

## Secure Key Box Overview

### Benefits

- **Proven technology.** whiteCryption SKB has been widely deployed on desktops, tablets, smartphones, game consoles, and embedded devices.
- **Robust protection.** The secure white-box cryptography implementation is designed to be safe in environments where hackers have full access to the execution environment.
- **Faster time-to-market.** whiteCryption SKB is delivered as a complete precompiled library that can be easily integrated into existing software frameworks.
- **Cost efficiency.** The hardware-independent implementation reduces implementation and maintenance costs.
- **Broad DRM support.** whiteCryption SKB can be integrated with any DRM system, including OMA, Marlin, PlayReady, and CPRM.
- **No dependency on security chips.** whiteCryption SKB is a completely software-based library that can protect secrets on platforms without dedicated chip-based security hardware.

**whiteCryption™ Secure Key Box (SKB)** is an innovative white-box protected cryptographic library specifically designed to protect cryptographic keys in DRM/CA systems, firmware, client applications and other security software.

### 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. The weak point of cryptographic algorithms is that in today's open architectures, such as smartphones, tablets, embedded devices, and desktops, the cryptographic keys are usually revealed in the code or memory at some point. Hackers can monitor such devices with special tools and extract the secret cryptographic keys. Without an efficient protection of cryptographic keys, security features are in danger to be broken.

### Ultimate Key Protection Solution

whiteCryption specializes in white-box cryptography techniques, which provide effective protection against hackers who have full access to the execution environment. Based on over 20 years of experience, whiteCryption has developed a robust white-box protected cryptographic library — whiteCryption SKB.

whiteCryption SKB is a simple C/C++ library that provides an extensive set of high-level classes and methods for operating with the most popular cryptographic algorithms, such as AES, RSA, ECC, ECDSA, and SHA. whiteCryption's white-box technology protects the implementation of the library and ensures that the secret keys are always encrypted, even during execution.

### Business Advantages

whiteCryption SKB enables companies to secure their sensitive information and digital content with a proven white-box cryptography technology on multiple operating systems and a broad spectrum of hardware platforms. It fulfills the growing need for solutions that offer top-level protection for secrets on platforms without dedicated chip-based security hardware. Using whiteCryption SKB reduces implementation costs and guarantees simple integration and deployment within an existing application.

## Main Features

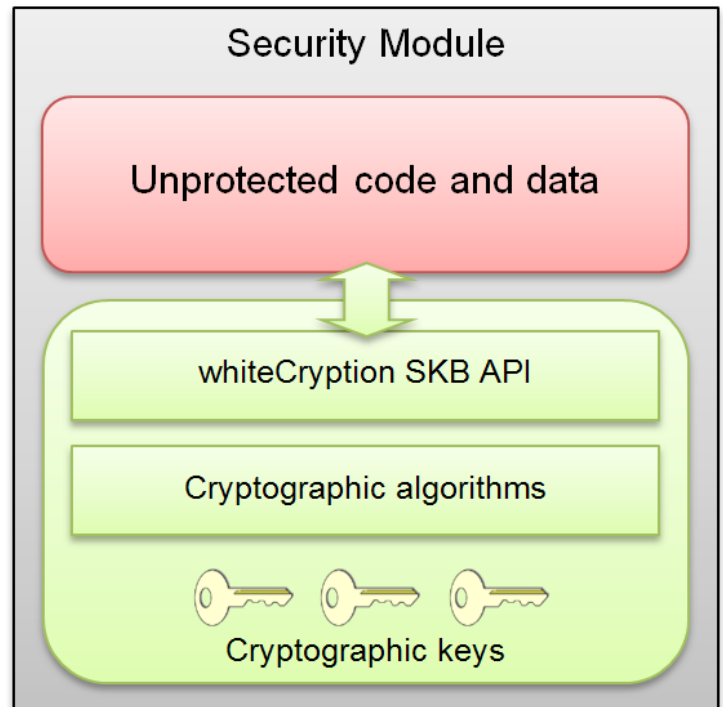
- **Cryptographic keys are always encrypted.** Once keys are imported into whiteCryption SKB, debugging and reverse engineering will not reveal them in plain form. Algorithms operate directly with encrypted keys.
- **Robust white-box cryptography implementation.** The technology behind whiteCryption SKB is based on a combination of unique mathematical techniques that enable computations with encrypted data.
- **Security is inseparable from the program code.** whiteCryption's white-box technologies do not rely on superfluous protection code or libraries, which could be circumvented or removed.
- **Diversified code and data.** By using whiteCryption's Trusted Deployment Service, you can obtain multiple whiteCryption SKB packages with different binary and data implementations, making it even harder to develop a universal tampering scheme.
- **Watermarked program code.** Each whiteCryption SKB package includes a unique watermark. If adversaries try to reuse your application illegally, it is possible to track them down.
- **Safe storage of cryptographic keys.** whiteCryption SKB 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.** whiteCryption SKB can work with both static keys that are embedded in the code and encrypted dynamic keys that are loaded and decrypted at run time.

## Technical Data

Supported Cryptographic Algorithms	
Ciphers	DES, AES, RSA, ElGamal ECC
Signing	AES-CMAC, HMAC-SHA, RSA, RSA-SHA, ECDSA, ECDSA-SHA
Verification	AES-CMAC, HMAC-SHA
Digests	SHA
Key agreement	DH, ECDH
Key generation	DES, AES, and ECC keys

Supported Target Platforms	
Desktop	Windows, GNU/Linux, Mac OS X
Embedded	Android, iOS, MIPS

## System Overview



## About whiteCryption

whiteCryption specializes in white-box cryptography solutions and has over 20 years of experience in software security. It has developed several unique proprietary software protection techniques that have been successfully deployed and used on many systems throughout the world.