EMBEDDED
SECURITY SOLUTIONS

IP delivered as
synthesizable Verilog
RTL source code

vaultIP

A Silicon IP Secure Element for 360° Mobile Device Security

Add 360° security to mobile processors, protecting against an increasing number of sophisticated threats to valuable data and private information. Gain competitive advantage by quickly and cost effectively delivering comprehensive protection with VaultIP as a stand-alone secure element or in combination with ARM® Trustzone® architectures.

Mobile Security Is No Longer Optional

Mobile devices with 24x7 connectivity are pervasive and enabling new ways of doing business. With the arrival of Multi-core performance for application processors these devices can run virtually any application, including many which handle highly sensitive, valuable and mission critical information.

Smartphones and tablets routinely hold confidential data for individuals and businesses, exponentially increasing the risk of theft or compromise. The value of that data has spawned a diverse range of attacks, all aimed at piercing mobile device security. Software attacks can exploit the weaknesses in an application or operating system by extracting, modifying or destroying information held within the device.

Security Built on ARM TrustZone Technology

ARM's TrustZone technology, part of the Cortex-A processor family, enables the development of a Trusted Execution Environment (TEE) within a mobile device. GlobalPlatform defines a TEE as a secure environment providing hardware protection against software attacks; it is comprised of two elements, the TrustZone hardware components and a Secure Operating System.

A TEE forms the foundation for mobile device security, an area where "trusted applications" can execute with protection from disturbance, tampering or eavesdropping by malicious software. Another layer is needed on top of this foundation to fully enable impenetrable protection for mobile devices.

→ Advanced Security to Support:

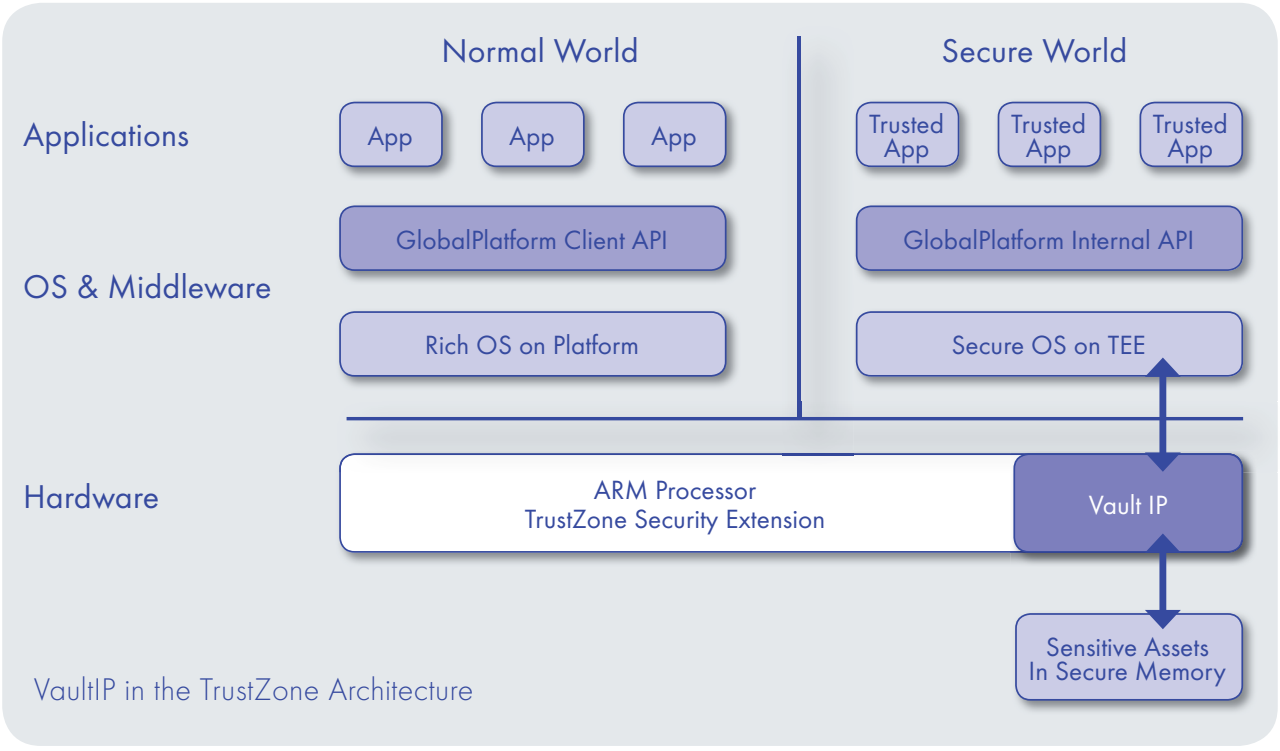
- Online Banking
- Ticketing
- Internet Transactions
- Proximity Payments
- Mobile Point-of-Sale
- Enterprise VPN
- DRM and Content Protection
- Data-at-Rest Protection
- Government ID

driving trust™ inside SECURE

www.insidesecure.com

VaultIP - 360° Security for TrustZone-based Processors

VaultIP is an embedded security platform that fortifies a TEE against software attacks. Implemented in Hardware IP, it comprises a tightly integrated set of modules optimized for the ARM architecture.



VaultIP in the TrustZone Architecture

VaultIP: Multi-Vector Protection

VaultIP provides the 'Trust Anchor' needed by a Secure Operating System to run effectively within a TEE. VaultIP manages sensitive assets, such as cryptographic keys, so they are never exposed to non-secured access. It provides secure storage of root keys and enforces the key management policies, so that key material cannot be moved to the primary CPU. With VaultIP, keys are never exposed to the vulnerabilities that come with handling by software.

Further protection against software attacks are provided by additional VaultIP-enabled capabilities, including Secure Timers, Secure Boot, Secure Debug and Password Authentication. Underlying all these capabilities is a library of cryptographic algorithms and a True Random Number Generator (TRNG).

Protection for Designs without a TEE

The VaultIP 'Trust Anchor' can also be implemented in semiconductor designs that do not include a TEE. The secure, non-volatile memory management capabilities are integrated with software operations via a set of VaultIP Access APIs, protecting keys and other sensitive material from any exposure to software attacks.

Standards-Based and Certification Ready

VaultIP is compliant with the specifications of GlobalPlatform and the ARM TrustZone Ready Program. Mobile devices incorporating VaultIP will be prepared for multiple security certifications, including FIPS-140-2 Level 2 and Common Criteria.

→ The VaultIP Trust Anchor:

Secure, Non-volatile Memory Management, enabling:

- **Secure Boot:** prevent loading of compromised OS versions
- **Secure Debug:** stop unauthorized access to system information
- **Secure Counters:** prevent rollbacks and license tampering
- **Secure Timers:** locality checks and limits on time for key use
- **Authentication and Authorization:** ensure confidentiality of private information
- **Secure Key Provisioning, Storage, Management and Use:** control storage and access to core key material

For further details on all of INSIDE's security solutions, visit www.insidesecure.com

Arteparc Bachasson, Bât A - Rue de la carrière de Bachasson, CS70025 - 13590 MEYREUIL - FRANCE - Tel. : +33(0)4 42 905 905 - Fax : +33(0)4 42 370 198 - E-mail: info@insidefr.com