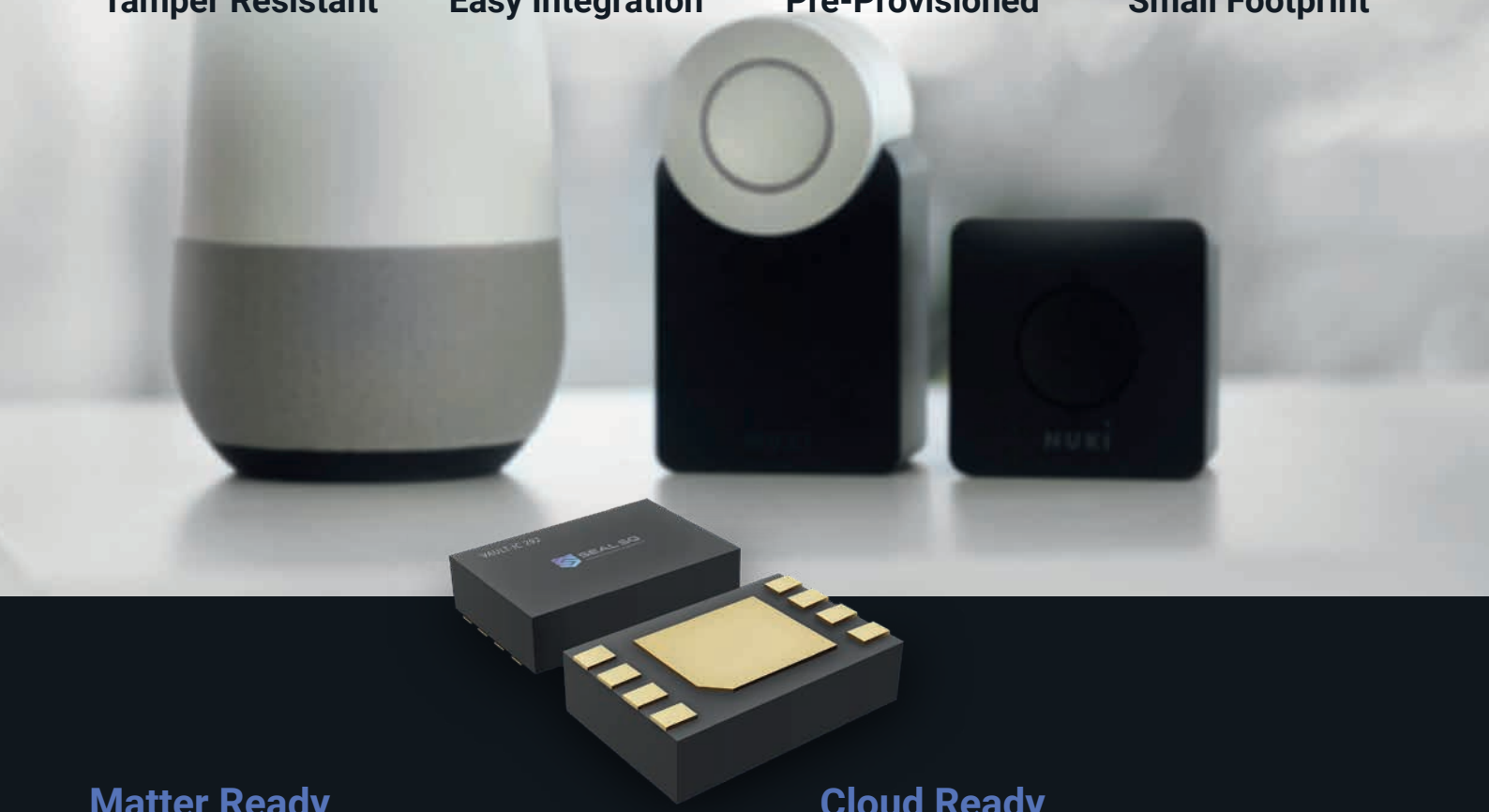
V. 05/23

VaultIC292

With pre-provisioned DAC (Matter Certificate)

Ready-to-use Secure Authenticator for Matter compliant devices. Embeds a unique digital identity signed by WISeKey PAA, a CSA accredited Root Certificate Authority

Tamper Resistant **Easy Integration** **Pre-Provisioned** **Small Footprint**



Matter Ready

VaultIC292 can be pre-configured with the Device Attestation Certificate (DAC), the Product Attestation Intermediate (PAI) Certificate, the passcode verifiers and related material.

matter

Cloud Ready

VaultIC292 can be pre-configured with private keys & X509 Certificates to be used for AWS and Azure Cloud commissioning.

Microsoft Azure

aws

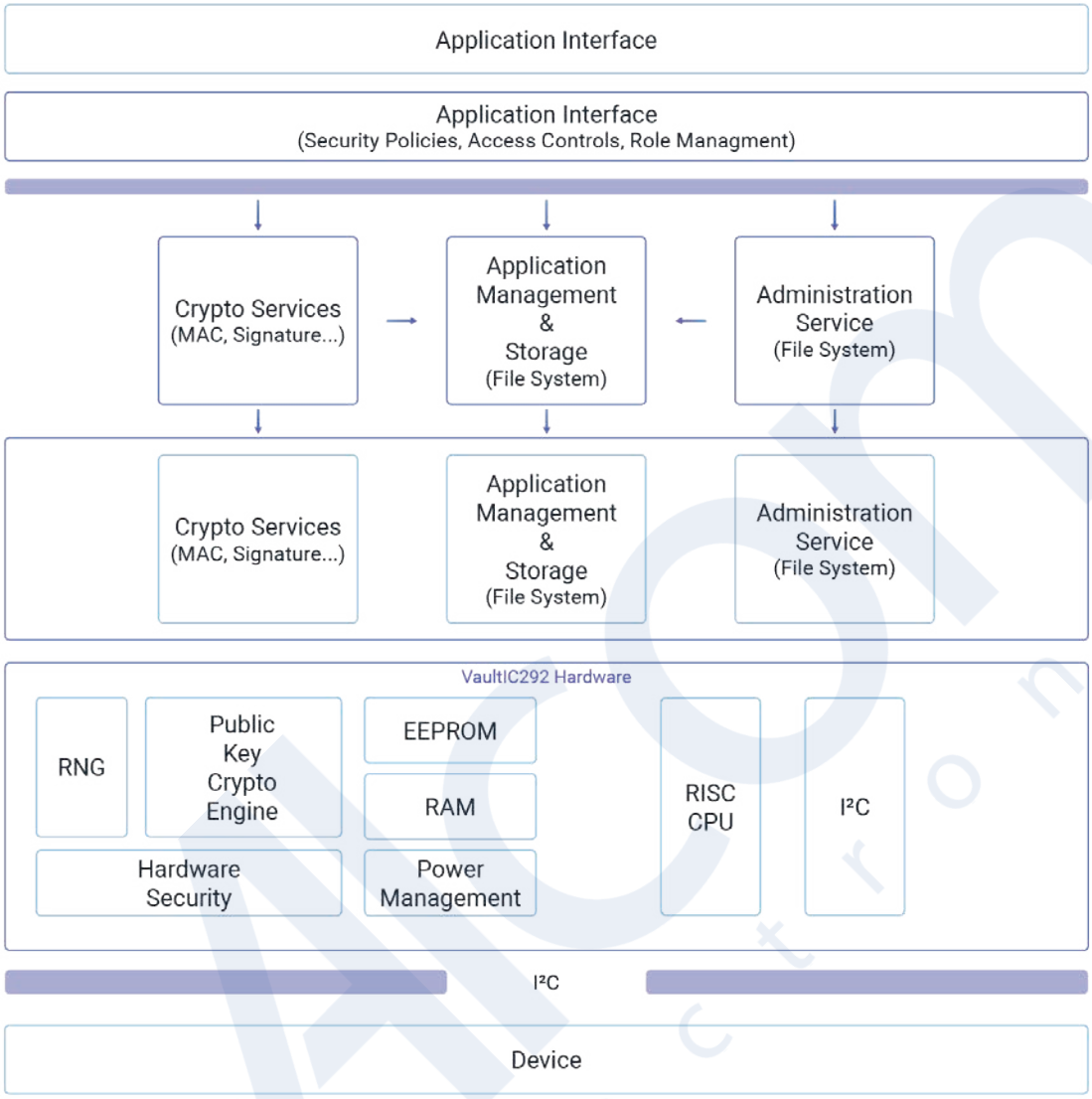
Explore our Solutions for Matter

Visit VaultIC292 Product Page

Alcom
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

SEALSQ semiconductors + quantum

Block Diagram VaultIC292



Technical Features

Cryptographic Services:

- Key pair generation
- Digital signature (ECDSA) P-256
- Shared secret generation (ECDH)
- True Random Number Generation
- Stores up to 5 static key pairs and 3 ephemeral key pairs

Certifications / Standards:

- Hardware: CCEAL5+ ready
- True RNG: NIST SP 800-90A, NIST SP 800-90B
- ECDSA: FIPS 186-4
- ECC Parameters: NIST SP 800-186

Hardware Platform:

- Hardware 16-bit Public Key Crypto Accelerator
- Power consumption: 64µA in standby mode and 3mA to 5mA during CPU-intensive operations
- Operating temperature : -40°C to +105°C
- Operating range: 1.62V to 5.5V
- I²C
- UDFN-8 (RoHS compliant) 2mm x 3mm
- DFN-6 (RoHS compliant) 2mm x 3mm

Trust Services

- Secure Data (keys, X509 certs, etc) Provisioning on wafer or on package : Vaultitrust
- X509 Device Identity Management (managed PKI) : INeS