BeID-lab

Berlin **e**lectronic **ID**entity **lab**oratory

https://sar.informatik.hu-berlin.de/BeID-lab/ Wolf.Mueller@informatik.hu-berlin.de

Wissen: Lehre

Operating Systems Principles

Kryptografie

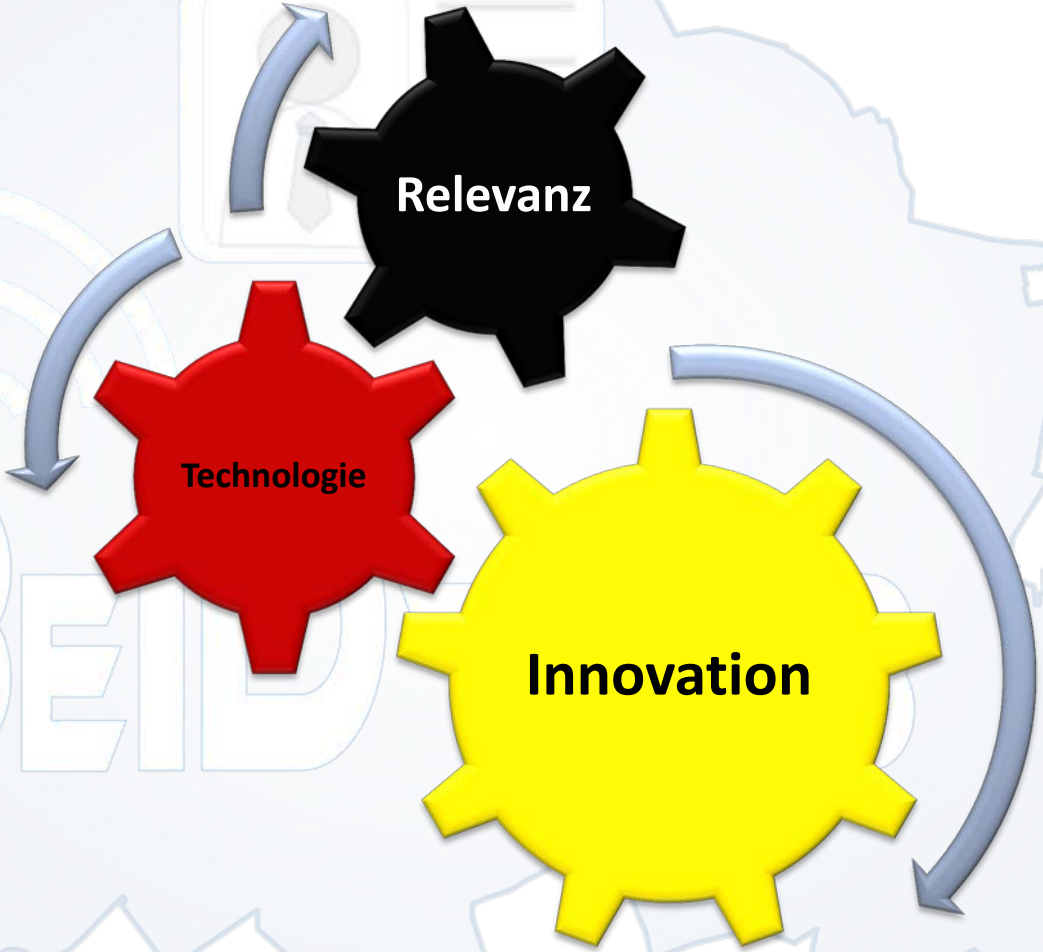
IT-Security

IT-Security Workshop

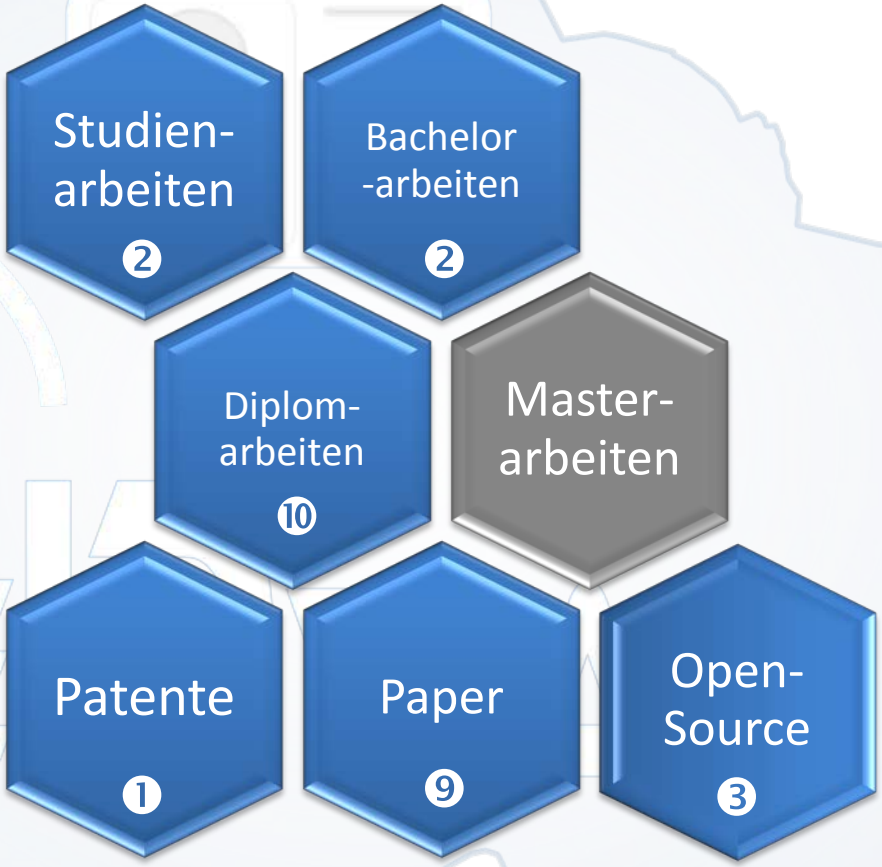
Electronic Identity

Ideen: Projekte

Praxis: Industriekontakte



= relevante Ergebnisse



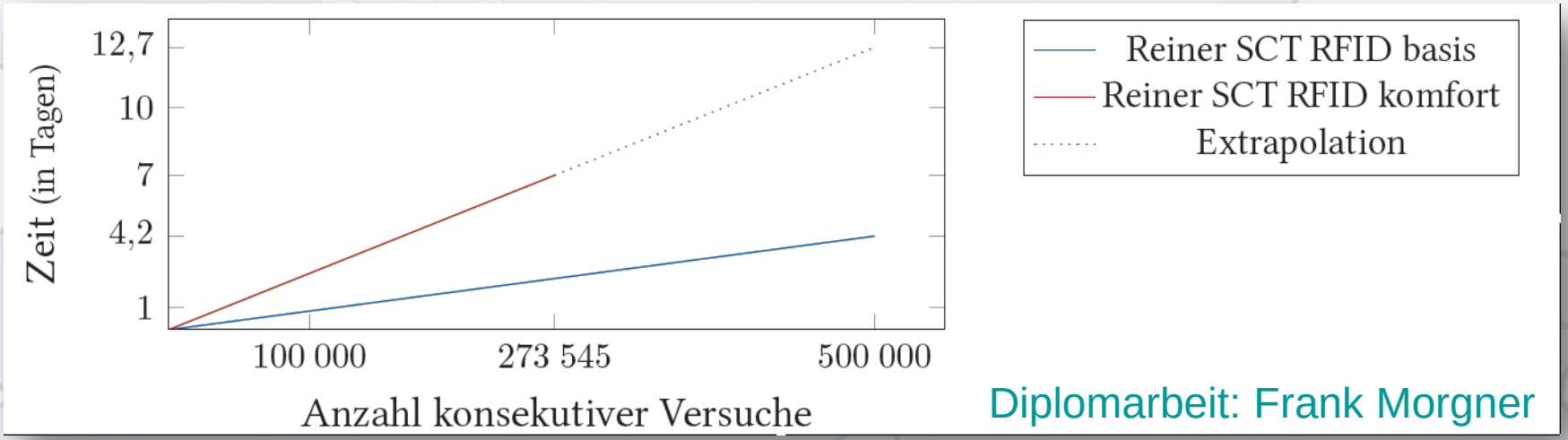
https://sar.informatik.hu-berlin.de/research/identity_management/

Konkrete Beiträge für nPA(1)

- **„zero footprint“** Leser (establishPACEChannel)

  → in nächster BSI TR-03119 (über Pseud-APDUs)

- **„brute force CAN“** in 4.2 Tagen



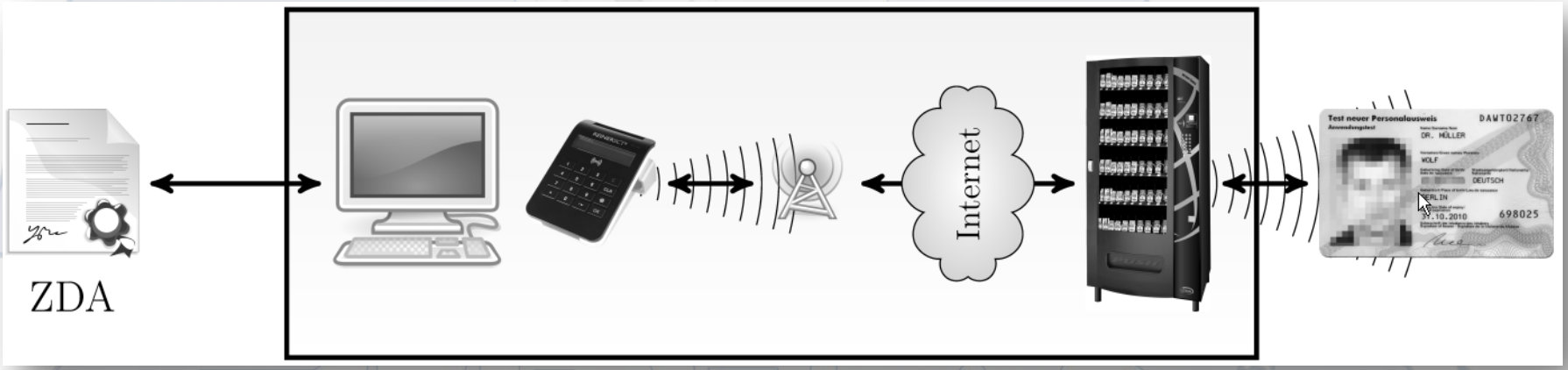
Diplomarbeit: Frank Morgner

→ BSI-TR-03116-2 (S. 18, 19)

Anforderung: >= 30 Tage

Konkrete Beiträge für nPA (2)

- **Relay-Angriff auf nPA** (eSign & Basisleser?)



→ **gehärtetes Verfahren**,

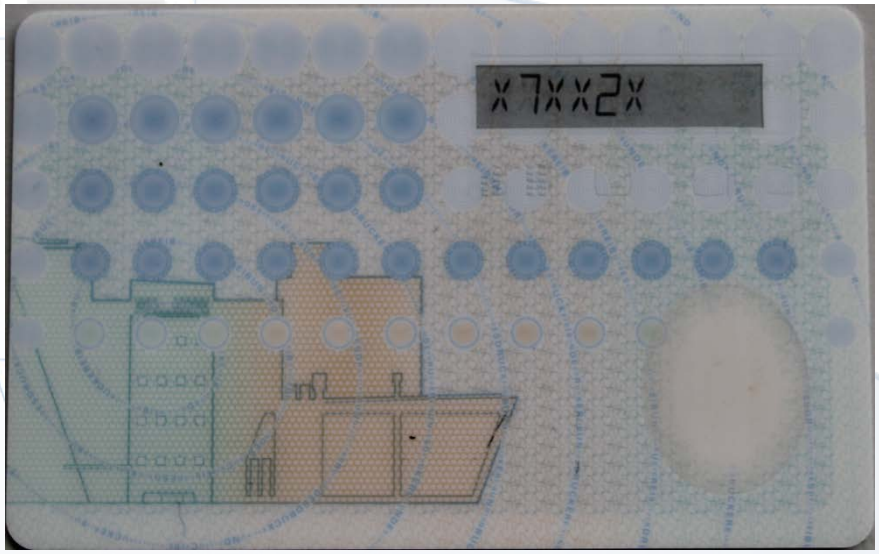
Freischaltung mit PIN-Brief

Da ist die Bundesnetzagentur, die einen **Riegel vor das medienbruchfreie Aufspielen** einer qualifizierten elektronischen Signatur (QES) gelegt hat.

(http://heise.de/-1736387)

Konkrete Beiträge für nPA(3)

- (Teil-)Dynamische PIN



Bachelorarbeit: Paul Bastian

Vorbereitungen für nPA „next generation“

IT-Security Workshop

- 17.-28. September, Projekte
- https://sarwiki.informatik.hu-berlin.de/W2012-ITS

„Studie zur Nutzung von Smartphones“

- BMI: B 3.50 - 0005/12/VV:1

eIDClientCore as **Open Source**

BUNDESDRUCKEREI

- https://sar.informatik.hu-berlin.de/BeID-lab/

New Release OpenPACE

- git://openpace.git.sourceforge.net/gitroot/openpace

Perspektive

OpenSource

- OpenPACE
- Virtual Smart Card
- eIDCC
- eSIGN
- Email Signatur / Verschlüsselung?

Konzepte

- Cat-M
- Auth2(nPA)
- Evaluierung
- Mehrkomponenten Smartcards / IDs

Quellen

https://sar.informatik.hu-berlin.de/research/publications/

- ***Mobiler Chipkartenleser für den neuen Personalausweis: Sicherheitsanalyse und Erweiterung des „Systems nPA“***, Frank Morgner, 161 Seiten, Diplomarbeit, 2012. [SAR-PR-2012-05]
- ***Display-Javakarte mit dynamischer eID-PIN für den neuen Personalausweis.*** Paul Bastian, Bachelorarbeit, 49 Seiten, 2011. [SAR-PR-2011-15]
- ***Mobiler Leser für den neuen Personalausweis.*** Frank Morgner, Dominik Oepen, Wolf Müller und Jens-Peter Redlich, in "Sicher in die digitale Welt von morgen: Tagungsband zum 12. Deutschen IT-Sicherheitskongress, ISBN: 978-3-922746-96-6, Herausgeber: SecuMedia, S. 227-240, 2011. [SAR-PR-2011-04]

BSI-Technischer Richtlinien:

- BSI-TR-03116, BSI-TR-03119

Presse:

- http://heise.de/-1736387, http://heise.de/-1751434
- http://www.bundesdruckerei.de/de/199-sign-me
- https://www.chipkartenleser-shop.de/shop/cert_bdr