

eqiva Bluetooth
Türschlossantrieb

REVERSING THE PROTOCOL

Mira Weller
mweller@seemoo.de



BTM

MP5

MP3

MP4

BTM
BTM
BTM

STMBL052
ST
©

RST?:
touching with osci probe
resets connection

Seriellport 2

PRG1 = BCM debug conn.

ADR

Seriellport 1

SWIM
VDD
RESET
GND

PRG2 = STM8 SWIM connector

STM -> BCM

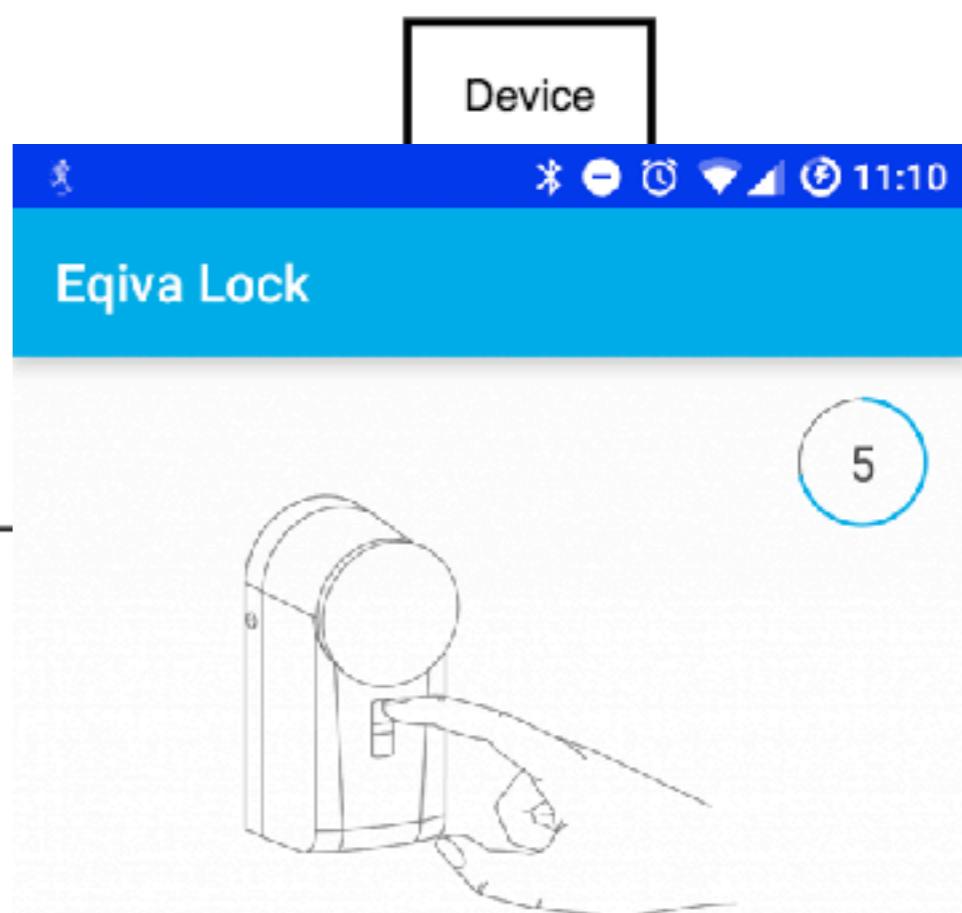
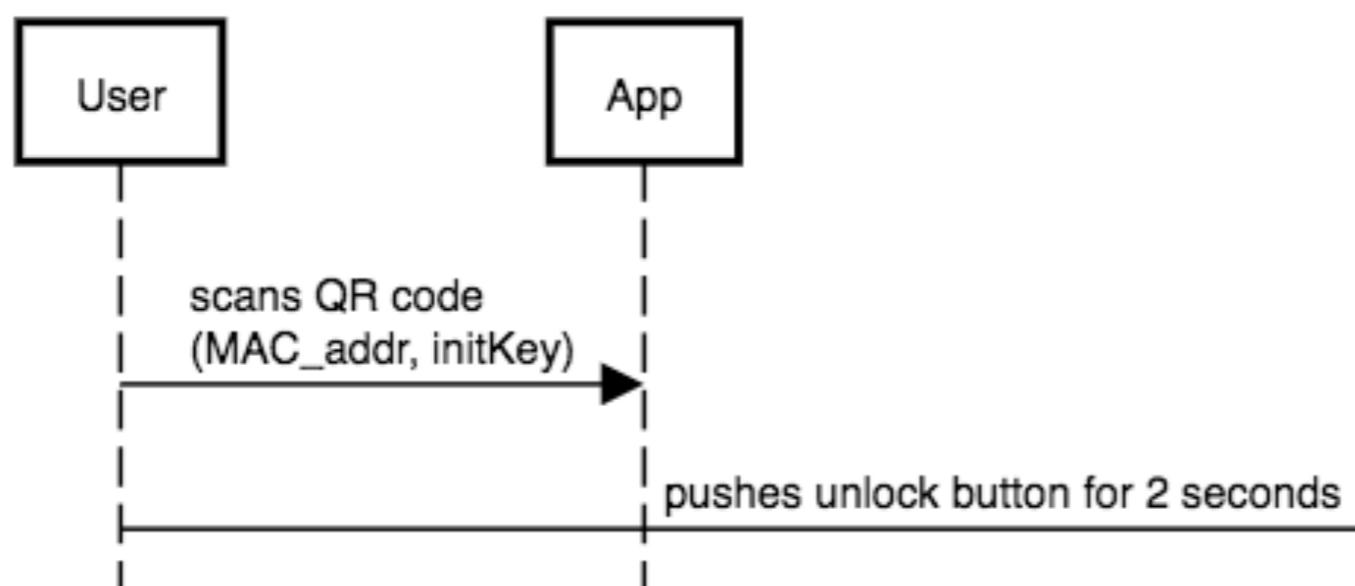
BCM -> STM

```
import net.sourceforge.zbar.Symbol;

public class QRCodeScannerFragment extends b<SetupWizardActivity> implements PreviewCallback {
    private static final Pattern c = Pattern.compile("M( [A-F0-9]{12})K( [A-F0-9]{32})( [A-Z0-9]{10})");
    ImageScanner a;
    ...
    ...
    | scans QR code
    | (MAC_addr, initKey)
    ...
}
```



Pairing (first user)



Aktivieren Sie den Pairingmodus an
Ihrem Gerät. Drücken Sie die obere
Gerätetaste und halten Sie diese, bis die
LED orange blinkt.



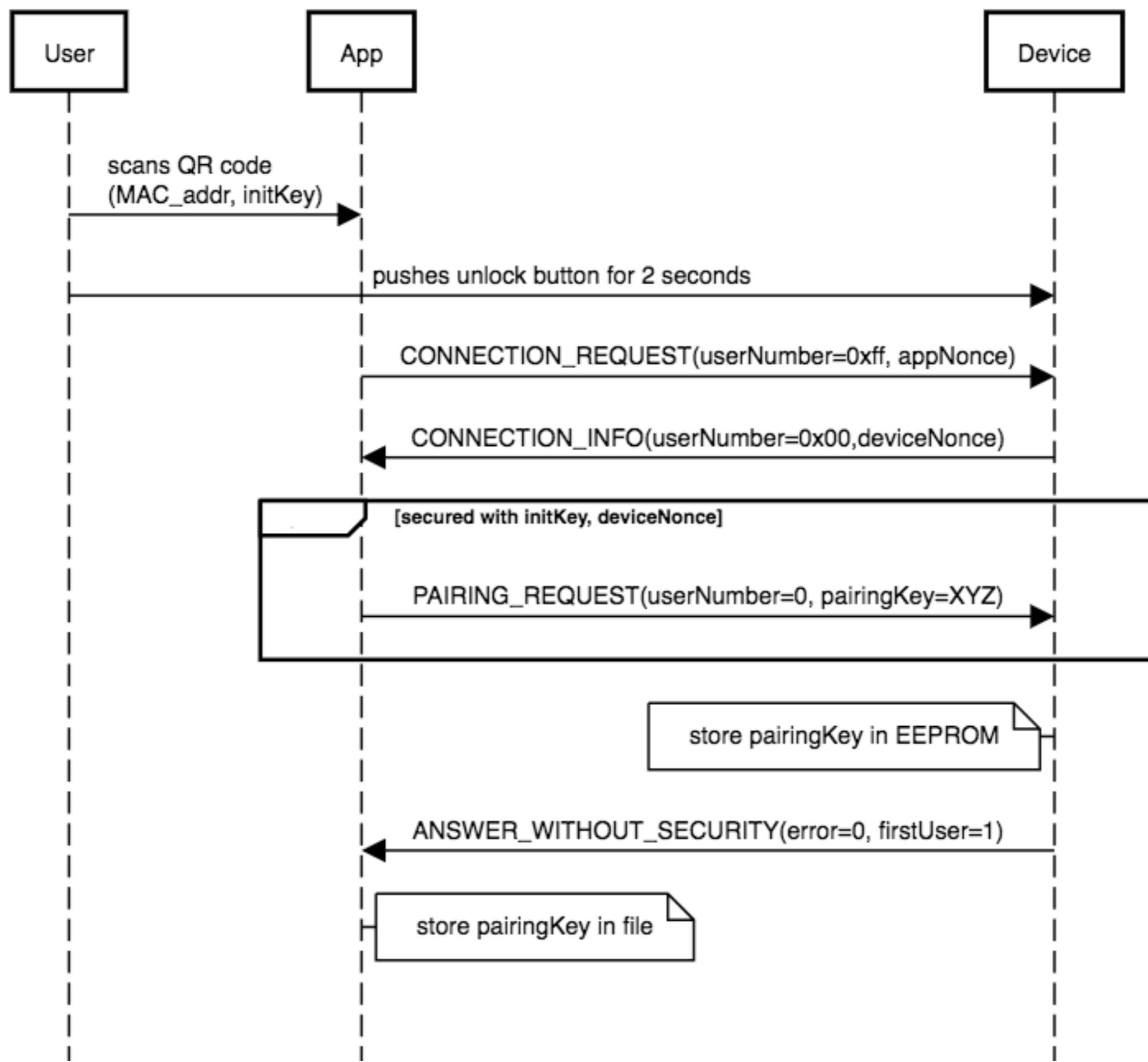
Weiter



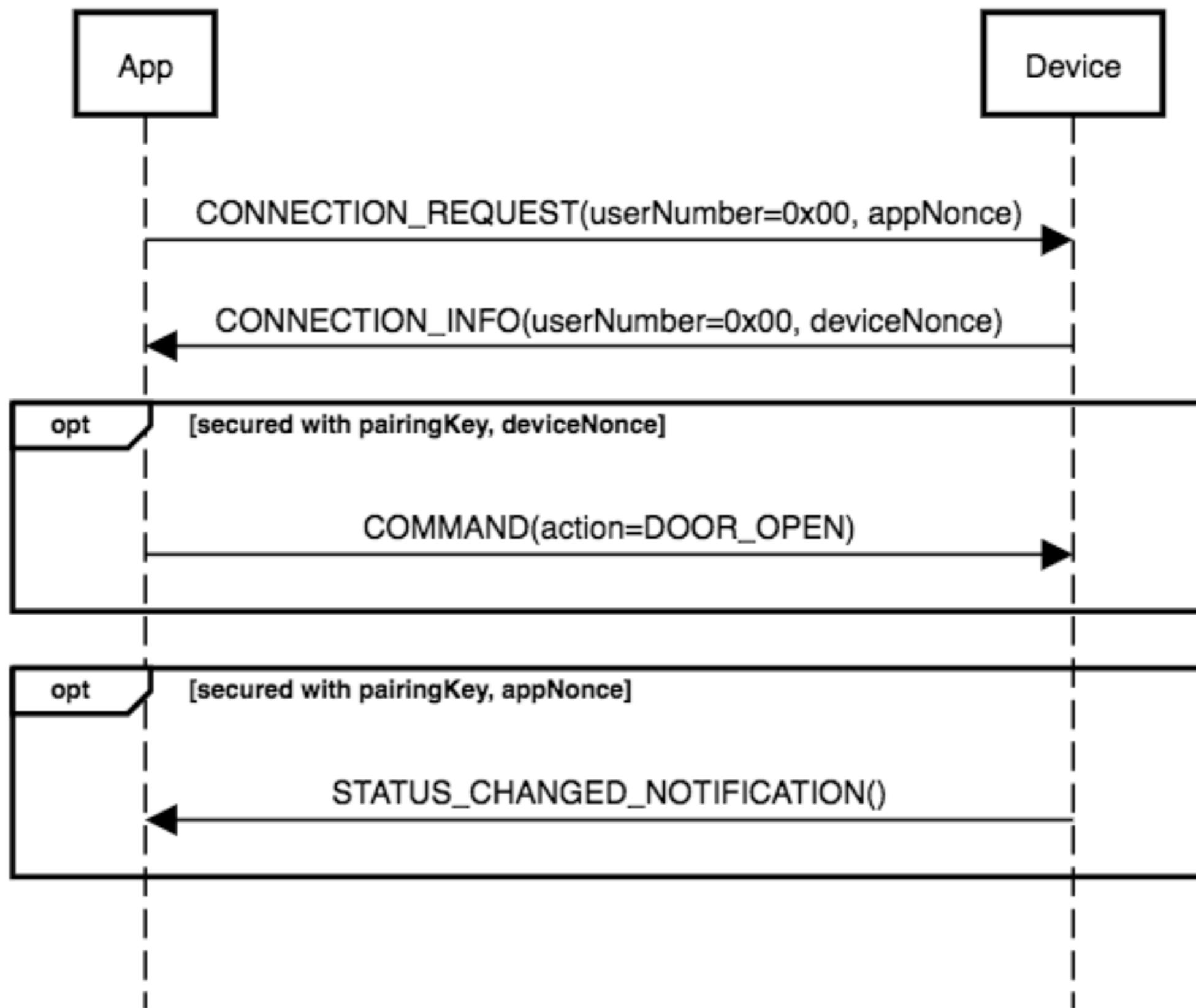


```
public enum CommandTypeEnum {  
    FRAGMENT_ACK(0),  
    ANSWER_WITHOUT_SECURITY(1),  
    CONNECTION_REQUEST(2),  
    CONNECTION_INFO(3),  
    PAIRING_REQUEST(4),  
    STATUS_CHANGED_NOTIFICATION(5),  
    CLOSE_CONNECTION(6),  
    BOOTLOADER_START_APP(16),  
    BOOTLOADER_DATA(17),  
    BOOTLOADER_STATUS(18),  
    ANSWER_WITH_SECURITY(129),  
    STATUS_REQUEST(130),  
    STATUS_INFO(131),  
    MOUNT_OPTIONS_REQUEST(132),  
    MOUNT_OPTIONS_INFO(133),  
    MOUNT_OPTIONS_SET(134),  
    COMMAND(135),  
    AUTO_RELLOCK_SET(136),  
    PAIRING_SET(138),  
    USER_LIST_REQUEST(139),  
    USER_LIST_INFO(140),  
    USER_REMOVE(141),  
    USER_INFO_REQUEST(142),  
    USER_INFO(143),  
    USER_NAME_SET(144),  
    USER_OPTIONS_SET(145),  
    USER_PROG_REQUEST(146),  
    USER_PROG_INFO(147),  
    USER_PROG_SET(148),  
    AUTO_RELLOCK_PROG_REQUEST(149),  
    AUTO_RELLOCK_PROG_INFO(150),  
    AUTO_RELLOCK_PROG_SET(151),  
    LOG_REQUEST(152),  
    LOG_INFO(153),  
    KEY_BLE_APPLICATION_BOOTLOADER_CALL(154),  
    DAYLIGHT_SAVING_TIME_OPTIONS_REQUEST(155),  
    DAYLIGHT_SAVING_TIME_OPTIONS_INFO(156),  
    DAYLIGHT_SAVING_TIME_OPTIONS_SET(157),  
    FACTORY_RESET(158);
```

Pairing (first user)



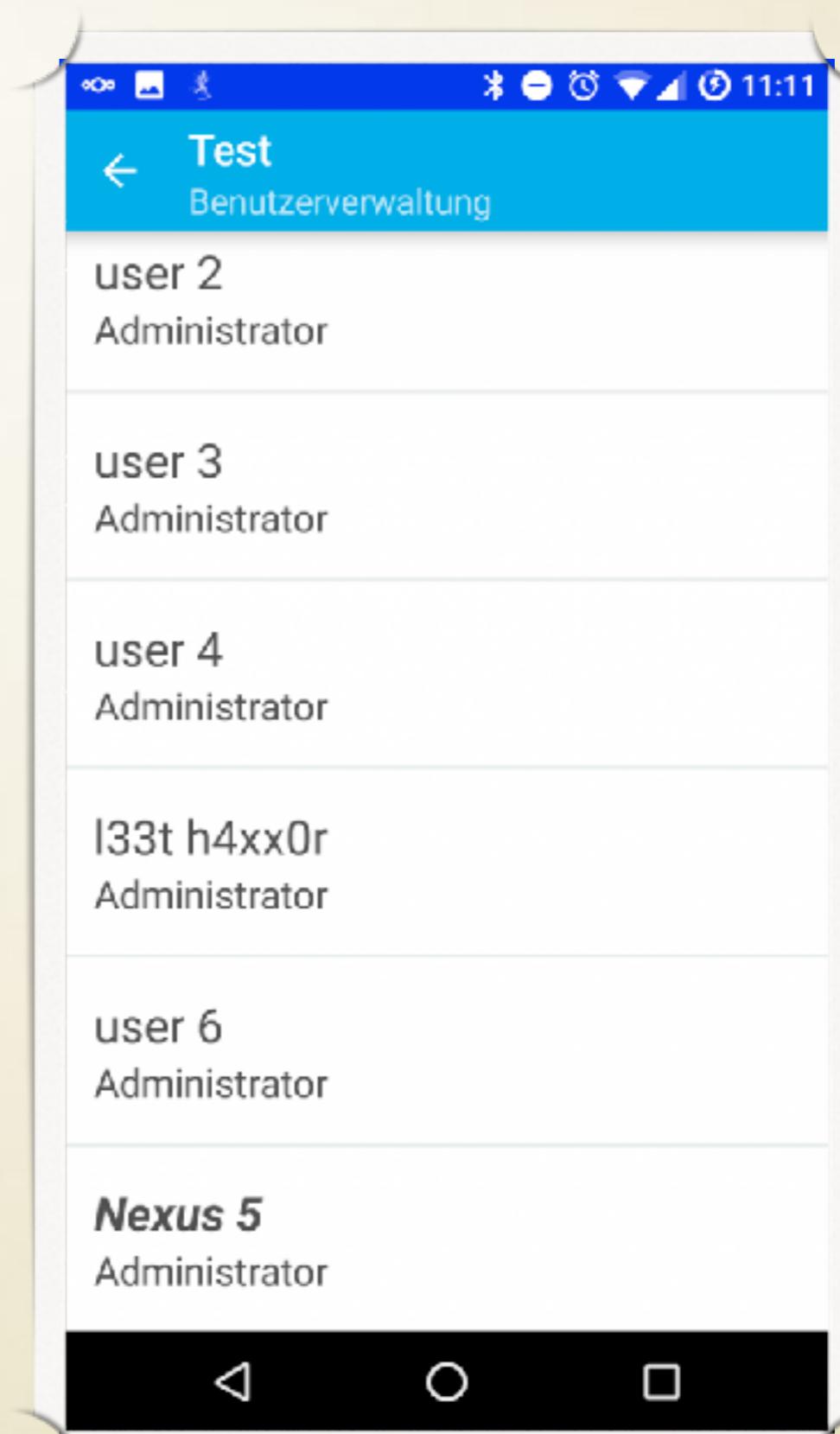
Door action command



MALICIOUS VENDOR ATTACK

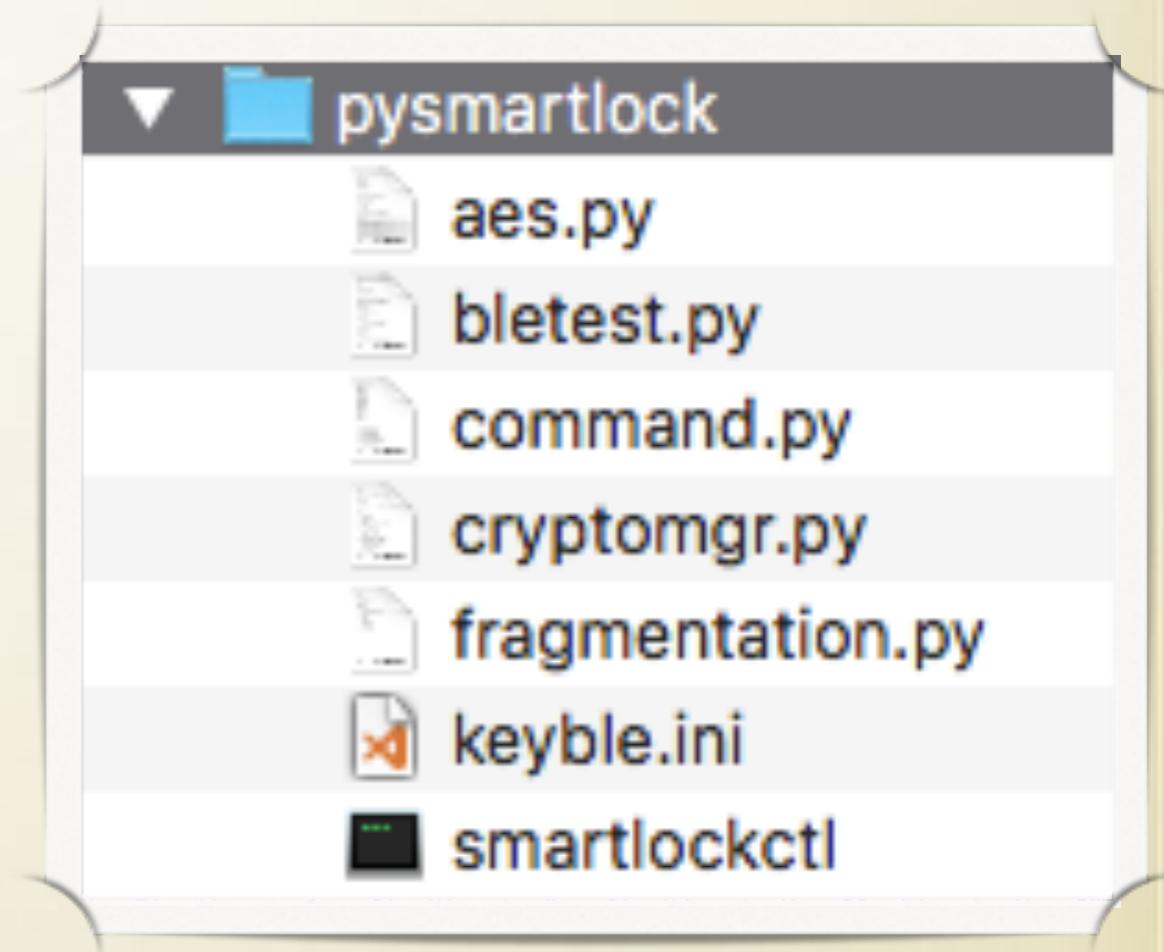
- verkauft vorgepairstes Gerät, „besucht“ einige Zeit später Lieferadresse
- Kunde könnte es unter *Einstellungen -> Benutzerverwaltung* entdecken

```
|-----  
| ANSWER_WITHOUT_SECURITY(error=0, firstUser=1)  
|-----
```



ERGEBNIS

- Protokoll macht einen vernünftigen Eindruck
- Keine Cloud
- Keine Aussage zur Firmware möglich (Bugs/Backdoors unklar)



[https://github.com/
luelista/hwreverse/](https://github.com/luelista/hwreverse/)