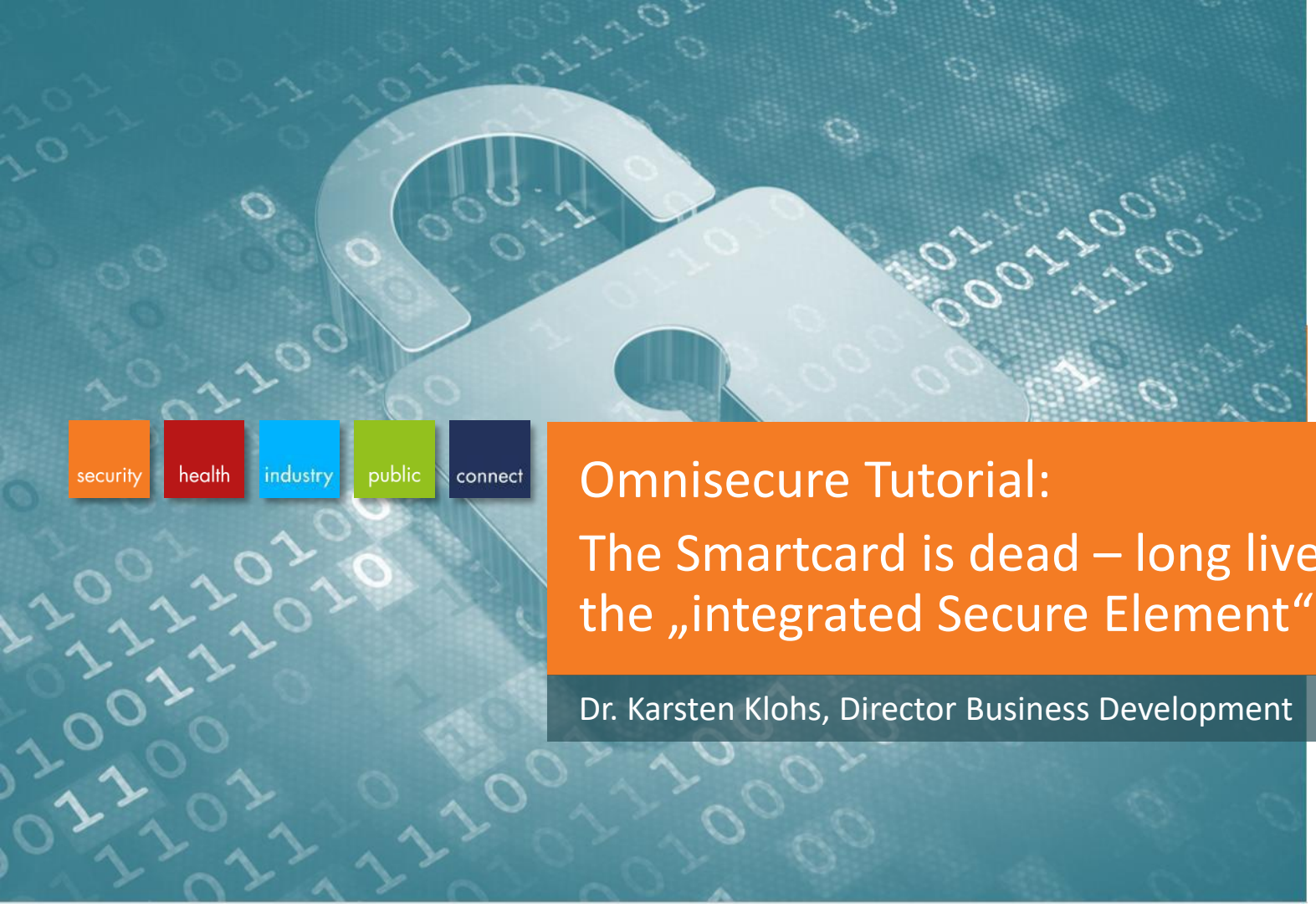


security health industry public connect

Omnisecure Tutorial:

The Smartcard is dead – long live the „integrated Secure Element“

Dr. Karsten Klohs, Director Business Development

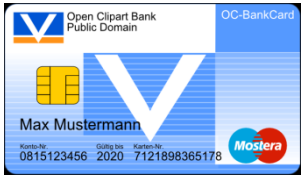
achelos

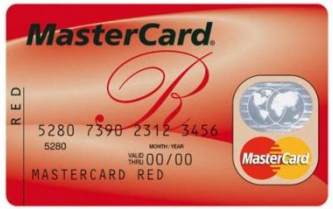
Integriertes Managementsystem ISO 9001 ISO/IEC 27001

Allianz für Cyber-Sicherheit Partner

SecurITy made in Germany

How many Smartcards have you encountered in the last weeks?



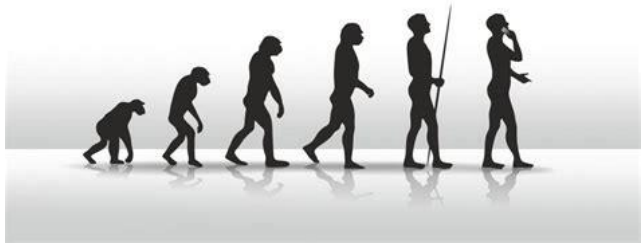


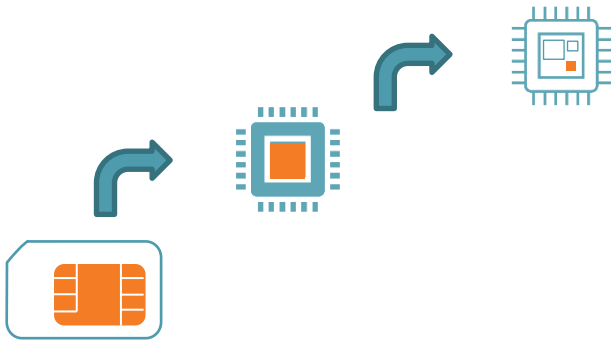
How many “Secure Elements” have you encountered in the last weeks?

G Pay
SAMSUNG pay
Pay

, and many others…

From Smartcards to embedded to integrated Secure Elements – Core Drivers





Definitions (as used in this presentation, others exist in the market):

- “embedded SE” == still a dedicated security IC but permanently bound and a small part to a complex device (smartphone, car, wearable, IoT devices, …)
- “integrated SE” == also bound to a device but integrated into a larger System-on-Chip

Evolution to “embedded SEs” driven by:

- Separation of the device owner from the subscription provider (in Telco market)
- Need for a strong hardware security anchor to securely boot, system management and to support security solutions the OEM is interested in (e.g. OEM Pay)

Evolution to “integrated SEs” driven by:

- Substantial cost savings (no dedicated IC needed)
- Shared-memories, peripherals, and higher-source powers enable more complex use-cases

How does an “integrated secure element” look like and how does it differ from a stand-alone Security IC?

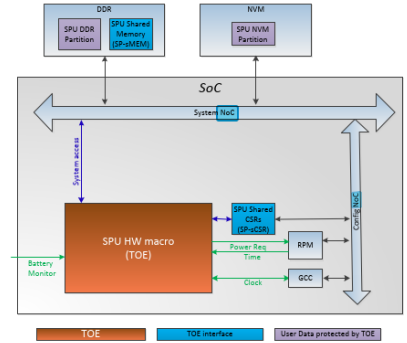


Figure 3-1 TOE components and their interfaces to the SoC

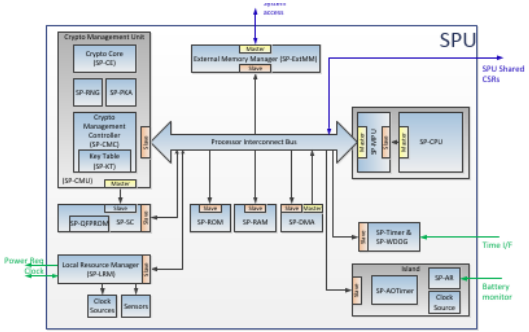


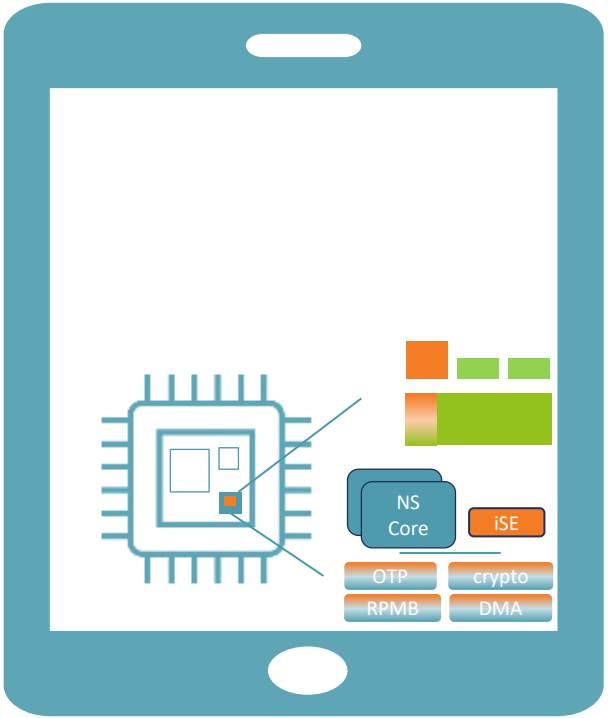
Figure 3-3 TOE hardware components

- **Example:** Qualcomm SPU230
  (first Common Criteria AVA_VAN.5 certified iSE, BSI 2019)

- Integrated as a Hard Macro (independently synthesized) into larger SoC designs:
  - connected via SoC standard busses
  - use of shared memories protected by TOE encryption techniques
  - integrated into the power domains of the SoC

- Design (this TOE, many other design strategies exist):
  - Dedicated crypto core, including secure key store
  - Secure ROM, RAM and DMA
  - Dedicated external memory management unit controlling shared (untrusted) memory usage
  - Dedicated Units to control (untrusted) externals, like power and clock

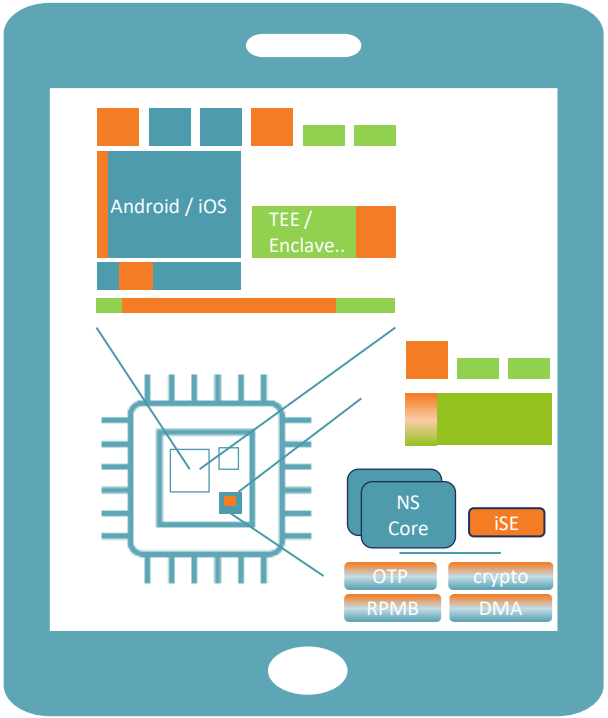
Zooming out: Integrated Secure Element from the birds-eye view



Consequences of using (integrated) Secure Element as part of complex system and for a wide variety of purposes in complex devices and systems:

1. **"You are not alone" (Device manufacturers integrate secure elements and supporting HW not only for your use case, but for many other purposes, like secure boot, securing keys, commercial use cases)**
   => sharing of system resources and being co-located with other sensitive software massively **increase the complexity of a security solution and resource sharing**

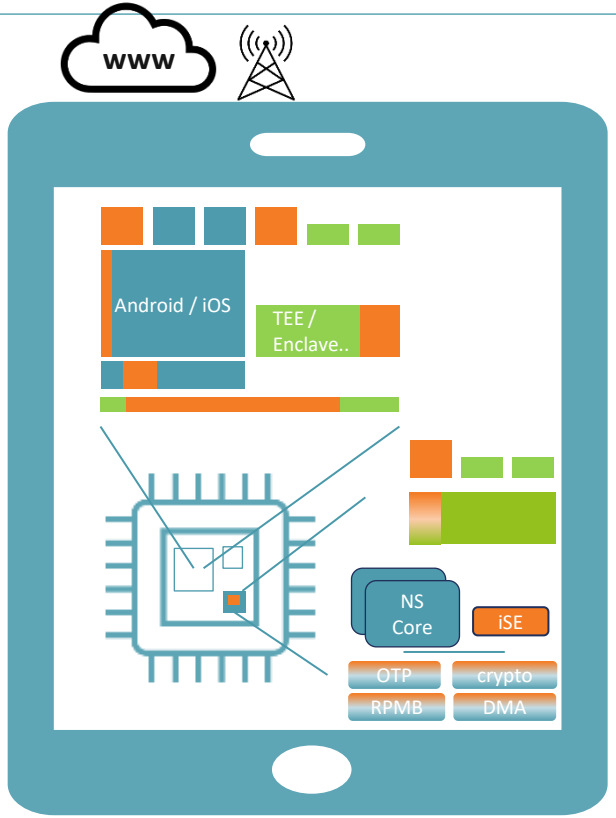
Zooming out: Integrated Secure Element from the birds-eye view



Consequences of using (integrated) Secure Element as part of complex system and for a wide variety of purposes in complex devices and systems:

1. sharing of system resources and being co-located with other sensitive software massively **increase the complexity of a security solution and resource sharing**
2. **"You can no longer interface with an iSE using an interface defined by few use case specific extensions to standard protocols (like ISO716, ISO14443-based Smartcard Command layers) "**
   => **Security solutions have use and deploy on heterogeneous HW and SW infrastructures** which leads to challenges for deployment, and operation and maintenance, in particular for the provisioning of keys, application logic and updates

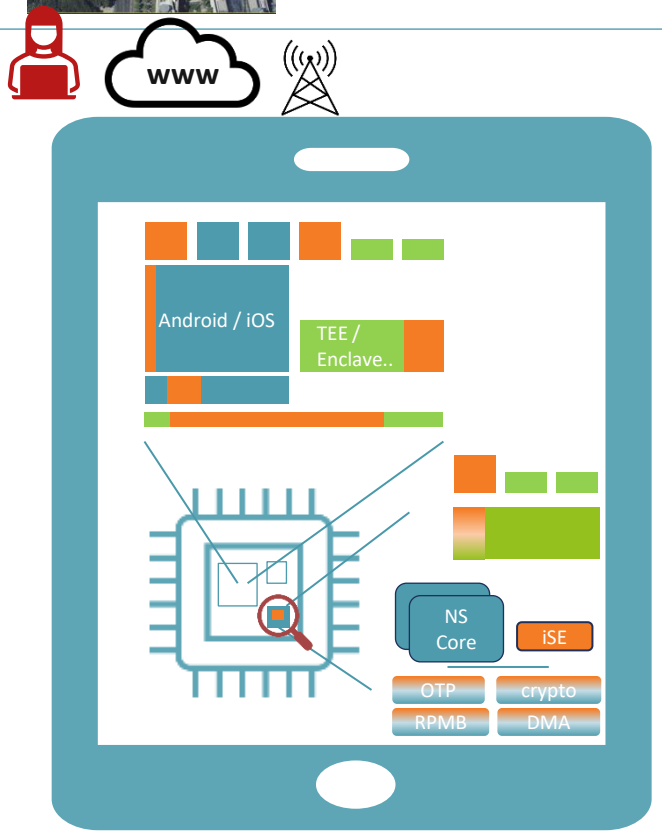
Zooming out: Integrated Secure Element from the birds-eye view



Consequences of using (integrated) Secure Element as part of complex system and for a wide variety of purposes in complex devices and systems:

1. sharing of system resources and being co-located with other sensitive software massively **increase the complexity of a security solution and resource sharing**
2. **Security solutions have use and deploy on heterogeneous HW and SW infrastructures** which leads to challenges for deployment, and operation and maintenance, in particular for the provisioning of keys, application logic and updates
3. **"The device hosting the iSE is almost always connected"**
   => **Continuous device connectivity enables fast and continuous develop and update cycles** (OS release in months, app release in weeks, security patches in days)

Zooming out: Integrated Secure Element from the birds-eye view



Consequences of using (integrated) Secure Element as part of complex system and for a wide variety of purposes in complex devices and systems:

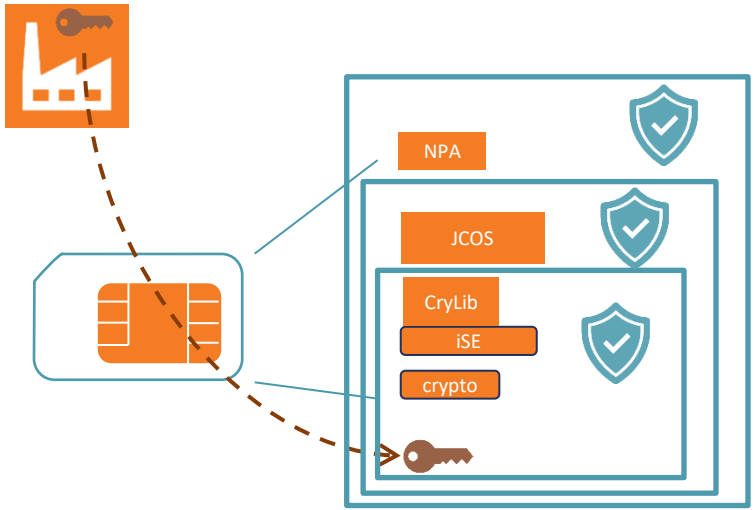
1. sharing of system resources and being co-located with other sensitive software massively **increase the complexity of a security solution and resource sharing**
2. **Security solutions have use and deploy on heterogeneous HW and SW infrastructures** which leads to challenges for deployment, and operation and maintenance, in particular for the provisioning of keys, application logic and updates
3. **Continuous device connectivity enables fast and continuous develop and update cycles** (OS release in months, app release in weeks, security patches in days)
4. **"Attackin g a SoC-HW is more complex but what is most critical are scalable SW exploits"**

   => **New technology characteristics pose new challenges for hardware attacks and the main concern from single device hacking to scalable attacks**

The Core Challenges for efficient security evaluations

	1	2	3	4
Challenges	Increasing system complexity and resource sharing	Security solutions use and deploy on heterogeneous HW and SW infrastructures	Continuous device connectivity enables fast and continuous develop and update cycles	New technology characteristics pose new challenges for hardware attacks and the main concern from single device hacking to scalable attacks
Needs	Scale security evaluations to complex security solutions	More flexible, and faster composition strategies to cover more complex stakeholder-landscapes, supply chains and Dev(Sec)Ops-infrastructures	Faster security evaluation cycles	Evolution of attack methods and more holistic rating methodologies

Recap: How do we evaluate traditional Smartcard Solutions (NPA, eGK…)?



Most complex scenario we handle:

1. Evaluate and certify Security IC HW, Firmware, Crypto Lib of Vendor A (10 months)
2. Evaluate and certify Card OS of Developer B (8 months)
3. Evaluate product application of Developer C (6 months)
4. Luckily updates hardly needed because single, simple use case only. Migration to new chip version (~ 6 months?)
5. Key provisioning is usually part of the production process and integrated I the evaluation

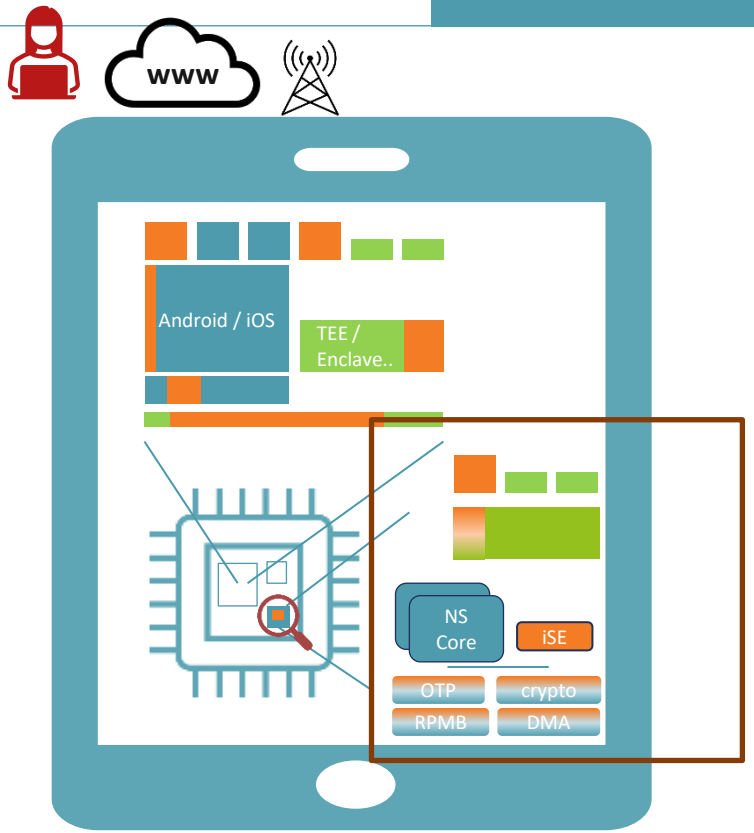
In principle an integrated Secure Element can also achieve a high attack resistance!

Why not use an iSE in a mobile to host an NPA, eGK, …?

The Core Challenges for efficient security evaluations

	1	2	3	4
Challenges	Increasing system complexity and resource sharing	Security solutions use and deploy on heterogeneous HW and SW infrastructures	Continuous device connectivity enables fast and continuous develop and update cycles	New technology characteristics pose new challenges for hardware attacks and the main concern from single device hacking to scalable attacks
Needs	Scale security evaluations to complex security solutions	More flexible, and faster composition strategies to cover more complex stakeholder-landscapes, supply chains and Dev(Sec)Ops-infrastructures	Faster security evaluation cycles	Evolution of attack methods and more holistic rating methodologies

1 Increasing system complexity and resource sharing



Detailed problems / unsolved questions:

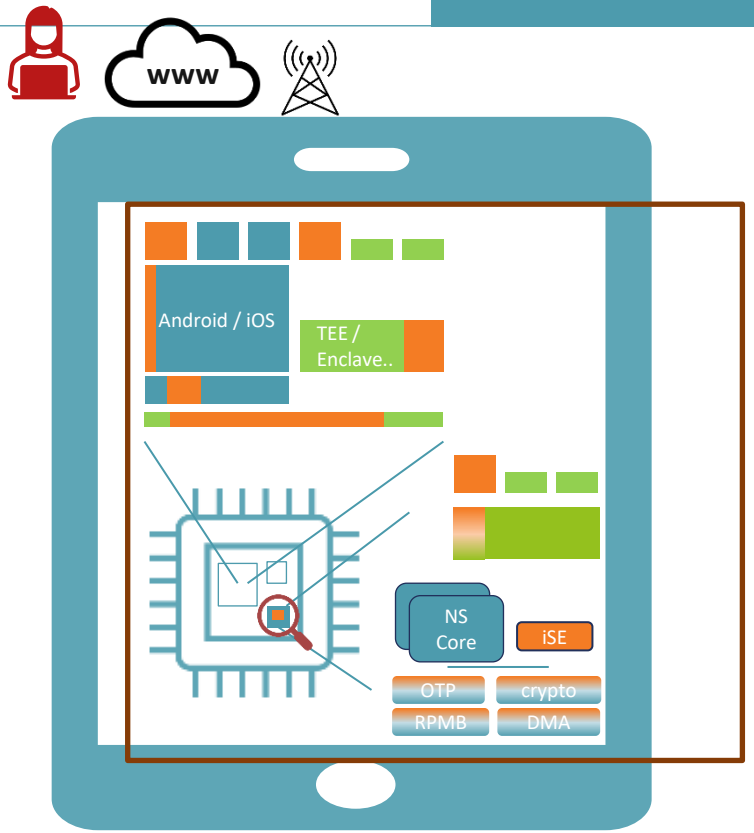
- Traditional approaches of manual code reviews do scale well to a massive increase of the “Trusted Code Base” – how to scale / augment / replace manual code review with other techniques?
- Multi-purpose use of iSEs implies more and more “non-interfering” code in the same security domain - how to deal with this situation?
- Data exchange with an iSE is no longer restricted by an APDU buffers and the SW stack becomes more complex so the software attack surface will substantially increase

Our running example:

- Assume there is an multi-purpose iSE that offers means to load additional applications for governmental IDs. However, this iSE is also responsible for secure device boot, and contains substantial code that is a cornerstone of OEM security solutions (OEMPay, etc…)

What are your market observations and solution proposals?

2 Complex, heterogeneous infrastructures



Detailed problem characteristics / Unsolved problems:

- Key areas: key provisioning + key access control (Trusted UI) + use case application logic interfere with the device / OEM infrastructures that are non-standardized => how to evaluate these?
- Increasing specialization leads to an increasing fragmentation of the landscape (IP providers, HW integrators, OS providers, OS driver extensions, OEMs…) => how to compose all of these?
- Security is addressed but in many different forms (bounty programs, internal blue teams, external security assessment, proprietary schemes, …) => how to leverage on this?

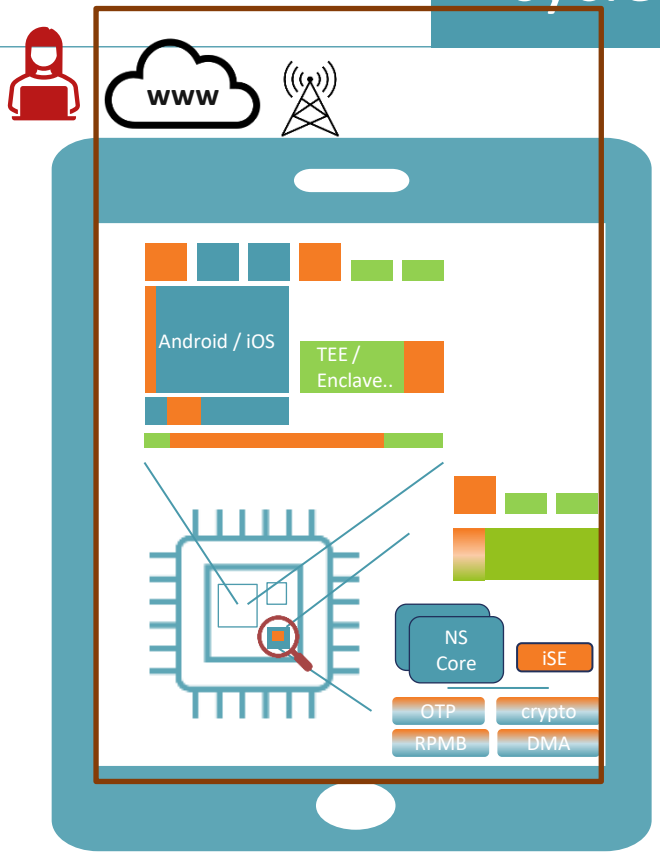
Our running example:

- How to deploy an Governmental ID on eSE / iSEs of ***all*** big OEMs and how to evaluate all the different deployment device infrastructures?

What are your market observations and solution proposals?

Faster and continuous develop and update cycles

3



Detailed problem characteristics / Unsolved problems:

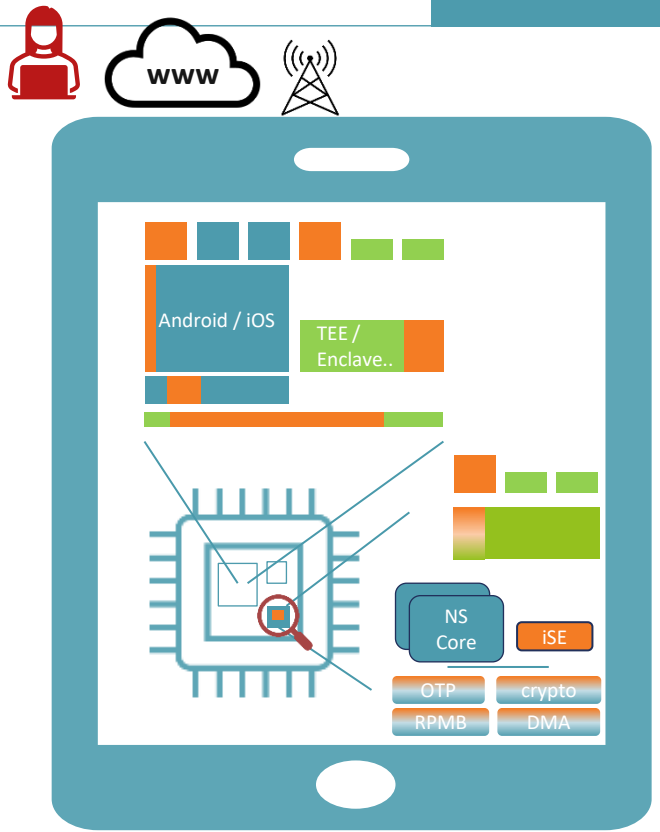
- What the market needs from security evaluations: baseline in months, updates in weeks, and security patch in days
- update becomes as heterogeneous as the system (ROM patch, boot-loader update, OS update, driver loading, application loading…)
- Most updates will relate not to the security solution but to other (still security sensitives) parts of the system
- devices operating security solutions matures and adapts over time – snapshot-evaluations of a specific product version are no longer viable

Our running example:

- What happens to a deployed Governmental ID if supporting parts of the system evolve?

What are your observations and solution proposals?

4 New technology characteristics and evolution of rating methodologies



Detailed problem characteristics / Unsolved problems:

- Hardware more difficult to decompose (e.g. package-on-package, …)
- Approaches to Fault Injection and Side Channel Analysis have to evolve (attacking the SE w/o impacting the SoC, differing noise and acquisition speeds, …)
- Scalable SW attacks have the most devastating effect, a single device hacks a lesser concern => not well covered in current rating methodologies

What are your observations and solution proposals?

The Core Challenges for efficient security evaluations

	1	2	3	4
Challenges	Increasing system complexity and resource sharing	Security solutions use and deploy on heterogeneous HW and SW infrastructures	Continuous device connectivity enables fast and continuous develop and update cycles	New hardware characteristics and shift of the main concern to scalable SW attacks
Needs	Scale security evaluations to complex security solutions	More flexible, and faster composition strategies to cover more complex stakeholder-landscapes, Dev(Sec)Ops-infrastructures	Faster security evaluation cycles	Evolution of attack methods and more holistic rating methodologies
Solutions ???	Automation and tools Accumulative assurance Minimization of the TCB	Black-box composition and ight-weight integration iSE API Standardization Meta-schemes	“Predictive assurance” Security monitoring	SW Quality metrics like potential vulnerability density Exploit mitigations

Vielen Dank! | Thank you!

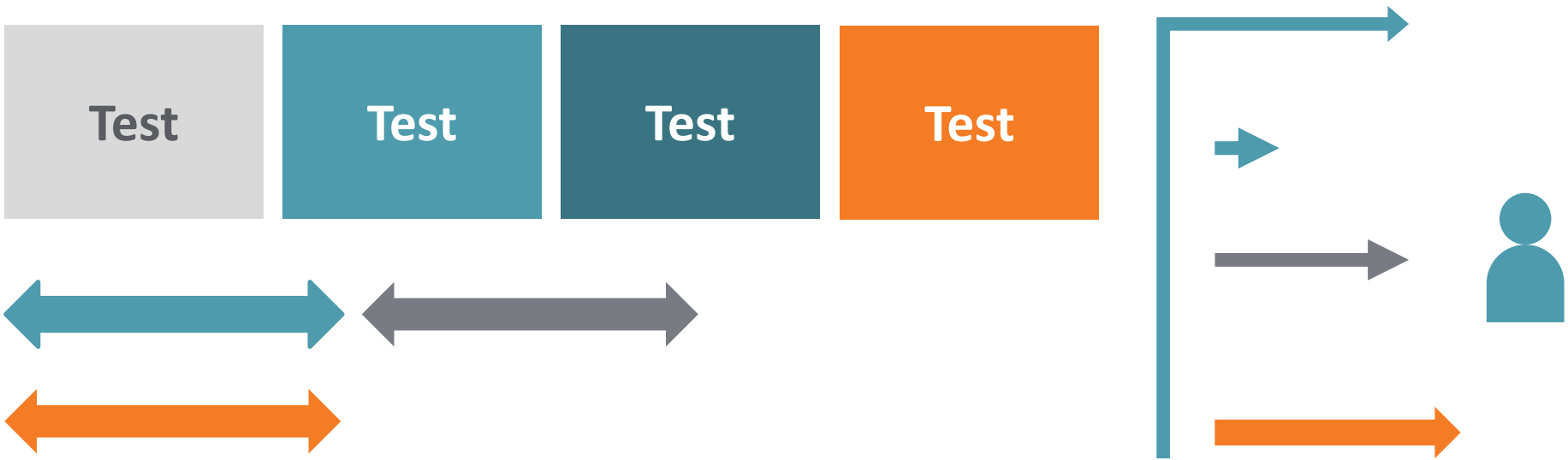
achelos GmbH
Vattmannstraße 1 | 33100 Paderborn | GERMANY
T +49 5251 14212-0 | info@achelos.de
achelos.de | IoT.achelos.com

achelos Farbpalette | Farbwerte Segmente

244 | 124 | 36	77 | 155 | 173	157 | 201 | 211	217 | 217 | 217	120 | 123 | 129	RGB

	security	health	mobility	public	IoT
RGB	244 | 124 | 36	185 | 24 | 24	0 | 179 | 255	148 | 193 | 30	33 | 48 | 91
HEX	f47c24	b91818	00b3ff	94c11e	21305b

Standardformen



- Verwendung der Formen ohne Schatten
- bei weißer Schrift im farbigen Kasten, Schrift OHNE Schatten hinterlegen
- Schriftart Calibri | Aufzählungszeichen: Quadrat -> achelos Orange

Verwendung der Piktogramme

Die Piktogramme lassen sich frei umfärben.
(Fülleffekt | Farbe auswählen)

Generic | achelos Services

Features 

Benefits 

Customer Value 

Knowhow 

Innovation 

Qualität 

Training 

Test 

Development 

Consulting 

Engineering 

Network and components

Server

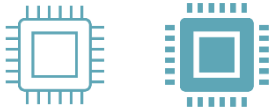
Datenbank

Cloud

WLAN

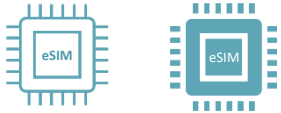
LAN

Testobjekt



SIM Karte

eSIM /
embedded SIM



Test suite

Devices

Mobile Phone

Arbeitsplatz Bildschirm

Tablet

Kartenleser

Smart Meter

People

Status and security

okay

nicht okay

Information

Achtung

Security Shield

Schloss

Schlüssel

Lupe

Fingerabdruck

www & Finance

www

Kreditkarte /$ / €

Umsatz

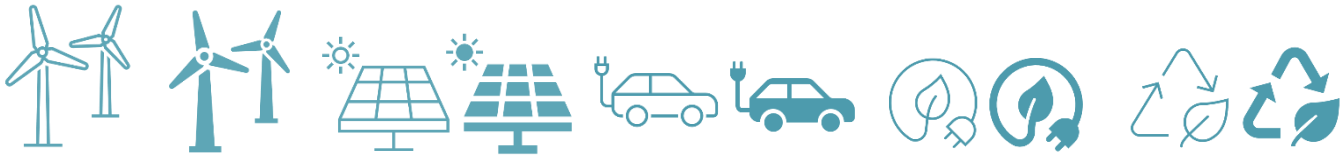
Unternehmen

Dokumente

Health & Energy

Krankenhaus / Praxis

erneuerbare Energie



Energie

Processes