Breaking Access Controls with

BLEKey

Most access controls

suck,

so we made
a thing!

Us

Eric Evenchick

Embedded Systems Architect

Faraday Future

@ericevenchick

Mark Baseggio

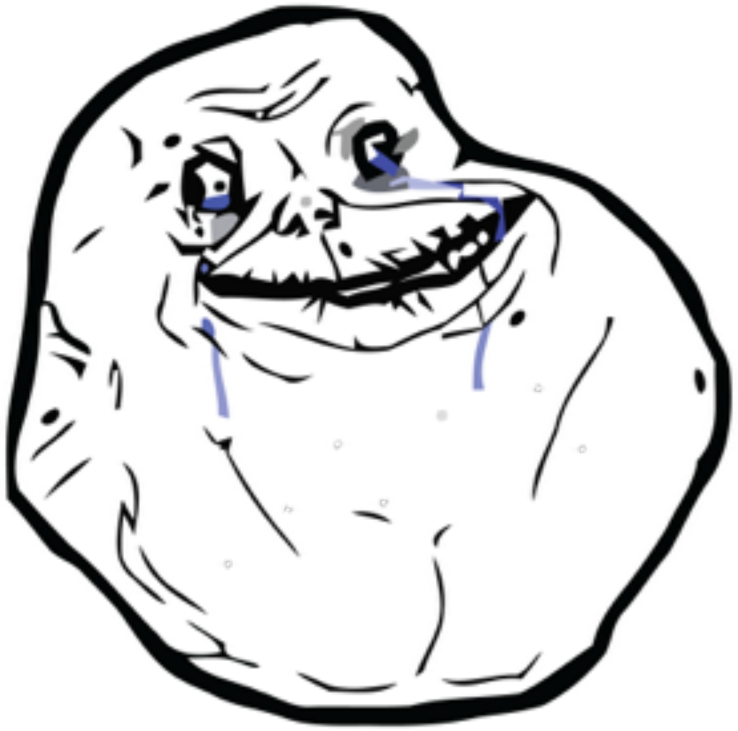
Managing Principal Consultant

Optiv

@markbaseggio

Why?

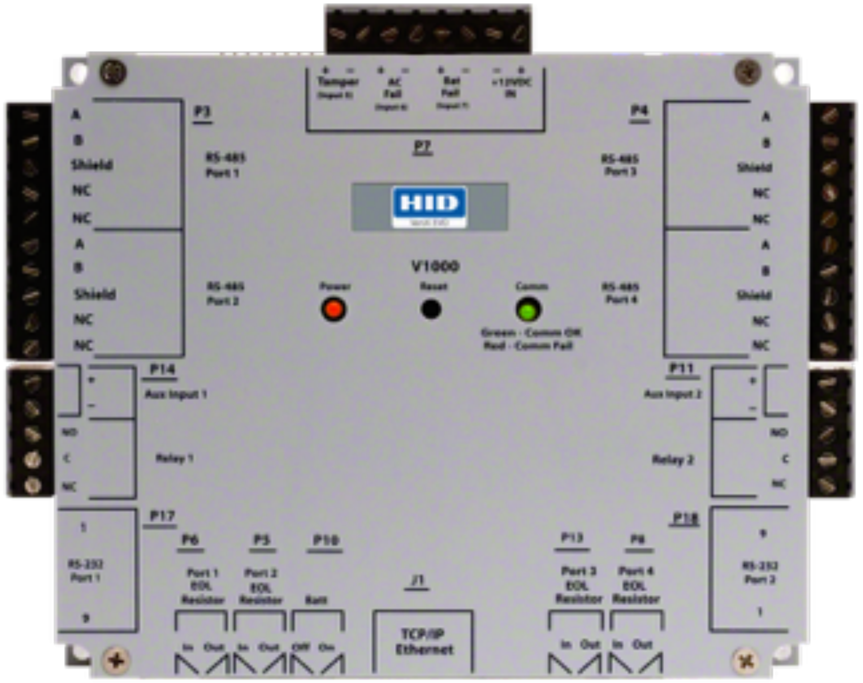
JOHNSON
CONTROLS
1 2 3
4 5 6
7 8 9
* 0 #
Cet
s'ou
you
vous

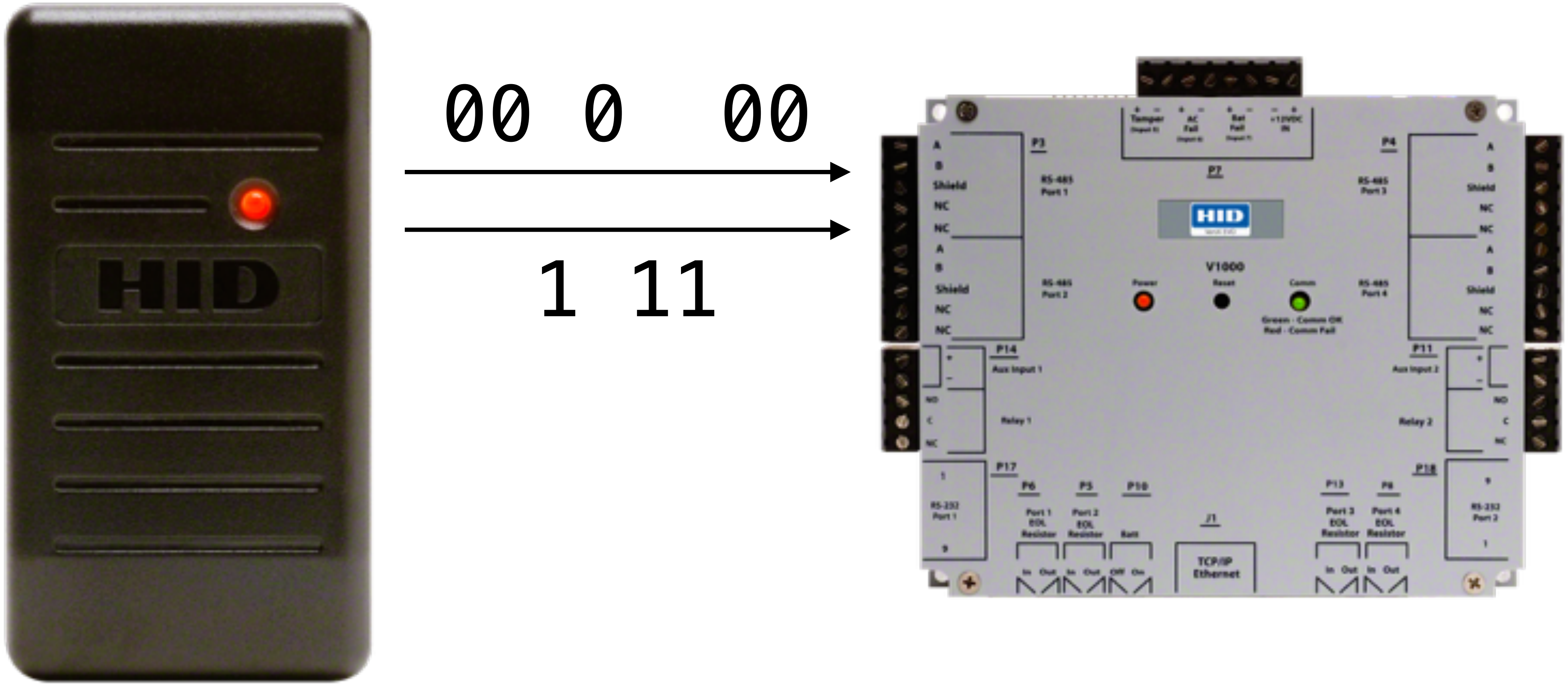


HID

HID
HID

HID

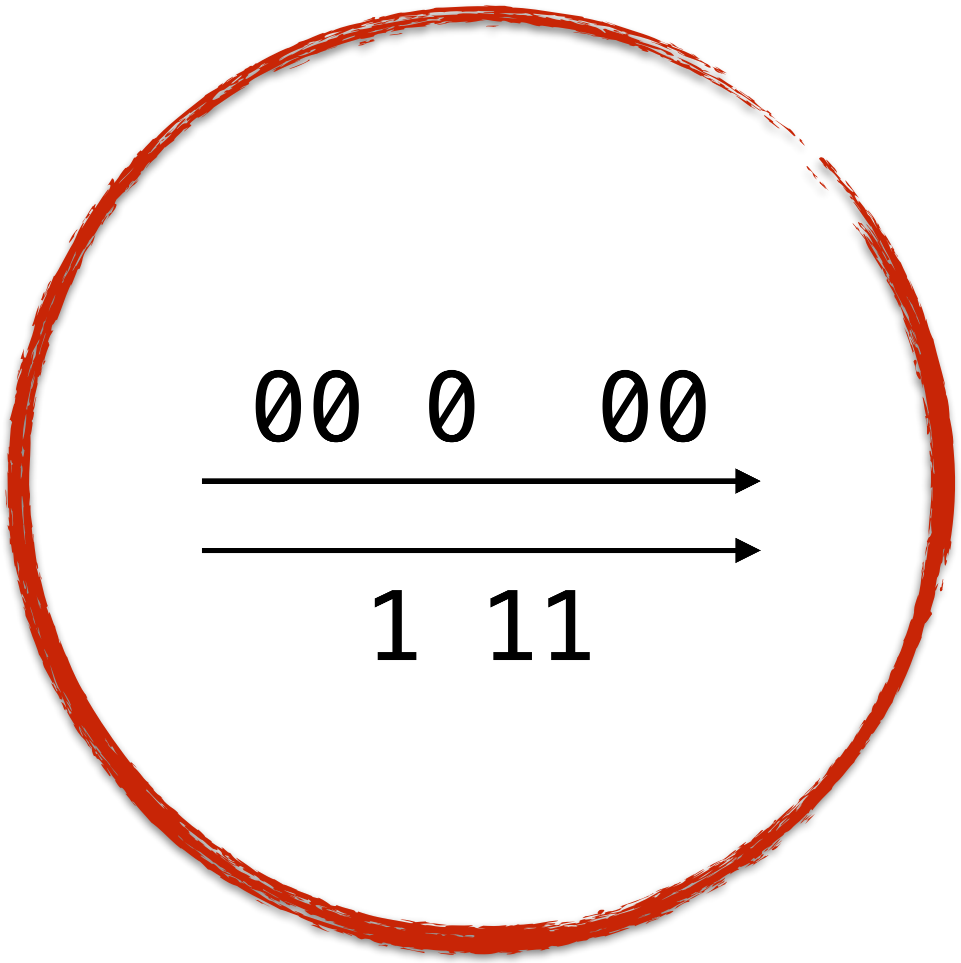

Tamper
AC Fail
Bat Fail
+12VDC IN
P7
P3
RS-485 Port 1
RS-485 Port 2
P4
RS-485 Port 3
RS-485 Port 4
A
B
Shield
NC
NC
HID
V1000
Power
Reset
Comm
Green - Comm OK
Red - Comm Fail
P14
Aux Input 1
Relay 1
NO
C
NC
P11
Aux Input 2
Relay 2
P17
RS-232 Port 1
P18
RS-232 Port 2
P6
Port 1 EOL Resistor
P5
Port 2 EOL Resistor
P10
Batt
J1
TCP/IP Ethernet
P13
Port 3 EOL Resistor
P8
Port 4 EOL Resistor
In
Out
Off
On



00 0   00

1 11

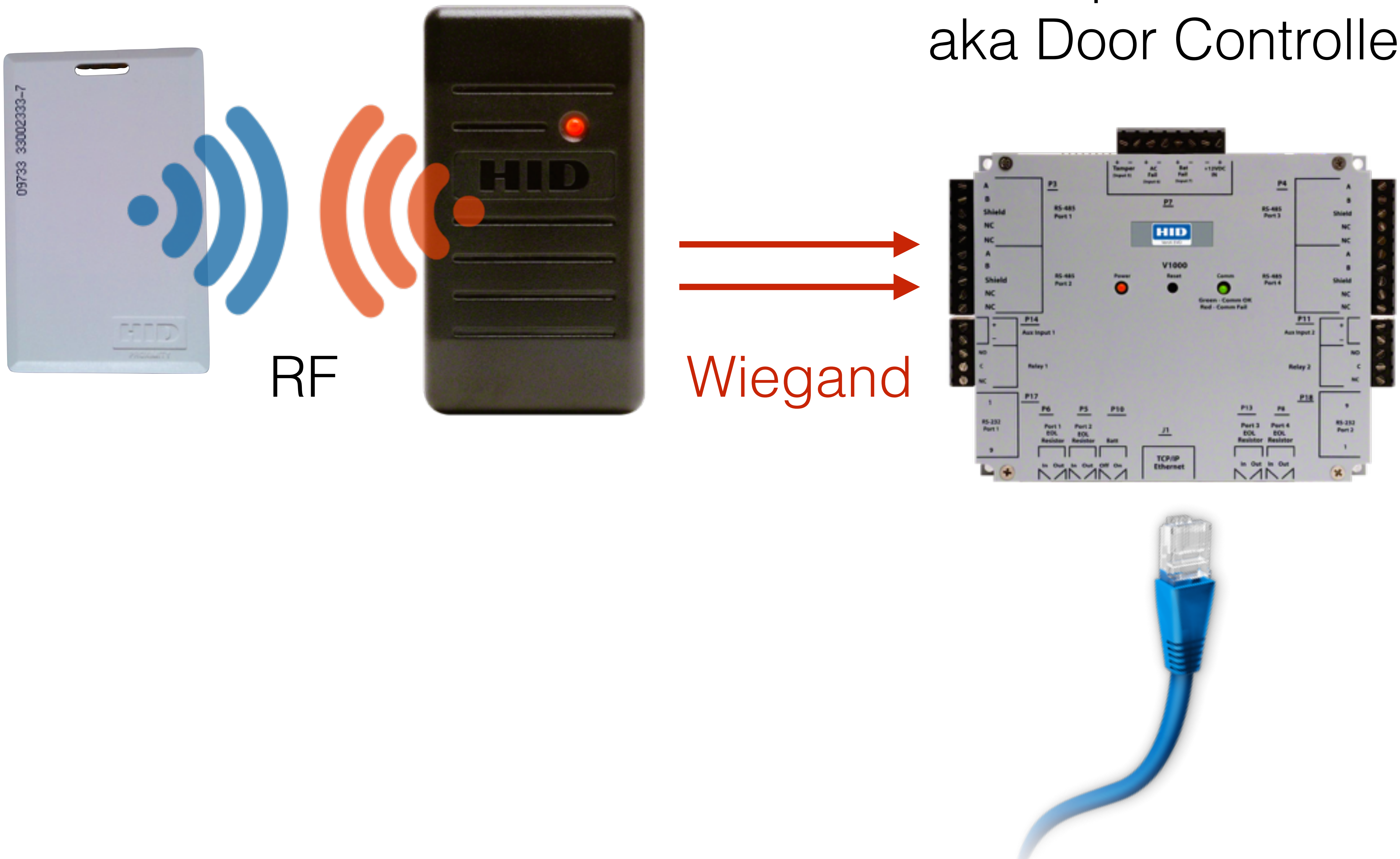
Wiegand



Card

Reader

Upstream
aka Door Controller



RF

Wiegand

HID Prox

HID iCLASS

Wow

Such enhanced security

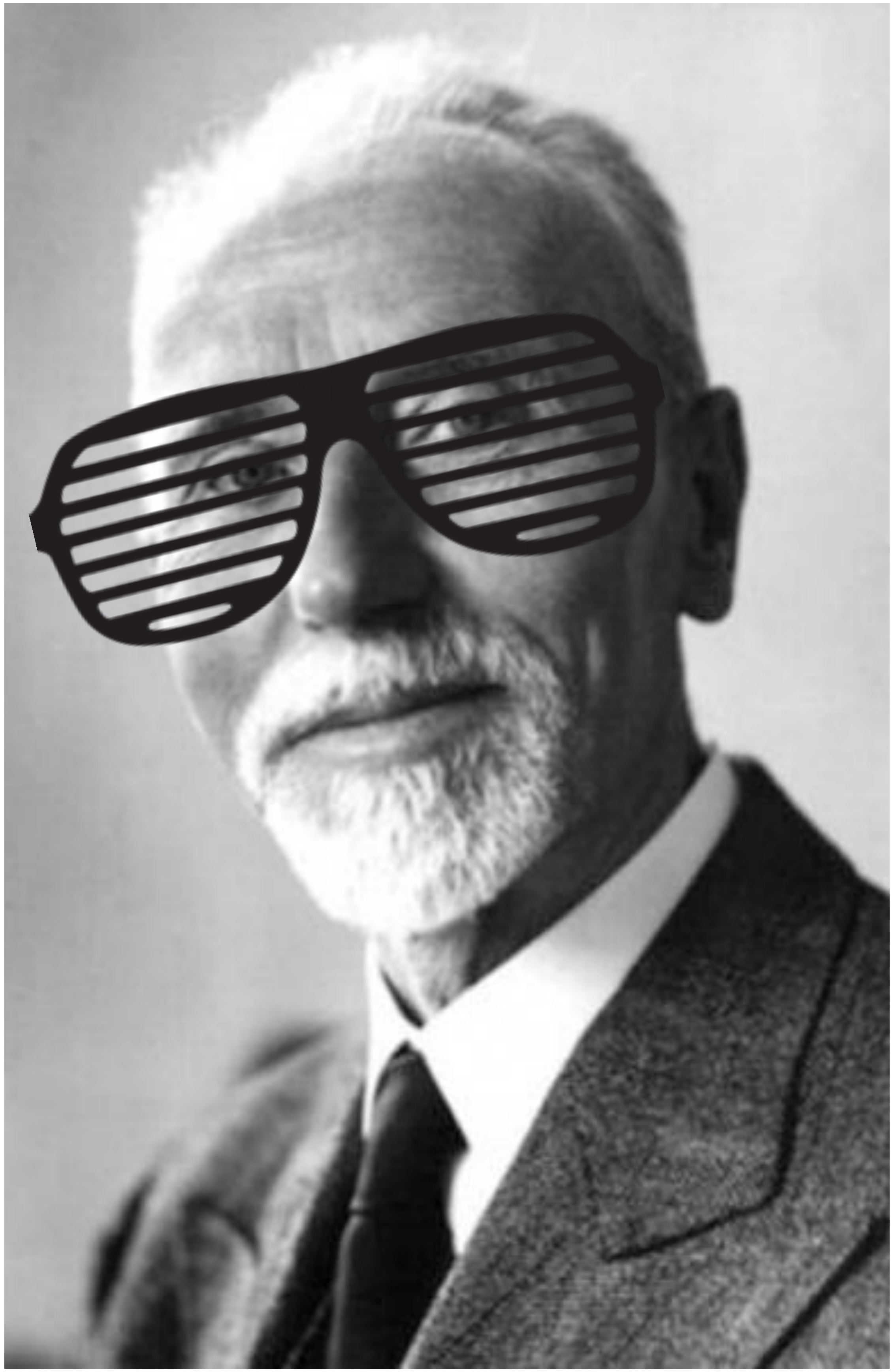
So mutual authentication

Very encryption

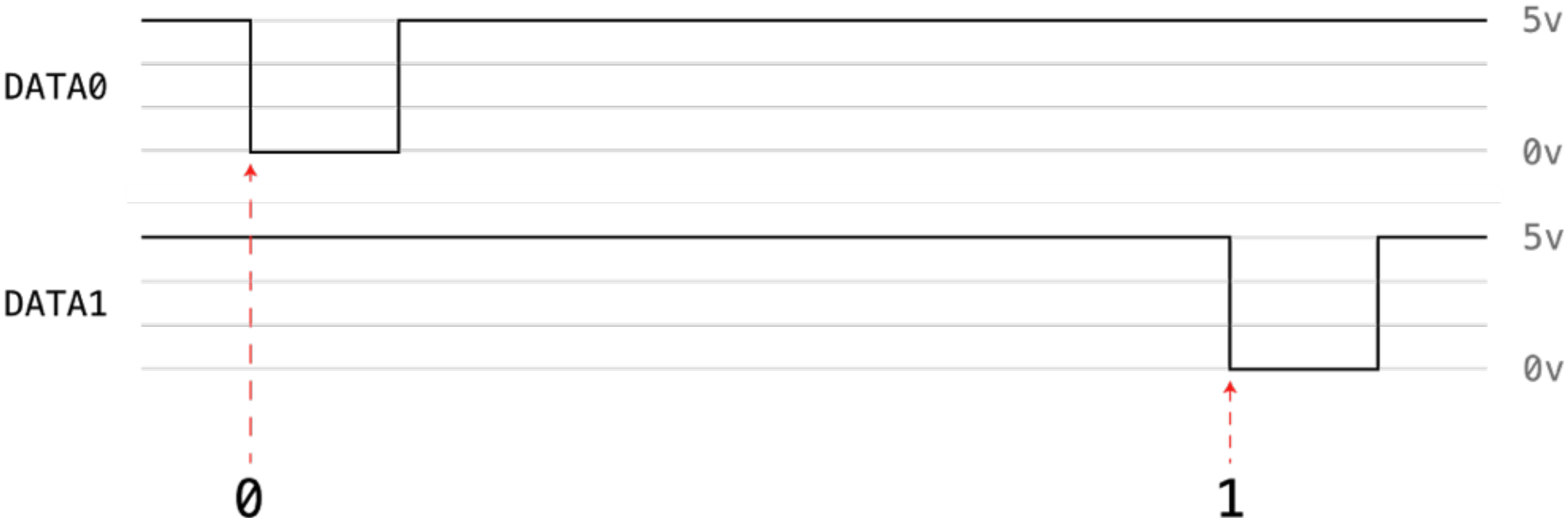
iCLASS SE

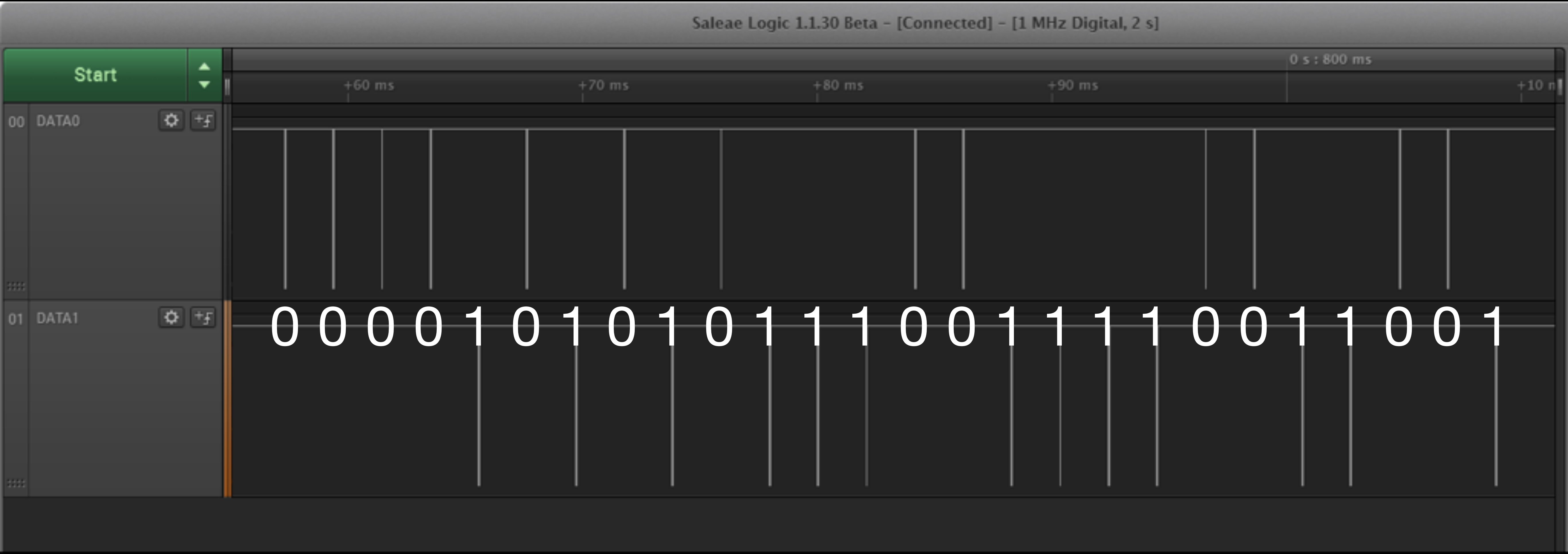
Does anyone
use one of
these readers?

Wiegand, the man, the protocol, the legacy.



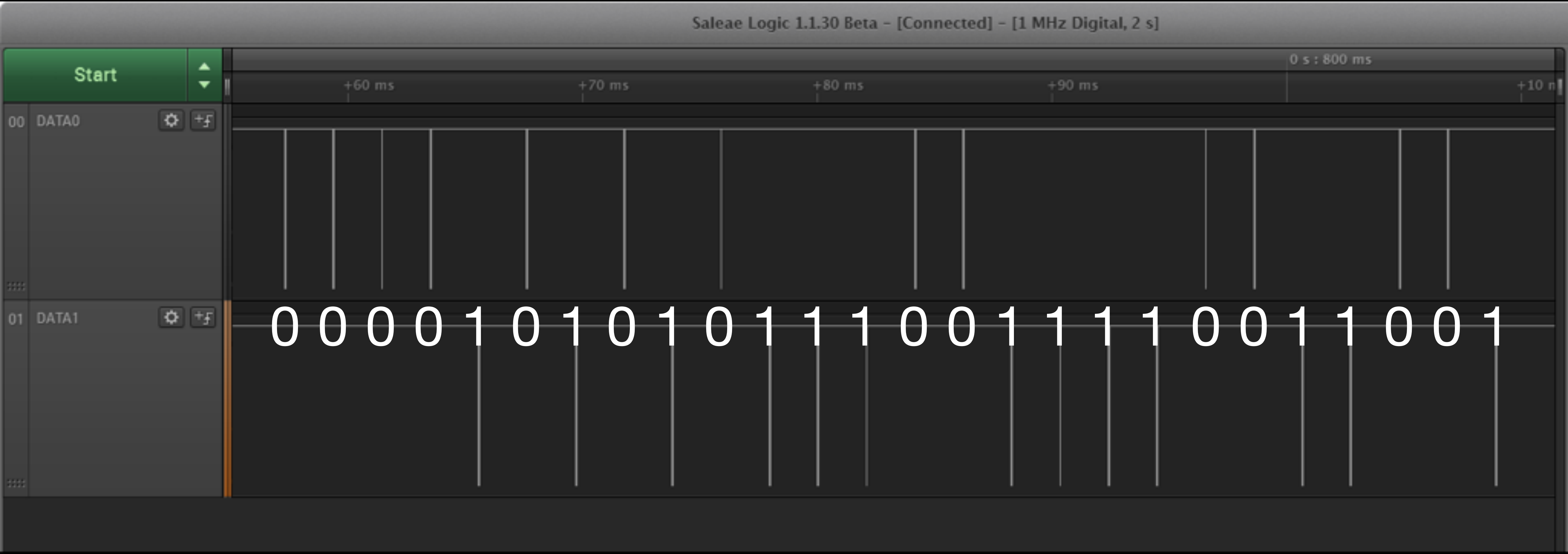
Visualizing Wiegand





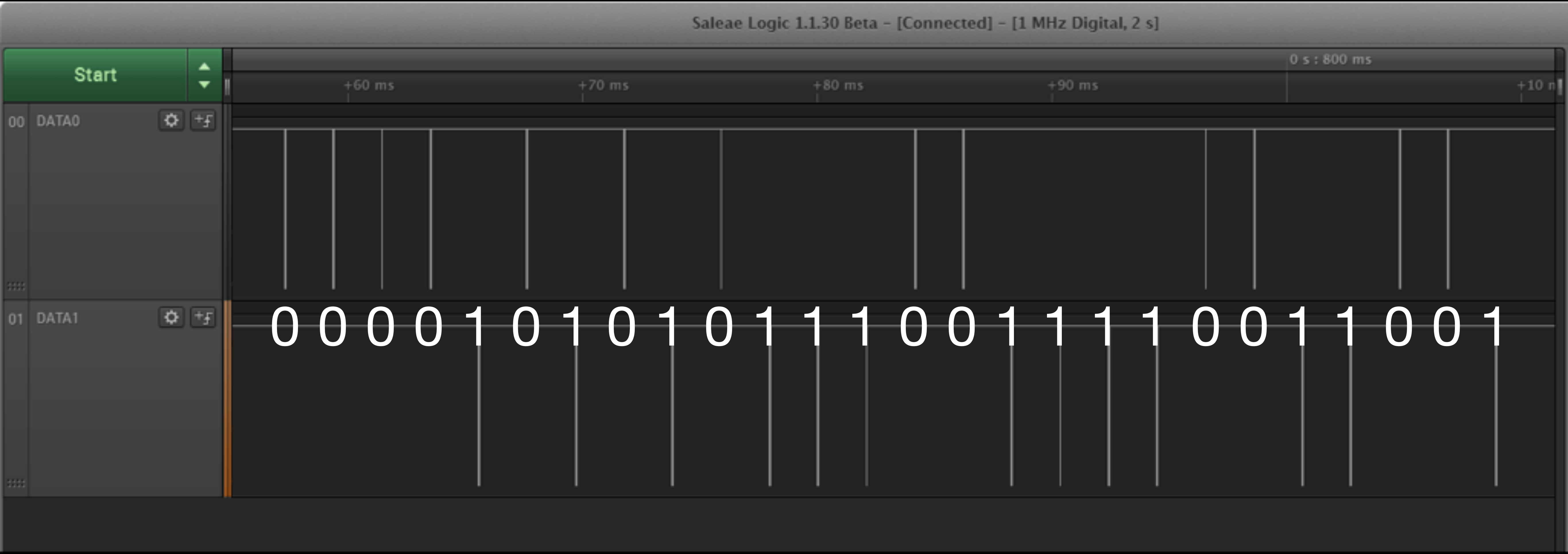
0 0 0 0 1 0 1 0 1 0 1 1 1 0 0 1 1 1 1 0 0 1 1 0 0 1

Wiegand Protocol



0 0 0 0 1 0 1 0 1 0 1 1 1 0 0 1 1 1 1 0 0 1 1 0 0 1

Facility Code = 21

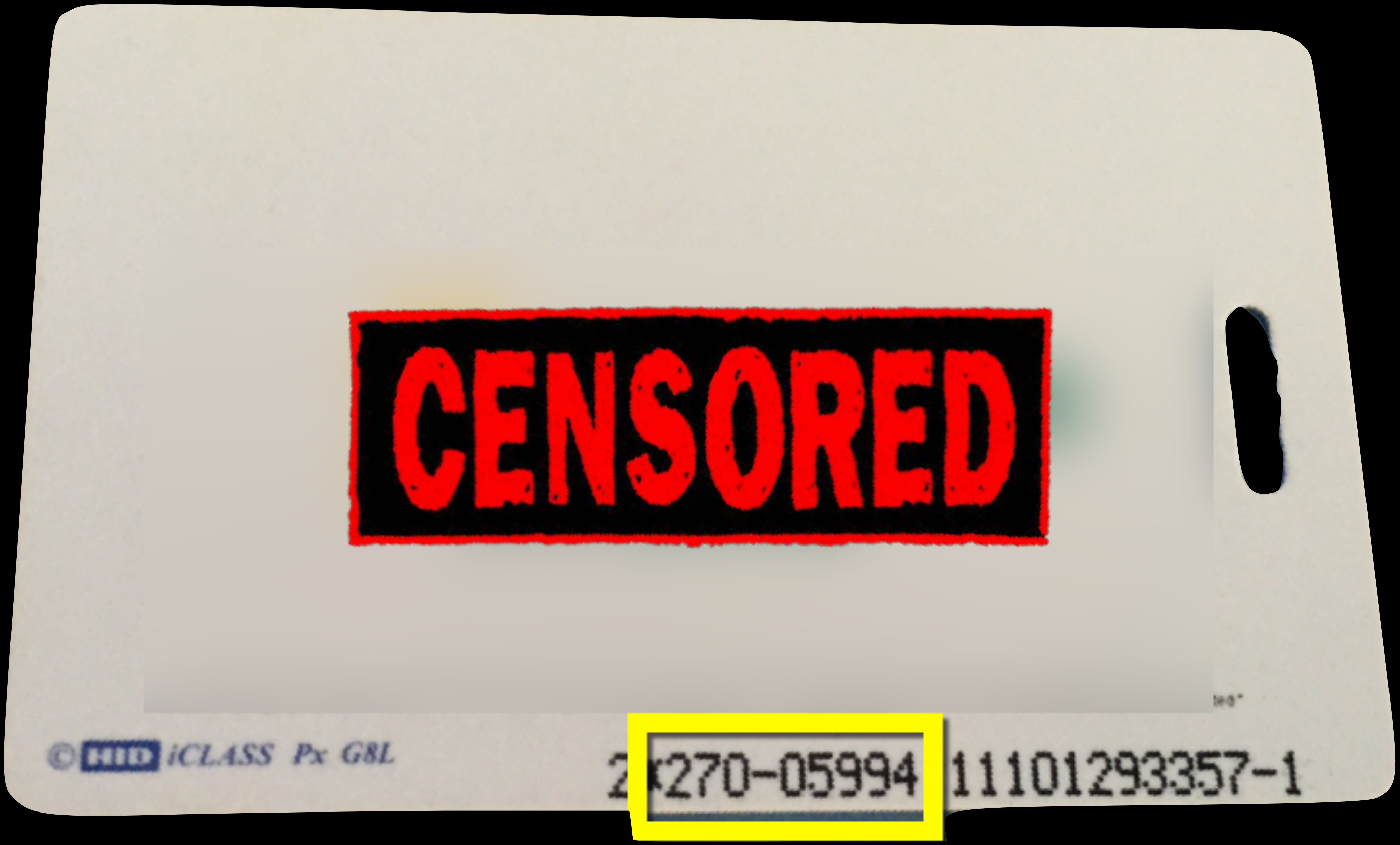

Saleae Logic 1.1.30 Beta - [Connected] - [1 MHz Digital, 2 s]
Start
0 s : 800 ms
+60 ms
+70 ms
+80 ms
+90 ms
+10 m
00
DATA0
01
DATA1

0 0 0 0 1 0 1 0 1 0 1 1 1 0 0 1 1 1 1 0 0 1 1 0 0 1

Facility Code = 21

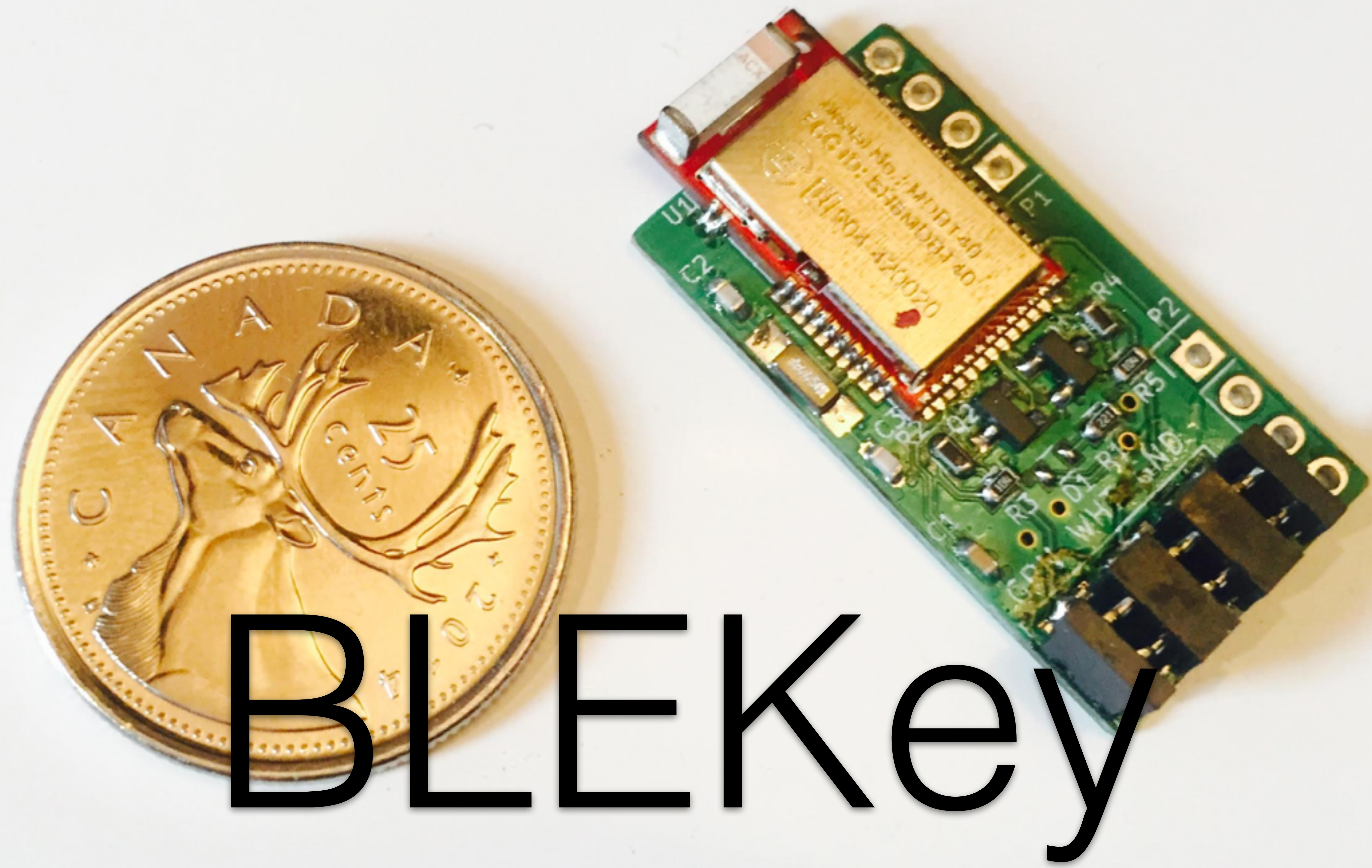
Card Code = 29644

Facepalm

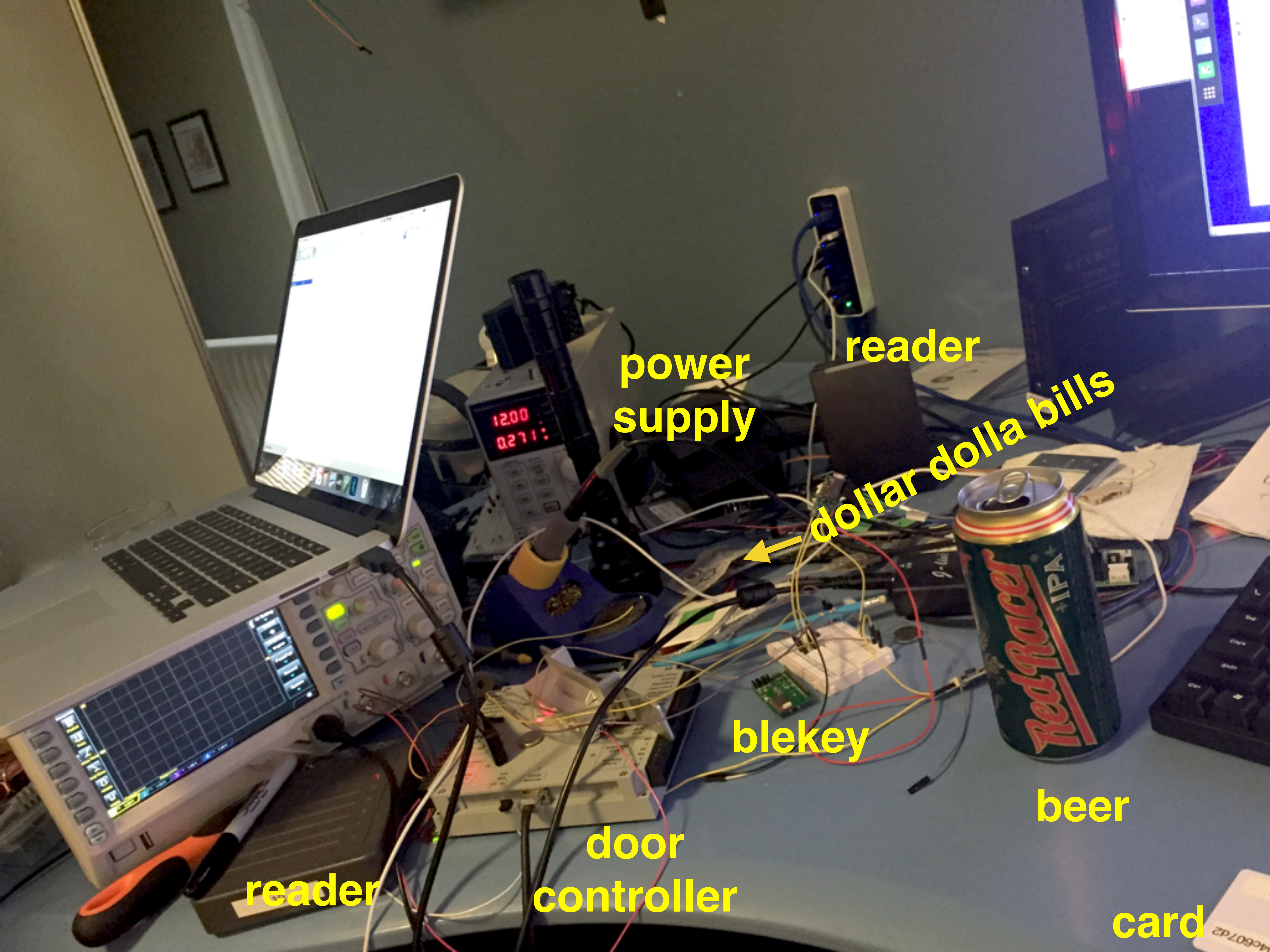


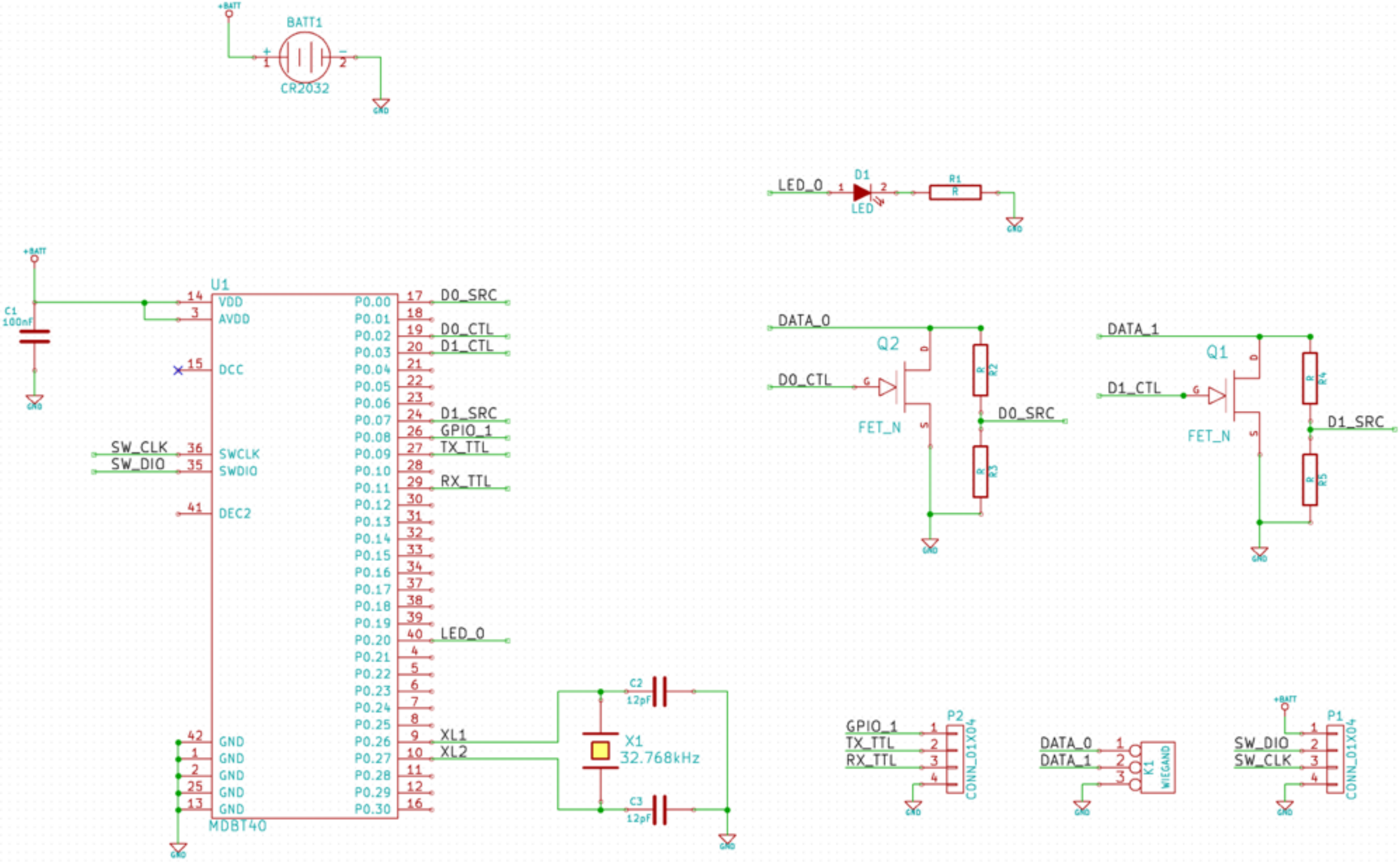
Physical Access =

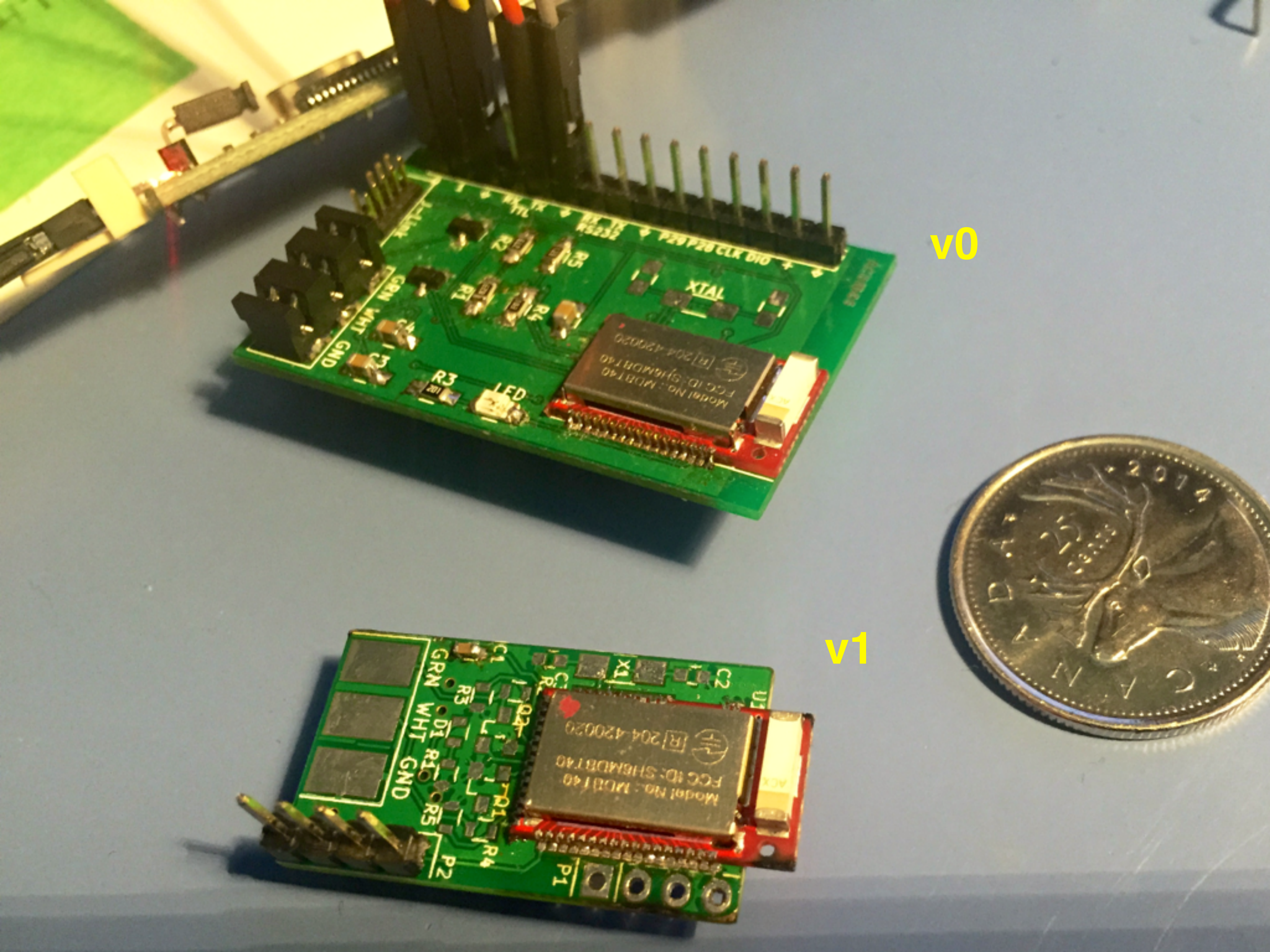
Winning



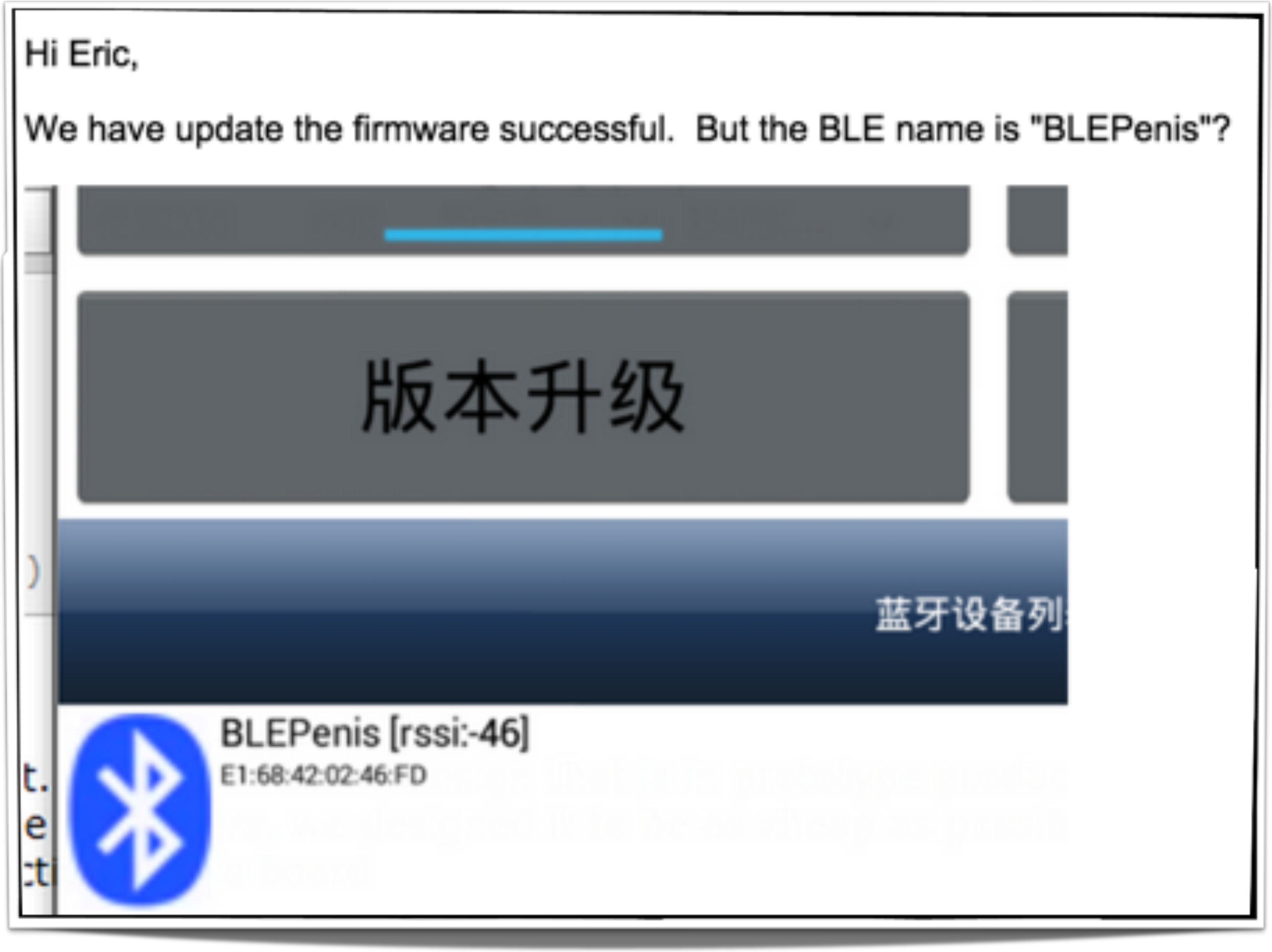
BLEKey


power supply
reader
dollar dolla bills
blekey
beer
door controller
reader
card


+BATT
BATT1
CR2032
GND
D1
LED_0
LED
R1
R
U1
MDBT40
C1
100nF
VDD
AVDD
DCC
SWCLK
SWDIO
DEC2
GND
SW_CLK
SW_DIO
P0.00 D0_SRC
P0.02 D0_CTL
P0.03 D1_CTL
P0.07 D1_SRC
P0.08 GPIO_1
P0.09 TX_TTL
P0.11 RX_TTL
P0.20 LED_0
P0.26 XL1
P0.27 XL2
X1
32.768kHz
C2
12pF
C3
12pF
DATA_0
D0_CTL
Q2
FET_N
R2
R3
D0_SRC
DATA_1
D1_CTL
Q1
R4
R5
D1_SRC
P2
CONN_01X04
GPIO_1
TX_TTL
RX_TTL
K1
WIEGAND
DATA_0
DATA_1
P1
CONN_01X04
SW_DIO
SW_CLK


v0
v1

Oops…

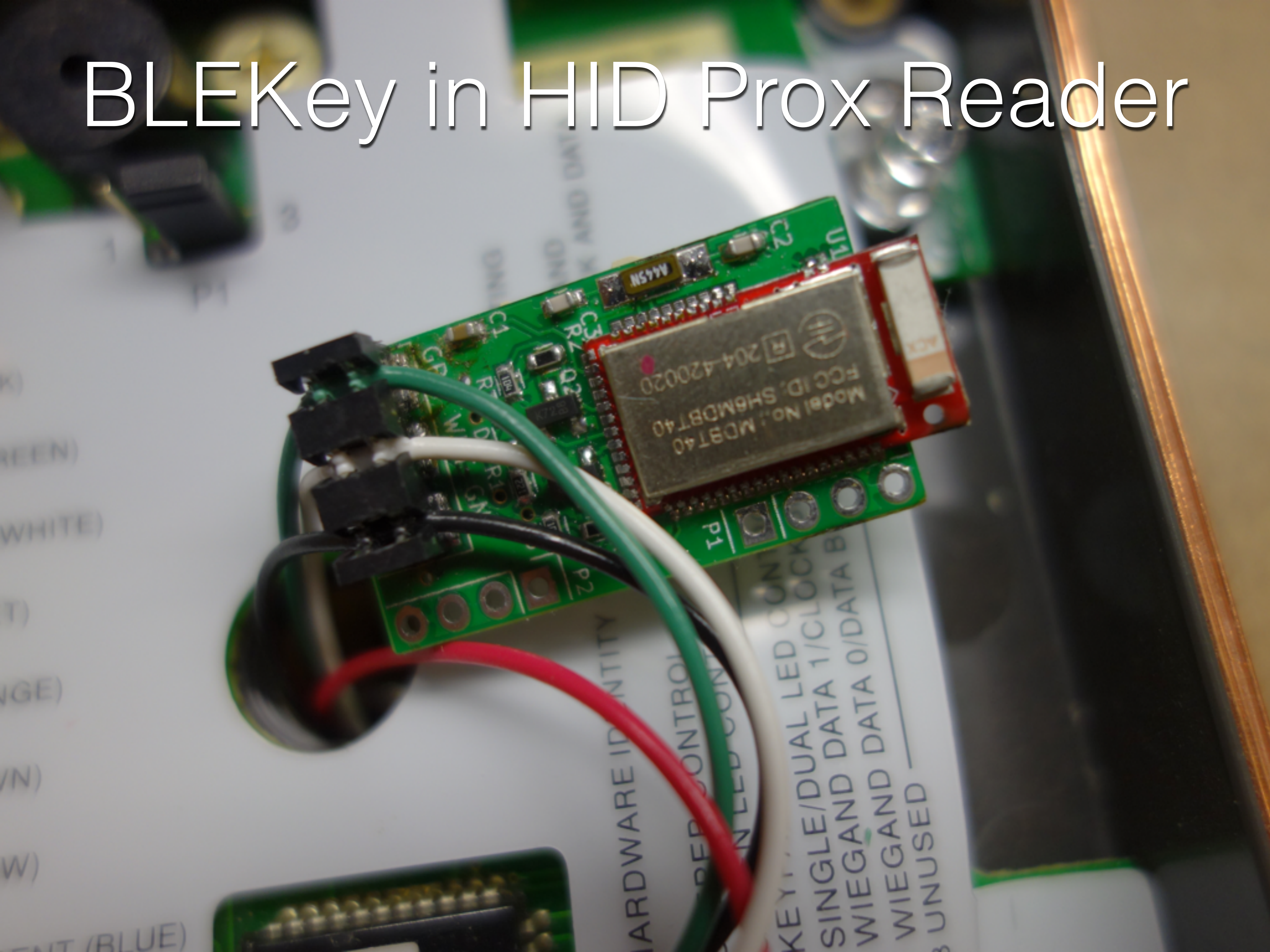


Hi Eric,

We have update the firmware successful. But the BLE name is "BLEPenis"?

BLEPenis [rssi:-46]
E1:68:42:02:46:FD

BLEKey in HID Prox Reader



The

Attacks

Record Card Data

1. Alice taps card
2. BLEKey records data
3. Eve recovers data over Bluetooth
4. Eve creates cloned card

Replay Card Data

1. Alice taps card

2. BLEKey records data

3. Eve requests replay from BLEKey

4. Door opens

Reader DoS

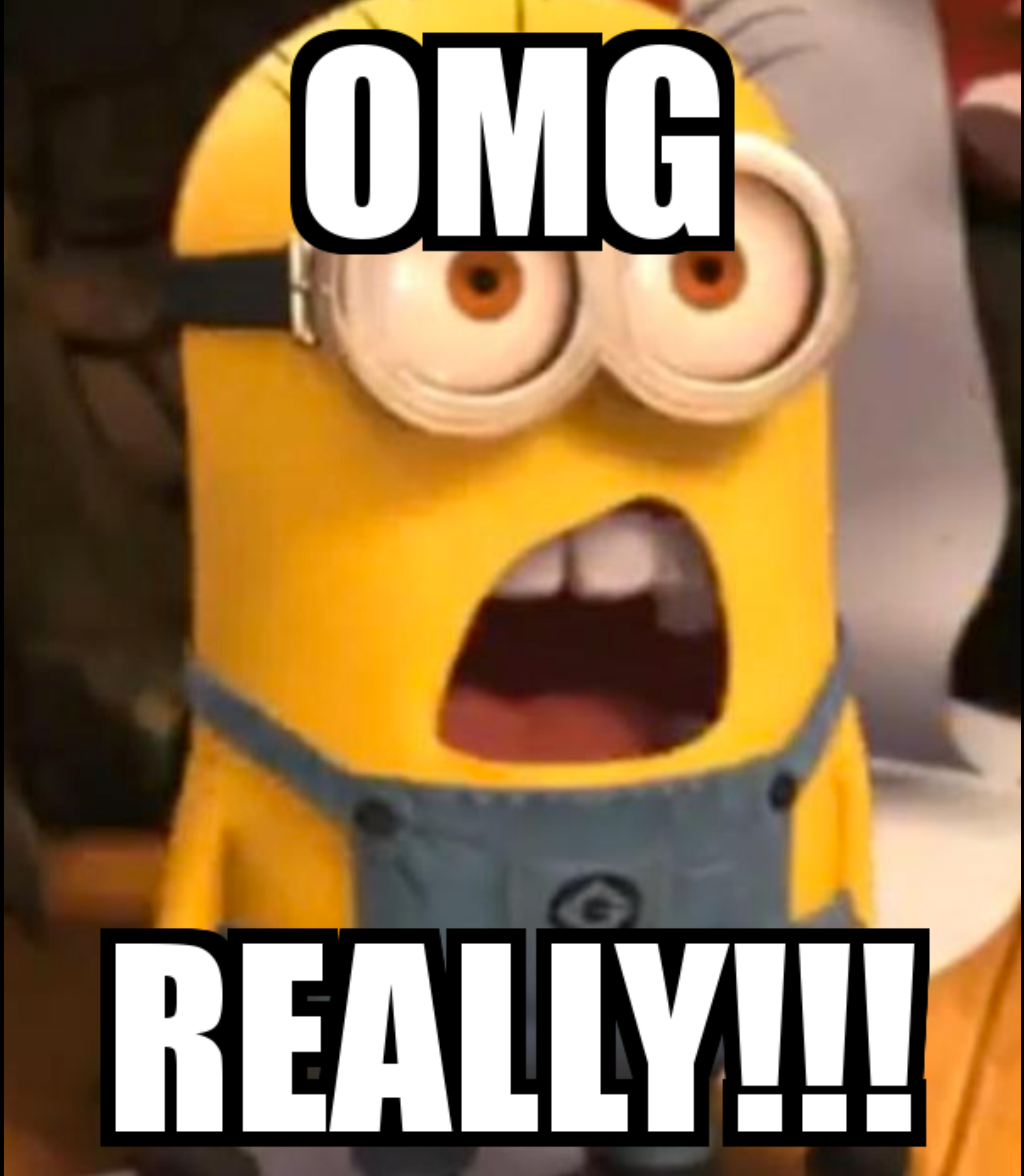
1. Eve taps control card
2. BLEKey replays Alice’s card
3. BLEKey pulls both lines low to DoS
4. Nobody can use the reader until timeout occurs

Skimmer

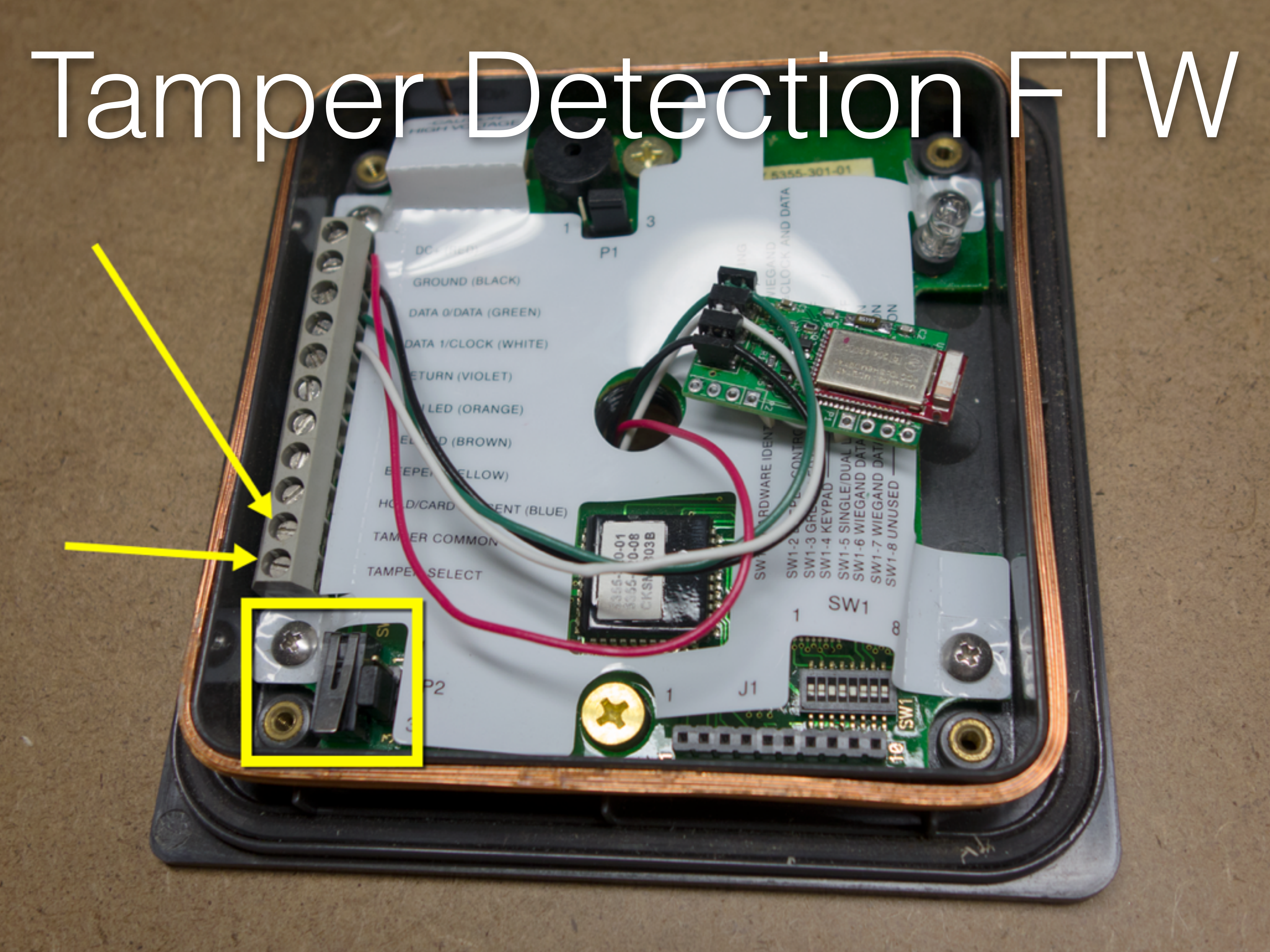
1. Eve installs BLEKey in Maxi Prox reader

2. Eve hides reader in book bag or back pack

3. Eve skims cards.


OMG
REALLY!!!

Tamper Detection FTW



Logging

Video Surveillance

In closing.

So thanks, eh?

@ericevenchick
eric@evenchick.com

@markbaseggio
mark@basegg.io