Secure Local Storage (SLS) by YESsafe AppProtect+

YESsafe AppProtect+

How do you store your app data?

Mobile devices are increasingly used for security-sensitive activities such as online banking or mobile payments. This usually involves cryptographic operations, and may introduce challenges related to securely storing data on the device. At the same time, attacks and exploits on mobile devices continue to mature in sophistication.

What are your options?

Store data unencrypted: You can store data unencrypted, but it's not advisable for sensitive data.

Roll your own: You could «roll your own» by storing crypto keys in plain text in your application code. However, using plain text means there is limited protection to a user's run-time data.

Whitebox crypto solution: You could implement a stand-alone whitebox crypto solution. This is however complex, time-consuming and costly. A whitebox solution is comparable to building a safe deposit box from scratch. Why not buy one in-store?

Hardware backed storage: You could choose hardware backed storage. Not all devices have the necessary hardware components to support this. Secondly, if your app or the end-user device is compromised (rooted/jailbroken), sensitive data could potentially leak.

Secure Local Storage (SLS) by YESsafe AppProtect+: A state-of-the-art security feature that provides the ability to store app secrets locally on the end-user device in a secure manner. Compared to other solutions, SLS by YESsafe AppProtect+ is unparalleled in terms of simplicity and user-friendliness, while ensuring the security of your data.

Secure local storage made easy

All data stored using Secure Local Storage (SLS) by YESsafe AppProtect+ will be encrypted according to the latest standards and recommendations protected by YESsafe AppProtect+'s proven security technology.

The feature does not rely on device functionality (such as keychains) to provide secure storage of sensitive data and is fully self-contained.

The encryption keys used are never stored on the device, or added in the static code of the app, but are dynamically generated on the device protected by YESsafe's whitebox backed solution. This further ensures that the data is device-bound, and cannot be copied to a different device.

Key benefits using SLS by YESsafe AppProtect+

Easy to integrate: Reference code and well-defined APIs are provided.

No crypto knowledge required: As an app provider, you don't have to deal with crypto complexities. This is time-consuming and often cumbersome.

State-of-the-art RASP: The feature uses YESsafe AppProtect+ to protect app secrets when used in an unencrypted state.

Cross-platform: SLS by YESsafe AppProtect+ is offered as an extension on Android, iOS and Windows.

Use case examples

Tokens

Session tokens or persistent tokens can be securely stored, and removed by the app, and app publishers can be ensured that tokens can not be cloned onto other devices.

Sensitive data

Apps storing personal information about the user on the device can with this feature ensure that data is stored securely, even if the device integrity is broken (e.g. rooted/jailbroken).

API Keys

The increased use of private or semi-private API access between device and server has shown the importance of protecting one's API keys. SLS by YESsafe AppProtect+ enables trust in that these keys are not only protected but can also ensure that they cannot be cloned.

YESsafe AppProtect+ provides vulnerability scanning service for apps, to detect security weaknesses such as hardcoded sensitive information that uses unsecured HTTP links. YESsafe AppProtect+ will also detect and protect mobile apps from a variety of threats, such as reverse-engineering, tampering, code-injection and more. In an unsecured OS environment, apps that have been integrated with YESsafe AppProtect+ will now have rooted and jailbreak detection mechanisms that allows the app to operate securely without compromising the app's integrity and confidentiality.

These AppProtect+ shielded apps can even function securely in the absence of an internet connection or without an updated virus database. On top of that, AppProtect+ also protects mobile apps against static and dynamic attacks (e.g. repackaging, source code modification), and respond by taking necessary measures when real-time attacks are detected. AppProtect+ has a build-in audit mechanism that allows auditor to easily review all apps shielding statistics, whilst the attack insight dashboard identifies and provides the user with alerts and critical information that their apps are facing in real time.

Moreover, AppProtect+ is EMVCo SBMP certified. An EMVCo certified app solution ensures that mobile apps can withstand real-time threats and attacks.

i-Sprint
Trust without Boundaries