VaultIC155

Summary Datasheet

SEAL SQ
semiconductors + quantum

Description

The VaultIC155 is a solution designed to secure various non-connected objects against counterfeiting or cloning. Specially dedicated for Wines or Spirits anti-counterfeiting, the VaultIC155 embeds the opening detection feature.

The VaultIC155 embeds 259 bytes of data such as small pictures, recipes, customs forms... for the user.

The proven technology used in VaultIC155 has already been widely adopted and is used in national ID/health cards, e-passports, bank cards (storing user Personal Identification Number, account numbers, authentication keys etc.), pay-TV access control and cell phone SIM cards, where cloning must definitely be prevented.

Designed to keep content secure and avoid leaking information during code execution, the VaultIC155 includes voltage, frequency and temperature detectors, illegal code execution prevention, tampering monitors and protection against side channel attacks and probing. The chip can detect tampering attempts and destroy sensitive data in such events, thus avoiding data confidentiality from being compromised.

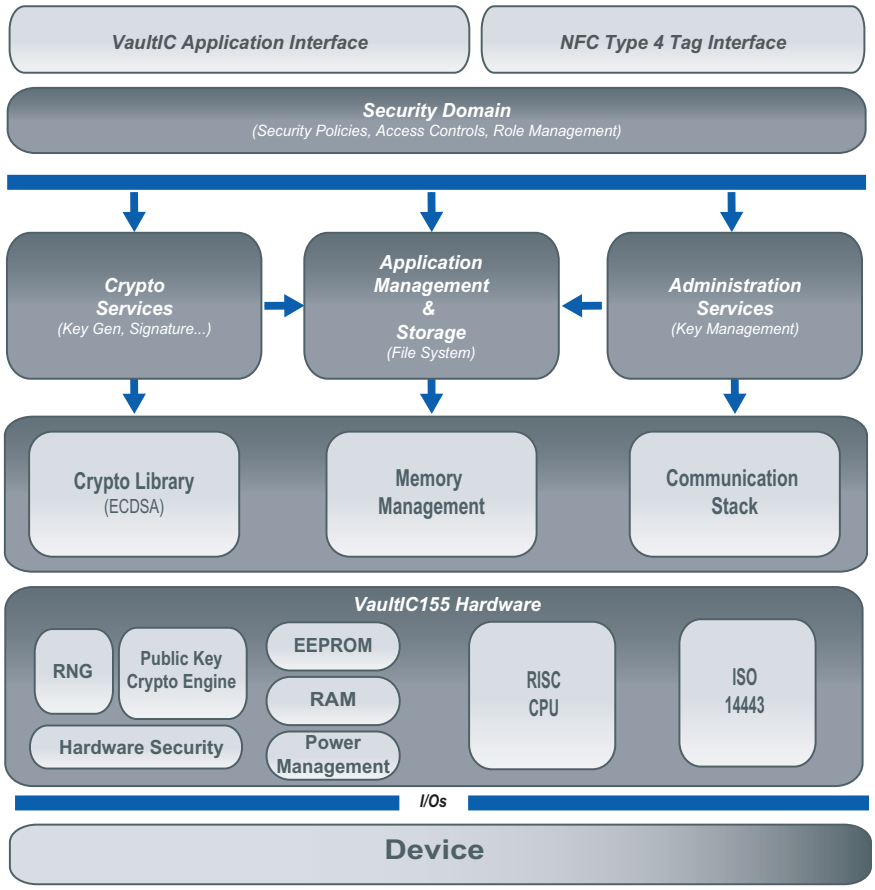
Strong Authentication capability, opening detection, secure storage and low power consumption are main features of the VaultIC155. Its embedded firmware provides advanced functions such as Identity-based authentication, cryptographic command set, ECC Public Key cryptographic algorithm and robust communication protocol.

”Opening Detection” feature prevents authentication in case of bottle opening.

VaultIC155 can also be used as a simple NFC Forum Type 4 Tag that can encapsulate NDEF messages (NFC Data Exchange Format) encoding data in more than 1.5 KBytes of memory.

The VaultIC155 includes DYNA-A authentication that allows PKI-based signature verification through a simple URL (NDEF message). This protocol works on both iOS and Android.

Figure 1 Software and Hardware Architecture



Features

Cryptographic Services

- Public Key Pair Generation (ECC)
- Digital Signature
- Message Digest
- Deterministic Random Number Generation (FIPS compliant)

Cryptographic Algorithms

- ECC GF(2^n) up to 303 bits, including FIPS recommended curves B163, K163, B233, K233, B283, K283

Software Features

- FIPS 140-2 Identity-based Authentication using Mutual Strong Authentication
- Rights Management (Manufacturer, User)
- Opening Detection
- Secure Counters
- Static File System
- NFC Forum Type 4 Tag Operation (T4TOP 2.0) using NFC-Type B
- DYNA-A mode for authentication over NDEF (URL)

Memory

- File System : 1 Kbyte for certificate, 259 bytes User, 2 Kbytes for NDEF files
- Write Endurance 500 Kcycles
- Data Retention 20 Years
- 2ms Program + 2ms Erase

Communication

- Contactless Interface with Full Support for ISO/IEC 14443, On-chip Tuning Capacitance: 104pF (Baud Rate: 106 kbps)

Hardware Platform

- 8-/16-bit RISC CPU
- Hardware Random Number Generator
- Hardware 16-bit Public Key Crypto Accelerator
- Many security features (environmental detectors, tampering monitor, protection against attacks and probing)

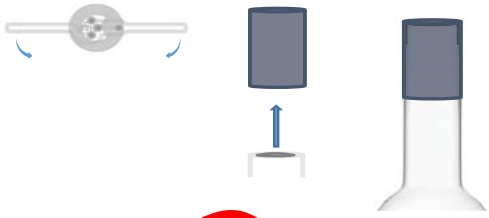
Packages

- Inlays
- Several form factors available, including:
  - LuxSeal Square (Epoxy flexible tags (30 x 30 mm²))

6651BS – 16Jan23

- CapSeal family (Round Flexible and Rigid (25mm diameter)

CapSeal Top:
Round Flexible Tag
(23 mm diameter)
with 2 stripes,
integrated in caps



- Other form factors are available upon request

TBD

Certifications / Standards / Tests

- Targeted Hardware Common Criteria EAL4+
- Targeted FIPS 140-2 Security Level 3
- Fully compliant NFC Forum Type 4 Tag Operation (T4TOP2.0)
- Interoperability proven by StarDust lab

StarDust
THE DIGITAL TESTING COMPANY

Ordering Information

- **Legal**
  - A **Non-Disclosure Agreement** must be signed with SEAL SQ.
  - An **Export License** for cryptographic hardware/software must be granted.
- **Quotation and Volume**
  - For the minimum order of quantity and the annual volume, please contact your local SEAL SQ sales office.
- **Part Number**

Reference		Description
VAULTIC155-xxx-P		**xxx** : Chip “Chrono” Number* **P** = TBD
Reference	**Application**	**Description**
VAULTIC-DK-155	Anti-counterfeiting	Demo Kit for VaultIC155 in PET disk package

* For more details about the Chip “Chrono” Number, please contact your local SEAL SQ sales office.

Demo Kit (coming soon)

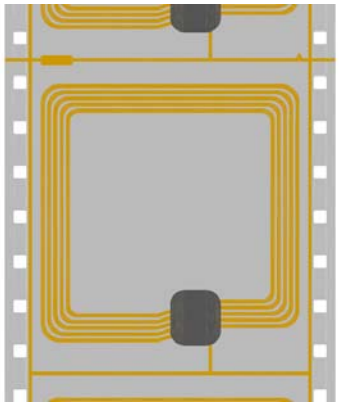
The VaultIC155 Demo Kit provides an overview of the VaultIC155 in an anti-counterfeiting application using VaultNFC mobile application (on Android and on IOS). The content includes samples in CapSeal Disks samples and some instructions to download and use the VaultNFC application.

6651BS – 16Jan23

Pinout & Packaging

Below are some examples of available packages.

Figure 2 LuxSeal Square (30x30mm²)



(here presented in reel)

Figure 3 CapSeal Disk - diameter 25mm

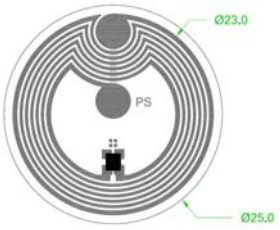


Figure 4 CapSeal Top - diameter 23mm