intertrust®

whiteCryption® Secure Key Box™

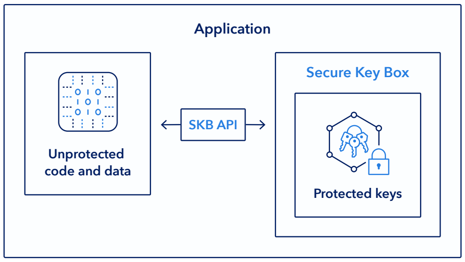
Industry-leading white-box cryptography keeps secrets and keys safe on any device

Equip your software with enterprise-grade key security

Even the strongest encryption methods fail when the cryptographic keys are compromised. Hackers can easily find and steal exposed keys in code or memory. whiteCryption Secure Key Box protects your data and secrets by transforming keys and obscuring cryptographic algorithms so that keys never appear in the clear and the execution logic is untraceable. Your keys cannot be extracted–even if the device itself has been breached.

Protect your cryptographic keys at all times

Secure Key Box keeps cryptographic keys safe whether at rest, in transit, or in use, securing them against sophisticated side-channel attacks and unsafe operating environments. It protects all your cryptographic functions including key generation, encryption, digital signatures, key agreement, and dynamic key unwrapping.



Seamless, secure, software-based key protection

With Secure Key Box, eliminate hardware dependence, cost, and complexity while ensuring universal, uniform security across platforms. Reduce time to market with quickly integrated key protection based on industry-leading white-box cryptography.

Simplify your regulatory compliance

Comply with data privacy laws and encryption key security requirements set by strictly regulated industries such as financial services and healthcare. Accelerate regulatory approval and testing timelines with solution-driven key protection, including out-of-the-box support for cryptographic protocols specified by PCI-DSS.

Retain control and flexibility

Secure Key Box gives you full control over your keys. Configure features to optimize application performance and binary size. Respond to threats with custom callback functions through our Code Protection integration. Diversified libraries with unique binary footprint and root keys ensure your keys work only for you.

Benefits

Strongest software-based key protection
Conceals and obscures keys and algorithm logic so keys can't be extracted and tampering attempts are shut down.

Protect keys when stored, in transit, and in use
Keep keys safe at all times, even on compromised, jailbroken, or rooted devices. Keys are never exposed in memory; algorithms operate directly on encoded keys.

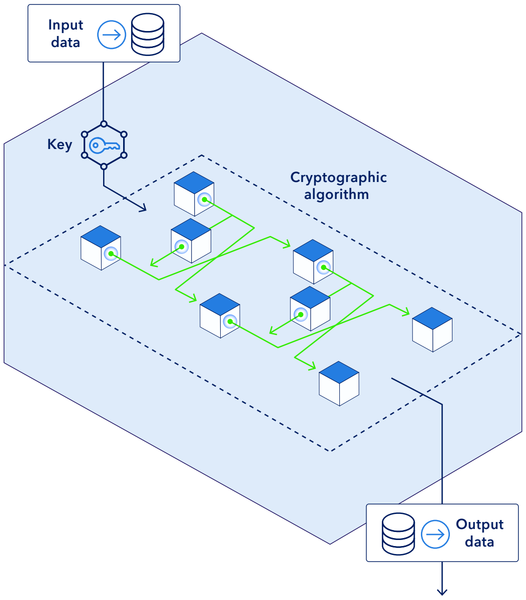
Accelerate time to market
Replace your standard cryptographic libraries with plug and play white-box secured key protection.

Any algorithm, any platform
Agnostic security works on all platforms and devices. Protect any cryptographic algorithm such as AES, 3DES, RSA, ECC, HMAC, and others. Custom algorithm support also available.

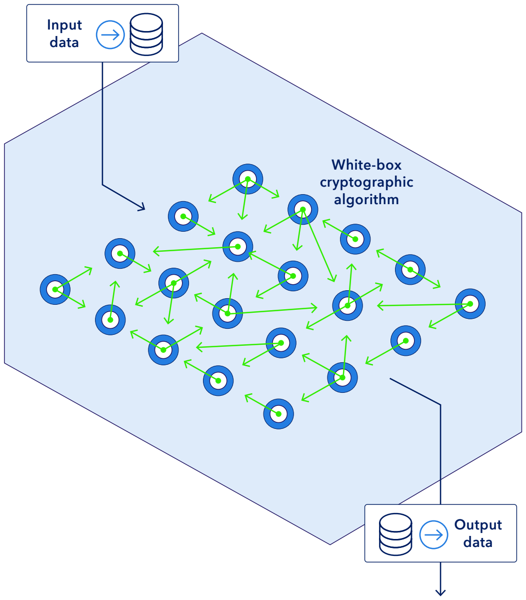
Comply with regulations
Meet and exceed application security and data privacy requirements while minimizing approval and testing timelines. Supports PCI-DSS specifications including separation of payment card and PIN data.

Backed by experts
Intertrust's deep cryptographic expertise guides every step of your deployment. Secure Key Box protects keys in millions of installed apps and undergoes regular independent security testing.

Standard cryptography



Secure Key Box white-box cryptography



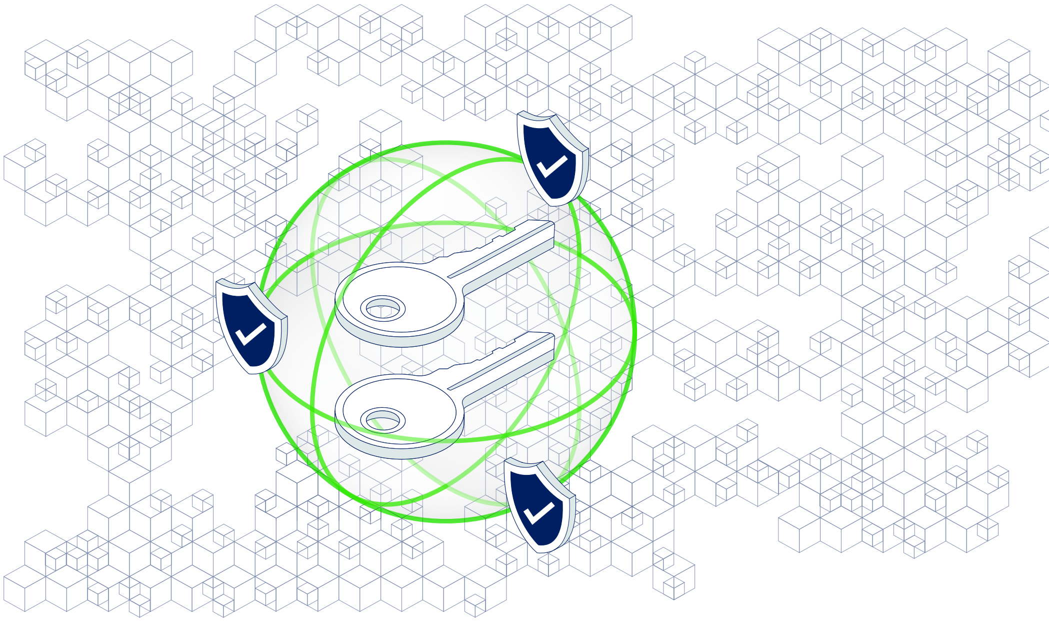
Features

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 and decryption:** Popular algorithms and modes are supported to ensure privacy.
- **Hashing, signing, and verification:** Popular algorithms are supported to ensure integrity and authenticity of payloads.
- **Wrapping and unwrapping:** Wrapping and unwrapping enable delivering protected keys to and from the application without revealing them.
- **Static keys:** Keys that are fixed and not intended to change can be securely embedded into the application at compile time.
- **Dynamic keys:** Secure Key Box can safely work with encrypted keys that are loaded at runtime.
- **Key agreement:** Secure Key Box supports industry standard algorithms for establishing a shared secret with a second party over an unsecure channel.
- **Separation of isolated crypto modules:** Integrate multiple diversified white-box implementations in a single application to ensure separation of cryptographic modules, such as payment card and PIN data processing.
- **Device binding:** Bind keys to a specific hardware device, using its unique information.

Popular cryptographic algorithms

- **Encryption:** AES-128/192/256, DES and 3DES, Speck
- **Decryption:** AES-128/192/256, DES and 3DES, RSA-1024 to 4096, ElGamal Elliptic Curve Cryptography (ECC), Speck
- **Authenticated encryption:** AES-128/192/256 (GCM, CCM)
- **Signing**: AES-CMAC, HMAC, RSA, Elliptic Curve Digital Signature Algorithm (ECDSA), Speck-CMAC, Retail MAC, DSA, and Elliptic curve signing
- **Verification:** AES-CMAC, HMAC, Retail MAC, Speck-CMAC
- **Key wrapping/unwrapping:** Wrapping/unwrapping symmetric keys with 3DES, AES, RSA, and ECC, unwrapping private RSA, ECC, and DSA keys with AES, and more
- **Wrapping plain data:** AES-128/192/256, 3DES
- **Key generation:** DES, 3DES, AES, RSA, DSA, ECC
- **Key agreement:** Classic Diffie-Hellman (DH), Elliptic Curve Diffie- Hellman (ECDH), Montgomery-X-coordinate DH function (X25519)
- **Digests:** MD5, SHA-1/224/256/384/512
- **Key derivation:** A large variety of byte and key manipulation routines allowing to derive new keys from various types of input.
- **Professional services:** Our security experts are ready to create white-box implementation of custom algorithms, and provide assistance with your specific requirements.



Easy implementation that accelerates time-to-market

- **Seamless integration:** Secure Key Box is a simple to integrate plug and play replacement for standard cryptographic libraries.
- **Built-in support for security regulations:** Undergoes regular penetration testing and supports DUKPT key management, TR-31 key blocks, and separation of payment card and PIN data as specified by PCI-DSS.
- **Security expertise:** Deep cryptographic expertise is built-in and continuously improved to stay ahead of changing conditions and customer needs.

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, watchOS, WebAssembly and others.

Comprehensive security solutions

Secure Key Box is one part of Intertrust's suite of application and IoT security solutions.

- **whiteCryption® Code Protection™** makes your software self-defending with enterprise-grade obfuscation and tamper protection.
- **Seacert™** provides rich, cryptographically secure identities for IoT devices with customized X.509 certificates and a robust PKI infrastructure.

Start protecting your applications today. For a free trial of Secure Key Box, visit: intertrust.com/whitecryption-free-trial

intertrust®

**Building trust for
the connected world.**

Learn more at: intertrust.com/whitecryption/secure-key-box
Contact us at: +1 408 616 1600 | information@intertrust.com

Intertrust Technologies Corporation
920 Stewart Drive, Sunnyvale, CA 94085