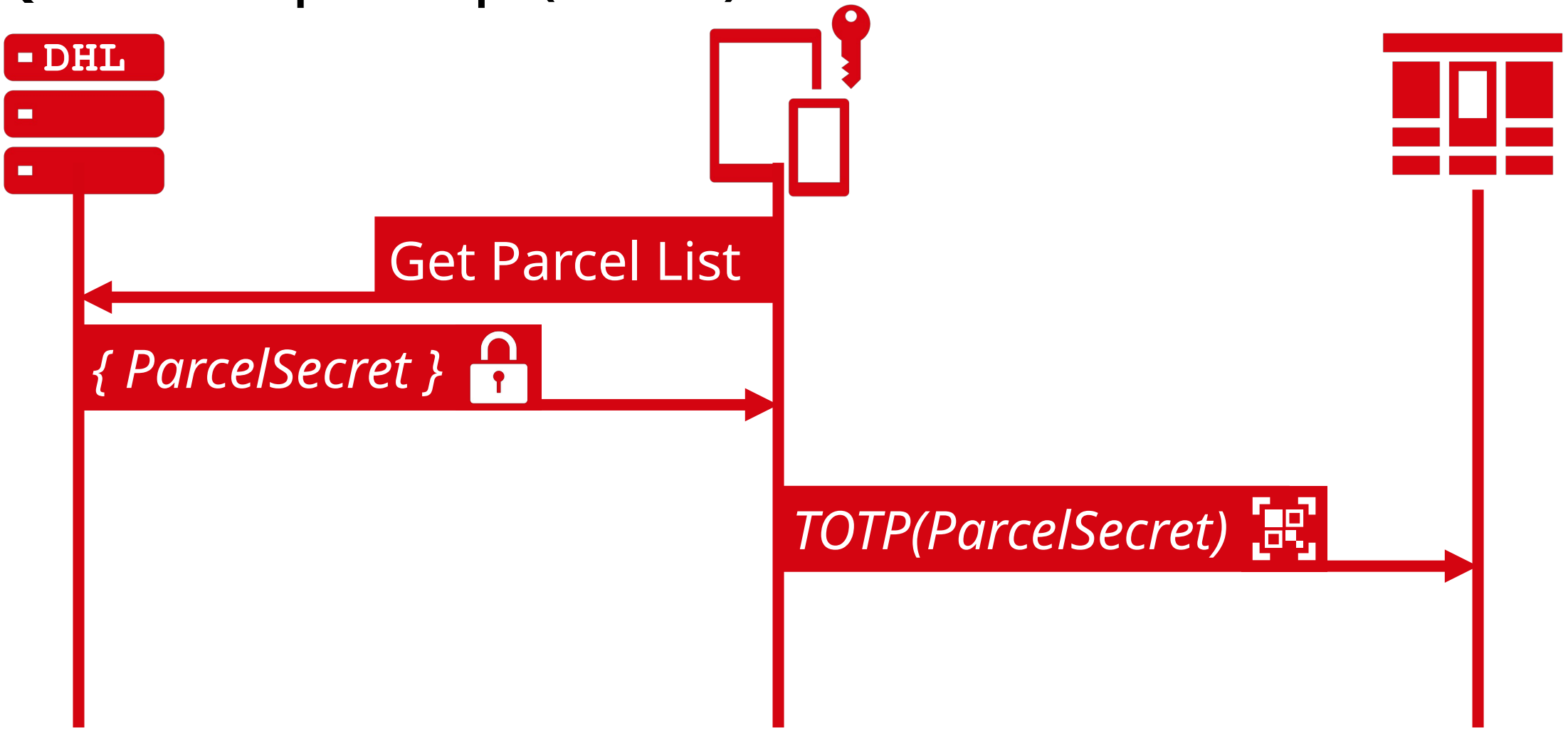
# demo

# QR-code pickup (FLAC)

- Scan a QR code, get your parcel
- Uses off-the-shelf TOTP algorithm
  - Get TOTP secret from DHL server
  - Calculate TOTP token
  - Locker checks TOTP token
- TOTP secret is encrypted with public key



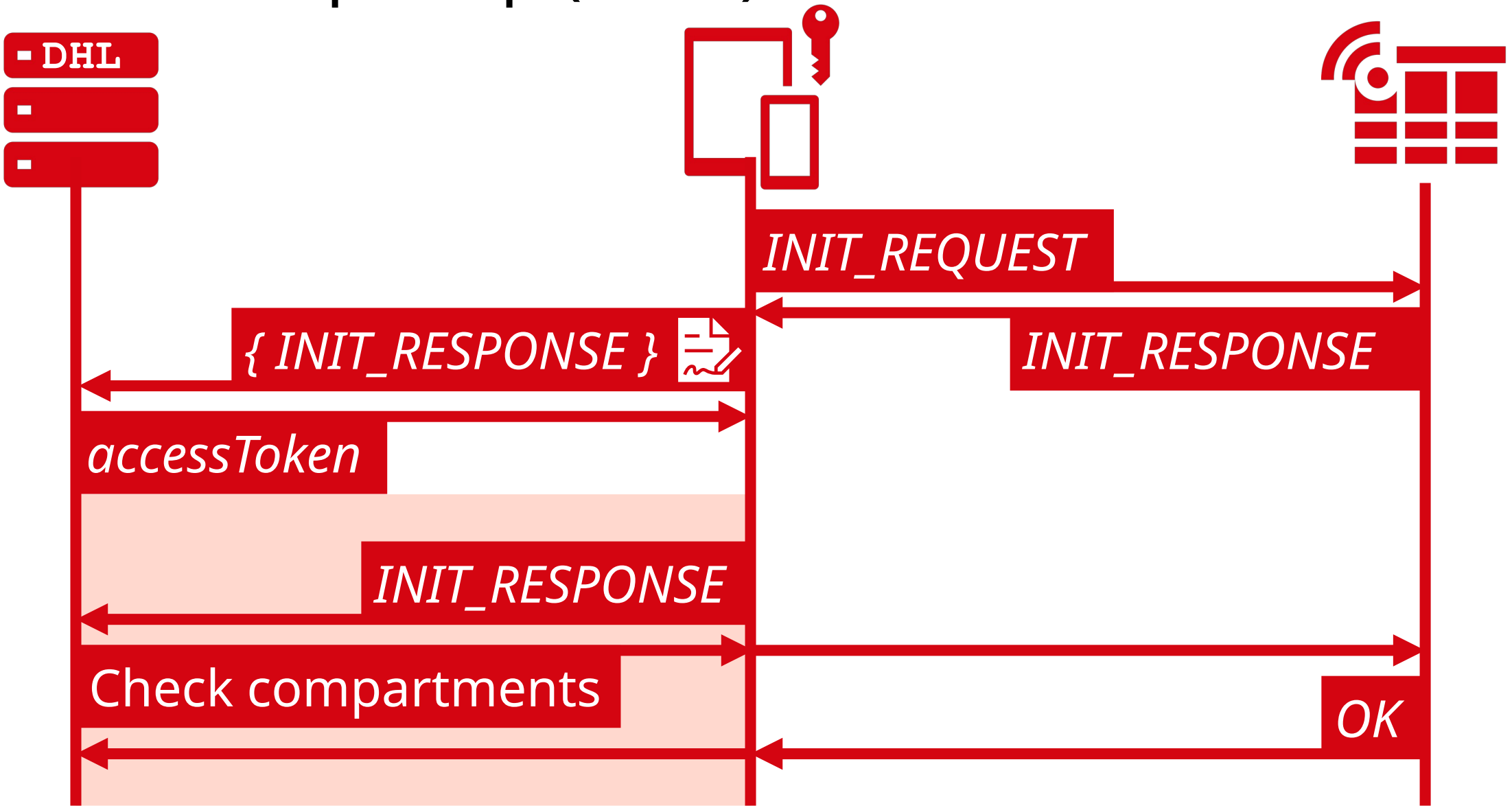
# QR-code pickup (FLAC)



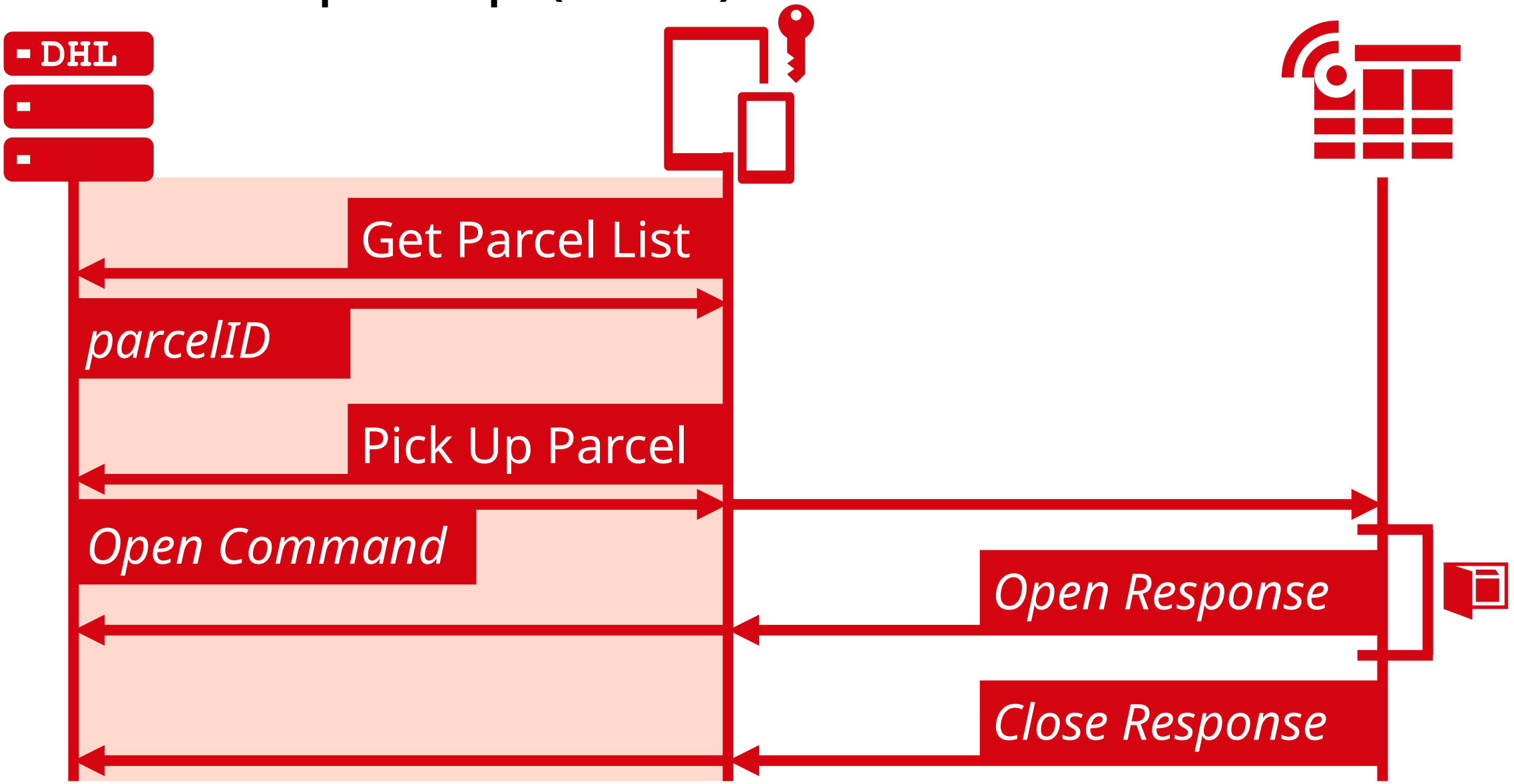
# Bluetooth pickup (Lean)

- Lean Packstation (LPS) lockers don’t need internet connectivity
  - User’s device is used to relay messages
  - Saves costs by using the user’s bandwidth
- We control our device → Straightforward MiTM vector
  - See all messages
  - Manipulate messages arbitrarily, in both directions
- Two communication layers
  - Bluetooth message layer
  - Logical message layer

# Bluetooth pickup (Lean)



# Bluetooth pickup (Lean)



# Attacks by Design

- We experimented with many attacks on the implementation
- Black box cryptography is hard to audit
  - All the crypto we can see seems solid
  - We poked at the black box crypto at it didn’t fall apart
- But a few attacks are possible by design

# Malicious User

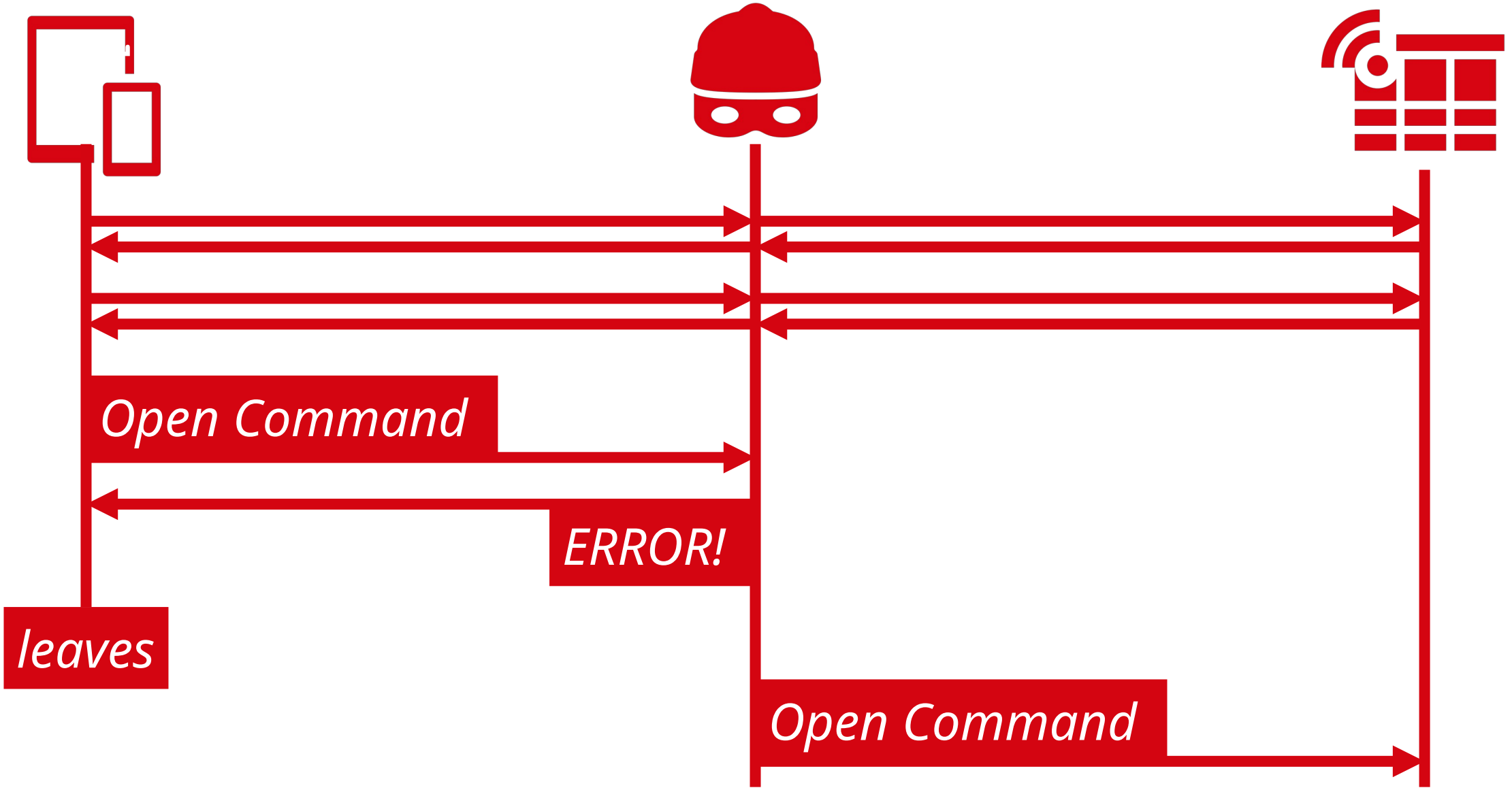
- Scenario: Defraud the sender of a parcel
- Idea: Never send the “Close“ notification to the API
- Parcel is marked as delivered when the compartment is closed
- API thinks the parcel is still in the locker
- After seven days, the parcel is “sent back“
- Users claims they never picked up the parcel → Refund

# demo

# Machine-in-the-Middle

- Scenario: Steal a parcel from an honest user
- Lean Packstation uses unpaired Bluetooth connections
  - No encryption, no authentication
- Passive attacks not possible (replay does not work)
- Active attack possible by spoofing BLE advertisment

# Machine-in-the-Middle



# Response to our research

- DHL Group has a Vulnerability Disclosure Program
  - All our research was in the scope of this program
- During our research, DHL saw our requests in their API logs
  - X-Bug-Bounty header
- **They contacted us** for a meeting about our findings
- Attacks “work as intended“
  - Trade-off between convenience and security
- Opinion: Impressive response by DHL
  - Some vendors actually value security research!

# Questions?

@fre@infosec.exchange

frereit.de

fre.99

github.com/frereit/pydhl