

13.10.2020 // Mitschnitt - OTA Proof-of-Concepts

```
connected
send 901a0000010000
recv a1bf8c11e96c9e4491af
RndA: eba87149d88ced0d
send 90af000010e055e9553cbfd8ae34cb7e0b9051bd4e00
recv 83ee10665e78da619100
send 90fc000000
recv 56730aec09169b2e9100
send 901a0000010000
recv 18e7f105cdfc574291af
RndA: 0278d460c6aa4af4
send 90af000010ac299e117b1c7eeb8984737978c546a800
recv b36cebe94cee71799100
session_key: 0278d46084f2ccea
iv: 0000000000000000
send 90ca000005eeffc00b8300
recv 89bad4f6f92dbc479100
session_key: 0278d46084f2ccea
iv: 0000000000000000
send 905a000003eeffc000
recv 9100
send 90aa0000010000
recv eda2aa1582cc7252d9bf19a330d4a9d191af
RndB_Enc: eda2aa1582cc7252d9bf19a330d4a9d1
RndB: 482ddc54426e6dee560413b8d95471f5
RndA: bc14dfde20074617e45a8822f06fdd91
send
90af0000207c2f74c3df09a484fc71e6e19b5ba3523a69b853cd91c6d603a1d714d8c37848
00
recv b704f5283f60a82869e9252732a9f6ae9100
RndA_Enc: b704f5283f60a82869e9252732a9f6ae
changing key #00 to 45eeb8338ae8f49a032e85bb11143530
hdr: c400
cmd: c40045eeb8338ae8f49a032e85bb1114353010
cryptogram:
45eeb8338ae8f49a032e85bb111435301095c3894b000000000000000000000000
session key: bc14dfde482ddc54f06fdd91d95471f5
```

iv: 00000000000000000000000000000000
cryptogram_enc:
c4dc9ae48dd8a8073f7f9e9159335f29d16637cf3db18f982180f0b4de5d7a86
send
90c400002100c4dc9ae48dd8a8073f7f9e9159335f29d16637cf3db18f982180f0b4de5d7a8
600
recv 9100
send 90aa0000010000
recv 189aa068a47e2f21ec81b1bc39f719d891af
RndB_Enc: 189aa068a47e2f21ec81b1bc39f719d8
RndB: 44c29525f6e679c0fea16b44d1af57e7
RndA: 3a100d71772cbf182c307691bc63d9ea
send
90af000020cbe7fc1f24ba588eb6a6562f92d0d74d9acd7af44e70e300df24a47ce37789450
0
recv 9607d533b5e018e51e33eea26f2b0a379100
RndA_Enc: 9607d533b5e018e51e33eea26f2b0a37
changing key #01 to 8db1f942f2d7cc82f6fa1486a30f8c12
session_key: 3a100d7144c29525bc63d9ead1af57e7
iv: 00000000000000000000000000000000
send
90c400002101619db367d23d64798871530300f5802ea9d55be543569934f5c47382d9075
fbe00
recv da11d391cae880d39100
session_key: 3a100d7144c29525bc63d9ead1af57e7
iv: 00000000000000000000000000000000
changing key #02 to 77611d170c449df6f294c48581ab315d
session_key: 3a100d7144c29525bc63d9ead1af57e7
iv: 00000000000000000000000000000000
send
90c40000210234dfb57fd4aa1958244b415d098f96c571e0adf96bb3a5a01cb41d605e3d32
cc00
recv 301e8cc99fe418549100
session_key: 3a100d7144c29525bc63d9ead1af57e7
iv: 00000000000000000000000000000000
session_key: 3a100d7144c29525bc63d9ead1af57e7
iv: 00000000000000000000000000000000
send 90cc0000110103102000000000ffff000000000000000000
recv 9fe32c9db79aae139100
session_key: 3a100d7144c29525bc63d9ead1af57e7
iv: 00000000000000000000000000000000
session_key: 3a100d7144c29525bc63d9ead1af57e7

iv: 00000000000000000000000000000000
send 90cc0000110203102000000000ffff0000000000000000
recv 014f0d71b8b85ceb9100
session_key: 3a100d7144c29525bc63d9ead1af57e7
iv: 00000000000000000000000000000000
done
websocket connection closed

Version #1

Erstellt: 15 Oktober 2024 10:59:56 von Mario Voigt (Stadtfabrikanten e.V.)

Zuletzt aktualisiert: 25 Februar 2025 21:22:13 von Mario Voigt (Stadtfabrikanten e.V.)