Overview of major security trends

Jean-Pierre Tual, Gemalto VP Open Innovation

Nereid workshop, Athens, April 6th-7th , 2017

gemalto
security to be free

Global trends

- High Bandwidth Wireless World: **hyperconnectivity**
- Smart objects: phones, tablets, wearables: **mobility**
- Internet of Things / M2M: massive, **scalability**
- Cloud Computing : **Everything as a Service**
- Data explosion: **Big data, Analytics and AI**
- HW/SW Virtualization: **commoditization**
- Convergence IP and Telecom: **ubiquity**
- Open Source SW: **transparency**
- Security and privacy management: **key enabler for TRUST**

DIGITAL REVOLUTION

Digitization leads to a change of security model

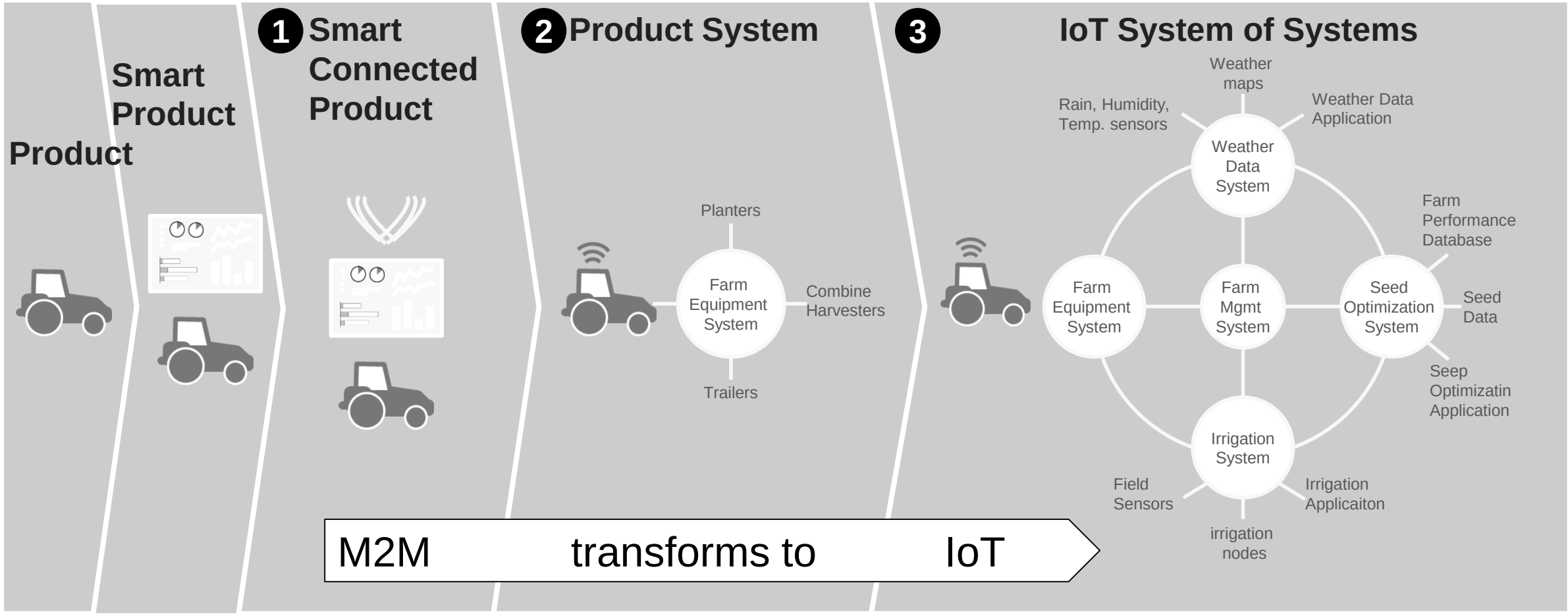
- Protected environment
- Trusted users
- Direct access to data

- Unprotected environment
- Non trusted users
- No direct access to data
- **Tamper resistant devices**

Classical security model (Server, PC,..)

Embeded security model (M2M, IoT,….)

IT goes M2M then IoT – a phase of business transformation



Prediction 2: Security tops the list of IoT concerns

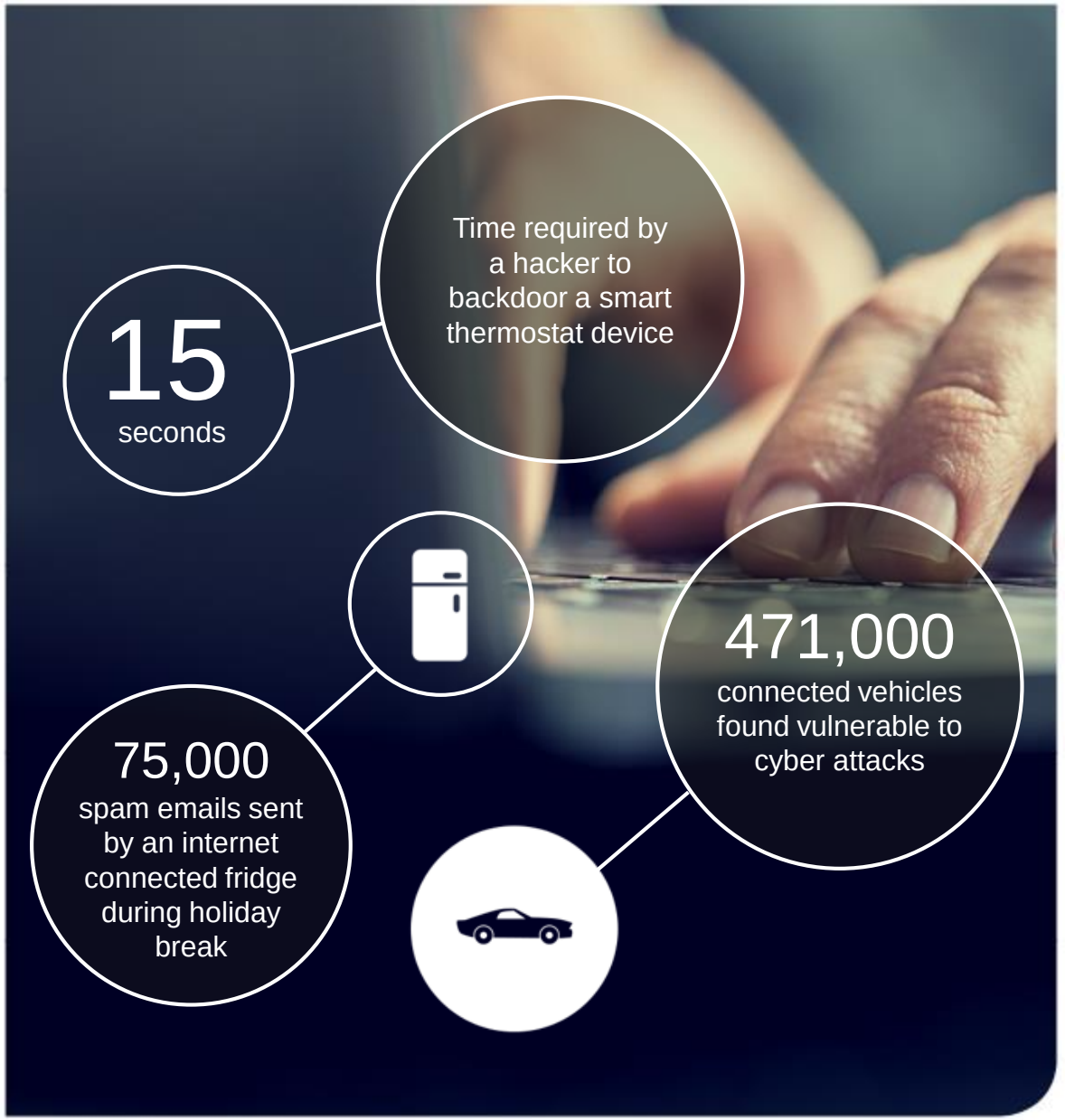
What are your firm's concerns, if any, with deploying M2M/Internet of Things technologies? *(All that apply)*

Base: 3627 global business and technology decision makers (20+ employees) in 7 online countries only

Source: Forrester's Global Business Technographics® Networks And Telecommunications Survey, 2015

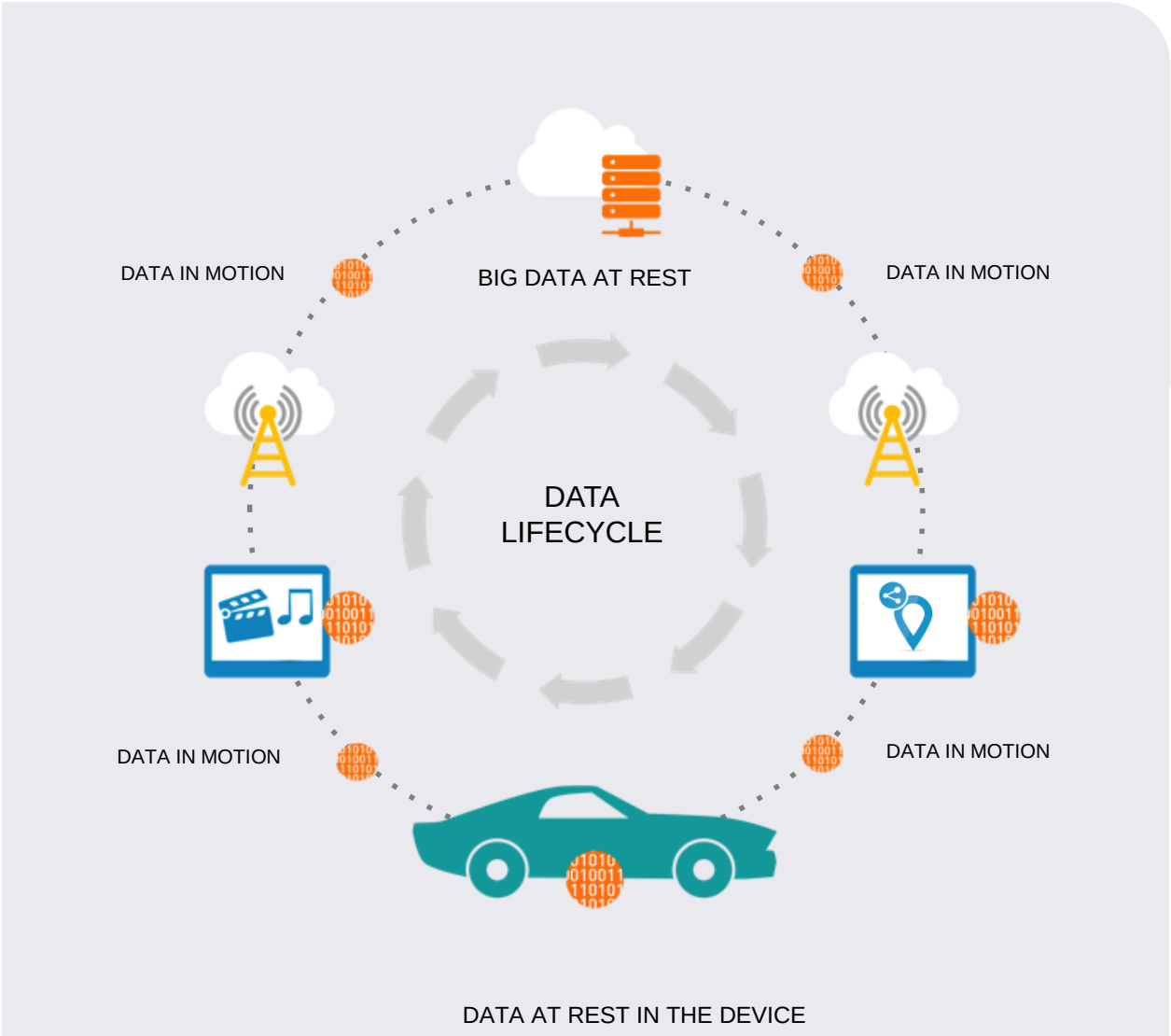
Authentication & Privacy is Critical

- Consumers and Enterprises only want authorized entities to have access to their devices or data
- Secure components and solutions must be embedded into “things” to protect data at rest and data in motion
- Hackers will take advantage, whenever there is a security loophole



Influx of Data in Connected Ecosystems

- Data is ***at rest*** in the device and in the cloud
- Or ***in motion*** between devices and the cloud
- The nature of data varies, such as vehicle location data or streamed media
- Which requires different levels of privacy and security



Three major dimensions to address in the future

Connect

> Out-of-the-box connectivity

> Multiple form factors

> Quality of Service

> Subscription Management

Secure

> Secure the device

> Secure the cloud

> Security lifecycle management

Monetize

> Flexible monetization

> Licensing and entitlement software

> IoT application upgrades

> Application Development

What is the (big) problem we have to solve ?

- Connected objects
  - Combination between massive IoT + local computing power + network connectivity => transformation of all connected object from our day to day live give birth to an un-precedented set of usages **and threats .**
  - **Mirai is just an appetizer!!!**
- Big-data issue
  - In 5 years time frame it will be possible to provision for analytics purpose about **~ PB of data in less than one hour**
  - Fine for legitimate organizations
  - **What does it imply for structured malevolent organizations or governments?**

Main Research Challenges

- On the device, service side
  - Solve the Secure, Connect, Monetize issue
- On the Big-Data side
  - Develop large, secure, scalable Big-Data platform efficiently coupled with massive IoT configuration
  - Algorithms and metrics to assess validity and veracity of data
  - Methodologies and tools for anonymization, privacy keeping, ethics preserving => Multidisicplinary approach for scientific foundations of Cybersecurity (including Human Sciences)
- On the BI/Analytics side
  - Increasing role of AI techniques: machine/deep learning, cooperative IA systems
  - New methods for managing IA systems/Security professional interaction
  - Availability of sharable massive Data Sets

Keep in mind: everything that can be hacked *will* be hacked !

Major issues with embedded systems

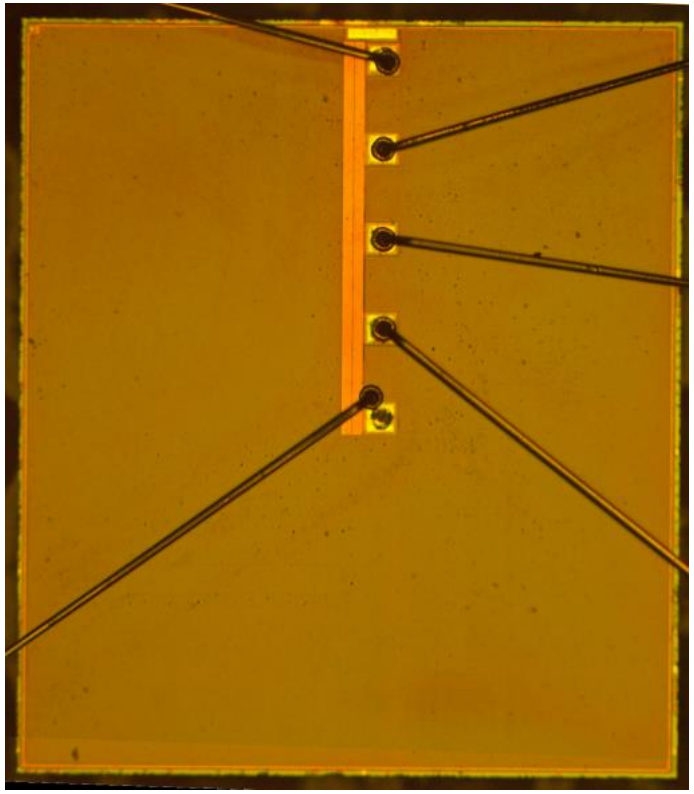
- Scalable architecture
- Remote management
- Long-life cycle
- Intrinsic Security
- Privacy
- Overall cost

Basic security technology building block in embedded security

- Smart cards / security elements (SE)
- TPMs and Hardware Root of Trust
- Trusted Execution Environment
- OTA servers
- Trusted service manager
- Device remote personalization

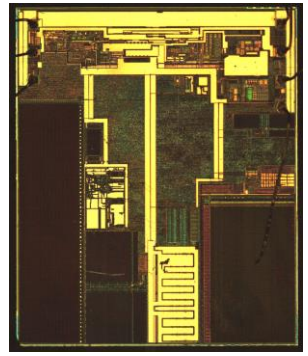
Tamper resistance at chip level

- Blocks can be easily identified
- No shield
- No glue logic
- Buses clearly visible



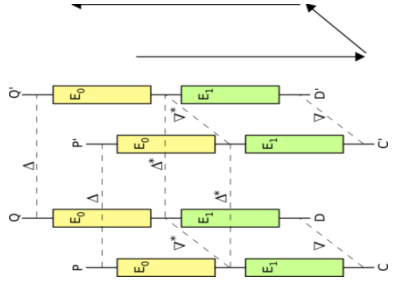
- Shield
- Glue logic
- No Buses visible
- Memories and buses encryption
- Sensors

Key challenges to address…



- Physical Attacks against secure tokens
  - Invasive probing
  - Reverse engineering
  - Fault injection
  - Side-Channel analysis
  - Relay attack

- Remote attacks against S/W applications
  - DoS – Denial of Service –
  - Man-in-the-middle
  - Sniffing
  - Spoofing
  - … by mean of virus, worm, buffer overflow, bug exploitation…

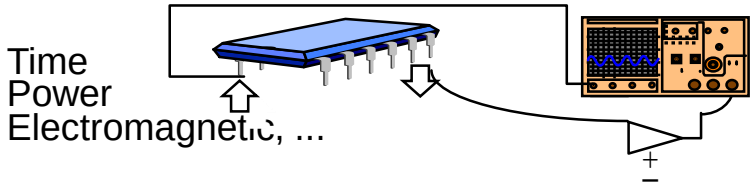


- Mathematical attacks against cryptographic protocols
  - Cryptanalysis
  - Brute force attack

Expected resistance to Physical and Logical attacks

Physical Attacks

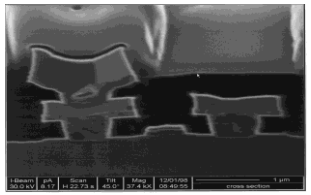
- **Side-Channel analysis***: Monitor analog signals on all interfaces and analyze:*



- **Fault injection***: use of Laser, Glitchers, Flash light…*

to bypass protections and infer secrets.

- **Invasive manipulation***:*
  - Chip observation
  - Deposit probe pads on bus lines
  - Reverse ROM mapping
  - Disconnect RNG
  - Cut tracks

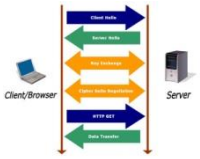


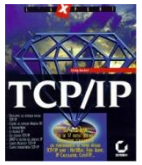
Logical Attacks

- **Aggressive software:** Buffer overflow, Aggressive applets, Trojan Horses, Viruses…

- **Investigate Servers, PCs, readers and handsets configurations:**

- **Scrutinize protocols and stack implementations:**

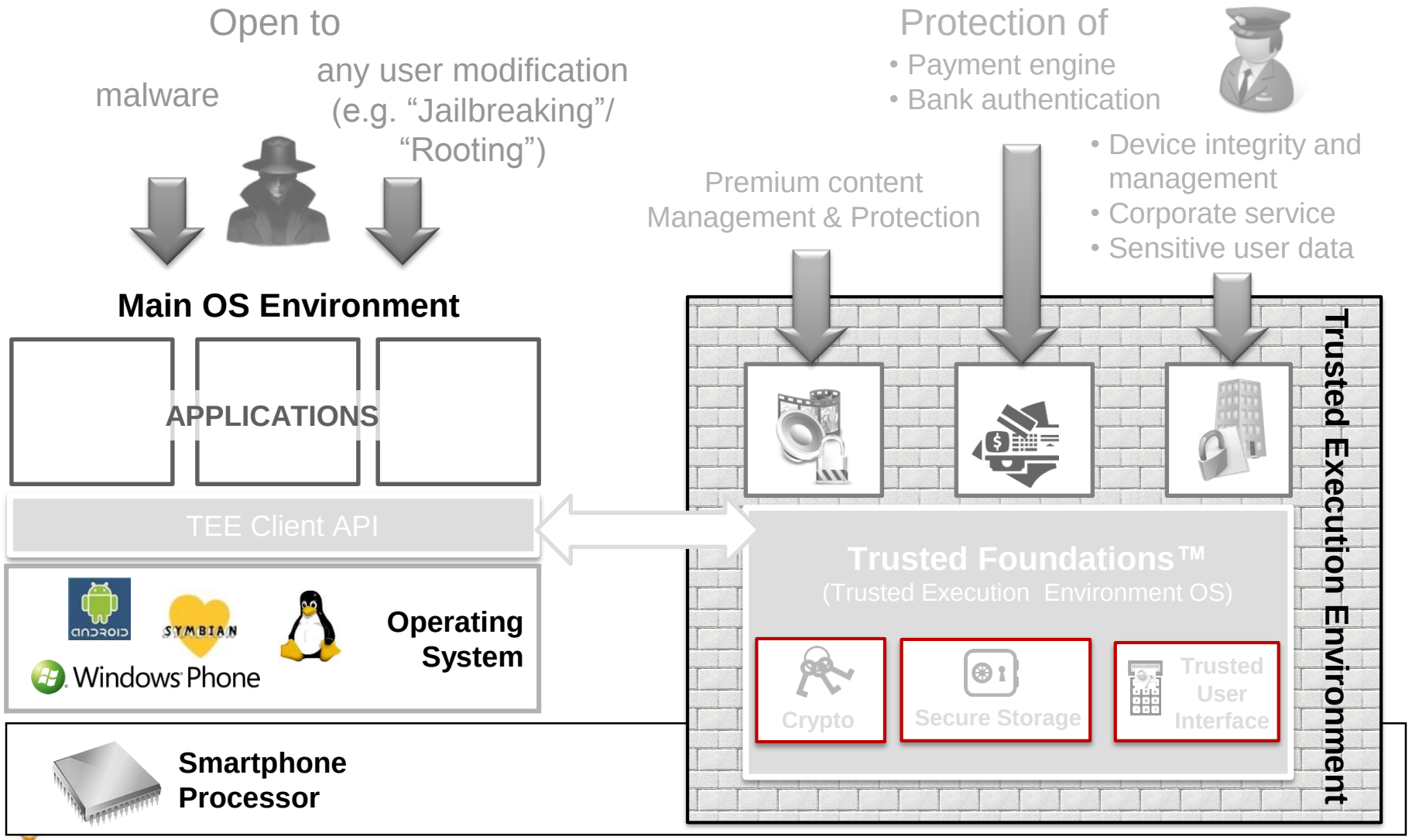




Impact on embedded SW components

- The software provisioning must to the following rules
  - Late personalization even after customer issuance
  - Full Remote update because the components are soldered/embedded and cannot be changed
  - Scalability of deployment schemes
  - Embedded local security
  - Long life cycle management (bugs and security patchs)
  - Flexibility according to the country and the field actors (late customization after issuance to the final customer
- Emerging concepts from the Mobile world can be customized on purpose
  - TEE
  - OTA
  - TSM

Enforcing Security: Trusted Execution Environment (TEE)



It’s important to find the right balance

- Secure Element
- Trusted Execution Environment
- Software

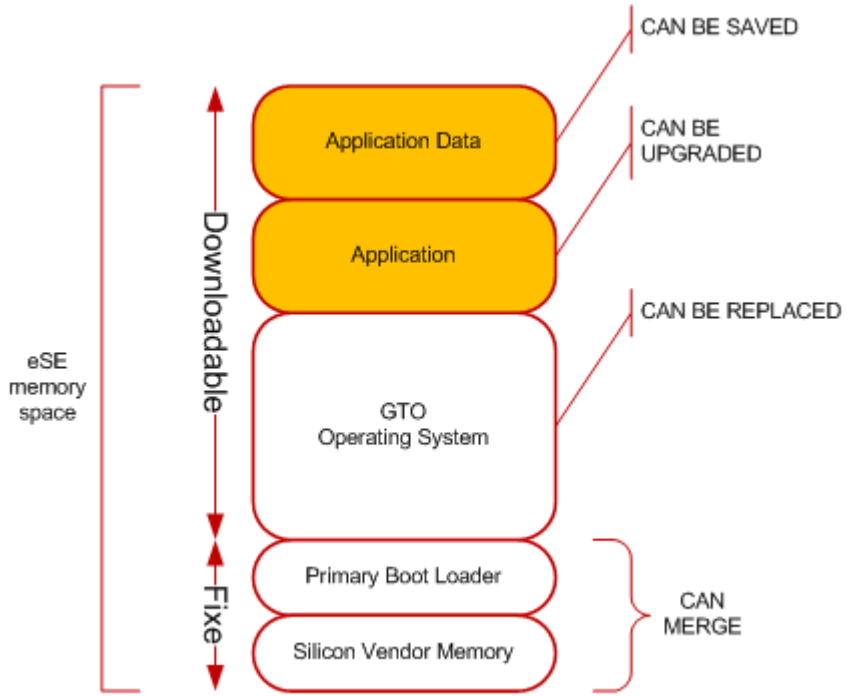
- Active Risk Managment
- Out of Band
- Tokenisation
- Security Firmware Upgrade

END-TO-END MOBILE NETWORK + SERVICE PROVIDER SECURITY FRAMEWORK

RISK

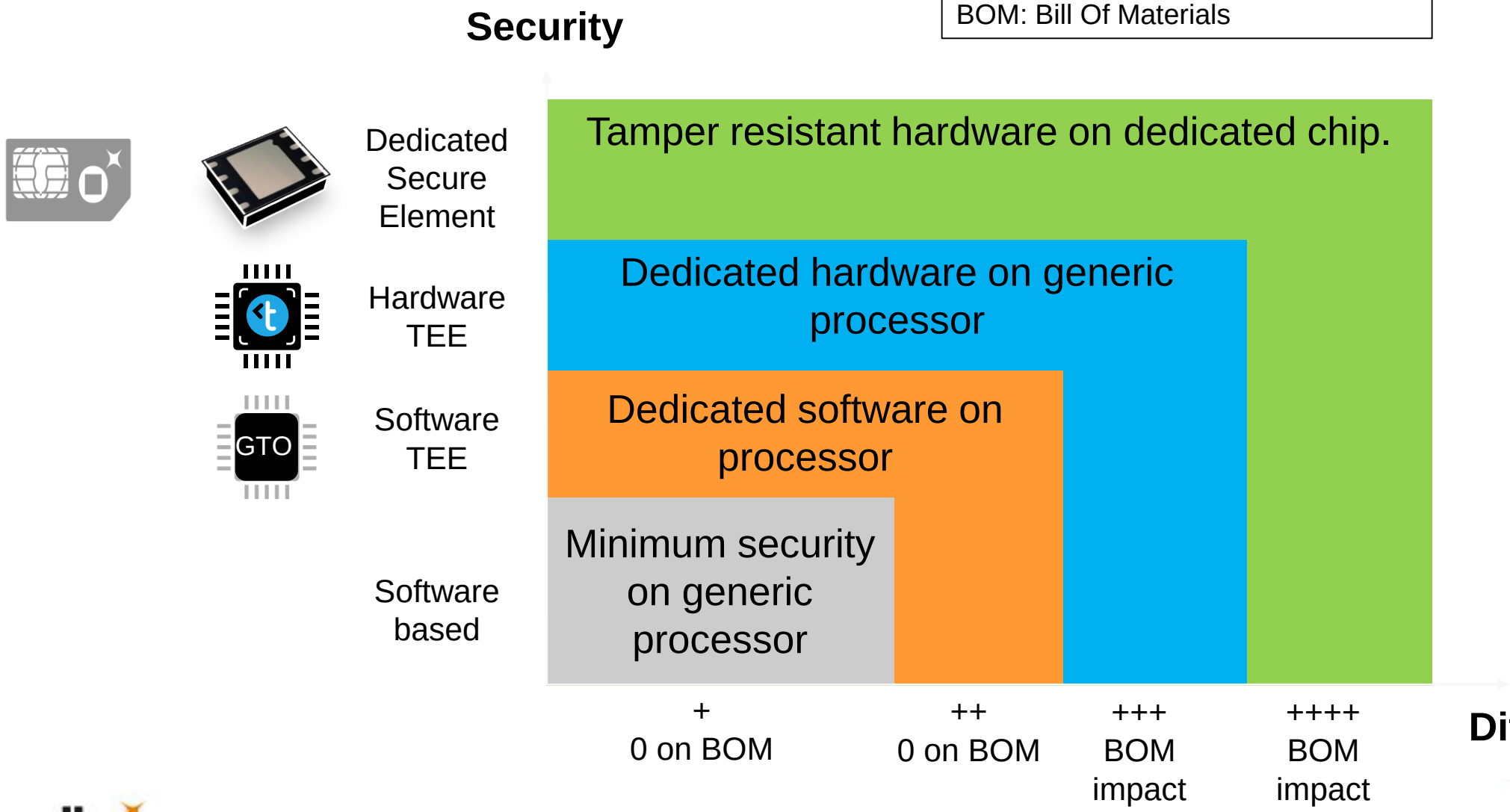
Full Remote Personalization

- Primary Boot Loader
  - Allow the downloading of the OS
  - Can be embedded into the silicon vendor dependent software
  - Can be generic (consolidated market)
  - Can be vendor dependent (fragmented market)
  - Independent of the OS
- Operating system
  - Market dependent
  - Bundled with the applications
  - Allow the application data saving (before OS upgrade)



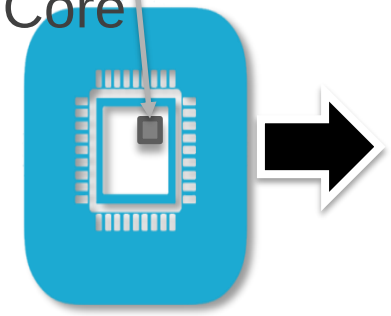
Embedded Security Choices (1)

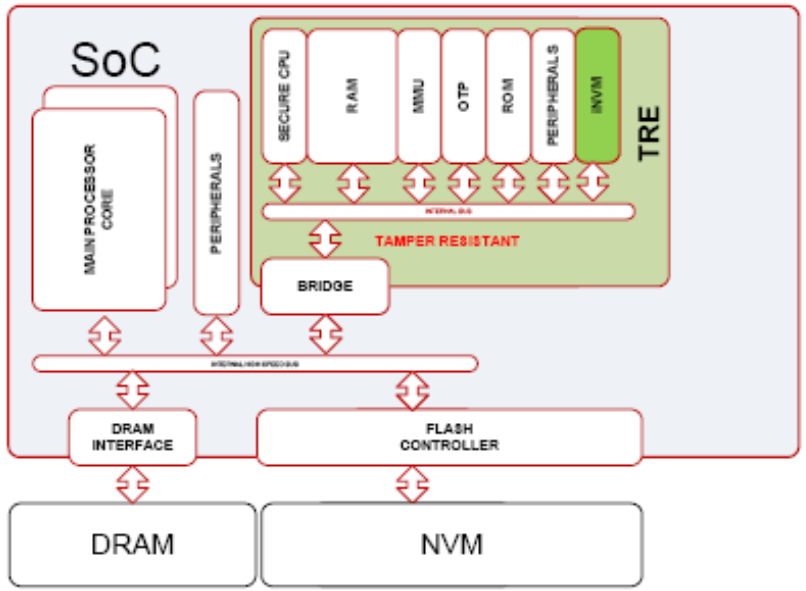
TEE: Trusted Execution Environment
BOM: Bill Of Materials



Alternative choice: Integrated Tamper Resistant Element

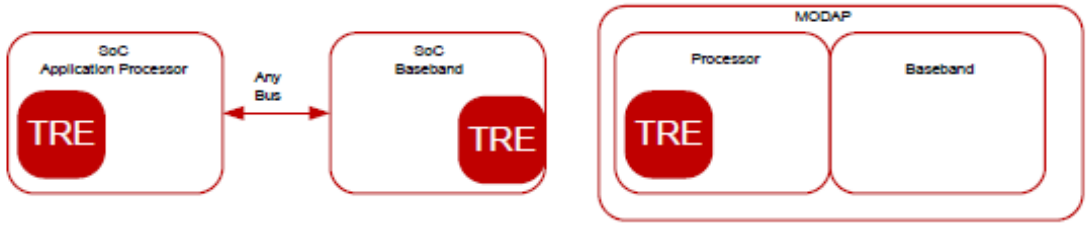
Embedded Secure Processor Core



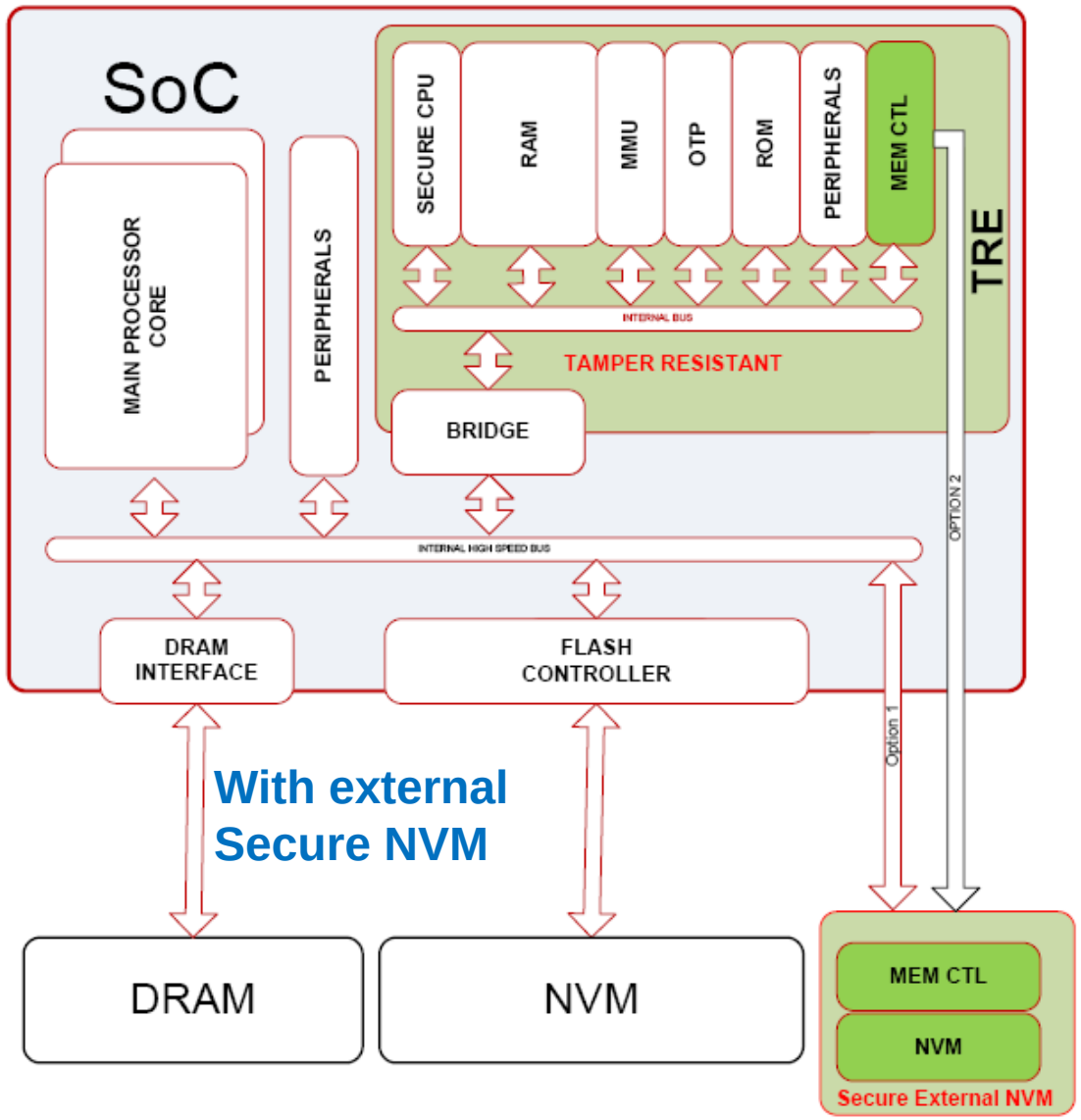


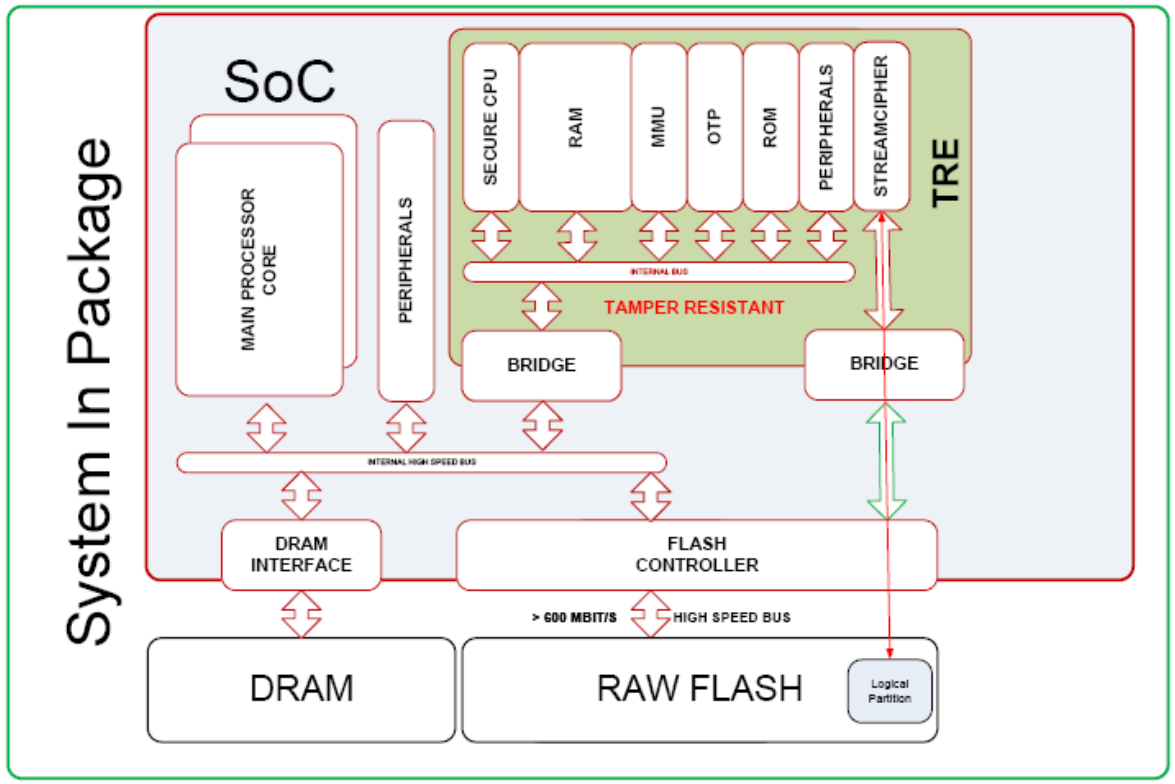
With internal NVM

- iUICC is an integrated TRE hosting a UICC firmware
- TRE can be integrated in any System on Chip as:
  - An Application Processor
  - A Baseband
  - …
- Neutral logical communication layer
  - For encapsulating legacy protocols
    - APDU
    - NFC HCP/HCI
  - Any new or application dependent protocols
- dedicated hardware resources
  - The TRE has its dedicated :
    - RAM, ROM
    - Secure Processor Core
    - Channel of communication
  - The TREE may share:
    - NVM



Alternative choice: Integrated Tamper Resistant Element (2)





With in package NVM

Cçomparison of ITRE architectures

		Architecture			
	Properties	Internal NVM	External NVM	In-Package NVM	Secure NVM
	Confidentiality during storage	Crypto	Crypto	Crypto	Crypto
	Confidentiality during transfer	Crypto	Crypto	Crypto	Crypto
	Authenticity during storage	Crypto	Crypto	Crypto	Crypto
	Authenticity during transfer	Crypto	Crypto	Crypto	Crypto
	Anti-rollback protection/Anti replay	In-die	-In-die + crypto	In-package	In-die
	Perfect Forward Secrecy	In-die	-In-die**	In-package	Crypto
	Denial of Service attack	Best efforts*	Best efforts*	Best efforts*	Best efforts*

Technology choices- 2020-2022 time Frame

- For Autonomous TRE
  - 40 nm CMOS with Embedded Flash or better MRAM (2020)- 28 nm in 2022 ?
  - Price identical to today's 65 nm generation
  - External additional Ciphered Non Volatile Memory with PUF link
- For integrated TRE
  - 10 nm CMOS in 2020 – 8 nm in 2022?
  - Is it imaginable to have an internal NVM?
  - L2 RAM (~2 MB) cache containing the image of the TRE
  - External memory enciphered (Flash)
  - Some Hardwired co-processors inside (AI, Crypto,…)

gemalto
security to be free

Thanks for your attention !