Attesting the Hardware Integrity of Constrained Embedded Systems

Velektronik

Bundesministerium für Bildung und Forschung

VE-ASCOT
03/2021-12/2024

Motivation

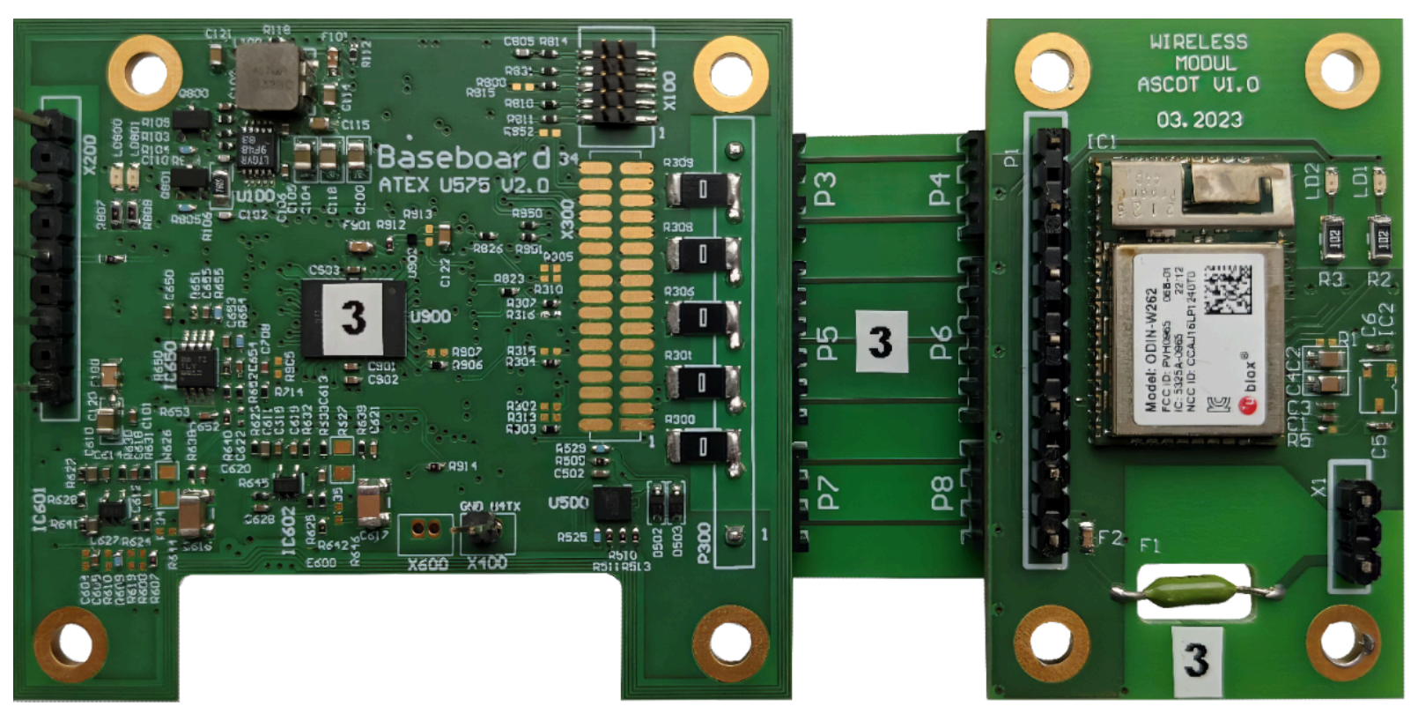
- Critical infrastructure requires methods to attest hardware (HW) and software (SW) integrity
- Physical anti-tamper methods may be infeasible
- Goal: Create lightweight HW/SW architecture to detect tampering on the supply chain and at runtime

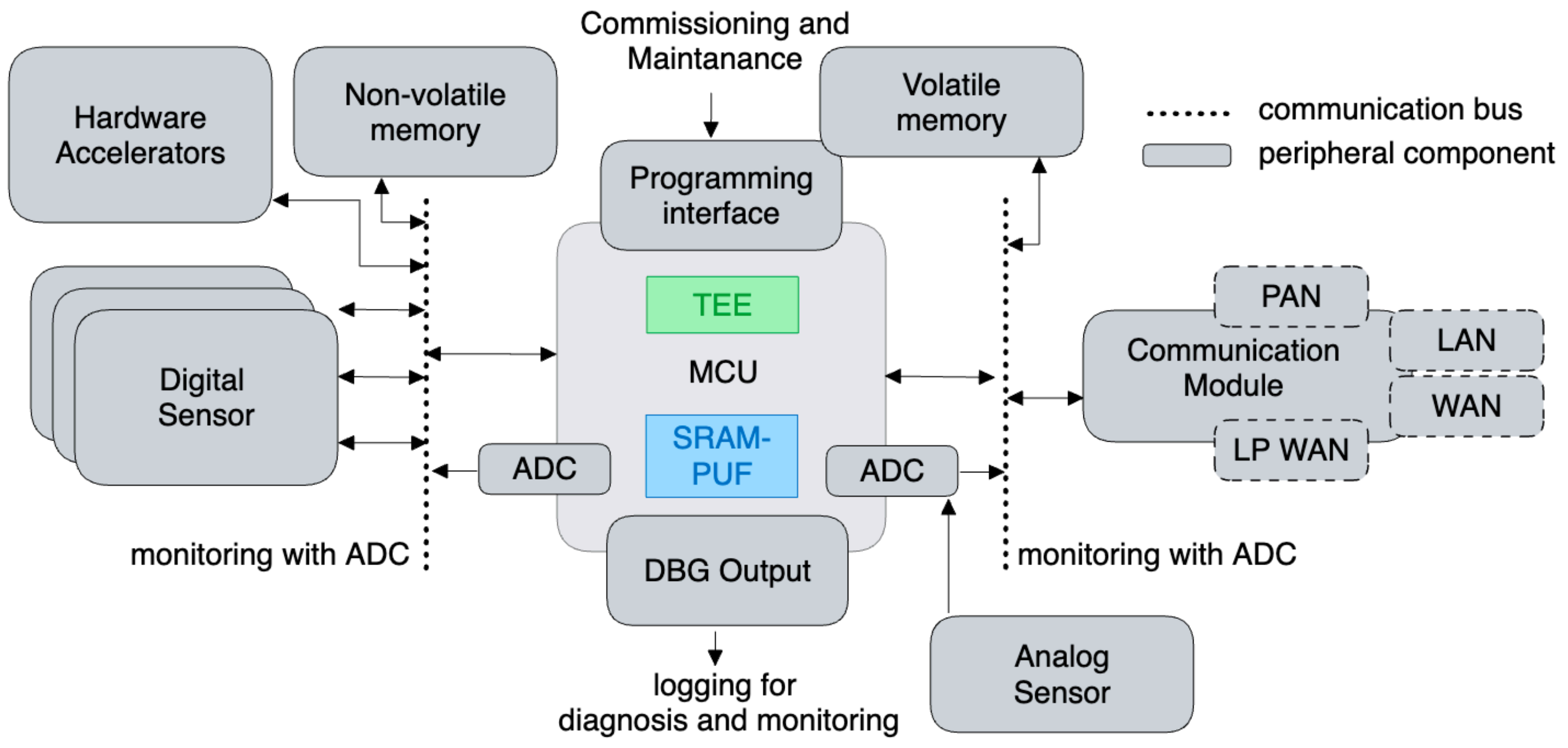
Solution Components

- **FHMQV-C**: Reduces the communication and processing overhead of remote attestations by combining key establishment and mutual authentication
- **tinyDICE**: Further reduces the communication and processing overhead of remote attestations by swapping explicit for implicit certificates
- **Hardware watchdog**: Detects tampering at runtime by extracting meaningful features from analog characteristics
- **SRAM Physically Uncloneable Function (PUF)**: Helps ensure supply chain integrity

Hardware Platform

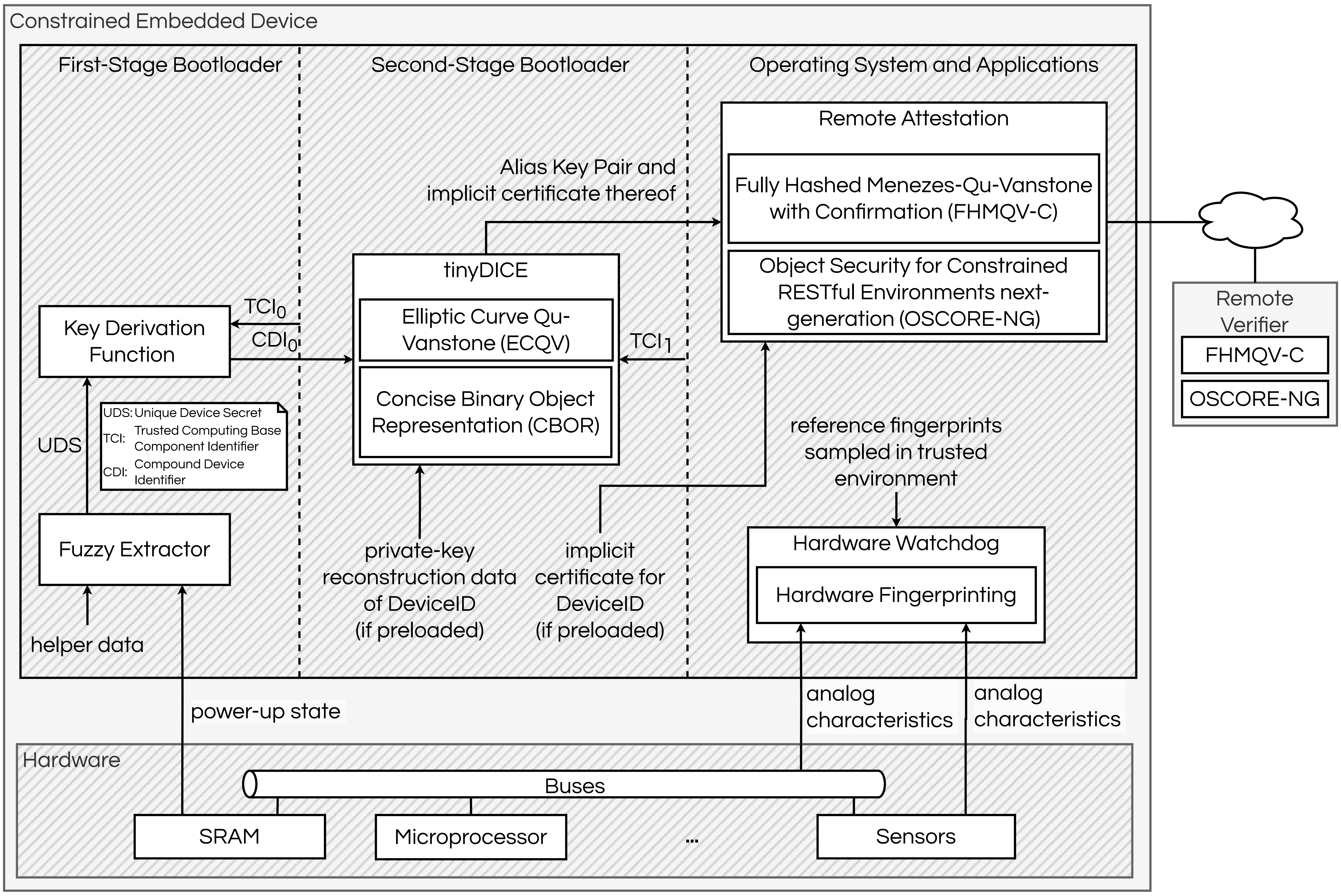
- Industrial IoT sensor system
- ARM Cortex-M33
- Monitoring of serial communication (I2C, SPI)
- On-device SRAM-PUF





Commissioning and Maintanance
Hardware Accelerators
Non-volatile memory
Programming interface
Volatile memory
TEE
MCU
SRAM-PUF
Digital Sensor
ADC
ADC
DBG Output
logging for diagnosis and monitoring
monitoring with ADC
monitoring with ADC
Communication Module
PAN
LAN
WAN
LP WAN
Analog Sensor
communication bus
peripheral component

Lightweight HW/SW Architecture



Constrained Embedded Device

First-Stage Bootloader

Second-Stage Bootloader

Operating System and Applications

Remote Attestation

Fully Hashed Menezes-Qu-Vanstone with Confirmation (FHMQV-C)

Object Security for Constrained RESTful Environments next-generation (OSCORE-NG)

Alias Key Pair and implicit certificate thereof

tinyDICE

Elliptic Curve Qu-Vanstone (ECQV)

Concise Binary Object Representation (CBOR)

TCI_0

CDI_0

TCI_1

Key Derivation Function

UDS

UDS: Unique Device Secret
TCI: Trusted Computing Base Component Identifier
CDI: Compound Device Identifier

Fuzzy Extractor

helper data

private-key reconstruction data of DeviceID (if preloaded)

implicit certificate for DeviceID (if preloaded)

reference fingerprints sampled in trusted environment

Hardware Watchdog

Hardware Fingerprinting

analog characteristics

analog characteristics

power-up state

Remote Verifier

FHMQV-C

OSCORE-NG

Hardware

Buses

SRAM

Microprocessor

...

Sensors

Contact

Christian Spinnler
Siemens AG
christian.spinnler@siemens.com

Konrad-Felix Krentz
Siemens AG
konrad-felix.krentz@siemens.com

UNIVERSITÄT BIELEFELD
SIEMENS
KIT Karlsruher Institut für Technologie
RevOne RevisionOne Engineering GmbH
WIBU SYSTEMS
Fraunhofer SIT
infineon
Schölly EXCELLENCE INSIDE

www.ascot-trust.info