ZIMPERIUM®
ADVANCED MOBILE SECURITY

zKEYBOX™

Solution Brief

Building safe and secure apps

Today, mobile applications are an effective digital channel for worker productivity and business growth, but they also introduce unprecedented risk. Organizations developing and using mobile apps are keenly aware of security risks as mobile apps access and process more sensitive information than ever before. The biggest hurdle for enterprises today is having to work with a highly fragmented set of point products that provide limited-to-no visibility into real-world risks, threats, and attacks.

Zimperium's Mobile Application Protection Suite (MAPS) is the only unified solution that combines comprehensive in-app protection with centralized threat visibility.

zKeyBox: Advanced security for your keys and secrets

Mobile applications use keys to encrypt outgoing and decrypt incoming communications as they contain sensitive data. Even the strongest encryption methods fail when the cryptographic keys are compromised. Hackers can easily find and steal exposed keys in code or memory. Zimperium zKeyBox leverages white-box cryptography to protect keys and secrets within your mobile app. It transforms and obscures 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.

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. No dependency on any hardware-based mechanisms provided by the platforms. (Ex. Keystores, Secure Enclave, Trusted Execution Environment (TEE) on Android)

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 is 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
Zimperium's deep cryptographic expertise guides every step of your deployment. zKeyBox protects keys in millions of installed apps and undergoes regular independent security testing.

Easy implementation that accelerates time-to-market

- **Seamless integration**: zKeyBox 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.
- **No dedicated security hardware:** No TPM, TEE, SE, SIM or HSM devices are required.
- **Wide Platforms Support:** Linux (glibc, uClibc, musl), Windows, macOS, Android, iOS, tvOS, watchOS, WebAssembly and others.

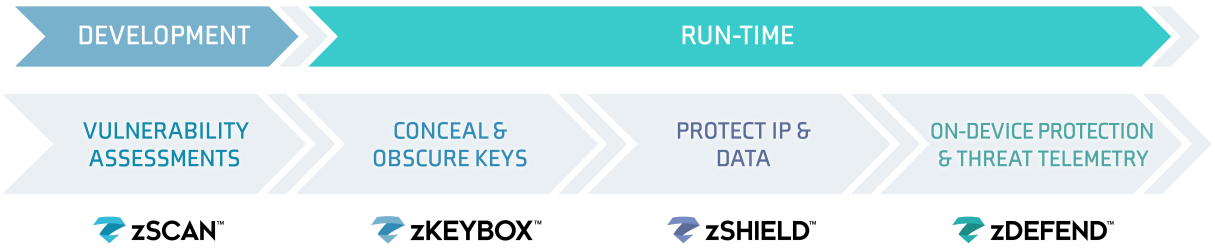
Protect your keys today

If you are interested in more advanced security for your cryptographic keys, please contact us.

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 is comprised of four capabilities, each of which address a specific enterprise need as shown below.



Solution	Value Proposition
zSCAN™	Helps organizations continuously discover and fix compliance, privacy, and security issues prior to being published
zKEYBOX™	Protects your keys so they cannot be discovered, extracted, or manipulated
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

ZIMPERIUM®