whiteCryption®

Cryptanium Secure Key Box

An innovative white-box protected cryptographic library designed to protect cryptographic keys in DRM systems, games, firmware, client applications, and other types of sensitive software.

Cryptanium Secure Key Box Benefits:

- Cryptographic keys are always encrypted. Once keys are imported into Secure Key Box (SKB), debugging and reverse engineering will not reveal them in plain form. Algorithms operate directly on encrypted keys.
- Support for industry-standard cryptographic algorithms. SKB supports the most commonly used cryptographic algorithms.
- Implementation design with performance in mind. SKB is customizable and provides separate implementations of cryptographic algorithms for different purposes and target platforms, considering the computational capabilities and memory available on the target devices.
- Cross-platform support. SKB supports a wide range of operating systems and hardware architectures.
- Safe storage of cryptographic keys. SKB ensures that cryptographic keys are exported, imported, and stored in a unique encrypted format to prevent adversaries from reading and altering them.
- Diversified code and data. You can order multiple SKB packages with different binary and data implementations, making it even harder for hackers to develop universal tampering schemes.

Threat to Cryptographic Keys

Cryptographic algorithms and keys are used to protect sensitive data, authenticate communication partners, verify signatures, and implement various other security schemes.

In today's open architectures (smartphones, tablets, and desktops) keys are revealed in the code or memory. The threat of leaks are growing every day. Hackers easily monitor devices with special analysis tools and extract the secret keys. Without efficient key protection, security features are in danger of being broken.

Keep Your Keys Safe

Cryptanium Secure Key Box is a library that uses white-box cryptography techniques to provide effective protection against hackers.

Cryptanium Secure Key Box is a simple C/C++/Java library that implements the whiteCryption SKB API, providing an extensive set of high-level classes and methods for operating with the most popular cryptographic algorithms, such as DES, AES, RSA, ECC, ECDSA, DH, ECDH, and SHA. Cryptanium white-box technology protects the implementation of the library and ensures that secret keys are always encrypted, even during execution.

whiteCryption®

Secure Sensitive Information

Cryptanium Secure Key Box offers top-level protection for secrets on platforms without dedicated chip-based security hardware. Using Cryptanium Secure Key Box reduced implementation costs and guarantees simple integration and deployment within an existing application.

Cryptanium Secure Key Box Features:

- Comprehensive cryptographic library - Cryptanium Secure Key Box is a precompiled library that can simply replace the sensitive algorithms in an original cryptographic module.
- Keys are always encrypted - Once keys are imported into Cryptanium Secure Key Box, debugging and reverse engineering will not reveal keys in plain form. Algorithms operate directly with encrypted keys.
- Robust white-box implementation - The technology behind Cryptanium Secure Key Box is based on a combination of unique mathematical techniques that enable computations with encrypted data.
- Security is inseparable from the program code - Cryptanium Secure Key Box white-box technologies do not rely on superfluous protection code or libraries, which could be circumvented or removed.
- Cost efficiency - The hardware-independent implementation reduces development and maintenance costs.
- Broad DRM support - Cryptanium Secure Key Box can be integrated with any DRM system, including Marlin, DTCP, PlayReady, CPRM, and OMA. No dependency on security chips Cryptanium Secure Key Box is a completely software- based library that can protect secrets on platforms without dedicated chip-based security hardware.
- Diversification - Multiple Cryptanium Secure Key Box packages can be ordered with different binary and data implementations, making it even more difficult for hackers to develop universal tampering schemes.
- Configurability - Features that are not needed can be removed from the Cryptanium Secure Key Box code, greatly reducing the binary size. Safe storage of cryptographic keys Cryptanium Secure Key Box ensures that cryptographic keys are exported, imported, and stored in a unique encrypted format to prevent hackers from reading and altering them.
- Support of static and dynamic keys - Cryptanium Secure Key Box can work with both static keys that are embedded in the code and encrypted dynamic keys that are loaded and decrypted at run time.

Let whiteCryption Secure Your Enterprise

Threats evolve. Stay on top of today's threats and tomorrow's while securely harnessing the latest applications and technologies. **Cryptanium Secure Key Box** is the best solution to provide a higher level of security against the extraction of secret keys.

Development Platforms

Linux, OS X, Windows

Target Platforms

Mobile: Android, iOS, Windows Phone, Windows RT, BlackBerry PlayBook

Supported Languages

C, C++, Java