SAFEZONE FIPS CRYPTOGRAPHIC MODULE

inside secure

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 OEM Customer Support

Increasing demand for critical infrastructure protection

Under increasing threat a growing number of Cyber systems and assets so vital their incapacity or destruction would have debilitating impact on physical, economic security or public health and safety include :

- Banking and Finance
- Chemical Production
- Communications
- Critical Manufacturing
- Defense Industrial Base
- Emergency Services
- Energy Production & Grids
- Government Facilities
- Healthcare and Medical
- Information Technology
- Postal and Shipping
- Transportation Systems

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 detailed 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

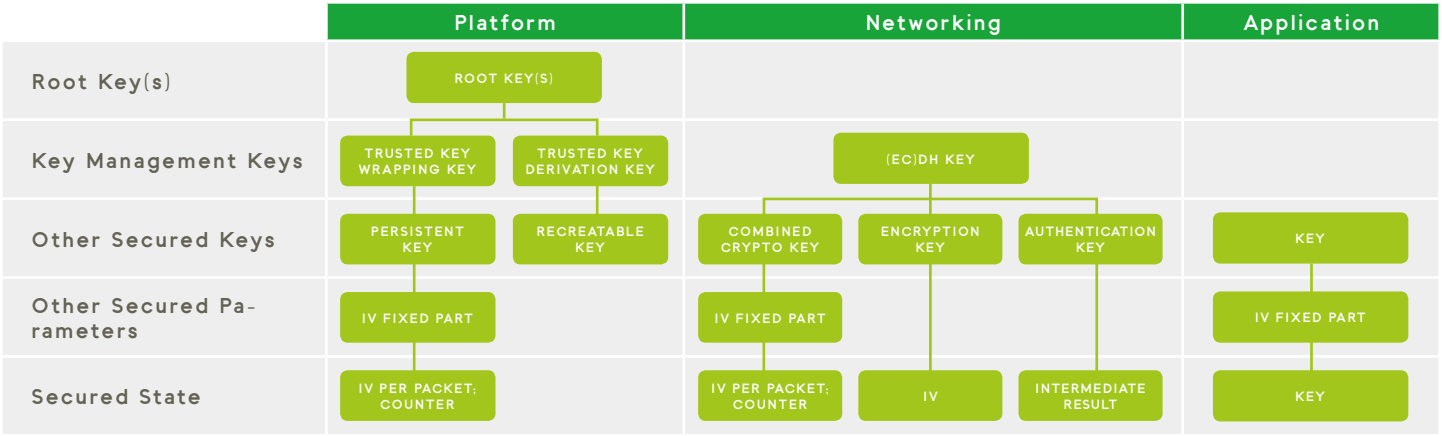
SafeZone FIPS Cryptographic module supports NIST Approved cryptographic algorithms for symmetric and asymmetric cryptography as shown on the table. The module has support for using cryptographic secrets like a Root Key or Hardware Unique Key (HUK) on platforms that have them, as a root of trust for a 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.

Supported algorithms		
Security concept	**Algorithms**	**Key length**
Confidentiality	AES 3DES	128-256 bits 192 bits
Authenticity	SHA-1 SHA-2 AES CMAC GMAC	80-160 bits 112-512 bits 128-256 bits
Confidentiality & Authenticity	AES CCM GCM	128-256 bits
Digital Signatures	RSA DSA EC-DSA	1024-4096 bits 1024-3072 bits 192-521 bits
Key Transport	AES-WRAP RSA	128-256 bits 1024-4096 bits
Key Agreement	DH EC-DH	1024-3072 bits 192-521 bits
Key Derivation	NIST IKEv2 TLS 1.2 TLS 1.0-1.1	80-512 bits 384 bits
Data At Rest Confidentiality	XTS-AES	256-512 bits

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 and Linux. On other platforms, if the code can be ported without any source code modification, the certification can be vendor affirmed.

FIPS140-2 VENDOR AFFIRMATION

If the code can be ported without any source code modification, to a platform similar to the certified ones, the certification can be vendor affirmed. It requires that the vendor re-compile the cryptographic module on its customer platform.

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

inside secure