Sensitive Data Protection (SDP)

Samsung Knox can enforce two classes of protection for data generated from within Knox Workspace: protected data and sensitive data. All data generated from within Knox Workspace is considered to be protected. Protected data residing in storage is always encrypted, and is thus protected against offline attacks, such as forensic analysis on a flash memory image extracted from a stolen device. Furthermore, access controls are used to prevent applications outside Knox workspace from attempting to access protected data. The decryption key for protected data is stored encrypted by the device-unique hardware key (DUHK). Therefore, the key is only recoverable on the same device.

Sensitive data, on the other hand, provides an even stronger security guarantee. Like protected data, sensitive data is always encrypted when on disk. Additionally, the data remains encrypted as long as Knox Workspace is locked. The key used to encrypt sensitive data on disk is recoverable only if the user enters the Workspace password, PIN, or pattern. Thus, if a device is stolen, the key cannot be extracted from anywhere on the device. As with protected data, the stored key material is encrypted by the DUHK, thus binding it to the device.

Enforcement of this guarantee for sensitive data is performed by Knox Sensitive Data Protection (SDP). SDP creates a Container Master Key (CMK) that can only be decrypted with user input. If desired, the Mobile Device Management (MDM) can also be used to unlock the CMK, thus preventing total data loss in the event of a forgotten Workspace password. Once Workspace is locked, SDP clears all keys in memory after a configurable timeout (five seconds by default). In addition, SDP also flushes sensitive file data from the operating system (OS) kernel's disk caches if the file is not in use by a Workspace application.

Any sensitive data received when Workspace is locked is still protected by SDP. This works by using a public key algorithm in which the private part of the key is maintained in an encrypted partition, and the public part is used to encrypt the new sensitive data. Once Workspace is unlocked, the data is decrypted with the private key, and re-encrypted using the usual symmetric key, which is guarded by the CMK. Currently, email subjects, bodies and attachments are marked sensitive. Additionally, the SDP Chamber provides a directory, in which all files are automatically marked as sensitive, and protected by SDP.