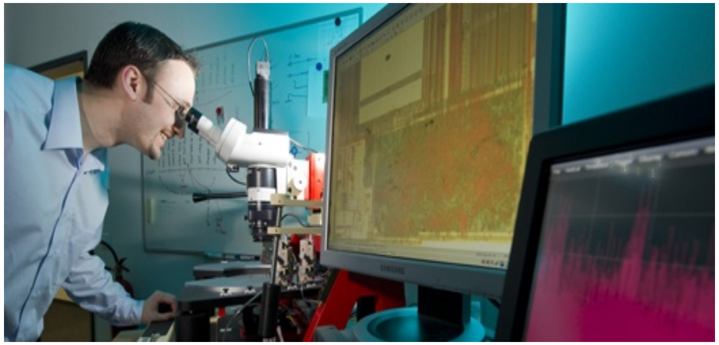
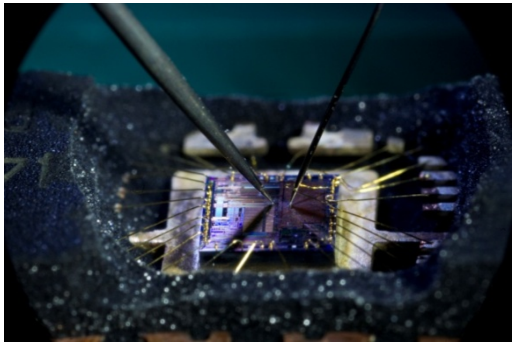
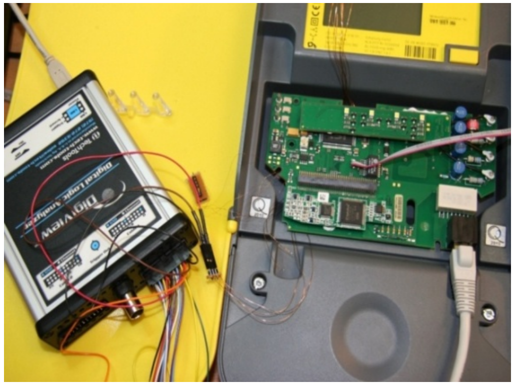
Fraunhofer
AISEC

Applied and Integrated Security







Joseph von Fraunhofer (1787 - 1826)

Researcher

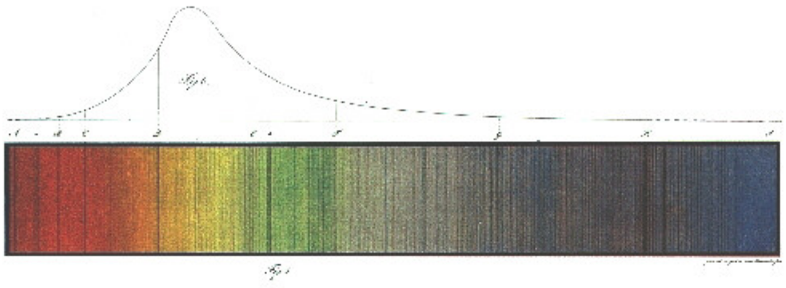
*discovery of "Fraunhofer Lines"
in the sun spectrum*

Inventor

new methods of lens processing

Entrepreneur

head of royal glass factory



Fraunhofer Profile in 2010

60 Institutes

80 research units

at approx. 40 locations

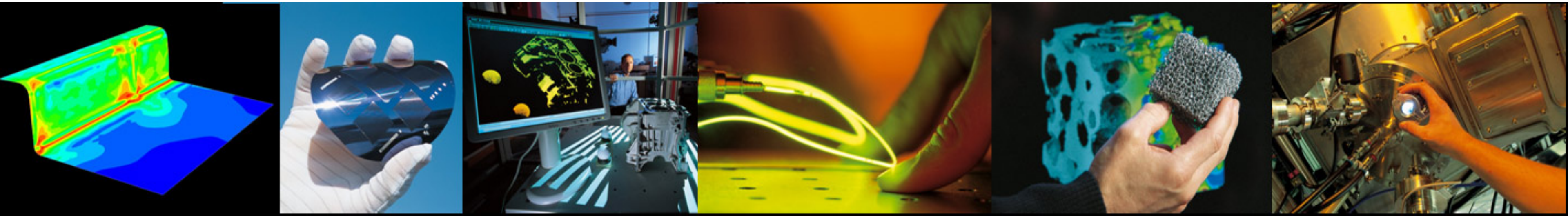
Europe, Asia, USA

17 000 employees

€ 1.7 billion
research budget

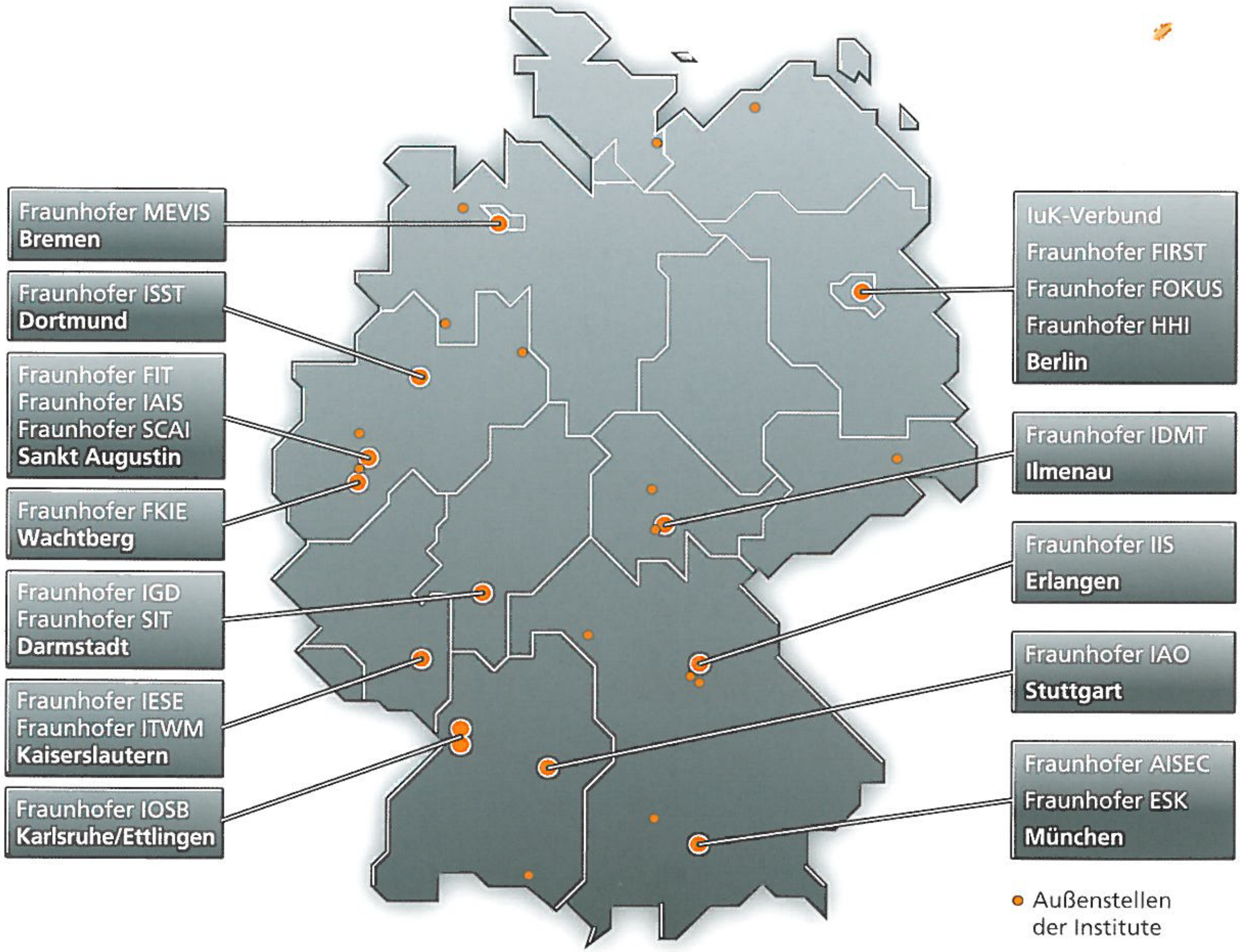
7 Alliances

- **Information and Communication Technology**
- Life Sciences
- Materials and Components
- Microelectronics
- Production
- Surface Technology and Photonics
- Defense and Security



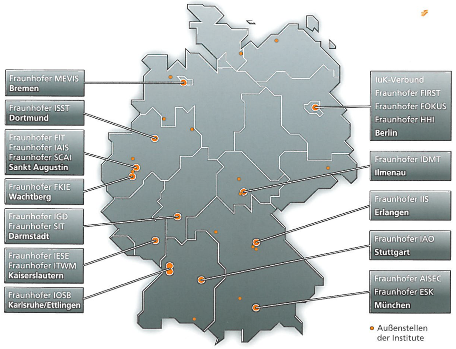
Fraunhofer Profile in 2010

Alliance: Information and Communication Technology



Fraunhofer Profile in 2010

Alliance: Information and Communication Technology



MEVIS Medical Image Computing
http://www.mevis.fraunhofer.de/

ISST Software and Systems Engineering
http://www.isst.fraunhofer.de/

FIT Applied Information Technology
http://www.fit.fraunhofer.de/

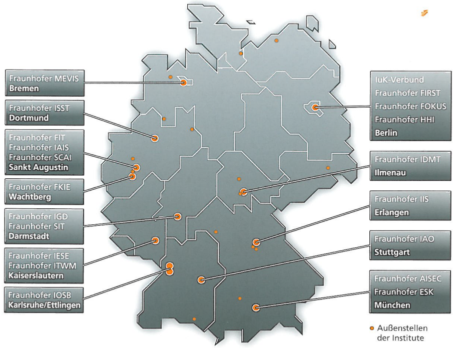
IAIS Intelligent Analysis and Information Systems
http://www.iais.fraunhofer.de/

SCAI Algorithms and Scientific Computing
http://www.scai.fraunhofer.de/

FKIE Communication, Information Processing and Ergonomics
http://www.fkie.fraunhofer.de/

IGD Computer Graphics Research
http://www.igd.fraunhofer.de/

Fraunhofer Profile in 2010
Alliance: Information and Communication Technology



SIT Secure Information Technology
http://www.sit.fraunhofer.de/

IESE Experimental Software Engineering
http://www.iese.fraunhofer.de/

ITWM Industrial Mathematics
http://www.itwm.fraunhofer.de/

IOSB Optronics, System Technologies and Image Exploitation
http://www.iosb.fraunhofer.de/

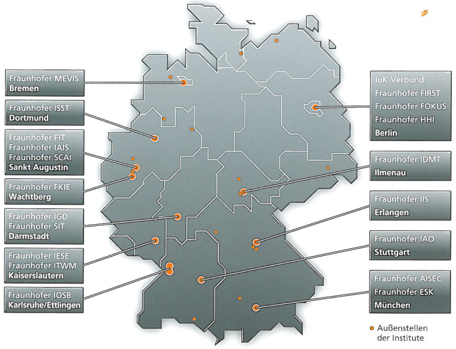
FIRST Computer Architecture and Software Technology
http://www.first.fraunhofer.de/

FOKUS Open Communication Systems
http://www.fokus.fraunhofer.de/

HHI Telecommunications, Heinrich-Hertz-Institut
http://www.hhi.fraunhofer.de/

Fraunhofer Profile in 2010

Alliance: Information and Communication Technology



IDMT Digital Media Technology
http://www.idmt.fraunhofer.de/

IIS Integrated Circuits
http://www.iis.fraunhofer.de/

IAO Industrial Engineering
http://www.iao.fraunhofer.de/

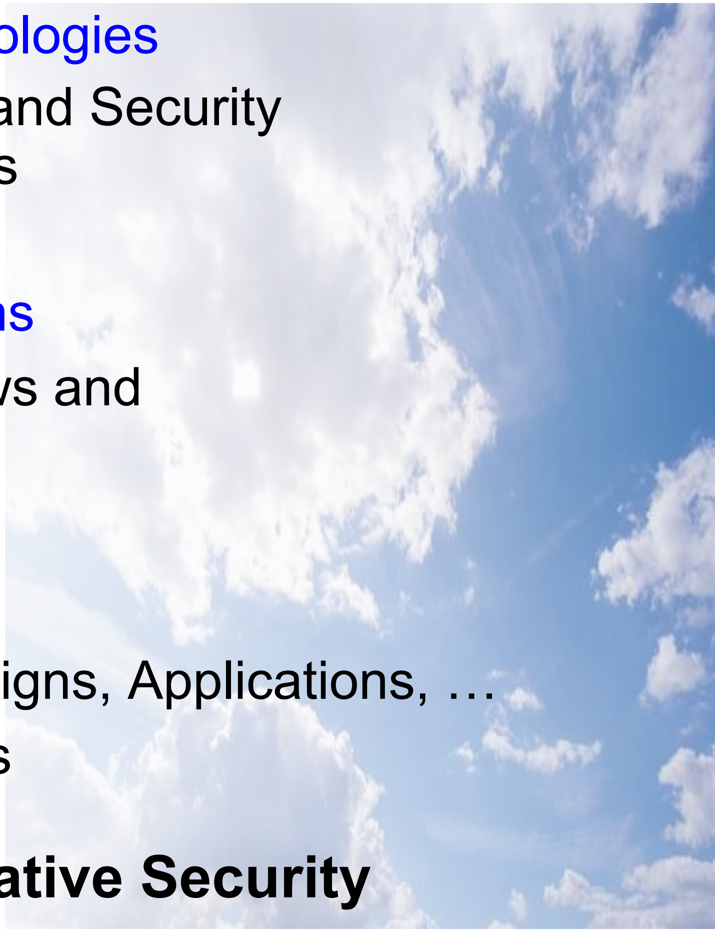
AISEC Applied and Integrated Security
http://www.aisec.fraunhofer.de/

ESK Communication Systems
http://www.esk.fraunhofer.de/

Fraunhofer AISEC Mission

Fraunhofer
AISEC

- Development of innovative Security Technologies
  - to improve Robustness, Dependability and Security of IT-based Systems and Infrastructures
- Development of innovative, new Applications
  - to improve existing (IT-based) Workflows and
  - to enable new Business Models
- Development of Test Methods and Tools
  - to improve the Quality of Products, Designs, Applications, …
  - to minimize Risks and reduce Damages



Innovation through Security & Innovative Security

AISEC Key Figures

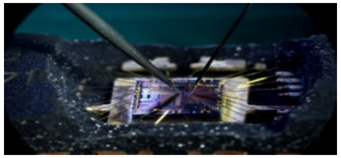
- Employees: 2011: 54 (FTEs) + > 20 research students
- 2012: > 65 (FTEs)
- 2014: > 80 (FTEs)

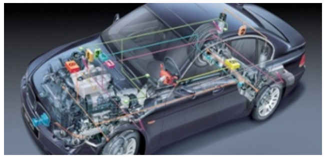
Financing (Fraunhofer Model)

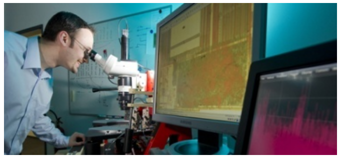
- Up to 30% state directly
- 70% 3rd party research projects

AISEC Competences

- *Embedded Security*
- *Smartcard & RFID Security*
- *Product Protection*
- *Cloud & Service Security*
- *Network Security*
- *Automotive Security*
- *IT Early Warning*
- *Smart Grid & Cyber Phys. Systems*
- *Security Evaluation*





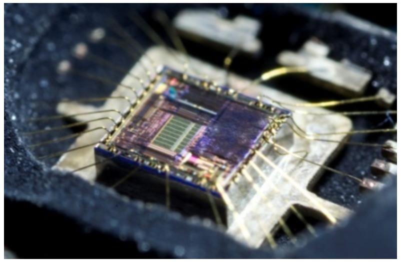


AISEC Research & Development Groups

Embedded Security, Dr. F. Stumpf

- Secure Hardware Platforms
- Mobile Phones, Smartphones etc.
- Anti-Piracy, Know-how protection

infineon



BMW
Freude am Fahren

Giesecke & Devrient

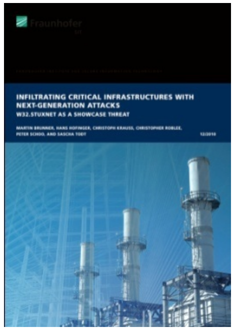
Network Security P. Schoo

- Security in IP-based networks
- Automotive Security, Car2X
- Automated Malware-detection

Deutsche Telekom

Nokia Siemens Networks

CASSIDIAN
AN EADS COMPANY


Fraunhofer SIT

INFILTRATING CRITICAL INFRASTRUCTURES WITH NEXT-GENERATION ATTACKS
W32.STUXNET AS A SHOWCASE THREAT

MARTIN BRUNNER, HANS HOFINGER, CHRISTOPH KRAUSS, CHRISTOPHER ROBLEE, PETER SCHOO, AND SASCHA TODT 12/2010

Secure Services & Quality Testing M. Hoffmann

- Secure Cloud Computing
- Identity Management
- Testframeworks for SOA, Cloud

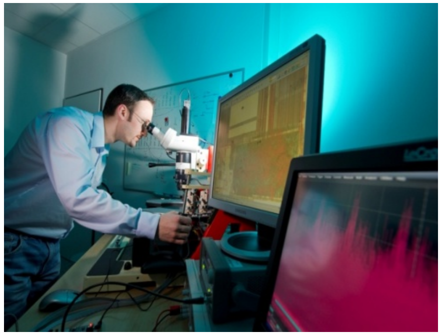
Deutsche Post

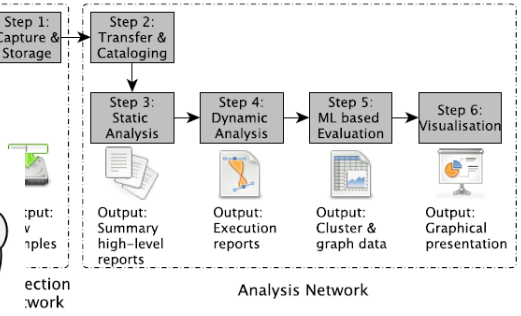
Salesforce

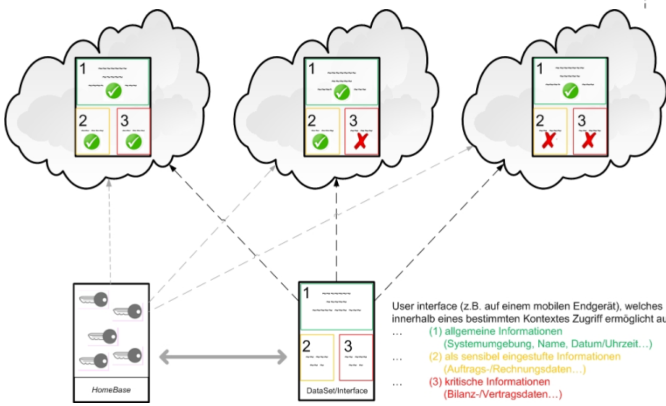
Google

AISEC Security-Labs

- **Hardware-Lab**
  - Side Channel & Fault attacks
- **Smart Meter Lab**
  - Security Analysis, Hacking
- **Mobile Payment Lab**
  - NFC-based solutions
- **Network-Lab**
  - Malware Analysis
  - Automotive Lab
- **Cloud-Lab**
  - Cloud-Cockpit




Step 1: Capture & Storage
Step 2: Transfer & Cataloging
Step 3: Static Analysis
Step 4: Dynamic Analysis
Step 5: ML based Evaluation
Step 6: Visualisation
:put: v nples
Output: Summary high-level reports
Output: Execution reports
Output: Cluster & graph data
Output: Graphical presentation
ection :work
Analysis Network



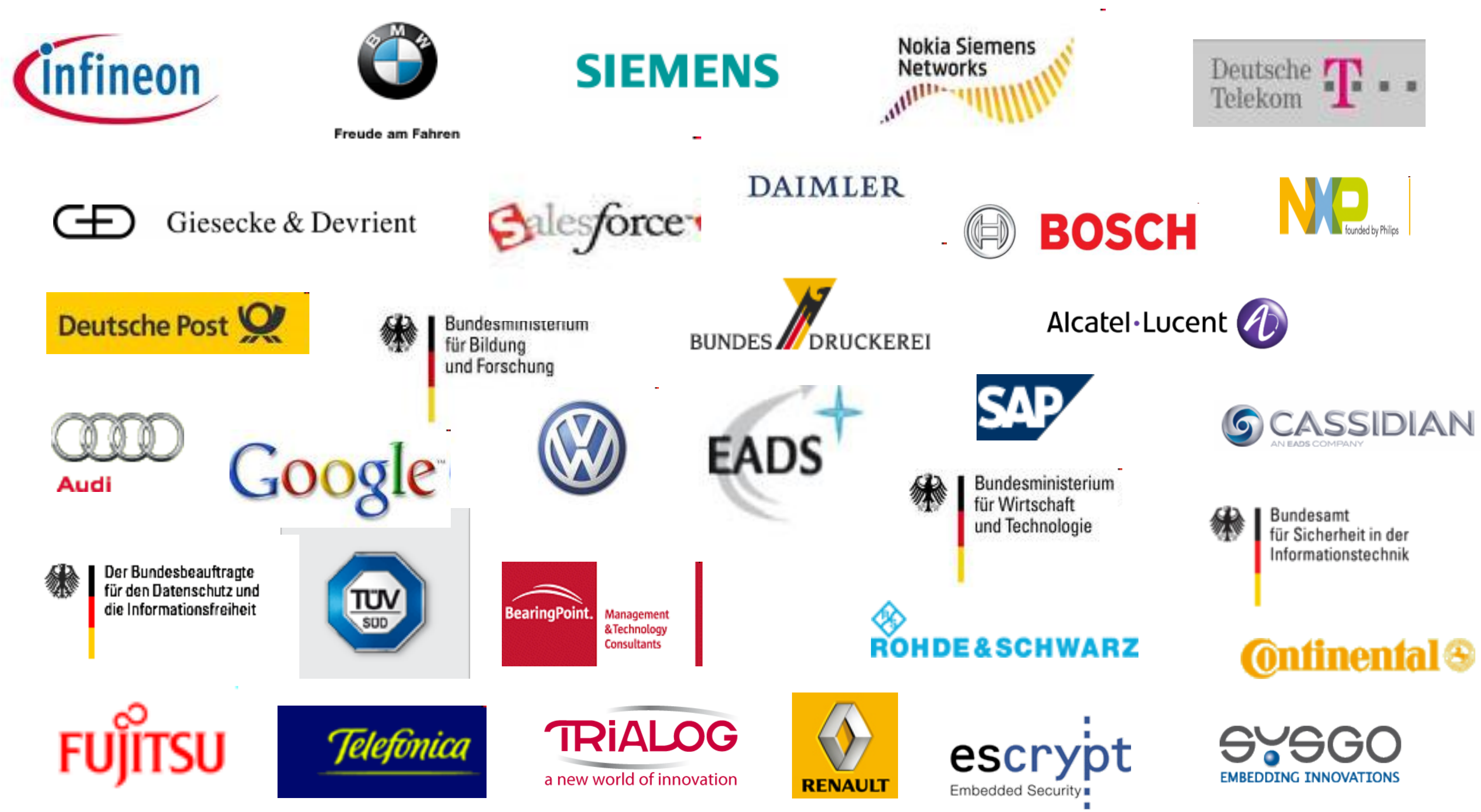
User interface (z.B. auf einem mobilen Endgerät), welches innerhalb eines bestimmten Kontextes Zugriff ermöglicht auf …

… (1) allgemeine Informationen (Systemumgebung, Name, Datum/Uhrzeit…)

… (2) als sensibel eingestufte Informationen (Auftrags-/Rechnungsdaten…)

… (3) kritische Informationen (Bilanz-/Vertragsdaten…)

Some of our Partners



Services and Offerings at a Glance

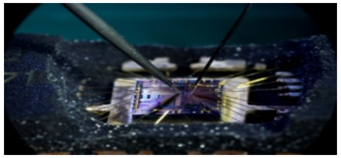
- **Studies**
  risk analyses, evaluation of technologies and concepts
- **Tests**
  vulnerability analyses, technical pre-auditing
- **Development**
  concepts, proofs-of-concepts, implementation, integration
- **Modeling**
  security concepts, optimization of infrastructures & solutions
- **Training & Consulting**
  seminars, coaching

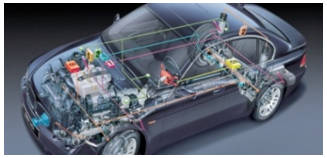
Our Strengths

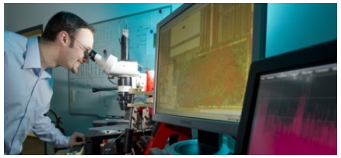
- Our labs provide ideal environment for evaluations.
  - Security Analysis and Testing
  - Interoperability Testing, conformance testing
- We have the right competences, environment and labs to
  - design prototypes demonstrating tailored solutions,
  - develop proof-of-concepts demonstrating improved solutions
- Our knowledge about all layers:
  - Hardware, Embedded,
  - Networking,
  - Services, Cloud, Processes

  allows us to provide holistic security solutions.
- We participate in leading research projects (national and EU level)

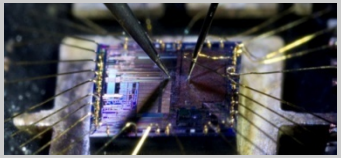
AISEC Research Labs







Embedded Security



Fraunhofer AISEC

Secure Remote Keyless Entry (RKE)

Problem:

- *Access and electronic blocking can be broken easily*

Innovative Solution:

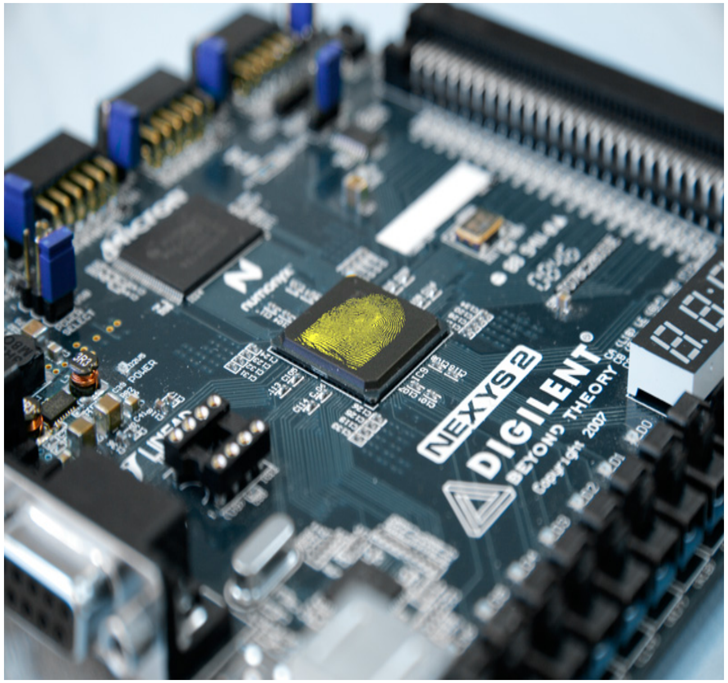
- *Elliptic Curve Cryptography strong asymmetric cryptography*
- *New efficient protocol for RKE.*

Advantage:

- *Tailored Security Solution*
- *Only public key stored in car: Easier key management and better security*

Smart Card and RFID

‘Fingerprint’ for Objects: *Unclonable Material-Based Security*



Problem

- *Secure Storage of Keys in Chips and other Components*
- *Binding of different Components*

Innovative Solution

- *Chip und Card Body build a common Physical Unclonable Function (PUF)*

Advantage

- *Physical Protection of Card and Body*
- *Invasive Attacks Destroy the Secrets*

Piracy Protection

Problem

- *Cloning of High-Tech Components*

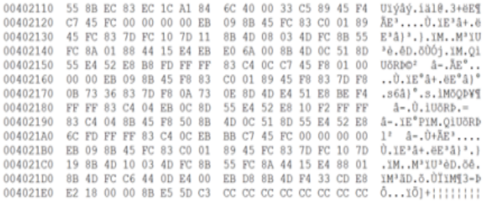
Innovative Solution

- *Secure Element as Hardware Trust Anchor*
- *Authentication between Firmware und Hardware*
- *Software Obfuscation for Firmware*

Advantage

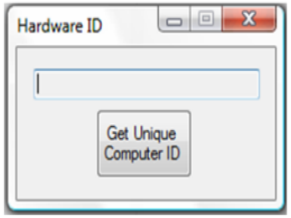
- *Verification of Original HW and SW before System Start*

+



```
00402110  55 8B EC 83 EC 1C A1 84  6C 40 00 33 C5 89 45 F4  Uìýâý.ìäl@.3+ëE¶
00402120  C7 45 FC 00 00 00 00 EB  09 8B 45 FC 83 C0 01 89  ÃE³....Ù.ïE³â+.ë
00402130  45 FC 83 7D FC 10 7D 11  8B 4D 08 03 4D FC 8B 55  E³â}³.}.ïM..M³ïU
00402140  FC 8A 01 88 44 15 E4 EB  E0 6A 00 8B 4D 0C 51 8D  ³è.êD.õÙÓj.ïM.Qì
00402150  55 E4 52 E8 B8 FD FF FF  83 C4 0C C7 45 F8 01 00  UõRÞ©²  â-.ÃE°..
00402160  00 00 EB 09 8B 45 F8 83  C0 01 89 45 F8 83 7D F8  ..Ù.ïE°â+.ëE°â}°
00402170  0B 73 36 83 7D F8 0A 73  0E 8D 4D E4 51 E8 BE F4  .s6â}°.s.ìMõQÞ¥¶
00402180  FF FF 83 C4 04 EB 0C 8D  55 E4 52 E8 10 F2 FF FF    â-.Ù.ìUõRÞ.=
00402190  83 C4 04 8B 45 F8 50 8B  4D 0C 51 8D 55 E4 52 E8  â-.ïE°PïM.QìUõRÞ
004021A0  6C FD FF FF 83 C4 0C EB  BB C7 45 FC 00 00 00 00  l²  â-.Ù+ÃE³....
004021B0  EB 09 8B 45 FC 83 C0 01  89 45 FC 83 7D FC 10 7D  Ù.ïE³â+.ëE³â}³.}
004021C0  19 8B 4D 10 03 4D FC 8B  55 FC 8A 44 15 E4 88 01  .ïM..M³ïU³èD.õê.
004021D0  8B 4D FC C6 44 0D E4 00  EB D8 8B 4D F4 33 CD E8  ïM³ãD.õ.ÙÏïM¶3-Þ
004021E0  E2 18 00 00 8B E5 5D C3  CC CC CC CC CC CC CC CC  Ô...ïÕ]+¦¦¦¦¦¦¦¦
```

+



= ✓

Cloud & Service Security

Fraunhofer AISEC

Cloud-Monitor

Problem

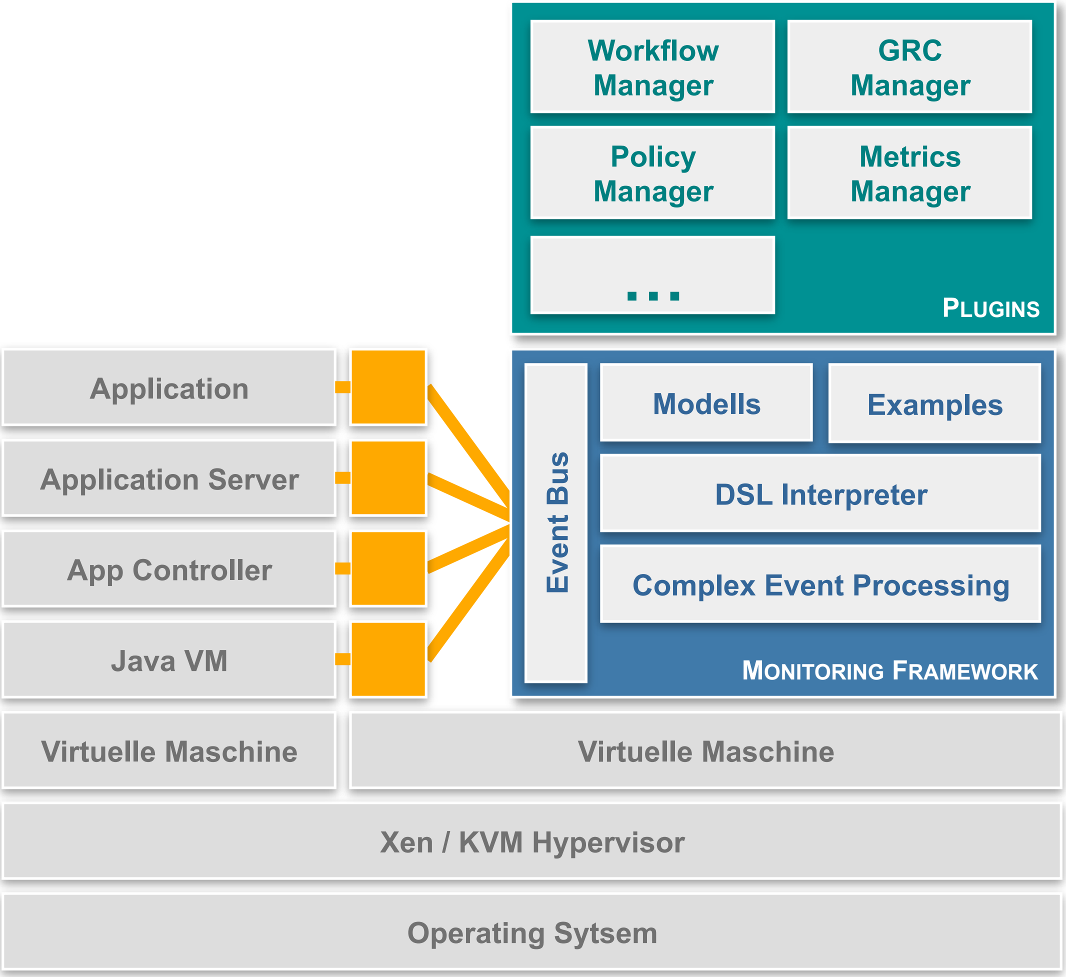
- *Cloud User loose Control*

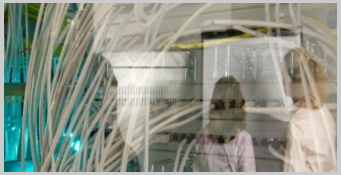
Innovative Solution

- *Select Control Parameters*
- *Continuous Check with predefined values*

Advantage

- *Individual configuration of Monitoring Services*
- *Data Flow Analysis Log-Check, Error Detection*





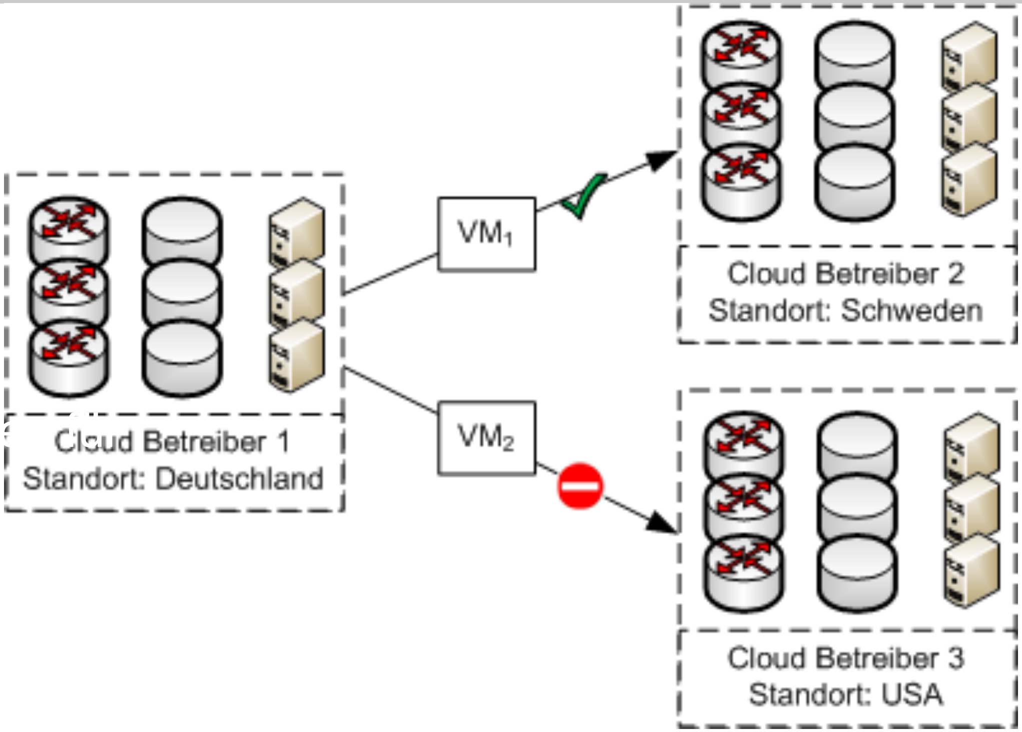
Secure *Cloud Networking*

Problem

- *Where are my Data!*

Innovative Solution

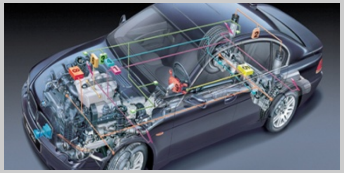
- *User Defined Policies*
- *Automated Check of Security Relevant Parameters*



Advantage

- *Cloud-User: Individually Adapted Policies and Proof of Compliance*
- *Cloud-Provider: Offer and Accounting of User Defined Services*

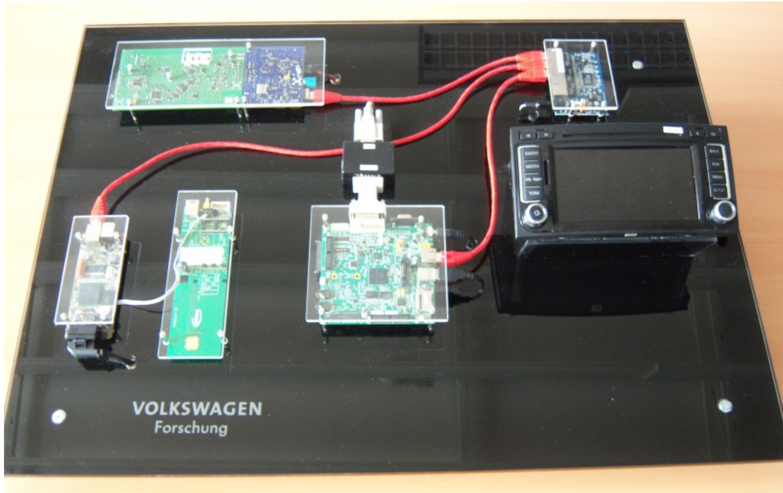
Automotive Security



Fraunhofer AISEC

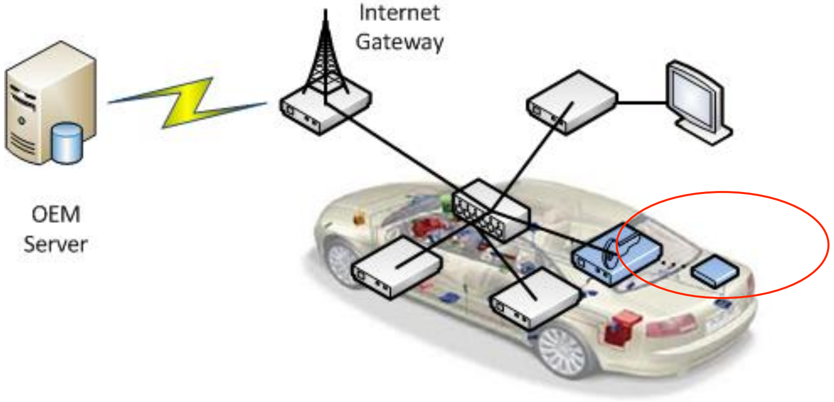
Problem

- *Local Storage of Cryptographic Keys in Standard Flash-Memories is not secure*



Innovative Soultion

- *Central Key Management with Secure Element*
- *Secure Memory and Cryptographic Services*



Advantage

- *Secure Authentication of Vehicles and Components*
- *Base for In-Car and external communication (C2X)*

IT-Early Warning

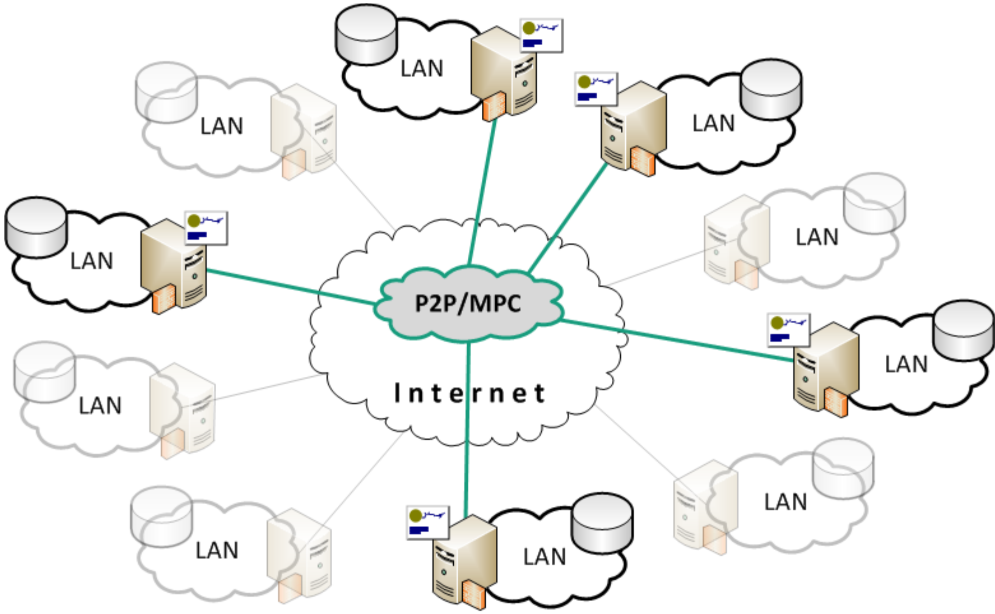
Fraunhofer AISEC

Problem

- *Exchange of Information about Security Incidents across Domains*

Innovative Solution

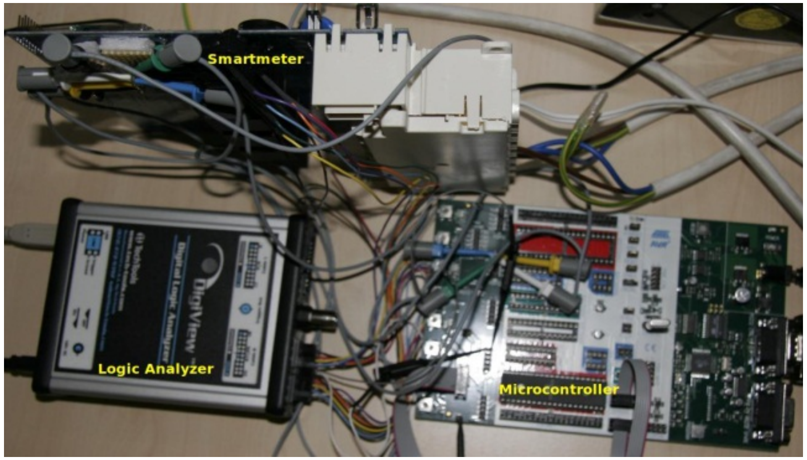
- *Anonymous Certificates*
- *P2P-Nets*
- *Secure Multiparty Protocols*



Advantage

- *Immediate Information Exchange and Data Analysis across Domains*
- *Early Detection of Threats: In-Time and Focused Reaction*

Smart Grid
Smart Meter



Problem

- *Attacks on Control Systems*
- *Fraud*
- *Privacy Protection*

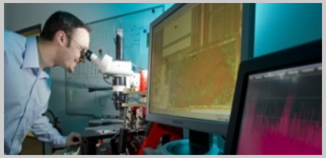
Innovative Solutions

- *Security Concepts for Smart Meter and Gateways*
- *Adapted Hardware Security Modules and Efficient (Cryptographic) Protocols*
- *Concepts for Anonymity and Pseudonyms*

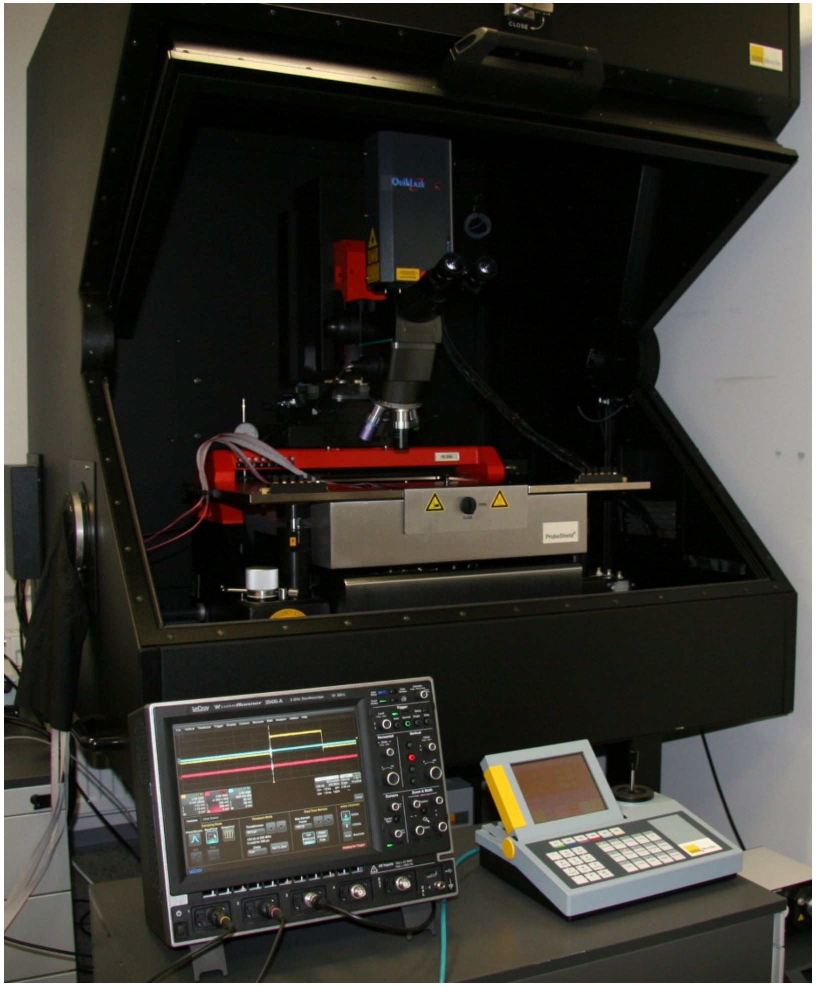
Advantage

- *Development of Smart Grid Reference Architectures*

Security-Evaluation



Fraunhofer AISEC



Problem

- *Security needs to be tested*
- *Real attack vectors have to be applied*

Solutions

- *New attack tools*
- *Wide spectrum of test benches*
- *Tailored test labs: Hardware, Nets, Automotive, Grid, Cloud , Apps*

Advantage

- *Holistic Analysis: HW/SW*
- *Test during development*

AISEC Fields of Expertise

Fraunhofer AISEC

	SST	NES	EMS
Embedded Security			☑
Smart Card & RFID		☑	☑
Cloud & Service Computing	☑	☑	
Security Evaluation	☑	☑	☑
Product Protection			☑
Automotive Security		☑	☑
Network Security	☑	☑	
IT Early Warning		☑	
SmartGrid Security		☑	☑