Vault IC 155

This Near Field Communication (NFC) secure element allows any object to authenticate itself and communicate online through any NFC enabled smartphone. Highest security available on the NFC tag market, built for specific anti-counterfeiting applications like real-life authentication of high value tangible NFT assets or luxury good authentication with consumer engagement.

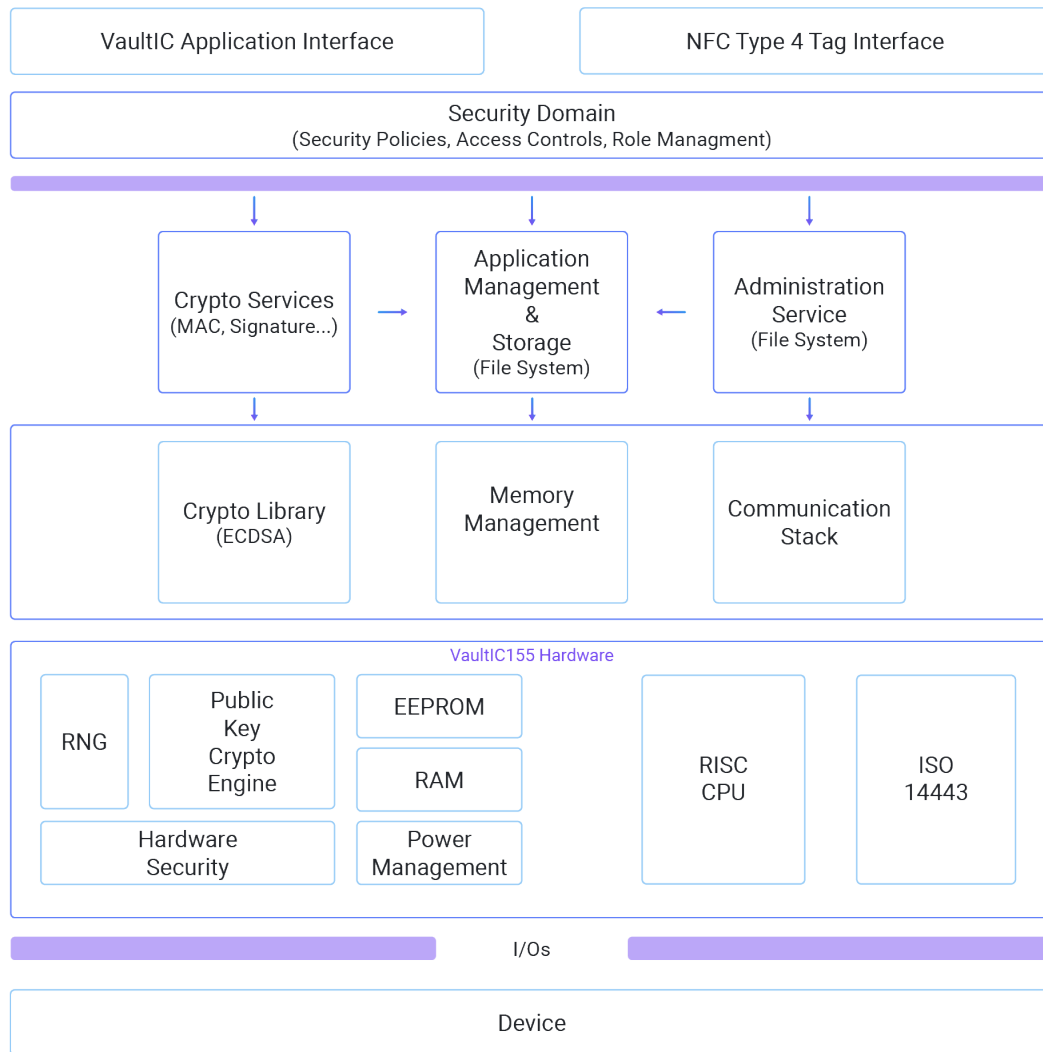**Highest Security**   **Personalized**   **Detects Opening**   **Flexible**

COMMON CRITERIA CERTIFIED

NFC Type 4

ISO IEC 14443-3A Certified — Product Certified

They trust us

Dior   HUBLOT   ITALPREZIOSI   OpSec BrandSecure™

Visit us

SEAL SQ
semiconductors + quantum

Block Diagram Vault IC 155

| VaultIC Application Interface | NFC Type 4 Tag Interface |

Security Domain
(Security Policies, Access Controls, Role Managment)

Crypto Services
(MAC, Signature...)

Application Management & Storage
(File System)

Administration Service
(File System)

Crypto Library
(ECDSA)

Memory Management

Communication Stack

VaultIC155 Hardware

RNG

Public Key Crypto Engine

EEPROM

RAM

Hardware Security

Power Management

RISC CPU

ISO 14443

I/Os

Device

Technical Features

Tamper-resistant secure hardware (derived from Common Criteria EAL4+ certified product family) e.g.:
- Protection against side channel attacks
- Monitoring of environmental parameters
- Protected memory

- Elliptic Curve digital signature (GF2n) up to 303 bits for both iOS and Android.
- Dynamic one-tap authentication over NDEF (DYNA-A mode)
- On-chip key pair generation
- VaultiTrust service keys/certificates generation and provisioning service as a fully managed option

- NFC interface (ISO14443-B, NFC Forum Type 4)
- Opening detection when embedded in e.g. CapSeal® Top tag
- EEPROM: 1 Kbyte for certificate, 2Kbytes for NDEF, 259 bytes for user files with configurable access control
- CapSeal Disk and CapSeal Top tags as a standard, tailored tag form factors as a service
- SEALSQ can provide the low level libraries to integrate Vault IC 155 in any host system.