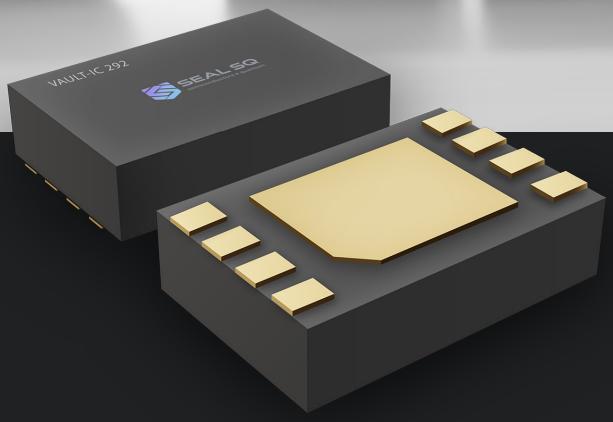
Vault IC 292

The Vault IC 292 is a ready-to-use secure authenticator designed to bring a robust, unique digital identity to a device, essential for applications, such as creating a secure connection to a cloud or a local network based on TLS, or authenticating a USB-C device or a QI Wireless charger.

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



Protocol Ready

Vault IC 292 can be pre-configured with private keys & X509 Certificates compliant with protocols such as Matter, Wi-SUN or OPC, for seamless authentication.

matter Wi SUN OPC

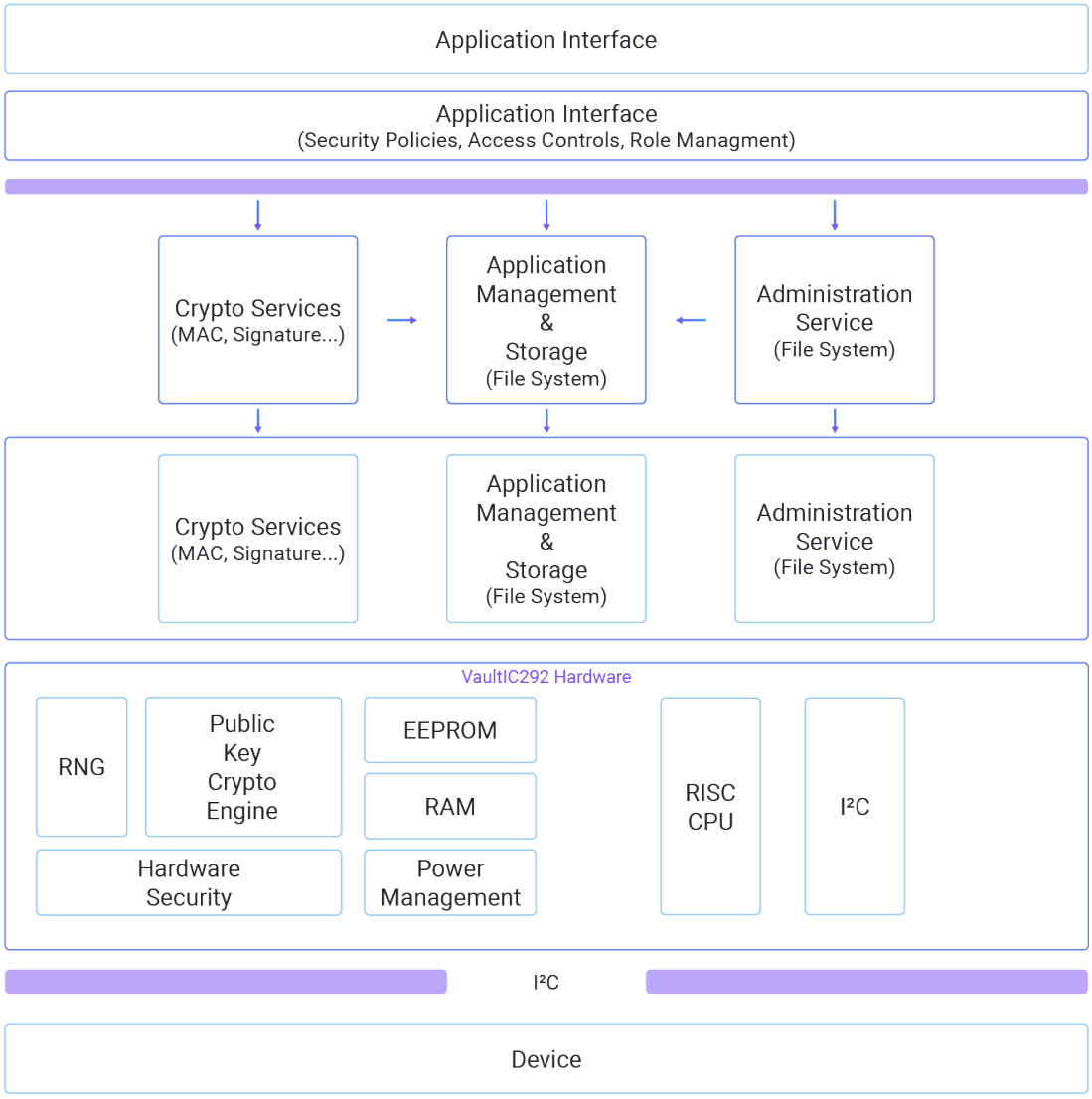
Cloud Ready

Visit us

aws Microsoft Azure

Vault IC 292 can be pre-configured with private keys & X509 Certificates to be used for AWS and Azure Cloud commissioning.

Block Diagram Vault IC 292



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 3 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