

Trends in der Forschung für kontaktlose Anwendungen

8. Dresdener RFID Symposium
4. – 5. 12. 2014; Dresden, Deutschland

Holger Bock, Infineon Technologies Austria AG



Überblick

- Einleitung
- CATRENE-Projekt „NewP@ss“
- IKT-Projekt „HINT“ im 7. Rahmenprogramm
- IKT-Projekt „MATTHEW“ im 7. Rahmenprogramm
- Zusammenfassung

Einleitung

■ „Klassische“ RFID-Applikationen

- Logistik
- Transport
- Ticketing
- ...

■ Erweiterte Anwendungsfelder

- kontaktloses Bezahlen
- elektronische Pässe und ID-Karten

■ Trends aus den Anwendungsfeldern

- VHBR
- Authentizitätsanker
- Aktive Rückmodulation



MATTHEW



This project is co-financed by the European Union
under the Seventh Framework Programme

matthew 

Multi-entity-security using active
Transmission Technology for improved
Handling of Exportable security
credentials without privacy restrictions

Acktive Rückmodulation in MATTHEW

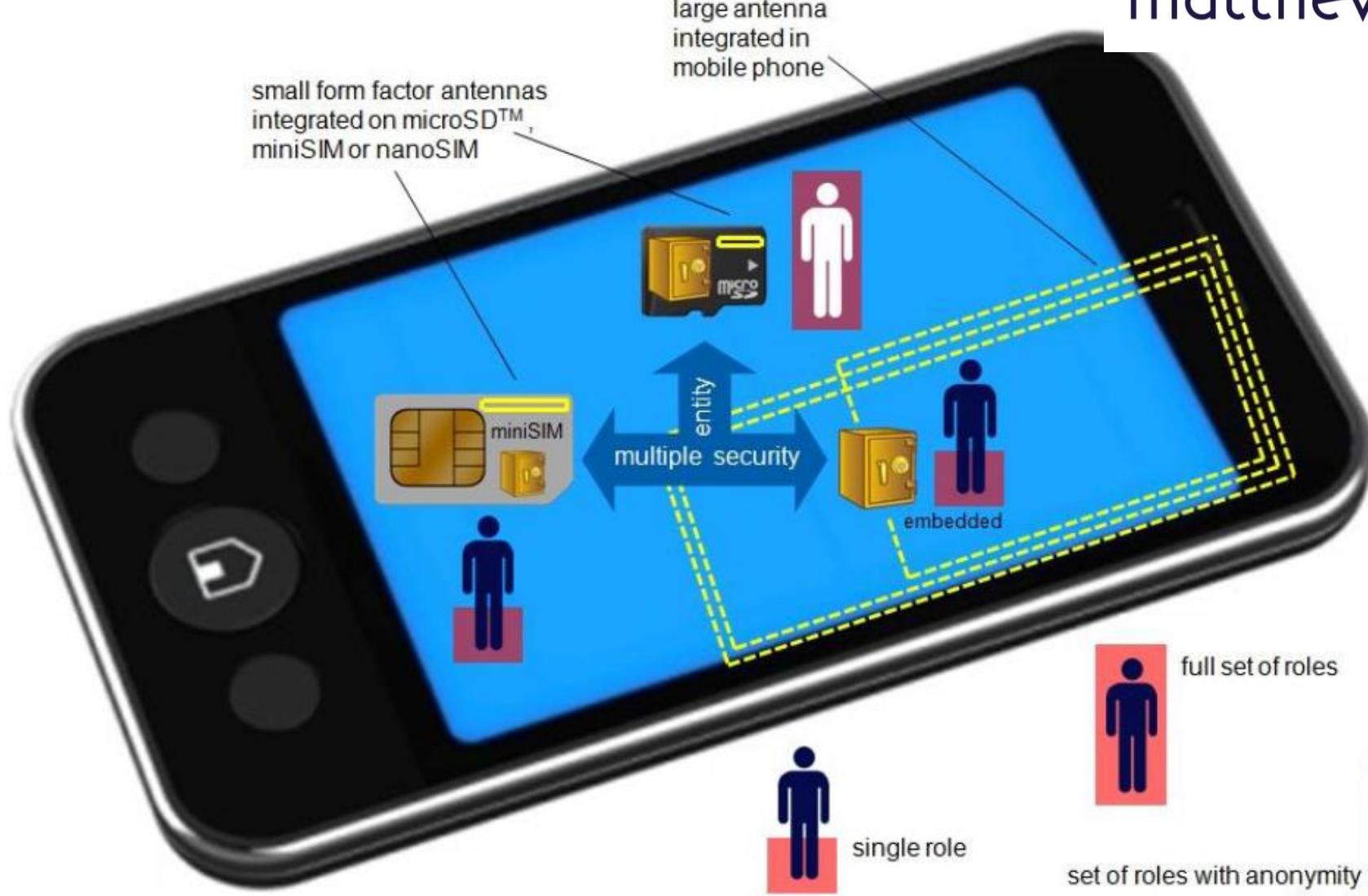
8. RFID-Symposium Dresden, 5. Dez. 2014



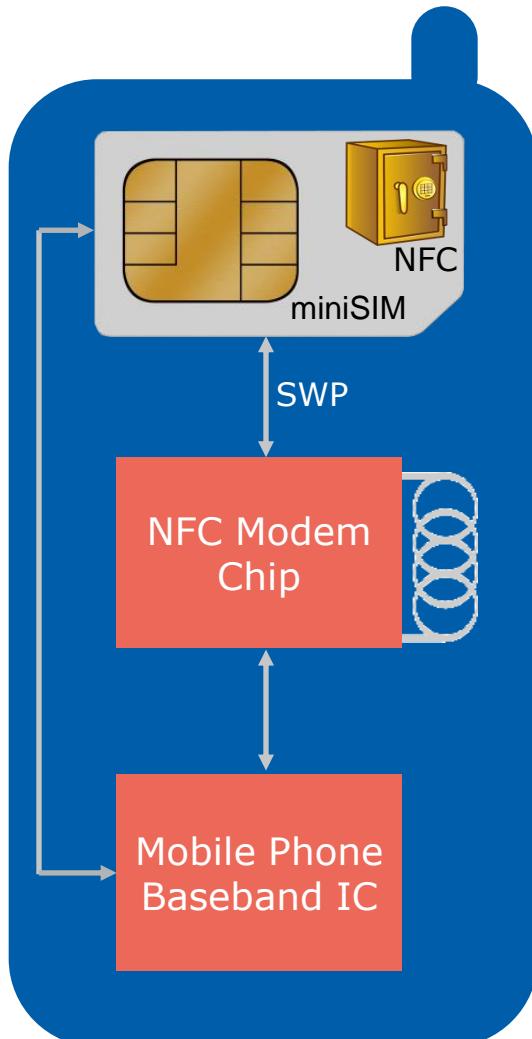
THEME [ICT-2011.1.4]
[Trustworthy ICT]

- European Commission public funding project under FP7;
- Project Start **CY 2013**, 3 years run time;
- **8 Parties from 4 EU Member States**;
- International Coordinator: Infineon Technologies Austria;
Scientific Leader: Crypoexperts, France;
- Target: **Multi-entity-security using active Transmission Technology**;
active modulation, privacy-preserving transfer of credentials;

Mehrere Sicherheitsanker in einer mobilen Plattform

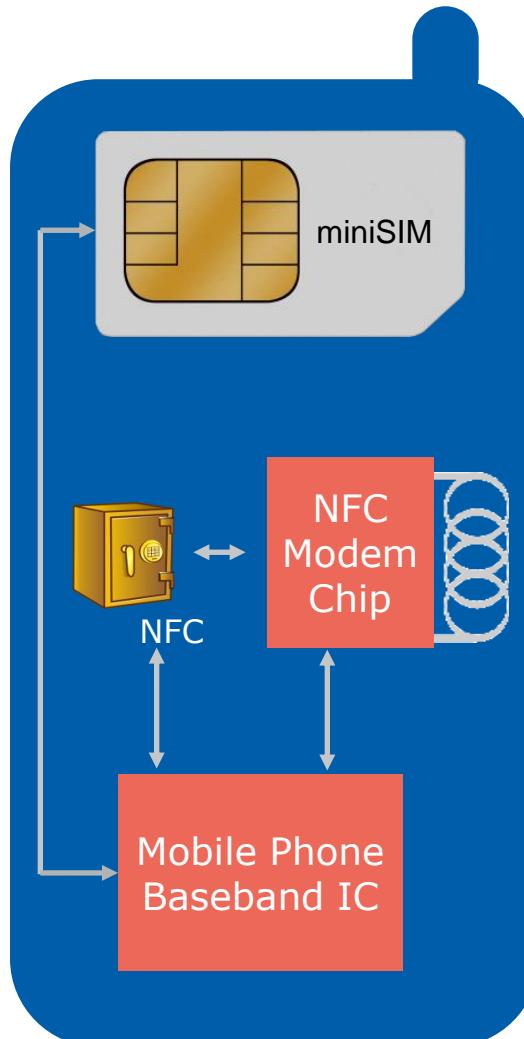


Bisherige NFC Implementierungen



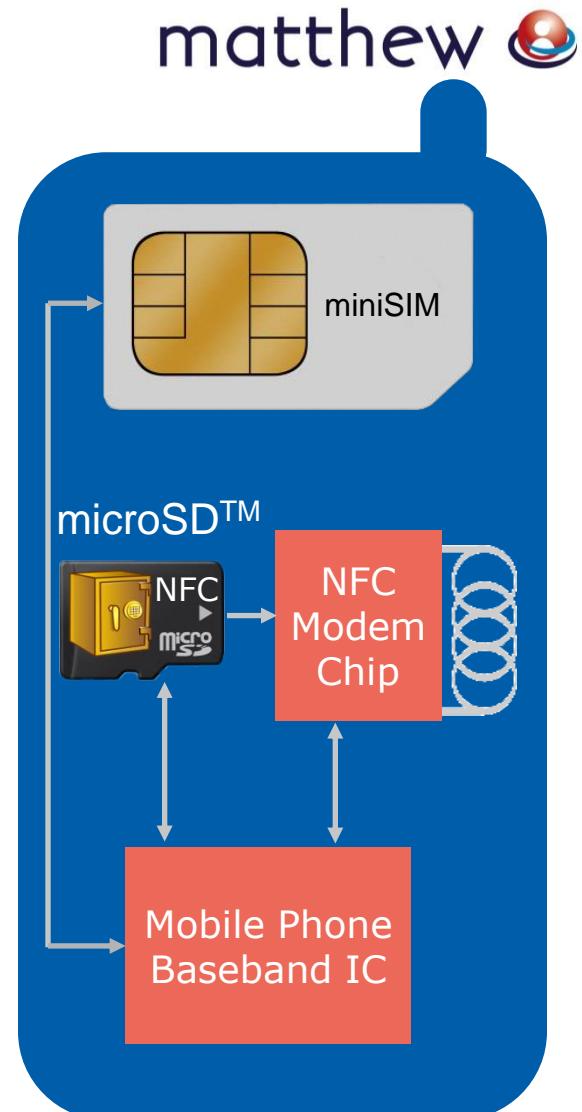
Mobile Network Operator (MNO)

2014-12-05



OEMs, Google Wallet

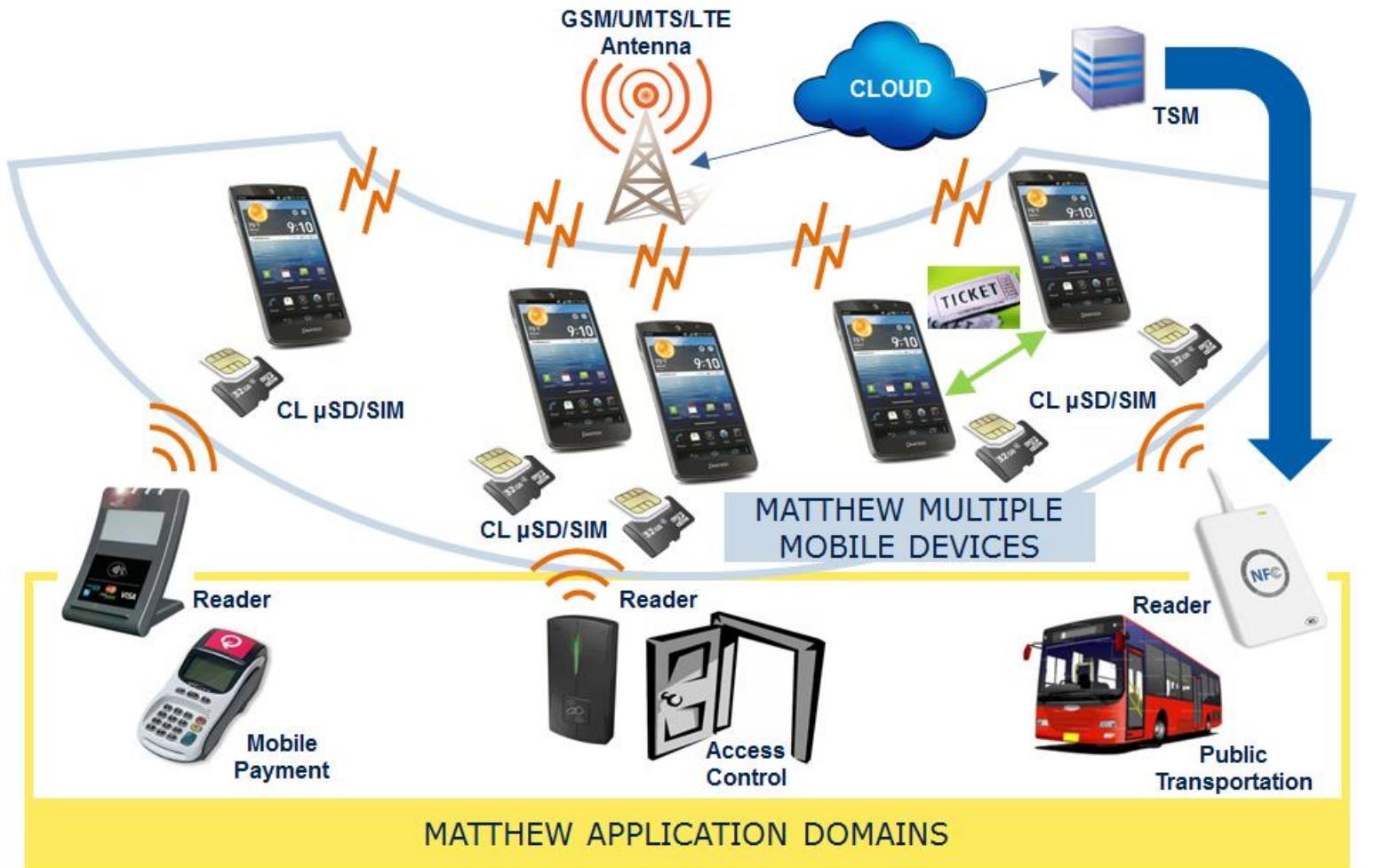
Copyright © Infineon Technologies AG 2014. All rights reserved.



Banks

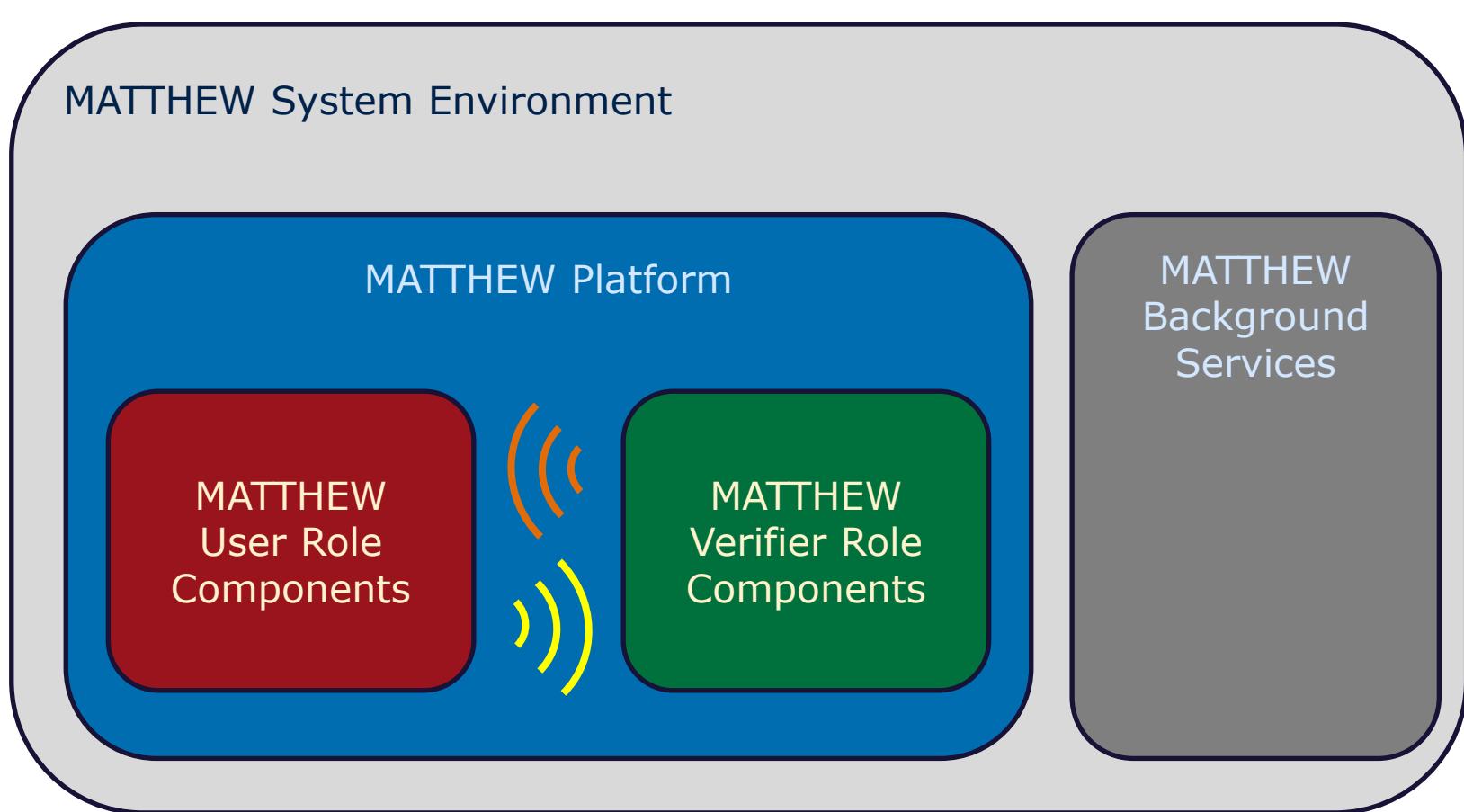
Anwendungsszenarien in MATTHEW

matthew



Das Rollenmodell in MATTHEW

■ The MATTHEW architecture break down



Die MATTHEW Platform

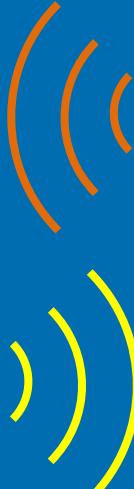
■ MATTHEW platform and its Komponenten



MATTHEW Platform

MATTHEW User Role Components:

- Mobile device(s)
 - App
 - Operating System
 - Device Drivers
 - Hardware
- Secure Entity
 - Hardware, Interfaces
(CB, CL) & Antennas
 - Firmware
 - Secure OS
 - Protocol SW

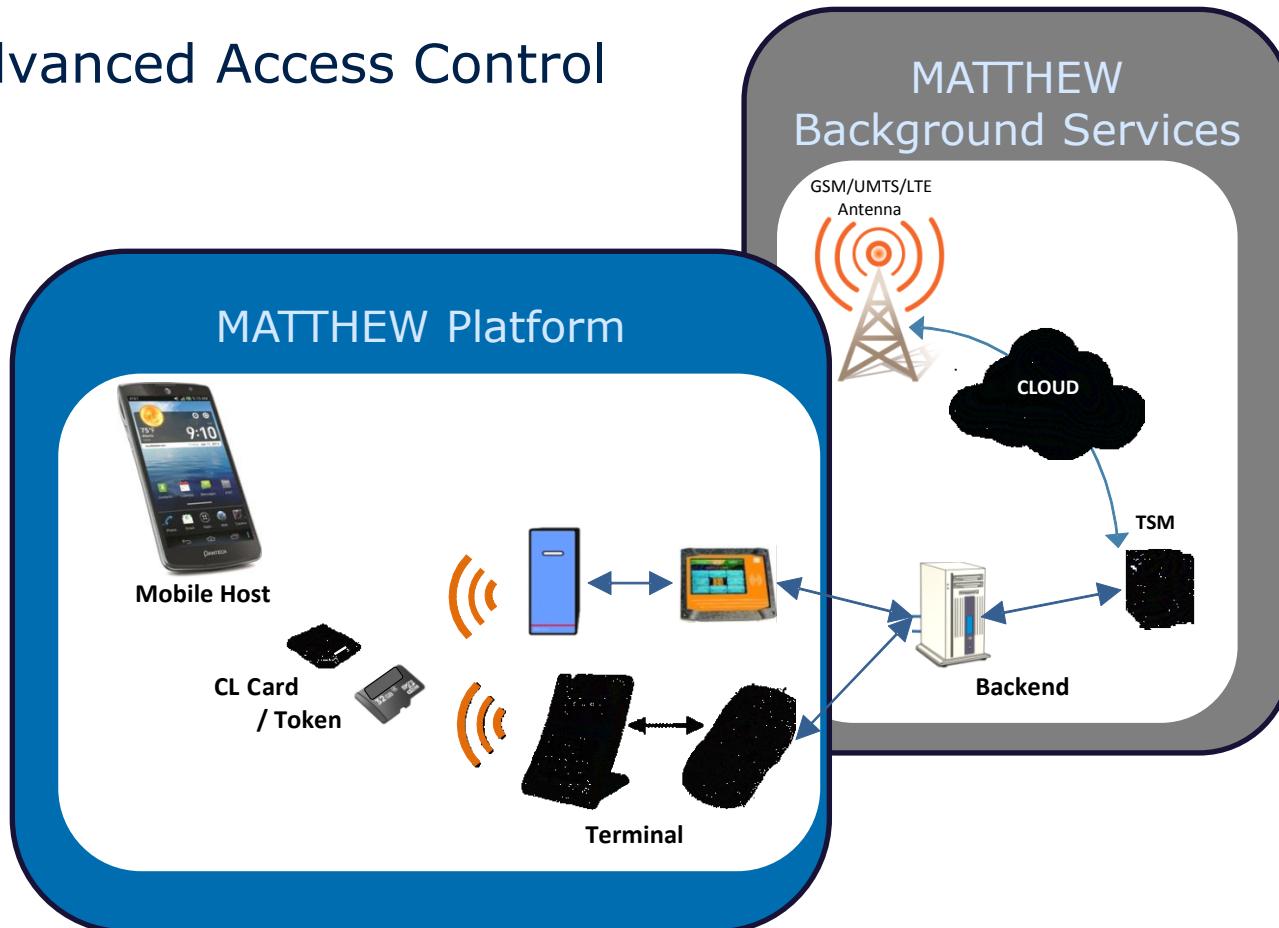


MATTHEW Verifier Role Components:

- CL Reader
 - Interface Controller
 - SAM
 - Reader Hardware
- Terminal
 - Application Controller
 - Verifier Software
 - Protocol SW
 - Actuator
 - Background System Interface

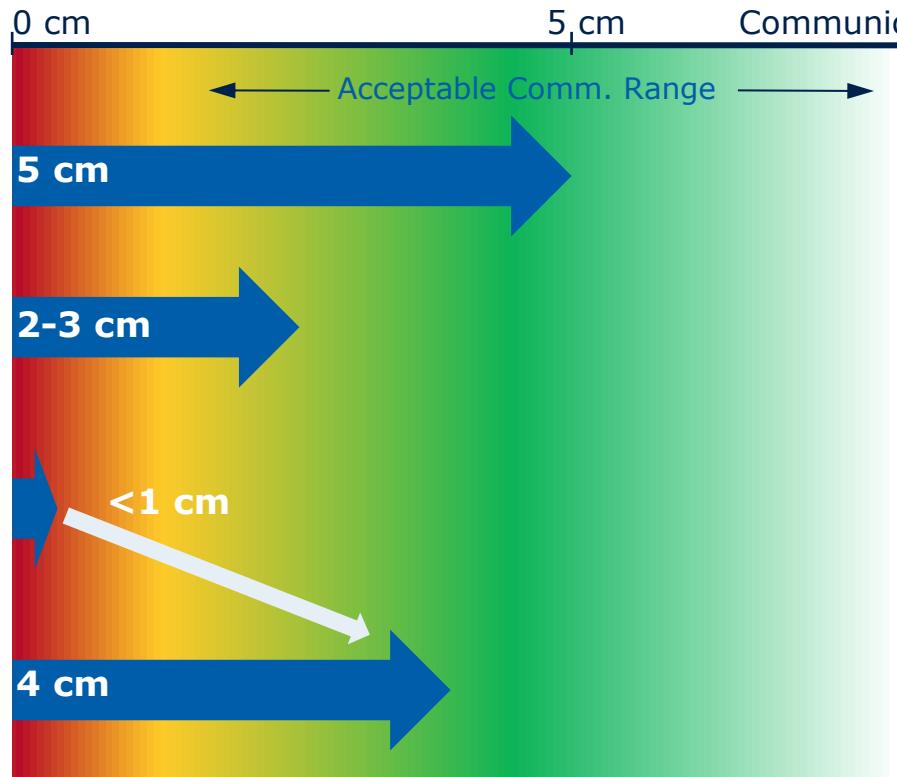
Anwendungsszenarien mit ATT

- Mobile Payment
- Advanced Access Control



MATTHEW Project scope ATT

■ Communication Range of Contactless Cards and NFC:



Passive ID1 Antenna (4000 mm^2)



NFC-Mobile, **passive** Modulation ($\sim 1350 \text{ mm}^2$)



NFC-Mobile, **passive** Modulation in microSDTM Card ($\sim 130 \text{ mm}^2$)



NFC-Mobile with **active** transmission technology in microSDTM Card ($\sim 130 \text{ mm}^2$)

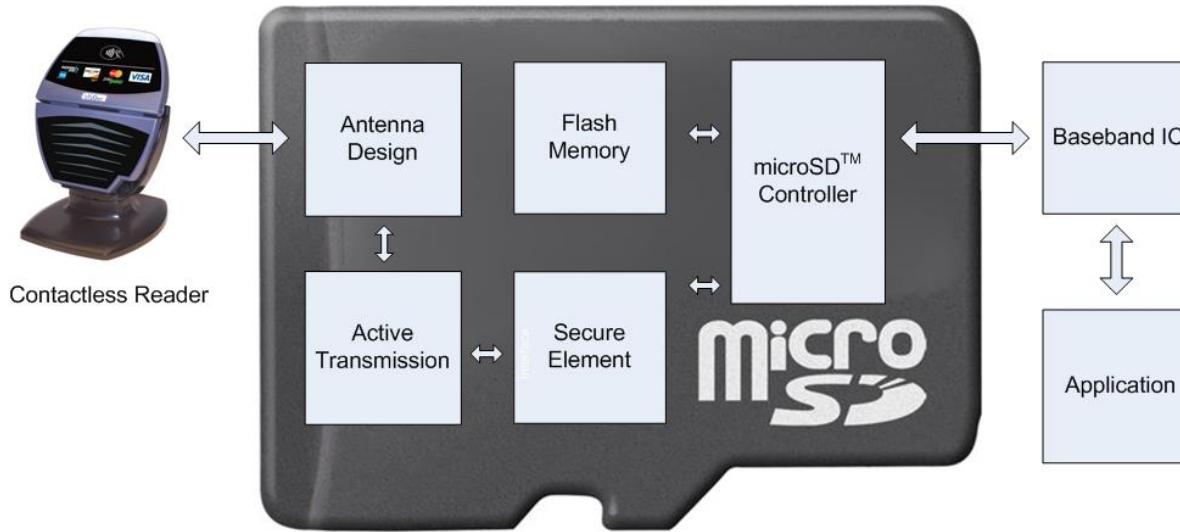
matthew

■ Add-On for Security Controller: **Active Communication Interface**

- New applications, e.g. „standalone NFC“ in microSDTM or SIM cards
- Performance and cost reduction with integrated Solution

Concept

matthew



Target: Enabling small form factors using active transmission technology

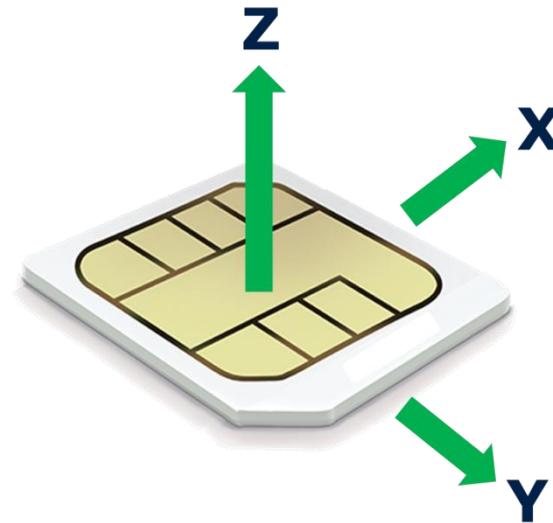
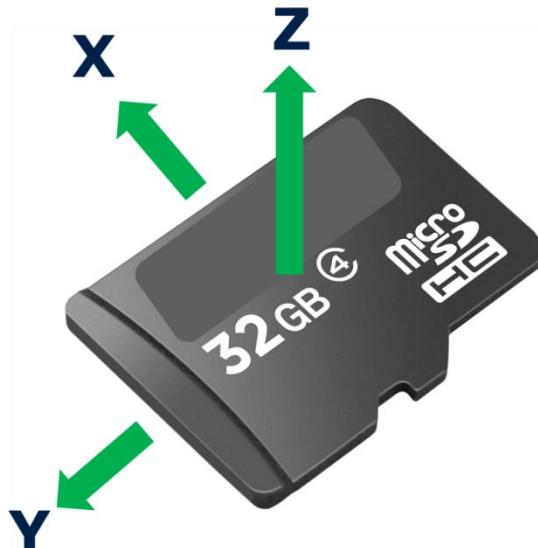
- Communication in spite of mobile-casing and –battery
- Extended communication range due to active modulation
-also possible for miniSIM (2FF), microSIM (3FF) and nanoSIM (4FF)

Projekt Fokus Aktive Rückmodulation (ATT)

Forschungsfelder:

matthew 

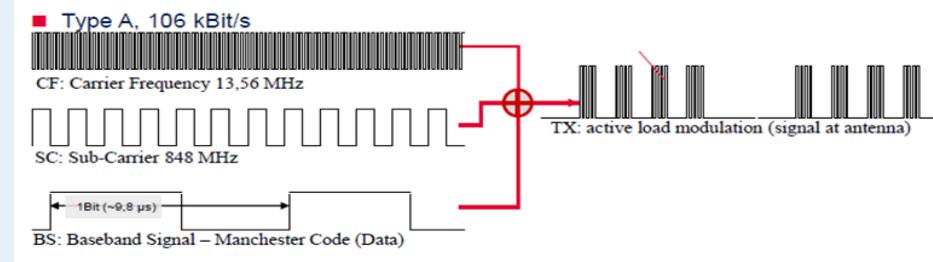
- Antenna Design und Bevorzugte Abstrahlcharakteristik
- Simulationsmodelle für diverse Mobile Plattformen
- Active Transmission Technology (ATT)
- Standardisierung der ATT (ISO)
- Interoperabilität mit existierende Reader Infrastruktur
- Integration der ATT mit einem Secure Element



Active Load Modulation – how it works

matthew

- Active Modulation drives against terminal (180° signal shift)
- Uses battery power



- Active Load Modulation applied in micro antenna form factor



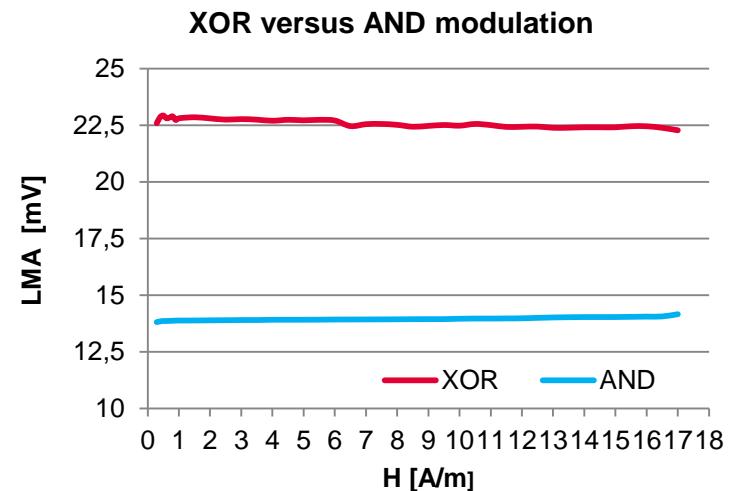
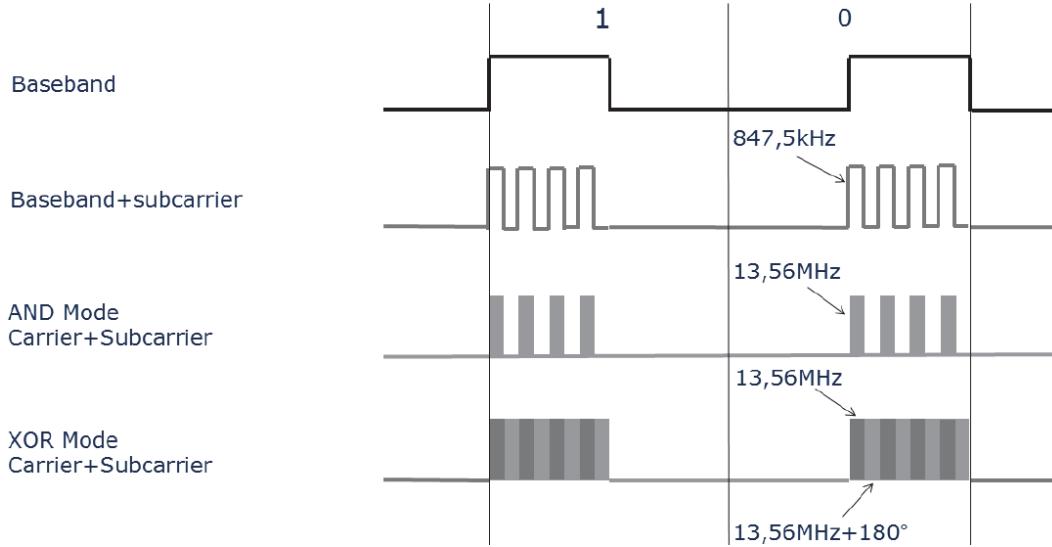
- Reader sees same signal like on contactless ID1 card



Active Modulation Modi

Type A:

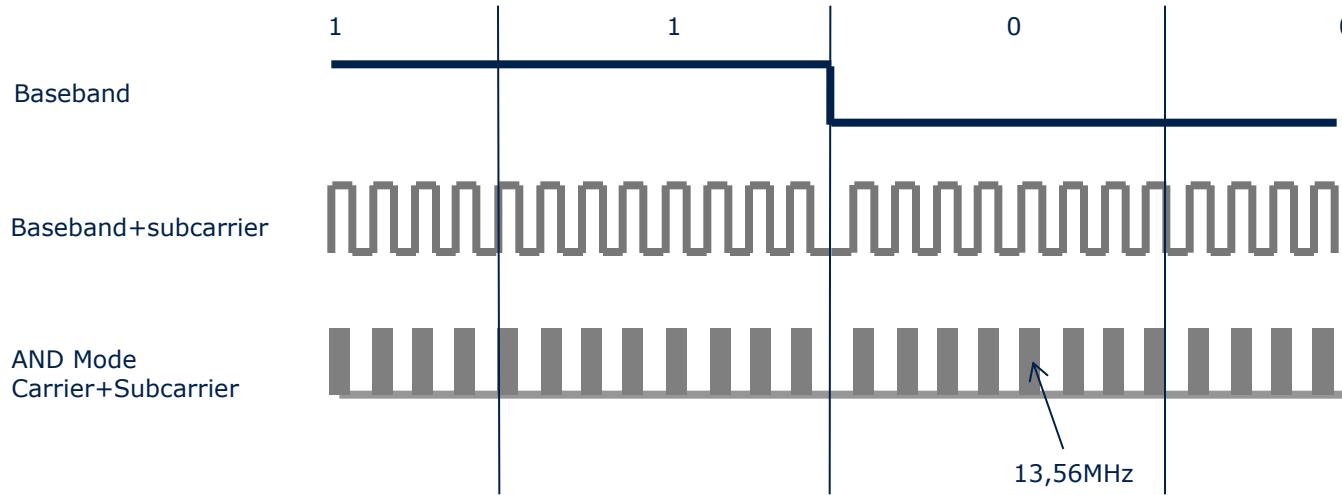
matthew



Active Modulation Modi

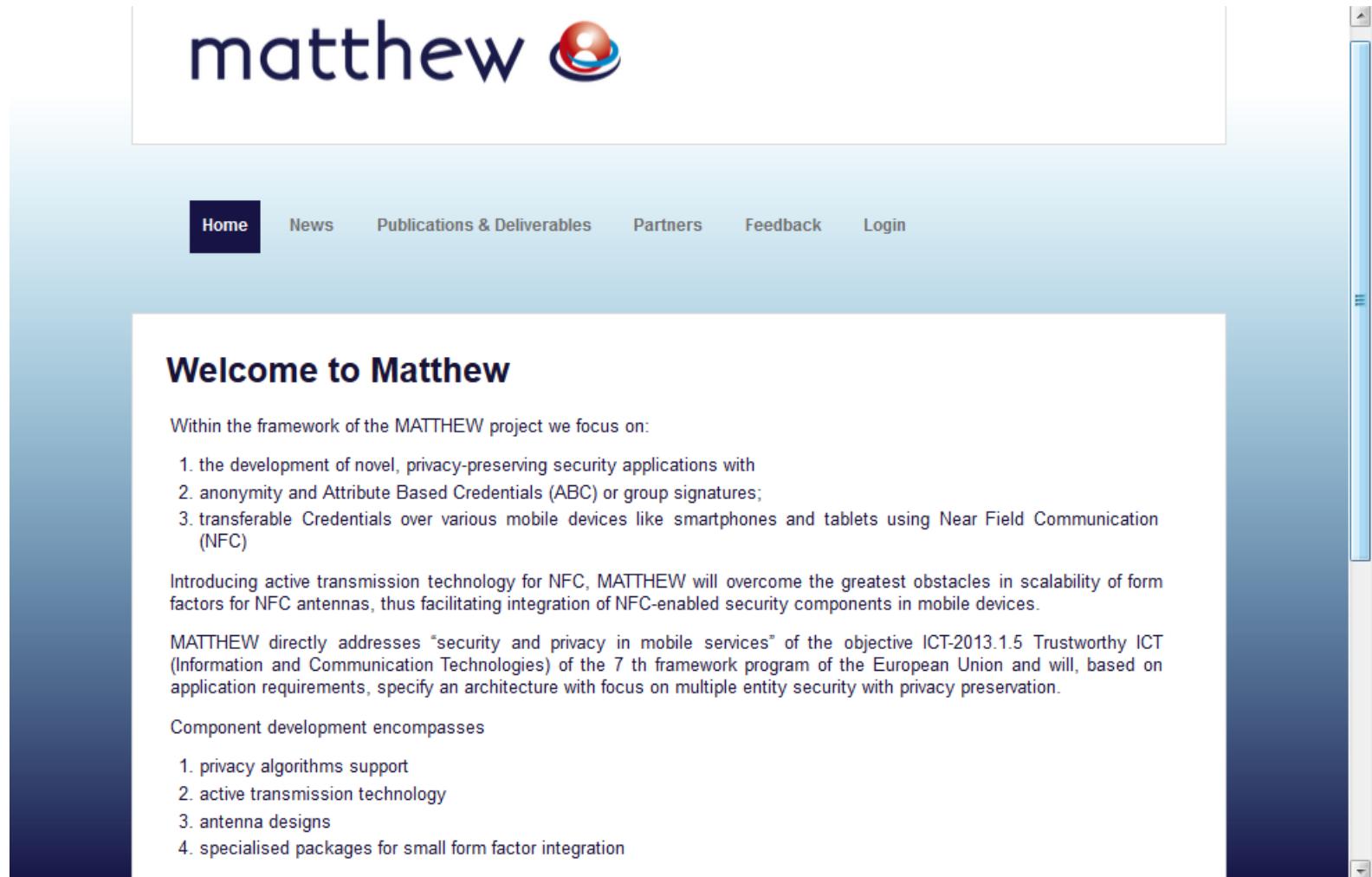
Type B:

matthew 



- ISO/IEC 14443, Type A: AND and XOR modulation supported → XOR recommended
- ISO/IEC 14443, Type B: AND modulation supported

Projekt-Homepage



The screenshot shows the homepage of the Matthew project. At the top, there is a large logo with the word "matthew" in a stylized font and a small circular icon. Below the logo is a navigation bar with links: Home (highlighted in dark blue), News, Publications & Deliverables, Partners, Feedback, and Login. The main content area has a white background and features a section titled "Welcome to Matthew". It contains text about the project's focus on developing privacy-preserving security applications using NFC technology. It also mentions the project's address under the ICT-2013.1.5 Trustworthy ICT program. Below this, there is a section titled "Component development encompasses" with a list of four items related to privacy algorithms support, active transmission technology, antenna designs, and specialised packages for small form factor integration.

Welcome to Matthew

Within the framework of the MATTHEW project we focus on:

1. the development of novel, privacy-preserving security applications with
2. anonymity and Attribute Based Credentials (ABC) or group signatures;
3. transferable Credentials over various mobile devices like smartphones and tablets using Near Field Communication (NFC)

Introducing active transmission technology for NFC, MATTHEW will overcome the greatest obstacles in scalability of form factors for NFC antennas, thus facilitating integration of NFC-enabled security components in mobile devices.

MATTHEW directly addresses "security and privacy in mobile services" of the objective ICT-2013.1.5 Trustworthy ICT (Information and Communication Technologies) of the 7 th framework program of the European Union and will, based on application requirements, specify an architecture with focus on multiple entity security with privacy preservation.

Component development encompasses

1. privacy algorithms support
2. active transmission technology
3. antenna designs
4. specialised packages for small form factor integration

<http://matthew-project.eu/>

Zusammenfassung

- Trends aus den Anwendungsfeldern eGovernment und mobile Payment
 - VHBR
 - Authentizitätsanker
 - Aktive Rückmodulation
- Anwendungen zeigen den Bedarf nach weiterer Forschung im Sinne von
 - Kommunikationstechnik ("connectivity") und
 - Sicherheit ("Security")





ENERGY EFFICIENCY MOBILITY SECURITY

Innovative semiconductor solutions for energy efficiency, mobility and security.

