EmSPARK Suite

CoreLockr Libraries User Guide

EDES-0002-Rev D

Errata

Published: August 9, 2022

Section: 3.1.2. Opaque Key Example

Point **a.** reads:

> **a.** Create Opaque Key package
>
> Opaque Key packages are DER-encoded structures containing key information (key type, key name in the persistent store, and key data). The key information is encrypted inside the package, so none of the information is accessible until it is decrypted first. The MAC tag for the unencrypted information is also added to the package for verifying that the decryption on the device was successful. The encrypted key information, MAC tag, and the remaining information required for decryption are hashed and signed to ensure the integrity and verify the source of the package.

Corrected text:

> **a.** Create Opaque Key package
>
> Opaque Key packages are DER-encoded structures containing key information (key type, key name in the persistent store, and key data). The key information is encrypted inside the package, so no key information is accessible until decrypted. The MAC tag for the encrypted information is also added to the package. The encrypted key information, MAC tag, and the remaining information required for decryption are hashed and signed to ensure the integrity and verify the source of the package.