VaultIC 408

Our most versatile Secure Element VaultIC 408, provides all cryptographic algorithms and tamper resistant storage to provide state-of-the-art security features to a large panel of devices: Immutable digital identity, Secure communication, Firmware download, Encryption and more...

End-to-End Security

Certified

Fast time-to-Market

Flexible

They trust us

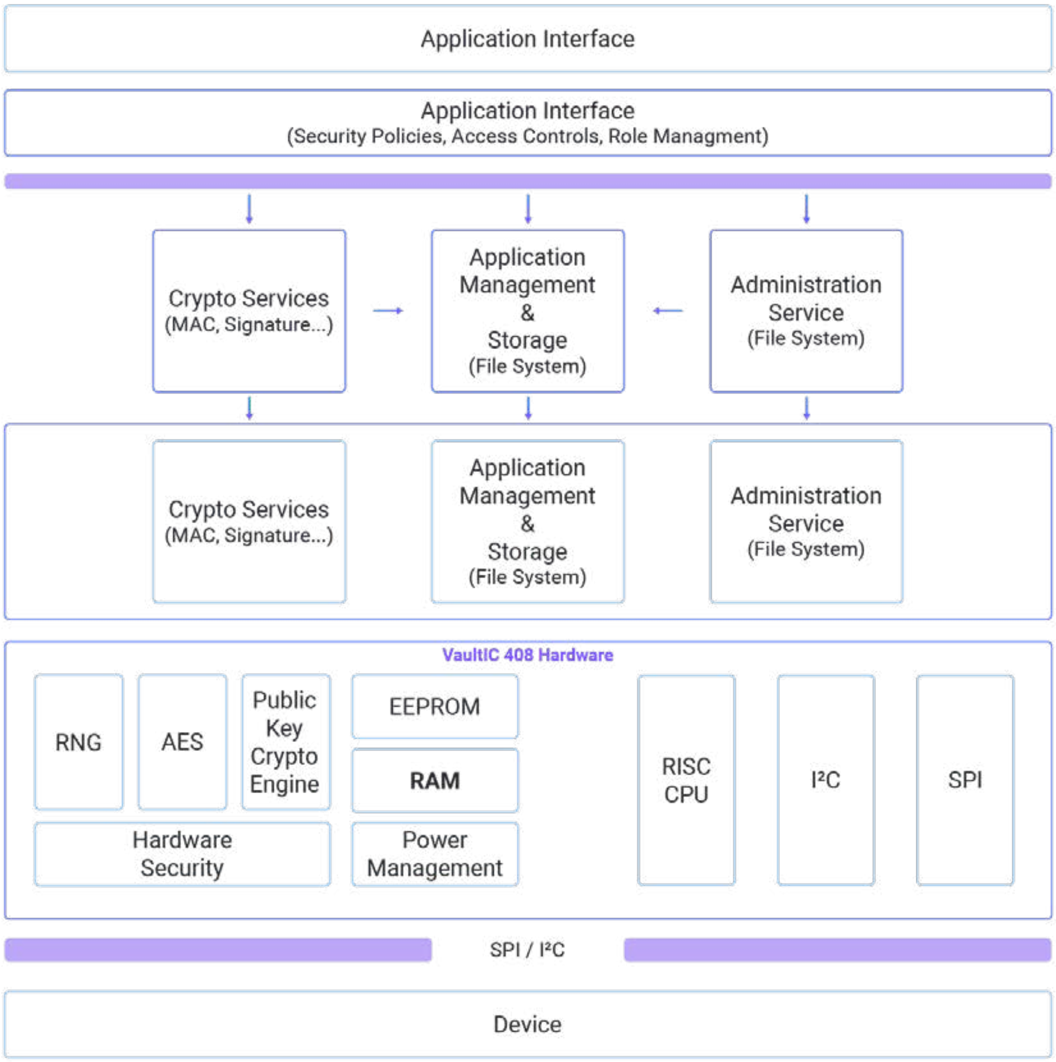
Parrot

Landis+Gyr

VESTEL

SEAL SQ semiconductors + quantum

Block Diagram VaultIC 408



Technical Features

Cryptographic services authentication:

- Elliptic Curve digital signature generation and validation (ECC - GF2n, GFp) up to 572 bit.
- Key Establishment ECC-DH, Message encryption AES, Message Digest SHA256, 384 or 512, Strong Authentication Global Platform SCP03
- On-chip key pair generation or VaultiTrust™ data generation and provisioning

Certifications / Standards:

- VaultIC 408 is FIPS 140-3 CMVP
- True RNG: NIST SP 800-90A, NIST SP 800-90B
- ECDSA: FIPS 186-4
- ECC Parameters: NIST SP 800-186

Hardware Platform:

- User file system up to 16 kBytes.
- Operating range: 1.62V-5.5V.
- Extended industrial temperature range (-40°C to +105°C).
- Available package: SOIC8 (8.0mm x 5.2mm x 2.0mm), QFN20 (4.00mm x 4.00mm x 0.75mm).