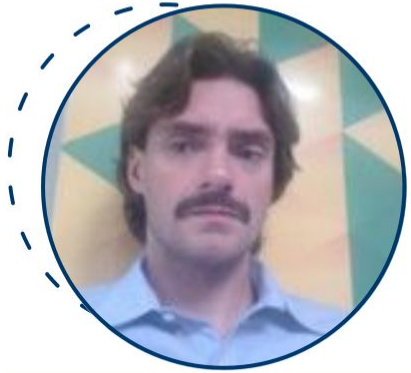
EMBARCADOS WEBINAR | MOUSER ELECTRONICS

Como implementar soluções fáceis e robustas de Segurança em Hardware

Conheça tecnologias de autenticação segura e encriptação em hardware da Analog Devices e como elas podem ser utilizadas em seu projeto



Juliano Kowalczuk

Engenheiro de Aplicações

ANALOG DEVICES

AHEAD OF WHAT'S POSSIBLE™

EMBARCADOS

Patrocinado por

MOUSER ELECTRONICS

EMBARCADOS experience 2023

28 DE OUTUBRO

Local: São Paulo

- ✓6 Palestras
- ✓4 Workshops
- ✓Networking

GARANTA SUA VAGA

MOUSER ELECTRONICS

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

Analog Devices / BP&M

04/10/2023

Webinar Embarcados

Secure Authenticators

Implementing Security is Easier Than You Think

Juliano Kowalczuk Cioffi – ADI FAE for Brazil

Agenda

- Desafios de segurança em produtos conectados ou em acessórios.
- O que é a autenticação segura e a encriptação de dados, e quais são as técnicas utilizadas.
- Soluções da Analog Devices.
- Exemplos de casos de uso.

Agenda

- Part 1
  - Desafios de segurança em produtos conectados ou em acessórios.

Attackers Target or Leverage Connected Devices

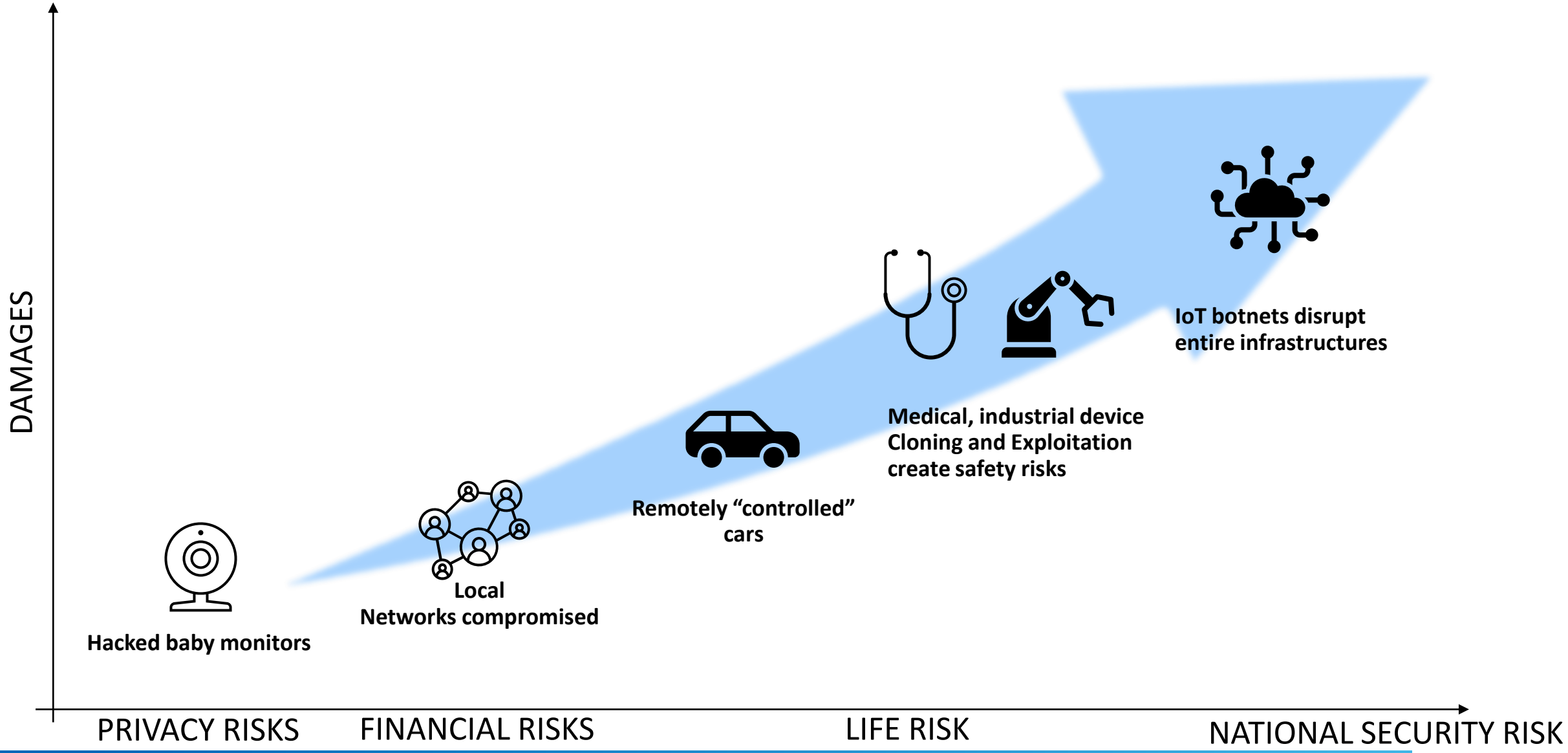
Why attacking connected devices?

- For research purposes / fame
- To steal personal / financial information
- To disrupt networks, web services, factories, critical infrastructures

Impacts?

- Privacy
- Financial losses
- Unacceptable safety concerns for people, risks of death
- Environmental catastrophes

Increasing risks due to devices connectivity



Overcoming Common Objections

I need no security at all

- Devices not hacked today will be tomorrow
- Attacks damage reputation that is hard to recover
- Our products enable easy implementation even if not anticipated

Software security is sufficient

- Software security is a first level
- Root of trust has to be hardware based (secure boot is a must)
- Hardware accelerators improve performance
- Key distribution is always a challenge

I use a secure micro with TrustZone™

- TrustZone™ does not protect against
  - Physical attacks
  - Side Channel attacks
- Secure authenticators solve key distribution issue for few cents
- ChipDNA™ brings the most secure storage

Agenda

- Part 2
  - O que é a autenticação segura e a encriptação de dados, e quais são as técnicas utilizadas.

Some Pre-conceived Ideas About Security

- Cryptography was invented in the 20th century
  - **False :** Cryptography started in antiquity : Caesar cipher was used to encrypt messages
- We use cryptography everyday, it is all around us
  - True : Whatsapp communication are encrypted, banking cars are authenticated, websites are authenticated
- Security is all about secrecy
  - **False** :
    - Modern security considers public specifications and algorithms
    - Serious certification schemes such as FIPS, PSA, Common Criteria, publish the certificates
- For secure communication, confidentiality is more important than authentication
  - **False :** they are equally important. Authentication is making sure the sender / receiver is the one expected, confidentiality is about making information readable only to authorized entities

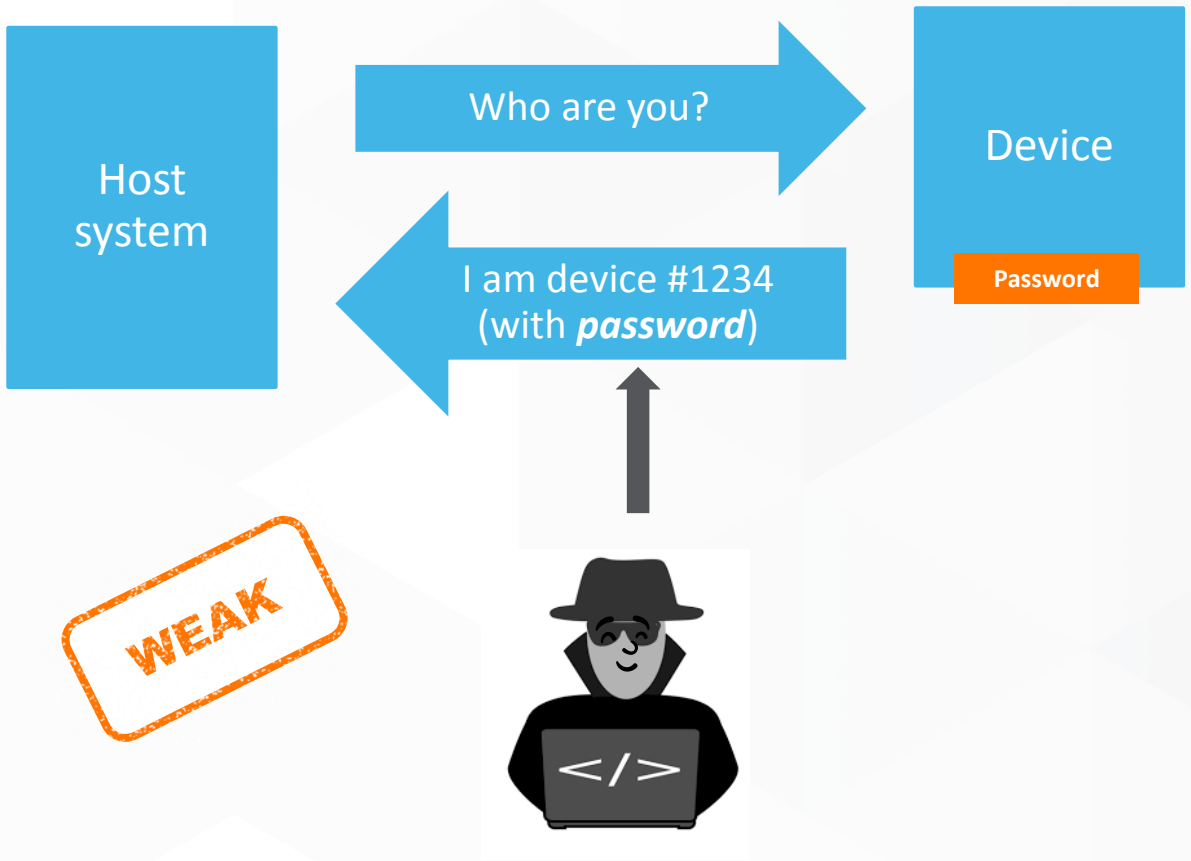
Secure Authenticators

- HW-based fixed function crypto
- From IP protection to IoT security
- No device level firmware
- Ease of use
- Full portfolio of products
- Factory personalization service aka Preprograming

Over 4 billion secure authenticators deployed into customer's applications!

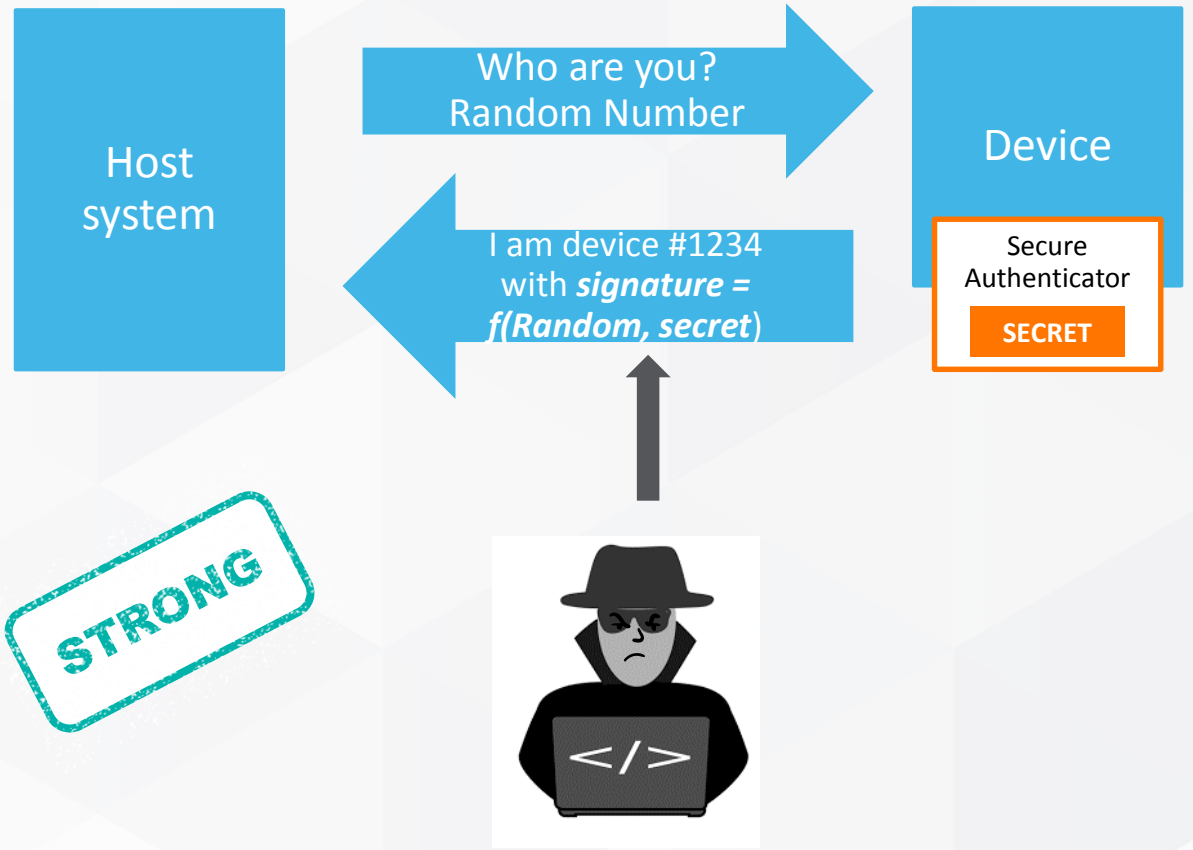
Device Authentication : How ?

Intuitive way



The hacker can easily read the password because it is **exposed**

Cryptographic way



The hacker cannot access the secret because it is **NOT exposed**

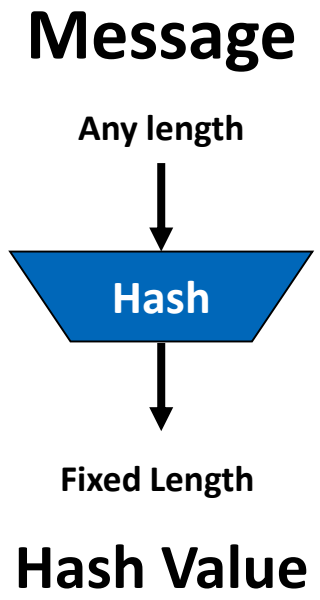
Device Authentication : How ? (cont'd)

- A **digital signature** = f(values, **secret or key**)

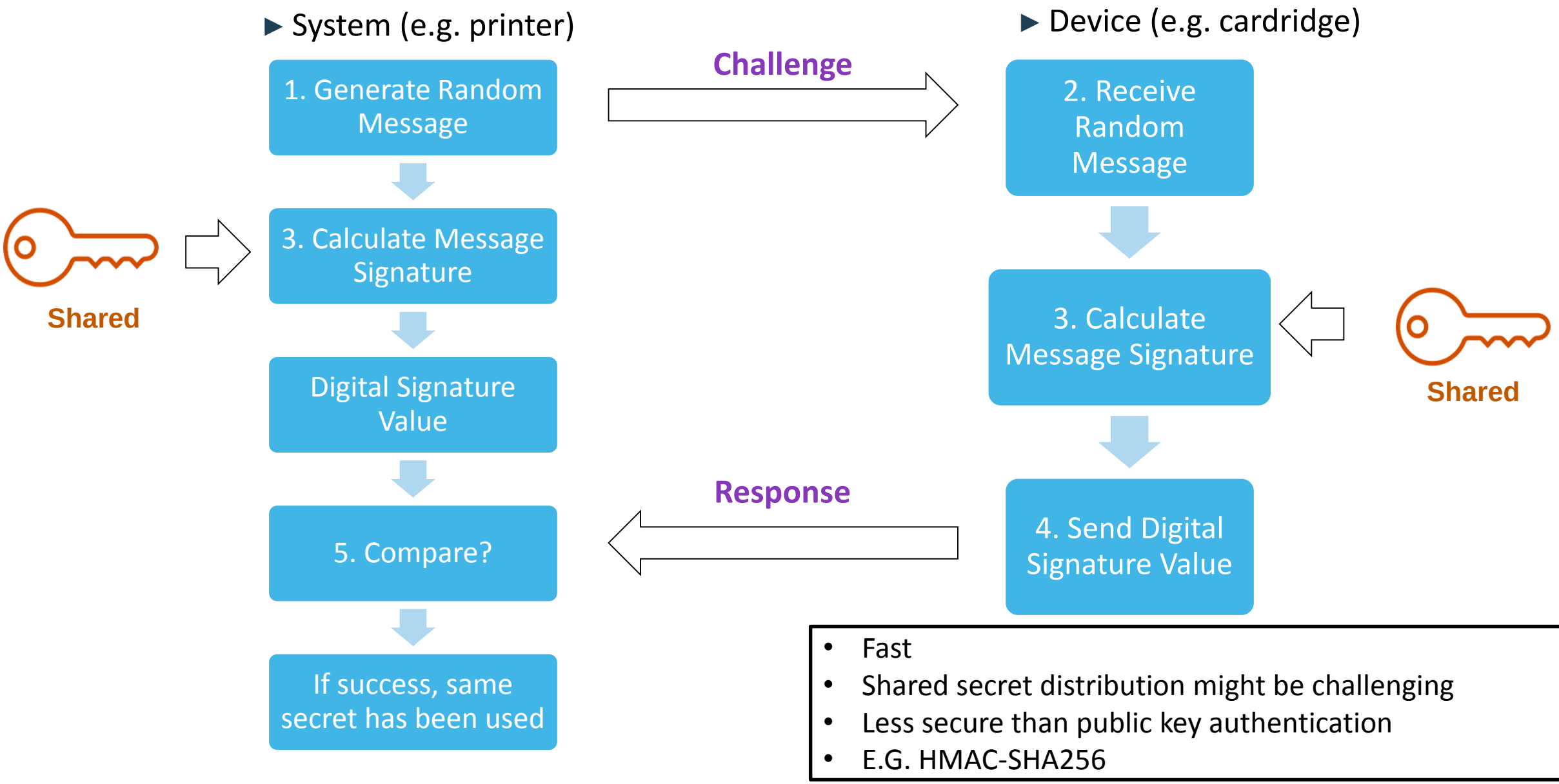
- « f » can be a *hash* function
  - Examples : **S**ecure **H**ash **A**lgorithm SHA-1, SHA-256, SHA-3

- Secure Hash functions properties
  - No way back
    - It is computentially infeasible to revert to the original message
  - Finding two messages leading to same hash value is computationally infeasible
    - No collision
  - Modifying a few bits gives completely different hash
    - Avalanche effect

- Hash (values, **secret or key**) = HMAC supports crypto strong authentication



Challenge Response Authentication w/ Secret Keys



- Fast
- Shared secret distribution might be challenging
- Less secure than public key authentication
- E.G. HMAC-SHA256

Key Distribution Challenge in Symmetric Crypto

Challenge ?

- The **same** key must be injected in each consumable and device
- The key is **exposed** during injection phase
  - Creates manufacturing constraints (secure room)
- If the key gets compromised, it is hard to replace it in deployed devices

Alternative : Asymmetric Cryptography

Who are you?
Random Number

I am device #1234
(with ***signature = f(Random, Private)***)

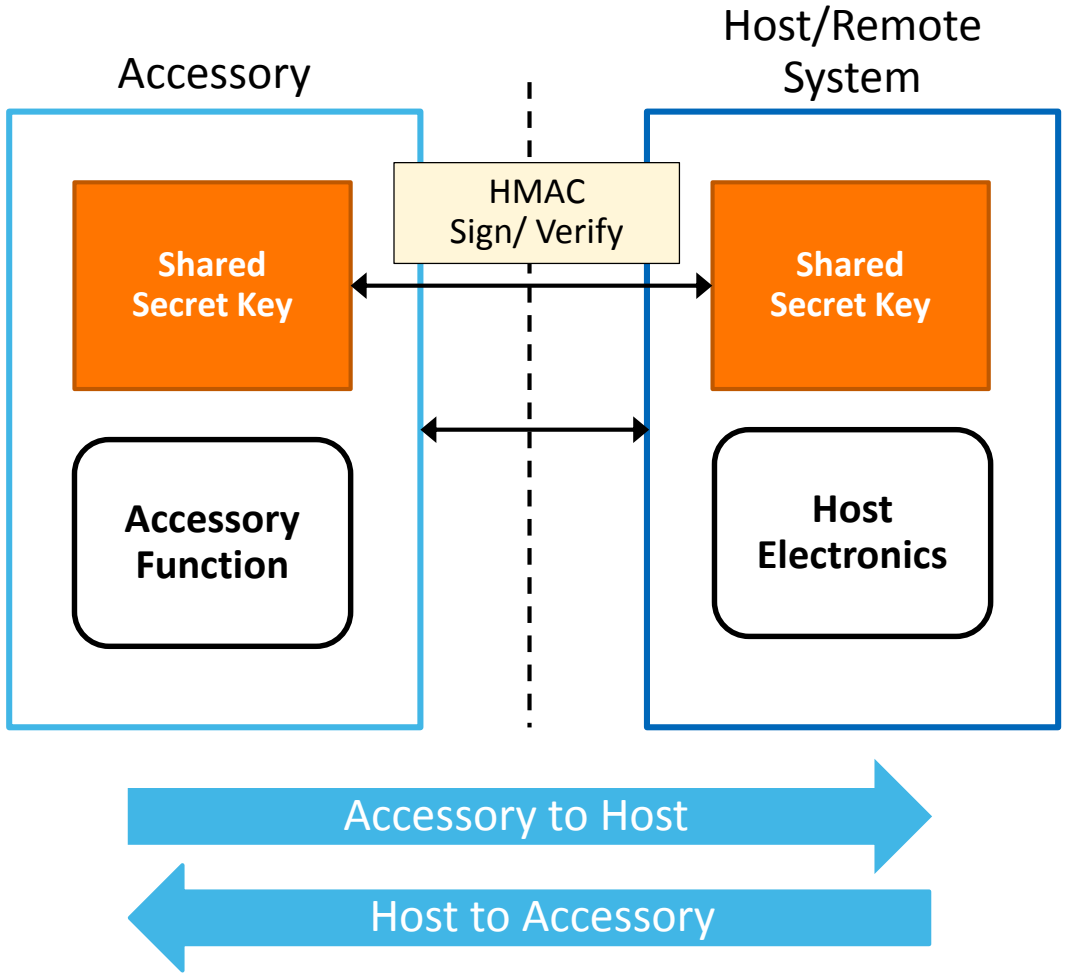
Signature is verified with Public Key

Signature is computed with Private Key

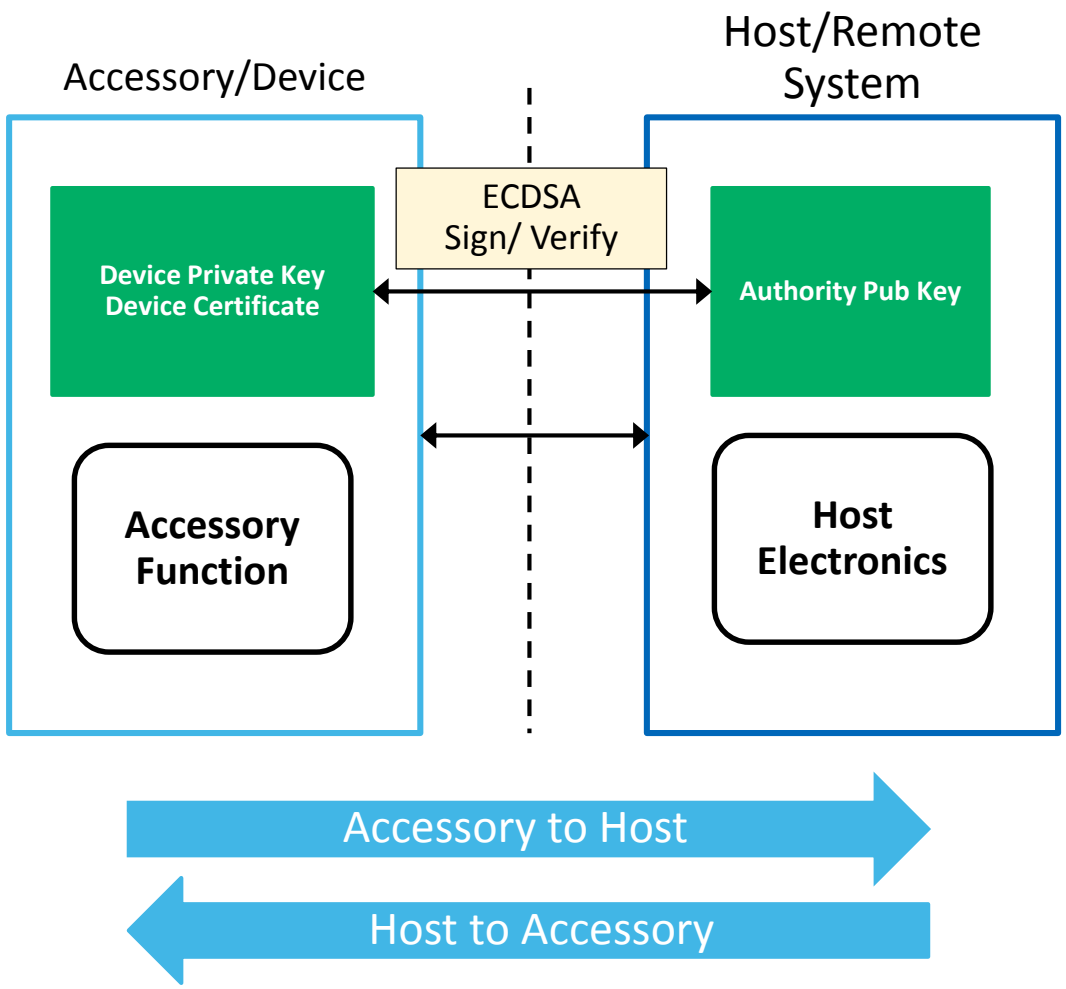
- A key pair is made of **matching** private and public keys
- The public key can be disclosed freely
- Anybody holding the public can verify authenticity
  - Updating public keys in deployed device is relatively easy
- Only those knowing the private key can sign
- In Secure Authenticators, our f() is ECDSA

Summary: HMAC-SHA vs. ECDSA based authentication

- Simple, Fast, Less secure, Less Memory
- E.G. HMAC-SHA256



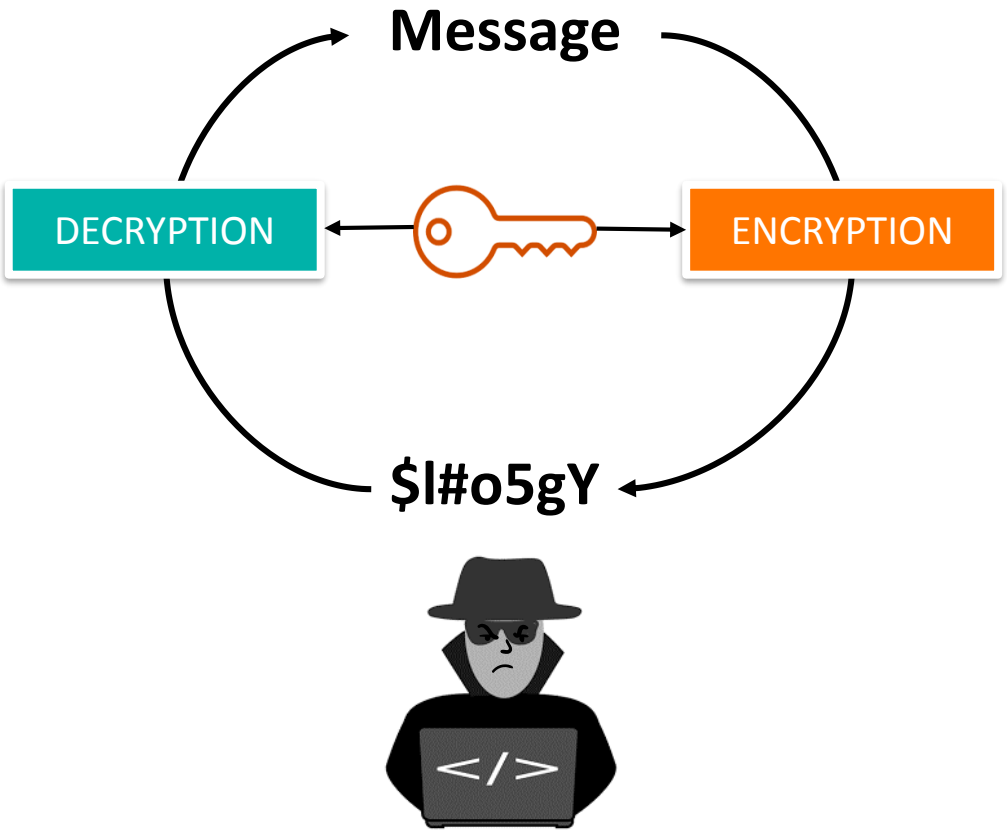
- More complex, Slower, More secure, More memory needed
- E.G. ECDSA 256

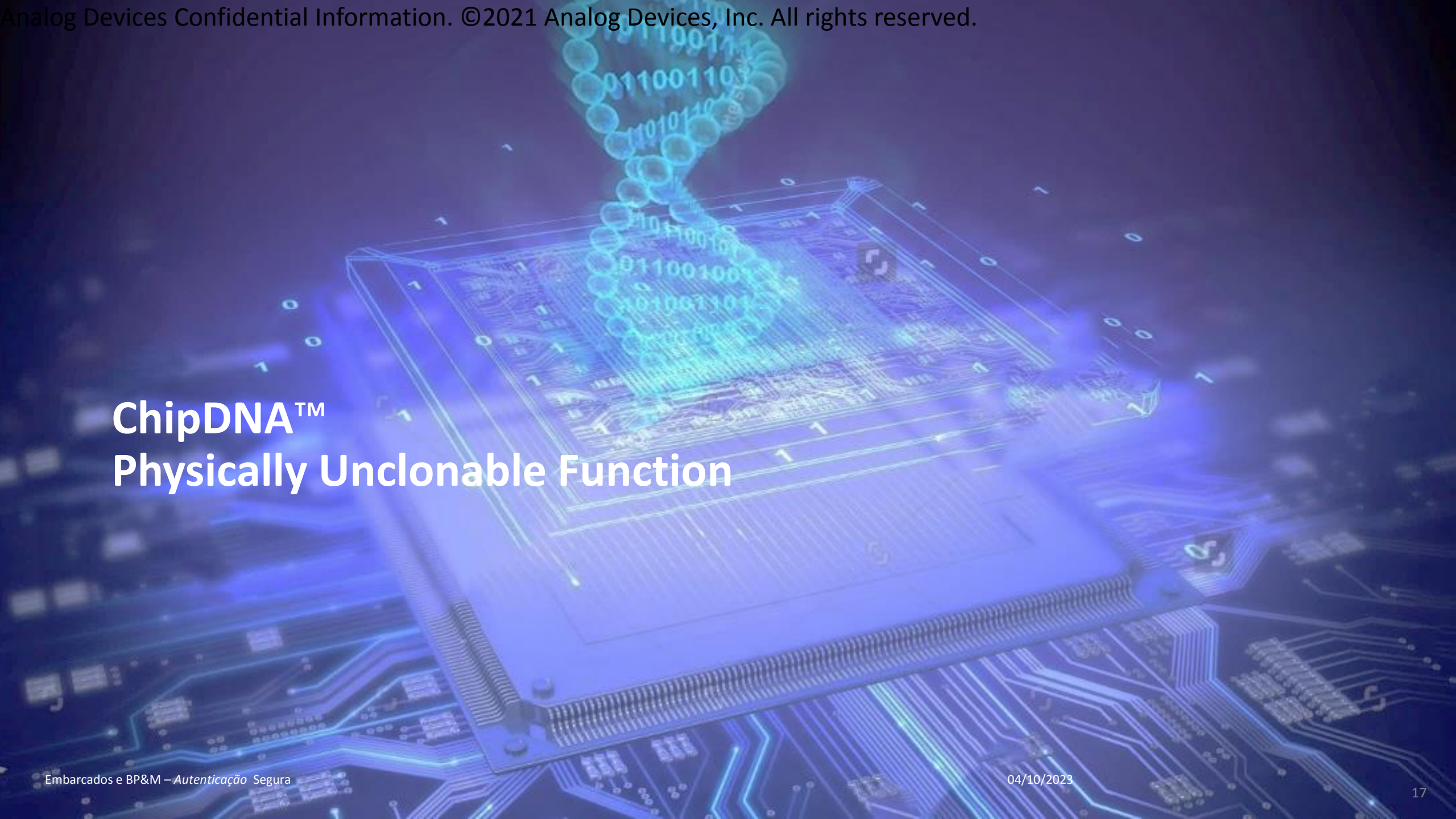


Data Confidentiality

Encryption enables data confidentiality

- Our products supports **symmetric** encryption
  - Asymmetric is a possibility too
- AES is the most popular standard in embedded systems
- Encryption key can be computed as a session key following **mutual** authentication
  - Elliptic Curve Diffie Hellman (ECDH) is a way to establish a session key
  - Solves the key distribution issue





ChipDNA™
Physically Unclonable Function

Security Solutions Are Under Relentless and Sophisticated Attack

Fault Injection
Voltage, timing, temperature, laser

SCA
DPA, SPA, EMI

Maxim's Solution
ChipDNA™

?
Invasive
Microprobe, FIB, reverse engineering

ChipDNA™ Technology

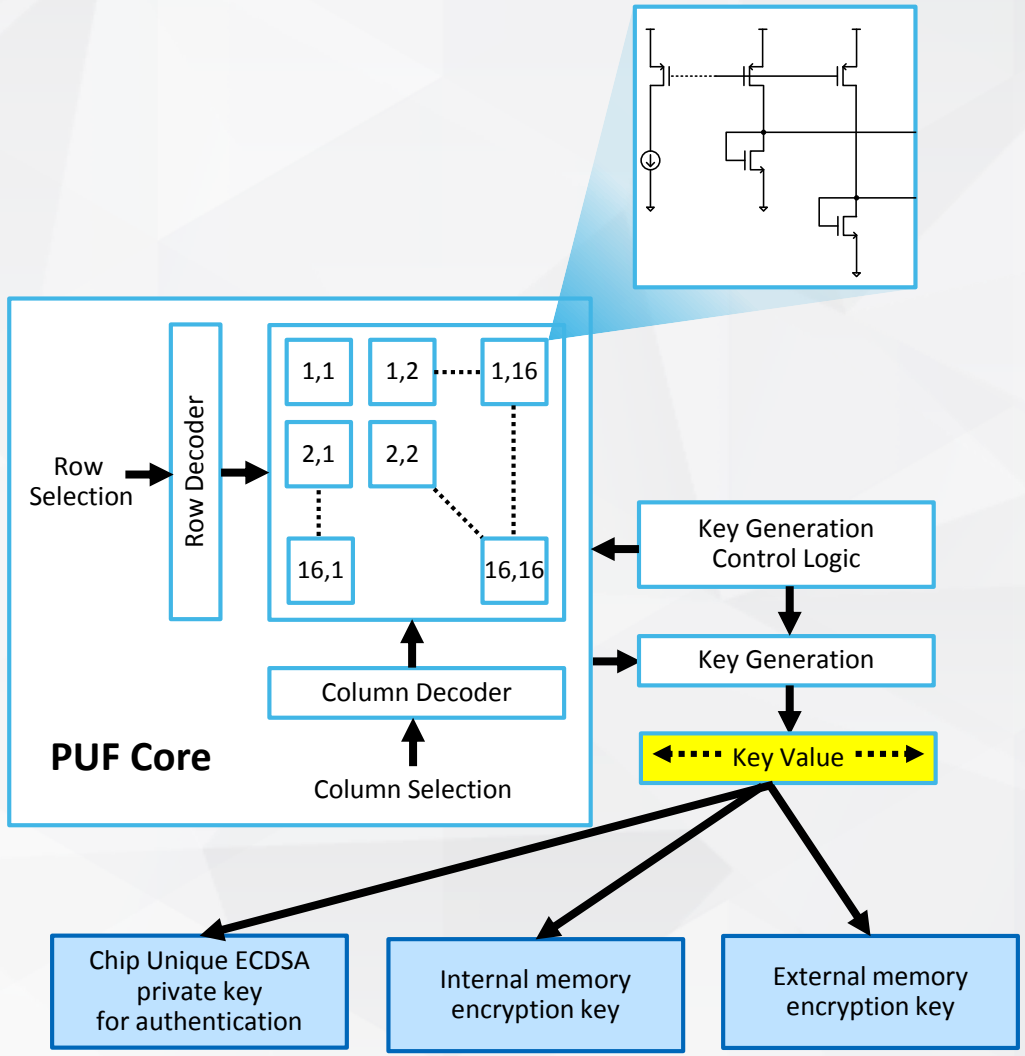
- CHIPDNA is ADIs PUF implementation
- What it does:
  - Utilizes random electrical properties of IC devices to implement a physically unclonable function (PUF)
  - PUF key is a fingerprint of the IC, tied to random manufacturing process variations
  - PUF produces unique and repeatable root cryptographic key for each IC
  - The key is removed from volatile memory once used
- Benefits:
  - Meets NIST cryptographic quality
  - Ultimate protection of cryptographic keys and sensitive data from invasive security attacks
  - Eliminates or simplifies system key management
  - High reliability

You Can’t Steal a Key that Isn’t There

CHIPDNA™

ADI'S PUF IMPLEMENTATION

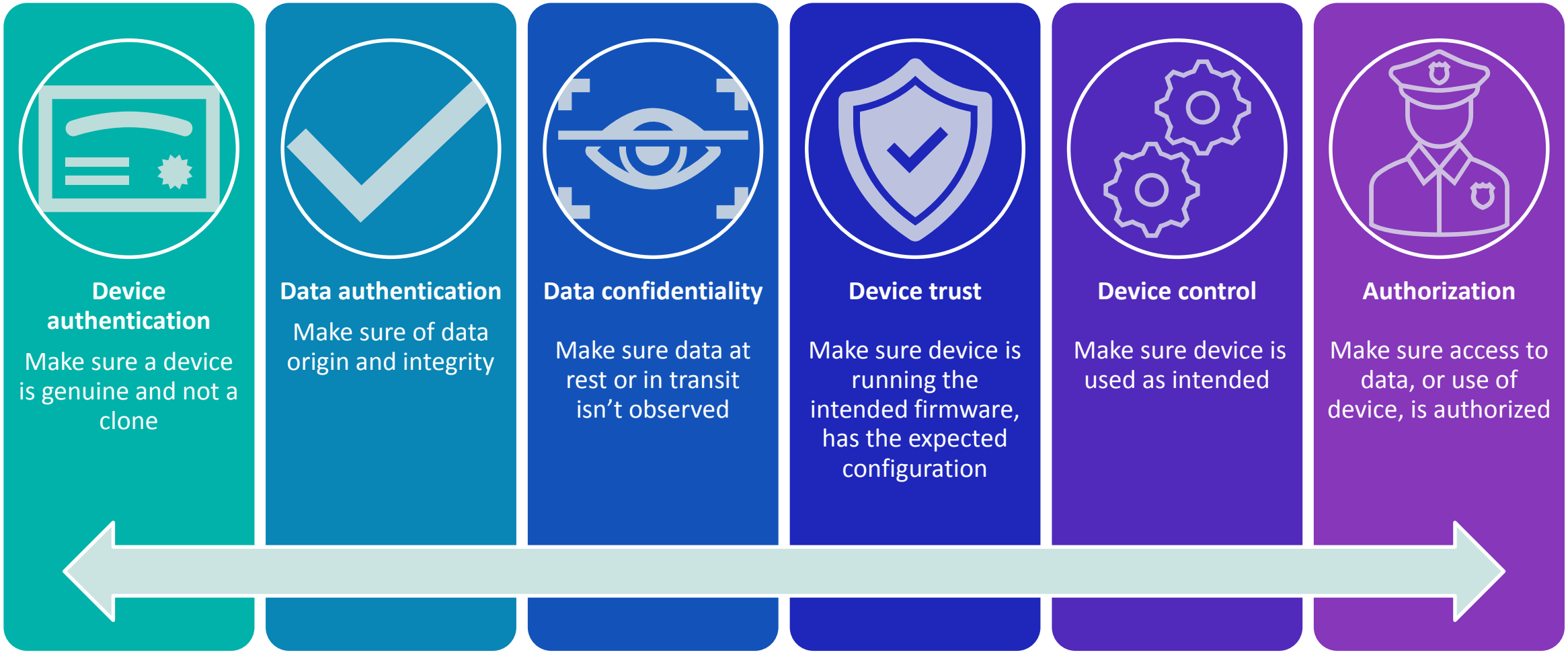
- PUF element
  - I/V characteristic of an analog structure
- Characteristics are random
  - Analog mismatches of PUF elements produce bit values for a crypto key
  - Scalable for required key size
- When needed, key generated and used in secure logic, then erased
- Otherwise, key does not exist
- High reliability – process, temp, age, voltage
- High crypto quality – NIST randomness



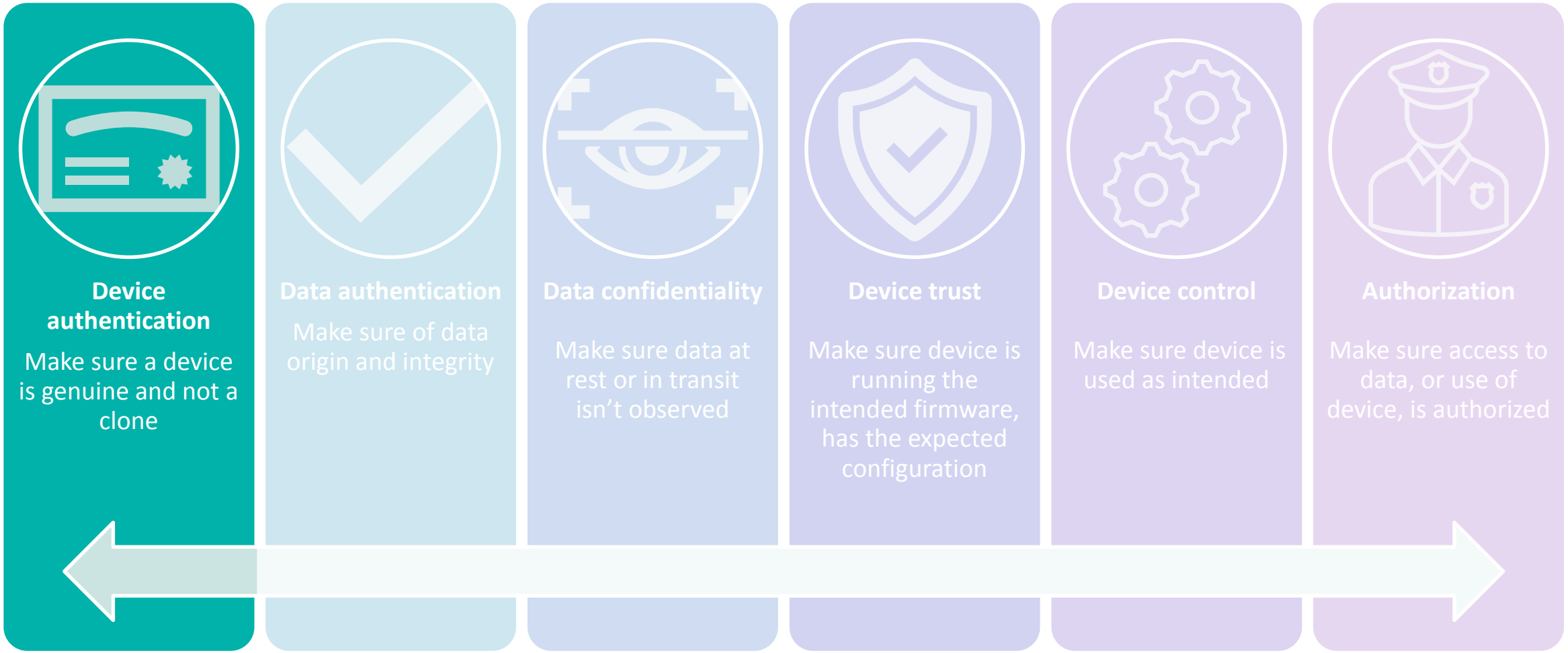
Agenda

- Part 3
  - Soluções da Analog Devices.

Secure authenticator capabilities



Device Authentication



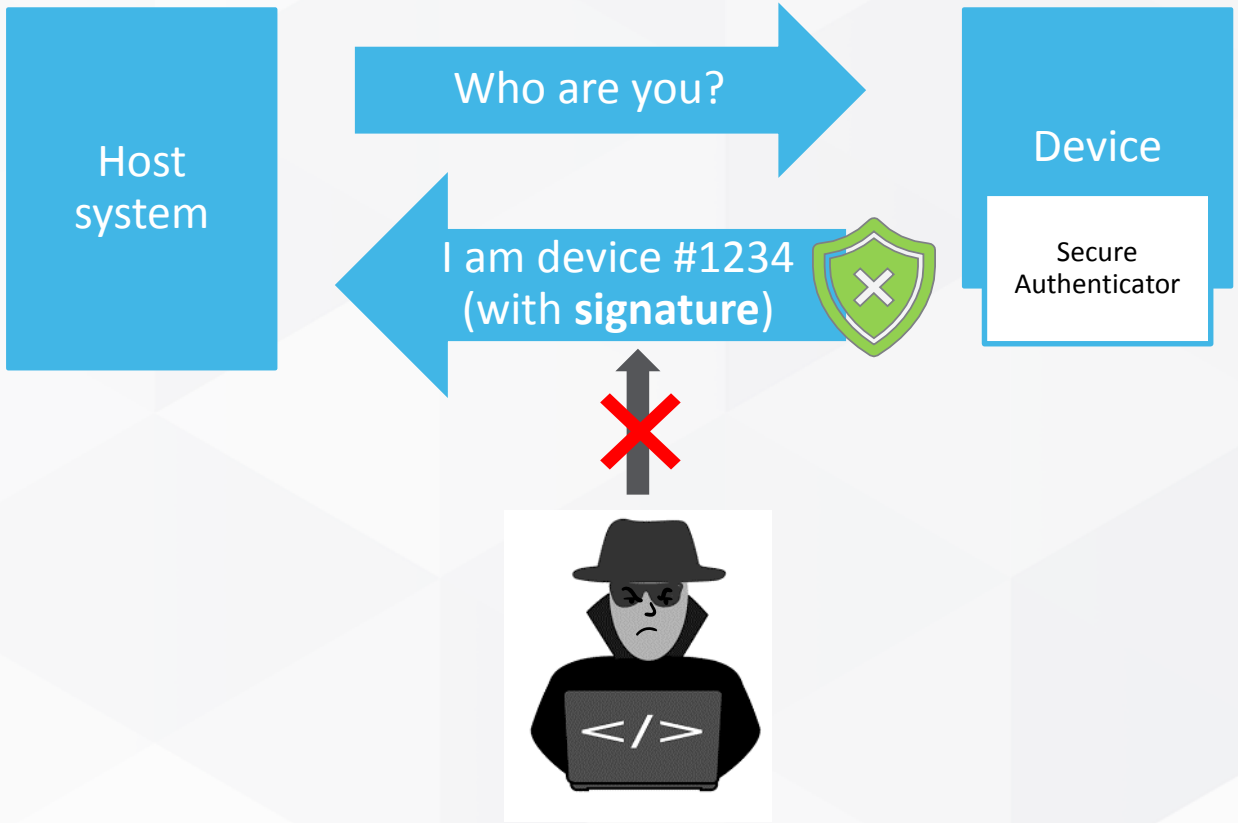
Device Authentication Use Case

Why ?

- Prevent counterfeit
  - Accessories, e.g module
  - Consumables, e.g. Ink Cardridge
- Prevent rogue devices on networks
- Access control
- IP protection

Device Authentication

- Device identifier is signed with a key
- Two-way authentication possible
- Device identifier cannot be forged or modified



System Configuration Example: 1-Wire® SHA-3

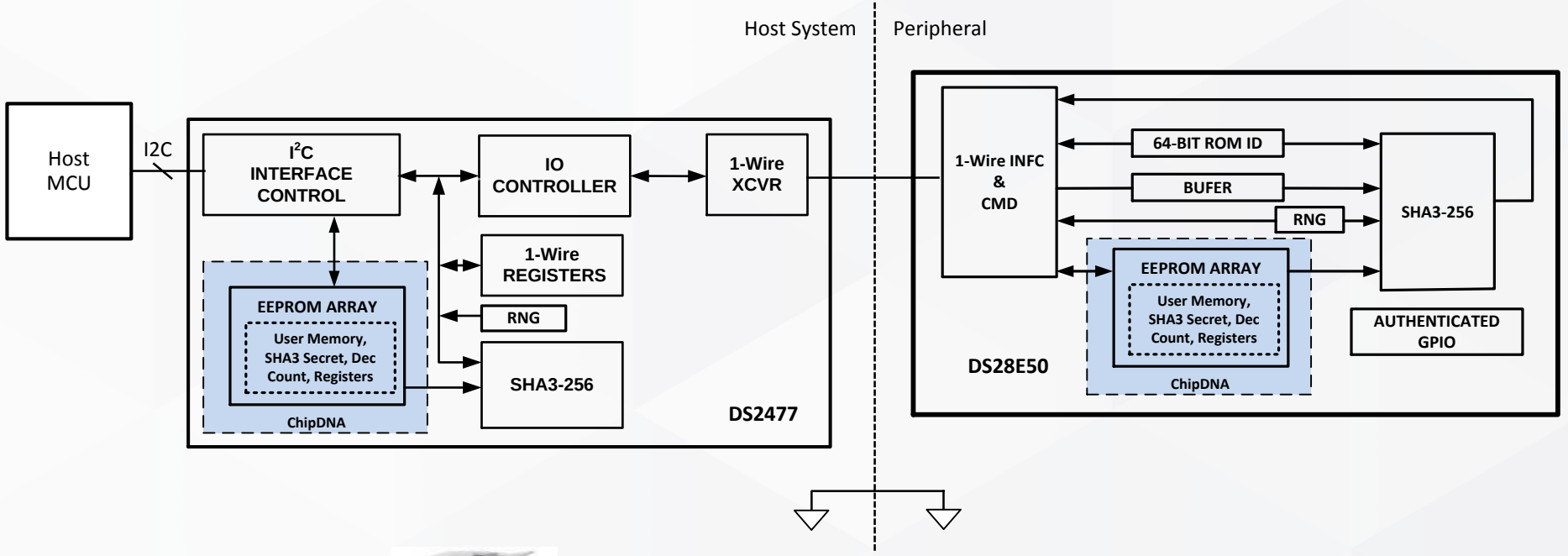
DS2477 / DS28E50

DS28E50

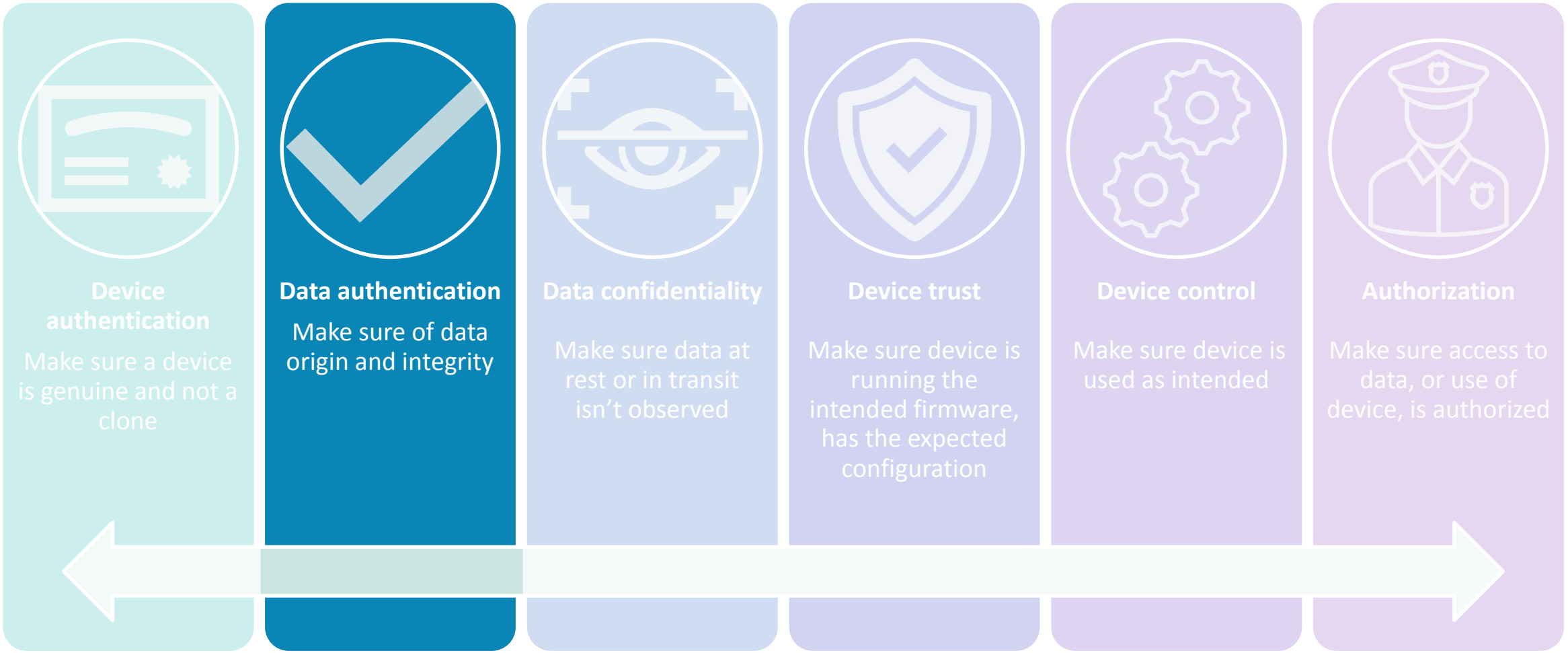
- Protected with ChipDNA PUF
- HW based SHA3-256 challenge & response authentication
- NIST SP 800-90B TRNG with command to output RND
- PUF protected E2 Array
- Decrement-only counter
- Unique read-only serial number (ROM ID)
- 3.3V; -40C to +85C, 3x3 TDFN

DS2477

- Host SHA3 coprocessor and 1-Wire Controller for DS28E50
- I2C, up to 1MHz, interface to host MCU
- 3.3V; -40C to +85C, 3x3 TDFN

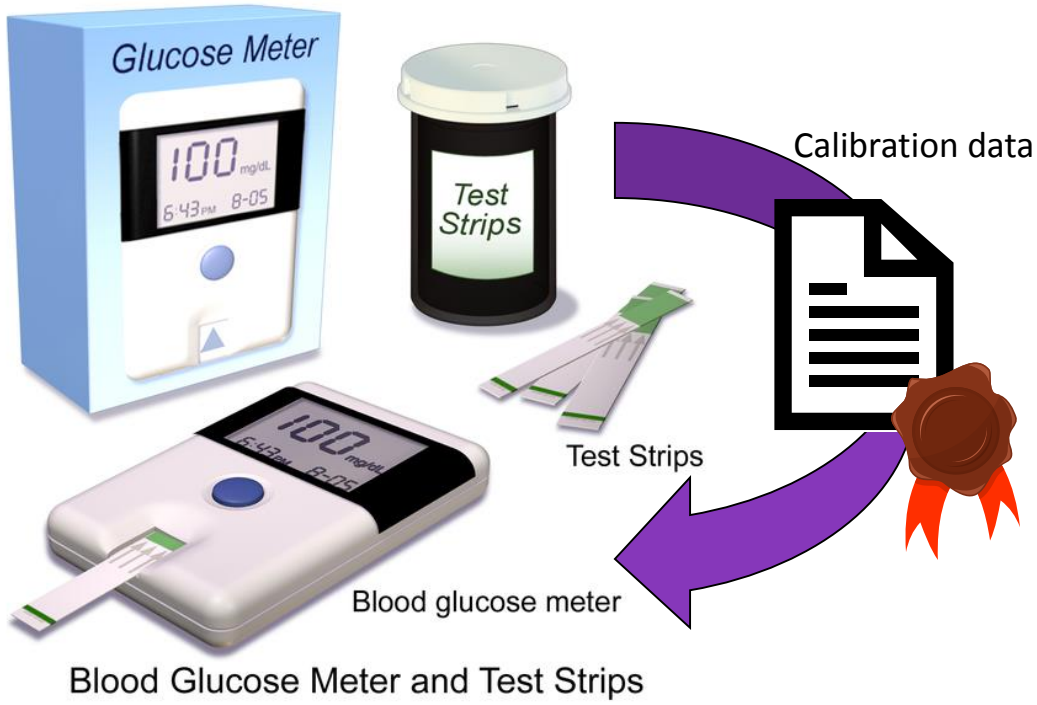


Data Authentication



Data Authentication : Why ?

- Make sure sensitive data are **trusted**
  - Authenticity : genuine, coming from a known entity
  - Integrity : not modified
- Example
  - Calibration data for industrial or medical sensors
  - Measured data from a sensor
- **Signed** but not necessarily **encrypted**
  - Authenticity, Integrity ≠ confidentiality



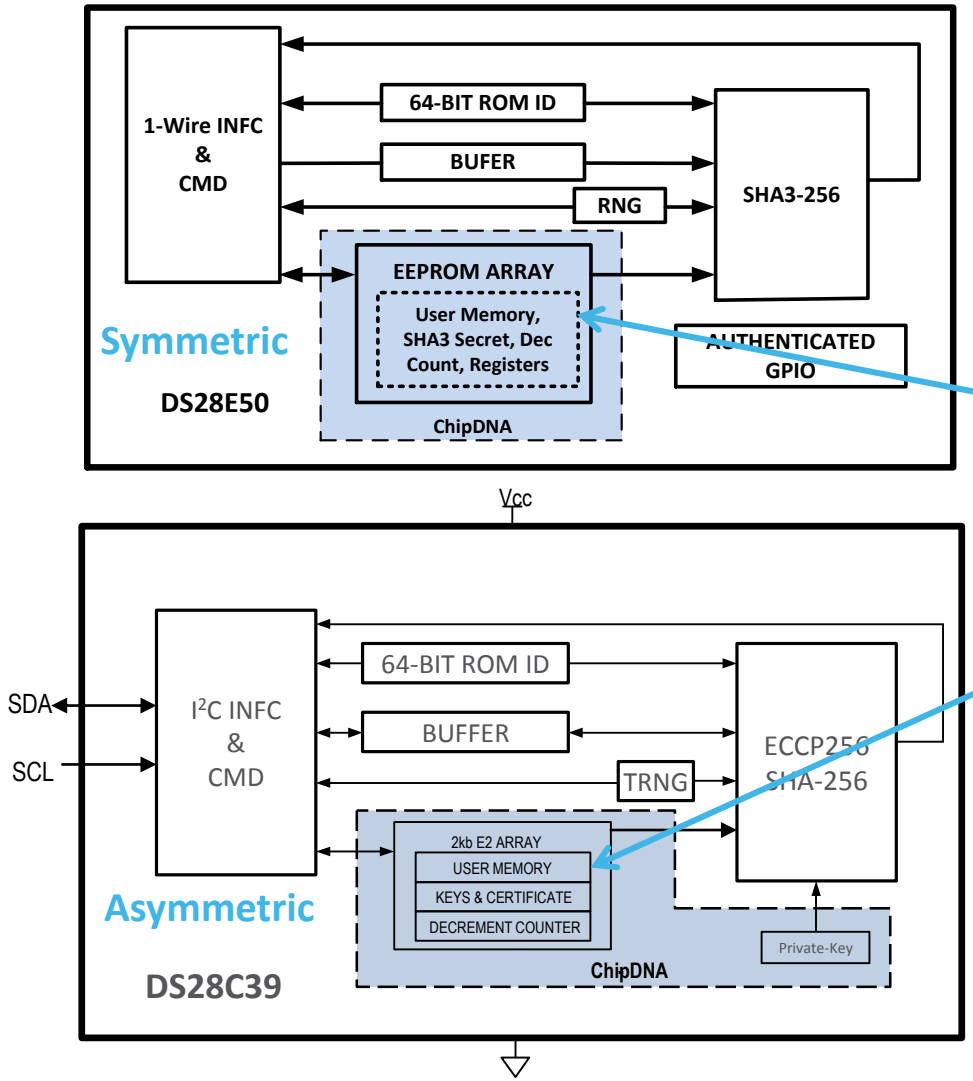
Blood Glucose Meter and Test Strips

Data Authentication Implementation

- Host issues an **Authenticated read** command
- DS28E50 returns
  - data,
  - SHA-3 (ROMID, Random, Secret, data)

OR

- DS28C39 returns
  - data,
  - ECDSA (ROMID, Random, Private Key, data)
- Host **verifies** with SHA-3, secret (DS28E50) or with ECDSA, public (DS28E39)

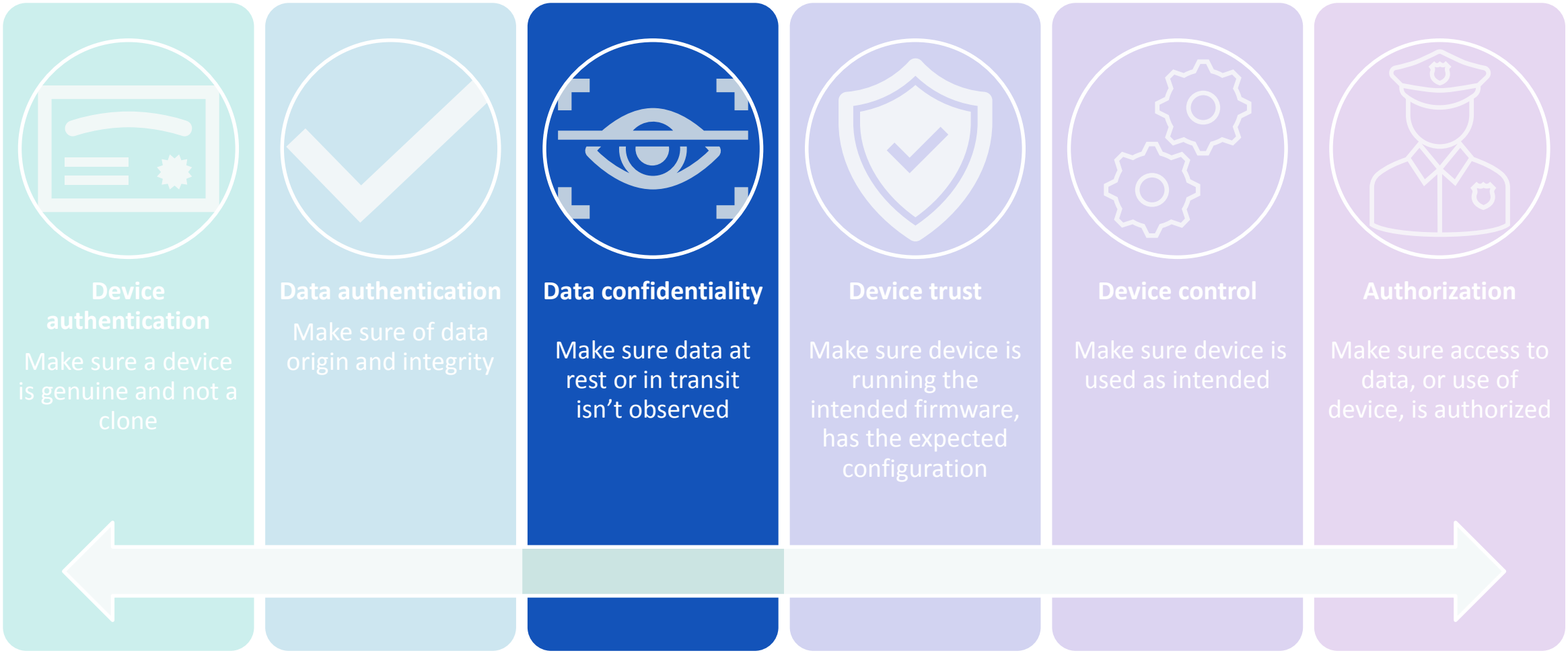


ChipDNA™ protects the secret

Data to be trusted is stored in EEPROM

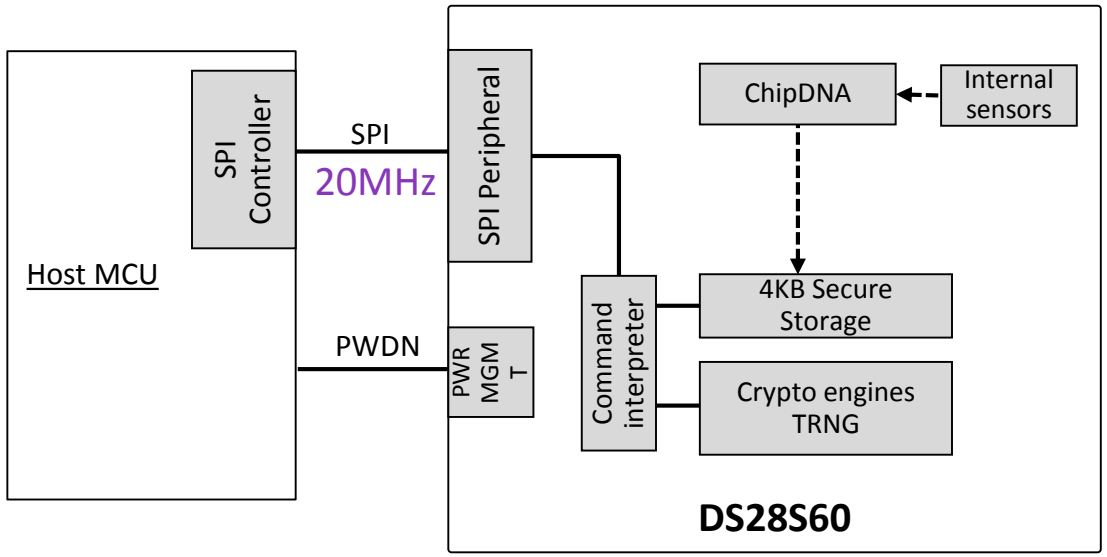
ChipDNA™ generates the private key

Data Confidentialty

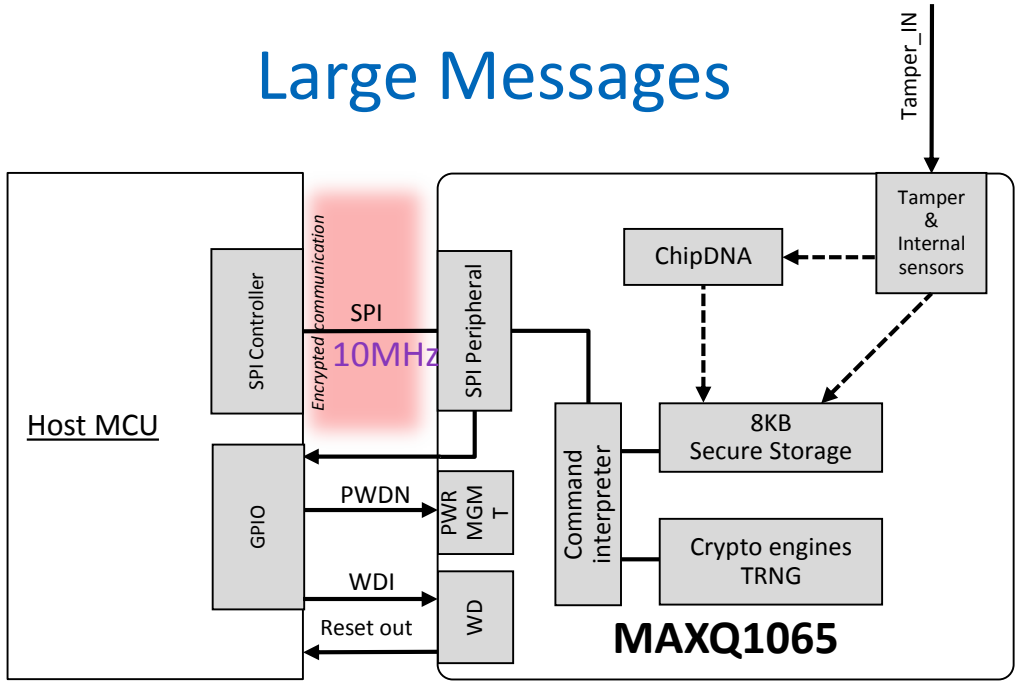


Encryption : Implementation

Small Messages



Large Messages

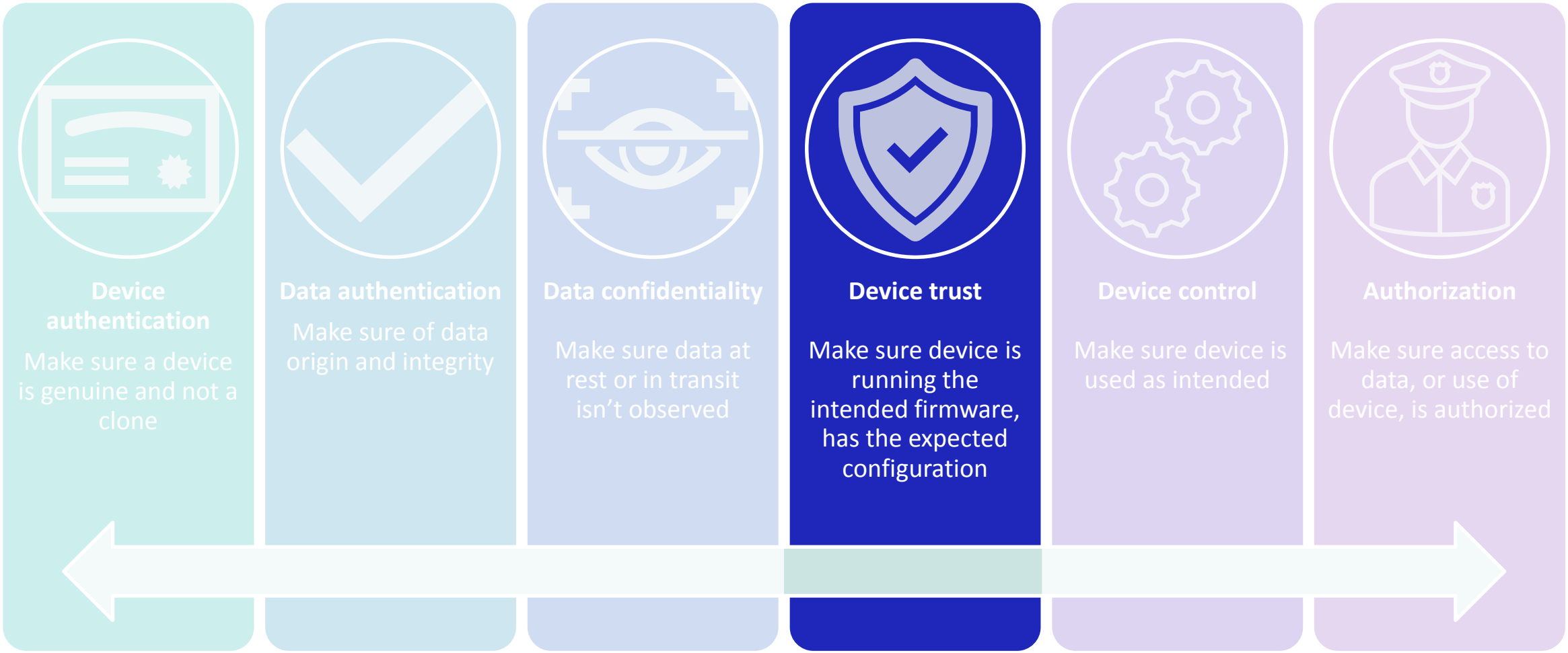


- **ChipDNA™ protection**
- **-40/+105°C, 1.8V/3.3V operation**
- **100nA shutdown mode (**)**
- **12-TDFN 3x3mm pitch 0.5mm**

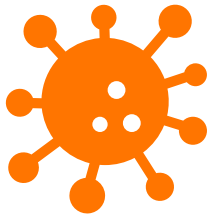
- Key exchange and 256 bytes data encryption/decryption
  - AES-GCM 128 bits
- Data signature/verification : SHA-2 / ECDSA 256
- Encrypted and authenticated read/write memory
- Secure host MCU firmware update

- Full TLS protocol : authentication + stream encryption
  - SHA-2-256
  - ECC (NIST P-256)*: ECDSA, ECDH
  - AES-128/256 (GCM, CBC, ECB, CCM)
- 8kB File System with custom security attributes
- Secure boot and firmware update for host MCU

Device Trust



Device Trust : Why ?



Edge device = entry door putting an entire network at risk

Untrusted software = unpredictable behavior (dumping secret keys..)

Secure boot guarantees genuine, malware free software at boot

Secure updates must guarantee same security level than secure boot

Trusted configuration and parameters

Device Trust / Secure Boot : How ?

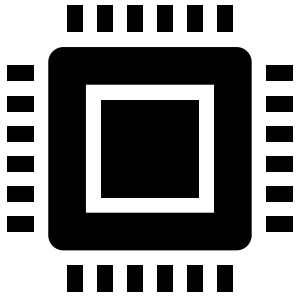
R&D Facility

```
#include <stdio.h>

Main()
{
..
}
```

Signed with **private** key

Field Equipment



Embedded Processor

I2C or SPI

Secure Authenticator

DS28S60 / MAXQ1065

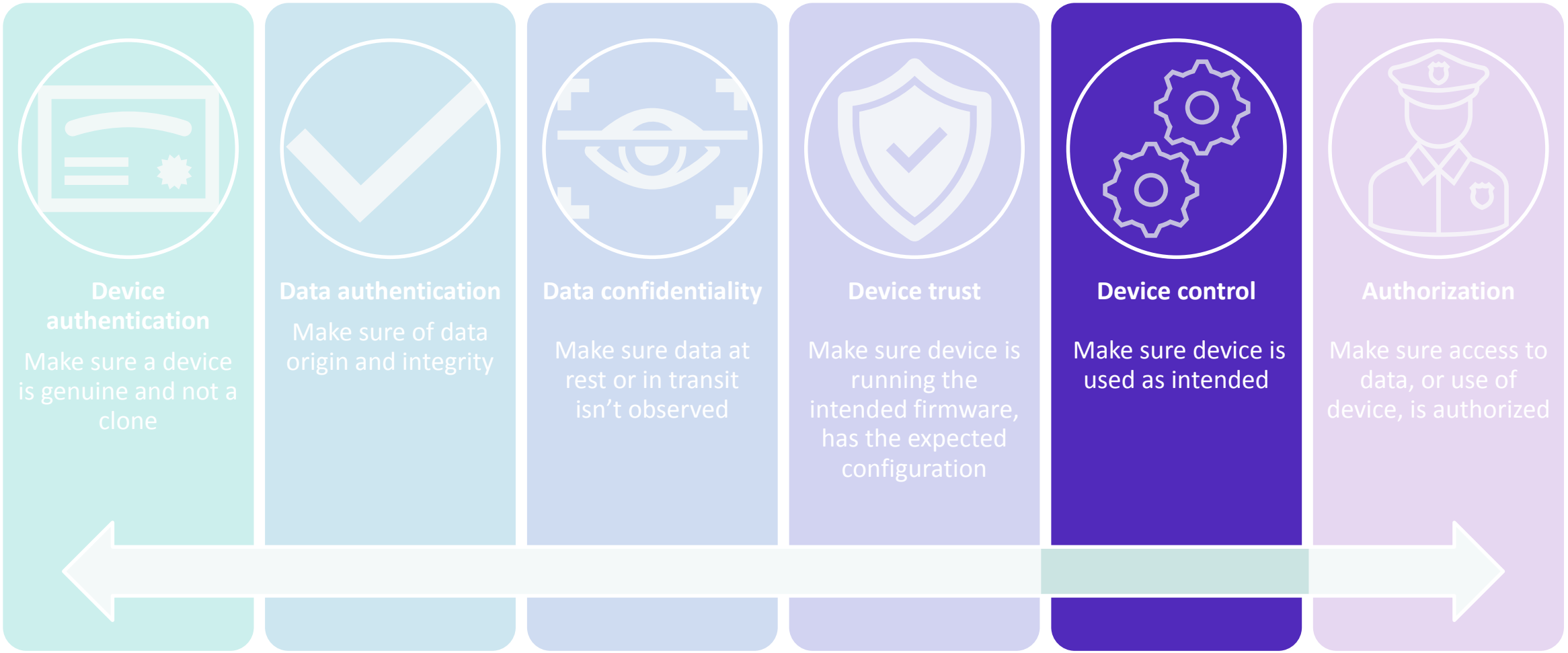
```
#include <stdio.h>

Main()
{
..
}
```

Verifies with **public** key

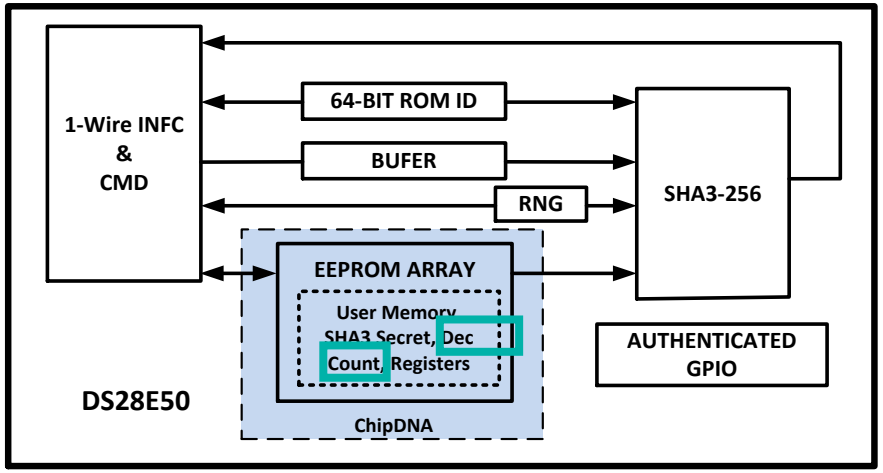
- Secure boot is better supported by Asymmetric crypto
  - No secret stored in the device in the field
  - Private Key stays in R&D facility
- Same technique is applied to secure updates

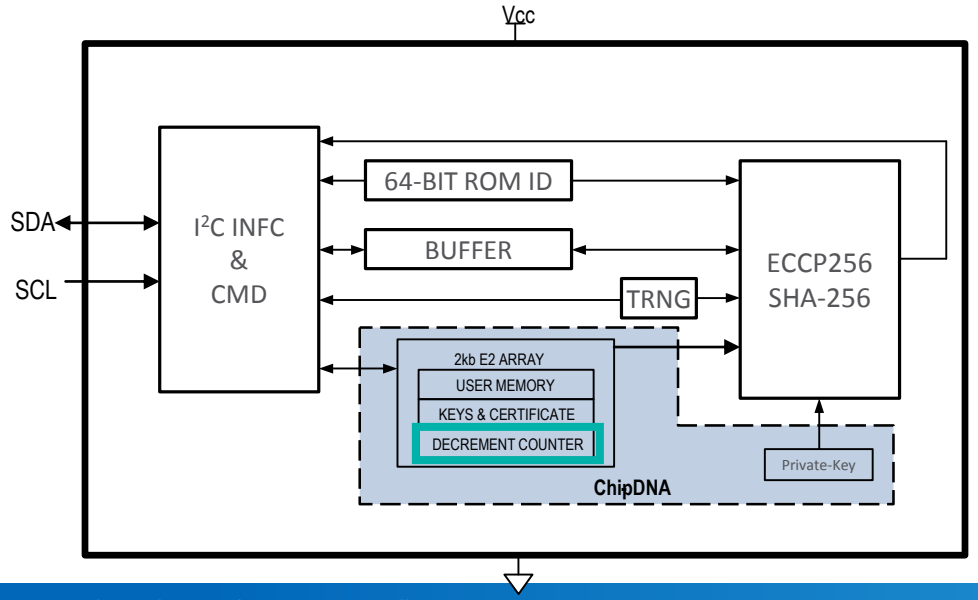
Device Control

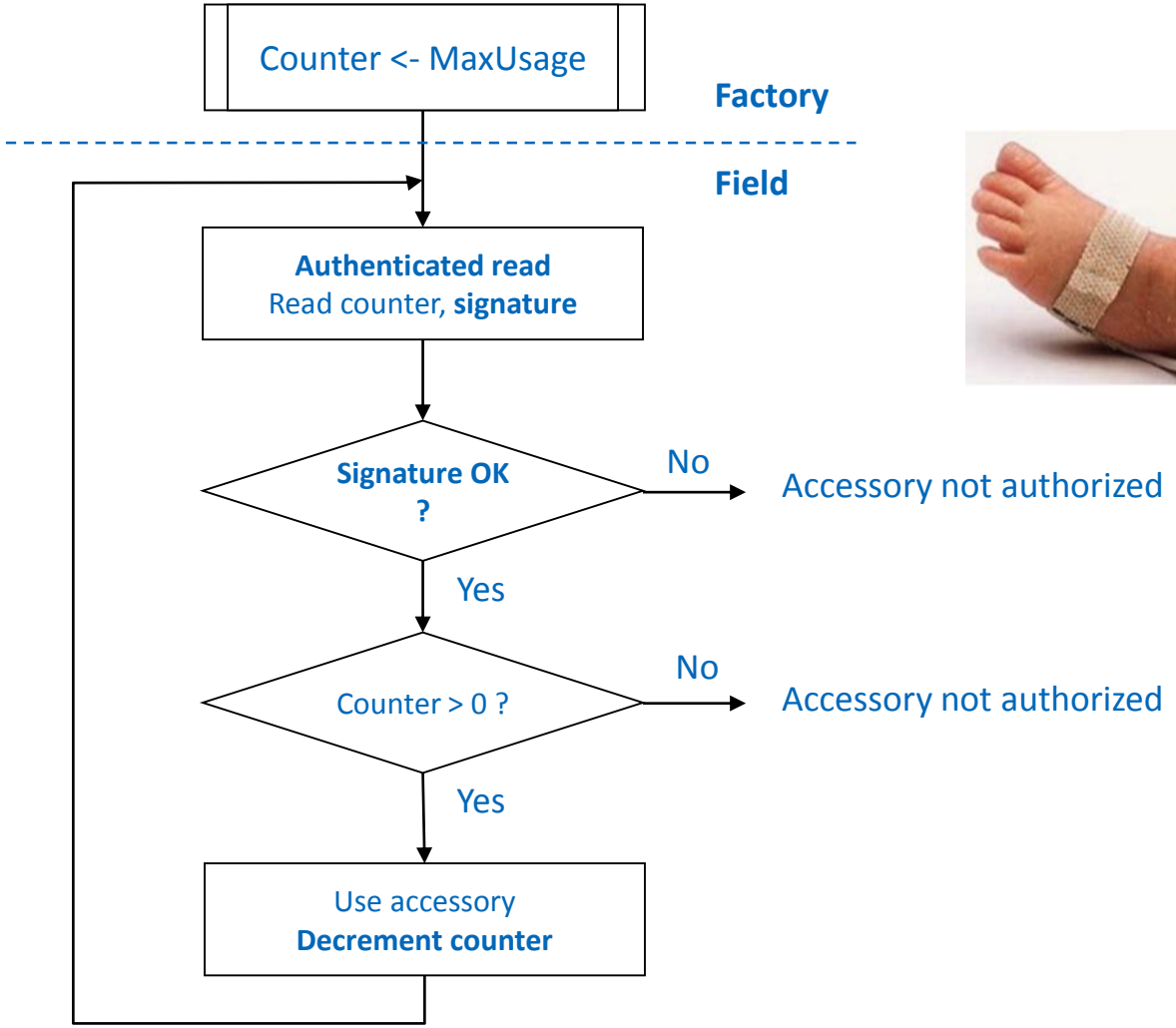


Device Control

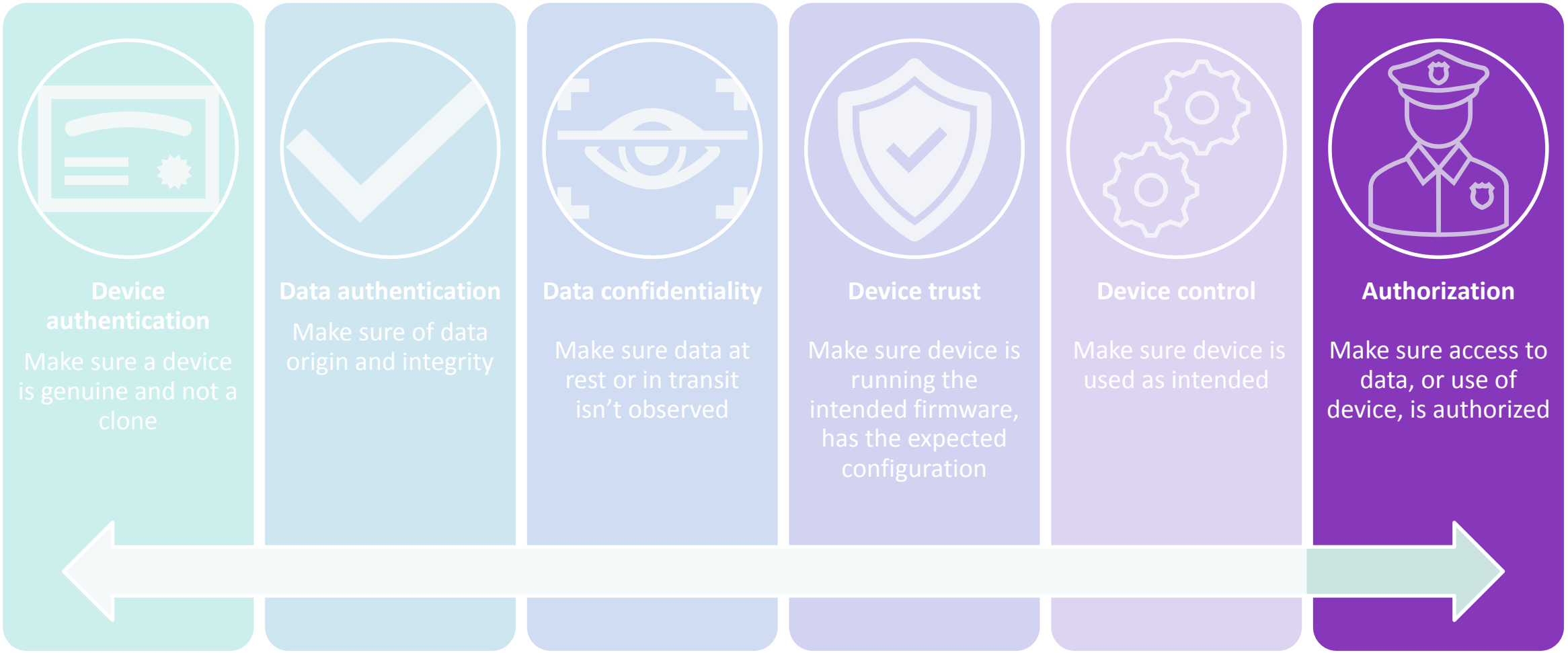
- Typical Case : limit the number of uses of a medical sensor





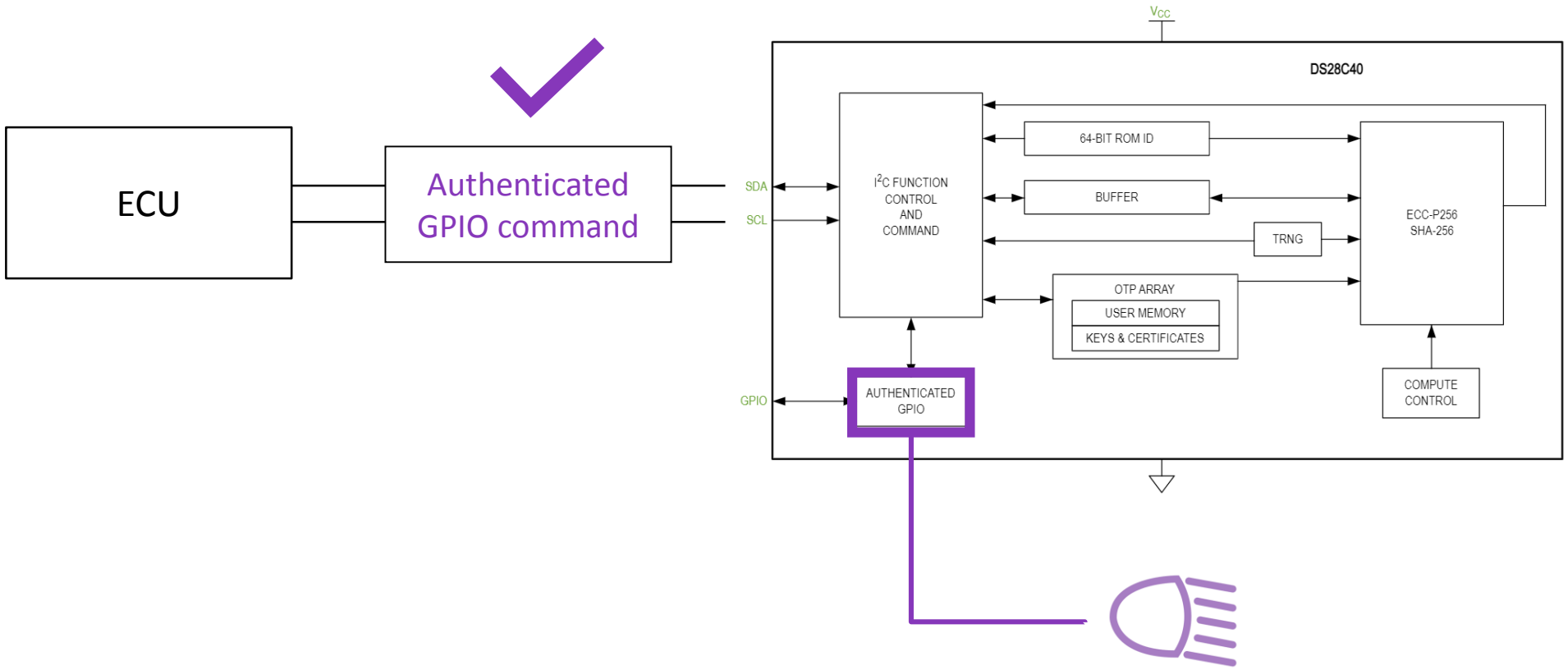


Device Control



Authorization

- Example : Enable Headlamp in a Vehicle



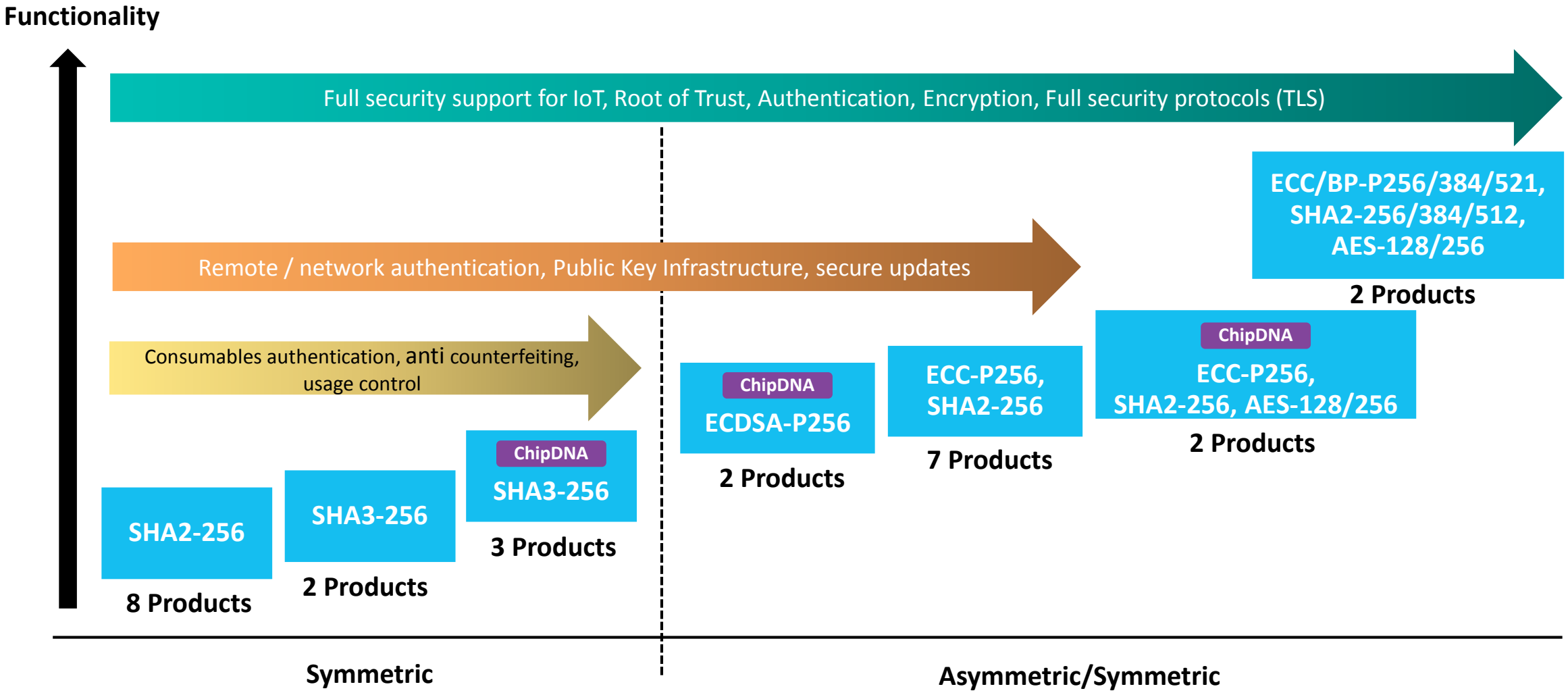
Symmetric/Secret Key Authenticators

	Base Part	Interface	Algo	Secret Keys	User	Memory Technology	Operating environment	Dec counter	Secure I/O	Summary
SHA-3	**DS28C50** **DS28E50**	I2C 1-Wire®	HMAC-SHA3-256	1	1536 (1)	EEProm ChipDNA	3.3V -40/+85°C	1*	1	HW-based SHA3-256 bi-directional authentication w/ ChipDNA PUF protection, 2Kb user EEPROM
	DS28C16 **DS28E16**	1-Wire	HMAC-SHA3-256	0/0	256	EEProm	1.71V-3.63V -40/+85°C	1	0	HW-based SHA3-128 authentication, decrement counter, 256b user EEPROM
	DS2477	I²C Peripheral for host MCU, 1-Wire Controller	HMAC-SHA3-256	2+1	1024	EEProm ChipDNA	2.2 – 3.63V -40/+85°C	0	1	Coprocessor: securely stores system Controller key, offloads SHA3 math, Chip DNA protection, performs 1-Wire communication
SHA-2	**DS28E(L)25**	1-Wire	HMAC-SHA256	1	4096	EEProm	3.3V (1.8V) -40/+85°C	0	0	HW-based SHA-256 w/ bi-directional authentication, 4Kb user EEPROM
	DS28C22 **DS28E(L)22**	I2C 1-Wire	HMAC-SHA256	1	3072 2048	EEProm	3.3V (1.8V) -40/+85°C	0	0	HW-based SHA-256 w/ bi-directional authentication, 2/3Kb user EEPROM
	DS28E(L)15	1-Wire	HMAC-SHA256	1	512	EEProm	3.3V (1.8V) -40/+85°C	0	0	HW-based SHA-256 w/ bi-directional authentication, 512b user EEPROM
	DS2465	I²C for host MCU, 1-Wire Controller	HMAC-SHA256	1	512	EEProm	3.3V -40/+85°C	0	0	Coprocessor: securely stores system Controller key, offloads SHA2 math, performs 1-Wire communication
	MAX66242 **/240**	ISO/IEC 15693 and 18000-3 MODE1 Compatible (13.56 MHz ±7kHz Carrier Frequency) I2C Controller/Peripheral	HMAC-SHA256	1	4096	EEProm	3.3V/harvesting -40/+85°C	0	1	HW-based SHA-256 w/ bi-directional authentication, 4Kb user EEPROM, I2C
	MAX66300	UART/SPI for host MCU, 13.56 NFC transceiver ISO/IEC 15693 and 14443 Type A	HMAC-SHA256	1	4096	EEProm	3.3V -40/+85°C	0	0	Coprocessor: securely stores system master key, offloads SHA2 math, performs 1-Wire communication

Asymmetric/Public Key Authenticators

Base Part	Interface	Algo	Public Keys	Private Keys	Secret Keys	Authority Pub Keys	User/ Certificate	Memory Technology	Operating environment	Dec counter	Secure I/O	Summary
MAXQ1065	SPI (10MHz)	ECDSA p256, ECDH, AES-128 & 256, HMAC SHA-256	Configurable (8Kbytes)					Flash ChipDNA	1.62V-3.63V	Configurable	0	Highly configurable. See Feature Comparisons slides.
DS28S60	SPI (20MHz)	ECDSA p256, ECDH, AES-128 GCM, HMAC SHA-256	4	4	4	4	65,536 (8KB)	Flash ChipDNA	1.62V-3.63V	0	0	HW-based ECDSA or SHA-256 bi-directional authentication, secure boot, 3.6KByte user flash
DS28E39	1-Wire	ECDSA p256	PUF derived	PUF derived	n/a	1 (512b)	1280 (1)	EEProm ChipDNA	3.3V -40/+85°C	1*	0	HW-based ECDSA authentication bi-directional w/ ChipDNA PUF protection, 2Kb user EEPROM
DS28E38	1-Wire	ECDSA p256	1/ PUF derived	1/ PUF derived	n/a	0/0	1024/1536 (1)	EEProm ChipDNA	3.3V -40/+85°C	1*	0	HW-based ECDSA authentication w/ ChipDNA PUF protection, 2Kb user EEPROM
DS28E30	1-Wire	ECDSA p256	1	1	n/a	1	1024/1536 (1)	EEPROM	1.62V-5.25V -40/+85°C	1	0	HW-based ECDSA authentication, 1Kb user EEPROM
DS28C36 DS28E36	I²C 1-Wire	ECDSA p256 ECDH HMAC-SHA256 OTP	2/3	2/3	2/2	1/0	4096/4096	EEProm	2.2V – 3.63V **-40/+105°C**	1	2	HW-based ECDSA or SHA-256 bi-directional authentication, secure boot, secure GPIO, 4Kbit user EEPROM
DS28E83 DS28E84	1-Wire	ECDSA p256 ECDH HMAC-SHA256 OTP	[2]	2	2	2	7168	OTP	3.3V 0/+50°C Gamma ray tolerant	0	1	HW-based ECDSA or SHA256 authentication, DS28E83: 10Kb user OTP memory DS28E84: 10Kb OTP + 15Kb user FRAM
							7168 15360	OTP FRAM		1		
DS28C40 DS28E40	I²C 1-Wire	ECDSA p256 ECDH HMAC-SHA256 OTP	[2]	2	2	2	3072	OTP	3.3V Automotive **-40/+125°C** AEC-Q100-1	0	1	HW-based ECDSA authentication bi-directional automotive grade, 3Kb user OTP memory
DS2476	I²C Peripheral for host MCU	ECDSA p256 ECDH HMAC-SHA256 OTP	2/3	2/3	2/2	1/0	4096/4096	EEProm	2.2V – 3.63V -40/+85°C	1	2	Coprocessor: securely stores system keys, offloads ECDSA math, and more…

Portfolio vs. Use Cases



Use Cases vs. Portfolio

Protect

Cloning, Refurbishing,
Life cycle tracking,
Software and hardware copy,
Feature/licensing control

Security Problem

Connect

Trusted operation
Root of trust, secure communication, secure storage

1-Wire	NFC	I²C	SPI
DS28E25	MAX66240 MAX66242		
DS28E16	MAX66250	DS28C16	
DS28E50 *ChipDNA*		DS28C50 *ChipDNA*	
DS28E30			
DS28E39 *ChipDNA*		DS28C39 *ChipDNA*	
DS28E35			
DS28E83/84			
DS28E40		DS28C40	
			DS28S60 *ChipDNA*
			MAXQ1065 *ChipDNA*

Legend

- Symmetric
- Asymmetric
- Symmetric/Asymmetric
- Radiation tolerant
- Automotive AEC-Q100

ADI Provides A Complete Security Solution

Peripheral Security ICs

- **Simple command set for:**
  - Secure storage and key management with access control
  - Cryptographic services
  - Secure Download/Boot
  - Secure GPIO
  - Secure counters
- **Tamper resistance**
- **ChipDNA Physically Unclonable Function**
- **Unique ID**
- **Low power**
- **1-Wire, I2C, SPI, NFC**
- **Small footprint packages**

Host Solutions

- EV-Kits & C-source for all products
- Reference designs
- TLS libraries
- **Host-side co-processor**
- 1-Wire line drivers
- HF transceiver/receiver

Value add Services

- **Factory Programming** of keys/secrets and certificates
- Device customization (ROMID, data)

Technical Support

- **C-source SW** for all products
- System design expertise
- Review of HW/SW implementation
- Antenna design support

Agenda

- Part 4
  - Exemplos de casos de uso.

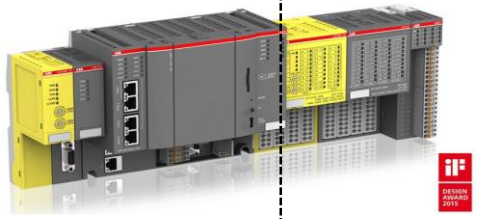
Device Authentication Use Cases

Battery authentication

DS2477
SHA-3 Coprocessor

DS28E16 or DS28E50
SHA-3 Authenticators

PLC I/O module authentication

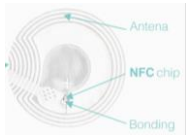


DS2477
SHA-3 Coprocessor

DS28E16 or DS28E50
SHA-3 Authenticators

Drug Cardridge Authentication

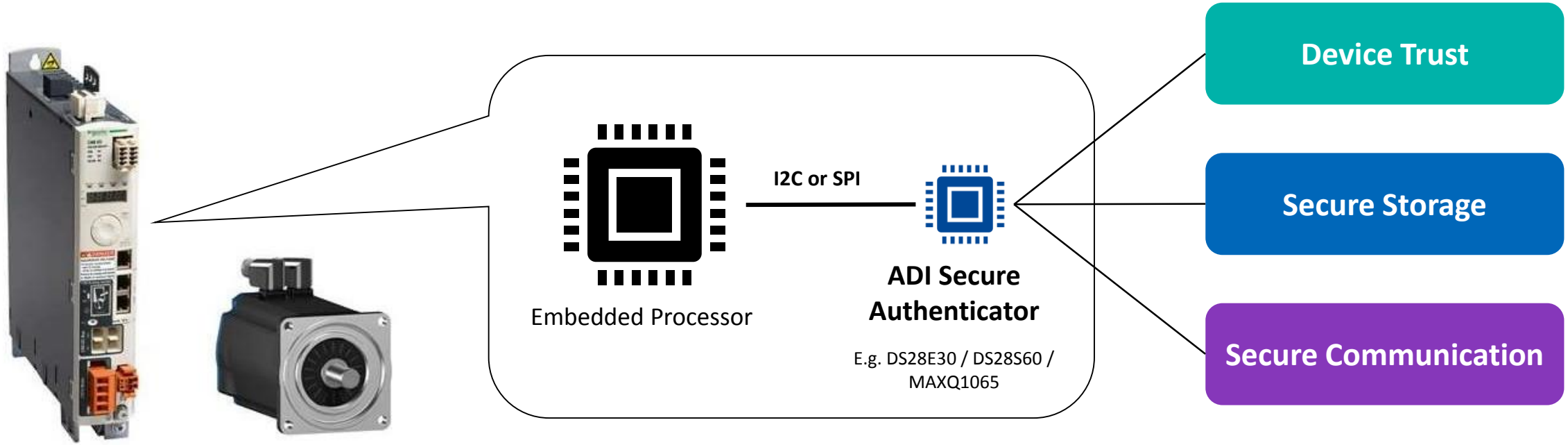
MAX66300
NFC/RFID Reader with SHA-3 Authentication



MAX66250
NFC/RFID SHA-3 Authenticator

Fundamentals of Connected Objects Security

Example : Connected Motor Control



Connected Object Security : EV Charging Station

- Security Requirements
  - User data protection
  - Secure communication with server
  - Root of Trust / Secure boot
- Products
  - DS28S60
  - MAXQ1065
- Drivers
  - Regulations (Germany)

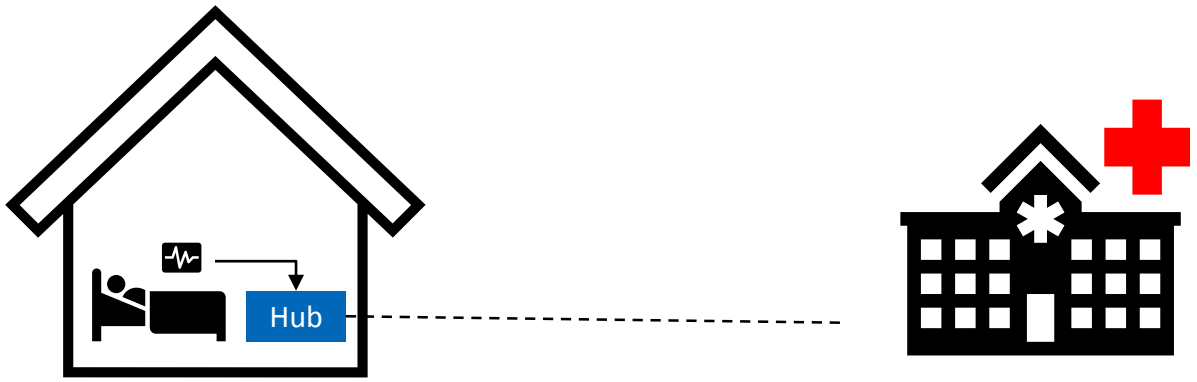
Connected Object Security : Metering

- Security Requirements
  - User data protection
  - Secure communication with server
  - Root of Trust / Secure boot
- Products
  - DS28S60
  - MAXQ1065
- Drivers
  - Regulations
  - Power grid availability

Electricity, gas, water

Connected Object Security : Medical Hub

- Security Requirements
  - User data protection
  - Secure communication with doctor / hospital o
    - Certificate distribution
    - Mutual authentication
    - Encryption
- Products
  - DS28S60
  - MAXQ1065

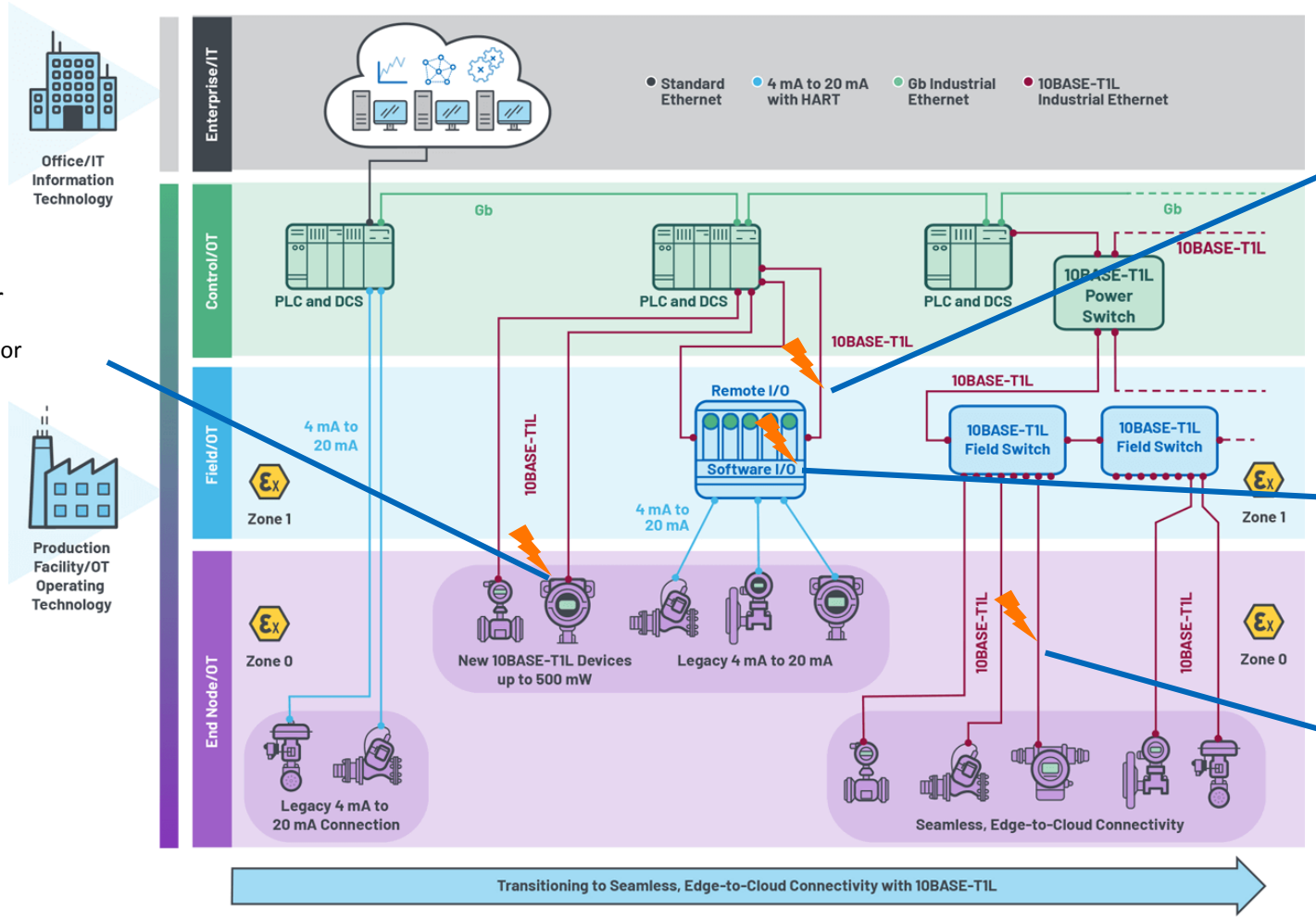


Security in Industrial Infrastructure

Threat : fake sensor inserted

Answer : authenticated sensor

DS28E39/C39 ECDSA Authenticator



Threat : rogue command sent by hacker

Answer : authenticated command

DS28S60, MAXQ1065

Ultra low power crypto controllers

Threat : malware infecting the infrastructure

Answer : secure boot, secure fw update

DS28S60, MAXQ1065

Ultra low power crypto controllers

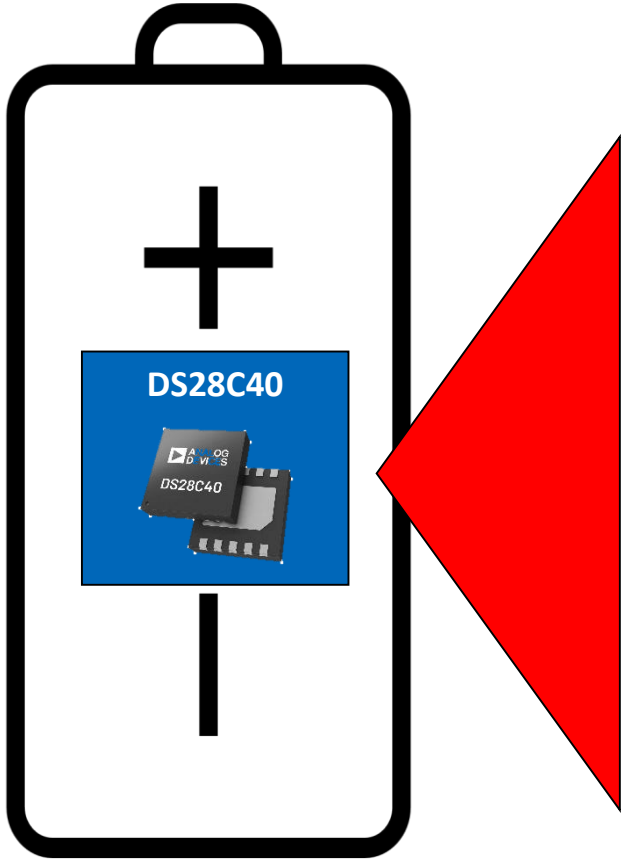
Threat : sensor data modified on its way

Answer : authenticated and integrity protected data

DS28S60, MAXQ1065

Ultra low power crypto controllers

Application of DS28C40 to EV batteries



Secret used to authenticate the battery stack/pack (*)

ROM ID

Unique ID to uniquely identify the battery stack/pack

Extra memory can be used to track historical information

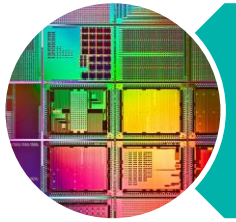
Various protection schemes possible for R/W

Safety: prevent use of unsafe batteries

Business: prevent unfair competition against low quality replacement

Usage control: Prevent misuse of decommissioned batteries

Competitive Advantages



Products you can get

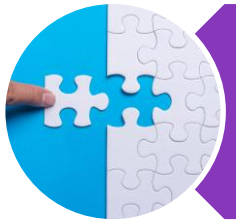
- 12 to 13 weeks current typical lead times

Widest Portfolio in the industry

- From cost effective SHA products to full IoT solutions
- Variety of interfaces including contactless NFC

Strongest security

- Future proof SHA-3
- ChipDNA™ Physical Unclonable Function provides the **most secure storage**



Differentiated features

- Down to 300µA idle, 100nA sleep
- Secure GPIO

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

Analog Devices / BP&M

04/10/2023

Webinar Embarcados

Thank you!

Questions: contato@bpmrep.com.br

Juliano Kowalczuk Cioffi – ADI FAE for Brazil