```
Datenspuren Dresden 2017
https://www.datenspuren.de/2017/
https://frab.cccv.de/de/DS2017/cfp/
https://www.nxp.com/applications/solutions/internet-of-things
```

PCB Design for Crypto

Instructor: Michael Schloh von Bennewitz
Contact: http://michael.schloh.com/

Short abstract

Our degree of data control depends on cryptography among other things. While software packages like *WolfSSL, OpenSSL, TinyCrypt*, and *Mbed TLS* have flourished, hardware parts have not. The few vendors with hardware cryptography offer circuits **lacking in some way**, but we try to arrive at an optimal arrangement for a given application.

Implementing strong cryptography in hardware

Individuals' degree of data control depends on cryptography among other things. While software packages have flourished, hardware parts have not. We consider the **meager offering** by reviewing secure elements from:

- Atmel and Microchip (*lacks elliptic curves*)
- STMicroelectronics (*integrate a useless MCU*)
- Gemalto M2M (*only Java Card accessible, nonconsumer*)
- TI? (*can't find anything at all from them*)

Hands on

Development analysis If time allows, we advance to create an application using the *secure element* and monitor traffic to and from integrated circuits.

Requirements

This is a hands on workshop, so please bring a portable computer of any kind with **one or more free USB ports**. Be able to understand **German**, unless all German speakers yield to another (French, English, or Spanish) language.

Addendum

Bonus: We might have a real PCB printer, solder, and reflow machine for review. Come with **your own hardware designs** and we'll try printing them! Write pcbguy a-t encambio d-ot com for details. **Note:** This workshop does not teach hardware design and will not spend time reviewing CAD applications.

Über die Datenspuren

Menschen hinterlassen Spuren - absichtlich und unwillkürlich. In Computersystemen hinterlassen sie ihre Daten als "Datenspuren". Diese Daten beziehen sich auf uns, folgen uns und holen uns ein. Sie sind oftmals belanglos, manchmal aber auch wichtig. Sie sind sowohl hilfreich als auch lästig. Sie erinnern sich an uns, auch wenn wir sie vergessen. Und vielleicht bleiben sie länger erhalten, als mancher sich das vorstellen mag.

Seit 2004 gibt es die Veranstaltung "Datenspuren" in Dresden.