The Impact of Cyber Resilience Act on Products Containing Digital Element

MICROCHIP

A Leading Provider of Smart, Connected and Secure Embedded Control Solutions

SMART | CONNECTED | SECURE

Tibor Szarka

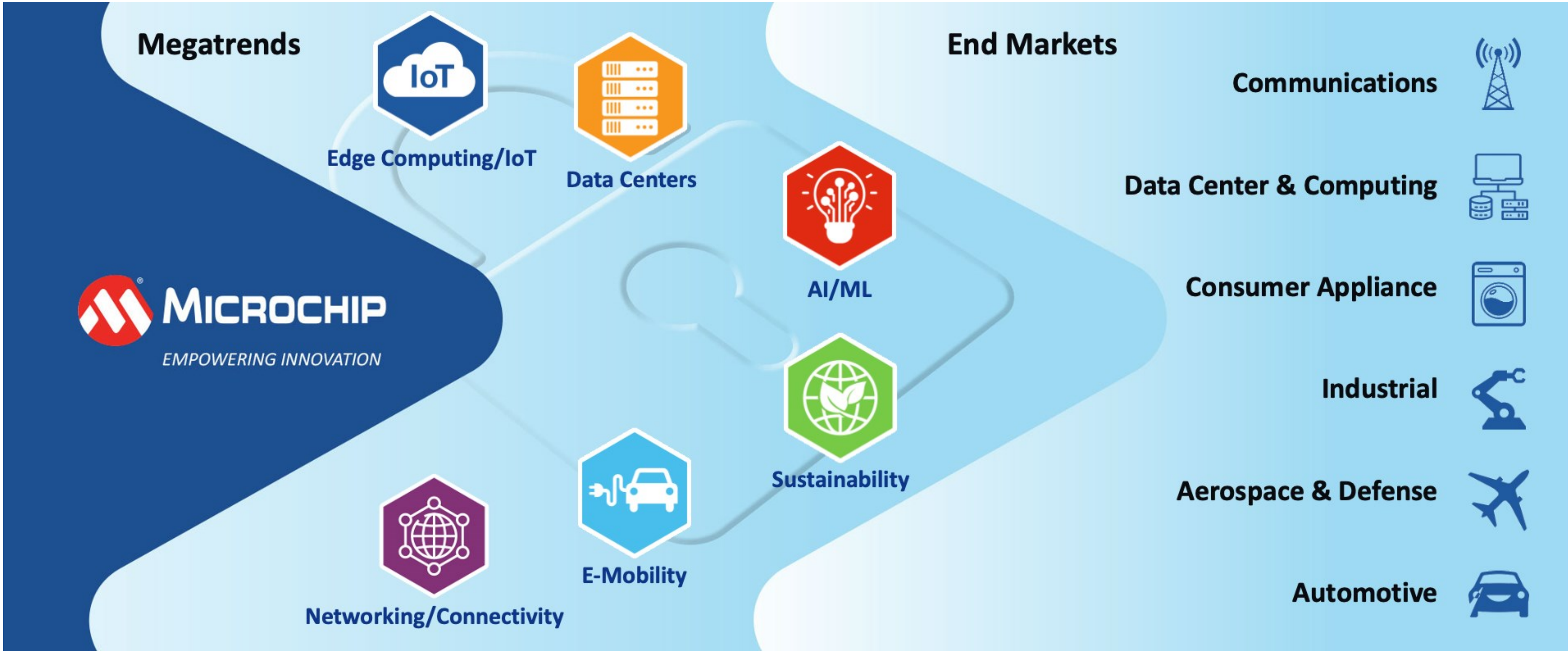
2025

Disclaimer

- This presentation provides general information about the European Union Cyber Resilience Act (EU CRA) and is intended as a high-level overview for informational purposes only. It is designed for individuals seeking an introduction or general details about the EU CRA.

- The content in this presentation does not constitute legal, regulatory, or professional advice and should not be used as a substitute for consulting relevant experts or authorities. While we strive to ensure that the information provided is accurate and up-to-date, we cannot guarantee its completeness or accuracy.

Strategic Focus and In-Depth Knowledge



Megatrends

End Markets

- Communications
- Data Center & Computing
- Consumer Appliance
- Industrial
- Aerospace & Defense
- Automotive

Influences Driving Security

Security is no Longer an Option; it is a Requirement

Mandated by Regulations: EU Cyber Resilience Act (CRA) and Network and Information Systems Directive 2 (NIS2)

Automotive
UNECE WP.29
R155/R156

ISO 21434

Industrial

IEC 62443

Power
Supply
Security

Wireless
Power
Qi® 1.3/2.0

Medical

IoT and
Consumer

EN 303 645

EU Cyber Resilience Act

Brief Summary of Regulation 2024/2847

Addresses

Commercial Entities placing products on the European market

- Manufacturers
- Importers
- Distributors

Scope

“Products with digital elements”

- Hardware
- Software
- “SaaS”
  (remote data processing solutions)

Purpose

Create a legal framework for cybersecurity ensuring digital elements are placed on the market with fewer vulnerabilities and entities take security seriously throughout the product’s life cycle.

Timeline

Entry into force (EIF)
December 10, 2024

Reporting Obligations
September 11, 2026

Product Conformity
December 11, 2027

Requirements

Fulfillment of essential requirements

Reporting
Incidents, exploited vulnerabilities

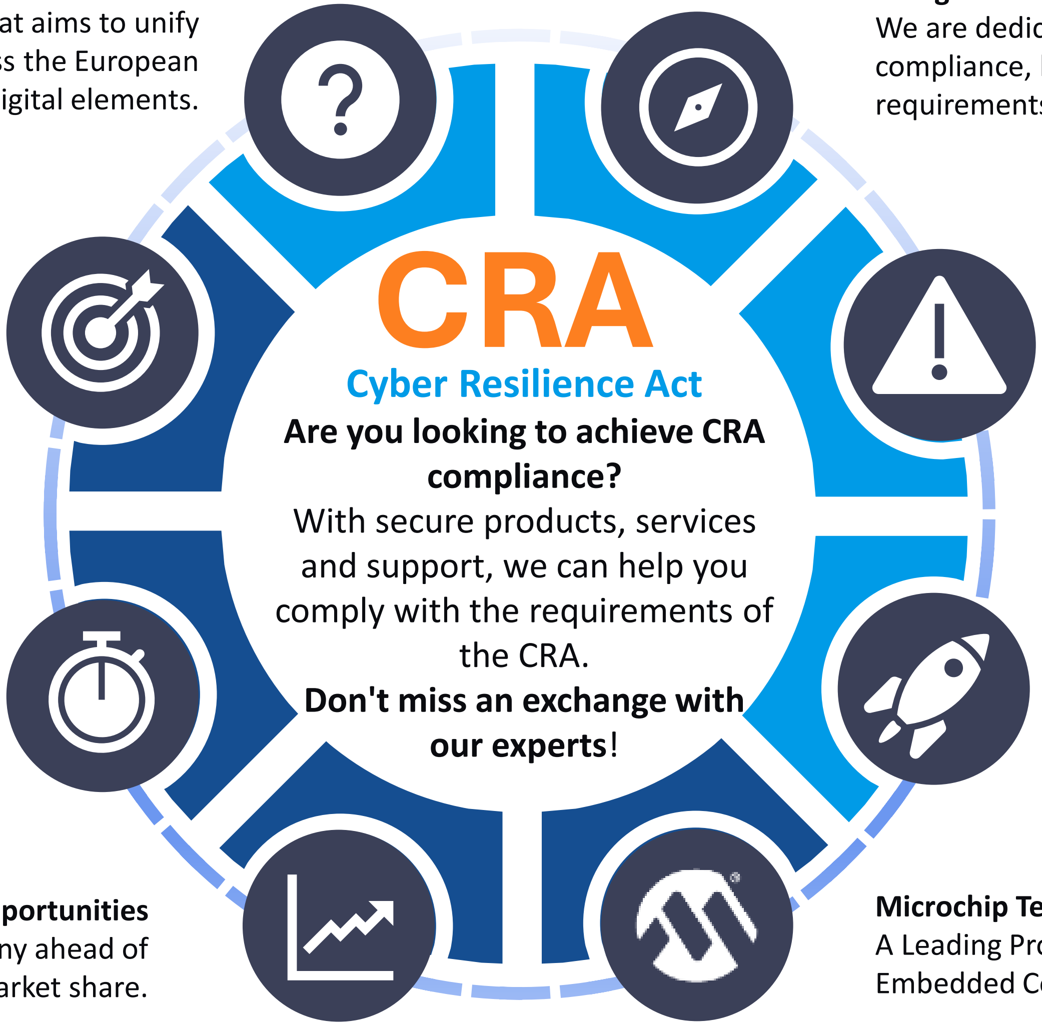
Conformity Assessment
(TÜV, bureau veritas..)

Benefits

Based on NLF
(New legislative Framework)
→ Binding in its entirety and directly applicable in all Member States (without national transposition by Member States e.g. Directive RED)

EU Cyber Resilience Act (CRA) Compliance - The Challenge

Let's do it - Proven Cyber Security Competence and Solutions from Microchip



CRA

Cyber Resilience Act

Are you looking to achieve CRA compliance?

With secure products, services and support, we can help you comply with the requirements of the CRA.

Don't miss an exchange with our experts!

What is the CRA?
The CRA is a regulation that aims to unify cybersecurity requirements across the European Union (EU) for products with digital elements.

What is the Goal of the CRA?
The goal of the CRA is to create a legal framework for cybersecurity and to ensure that digital elements are placed on the market with fewer vulnerabilities.

Why Work Towards Compliance?
Companies must comply with the cybersecurity requirements of the CRA to avoid severe penalties and market exclusions. Noncompliance can also lead to reputational damage.

Opportunities
Early compliance positions your company ahead of competitors, enhancing customer trust and market share.

Navigate Challenges
We are dedicated to supporting your journey to compliance, helping you meet regulatory requirements with confidence and expertise.

Implications for Your Business
The CRA includes requirements for risk assessments, vulnerability management and security patches. Compliance is mandatory.

Next Steps for You
Conduct a comprehensive cyber risk assessment, implement a secure product development process and ensure clear documentation and security update plans to ensure compliance and enhance your product security. ISO/IEC 62443 or ETSI EN 303645 Cyber Security standards are essentially supportive.

Microchip Technology
A Leading Provider of Smart, Connected and Secure Embedded Control Solutions.

EU Cyber Resilience Act

Categories

Product with digital elements (Default)

~ 90 % of products in scope

Important product with digital elements

Product with a core functionality of a category listed in ANNEX III

Critical product with digital elements

Product with a core functionality of a category listed in ANNEX IV

EU Cyber Resilience Act

Categories

Critical Products with digital elements - Annex IV

- Hardware Devices with Security Boxes
- Smart meter gateways within smart metering systems as defined in Article 2 (23) of Directive (EU) 2019/944 and other devices for advanced security purposes, including for secure crypto processing.
- Smartcards or similar devices, including secure elements

Important Products with digital elements - Annex III

- Divided into class I and class II as set out in Annex III and meet one or both of the following criteria:
  - a) The product with digital elements performs primarily functions critical to the cybersecurity of other products, networks or services, including securing authentication and access, intrusion prevention and detection, endpoint security or network protection
  - b) The product with digital elements performs a function which carries a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products or to the health, security or safety of its users through direct manipulation, such as a central system function, including network management, configuration control, virtualisation or processing of personal data.

EU Cyber Resilience Act

Important Products Class I

1. Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers
2. Standalone and embedded browsers
3. Password managers
4. Software that searches for, removes, or quarantines malicious software
5. Products with digital elements with the function of virtual private network (VPN)
6. Network management systems
7. Security information and event management (SIEM) systems
8. Boot managers
9. Public key infrastructure and digital certificate issuance software
10. Physical and virtual network interfaces
11. Operating systems
12. Routers, modems intended for the connection to the internet, and switches
13. **Microprocessors with security-related functionalities**
14. **Microcontrollers with security-related functionalities**
15. **Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities**
16. Smart home general purpose virtual assistants
17. Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems
18. Internet connected toys covered by Directive 2009/48/EC that have social interactive features (e.g. speaking or filming) or that have location tracking features
19. Personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 or Regulation (EU) 2017/746 do not apply or personal wearable products that are intended for the use by and for children.

EU Cyber Resilience Act

Important Products Class II

1. Hypervisors and container runtime systems that support virtualized execution of operating systems and similar environments

2. Firewalls, intrusion detection and/or prevention systems

3. **Tamper-resistant microprocessors**

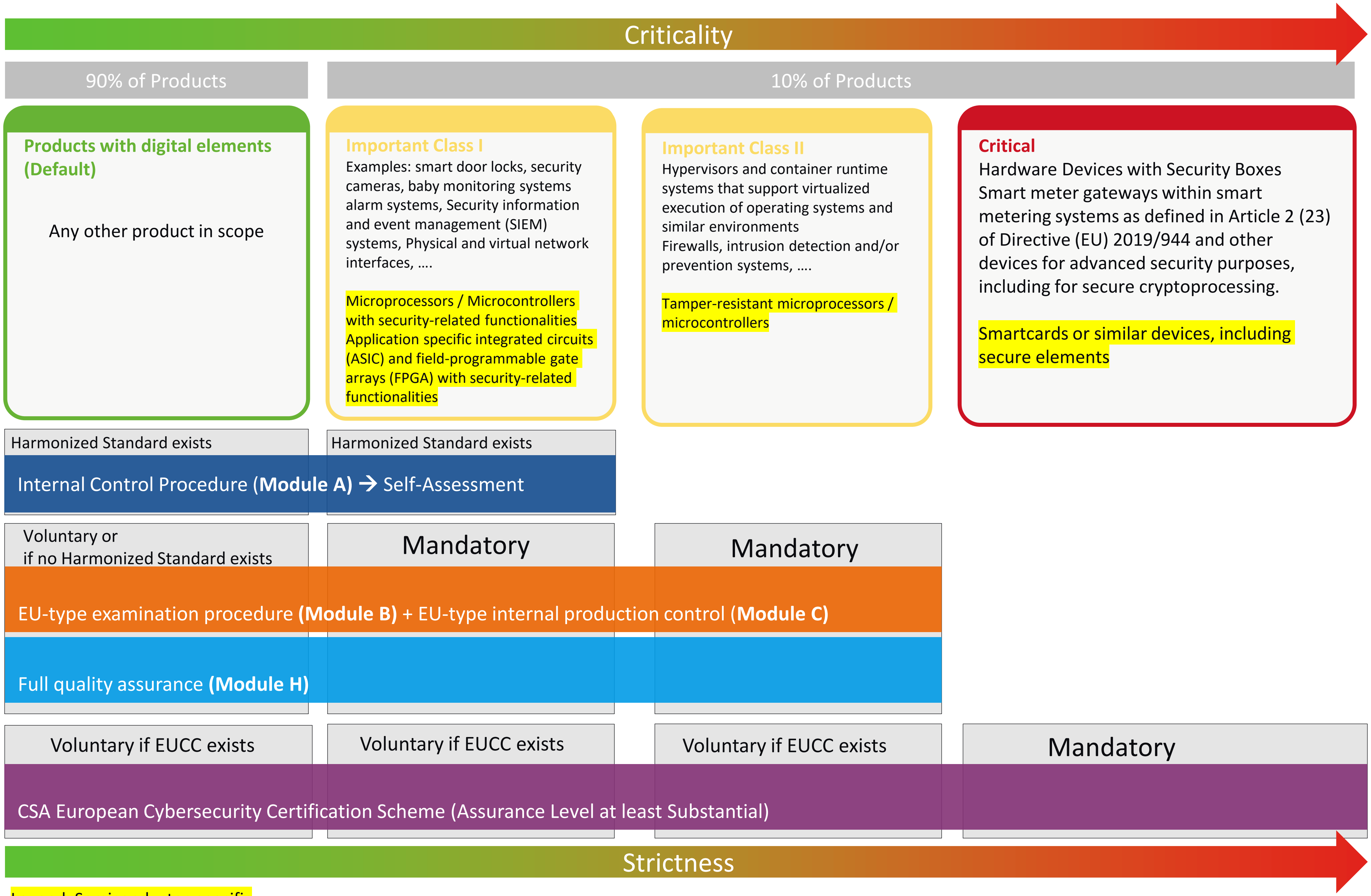
4. **Tamper-resistant microcontrollers**

New Approach (EU New Legislative Framework)

Conformity Assessment Procedure (768/2008/EG)

Module	Design	Production	Notified Body involved?
Internal control A	**Manufacturer** prepares technical documentation	**Manufacturer** declares the conformity by following the essential requirements	No
EU-Type examination B+C	**Manufacturer** prepares the technical documentation and evidence for the correct and secure functioning of the technical design via sample product. **Notified Body** ascertains the conformity of a type against the essential requirements, examines technical documentation and supporting evidence of the technical design and issues EU-type certificate.	**Manufacturer** establishes procedures to ensure consistent production quality and compliance. Regular internal checks and controls are performed to maintain conformity with the certified type. **Notified Body** may conduct periodic audits to verify continued compliance.	Yes
Full quality assurance H	**Manufacturer** establishes a quality system (e.g. ISO 9001) and submits technical documentation **Notified Body** assesses and certifies the quality system	**Manufacturer** operates a checked and approved quality system for production; declares conformity and affixes conformity marking. **Notified Body** controls the quality system	Yes

The manufacturer remains solely responsible for conformity, even if a notified body has been involved in the assessment.



Criticality

90% of Products

10% of Products

Products with digital elements (Default)

Any other product in scope

Important Class I

Examples: smart door locks, security cameras, baby monitoring systems alarm systems, Security information and event management (SIEM) systems, Physical and virtual network interfaces, ….

Microprocessors / Microcontrollers with security-related functionalities Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities

Important Class II

Hypervisors and container runtime systems that support virtualized execution of operating systems and similar environments

Firewalls, intrusion detection and/or prevention systems, ….

Tamper-resistant microprocessors / microcontrollers

Critical

Hardware Devices with Security Boxes

Smart meter gateways within smart metering systems as defined in Article 2 (23) of Directive (EU) 2019/944 and other devices for advanced security purposes, including for secure cryptoprocessing.

Smartcards or similar devices, including secure elements

Harmonized Standard exists

Harmonized Standard exists

Internal Control Procedure **(Module A)** → Self-Assessment

Voluntary or
if no Harmonized Standard exists

Mandatory

Mandatory

EU-type examination procedure **(Module B)** + EU-type internal production control (**Module C)**

Full quality assurance **(Module H)**

Voluntary if EUCC exists

Voluntary if EUCC exists

Voluntary if EUCC exists

Mandatory

CSA European Cybersecurity Certification Scheme (Assurance Level at least Substantial)

Strictness

Legend: Semiconductor-specific

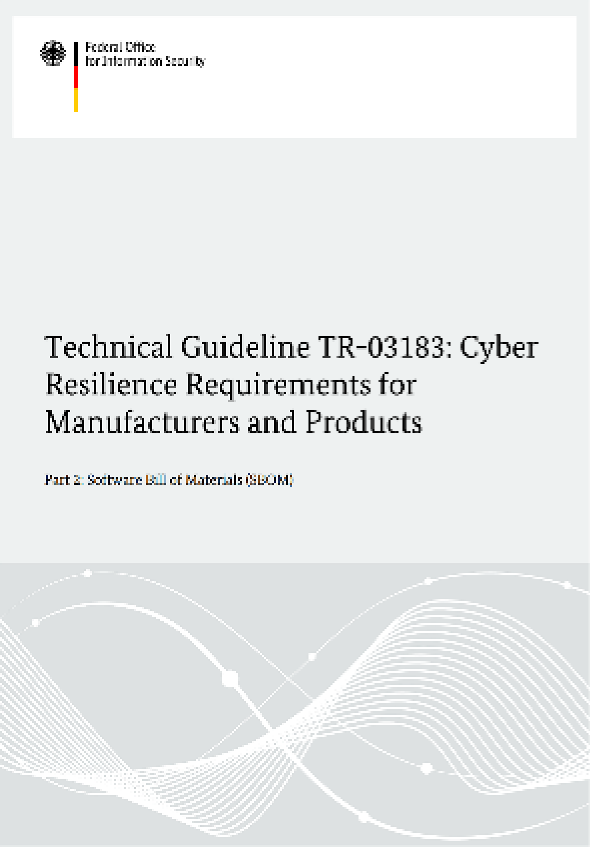
CRA

Technical Guidelines Help Comply With EU CRA

Federal Office for Information Security

Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products

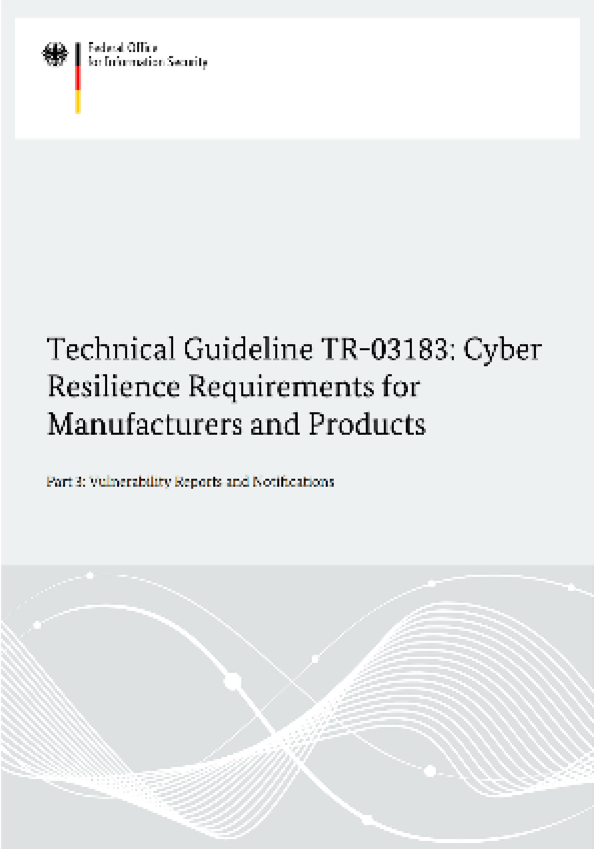
Part 1: General requirements



Federal Office for Information Security

Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products

Part 2: Software Bill of Materials (SBOM)



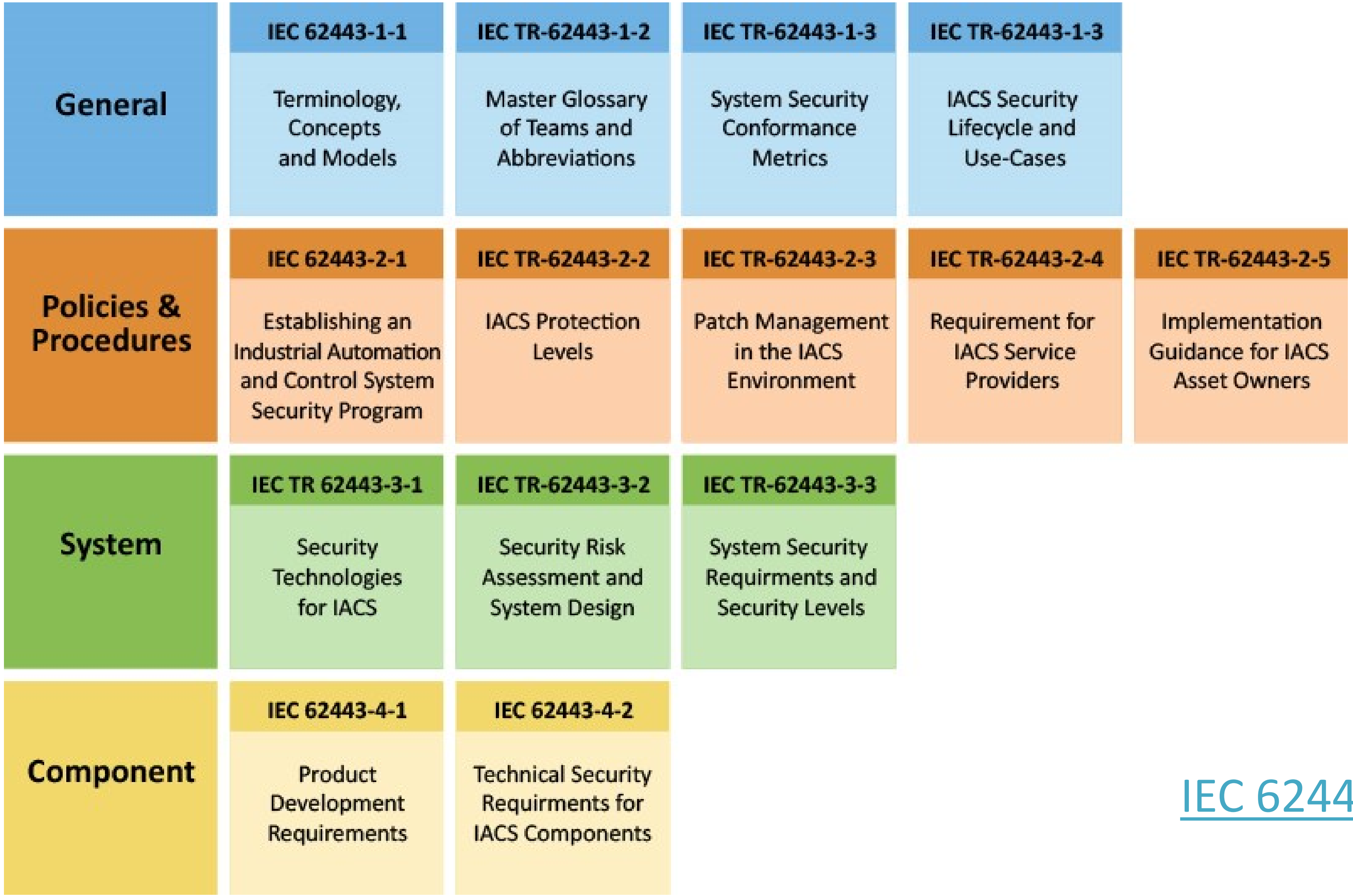
Federal Office for Information Security

Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products

Part 3: Vulnerability Reports and Notifications

BSI - Technical Guideline TR-03183

ISA/IEC 62443 requirements



General	IEC 62443-1-1 Terminology, Concepts and Models	IEC TR-62443-1-2 Master Glossary of Teams and Abbreviations	IEC TR-62443-1-3 System Security Conformance Metrics	IEC TR-62443-1-3 IACS Security Lifecycle and Use-Cases	
Policies & Procedures	IEC 62443-2-1 Establishing an Industrial Automation and Control System Security Program	IEC TR-62443-2-2 IACS Protection Levels	IEC TR-62443-2-3 Patch Management in the IACS Environment	IEC TR-62443-2-4 Requirement for IACS Service Providers	IEC TR-62443-2-5 Implementation Guidance for IACS Asset Owners
System	IEC TR 62443-3-1 Security Technologies for IACS	IEC TR-62443-3-2 Security Risk Assessment and System Design	IEC TR-62443-3-3 System Security Requirments and Security Levels		
Component	IEC 62443-4-1 Product Development Requirements	IEC 62443-4-2 Technical Security Requirments for IACS Components			

IEC 62443 App Note

Penalties

In the event of non-compliance with the requirements of the CRA, obligated economic operators face significant penalties. According to Article 64(1) of the CRA, Member States are required to establish provisions for effective, proportionate, and dissuasive sanctions.

Cause	Legal Basis	Fine
Providing false, incomplete, or misleading information to notified bodies or market surveillance authorities upon request for information.	Art. 64 Abs. 4 CRA	Up to EUR 5 million or up to 1% of the worldwide annual turnover of the preceding financial year, whichever amount is higher.
Violation of the obligations set out in Articles 18 to 23, Article 28, Article 30(1) to (4), Article 31(1) to (4), Article 32(1) to (3), Article 33(5), as well as Articles 39, 41, 47, 49, and 53 of the CRA.	Art. 64 Abs. 3 CRA	Up to EUR 10 million or up to 2% of the worldwide turnover of the preceding financial year, whichever amount is higher.
Failure to comply with the essential requirements of Annex I or breaches of the manufacturer obligations under Articles 13 and 14 of the CRA.	Art. 64 Abs. 2 CRA	Up to EUR 15 million or up to 2.5% of the worldwide annual turnover of the preceding financial year, whichever amount is higher.

Security Ecosystem

Cryptography

AES ECC RSA SHA

Key Management

Firmware

C CODE Secure Communication

Programming Debugging Interface Disable (PDID)

Secure Boot and Firmware Update

Factory Secure Provisioning Service

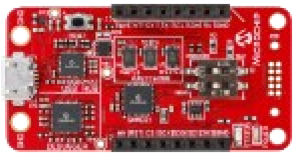
TRUST 6GD

TRUST MANAGER

TRUST CUSTOM

TRUST FLEX

Development Boards



Compliance

IEC ISO/IEC 62443

Qi® 1.3/2.0

EU Cyber Resilience Act

FIPS140-2

ISO/SAE 21434

Use Cases

aws

TLS

LoRa

Microsoft Azure

KUDELSKI IoTHINGS keySTREAM™

Development Tools and Libraries

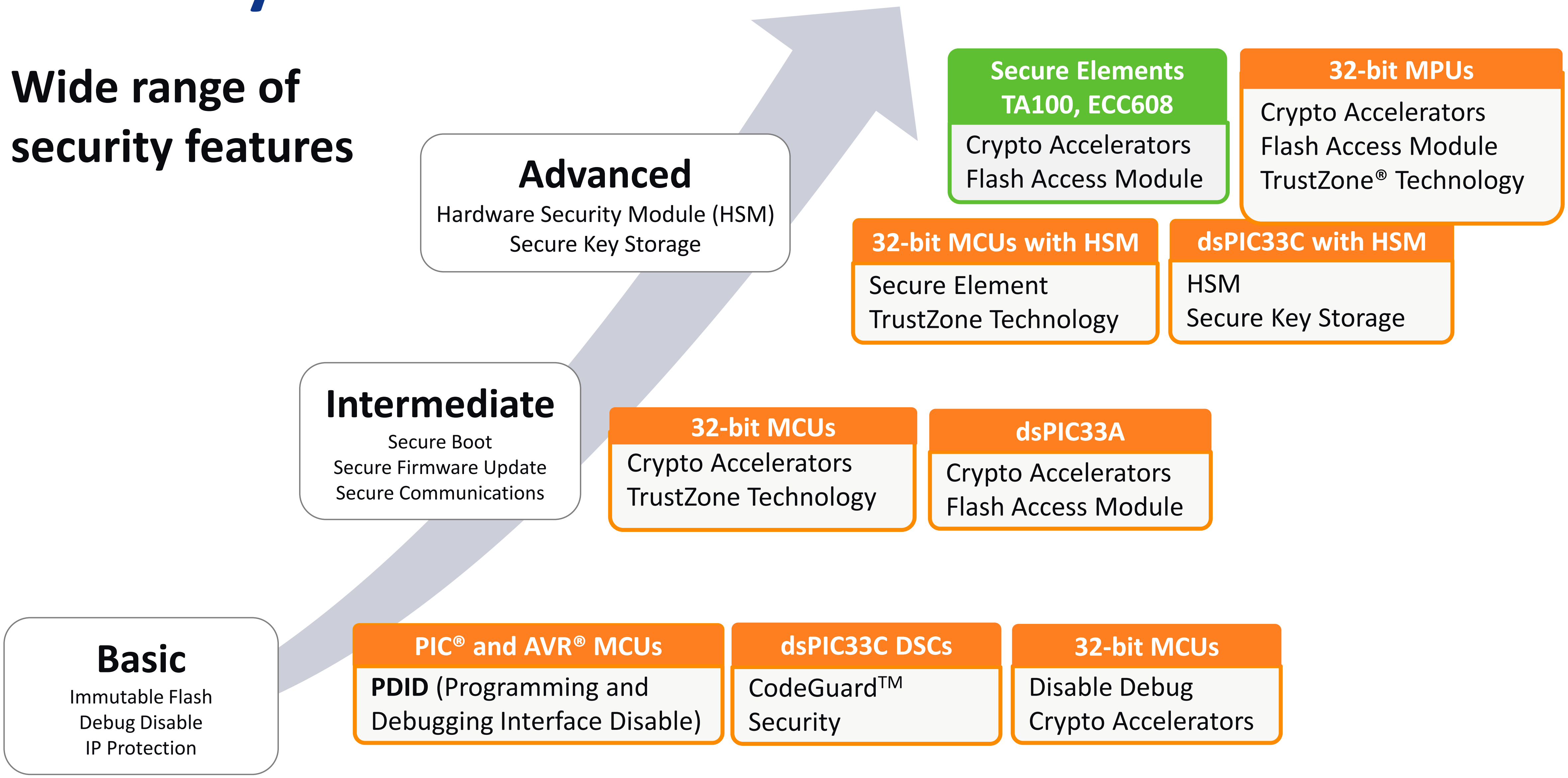
TRUST PLATFORM DESIGN SUITE — MCC and Harmony Secure Boot Firmware update

CAL CryptoAuthLib

AUTOSAR Crypto Drivers

Security Overview

Wide range of security features



Basic

Immutable Flash
Debug Disable
IP Protection

PIC® and AVR® MCUs

PDID (Programming and Debugging Interface Disable)

dsPIC33C DSCs

CodeGuard™ Security

32-bit MCUs

Disable Debug
Crypto Accelerators

Intermediate

Secure Boot
Secure Firmware Update
Secure Communications

32-bit MCUs

Crypto Accelerators
TrustZone Technology

dsPIC33A

Crypto Accelerators
Flash Access Module

Advanced

Hardware Security Module (HSM)
Secure Key Storage

32-bit MCUs with HSM

Secure Element
TrustZone Technology

dsPIC33C with HSM

HSM
Secure Key Storage

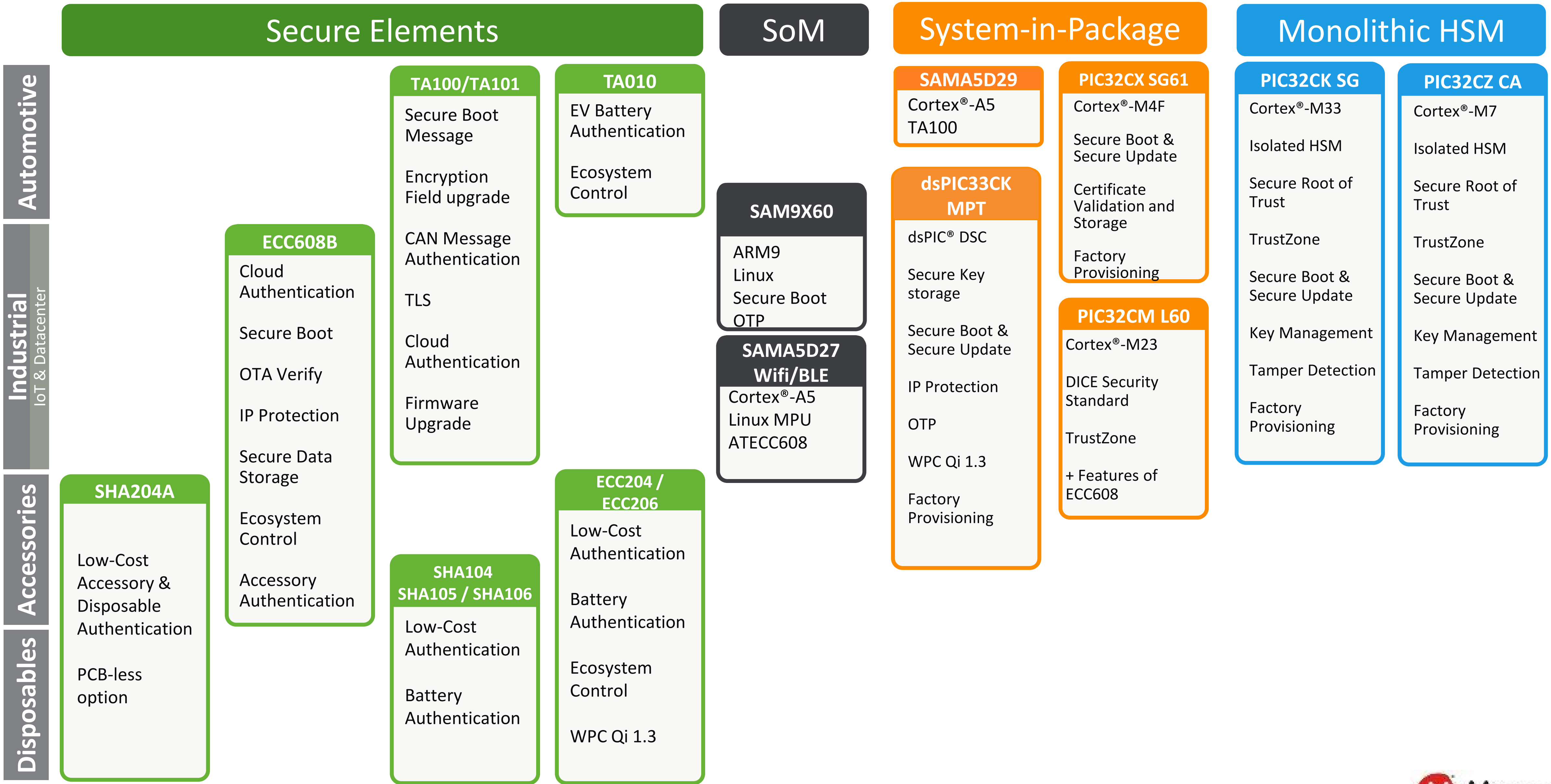
Secure Elements TA100, ECC608

Crypto Accelerators
Flash Access Module

32-bit MPUs

Crypto Accelerators
Flash Access Module
TrustZone® Technology

Microchip Security Solutions 1/2



Automotive

Industrial
IoT & Datacenter

Accessories

Disposables

Secure Elements

SHA204A

Low-Cost Accessory & Disposable Authentication

PCB-less option

ECC608B

Cloud Authentication

Secure Boot

OTA Verify

IP Protection

Secure Data Storage

Ecosystem Control

Accessory Authentication

TA100/TA101

Secure Boot Message

Encryption Field upgrade

CAN Message Authentication

TLS

Cloud Authentication

Firmware Upgrade

SHA104 SHA105 / SHA106

Low-Cost Authentication

Battery Authentication

TA010

EV Battery Authentication

Ecosystem Control

ECC204 / ECC206

Low-Cost Authentication

Battery Authentication

Ecosystem Control

WPC Qi 1.3

SoM

SAM9X60

ARM9
Linux
Secure Boot
OTP

SAMA5D27 Wifi/BLE

Cortex®-A5
Linux MPU
ATECC608

System-in-Package

SAMA5D29

Cortex®-A5
TA100

dsPIC33CK MPT

dsPIC® DSC

Secure Key storage

Secure Boot & Secure Update

IP Protection

OTP

WPC Qi 1.3

Factory Provisioning

PIC32CX SG61

Cortex®-M4F

Secure Boot & Secure Update

Certificate Validation and Storage

Factory Provisioning

PIC32CM L60

Cortex®-M23

DICE Security Standard

TrustZone

+ Features of ECC608

Monolithic HSM

PIC32CK SG

Cortex®-M33

Isolated HSM

Secure Root of Trust

TrustZone

Secure Boot & Secure Update

Key Management

Tamper Detection

Factory Provisioning

PIC32CZ CA

Cortex®-M7

Isolated HSM

Secure Root of Trust

TrustZone

Secure Boot & Secure Update

Key Management

Tamper Detection

Factory Provisioning

Microchip Security Solutions 2/2

Computer

Automotive

Industrial
IoT & Datacenter

Secure FPGAs

PolarFire

Crypto Coprocessor

Side-channel resistant cryptography

PolarFire SoC

Crypto Coprocessor

Side-channel resistant cryptography

64-bit MPUs

PIC64GX

64-bit RISC-V® quad-core processor

Secure Boot

Key Management

Built-in tamper detectors and countermeasures

DPA protection

SECDED on all memories

PIC64HX

64-bit RISC-V® quad-core processor

PIC64GX Features

Advanced Anti-Tamper Mechanisms

Post-quantum-cryptography

Hardware-Based Isolation

Root of Trust

CEC173x

Cortex®-M4

Real-time SPI Bus Monitoring

Secure Boot & Secure Update

Attestation

Physical Tamper Attack Detection and Prevention

Embedded Controller

MEC15xx

Arm Cortex®-M4

Authentication Integrity using SHA
AES Symmetric encryption

Public Key Crypto Engine (RSA, ECC)

OTP, TRNG

MEC17xx

Arm® Cortex®-M4F

Secure Boot Authentication

Integrity using SHA

AES Symmetric encryption

Public Key Crypto Engine (RSA, ECC)

OTP, TRNG, PUF

Trust Platform Design Suite Use Cases

- Training and education your self about security concepts
- Prototyping support: key generation for prototyping, dummy provisioning, code examples, interactive application notes
- Access to our provisioning system through a secure sub-system configurator and secure exchange process

Security Use Cases

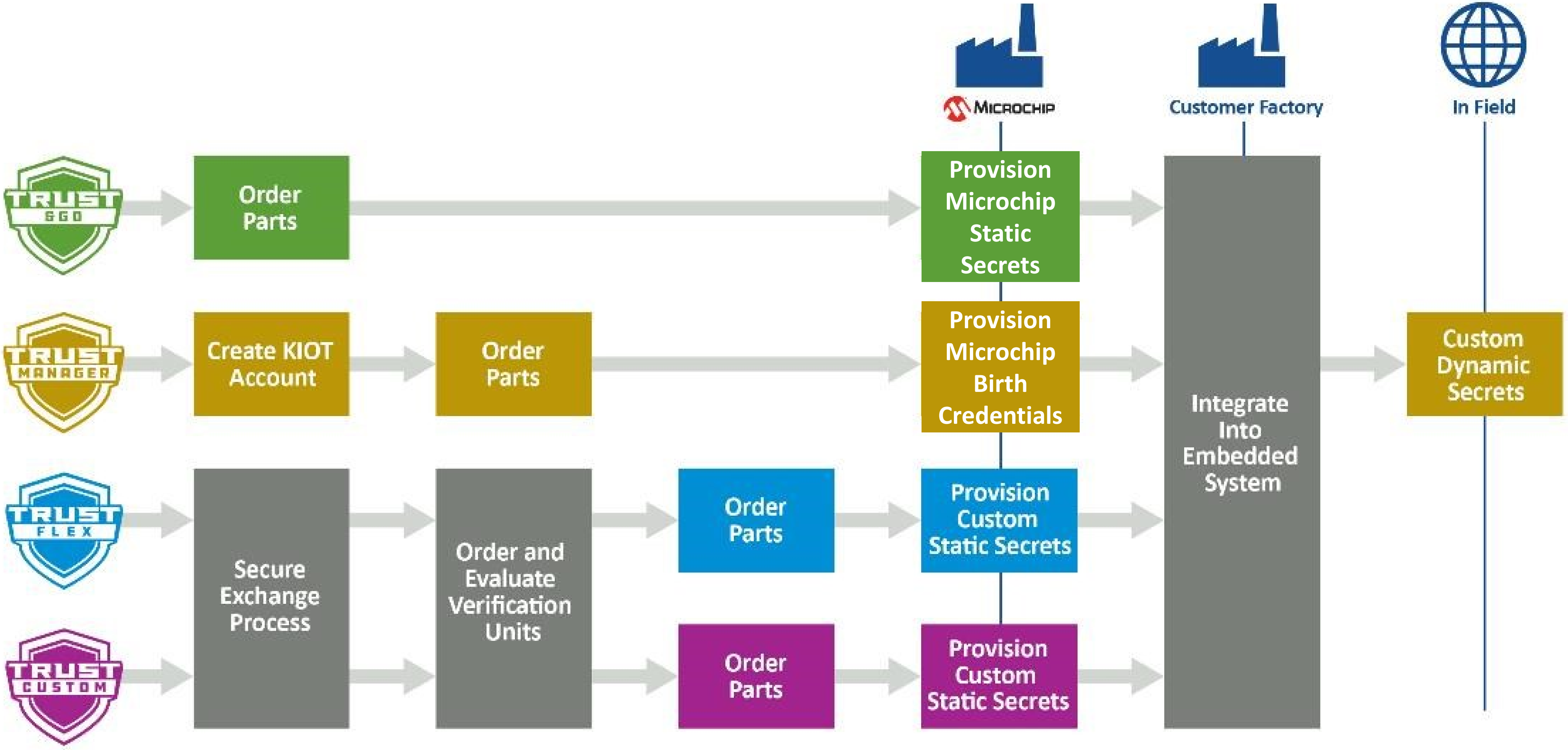
- **Authentication for any certificate authority**
  - Examples: AWS®, Azure®, on-premises TLS, Matter, Bluetooth® LE 1-to-1 pairing
- **Ecosystem control for accessories and disposable**
- **Message authentication (encrypted or not)**
- **Attestation: secure boot, secure OTA upgrades, firware verification**

- **Device management with keySTREAM™**
  - Certificate setup and hosting
  - Transfer of ownership, revocation (private key rotation)
  - Late-stage enrollment, certificate expiration
  - In-field key management
- **User access privileges**
  - Multi-tenant (public key attestation)
  - Permissions/rights management (attestation by PKI)
  - No default password

Trust Platform

	TRUST &GO	TRUST MANAGER	TRUST FLEX	TRUST CUSTOM
Pre-Configured	✓	✓	✓	✗
Provisioning	Zero touch (at Microchip)	Zero touch (in field)	Custom (at Microchip)	Custom (at Microchip)
Complexity	Lowest	Lowest	Lower	Custom
Secrets	Static by Microchip	Managed SaaS	Static by customer	Custom
Low MOW Flow	100 units	2000 units	2000 units	4000 units
High-Volume Flow	Starting 30 ku	Starting 30 ku	Starting 30 ku	Starting 30 ku
Use Cases	Any Cloud TLS, LoRaWAN® crypto mining - Helium	Any Cloud TLS, root certificate service, in-field PKI provisioning certificate management	Any Cloud TLS, firmware verification, key rotation, secure boot, wireless charging, local authentication	Any custom use case(s)
Devices	ECC608 for TLS, ECC608 for LoRa®, SAMA5D2 Wireless SOM, WFI32E01PC Wi-Fi® + MCU + ECC608 ECC608 for Helium	ECC608 TA101 MCU/Wireless/MPU	ECC608 TLS, ECC608 WPC PIC32CM (MCU + SE) ECC204 WPC/AUTH TA010 WPC/AUTH SHA104 AUTH, CEC1736	ECC608 SHA204A TA100 dsPIC33CK (MCU+SE) CEC1736, TA101

Trust Platform Factory Provisioning Services


Microchip
Customer Factory
In Field
TRUST SGO
TRUST MANAGER
TRUST FLEX
TRUST CUSTOM
Order Parts
Create KIOT Account
Order Parts
Secure Exchange Process
Order and Evaluate Verification Units
Order Parts
Order Parts
Provision Microchip Static Secrets
Provision Microchip Birth Credentials
Provision Custom Static Secrets
Provision Custom Static Secrets
Integrate Into Embedded System
Custom Dynamic Secrets

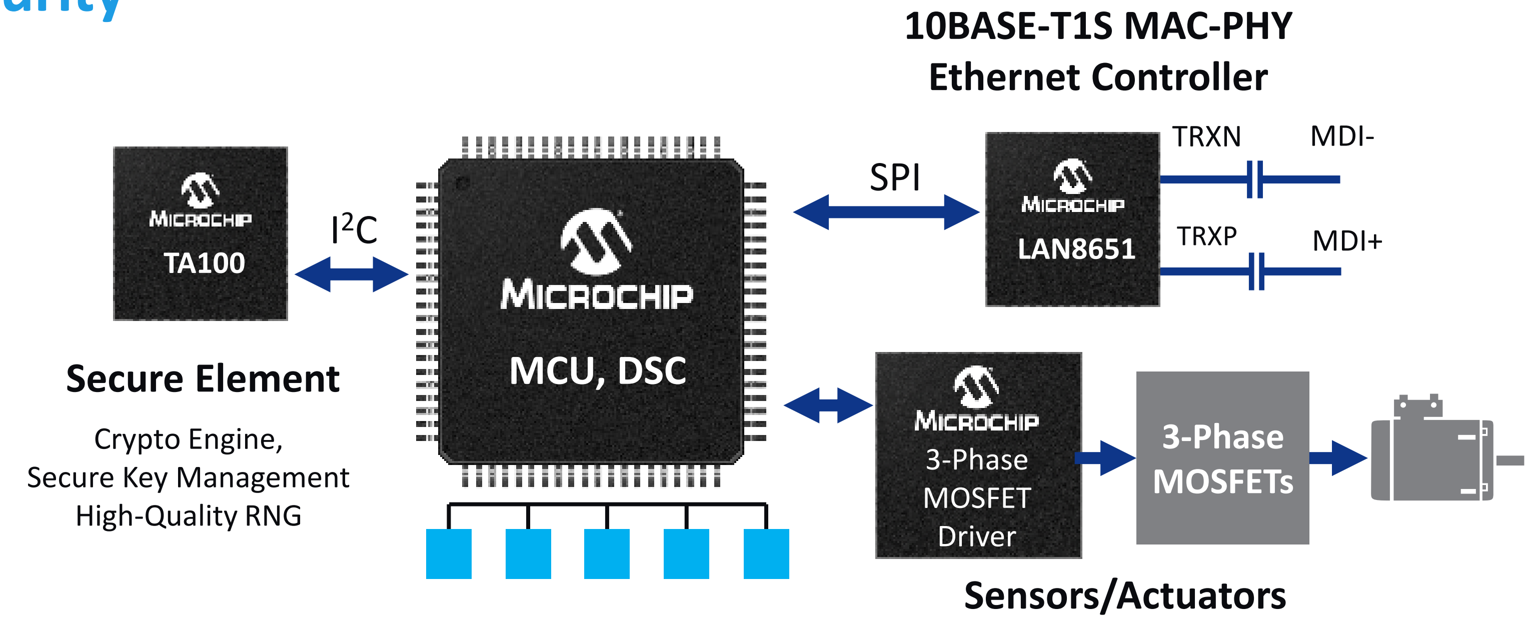
Secure 10BASE-T1S With MACsec

Media Access Control (MAC) Security

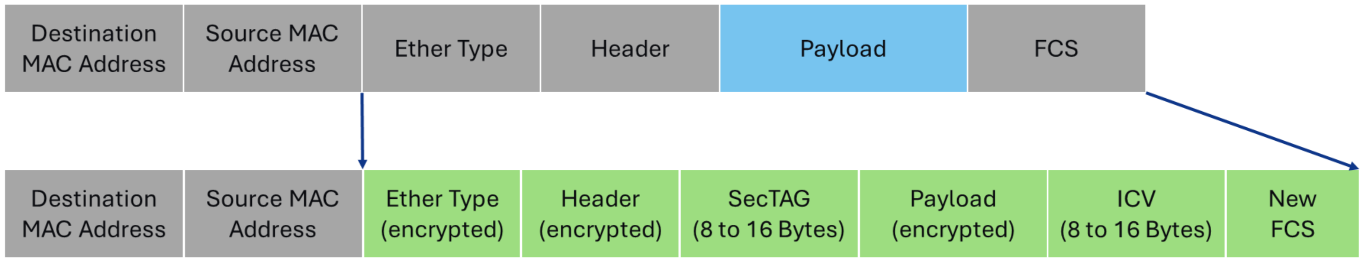
Point-to-point security protocol providing *confidentiality, integrity, authenticity* using encryption at the MAC layer

- **Protect against**
  - Eavesdropping
  - Replay attacks
  - Spoofing message sent from an imposter node
  - Sending arbitrary messages
  - Modifying messages in transit
  - Exploiting bugs in software to takeover machines

Contact Microchip for MACsec Demo



Ethernet frame before MACsec

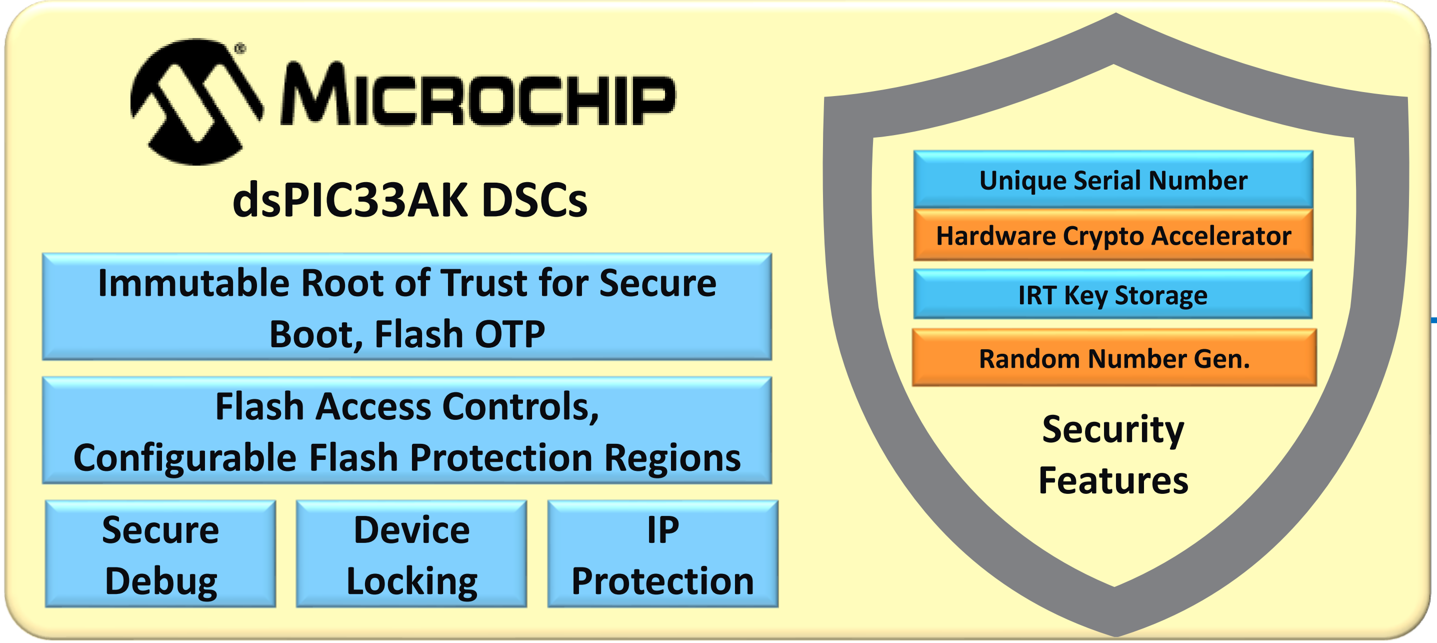


Destination MAC Address	Source MAC Address	Ether Type	Header	Payload	FCS

Destination MAC Address	Source MAC Address	Ether Type (encrypted)	Header (encrypted)	SecTAG (8 to 16 Bytes)	Payload (encrypted)	ICV (8 to 16 Bytes)	New FCS

Ethernet frame after MACsec

Secure Power Supply Design: dsPIC33A DSCs



MICROCHIP

dsPIC33AK DSCs

Immutable Root of Trust for Secure Boot, Flash OTP

Flash Access Controls, Configurable Flash Protection Regions

Secure Debug

Device Locking

IP Protection

Unique Serial Number

Hardware Crypto Accelerator

IRT Key Storage

Random Number Gen.

Security Features

- Immutable key storage in IRT for secure boot, firmware update and secure debug
- Authentication and key agreement using companion TrustAnchor device
- Hardware Crypto Accelerators
  - RSA, ECC, ECDSA, SHA, AES, HMAC, CMAC
  - Key generation
  - Signature generation/verification
- High-quality RNG, NIST SP800-90 A/B/C

Immutable Secure Boot

Secure Firmware Upgrade

Node Authentication

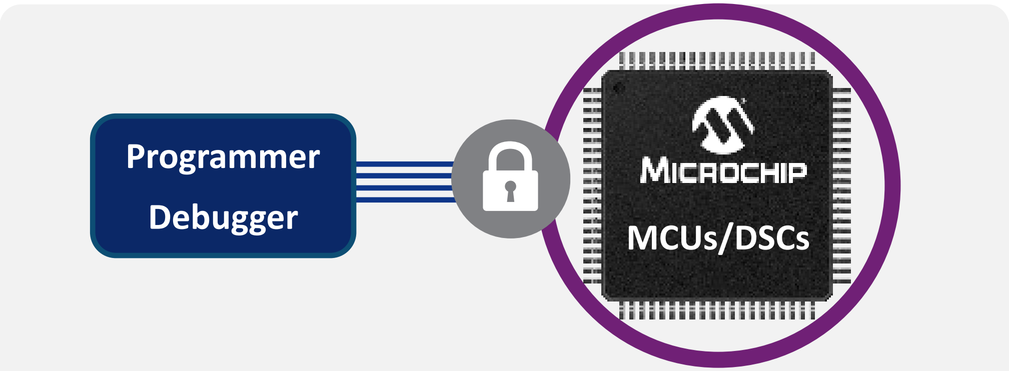
Secure Communication

OCP–SPDM Protocol

dsPIC33 DSCs: Security Against Remote Digital Attacks

Embedded Security – Security Use Cases

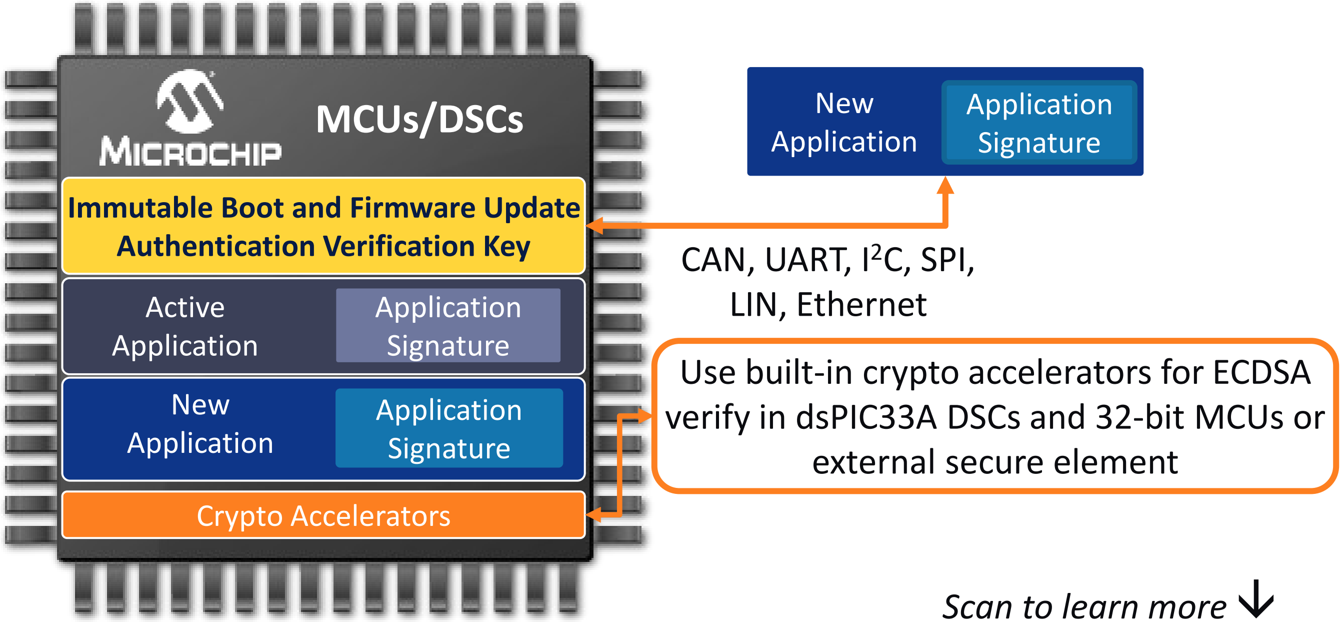
IP Protection



Prevent code modification and access to Flash

PIC® and AVR® MCUs	Programming and Debugging Interface Disable (PDID)
dsPIC33C DSCs	CodeGaurd™ Security, Immutable Boot, Flash OTP, Debug Disable
dsPIC33A DSCs	Flash Access Module, Immutable Boot, Flash OTP, Secure Debug
32-bit MCUs	Disable JTAG Debug, Integrity Check Monitor(ICM), TrustZone® Technology

Secure Boot and Firmware Update



Use built-in crypto accelerators for ECDSA verify in dsPIC33A DSCs and 32-bit MCUs or external secure element

Ensure integrity of the application firmware

Firmware update is over CAN, LIN, UART, I²C, SPI, Ethernet, USB or OTA

Supported in MCC and MPLAB® Harmony

Scan to learn more

MICROCHIP

TRUST PLATFORM DESIGN SUITE

TRUST MANAGER

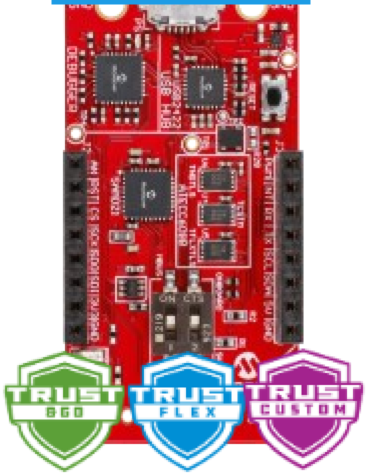
TRUST &GO

TRUST FLEX

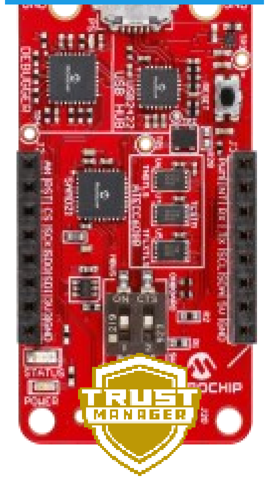
TRUST CUSTOM

TRUST PLATFORM DESIGN SUITE

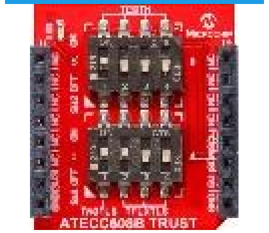
DM320118



EV10E69A



ATECC608

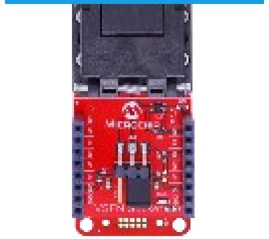


TA010

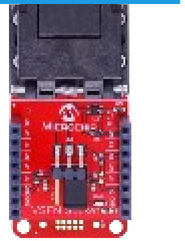
ECC20x

SHA10x

2-pin socket

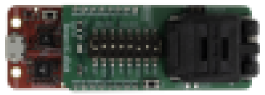


3-pin socket

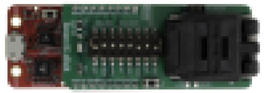


VQFN24 socket

uDFN8 socket



SOIC8 socket



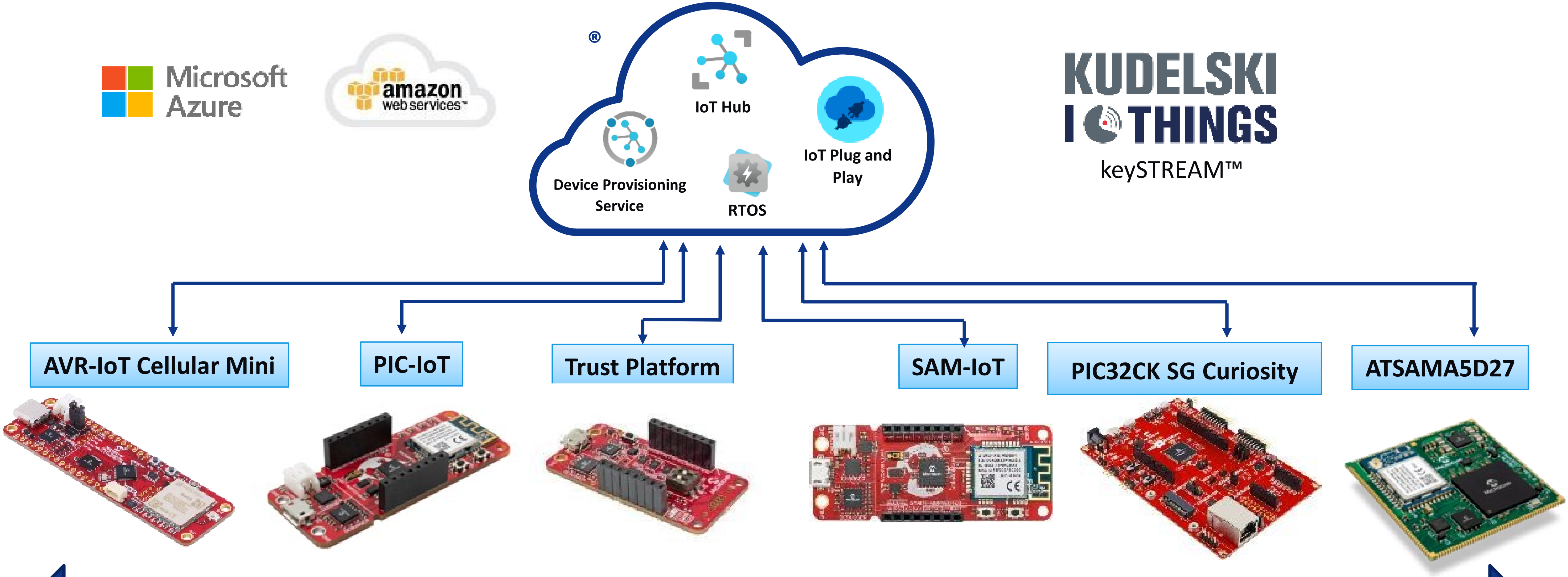
MICROCHIP

IoT Development Kits: Pick Your Core

Microsoft Azure

amazon web services

KUDELSKI IoT THINGS keySTREAM™



®

IoT Hub

Device Provisioning Service

RTOS

IoT Plug and Play

AVR-IoT Cellular Mini

PIC-IoT

Trust Platform

SAM-IoT

PIC32CK SG Curiosity

ATSAMA5D27

Scalable, Familiar, Trust Platform Secure

microchip.com/IoT

Thank you!

INNOELECTRO

Innovation in design, innovation in manufacturing

8–10 APRIL, 2025 | Budapest | BOK, HALL A

Visit our booth!

C07

www.innoelectro.com