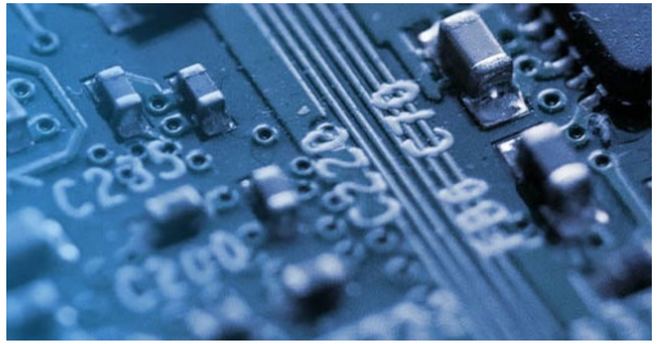
V9/23

SEAL SQ
semiconductors + quantum

- A WISeKey company

VaultIC292 Introduction

IoT Core Objectives for Manufacturers & Operators



ENSURING SUPPLY CHAIN INTEGRITY FROM CHIP TO DEVICE

- Unique device identity and key management
- Secured firmware and software delivery
- Transfer of ownership

SECURING DATA OPERATIONS & ENABLING a TRUSTED INFRASTRUCTURE

- Secured device enrollment
- Protect data at rest and in motion
- Secure updates at the edge
- Lifecycle management

NEED for a TRUST ENVIRONMENT with STRONG TRUST ANCHOR

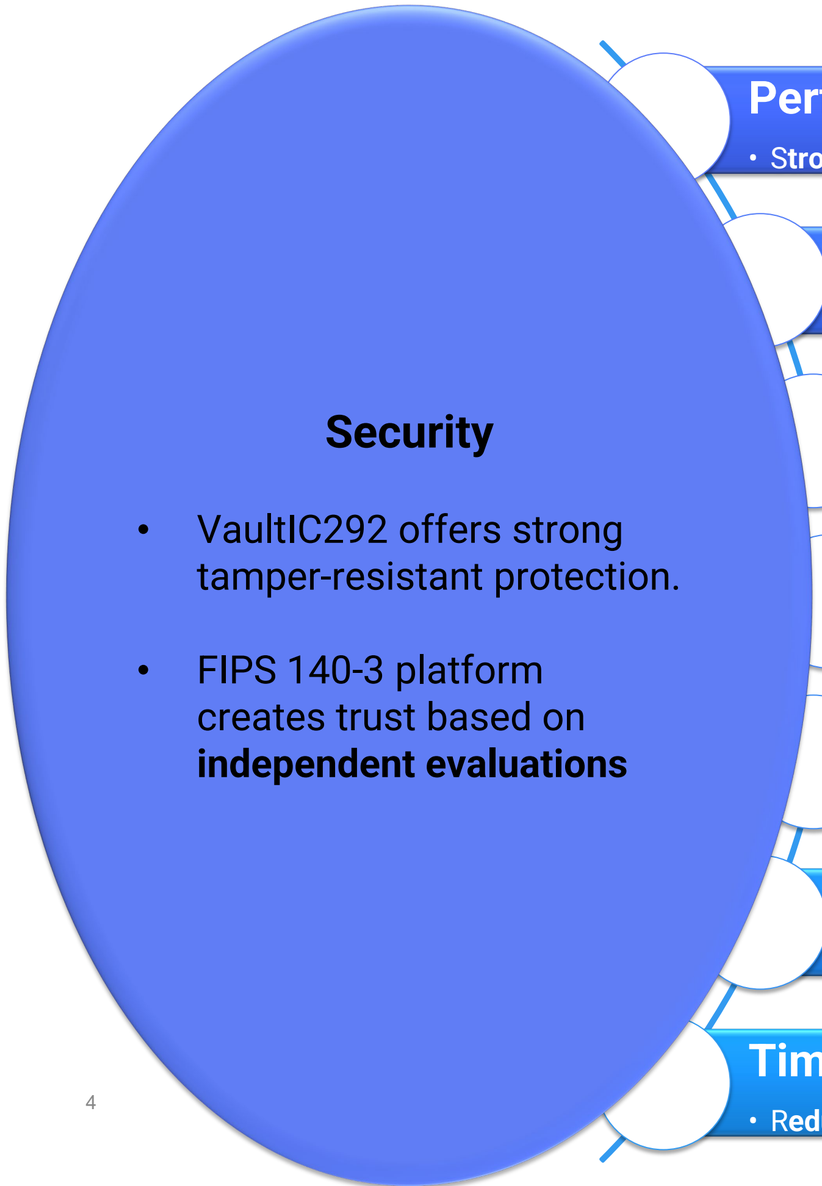
How to create a Trust Environment and Trust Anchor

Pure software protection in application processor

Separation of secure & “normal” world in a TEE

Secure Element: Hardware trust anchor + tamper resistance

VaultIC292 offers Unique Benefits even Beyond Strong Security



Performance

- **Strong performance** advantages compared to software-based solutions

Implementation

- Dedicated, protected hardware, leaves no room for weak implementations

Transposabilty

- Useable across various platform (RTOS / Linux) for different types of applications (TLS etc)

Innovation

- A Secure Element provides the latest **certified security**

Costs

- Reduced investment in secure manufacturing & security knowhow

Logistics

- Enabling production in non-trusted third-party environments and secured tracking of the value chain

Time to Market

- **Reduces system complexity** and **time to market** while reaching a measurable security level

Vaultic292 Principal Security Services

- **Execution of sensitive operations in e.g. TLS or MATTER**
- **Strong device authentication:**
  - ECC P256
  - Multiple key pairs available for different use
- **ECC Signature generation and verification**
- **ECDH Ephermeral Key generation**
- **Random Number Generation (NIST SP800-90B)**

Typical Use Case for VaultIC292: Cloud Connection

- Certificate X509
- Key pair generation
- Challenge Signature
- Session Key derivation

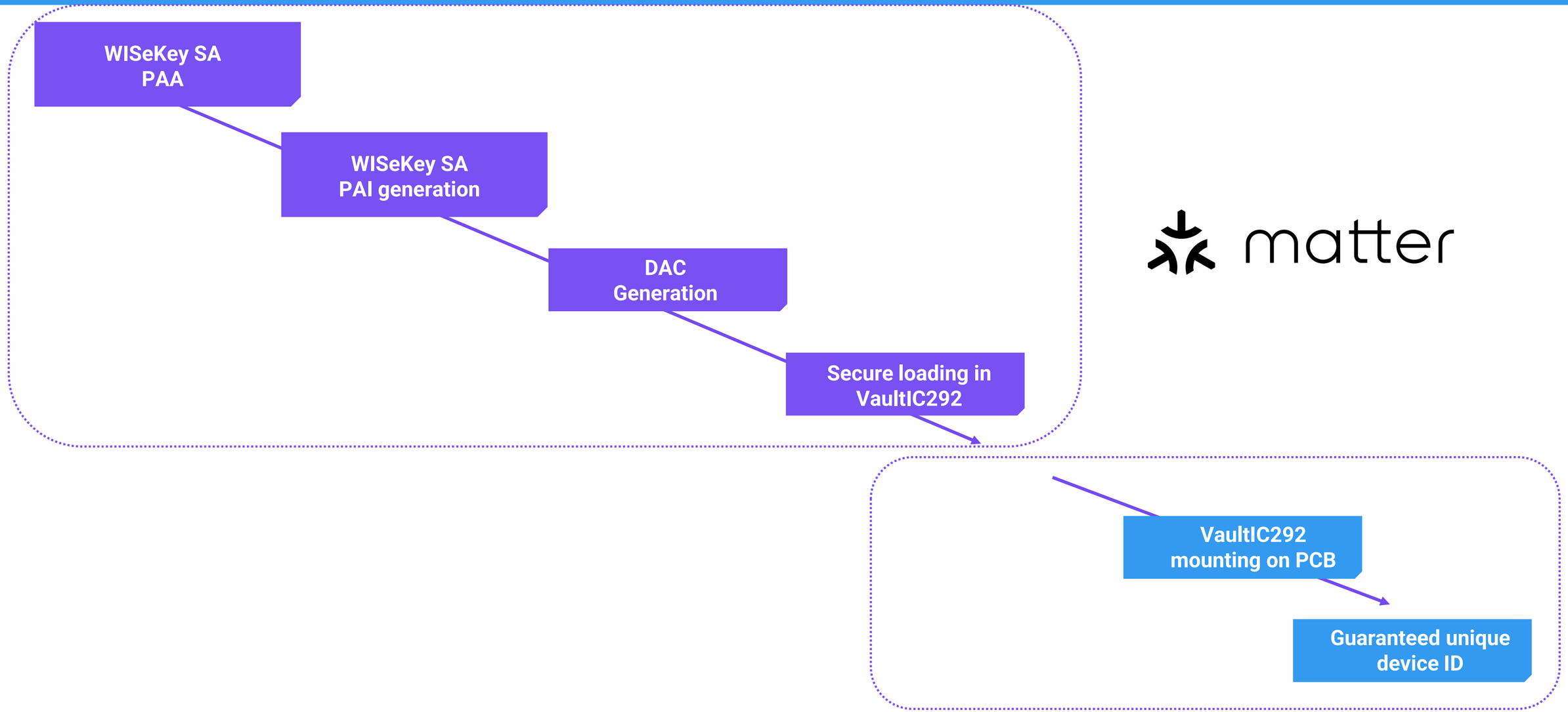
Device Identification

Device Authentication

Channel Protection

SEAL SQ
semiconductors + quantum

MATTER Smart Home Devices benefit from VaultIC292



matter

VaultIC292 Integration

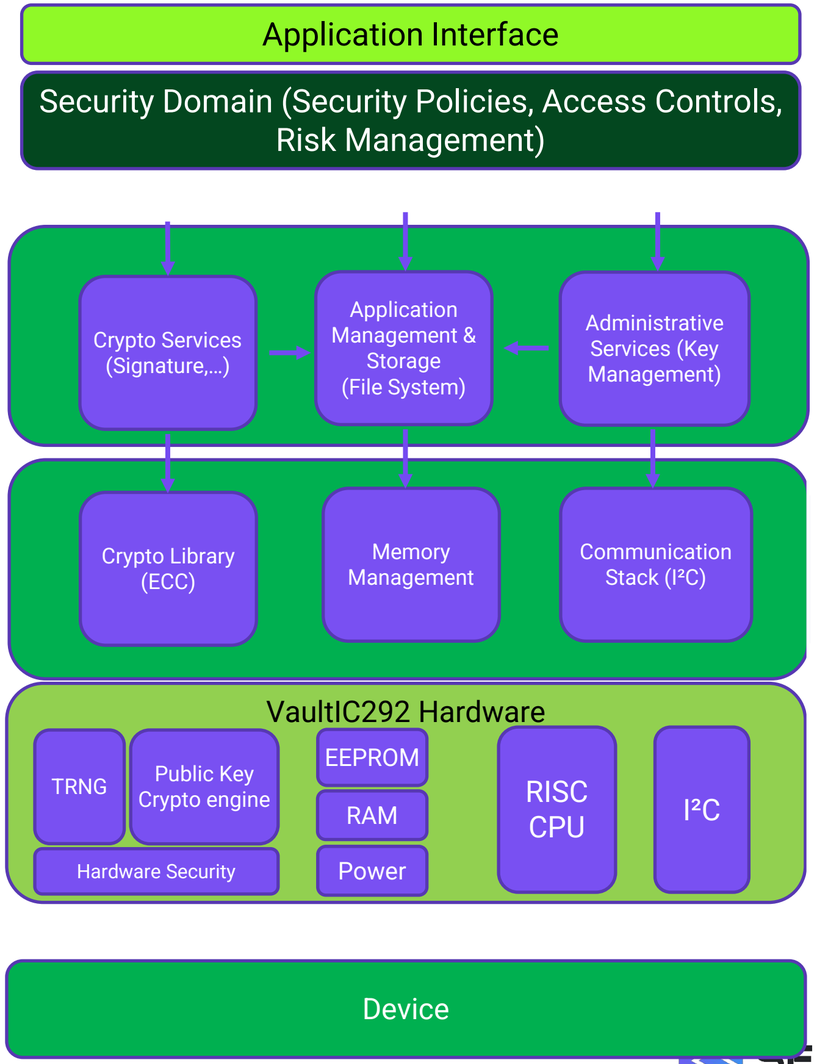
Easy integration in any system

Software Level (running in the Host)

- Host-VaultIC communication Drivers
- Host-VaultIC Secure Communication Channel
- Middleware WolfSSL, ESP32, RPi
- C source code

Hardware Level

- Standard communication interface: I²C
- SOIC8, UFDN8, DFN6 or customized packages
- Extended temperature ranges (-40° / +105°C)



VaultIC292 Characteristics

	VaultIC292
Hardware, Security	AT90SO2, EAL5+ level ready
Communication	I2C
Memory	5 key pairs, 2 X509 Certificates
ECC	P-256
Digital Sign	ECDSA
Secure Channel	✓
Key Agreement	ECDH
RNG, DRBG	✓ SP800-90B
KeyPair Generation	✓
Packages	Wafer, SOIC8, DFN6, UFDN8
Operating Ranges	[1.6V; 5.5V] [-40°C; +105°C]
Status	H2 2023

Take away

VaultIC292 brings a secure digital identity to a device, for MATTER or IoT

Singel 3 | B-2550 Kontich | Belgium | Tel. +32 (0)3 458 30 33
info@alcom.be | www.alcom.be
Rivium 1e straat 52 | 2909 LE Capelle aan den IJssel | The Netherlands
Tel. +31 (0)10 288 25 00 | info@alcom.nl | www.alcom.nl

VaultIC292

THANK YOU

SEAL SQ
semiconductors