



Secure Solution *ATVaultIC100 Summary*

General Features

Cryptographic Services

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

Cryptographic Algorithms

- ECC (GF2ⁿ) up to 303 bits, including FIPS recommended curves B233, K233, B283, K283

Software Features

- FIPS 140-2 Identity-based Authentication using Mutual Strong Authentication
- Rights Management (Manufacturer, User)
- Static File System

Memory

- File System 1.5 Kbytes
- Write Endurance 100 Kcycles
- Data Retention 10 Years
- 2ms Program + 2ms Erase

Communication

- I²C (Two Wire Interface), INSIDE's Proprietary Protocol
- One-Wire Interface, INSIDE's Proprietary Protocol

Packages

- 6-DFN (RoHS compliant) 2mm x 3mm

Hardware Platform

- 8-/16-bit RISC CPU
- Hardware Random Number Generator
- Hardware 32-bit Public Key Crypto Accelerator

Certifications / Standards

- FIPS 140-2 Security Level 3

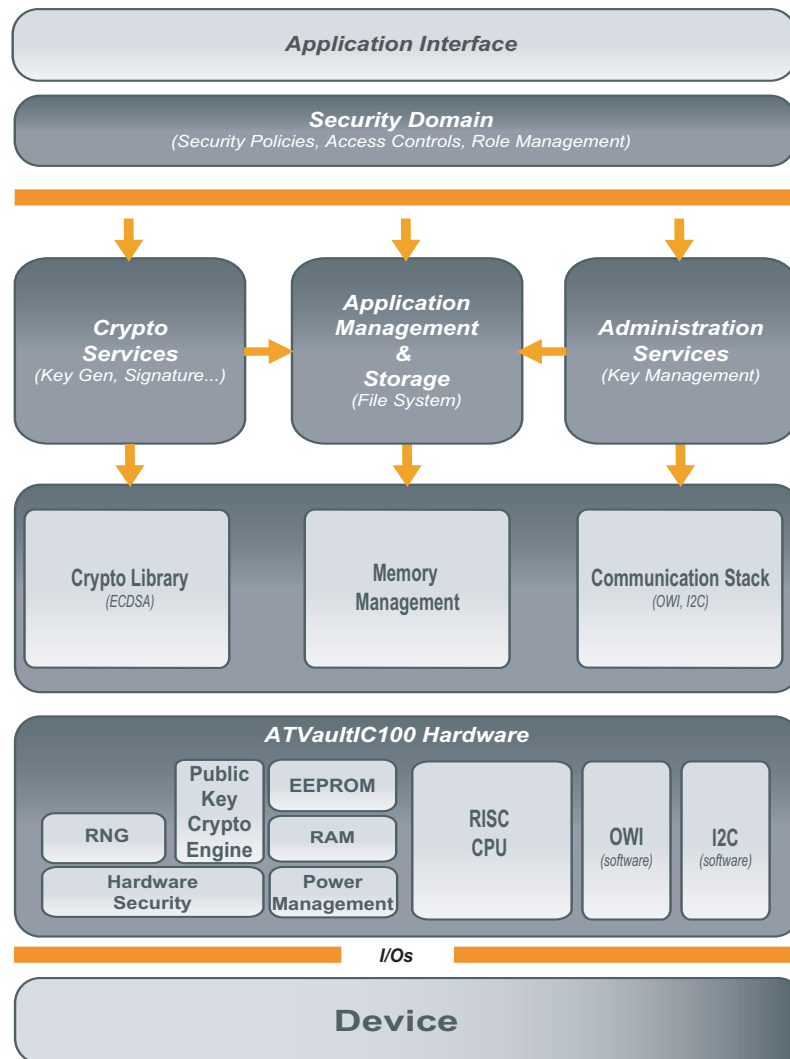
Description

The ATVaultIC100 is an ASSP designed to secure various systems against counterfeiting, cloning or identity theft. It is a hardware security module that can be used in many applications such as IP protection, access control or hardware protection.

The proven technology used in ATVaultIC100 security modules is already widespread and used in national ID/health cards, e-passports, bank cards (storing user Personal Identification Number, account numbers and authentication keys among others), pay-TV access control and cell phone SIM cards (allowing the storage of subscribers' unique ID, PIN code, and authentication to the network), where cloning must definitely be prevented.

Designed to keep contents secure and avoid leaking information during code execution, the ATVaultIC100 include voltage, frequency and temperature detectors, illegal code execution prevention, tampering monitors and protection against side channel attacks and probing. The chips can detect tampering attempts and destroy sensitive data on such events, thus avoiding data confidentiality being compromised. Strong Authentication-capability, secure storage and flexibility thanks to its interfaces (OWI, I2C), low pin count and low power consumption are main features of the ATVaultIC100. Its embedded firmware provides advanced functions such as Identity-based authentication, Cryptographic command set, ECC Public Key cryptographic algorithm, Robust communication Protocol.

Figure 1 Software and Hardware Architecture



Ordering Information

- **Legal**
 - A **Non-Disclosure Agreement** must be signed with Inside Secure.
 - 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 INSIDE Secure sales office.
- **Part Number**
 - See below.

Starter Kit

The VaultIC Starter Kit provides an easy path to master the cryptographic and secure data storage features of the ATVaultIC security modules. The content is :

- ATVaultIC100 samples with 1 dedicated test socket
- 1 generic USB to I²C adapter
- 1 CD-ROM containing a support documentation set (getting started, application notes, reference design), some demo applications to get an insight into the ATVaultIC features, the "VaultIC Manager" tool to design the file system and to personalize samples, a hardware independent cryptographic API with source code.

| Reference | | Description |
|-----------------------|-------------------|---|
| ATVaultIC100-xxx-P | | xxx : Chip Personalization Number* P = 6Z : DFN6 Package |
| Reference | Application | Description |
| ATVAULTIC-STK02-1006Z | Embedded Security | Starter Kit for ATVaultIC100 in DFN6 package |
| ATVAULTIC-STK12-1006Z | Embedded Security | Starter Kit for ATVaultIC100 in DFN6 package (no I2C adapter inside) |

* For more details about the Chip Personalization Number, please contact your local INSIDE Secure sales office.