

Zimperium zKeyBox



Secure Your Keys,
Safeguard Your Data



How Zimperium Can Help Secure Keys

Zimperium zKeyBox leverages white-box cryptography to protect the cryptographic keys used within your mobile applications. This solution provides a white box-protected cryptographic library for executing all cryptographic operations within applications while running on a mobile device. The main purpose of zKeyBox is to ensure that cryptographic keys are never revealed in plain text when they are at rest, in motion, or even when in use. With such security in place, it becomes challenging for attackers to locate, modify, and extract cryptographic keys even when the device is under the attacker's control.

Easy to Implement

Step 1:

Get the zKeyBox package, which includes a library and tools.

Step 2:

Transform your plain keys into protected keys using the tools.

Step 3:

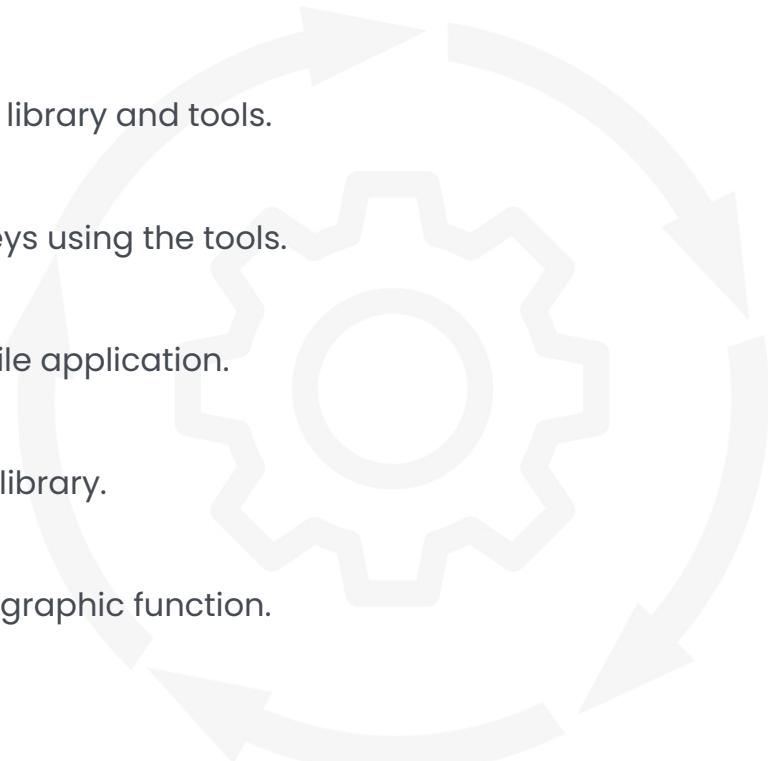
Integrate the zKeyBox library into your mobile application.

Step 4:

Import the protected keys into the zKeyBox library.

Step 5:

Call the zKeyBox library to perform a cryptographic function.



The average cost of a data breach rose to **\$4.24 million** in 2021 globally based on the 2021 IBM Data Breach Report. And these don't even take into account mega breaches where that cost jumps exponentially to **\$401 million**.

Key Benefits

Embed Protected Cryptographic Keys With Confidence: Once keys are protected by white-box cryptography, they can be embedded within your application code and used in open and insecure environments without exposing them at-rest, in-use, and in-memory.

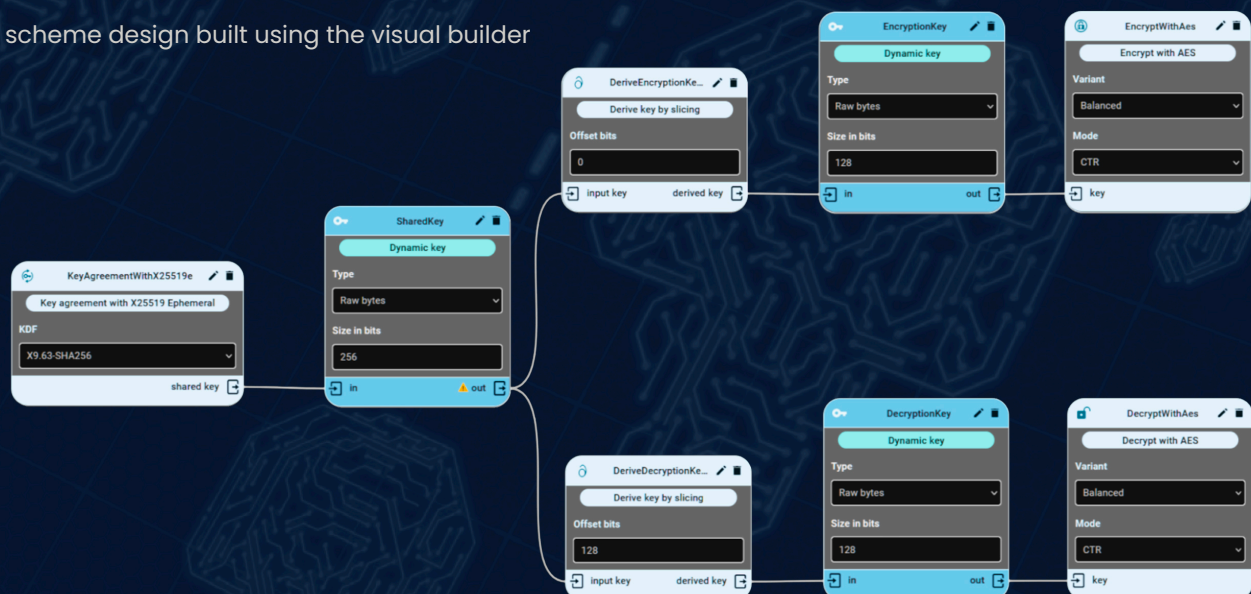
Enhanced Security in Untrusted Environments: White-box cryptography is designed to secure cryptographic keys in environments where attackers can access, view, or alter the application and its runtime memory. It protects keys even if the device is compromised, making it ideal for mobile applications that may run on insecure or compromised devices.

Platform-Independent: White-box cryptography offers robust protection without relying on hardware-based security mechanisms, such as Secure Enclave, Android Keystore, TPM modules, or other Trusted Execution Environments (TEEs). This ensures consistent and reliable security across various platforms and support for more algorithms than cryptographic hardware on mobile devices support. Furthermore, it eliminates the need for developers to implement different code bases for each platform and version.

Same Level of Security Across All Platforms: Ensures the same level of security on mobile and non-mobile platforms regardless of the OS version.

Empowers Security Architects: Our intuitive visual builder enables the creation of a customized white-box cryptography library that implements a cryptographic scheme that fits your use case with ease and precision. A graphical user interface makes it easy to design and visualize a scheme and define key usage rights to mitigate API misuse. Precision is delivered via the ability to provide algorithm parameters (block chaining mode, key sizes, padding schemes, etc) at build time, simplifying implementation.

Image: A scheme design built using the visual builder



Why Zimperium zKeyBox



Support Many Standard & Custom Algorithms

Protect any cryptographic scheme using algorithms such as AES, 3DES, RSA, ECC, HMAC, etc. Custom algorithm support is also available.



Comprehensive Platform Support

Linux (glibc, uClibc, musl), Windows, macOS, Android, iOS, tvOS, watchOS, Xbox, PlayStation, WebAssembly, and others.



Security Architecture Guidance

We provide guidance on the best security architecture and requirements to ensure optimal implementation for your specific needs.



Prevent Incorrect Schema Design

Visual builder guides the user by providing precise warnings and errors for invalid or suboptimal conditions, like when the key sizes don't match the chosen algorithm.



FIPS 140-3 Certification

Cryptographic modules developed by this solution meet the stringent requirements of FIPS 140-3 Level 1.



Built-In Support for Security Regulations

zKeyBox undergoes regular penetration testing, supports DUKPT key management, TR-31 key blocks, standards compliant random generation with reseeding capability and other features that help obtain various certifications for the protected application and separation of payment card and PIN data as specified by PCI-DSS.



Easy Integration

Plug-and-play replacement for standard cryptographic libraries. Easy to use APIs as there are no excessive parameters to specify.

PROTECT YOUR KEYS TODAY

We can ensure the security of your most sensitive data regardless of the hardware your mobile application runs on. [Contact us](#) for more information.

Customer Use Cases

Contactless Payments on Mobile Phones

Mobile phones are increasingly used as contactless payment terminals. Developing payment software for general-purpose phones is significantly cheaper and more convenient than creating specialized hardware for traditional point-of-sale systems. The danger lies in that software-based security systems are easier to reverse engineer than special-purpose hardware. By extracting the internal cryptographic keys, an adversary can collect sensitive data, steal money, or disrupt business operations. The industry-standard approach to mitigating key extraction risks on general-purpose devices is white-box cryptography. In fact, the Payment Card Industry Security Standards Council (PCI SSC) requires all vendors to employ white-box cryptography for mobile contactless payment applications to protect keys. zKeyBox is a white-box cryptography library, which means that by using it in a software-based payment system you are able to satisfy the PCI SSC security and testing requirements and ensure strong security.

Secure Keys to Reduce Content Piracy

Streaming providers leverage multiple crypto key algorithms in a layered fashion to encrypt the content and entitlements of the subscribers. They rely on secure chip hardware to store the content decryption keys within the set-top box. However, most providers use set-top-box (STB) hardware from several manufacturers who don't always support the encryption of their choice, making the content vulnerable to piracy. Customers are leveraging zKeyBox to protect content on set-top boxes with incompatible hardware in the short term. But in the long run, they plan to completely untether themselves from hardware-based security to save high refresh costs and reduce the risk of piracy.

Securing Keys for Cloud Applications

Customers migrate enterprise applications that were traditionally on-premise to the cloud. But, they do not trust cloud providers with their cloud data encryption keys due to the extent of provider access, limiting encryption options, and lack of control over the key management lifecycle. They are choosing to keep the key generation and management on-premise but leverage zKeyBox's white-box cryptography to secure all cryptographic activities carried out by the application.

Global digital piracy costs US film and TV industry at least an estimated

\$29.2 Billion

and as much as \$71 billion annually, according to a new study from the US Chamber of Commerce's Global Innovation Policy Center.

Organizations with a high level of cloud migration had an average cost of a breach of

\$5.12 Million

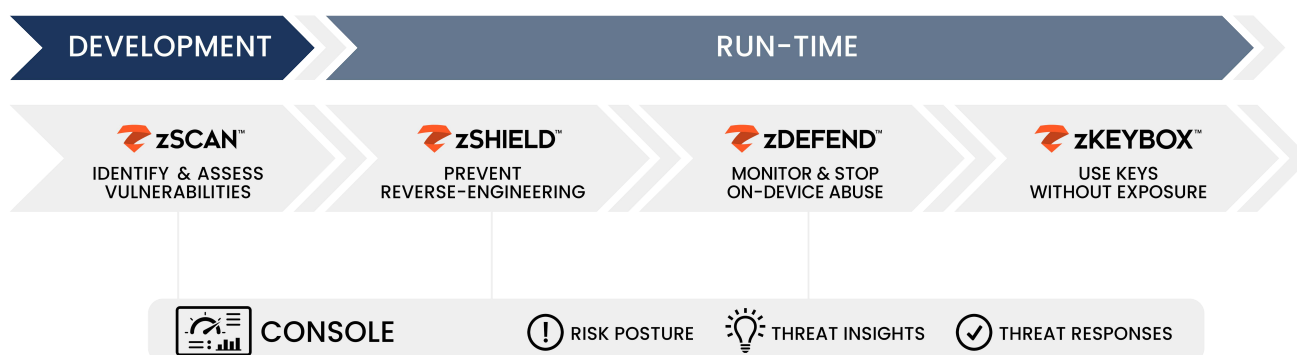
compared to \$3.46 million for organizations with low levels of cloud migration, for a difference of \$1.66 million or

38.7%.

Why Zimperium MAPS

Zimperium's Mobile Application Protection Suite (MAPS) helps enterprises build safe and secure mobile apps resistant to attacks. It is the only unified solution that combines comprehensive app protection with centralized threat visibility.

MAPS comprises four capabilities, each of which address a specific enterprise need as shown below.



Solutions	Value Proposition
zSCAN™	Helps organizations continuously discover and fix compliance, privacy, and security issues prior to being published.
zSHIELD™	Protects the source code, intellectual property (IP), and data from potential attacks like reverse engineering and code tampering.
zDEFEND™	Provides threat visibility and on-device ML-based run-time protection against device, network, phishing, and malware attacks.
zKEYBOX™	Protect your keys so they cannot be discovered, extracted, or manipulated.