inside SECURE Enterprise Security & Secure Access

SAFEZONE FIPS CRYPTOGRAPHIC MODULE

Fulfill your FIPS140-2 requirement quickly and cost effectively

• benefits

- Easy to integrate
- Wide set of algorithms supported
- Field-proven with IPsec, SSL and DAR
- Secure key management
- Low memory footprint (100 kB)
- Certified on a wide range of architectures:
  ARMv6, ARMv7, ARMv8, ARM64, x86, x86-64...
  and operating systems: Linux, Android, iOS, Trustonic TEE
- Highly portable: FIPS certification can be vendor affirmed on many platforms
- Reduced Development Costs and Shortened Time to Market
- Worldwide Developer-level Support
- Futureproof: Design according to latest NIST guidelines and draft FIPS140-4
- AES acceleration on x86 and ARMv8 64bit platforms

SafeZone FIPS cryptographic module is a compact and portable cryptographic software library validated by NIST (certificate 2389) providing a wide set of cryptographic algorithms. It has been designed to provide high performance on resource-constrained environments. This module is shipping with the market leading QuickSec VPN Client for Android, QuickSec IPsec Server Toolkit, MatrixSSL and MatrixDAR products.

Needs for FIPS140-2 validation

With an increasing number of number of industries and critical infrastructure becoming targets of cyber attacks, governments and industries mandate the use of certified cryptography modules. Federal Information Processing Standard (FIPS) 140-2 is a globally recognized U.S government security standard that is being widely adopted in commercial, government and defense applications. U.S and Canadian Government agencies have wide ranging requirements that the systems it deploys (including mobile devices) must use FIPS140-2 validated cryptographic modules. This requirement extends to civilian companies who contract to U.S., Canadian or U.K. governmental organizations.

Improve security and lower costs

FIPS 140-2 certification ensures that the security module has been independently reviewed by an approved test laboratory against government standards. This in-depth review is a slow and costly process during which the module is tested, the code is reviewed and detailled understanding of cryptography is needed. Re-using an already validated cryptographic module and benefiting from engineering level support allows to bring a product to market quickly and cost-effectively. It is far less expensive to discover product vulnerability during testing rather than after it is has gone to market.

Key features

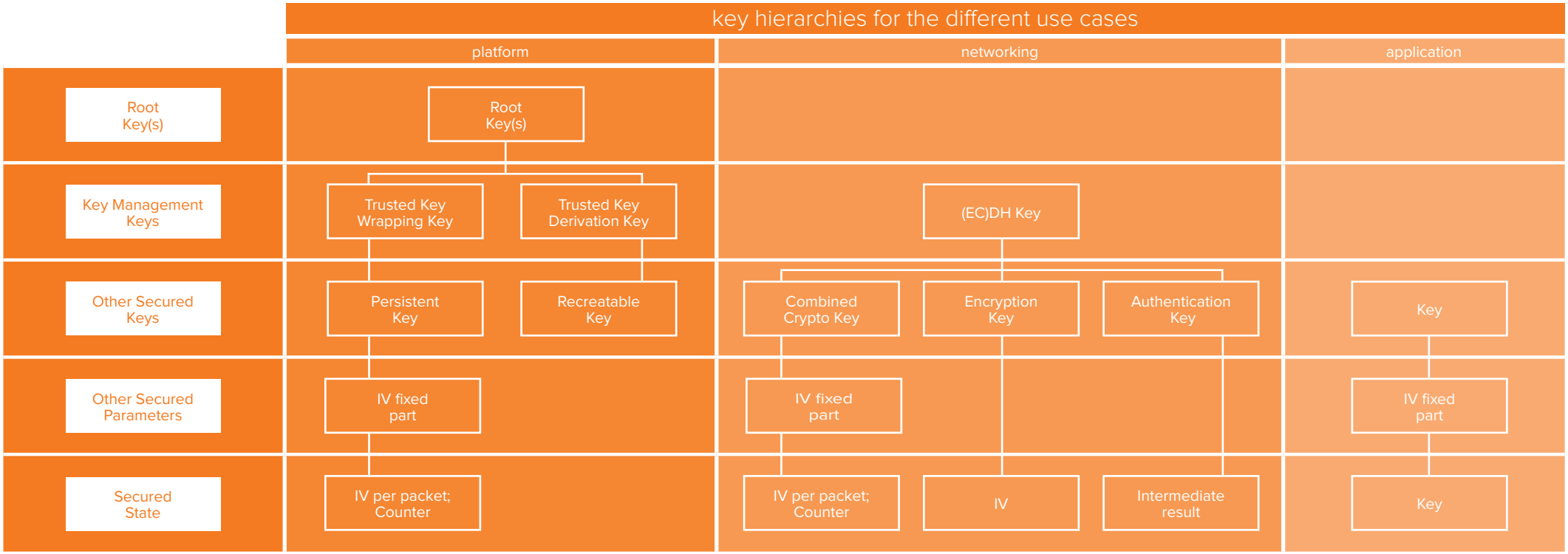
SafeZone FIPS Cryptographic module supports NIST Approved cryptographic algorithms for symmetric and asymmetric cryptography as shown on the table. The module has support for using cryptographic secrets like a Root Key or Hardware Unique Key (HUK) on platforms that have them, as a root of trust for a local hierarchy of trusted key material. Keys are securely managed by the asset store. It also supports self-testing functionality and two operator roles (Crypto Officer and User Role) as defined by the FIPS standard.

security concept	algorithm	Standard
Confidentiality	AES 3DES	FIPS 197 NIST SP 800-38A NIST SP 800-67
Authenticity	SHA-1 SHA-2 AES CMAC GMAC	FIPS 180-3 FIPS 198-1 NIST SP 800-38B
Confidentiality & Authenticity	AES CCM AES GCM	NIST SP 800-38C NIST SP 800-38D
Digital Signatures	RSA DSA ECDSA	FIPS186-4
Key Transport	AES-WRAP RSA	NIST SP 800- 38F NIST SP 800-56B
Key Agreement	DH EC-DH	NIST SP 800-56A
Key Derivation	IKEv1 IKEv2 TLS1.0 TLS1.1 TLS1.2	NIST SP 800-108 NIST SP 800-132 NIST SP 800- 135rev1
Data At Rest	XTS-AES	NIST SP 800-38E
Random Number	DRBG (AES-CTR)	NIST SP 800-90

Use cases

SafeZone FIPS Cryptographic module is used for three use cases:

- Platform security using root key(s) provided by the platform
- Networking security where the key is derived through asymmetric cryptography
- Application security where the key is provided by the application



FIPS140-2 CERTIFICATION

- The module is certified for FIPS140-2 level 1 on Android, iOS, Linux and t-300 operating systems. On other platforms, if the code can be ported without any source code modification, the certification can be vendor affirmed.

FIPS140-2 REVALIDATION SERVICE

- Inside Secure typically provides a vendor affirmed binary of SafeZone FIPS cryptographic module to its customer. It also provides revalidation service for the customers who want their name listed on the official FIPS140-2 certificate.

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

inside SECURE Driving Trust