Security for IoT
Landscape and trends

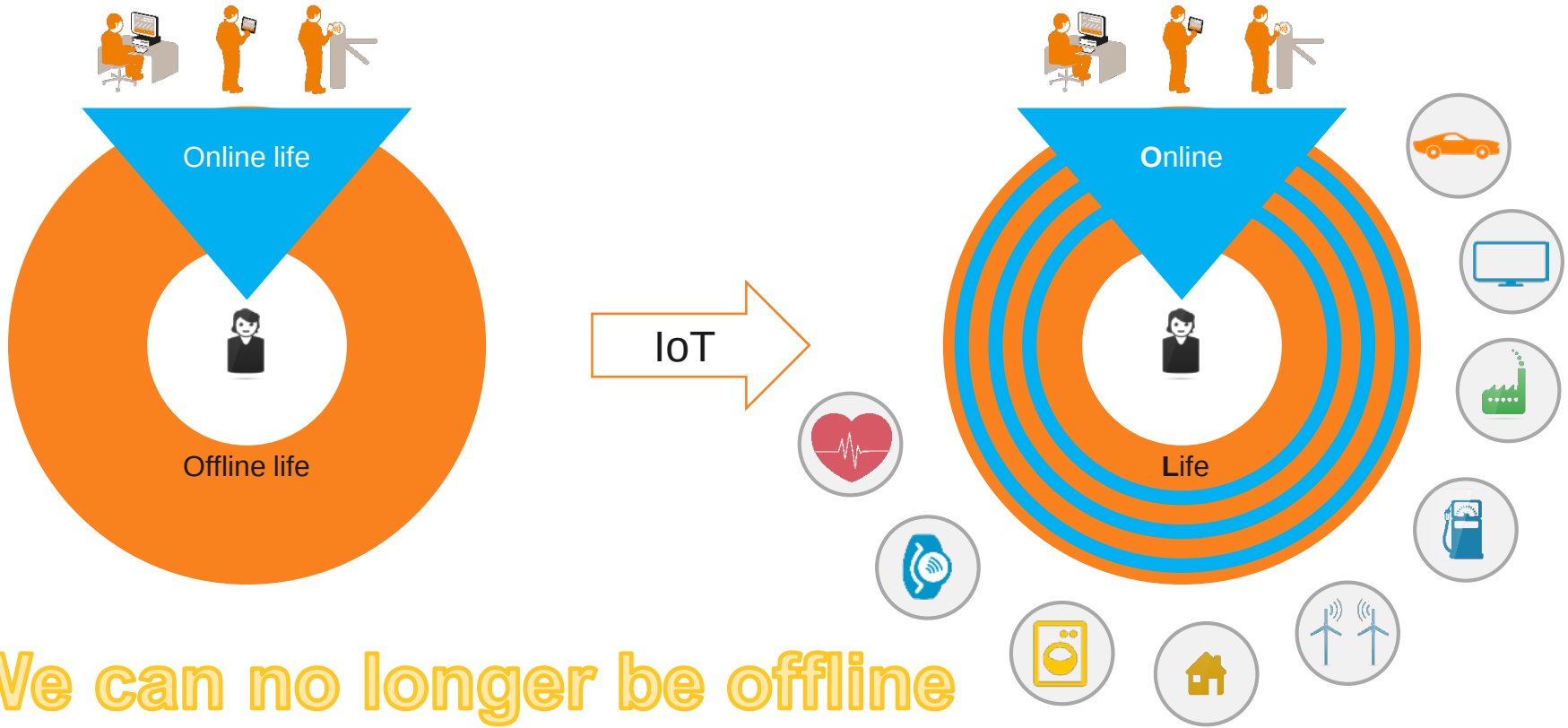
gemalto
security to be free

Pierre Girard
Lugano, November 13, 2017

How Gemalto brings trust into the IoT space

What is IoT?

Moving from the Internet of Men to the Internet of Things



We can no longer be offline

Agenda

- Why do we need IoT?
- Zoom on networks and LPWAN
- Trends in security solutions: integration and resilience
- Challenges ahead

Is there a good reason to hook things to the Internet?

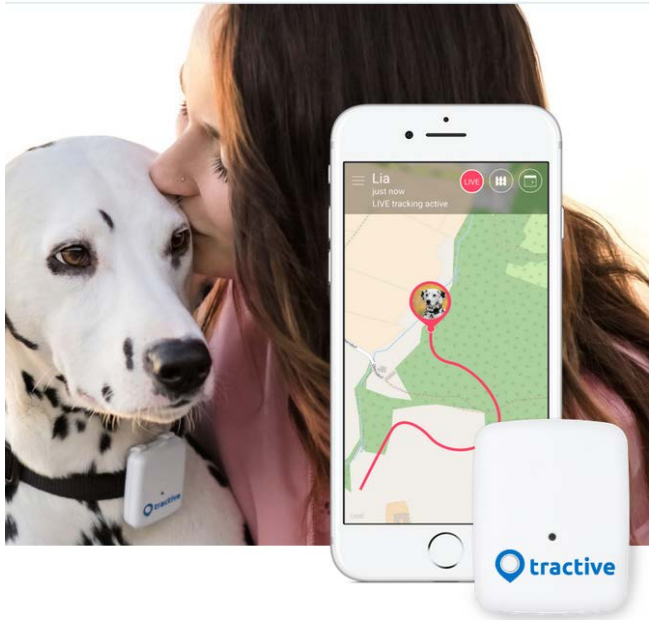
If No

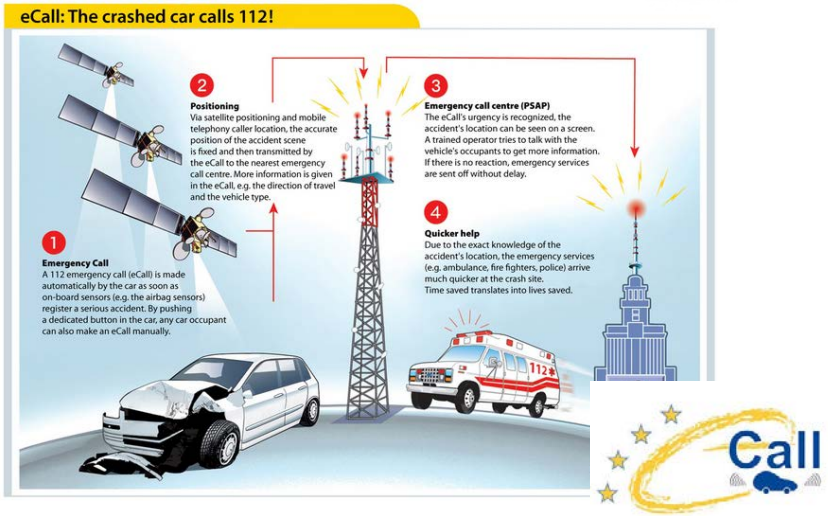
No value, no budget for security

If Yes

Well, we'll see …

Reason #1: Bringing new features

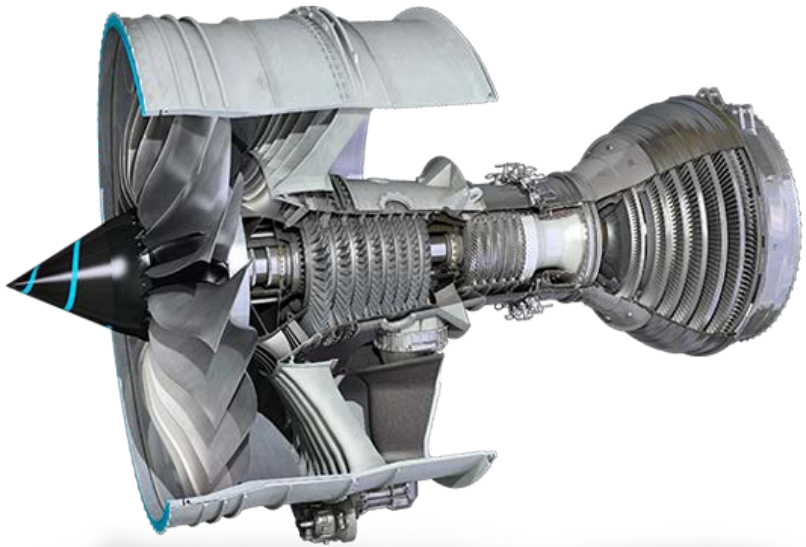




Reason #2: optimize

Reason #3: new business model

Reason #4: data collection



Why do we need trust in IoT ?

- Management of sensitive devices
  - Valve, pump, door, engine, …
- Management of sensitive transactions
  - Energy: (not) producing, (not) consuming, storing …
  - X as a Service: cleaning, manufacturing, flying, driving …
- Management of sensitive data
  - Location / presence, behavior / consumption patterns, …

IoT will redefine your business model …

… and you want to protect it !

Some constraints for IoT security

- Low cost
- High integration
- Low power consumption
- Extended life time
- Unattended
- Working 24/7

- Laaaarge scale

Consumer

Industrial

Agenda

- Why do we need IoT?
- Zoom on networks and LPWAN
- Trends in security solutions: integration and resilience
- Challenges ahead

Is there a common technical architecture ?

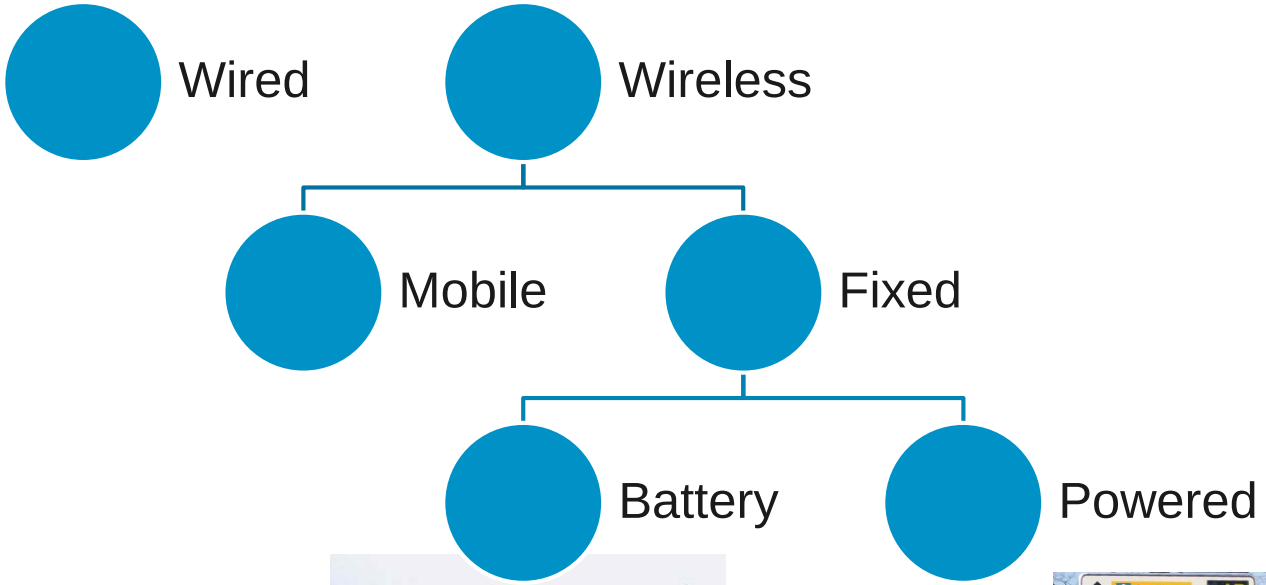
1 bit per ?

LTE Advanced Pro 600 Mbps

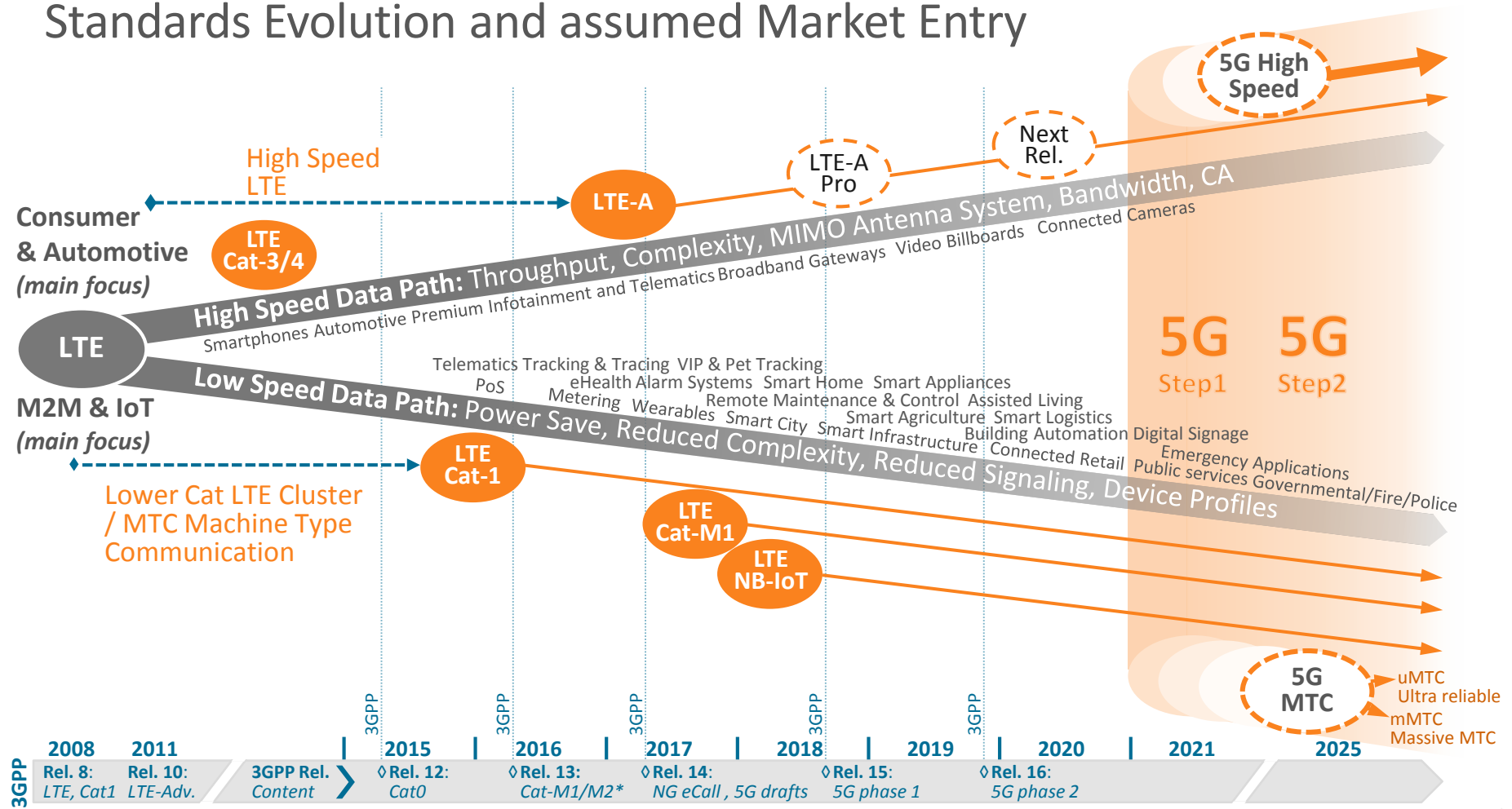
Heterogeneous networks for IoT

- Classical IT networks
  - Ethernet, Wifi, ADSL, …
- Classical GSM family
  - Start to be fragmented as well
- LPWAN
  - LoRa, Sigfox, Neul, …
- Specific / capillary / field bus …
  - CAN bus, Zwave, Thread, Modbus, PLC, …

Network typology for IoT



Standards Evolution and assumed Market Entry



gemalto

Two major LPWAN contenders

- Technology designed by Cycleo and acquired by Semtech, designing LoRa chipsets or selling techno IP
- **Strategy**: building Large ecosystem through LoRa Alliance and leverage MNO desire to use LPWAN for low cost low power use case while no equivalent 3GPP techno available.

- All integrated player
- Royalty free for devices
- Network subscription model
- **Strategy**: become the LPWAN leader thanks to deployment speed and global footprint

Key drivers for LPWAN solutions

Low cost

Low power consumption

Deep indoor penetration

Mission profile for LPWAN devices

- Battery powered
- Long life in the field
- Low data usage, mostly uplink
- Non critical

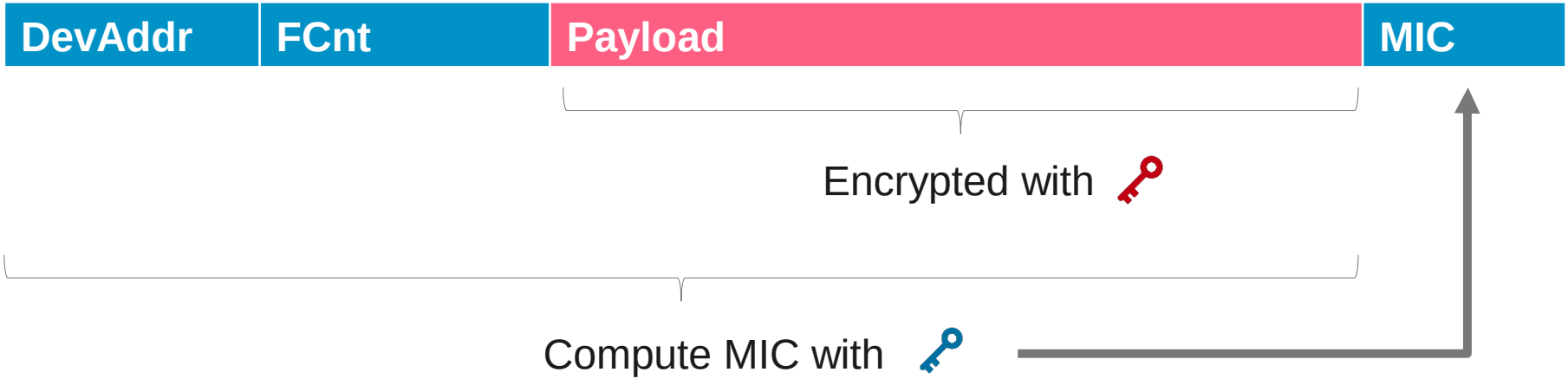
Main security requirements for LPWAN

- Device / network mutual authentication
- End-to-end applicative level security

Business as usual ?

Requirements	WAN	LPWAN
Mutual auth.	 + AKA	Too costly Too much power
E2E sec.	  + TLS	Too costly Too much power

LoRaWAN 1.0 frame content for payloads



: AES 128 bits keys derived from device unique AES key (once or almost !)

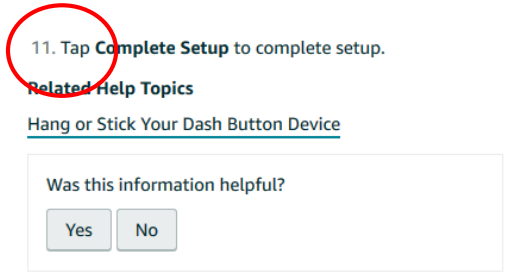
How to provision the keys ?

This …

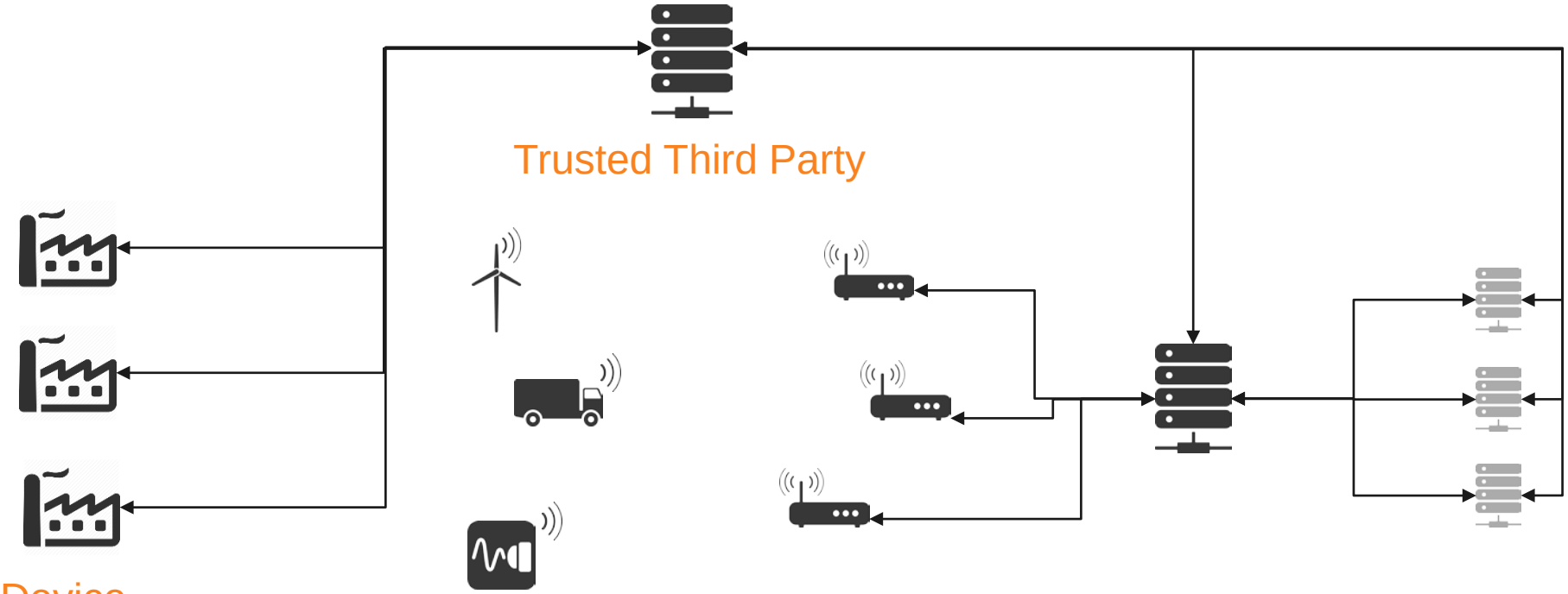
… is not an option

Industrial constraints in LoRa deployments

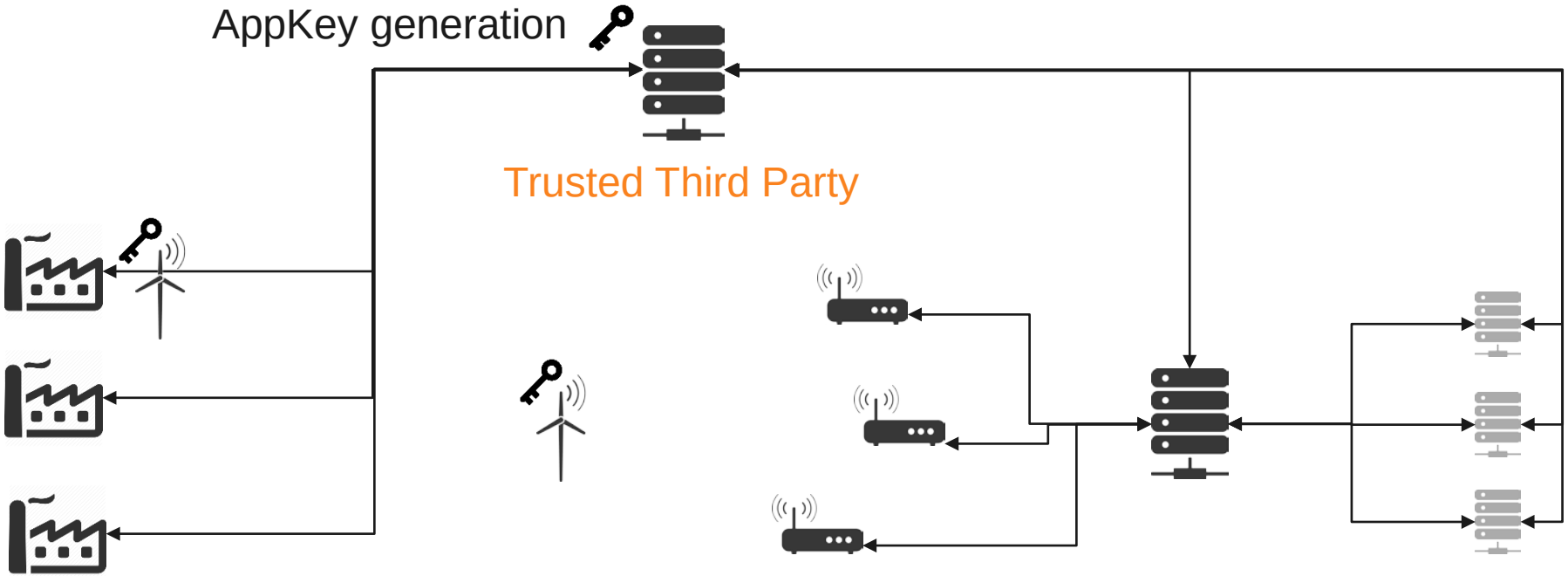
- Millions of generic devices will have to be manufactured
  - Flashed with their unique AppKey
  - Without knowing the final network
- Device manufacturers do not want to bother with keys
  - Flash and forget approach
- Users do not want to bother with security settings



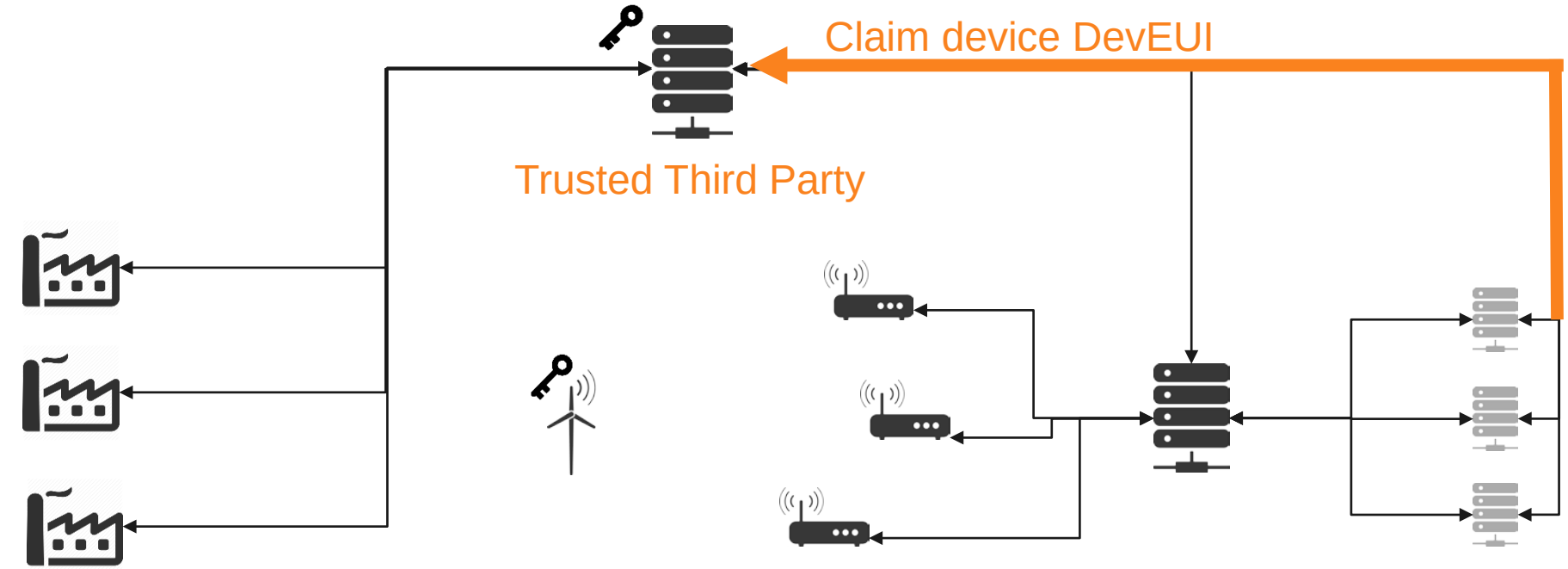
Introduction of a Trusted Third Party for LoRa 1.0



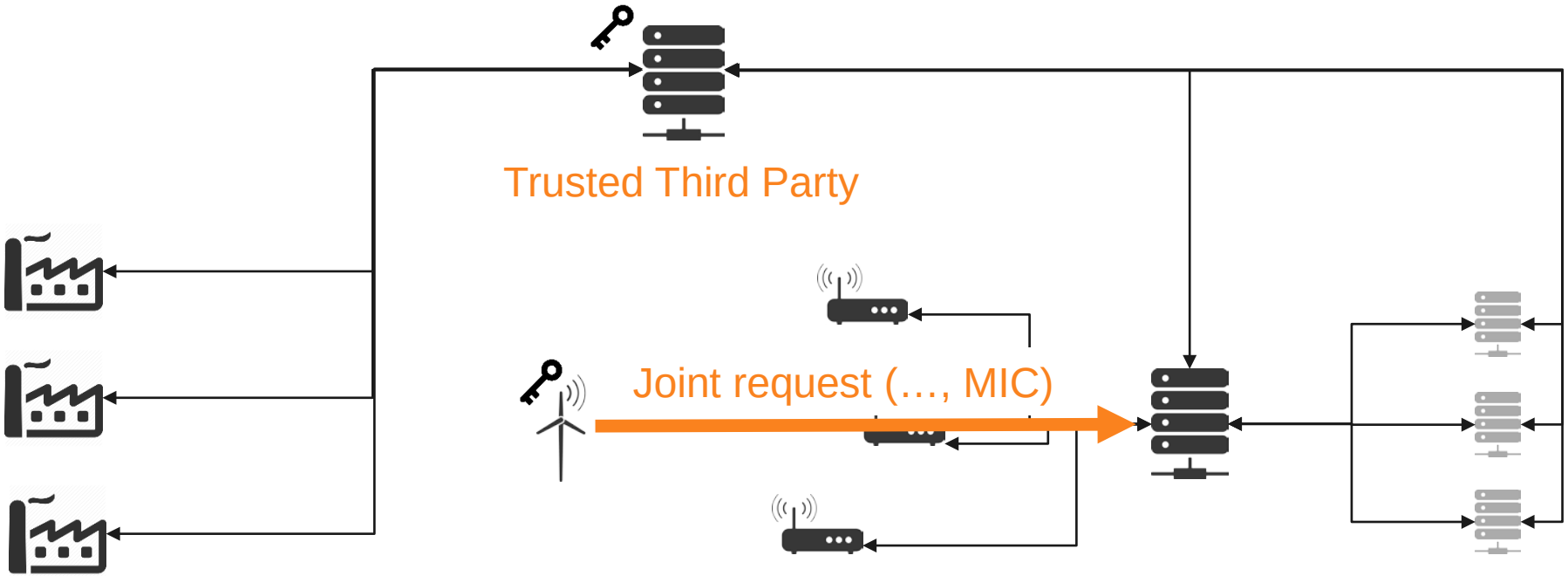
Device provisioning



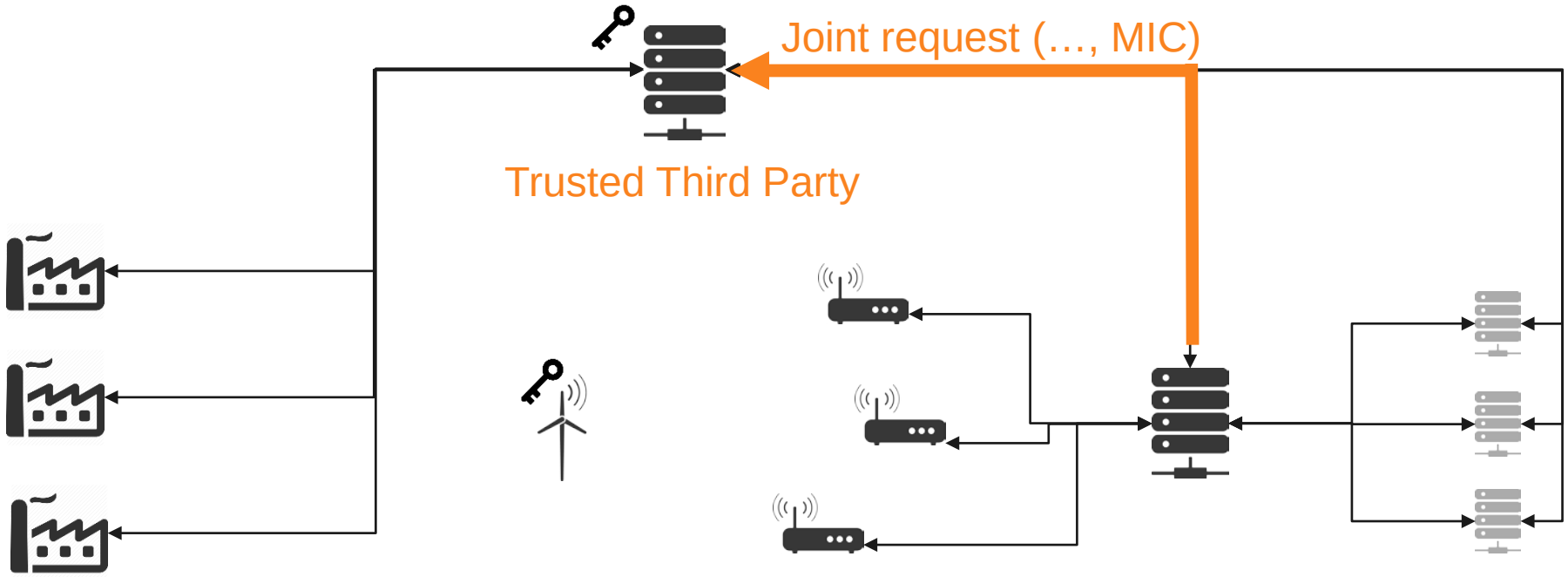
Device claiming



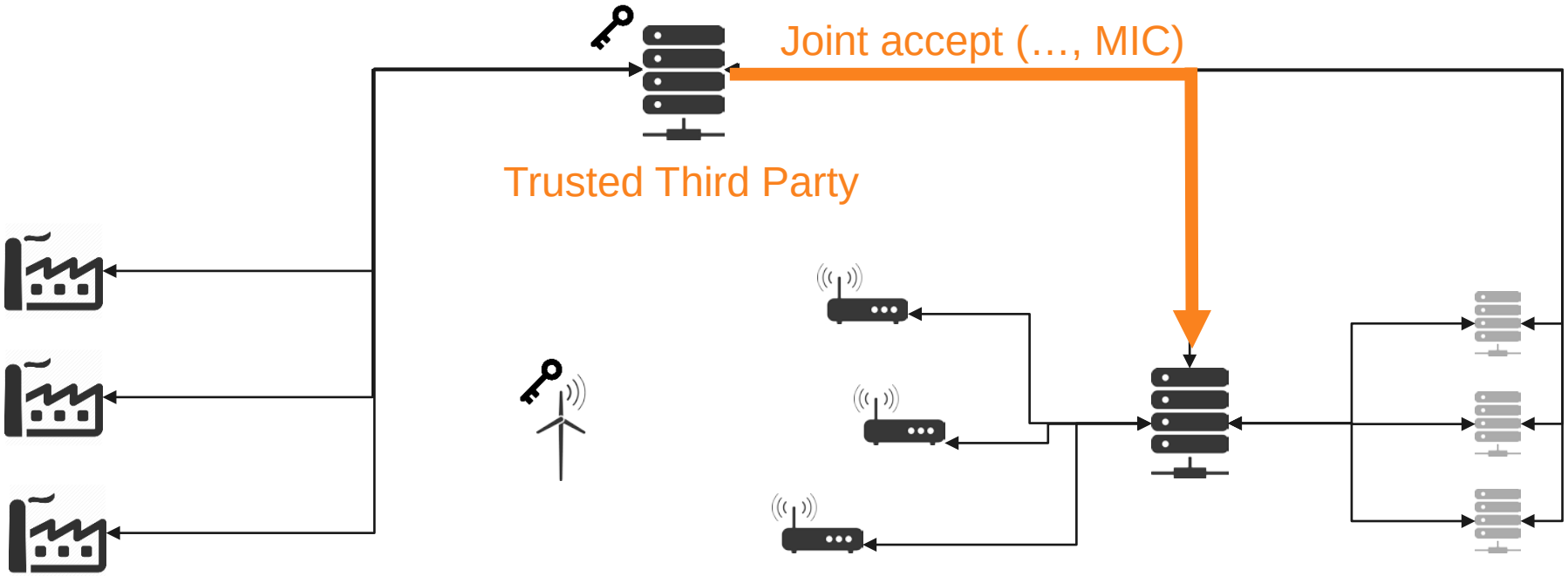
Network connection



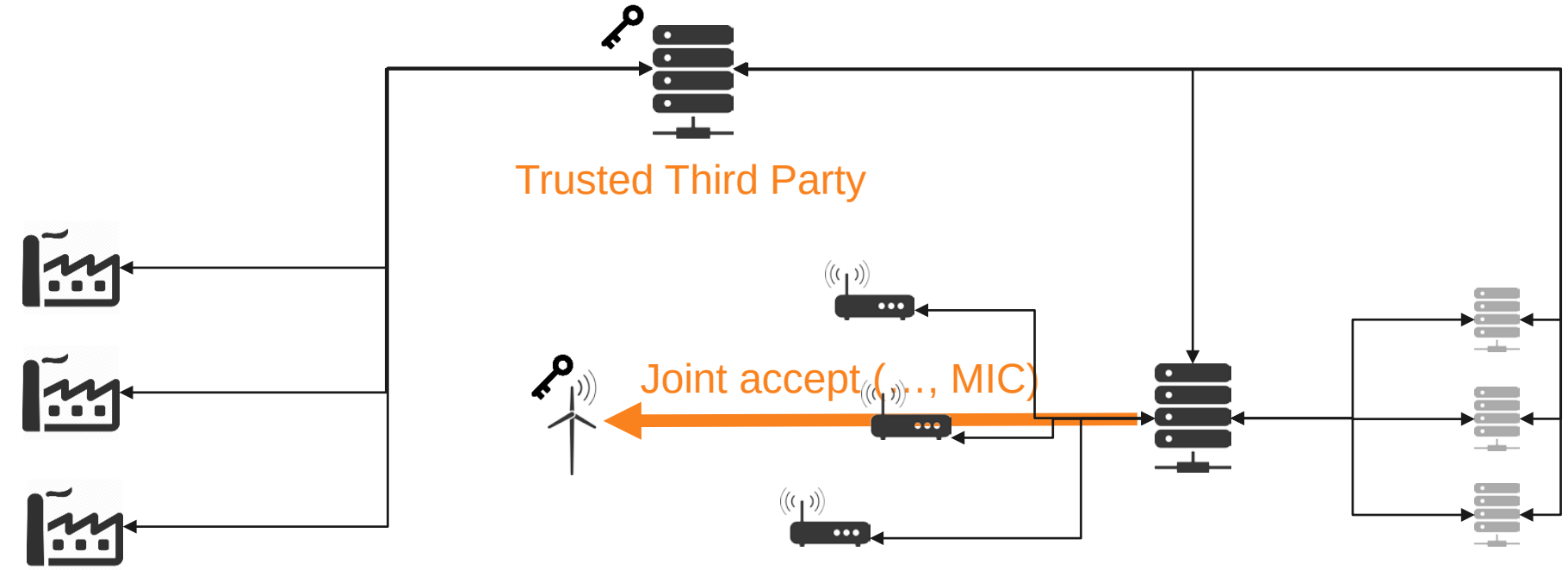
Network connection



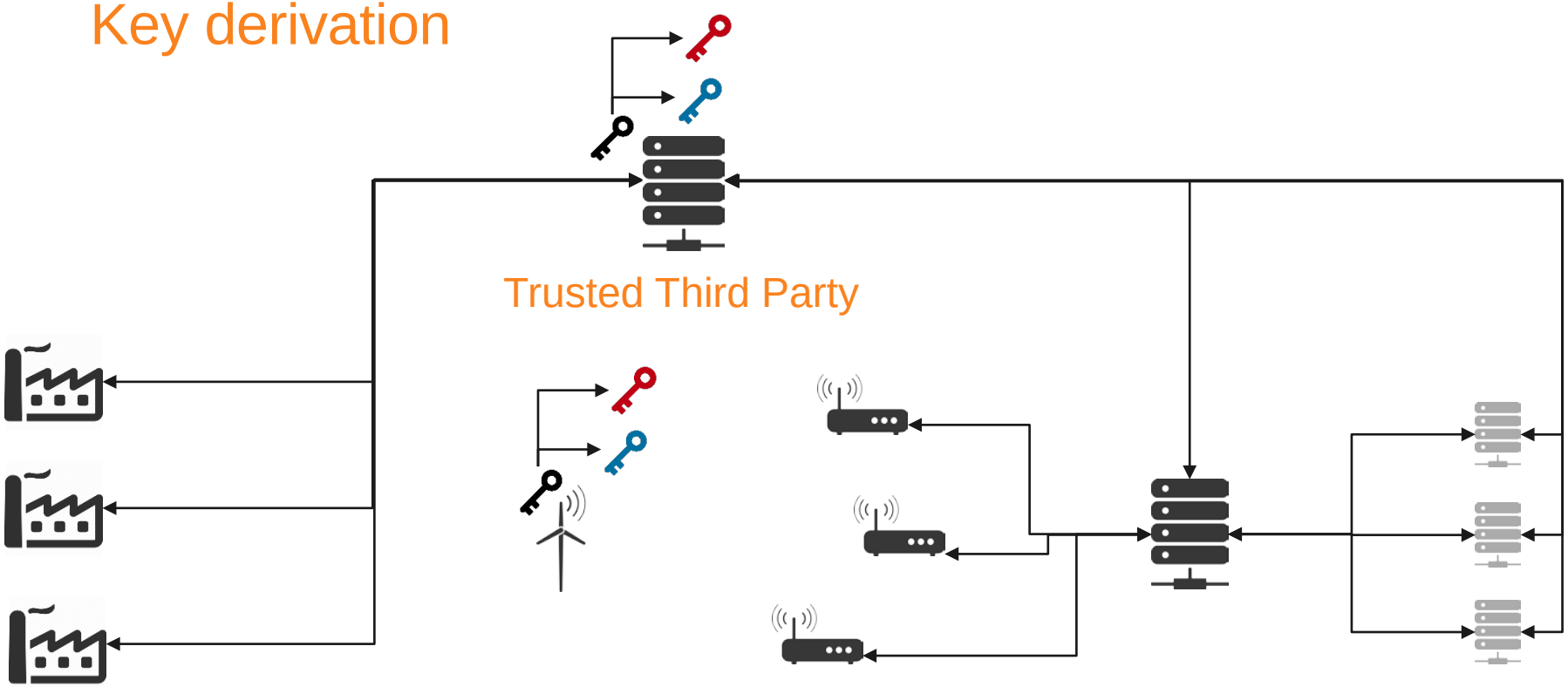
Network connection



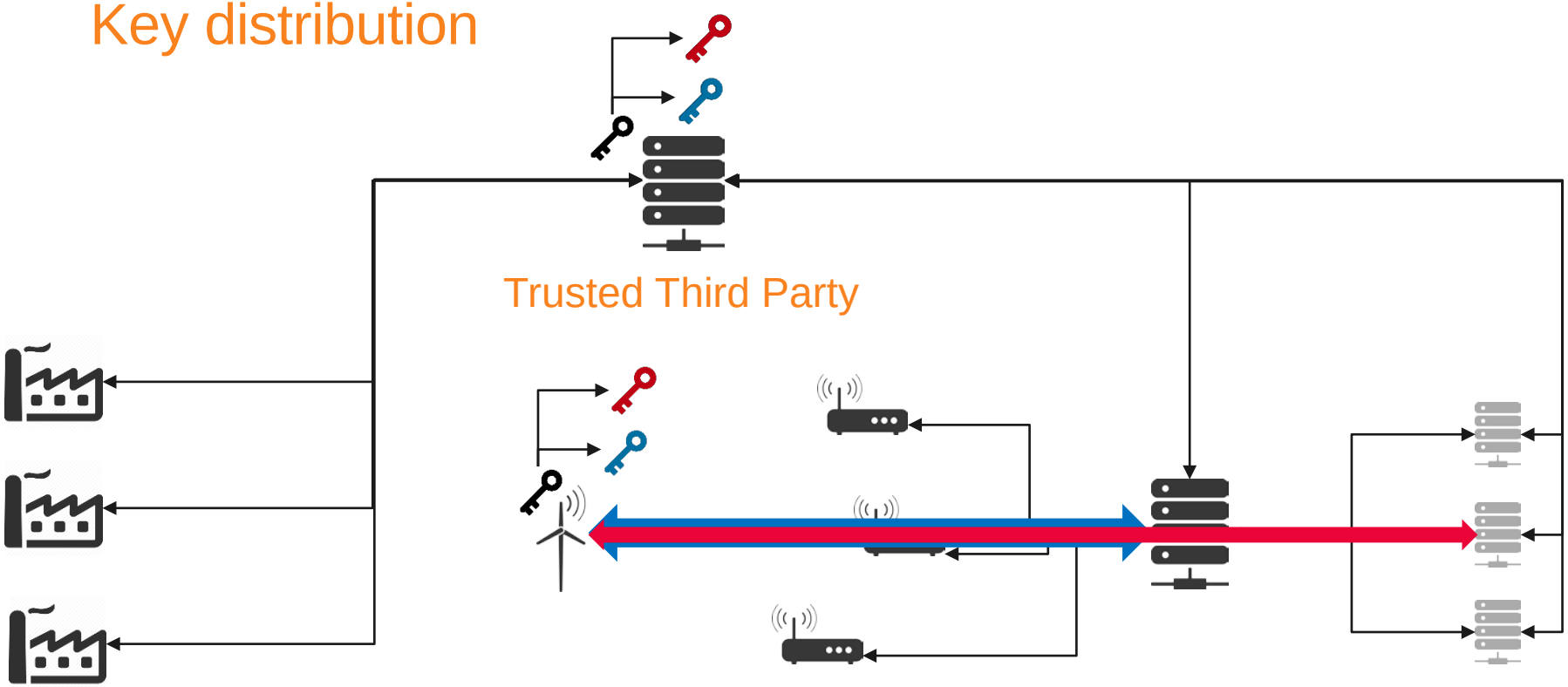
Network connection



Key derivation



Key distribution



Agenda

- Why do we need IoT?
- Zoom on networks and LPWAN
- Trends in security solutions: integration and resilience
- Challenges ahead

Security services and mechanisms (from ISO)

- Services
  - Confidentiality
  - Integrity
  - Authentication
  - Access control
- Mechanisms (on device)
  - Secure boot
  - Encrypted File System
  - Secure communication
    - Encryption / integrity
    - Mutual authentication

Will need credentials

How to store and process them securely ?

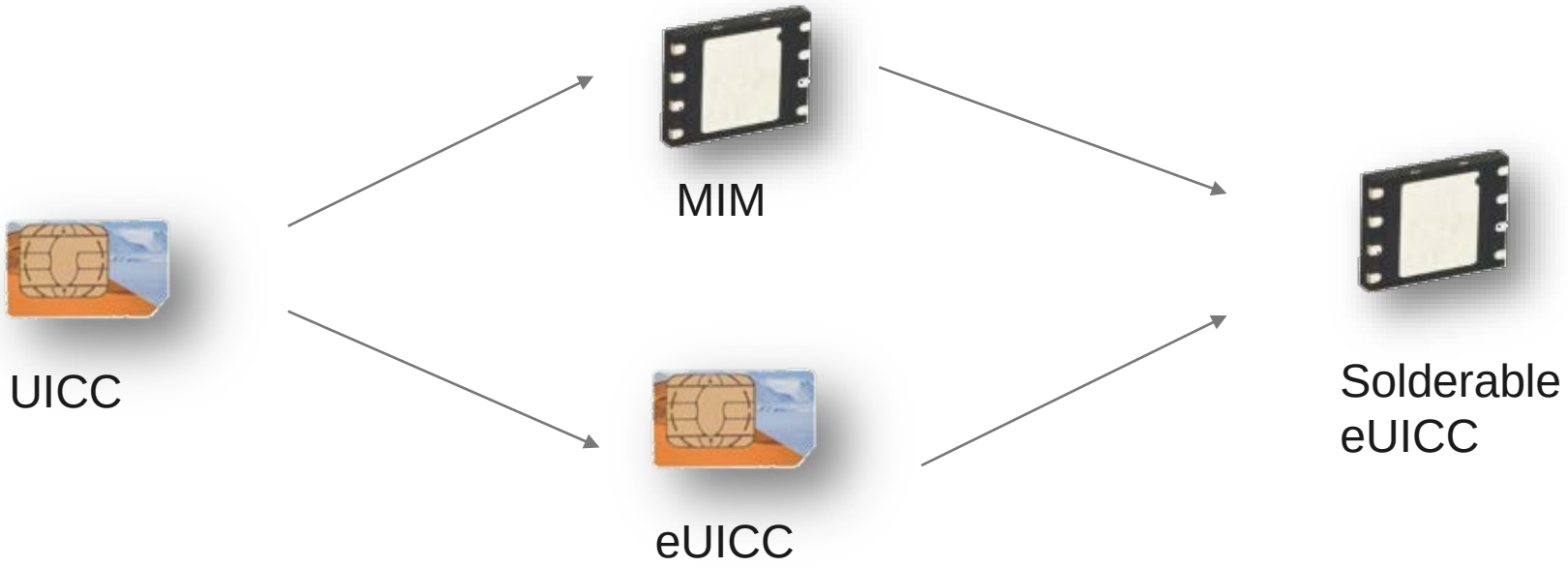
Classical IT solutions

Unsecure environment

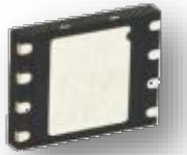
Secure environment

- Tamper resistant
- Managed
- Highly tested
- Certified

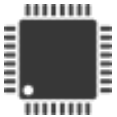
SIM for IoT



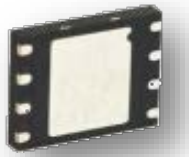
Recent evolutions of the SIM for IoT



Solderable
eUICC

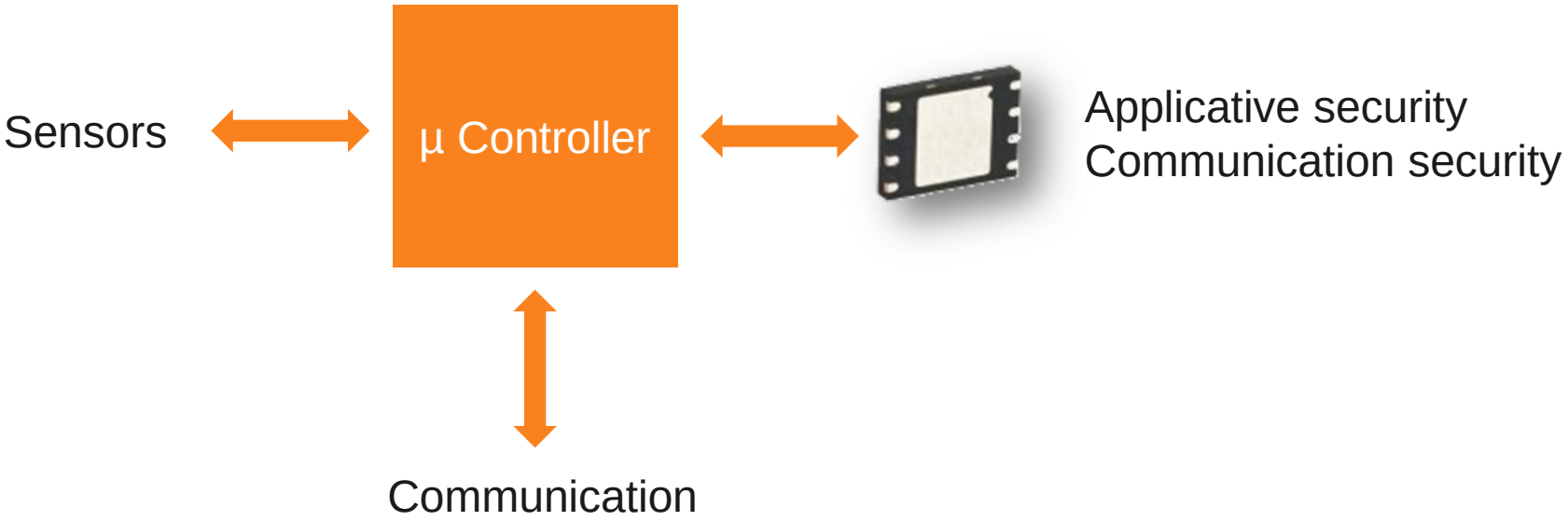


Secure Element
e.g. TLS client authentication



Multi-applicative
eUICC

Discrete component approach for LoRa



Example for LoRa device: MultiTech / Gemalto

MultiTech Introduces Cost-Optimized, Secure LoRaWAN Module

Press Release

February 23, 2016

Mounds View, MN – February 23, 2016 – Multi-Tech Systems, Inc., introduced the MultiConnect® xDot™, a secure endpoint module to communicate over LoRaWAN™ networks.

The xDot joins the MultiTech family of LoRaWAN communications devices which also includes the programmable MultiConnect® Conduit™ gateway, MultiConnect® mDot™ modules and MultiConnect® mCard™ gateway accessory cards. This latest addition to the LoRa™ product line features a compact, surface-mount form factor, mbed enabled tamper proof processor and very low power consumption for extended battery life.

For enhanced security, the xDot incorporates a hardware tamper resistant secure element from Gemalto, the world leader in digital security, which delivers secure key storage for AES-128 encryption used in LoRaWAN networks as well as secure applications capabilities.

Internet of Things World

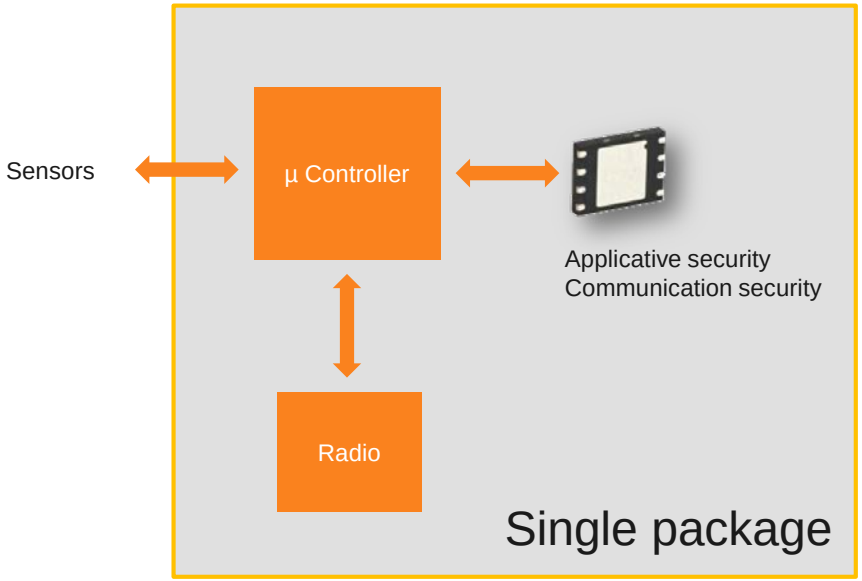
May 10, 2016

If you want to see how MultiTech is leading the way in IoT using the industry's most comprehensive LoRa® enabled products, we can show you here:

Gemalto (Booth #412) :See the MultiConnect® Conduit™, working with MultiConnect® mDot™ -a LoRaWAN™ ready, LPWAN RF module, and MultiConnect® xDot™ -a secure endpoint module to communicate over LoRaWAN networks. The products demonstrate how security is provided to LoRa networks

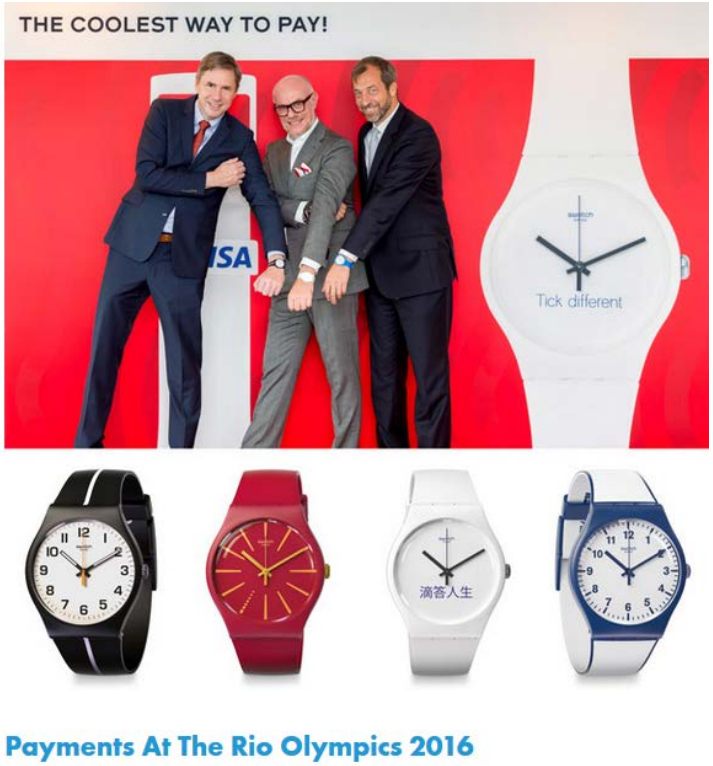
gemalto

Toward more integration: system in package

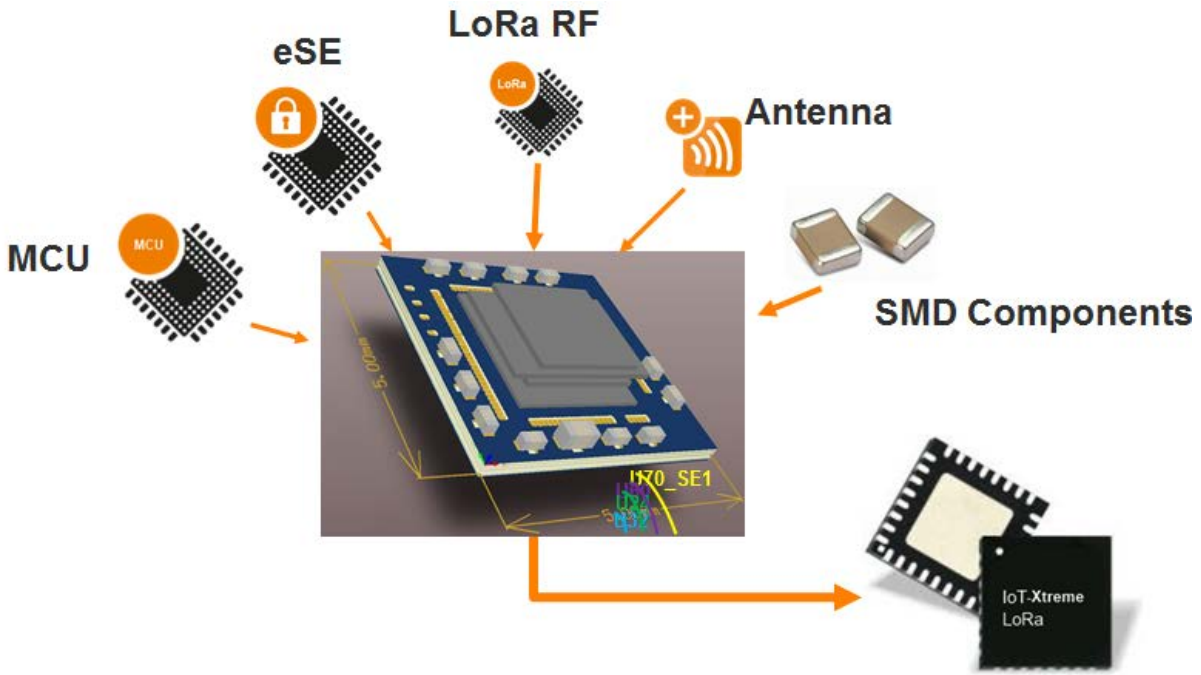


- Better integration
- Better TTM
- Lower cost
- Enhanced security

Example for payment: Gemalto at Rio Olympics 2016



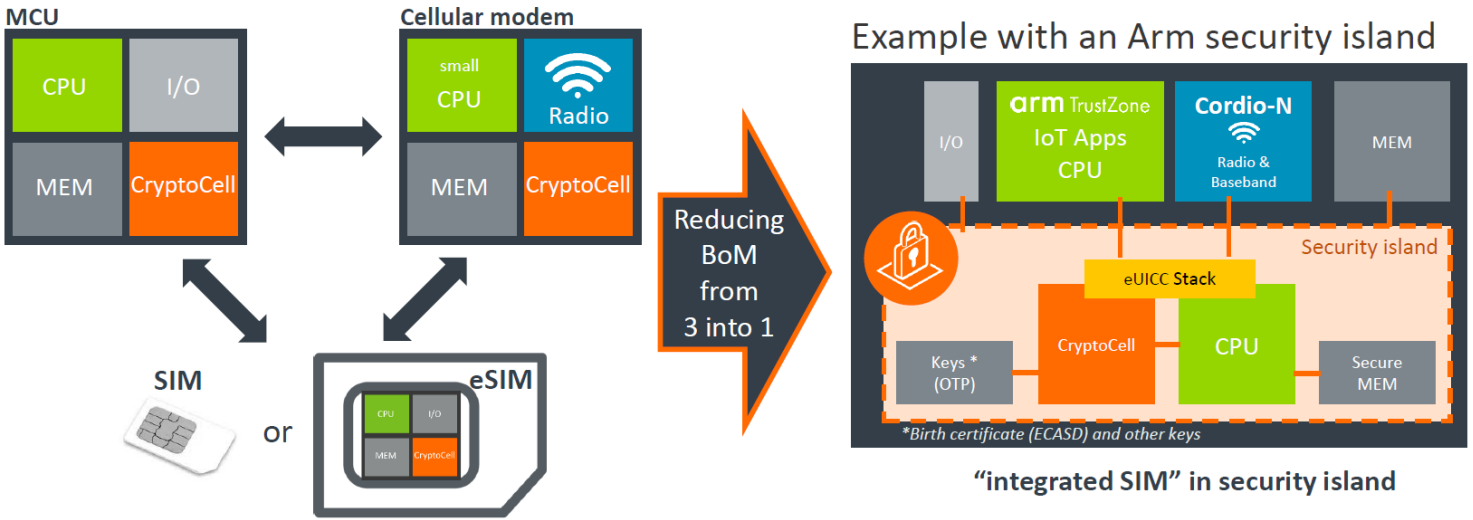
Example for LoRa: Gemalto Xtreme research project



Toward System on Chip

arm TechCon 2017

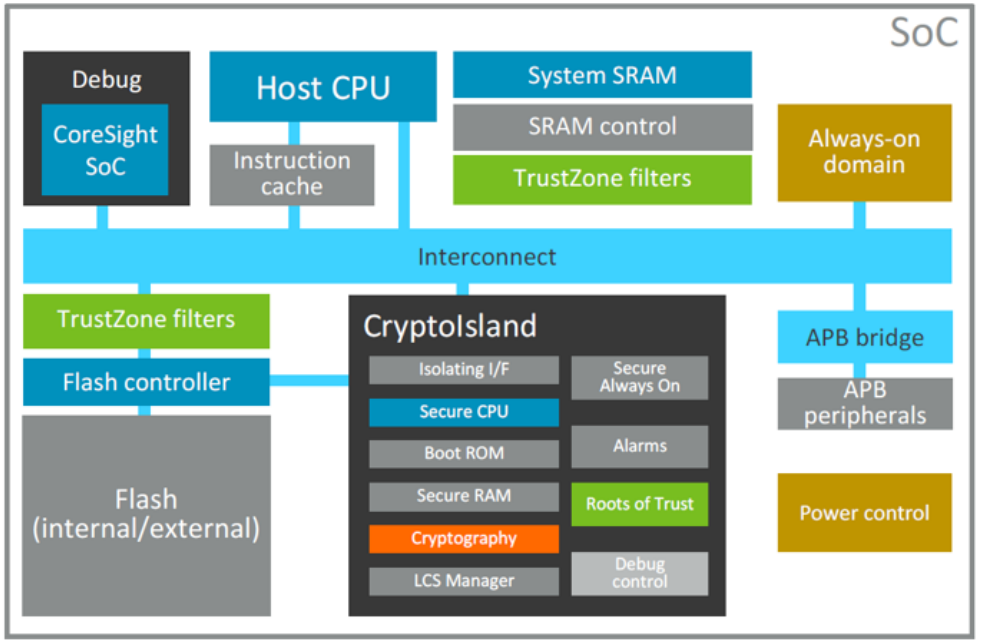
Combining a secure element, cellular modem and MCU into a single SoC



CryptoIsland

arm TechCon 2017

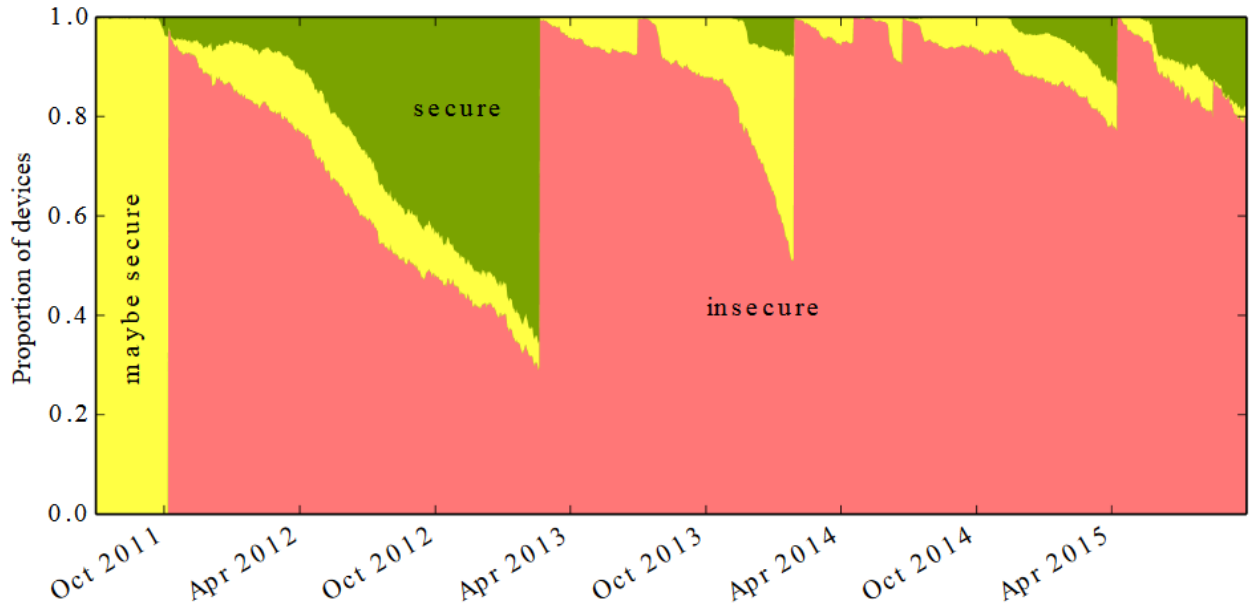
- A programmable security enclave to extend fixed function CryptoCell family
- **TrustZone CryptoIslands - an additional family of security solutions by Arm**
- Aimed at providing on-die security services, in a physically isolated manner (host CPU agnostic)
- Axiom: less sharing of resources leads to smaller attack surface and fewer vulnerabilities
- Certification, at a reasonable cost (i.e. reuse)



Support ARM v8-m & v7-m

Forget about rich OS security !

Proportion of devices running vulnerable versions of Android



Source AndroidVulnerabilities.org

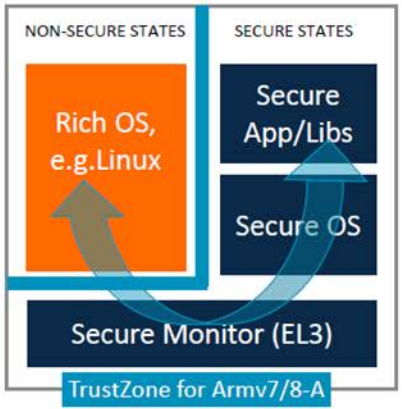
TrustZone on Cortex-A vs. TrustZone on Armv8-M

Differences in state transitions

Cortex-A processors

Transitions by Secure Monitor exception

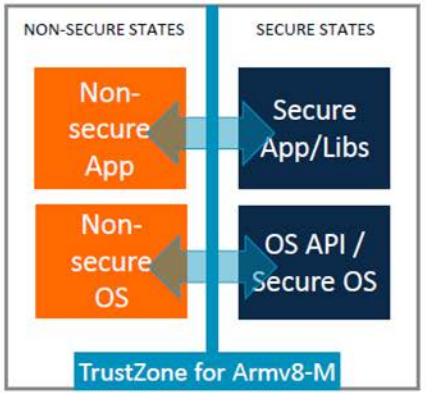
- Highly flexible
- Physical address agnostic



Cortex-M23 and Cortex-M33 processors

Transitions by function call/return, exception sequences.

- Fast switching
- No extra code size
- Easy to use
- Real-time



A parallel trend of evolution

µController → Adding crypto copro/core

OS → Adding TEE

Memory management in i.MX6

Feature		
TEE	Trusted	Untrusted
Copro	Secured	Unsecured
CPU	Kernel	User

→ 8 combinations for a memory page !!!

- Resist invasive attacks ?
- CC certifiable ?
- Complex security model

Agenda

- Why do we need IoT?
- Zoom on networks and LPWAN
- Trends in security solutions: integration and resilience
- Challenges ahead

Challenges ahead in IoT security

- Ultra low cost and low power security
  - Lightweight end-to-end security
- SoC security
  - Tamper resistance, certification, design patterns
- Credential provisioning
  - Manufacture and forget, connect out-of-the-box
- Long life cycle management
  - Multi layered security, resilience and attack recovery