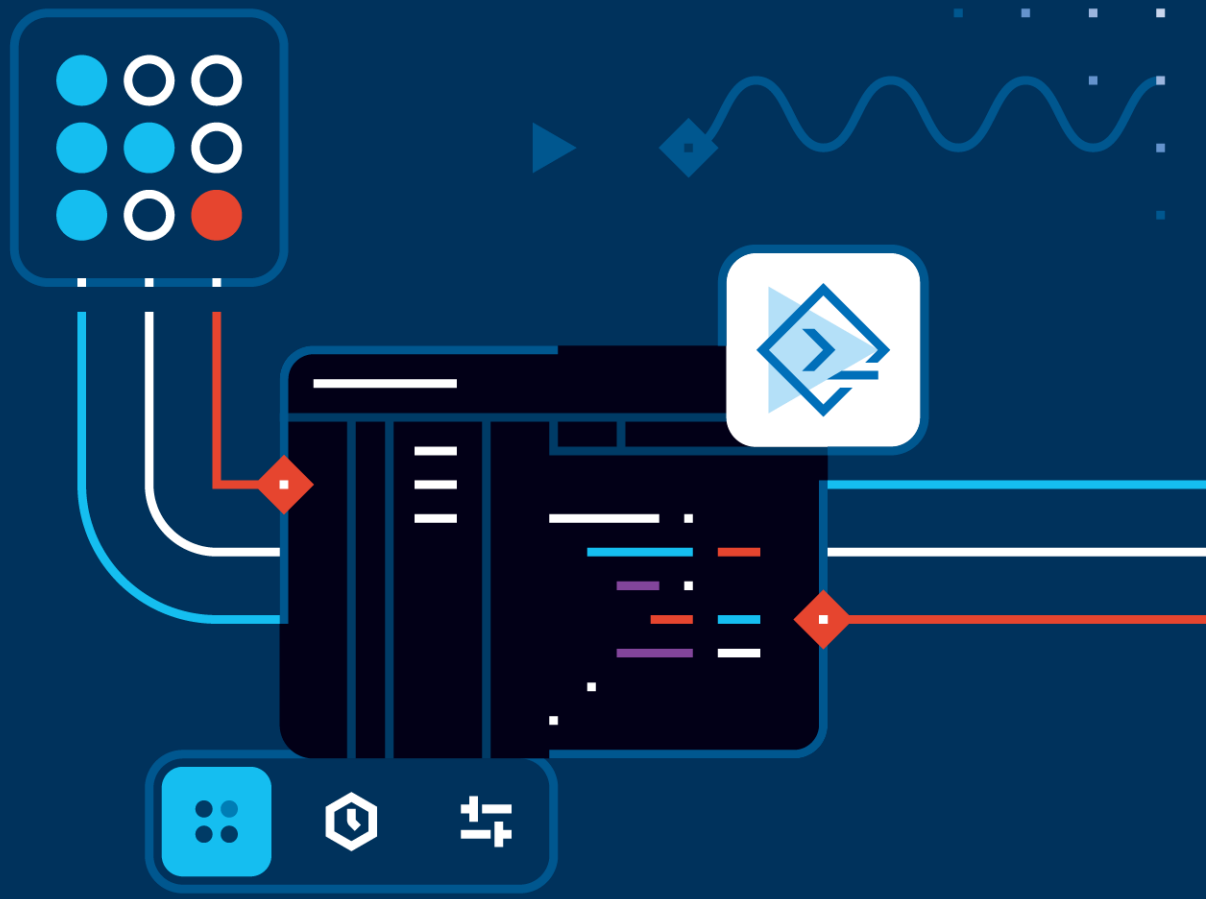
ANALOG DEVICES

EMBEDDED WORLD NORTH AMERICA 2024

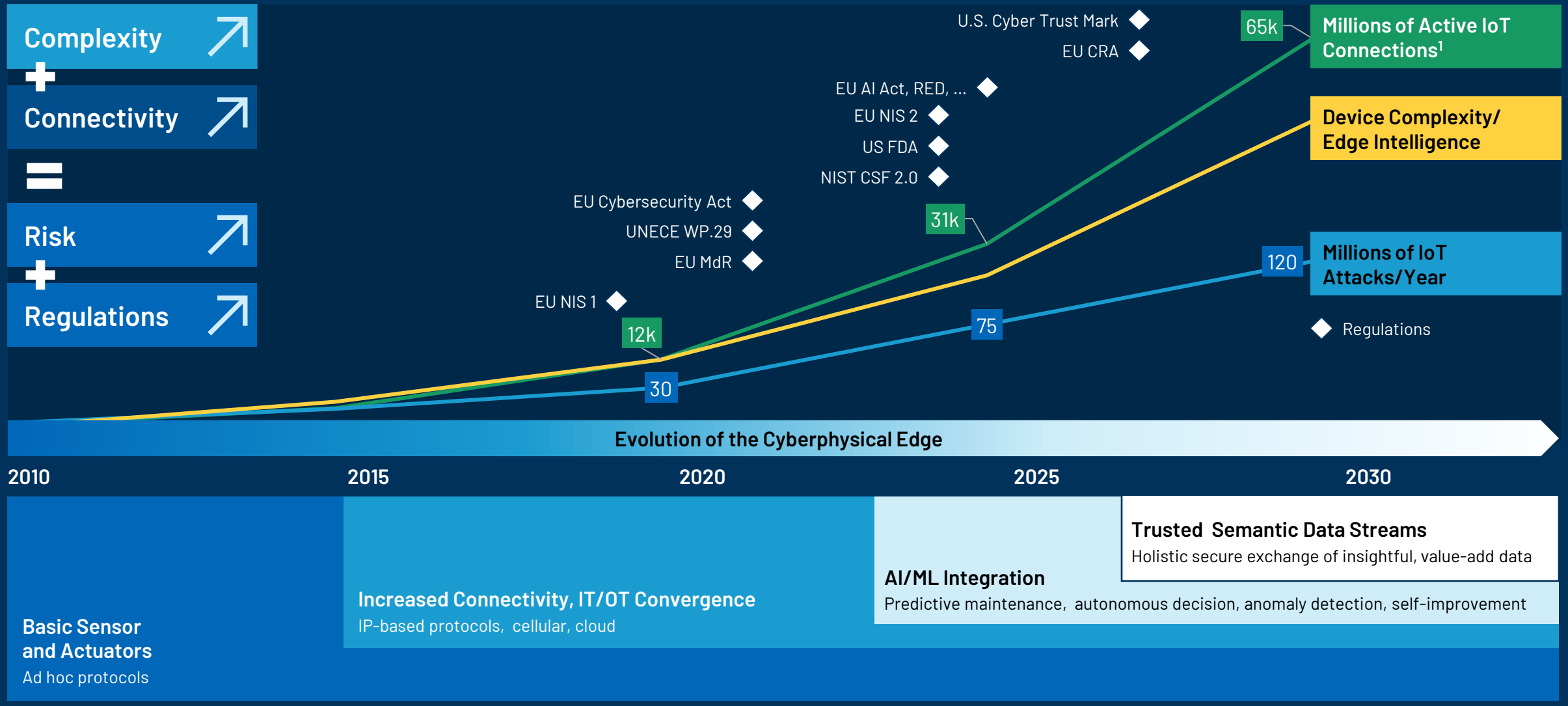
TRUSTED EDGE SECURITY

MEHMET ARIMAN



analog.com

Key Trends at the Cyberphysical Edge



[1] Lionel Sujay Vailshery. "IoT and Non-IoT Connections Worldwide 2010-2025." Statista, September 2022.

How ADI Enables Customers

ADI Assure™

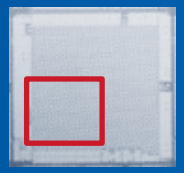
TRUSTED EDGE SOLUTIONS

Catalog of IP, digital ICs, and software meeting our customers' cybersecurity compliance and interoperability requirements

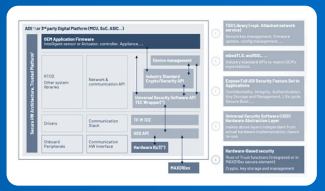
- Secure Elements

- MCUs + Security

- ASIC/SoC + Secure Enclave



- SDK and Toolchains



TRUSTED PRODUCT PORTFOLIO

ICs and software developed and manufactured to ADI security standard that spans the entire product life cycle

SECURE SUPPLY CHAIN

ADI's supply chain is trusted, delivering assessed and controlled products

ADI Provides Security Solutions

Digital ICs, software, and services meeting our customers' cybersecurity compliance and interoperability requirements with ease.

Key Attributes

- Ease of integration/use
- Scalable software stack
- Security assurance
- Supply chain security
- Hardware-based security
- Resilience

ADI Deliverables

*roadmap/**product depend.

CUSTOMER PRODUCT



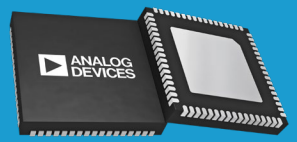

END-USER'S INFRASTRUCTURES

ADI PROTECT SOFTWARE
Embedded SDK and Tools

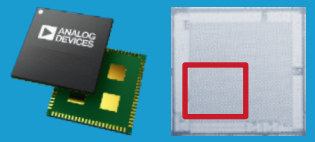
ADI TRUSTED EDGE SOFTWARE
Embedded SDK and Tools
Interoperable Industry-Standard APIs

ADI SECURE DEVICE MANAGEMENT*
Embedded SW
Remote Software Tools

ADI PROTECT AUTHENTICATORS



ADI MCU/MPUS/ASICS WITH SECURITY*



ADI CONNECT SECURE ELEMENTS

ADI FACTORY PROGRAMMING**

Protect Solutions
for brand, safety, and lifecycle protection (Detail C)

Trusted Edge Solutions
for securing Intelligent Edge devices (Detail A)

Device Management Solution*
(Detail C)

Trusted Edge Solution: Offering and Benefits

Delivers essential security functions for Intelligent Edge devices through a combination of hardware and software

OFFERING

Software

ADI TRUSTED EDGE SOFTWARE

- Embedded Security SDK
- TE-SFL Foundation SW

Hardware

ADI PROCESSORS

ADI SECURE ELEMENTS

Development Tools

ADI CodeFusion Studio™ IDE

+ Security Extensions

BENEFITS

Harmonized and **scalable security feature set**

Simplified implementation and **interoperability**

Future-proof with **updatable security** and **crypto agility***

Supply chain cybersecurity increased with **key provisioning****

Product security assurance
SBOM*, vulnerability management, PSIRT

Hardware-based security targets **most stringent current** and **future regulations and standards:**
IEC 62443-4-2 SL3, SESIP L3, US FDA, EU CRA, ...

*roadmap/**product depend.

A | Trusted Edge Solution: Features

Delivers differentiated security through a combination of hardware and software

1. SECURE DEVICE MANAGEMENT*
Allows managing device across life cycle

2. FOUNDATIONAL SECURITY
Scalable set of functions allowing to meet the device's security objectives

3. HARDWARE-BASED SECURITY
Enhance security and performance while easing certification

4. IDE BUNDLES SDK AND TOOLS TO EASE INTEGRATION

Software

ADI SECURITY SDK PROVIDES* THE FOLLOWING FEATURES

TE-SDM*
DEVICE MANAGEMENT

- Factory Provisioning*

TE-SFL
SECURITY FOUNDATIONS

- **Cryptography** Primitives (1)
- **Secure Communications** with TLS, BLE Security, ... (2)
- **Secure Processing Environment** (TEE)**
- Threat Detection* and Recovery
- **Secure Device Identity** (Incl. x.509 Certificate Management) Device Authentication and Attestation
- **Life Cycle** Management (4)
- **Secure Channel** (3)
- **Secure Boot**
- **Secure Update**
- **Secure Storage**
- **Access Control and Data Protection** (5)

*roadmap/**product depend
Deliverable—Future
Deliverable—WIP

Hardware

TE-HW
ROOT OF TRUST

- **Secure Boot ROM**
- **Security Primitives**
- **Hardware-Enforced Isolation** via Secure Architectures**
  Internal Root of Trust in ADI Processors, Arm® TrustZone
  OR Discrete Secure Elements
- **Hardware Crypto Engines**
- **HUK (OTP/PUF**)**
- **Silicon Life Cycle (incl. secure debug)**
- **Secure Storage (6)**
- **Countermeasures****
  Glitch and Side Channel Mitigations, Tamper Detection

Tools

ADI CodeFusion Studio™ IDE*
Security Extensions

- **Security SDK**
- **Secure Boot Tools: Code Signing**
- **Secure Debug Tools: Authenticated Debug**
- **Initial Key Provisioning**

(1) Broad support of cryptographic algorithms and modes for key management, hash, encryption, key derivation, signature, key agreement, and random number generation

(2) Most secure protocols can be addressed with the supported KDF options

(3) Provides an authenticated and encrypted protocol to manage the root of trust

(4) Life cycle of credentials, ownership transfers

(5) Access control to credentials, to root of trust functions

(6) Helper for the SW-defined secure storage: secret wrapping/unwrapping, using root keys

A | Trusted Edge Solution: Brings Mitigation of Risks

DEVICE PROPERTIES

- Is connected to a network/other devices
- Has hardware accessible test/debug ports
- Has discrete memory ICs
- Has removable media
- Runs updatable software
- Handles privacy-sensitive data or secrets
- Offers remote management service
- Runs complex OS, offers multiple user accounts

THREATS

- Software vulnerabilities
- Logic flaws: Improper access controls, hardcoded credentials, lack of authentication, ...
- Extraction of sensitive data or software
- Communication eavesdropping, replay, spoofing, ...
- No/weak/insecure crypto
- Invasive attack, fault injection, side channel attack
- Software manipulation in the field or via supply chain attacks
- Tampering with device, other supply chain attacks

MITIGATIONS

Software

ADI SECURITY SDK PROVIDES* THE FOLLOWING FEATURES

*roadmap/**product depend

TE-SDM*

DEVICE MANAGEMENT

- Factory Provisioning*

TE-SFL

SECURITY FOUNDATIONS

- **Cryptography** Primitives (1)
- **Secure Communications** with TLS, BLE Security, ... (2)
- **Secure Processing Environment** (TEE)**
- Threat Detection* and Recovery
- **Secure Device Identity** (Incl. x.509 Certificate Management) Device Authentication and Attestation
- **Life Cycle** Management (4)
- **Secure Channel** (3)
- **Secure Boot**
- **Secure Update**
- **Secure Storage**
- **Access Control and Data Protection** (5)

Hardware

TE-HW

ROOT OF TRUST

- **Secure Boot ROM**
- **Hardware Crypto Engines**
- **Silicon Life Cycle (Incl. Secure Debug)**
- **Security Primitives**
- **HUK (OTP / PUF**)**
- **Memory Encryption**
- **Secure Storage (6)**
- **Hardware-Enforced Isolation** via Secure Architectures**
  Internal Root of Trust in ADI Processors, Arm® TrustZone
  OR Discrete Secure Elements
- **Countermeasures****
  Glitch and Side Channel Mitigations, Tamper Detection

A.1 | ADI Trusted Edge Security Architecture for Processors

Foundational security and device management for Intelligent Edge devices built around ADI processors

TRUSTED EDGE SECURITY ARCHITECTURE IS:

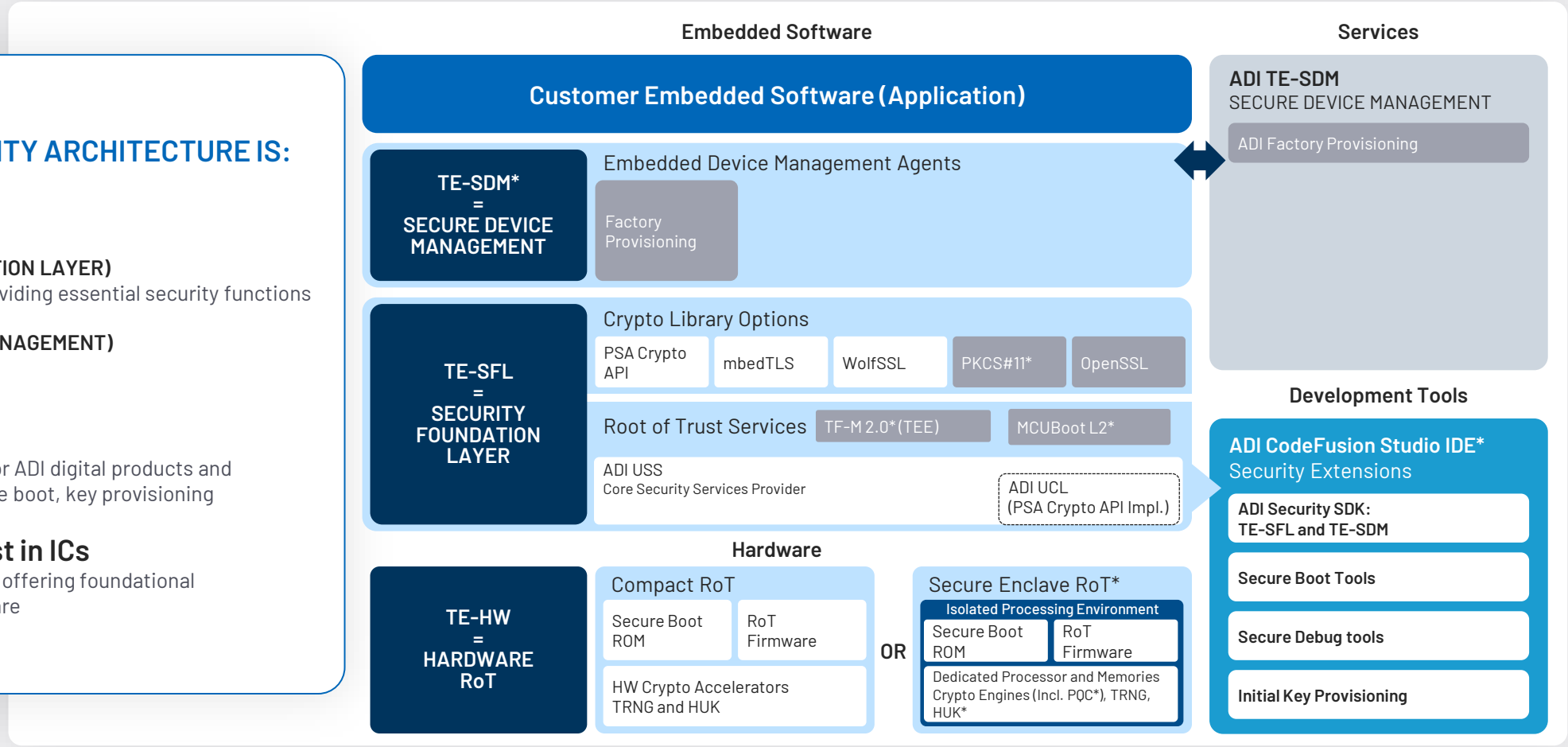
Trusted Edge SDK*

- **TE-SFL (SECURITY FOUNDATION LAYER)**
  scalable embedded stack providing essential security functions
- **TE-SDM (SECURE DEVICE MANAGEMENT)**
  Factory provisioning service
- **CodeFusion Studio™ IDE**
  IDE with essential software for ADI digital products and tools for secure debug, secure boot, key provisioning

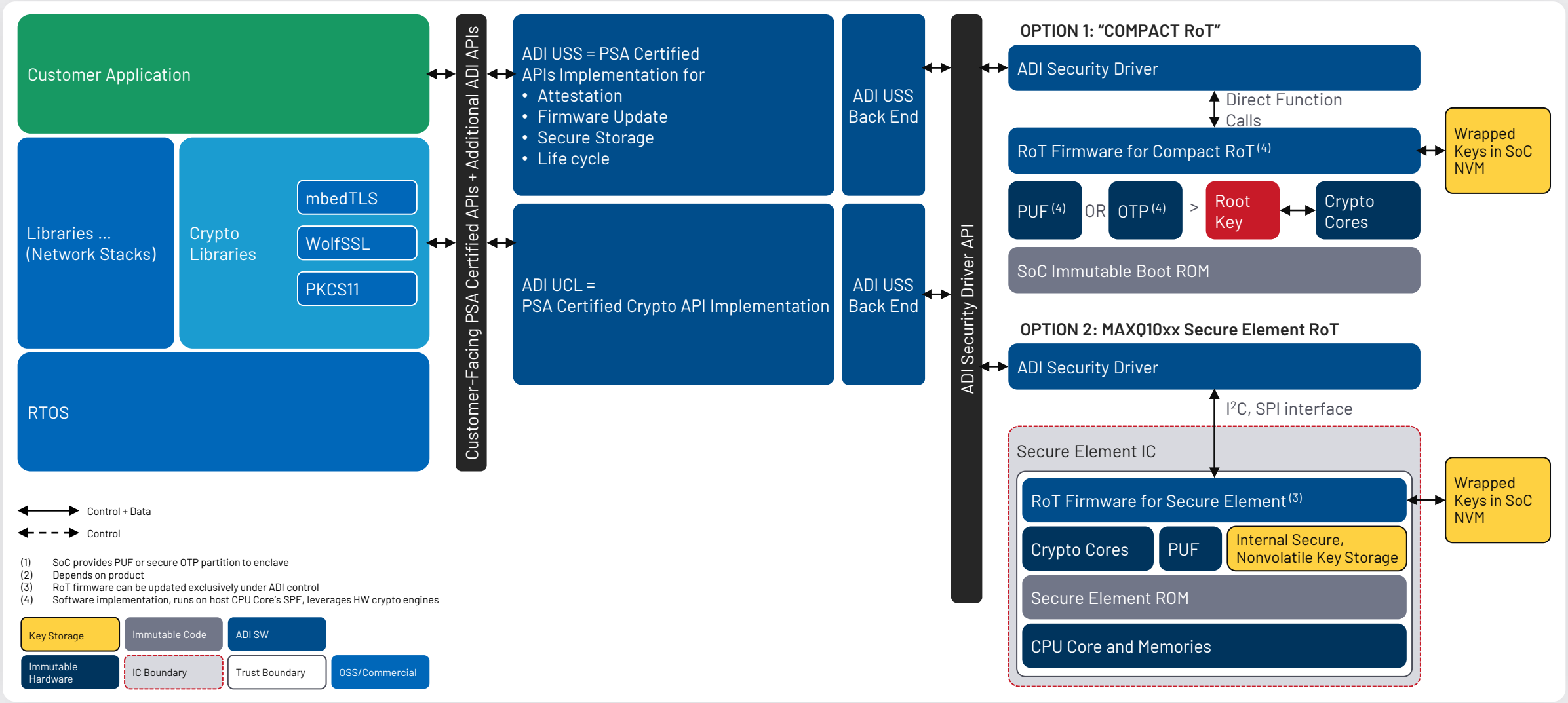
Hardware Root-of-Trust in ICs

adapted to the application needs offering foundational services to the embedded software

*Note: Supported products: MAX32690, MAX32670, MAX32651, more to come

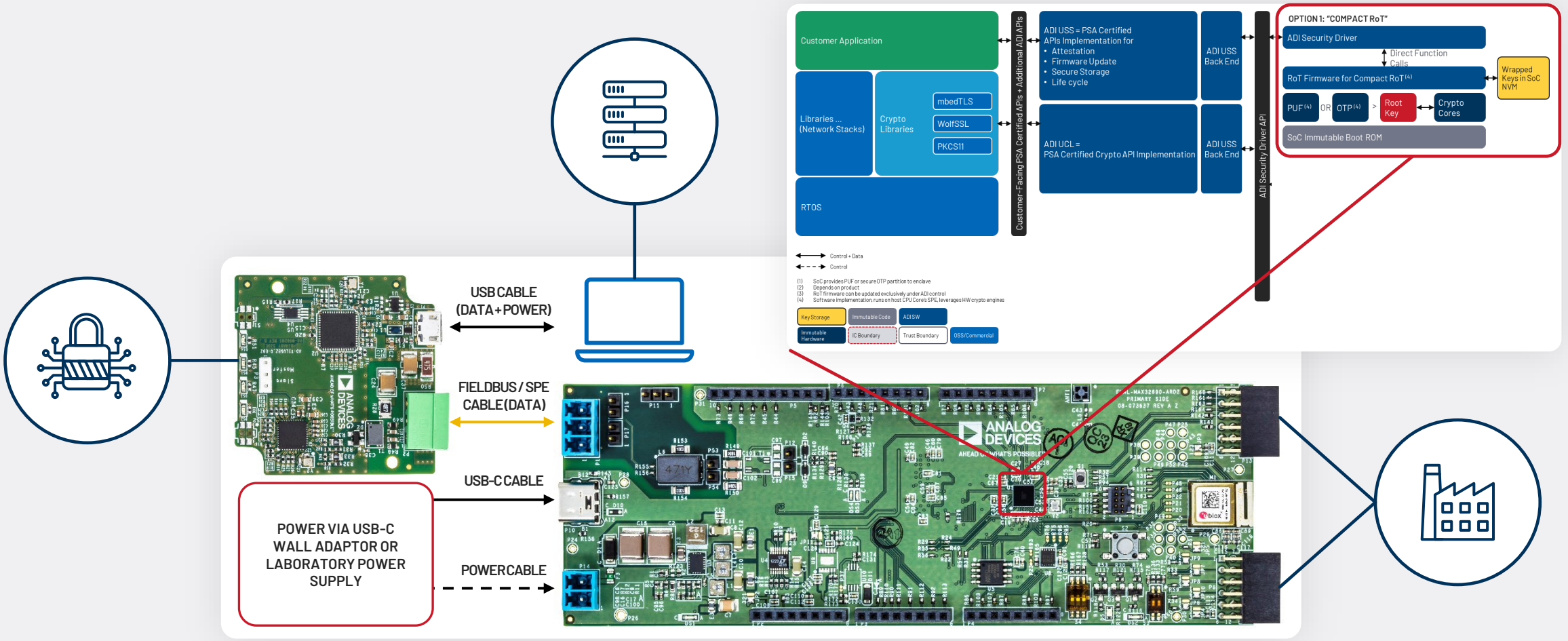


A.1 | Detailed Architecture



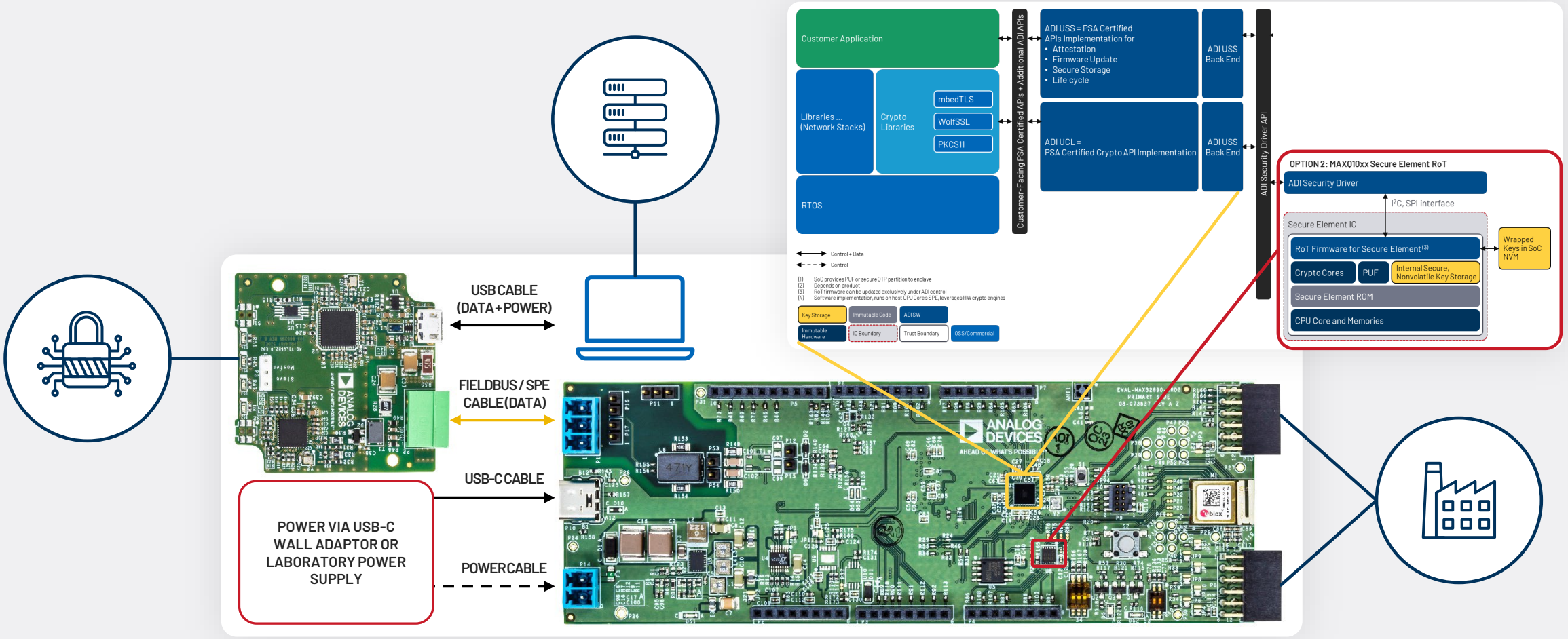
Cloud Connectivity

Compact RoT



Cloud Connectivity

Discrete Secure Element RoT



ANALOG DEVICES

AHEAD OF WHAT'S POSSIBLE

analog.com