AGILESEC CRYPTO

AGILESEC CRYPTO SDK

Reach new customers in new markets by adding sovereign and standards-based encryption, digital signatures and other security mechanisms into your secure products.

Cryptographic algorithm selection is critical to secure product design, affecting not only the security posture of a product but also the geopolitical regions of the world to which a product can be sold. Infosec Global's team of world renowned cryptography experts have carefully selected the strongest ciphers for inclusion in the Agilesec Crypto SDK, and can also make available country-specific sovereign cryptography, alleviating the uncertainty of marketing secure products on the global stage.

FEATURES AND BENEFITS

FIPS 140-2 Cryptography

- Supports 3rd party FIPS approved modules – Hardware or Software
- Use InfoSec Global's pre-approved FIPS 140-2 validated level 1 cryptographic provider. (Available 2017)

Standards-based Cryptography

- Secure and optimized implementations of carefully selected cryptographic algorithms generally used in today's most secure applications.
- Ensure that your products use the strongest cryptographic security as selected by InfoSec Global's advisory board of world renowned cryptographers.

"Plugin" Cipher Support (Multi-Crypto Framework)

- Support changing and evolving security needs by allowing end-product cryptography to be replaced after it is in the end user's hands.
- Simplifies development and reduces support costs in high security environments where proprietary cryptography is required.

Programming Language Support

- C, C++
- Integration into your existing software development environment.

Platform Support

- Windows (x86), Linux (x86, ARM), MacOS (x86), iOS(ARM), Android (ARM)

FEATURE OVERVIEW

SYMMETRIC ENCRYPTION & MODES
AES-ECB, AES-CBC, AES-GCM, AES-CTR, 3DES

ASYMMETRIC ENCRYPTION
RSA Encryption (RSA PKCS1v15, RSA OAEP, RSA Raw)

KEY AGREEMENT
DH, ECDH, RSA Key Wrap

DIGITAL SIGNATURES
ECDSA, RSA PKCS1v15, RSA PSS, DSA, EdDSA (Ed25519, Ed448), XMSS

HASH FUNCTIONS
SHA-3 (224, 256, 384, 512)
SHAKE 128, SHAKE 256
SHA-2 (224, 256, 384, 512)

MESSAGE AUTHENTICATION
HMAC, CMAC

RANDOM NUMBER
DRBG
HMAC DRBG

ELLIPTIC CURVES
NIST (224, 256, 384, 521)
Brainpool (256, 384, 512)
curve25519
curve448

SERVICES AND SUPPORT

INTEGRATION SERVICES
ISG's experienced software developers can help integrate premium security into your product as a consulting project.

DEVELOPER SUPPORT
ISG's security experts are available to answer your software development team's security and cryptography questions.

PRODUCT SUPPORT UPDATES AND UPGRADES
AGILESEC SDK's are backed by ongoing product support with annual subscription options for future updates and upgrades.

ABOUT INFOSEC GLOBAL

At a time when the integrity of cryptography and communication systems has been cast in doubt, ISG is committed to providing the most secure and transparent approach to cybersecurity that will re-establish certainty of protection for communications and information.

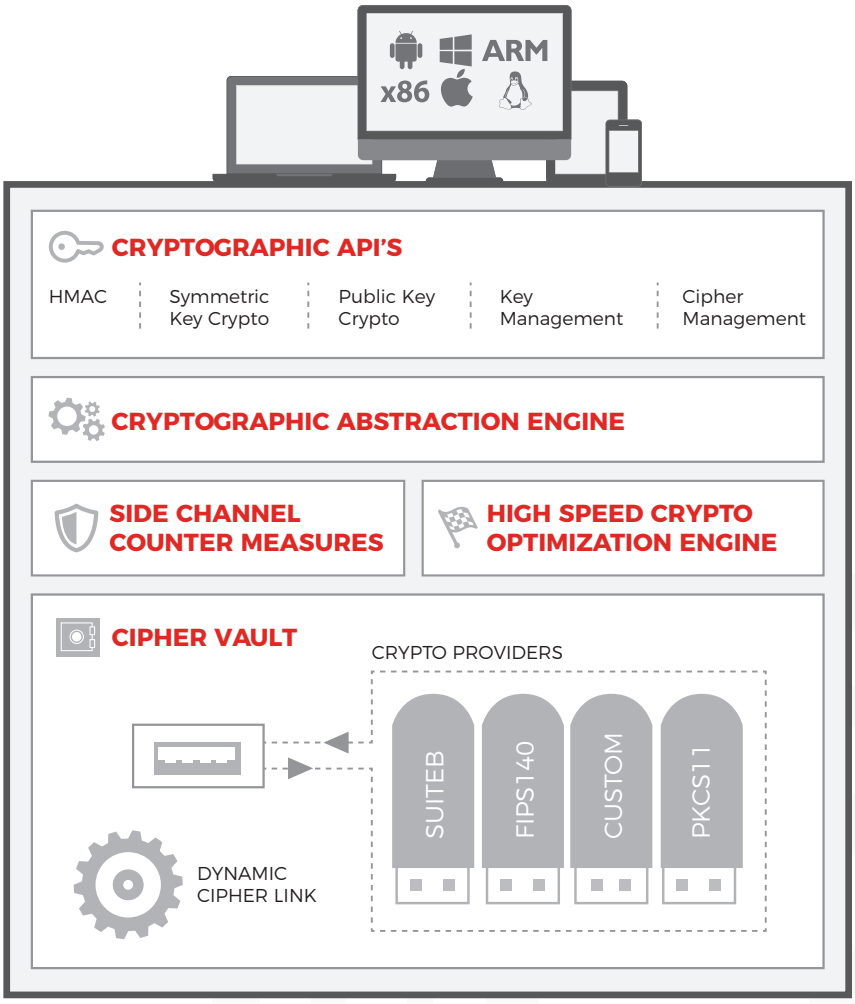
ISG delivers state of the art cryptography and cybersecurity solutions to embedded device designers, enterprise software vendors and government contractors.

Our solutions provide the strongest protection available and is often tailored for regions of the world with uniquely specific cryptography and cybersecurity requirements

GLOBAL CRYPTOGRAPHIC SUPPORT

The Agilesec Multi-Crypto framework allows ciphers to be replaced in products before and after delivery into the end customer's hands. Allowing products to be configured to meet the localized cryptography requirements of the most security conscious customers.

- Allows "pluggable" ciphers post-delivery
- Localized cipher variants can co-exist
- Ship product with standard Crypto
- Allow end-users to configure with localized Crypto



INFOSEC GLOBAL

ZÜRICH
Hardturmstrasse 103
8005, Zürich
Switzerland

TORONTO
Tel: +1 416-492-3333
2225 Sheppard Avenue East
Suite 1402, Toronto, ON
M2J 5C2 Canada

WWW.INFOSECGLOBAL.COM
info@infosecglobal.com