

DESIGN AUTOMATION EMBEDDED SYSTEMS

2 NOV ←
1931 CONGRESCESTRUM
BRABANTHALLEN
DEN BOSCH

2 NOV ←
BRABANTHALLEN
DEN BOSCH

D&E
event
2016

event
2016

FPGA - SECURITY - EMBEDDED - INTERNET OF THINGS - PCB TECHNOLOGIEËN - BLUETOOTH LE - ELECTRONIC DESIGN & PRODUCTION



Connected things in the IoT world challenge your security!

Wim van der Steeg

Accelerating Your Success™

What is network security about ?

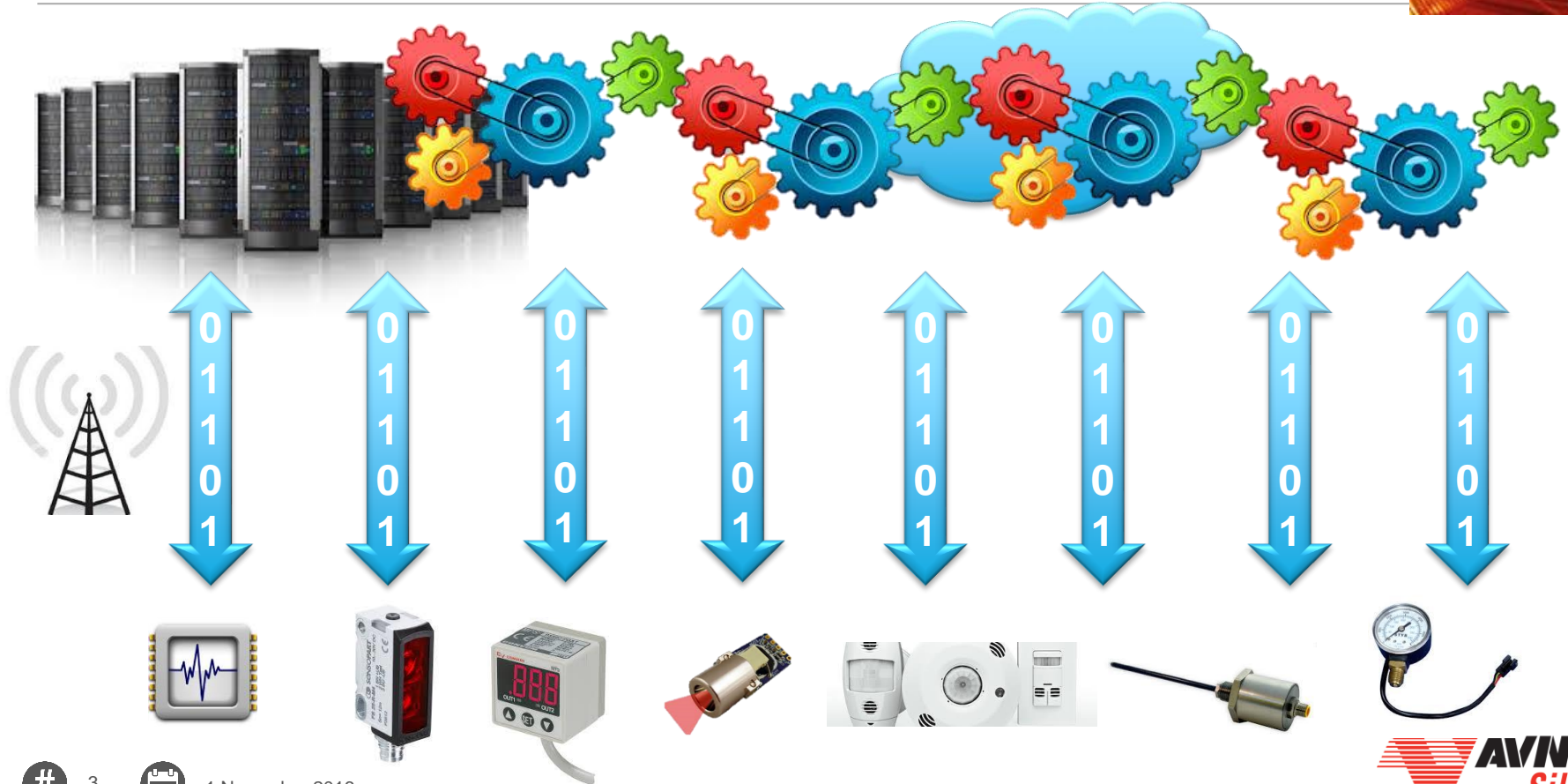


2

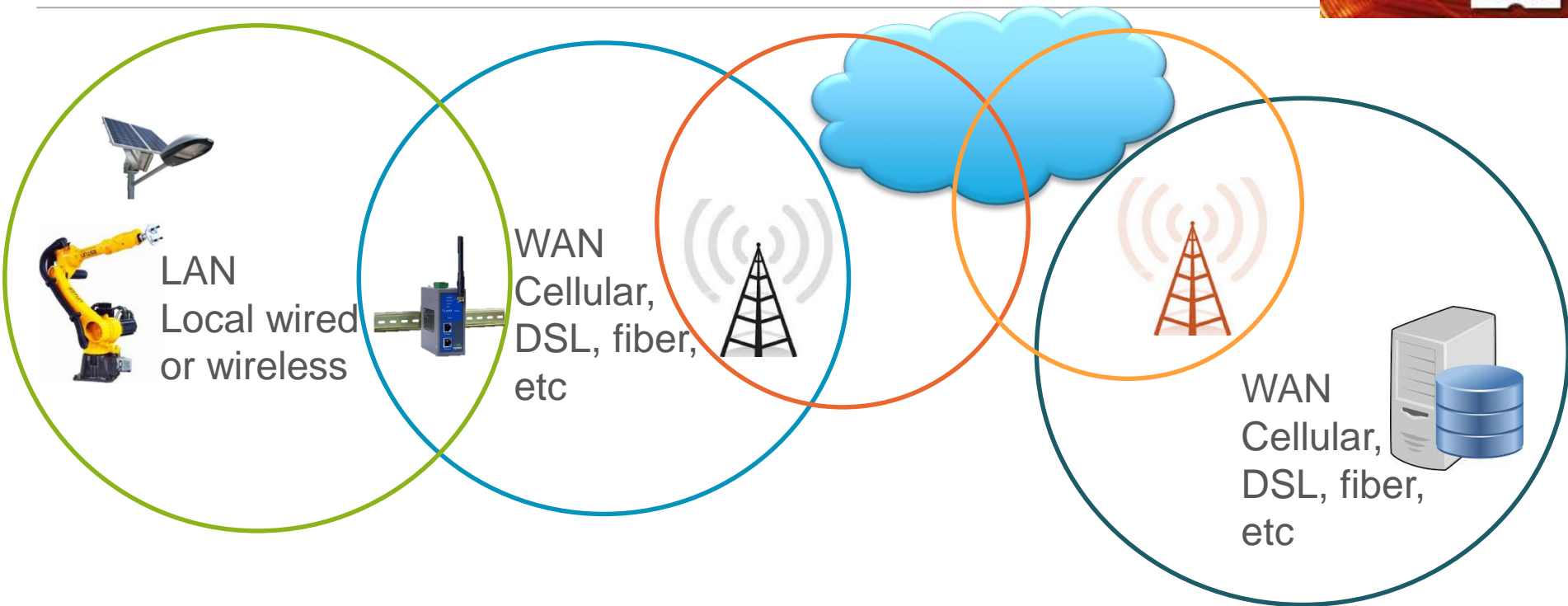


1 November 2016

IoT = process loops cross-harvesting data



Typical connection of IoT device – need to trust many!



Weak security

Ok-Good security

Good security

Ok-Good security

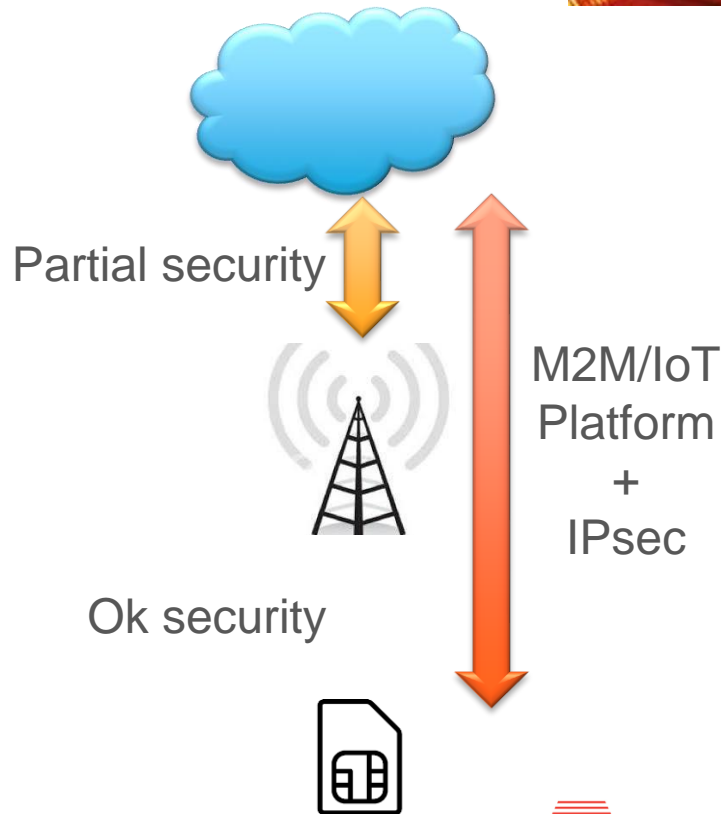
Relying on network security only ?

- When 2G was invented, security was designed with the following purposes:
 - Secure user authentication by MNO for proper billing
 - Encrypting communications from phone to phone with level of security equivalent to PSTN
 - Prevent fraudulent usage of the network
- Security optimized for phone to phone communication
- Is it what we need in the IoT space ?



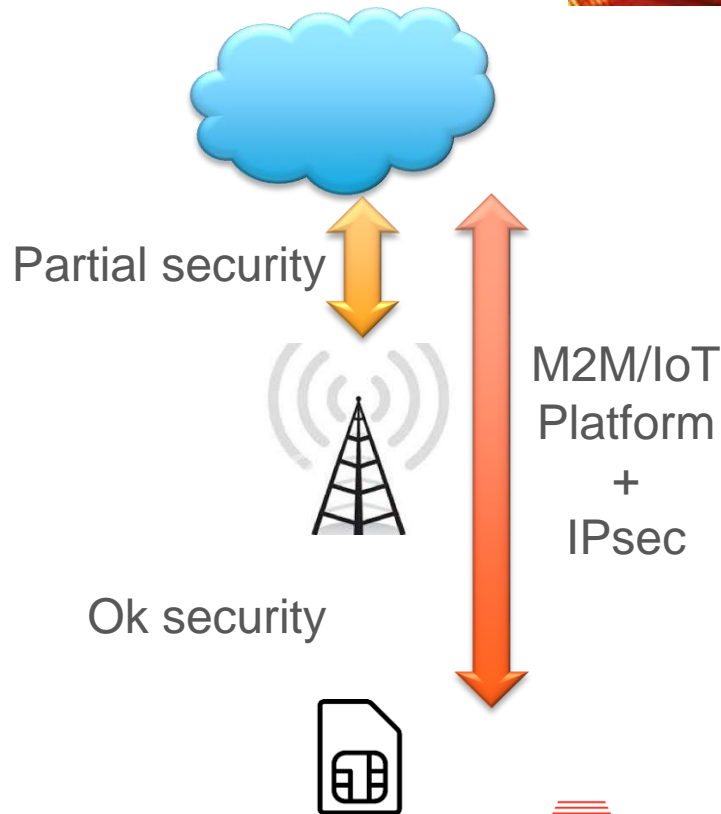
Security of 2G networks

- Authentication
 - 2G device SIM is authenticated to network
 - No authentication of network to device SIM
- Confidentiality
 - Encryption between device and base-station only
 - Data in the clear from BS to network backend
 - 64-bit key with implementation of 54-bit key padded with 10 zeros in practice resulting in very weak ciphering
- Anonymity
 - User IMSI never exposed making it difficult to track a user by eavesdropping the radio network



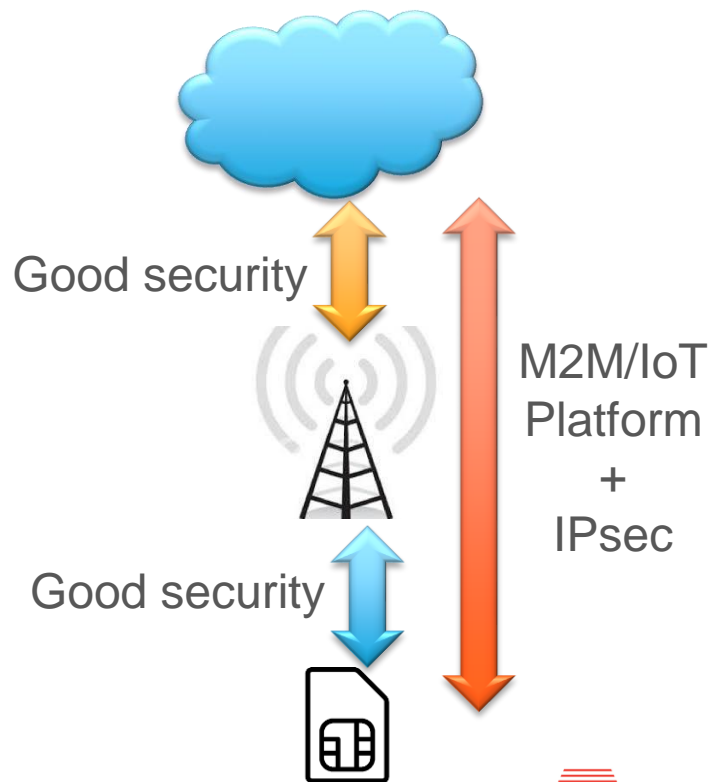
Security of 2G networks

- Authentication
 - 2G device SIM is authenticated to network
 - No authentication of network to device SIM
- Confidentiality
 - Encryption between device and base-station only
 - Data in the clear from BS to network backend
 - 64-bit key with implementation of 54-bit key padded with 10 zeros in practice resulting in very weak ciphering
- Anonymity
 - User IMSI never exposed making it difficult to track a user by eavesdropping the radio network



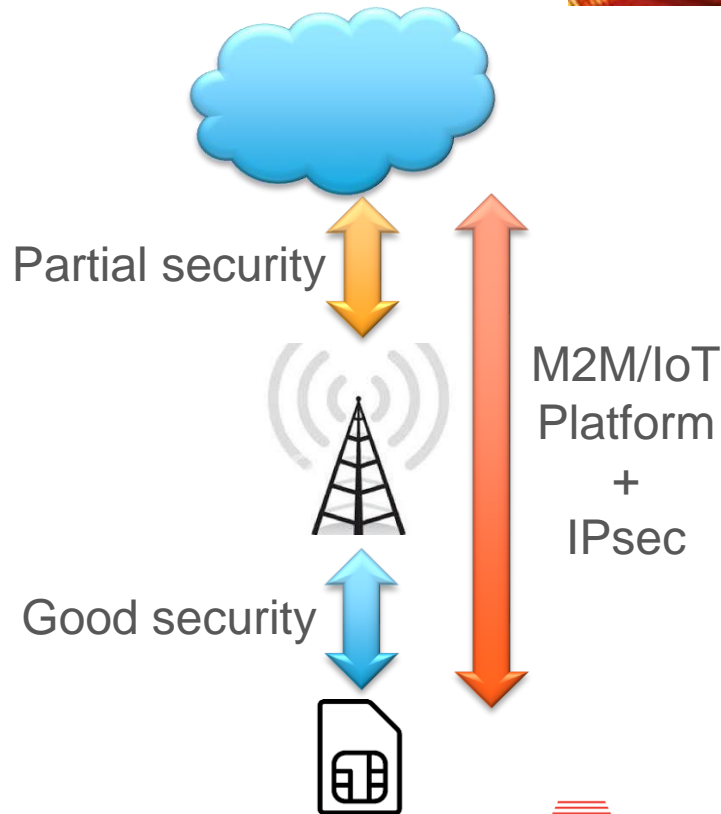
Security of 3G networks

- Authentication
 - Mutual authentication: the network also authenticates to the 3G device SIM
 - Signaling messages can be authenticated by the 3G device SIM
- Confidentiality
 - Stronger keys of 128-256 bits
 - Full network-to-network security
 - Not to be mistaken with end-to-end security
- Anonymity
 - User IMSI never exposed making it difficult to track a user by eavesdropping the radio network



Security of 4G networks

- First cellular all-IP network
- Authentication
 - Mutual authentication: the network also authenticates to the 4G device SIM
 - Signaling messages can be authenticated by the 4G device SIM
- Confidentiality
 - Encryption between device and base-station only
 - Data may be in the clear from BS to network backend if operator decides so
- Anonymity
 - User IMSI never exposed making it difficult to track a user by eavesdropping the radio network



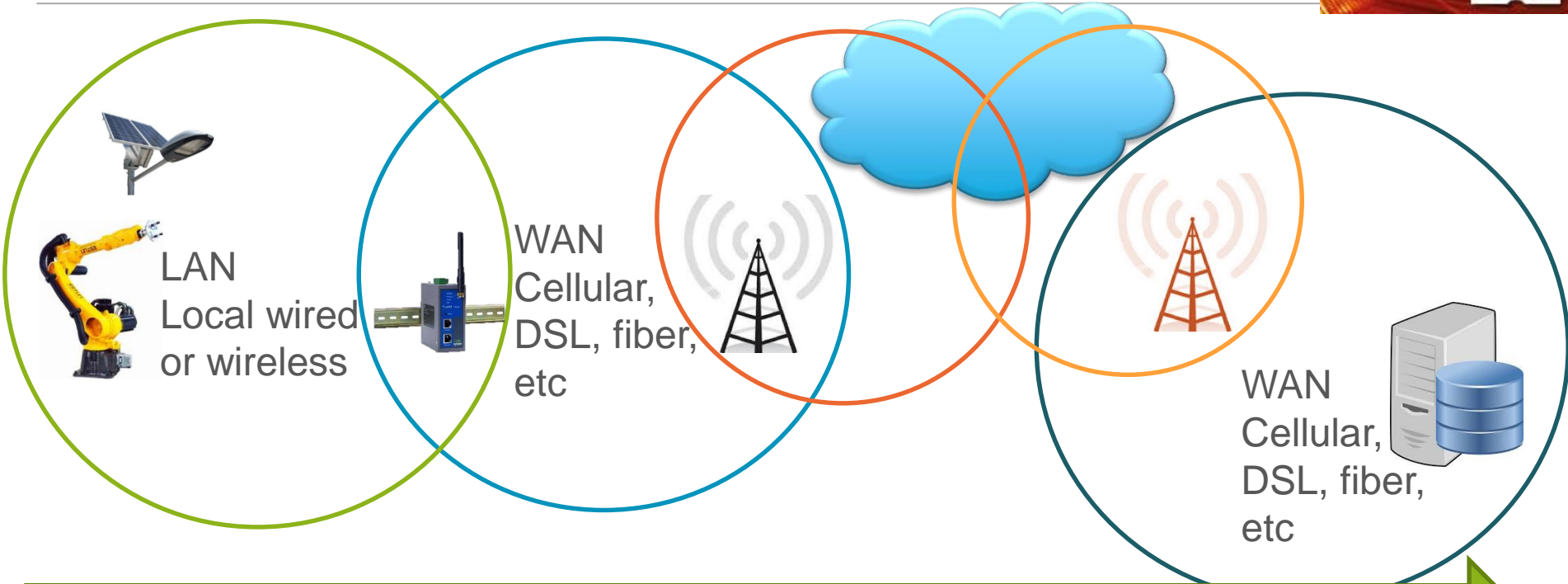
SIGFOX

- Device authentication to network
 - Unique private 128 bit AES key per device
 - Anti-replay mechanism
 - No key renewal
 - Protecting network access only
- No network authentication to device
- No data encryption

LoRaWAN

- 2 layers of security
 - Device \leftrightarrow network
 - Device \leftrightarrow applicative server
- Mutual authentication between device and network
 - Several unique private 128-bit AES keys per device
 - Anti-replay mechanism
 - Weak key renewal
- Applicative private keys for securing data between device and server

How about not having to trust anyone – just in case ?



How about an extra layer of device-to-server strong security ?

Weak security

Ok-Good security

Good security

Ok-Good security

What is really needed...



12



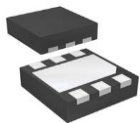
1 November 2016

End-to-end device-to-server security

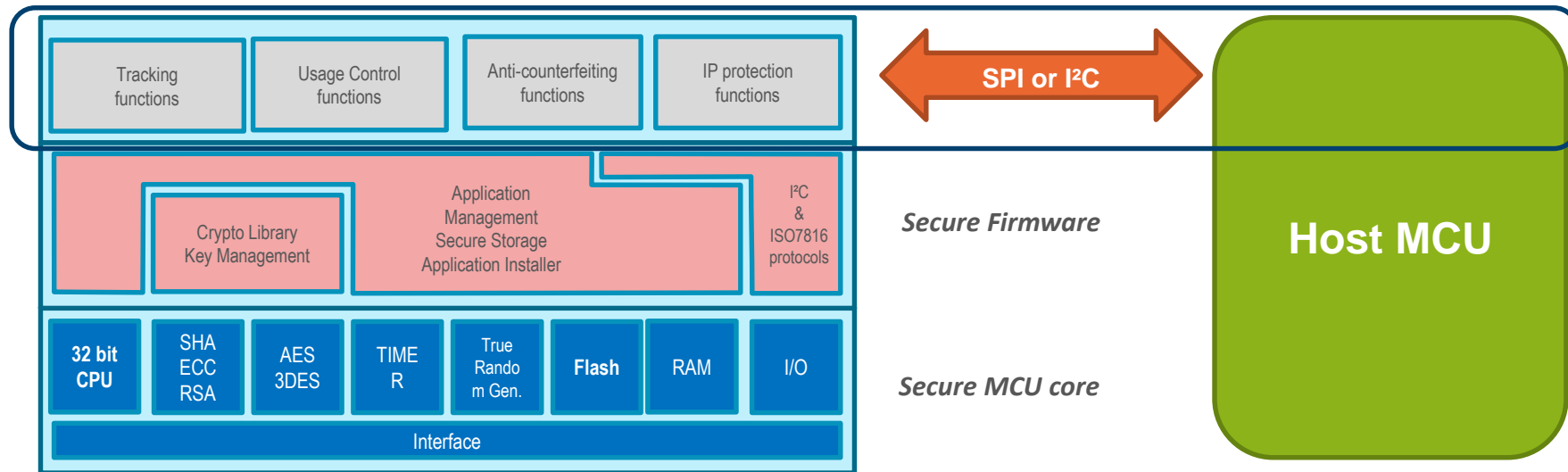


How about an extra layer of device-to-server strong security ?

This is what a Secure Elements is

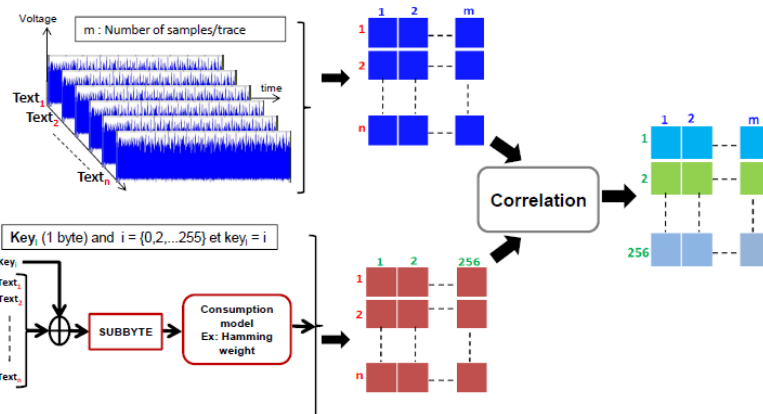


Customized and personalized with unique IDs and keys / certificates for the customer



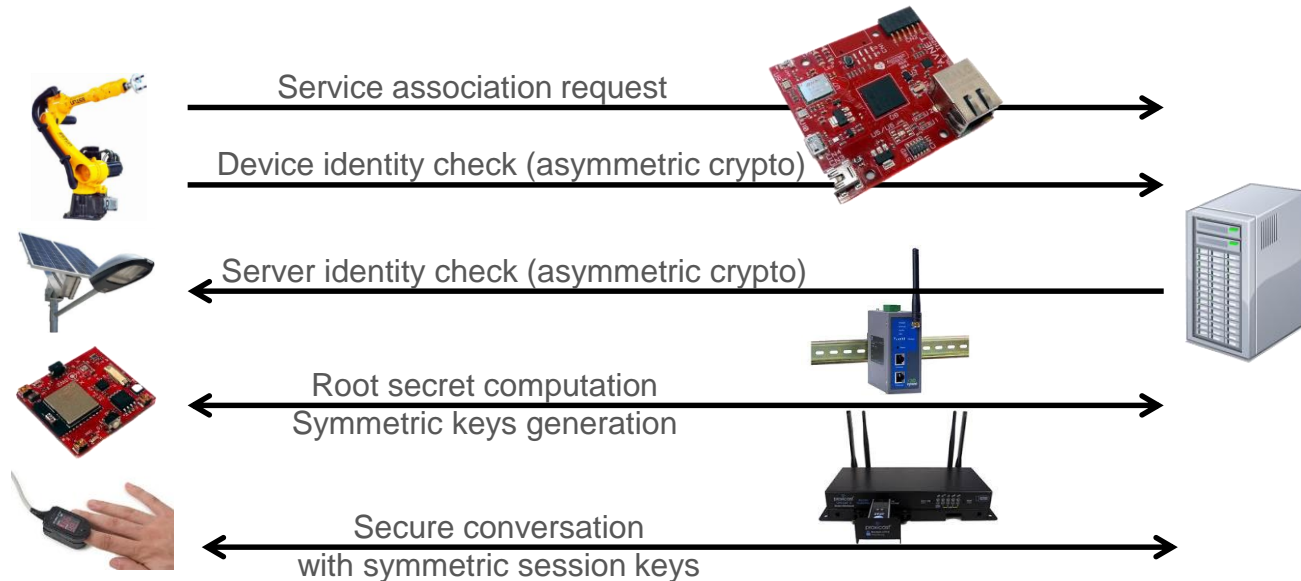
How secure are standard MCUs ?

It takes 16min, a laptop,
Matlab, a 150€ USB
oscilloscope & probe to
extract an AES128 key from
any non-secure MCU

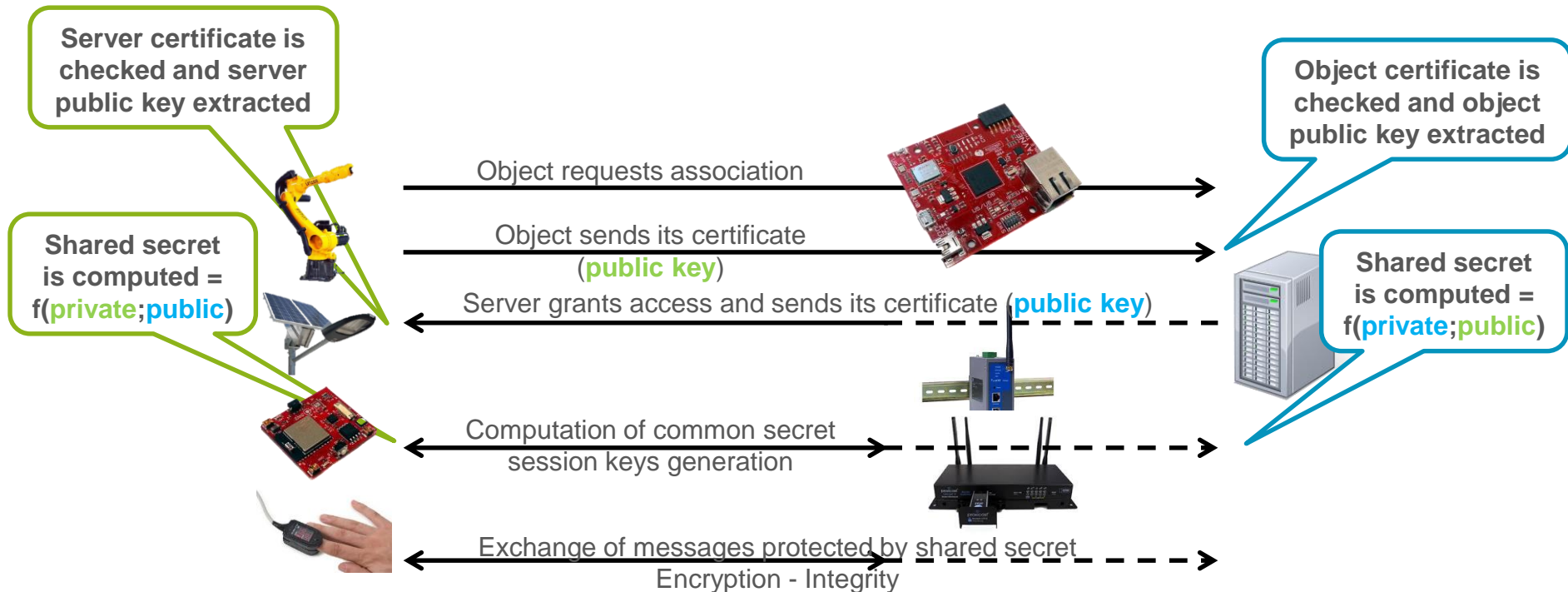


Courtesy of Driss Aboulkassimi – CEATech – FR – driss.aboulkassimi@cea.fr

Secure connectivity protocol model



Secure connectivity protocol example



Secure Element...What else?



- #1 Intellectual Property protection
- #2 Granting access to a system
- #3 Logistics assistance for managing unique devices
- #4 Secure communications

#1 – Intellectual Property protection

Problem

- Preserve IP from copying and counterfeiting
 - Useful when outsourcing manufacturing, especially offshore
- This IP can be HW and/or SW



Solution

- A small secure element attached to each board to protect
 - Personalized with a unique ID and corresponding secret keys / certificate
 - That cannot be copied
 - Acting as a passport
 - Validated by a local MCU or a distant server

#2 – Granting access to a system

Problems

- How to add an authorized device to a remote system (provisioning) ?
 - Famous: Ink cartridge – printer
 - Motherboard – daughterboard: sensitive/expensive spare parts
 - Home/building automation accessory inside a local network
 - Smart meter inside a global grid
 - iPhone's accessories
- Prevent device or service spoofing



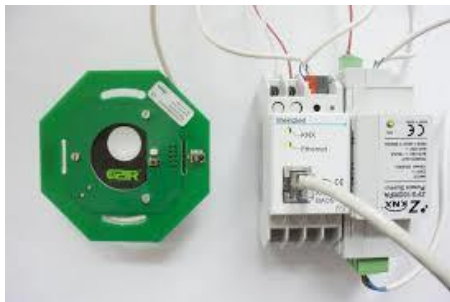
Solution

- A small secure element attached to each device to protect
 - Personalized with a unique ID and corresponding secret keys / certificate
 - That cannot be copied
 - Acting as a passport
- A mechanism such that this passport can be read from a local gateway or distant server in a secure way

#3 – Logistics assistance for managing unique devices

Problem

- Logistics assistance in local / global network / system provisioning involving some personalization for every single device
 - Minimizing in-the-field configuration
 - Securing whole supply-chain at minimum cost
 - Secure remote management throughout product life (up to 15 years)
 - Distribute and renew secret keys in a safe and simple way



Solution

- Our secure programming line with Avnet Logistic Services
 - Capable to personalize secure elements Handling volumes from 1k to 10M+
 - HSM: Hardware Security Module capable of generating secret keys
 - Compliant with EMVco standard (Europay – Visa – Mastercard) = highest level of security in the industry
- Key management with Trusted Third Party throughout product life

#4 – Secure communications

Problem

- Protect data exchanges from potential eavesdroppers
- Secure systems against hackers from sensor to server



Solution

- A secure element capable of:
 - Strong authentication
 - Root key storage
 - Session key generation and storage
 - Encryption / decryption

Secure Elements Solutions by Avnet Silica



23



1 November 2016



Many chips boast security features

Cortex M0/3/4
PIC, etc

	Crypto accelerators	High thruput crypto acc	Hardened certified HW	Personalized	Safe for keeping keys
Basic MCUs	✓	X	X	X	X
Crypto co-proc	✓	✓	X	X	~
Secure Elements	✓	X	✓	✓	✓

NXP Kinetis
MAXIM Deepcover secure MCUs
MARVELL, etc

2 sorts of Secure Elements



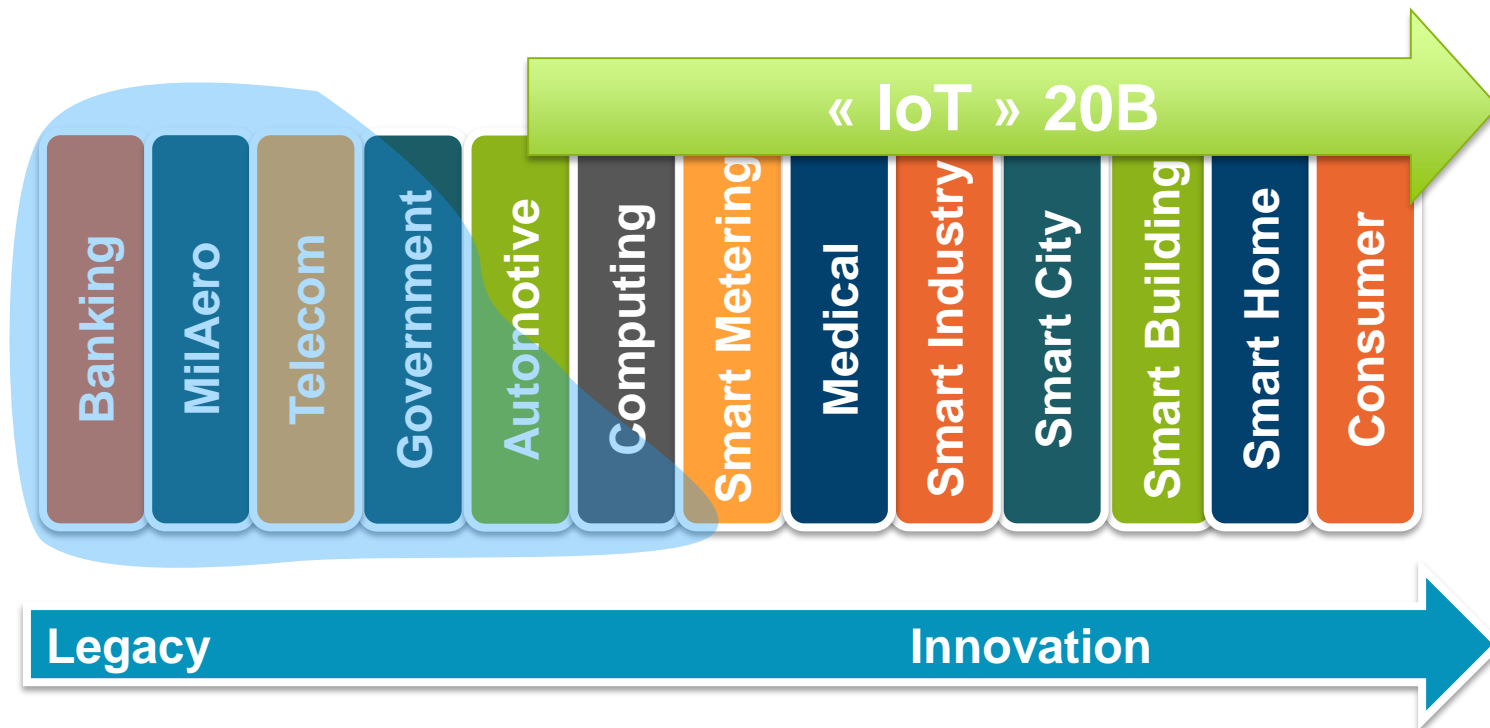
TPM

- TPM = Trusted Platform Module
 - Standardized security controller
 - Standard from TCG (Trusted Computer Group)
 - Used in every computer, main board, complex routers, etc
 - TPM 1.2 getting obsolete (SHA1 and RSA)
 - TPM 2.0 with new crypto such as ECC
- Security companion chip for MPUs (Marvell, NXP, etc)

“Universal”

- Able to perform and associate many crypto primitives for security schemes outside the TCG standard
- From basic authentication of a device to another (printer cartridge to printer)
- To TLS session enablement
- Asymmetric and symmetric cryptography
 - Digital signatures
 - Diffie-Hellmann
 - AES, DES, SHA2/3/256
 - RSA, ECC (NIST, Brainpool)
- Some are even FW customizable!

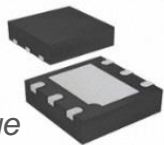
HW Security: Which markets?



Trusted Objects solution

Volumes: <1k-100M!

Flexibility: ++

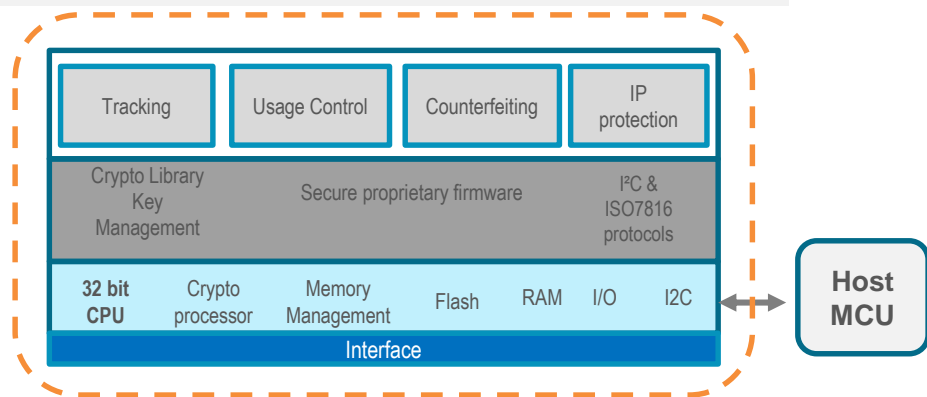


DFN6 package

TO 136 is a fully integrated solution:

- 32 bit Secure CPU hardware, compliant with EMV Co standard
- Customizable on-demand software, optimized for the IoT
- Host code to interface with secure hardware through I2C
- Product personalization with AVS-exclusive secure logistics

HW EMVco and CC EAL4+ certified



- Authenticate Device and/or Server
- Secure communication
- Session key establishment
- Broadcast key management
- Secure data storage
- Setup a TLS connection
- Implement USB Type C authentication

STM STSAFE-A – STSAFE-J (Java) & TPM

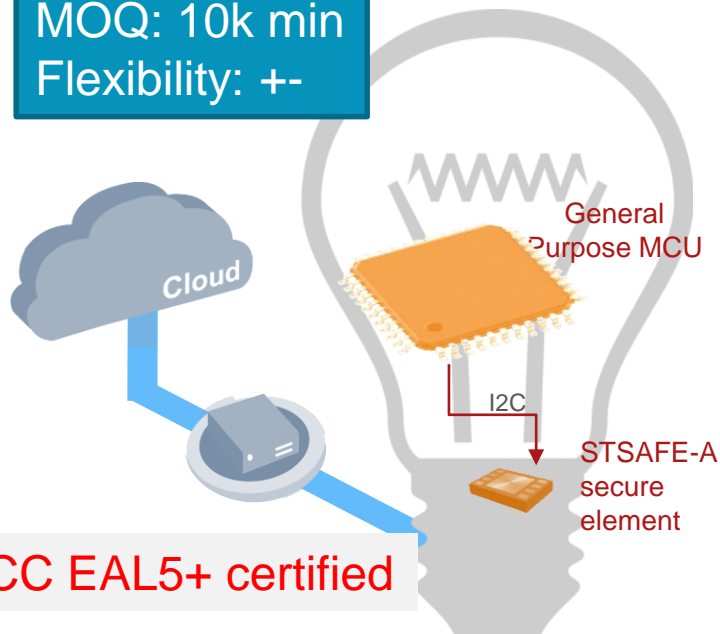
2 NOV
BRABANTHALLEN
DEN BOSCH

D&E
event
2016



Easy to use security services for IoT developers

MOQ: 10k min
Flexibility: +-



CC EAL5+ certified

Authentication

Secure communication

Secure storage

Secure Firmware upgrade

USB Type-C







28



1 November 2016

INFINEON OPTIGA™ - Hardware-based security solutions

	OPTIGA™ Trust	OPTIGA™ Trust E	OPTIGA™ Trust P	OPTIGA™ TPM
				
Security Level	+	+++	CC certified	CC certified
Design in complexity	low	low	medium	medium
Feature set	One function	Enhanced	Programmable	TPM standard
Personalization (loading of keys and certificates)	✓	✓	✓	✓
MOQ	12k	12k	30k	3k/5k
Certification	No	HW EAL5+	EAL5+	EAL4+

1-way Authentication only

NXP Turnkey Solution A70CM

2 NOV
BRABANTHALLEN
DEN BOSCH

D&E
event
2016

Key Features

Turnkey Solutions



**Off-the-Shelf Product
featuring:**

Security IC A700x	Key Injection Service
On-chip Application SW	Host Library, High-Level API

- Built on A700x NXP Security IC featuring state-of-the art Tamper Resistance technology
- Configurable Public Key cryptography with keys up to 2048 bits (RSA) and 256 bits (ECC)
- Signature generation and verification
- RSA encryption/decryption
- AES 128/256 bits encryption/decryption, large key store
- Factory Key pre-injection in certified (Common Criteria) secure environment
- On chip key generation
- Secure key management
- Device Life Cycle Management
- 100 Kbits/sec slave I²C interface
- -25 °C to +85 °C (A7001CMHN1), -40 °C to +90 °C (A7002CMHN1) operational ambient temperature
- HVQFN32 package

Volumes: 50k min

CC EAL5+ certified



MAXIM DEEPCOVER Security ICs

2 NOV
BRABANTHALLEN
DEN BOSCH

D&E
event
2016

Analog Micros

Integrated Analog and Security Support for private and public key cryptography

e.g. **MAX71637**



DeepCover Secure Microcontrollers

Generic cryptographic support enabling trusted boot and trusted communications

- **MAXQ1050**
- **Future micros**

DeepCover Authentication ICs

Enables hardware authentication as well as simple Public Key Infrastructure

- **DS28XXXX, MAX66300**

Volumes: 50k min

Not certified



And what is enough security?



- It is a complex process
 - Using AES is the right thing to do
 - How to personalize each device, with IDs?
 - How to generate unique AES keys manufacturing process
 - Your self?
 - The EMS? – Can you trust them?
 - Your customer or final user?
 - How much time / money does it cost?
 - How often to renew keys?
 - How to renew keys?

There is not one solution for
your problem.
&
Make use of experts.

Thank You!

Avnet Silica
Wim van der Steeg
076 – 5722352

wim.vandersteeg@avnet.eu

