# OpenPCD & PICC

**OpenPCD & OpenPICC Project presentation**

Milosch Meriac
mailto:meriac@bitmanufaktur.de

Hard copy of presentation:
http://openpcd.org/dl/foss.in-2006.pdf

# OpenPCD Hardware

## Who is speaking to you ?

- Milosch Meriac
- hard- & software developer
- focused on deeply embedded systems
- custom-tailored embedded Linux platforms
- Linux and Windows kernel drivers
- lowlevel/realtime programming
- reverse engineering

# OpenPCD & PICC

## OpenPCD

**Open P**roximity **C**oupling **D**evice

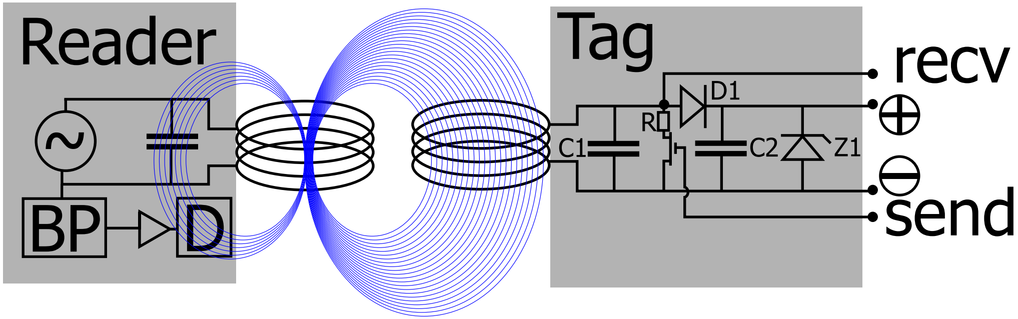
OpenPCD.org

**a free 13.56MHz RFID Reader & Writer design**

# OpenPCD Hardware

**Short introduction into tag->reader communication at 13,56MHz**

- applies to ISO14443 & ISO 15693
- can be compared with an air coupled transformer: inductive coupling



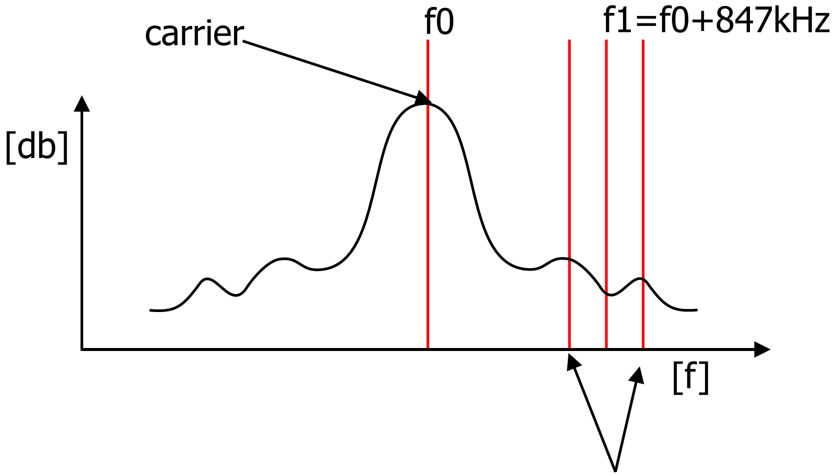
# OpenPCD Hardware

**Short introduction into tag->reader communication @13,56MHz**

- reader transmits a 13,56Mhz carrier
- carrier is used as tag power supply (rectifier D1, capacitor C2 & Zener diode Z1)
- reader->tag by AM-modulated carrier
- tag->reader by changing the load of the carrier (like carrier AM)

## ISO14443 Frequency Spectrum

the return channel
tag->reader :



return modulation products
@f1+106kHz & f1-106kHz

# OpenPCD Hardware

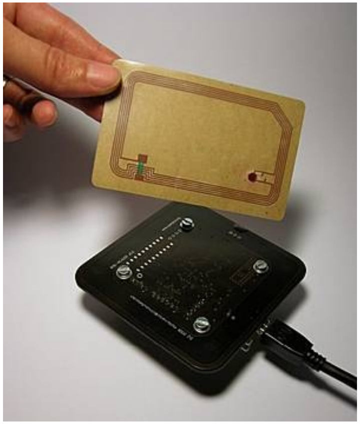
**Hardware details**

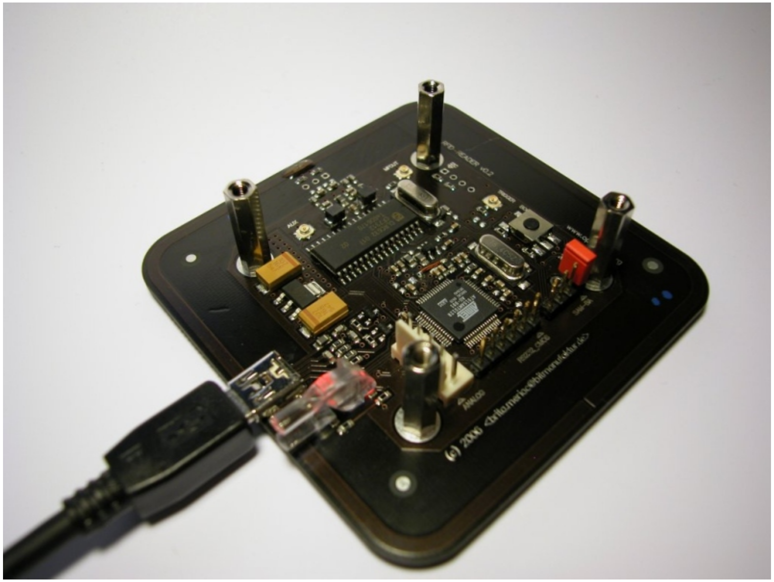
- embedded 32bit AT91SAM7x ARM CPU
- CL RC632 RFID reader IC with native ISO14443 A/B, ISO 15693 support
- native MIFARE / iCode support
- JTAG debug interface
- I2C & RS232-CMOS interface
- generic/proprietary emulation support with hardware acceleration

# OpenPCD Hardware

## How does our RFID reader look ?

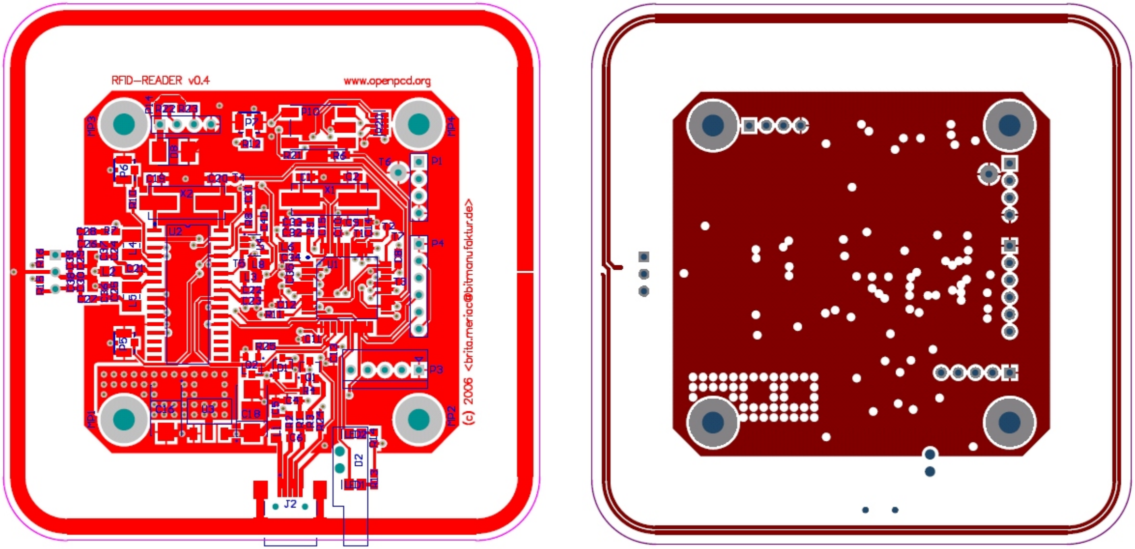
Self contained device with antenna and mini-USB interface. Mainly consists of an ARM processor and a RC632 RFID reader IC.





# OpenPCD Hardware

## Contains an embedded antenna



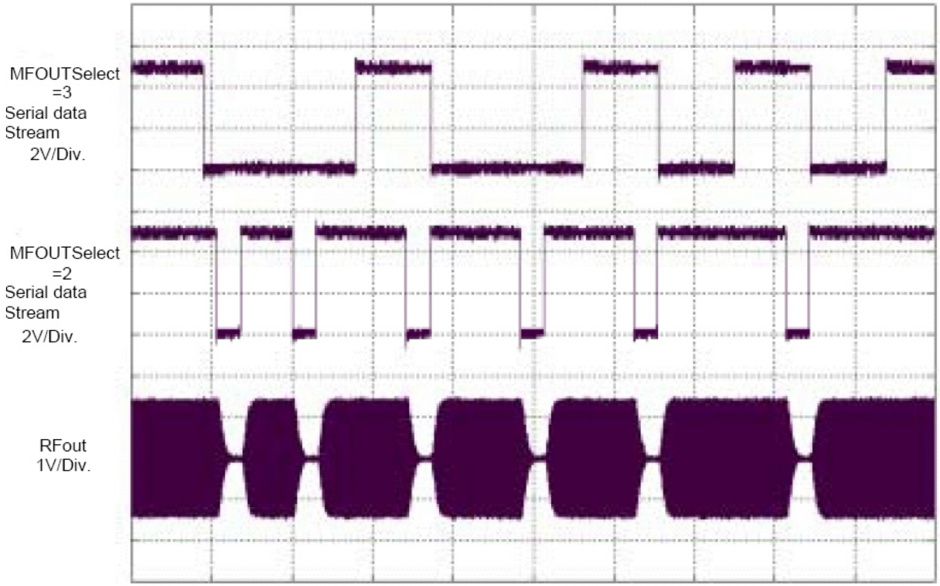
# OpenPCD Hardware

**Generic digital RFID emulation**

- MFIN/MFOUT interface of RC632 allows emulation and sniffing of proprietary 13.56MHz RFID protocols
- connected to ARM over DMA accelerated interface
- any modulation patterns possible

# OpenPCD Hardware

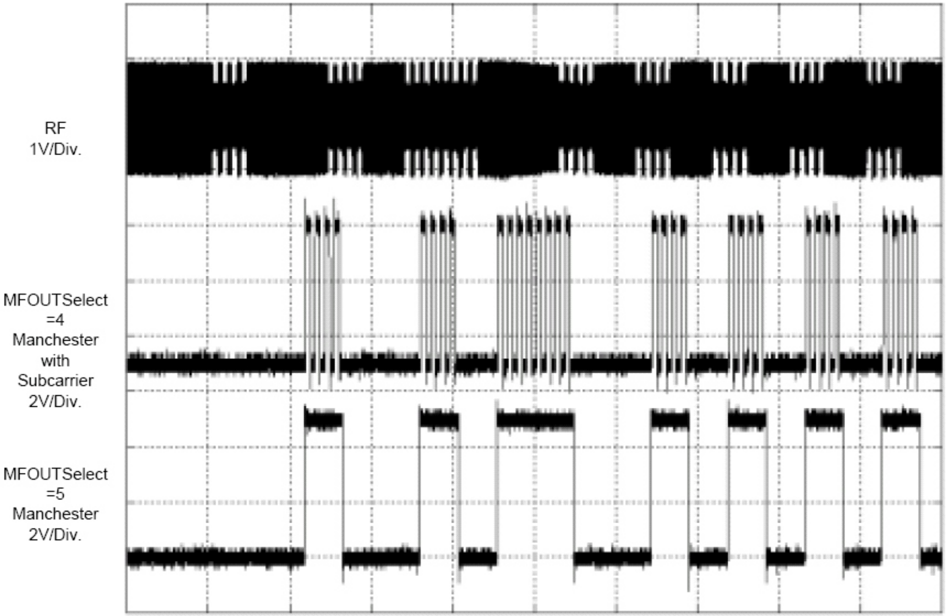
## Generic digital RFID TX interface



http://www.nxp.com/acrobat/other/identification/mc073930.pdf

# OpenPCD Hardware

## Generic digital RFID RX interface



http://www.nxp.com/acrobat/other/identification/mc073930.pdf

# OpenPCD Hardware

**Analog RFID debug interface**

- U.FL connectors for various digitally selectable demodulation steps. Analog and digital signals are brought out separately
- U.FL connector for trigger output. The idea is to let the realtime capable code decide when to trigger a connected oscilloscope on complex events

# OpenPCD Hardware

**What can it be used for ?**

- as stand-alone RFID reader for security systems. Integrated RS232-interface can be extended to RS485
- Isolate complex RFID protocol from existing (embedded) applications. Just regard OpenPCD as an RFID-to-I2C-slave gateway.
- High speed RFID card personalization

# OpenPICC Hardware

# OpenPICC

**Open P**roximity **I**ntegrated **C**ircuit **C**ard

# OpenPICC Hardware

**What the heck is OpenPICC ?**

- generic 13.56MHz RFID card emulator
- based on AT91SAM7 ARM processor
- full software emulation of every aspect of RFID data uplink / downlink
- software approach instead of FPGA/CPLD hardware to get single code base and a wider developer base

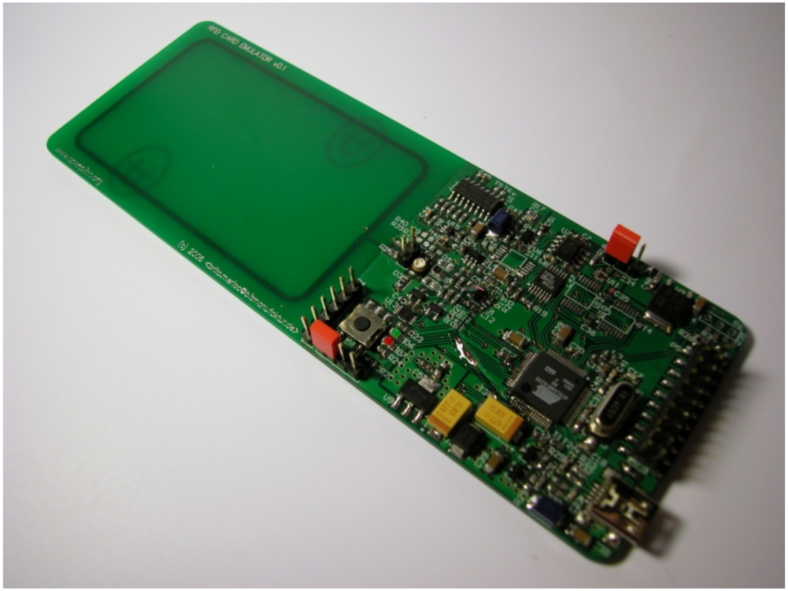
# OpenPICC Hardware

**Sophisticated hardware acceleration**

- CPU features are used to create bit-synchronous clocks to time the bit level DMA based sampling. Phase and sampling rate are freely selectable
- generic modulation patterns can be sent out sychronously
- several hardware timers as triggers

# OpenPICC Hardware

## How does current OpenPICC look ?

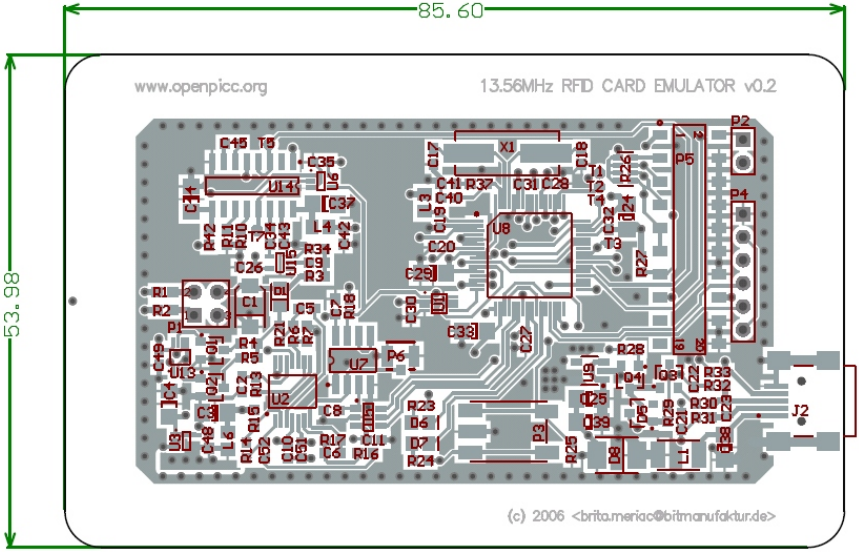


Our first prototype contains an ISO card sized PCB antenna to enable a realistic RFID card emulation.

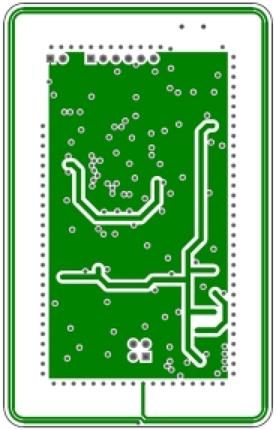
A PLL is used to maintain a virtual carrier signal during modulation pauses to ease software based demodulation.

# OpenPICC Hardware

## How will next OpenPICC look like ?


85.60
53.98
www.openpicc.org
13.56MHz RFID CARD EMULATOR v0.2
(c) 2006 <brita.meriac@bitmanufaktur.de>

The current design **is** a ISO card sized PCB antenna to enable a realistic and cool RFID card emulation.



# OpenPICC Hardware

**What can it be used for ?**

- reverse engineering and validation of readers and protocols
- Fuzzing attacks on reader firmware and software backend
- offline RFID card key cracking
- validating RFID RF interfaces
- replacement of lost RFID tags - especially during penetration tests :-)

# OpenPICC Hardware

**What do we want to achieve in near future:**

- GPL’ed toolset with tcpdump-like functionality and protocol decoding
- **full ISO1443 & ISO15693 emulation software implementation**
- reference implementation of a specific RFID devices like electronic passports

# OpenPICC Hardware

**Questions ?**

People who visited this presentation also visited http://openbeacon.org ;-)