

Effective Protection for DRM Systems

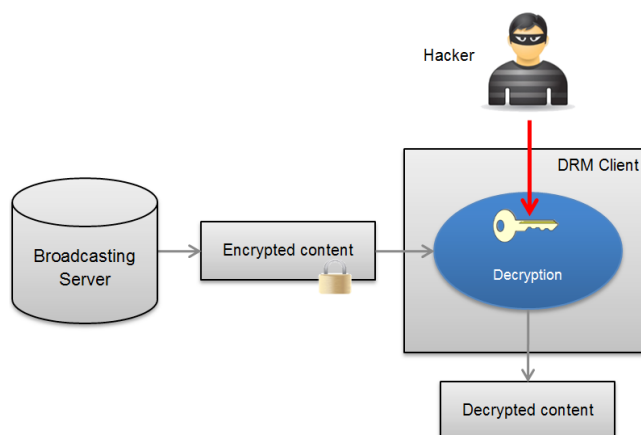
Leading software, hardware, and content industries rely on whiteCryption to protect their DRM keys

Benefits of whiteCryption SKB

- **Protection for industry-standard DRM systems.** whiteCryption SKB protects the cryptographic keys of a number of DRM clients, including PlayReady, Marlin, DTCP, and OMA.
- **Eliminates the dependency on security chips.** whiteCryption SKB is a completely software-based library that can protect secrets on platforms without dedicated chip-based security hardware.
- **Cross-platform support.** whiteCryption SKB protects DRM systems on Windows, Linux, Mac OS X, iOS, Android, and MIPS.
- **Reduces implementation costs and time.** whiteCryption SKB is delivered as a precompiled binary library that can be easily integrated and deployed within existing software frameworks.
- **Supports industry-standard cryptographic algorithms.** whiteCryption SKB supports the most commonly used cryptographic algorithms for encrypting, decrypting, signing, verifying, and digesting data.
- **Secure white-box cryptography implementation.** The secure white-box cryptography implementation is designed to be safe in environments where adversaries have full access to the execution environment.

Threat to Cryptographic Keys

Media broadcasters and software application producers need a secure channel to distribute their digital assets in the emerging markets of mobile devices, tablets, Smart TV, IPTV, and cloud services. DRM is an accepted technology for protecting digital assets and is widely deployed on mobile devices, desktop computers, and set-top boxes. Cryptographic keys used by DRM are very sensitive; if they are exposed, the protection is compromised. The keys can be extracted if a hacker has access to the device where the DRM software is run and if the keys are not sufficiently protected.



whiteCryption Secure Key Box

whiteCryption Secure Key Box (SKB) is a cryptographic library that provides secure and effective white-box implementations of the most commonly used cryptographic algorithms. DRM clients integrated with whiteCryption SKB can be safely deployed in insecure environments, such as on mobile devices, tablets, set-top boxes, and desktop computers.

Business Advantages of whiteCryption SKB

whiteCryption SKB enables companies to secure their sensitive information and digital content with a proven white-box cryptography technology on several 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 software framework.

Features of whiteCryption SKB

- **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 on encrypted keys.
- **Robust white-box cryptography implementation.** The technology behind whiteCryption SKB is based on a combination of unique mathematical techniques that enable performing 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 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 adversaries 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.

whiteCryption SKB 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

whiteCryption Technology

The primary technology behind whiteCryption's white-box cryptography solutions is Multi-Channel Finite Automata Code Transformation (MCFACT). It is a method of protecting secure data and the sensitive areas of the program code by transforming them into composite finite-state automata. Program code that is transformed into such automata is able to compute on encrypted data without the data ever being decrypted.

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.

Contact Information:

whiteCryption Corporation
920 Stewart Drive, suite #100,
Sunnyvale, California 94085, USA

contact@whitecryption.com
www.whitecryption.com