



# whiteCrypton® Secure Key Box™

## Robust Whitebox Cryptography

### BUSINESS BENEFITS

- **Don't be the Headline.** Protect your endpoints from attack, manage risk, and build brand. Prevent loss of revenue and reputation with application shielding.
- **Protect Secrets and Keys.** Provides deeper support and security than the iOS or Android keychains to protect passwords and keys in mobile apps, and supports IoT devices and general services.
- **Proven and Easy to Use.** Proven in millions of mobile apps, DRM and IoT systems world-wide; it is simple to integrate into your application for a wide variety of platforms.
- **Foil Hackers.** Protect secrets and keys in IoT devices and mobile apps where hackers could attack them.

### A CRYPTOGRAPHIC LIBRARY THAT PROTECTS YOUR SECRETS

Cryptographic keys are the root of your secure systems. All mission critical software must protect keys. whiteCrypton Secure Key Box performs common cryptographic functions while keeping secrets and cryptographic keys secure without requiring dedicated hardware security.

#### Whitebox Cryptography Library

Secure Key Box uses advanced mathematical technologies to protect secrets and keys. Particularly in open environments where anyone can gain full control over your code, memory and storage of the execution device. Secure Key Box provides the most common cryptographic algorithms in a secure manner where the cryptographic keys are encoded so they are never revealed in plain form – during runtime, at rest, or in transit.

#### No Dedicated Security Hardware Required

Certain computers, smartphones and tablets provide dedicated hardware to store secrets, but often the dedicated hardware is not available for general use by developers or is too costly. Platforms that run IoT devices and services may have no security hardware at all. That's why Secure Key Box provides unsurpassed protection for keys and secrets without requiring dedicated security hardware.

#### Drop-in Replacement

Secure Key Box is a drop-in replacement for standard cryptographic libraries. It is wrapped or used directly by applications to access the common services they depend on, while benefiting from the robust protection of secrets and keys it provides. Secure Key Box supports a wide variety of popular platforms, chip architectures and development environments.

### USE CASES



#### Payments & Banking

Protect host card emulation and authentication credentials for mobile payment systems, digital wallets and mobile banking.



#### Healthcare

Protects patient privacy and safety by protecting software that handles sensitive medical information.



#### Media & Entertainment

Shield apps to ensure content is protected and digital rights are enforced.



#### Connected Car

Provides application shielding for critical car components to ensure the integrity of the system and protection of the occupants.

## FEATURES

### Unsurpassed Security

- **Encoded Keys.** Innovative technology keeps keys encoded, even when they are being used by cryptographic algorithms, for unsurpassed protection against discovery.
- **Penetration Testing.** Secure Key Box is continually subjected to penetration testing by third-party experts to ensure the highest level of protection.
- **Encryption & Decryption.** Popular algorithms and modes are supported to ensure privacy.
- **Hashing, Signing & Verification.** Popular algorithms are supported to ensure integrity and authenticity of payloads.
- **Wrapping & Unwrapping.** Wrapping and unwrapping routines enable keys and secrets to be securely imported and exported.
- **Key Generation and Key Agreement.** Supports static keys, dynamically generated keys, derived keys, imported wrapped keys and agreed-upon keys.
- **Device Binding.** Bind keys to a specific hardware device, using its unique information.
- **FIPS 140-2** validation ensures the highest level of protection for passwords and keys to protect them from prying eyes.

### Wide Platform Support

- **No Dedicated Security Hardware.** No TPM, TEE, SE, SIM or HSM devices are required.
- **Platforms.** Linux (glibc, uClibc, musl), Windows, macOS, Android, iOS, tvOS, Google Native Client (NaCl), Playstation 3, MinGW, QNX and others.

### Popular Cryptographic Algorithms

- **Encryption:** AES-128/192/256 (ECB, CBC, CTR), DES & 3DES (ECB and CBC)
- **Decryption:** AES-128/192/256 (ECB, CBC, CTR), DES & 3DES (ECB and CBC), RSA-1024/2048 (OAEP or v1.5), ElGamal Elliptic Curve Cryptography (ECC)
- **Authenticated Encryption:** AES-128/192/256 (GCM)
- **Signing:** AES-CMAC, HMAC, RSA Signature, RSA Probabilistic Signature, Elliptic Curve Digital Signature Algorithm (ECDSA). Use MD5 or SHA-1/224/256/384/512 as the hash function

- **Verification:** AES-CMAC, HMAC, ISO/IEC 9797-1 MAC (Retail MAC)
- **Unwrapping Keys:** Uses AES-128/256/512 (ECB, CBC, CTR) algorithm for ElGamal ECC keys, AES-128/192/256 (CBC, CTR) algorithm for private RSA keys, RSA-1024/2048 (OAEP or v1.5) or AES-128/256/512 (ECB, CBC, CTR) or ElGamal ECC for raw bytes, AES key unwrapping defined by NIST, CMLA AES and CMLA RSA unwrapping.
- **Wrapping Plain Data:** AES-128/192/256 (ECB, CBC)
- **Wrapping Keys:** AES-128/192/256 (CBC) or AESKW or RSA-1024/2048 (OAEP or v1.5) for ECC keys or raw bytes, just XOR
- **Key Generation:** Random buffer of bytes for AES, DES, 3DES algorithms; key pairs for Elliptic Curve Cryptography algorithms
- **Key Agreement:** Classic Diffie-Hellman (DH), Elliptic Curve Diffie-Hellman (ECDH)
- **Calculate Digests:** MD5, SHA-1/224/256/384/512
- **Key Derivation:** A large variety of byte and key manipulation routines including slicing substrings, selecting odd or even bytes, iterated SHA-1, SHA-256, SHA-384, byte reversing, NIST 800-108 key derivation, Open Mobile Alliance (OMA) KDF2, derive raw bytes from private ECC key, CMLA key derivation, encrypt/decrypt raw bytes with AES-128/192/256, XORing a key and more.
- **Authentication:** CDMA2000 authentication algorithm

### Strengthen Your Security with Complementary Products



#### whiteCryption® Code Protection™

Shields mobile apps and code that operates on untrusted devices to foil hackers and protect code secrets.



#### Seacert™

Provides trusted identities for your IoT devices, mobile apps, services and users with customized X.509 certificates and a robust PKI infrastructure.