ELS -Encrypted Local Storage

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.

How do you store your app data?

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 runtime 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.

Encrypted Local Storage (ELS) by Trustsec: 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, ELS by Trustsec is unparalleled in terms of simplicity and user-friendliness, while ensuring the security of your data.

+48784784 504
info@trustsec.net
www.trustsec.net

Encrypted Local Storage

All data stored using ELS by Trustsec will be encrypted according to the latest standards and recommendations protected by The Guardian (Trustsec Mobile Apps Protection solution) 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 Trustsec's Whitebox backed solution. This further ensures that the data is device-bound, and cannot be copied to a different device.

Key Benefits

Easy to integrate

One of the most benefits of Trustsec Encrypted local storage solution is the reference code and well-defined APIs are provided.

No crypto knowledge required

Encrypted Local storage supports app providers as it deals with crypto complexities that considered time-consuming and often cumbersome to the app providers.

RASP latest technology

Trustsec Encrypted Local storage is based on Trustsec solution for mobile application protection "The Guardian" to protect app secrets when used in an unencrypted state.

Cross-platform

Encrypted Local storage is an extension on Android, iOS and Windows.

+48784784 504
info@trustsec.net
www.trustsec.net