Protecting Keys For Secure Passwordless Authentication

For businesses, there are many benefits to secure passwordless authentication. It reduces the risk of attack and saves admins time and resources, as they would no longer have to deal with password resets and maintenance. But most industry solutions are vulnerable to malware and SIM-swap scams.

ToothPic helps businesses protect their digital assets by embracing a more secure passwordless authentication mechanism for their mobile and web applications. The enhanced security is achieved by turning every end user's smartphone into a verification key to support secure passwordless authentication.

All this is made possible via ToothPic's Key Protection SDK. It provides a simple API for mobile apps to generate cryptographic asymmetric key pairs and perform cryptographic operations with the private key, e.g., computing digital signatures. The ToothPic solution differs from competing approaches because private keys generated by ToothPic Key Protection SDK are bound to the unique hardware characteristics of the smartphone camera sensor.

However, ToothPic recognized that securely storing keys was insufficient to achieve maximum security. Their primary concern was that keys are constantly in transit and stored in memory during cryptographic operations. And smartphone's memory can be subject to attacks using malicious software that can read and exfiltrate cryptographic data. As a countermeasure, Zimperium's white-box cryptography library was embedded into the SDK to secure keys from exposure and exfiltration. Whenever cryptographic operations requiring the protected key are needed, they run within a secure execution environment provided by the Zimperium solution. Compared to alternative hardware-based solutions, Zimperium zKeyBox solution was readily available on all mobile, web, and desktop platforms, guaranteeing maximum flexibility and best-in-class security with a wide range of possible hardware, firmware, and operating systems.

Today, ToothPic's SDK is used in digital banking, digital signature, crypto exchange, crypto wallet, and many more applications, making them immune from malware and SIM-swap scams.

"ToothPic's mission is to help companies to enhance the security of their digital services through our unique technology. We were looking for a technological partner who shared our same goal and Zimperium turned out to be the perfect one to collaborate with. The integration of Zimperium's zKeyBox in our Key Protection SDK has strengthened the robustness of our technology. Together we brought the security to the next level, offering on the market a solution never seen before."

-Giulio Coluccia, CEO & Co-Founder of ToothPic