



**XIII
JORNADAS
STIC
CCN-CERT**



DualDAR encryption for Samsung Knox Workspace

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT





José Mª Arroyo

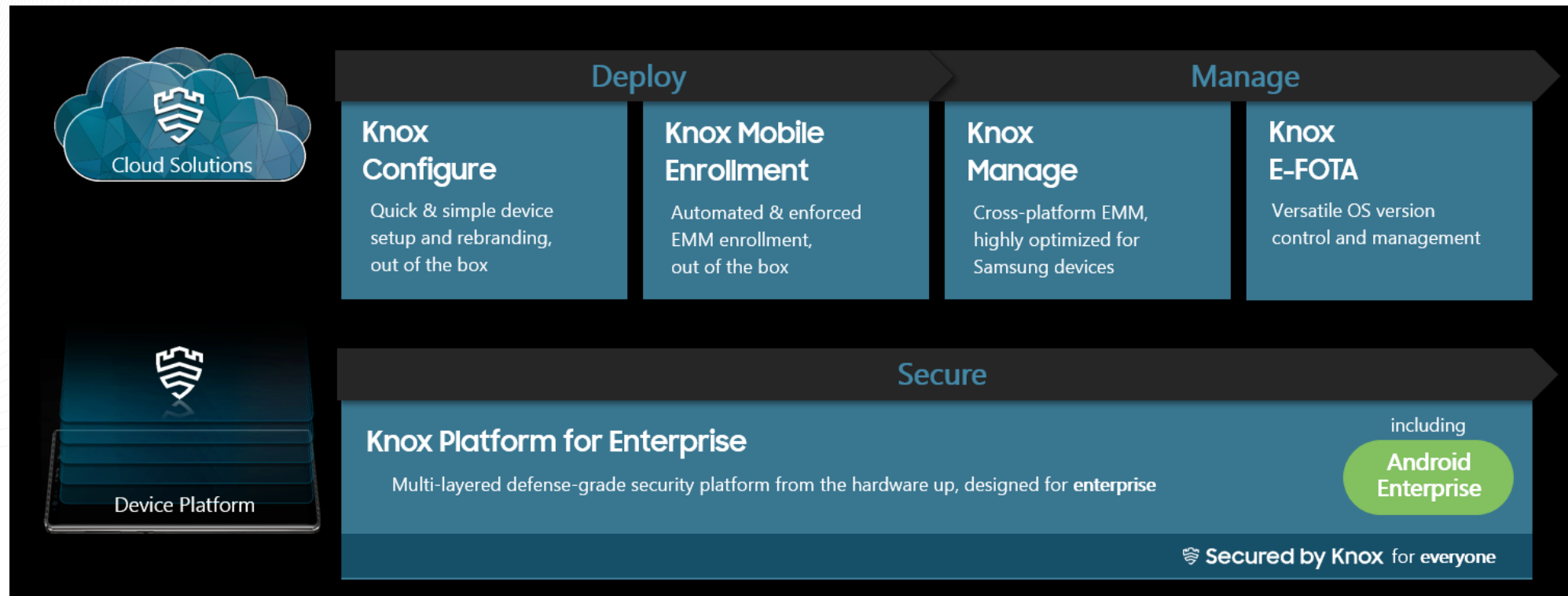
Samsung Electronics Co., Ltd.

Índice

- 1. Samsung Knox overview**
- 2. Data-At-Rest Protection**
- 3. What is DualDAR and why is it beneficial?**
- 4. Knox DualDAR features and architecture**
- 5. Deployment of a DualDAR Workspace**

Samsung Knox overview

What is Knox?



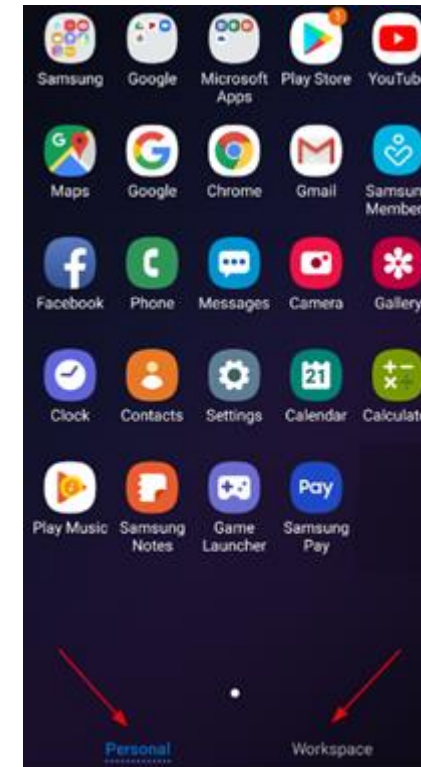
Samsung Knox is a leading mobile security solution that provides a secure environment for corporate data and apps for all Galaxy devices

Samsung Knox overview

What is a Workspace?



Security Layers



Knox Workspace



- **Knox Platform for Enterprise** is a defense-grade mobile solution for IT admins to manage and secure Samsung Android phones and tablets
- **Workspace** is a dual persona container product designed to separate and isolate work data on mobile devices

Samsung Knox overview

Use case deployments

COBO

Fully Managed Device
(Device Owner)



COPE

Fully Managed with Knox
Workspace



BYOD

Knox Workspace
(Profile Owner)



Scenarios

Data-At-Rest Protection

What is DAR?

- Storage security is the process of allowing only authorized parties to access and use stored information.
- Confidentiality of Data is achieved by encryption
- Data remains encrypted while the device is powered off



NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-111

Guide to Storage Encryption Technologies for End User Devices

- Physical exposure threat

Is when another person picks up your phone and transfers all the stored data to another device. Samsung devices encrypt all data they store preventing anyone who does not have the right keys from accessing your information.

Data-At-Rest Protection

Requirements



On Device Encryption

Full-disk / File-based

- Data remains encrypted while device is powered off
- Decrypted if device is unlocked after booting
- Recoverable only on the same device
- Common Criteria Data-at-Rest requirements

Protection Profile for Mobile Device Fundamentals



Version: 3.1

2017-06-16

National Information Assurance Partnership

FDP_DAR_EXT.1 Extended: Protected Data Encryption

FDP_DAR_EXT.2 Extended: Sensitive Data Encryption

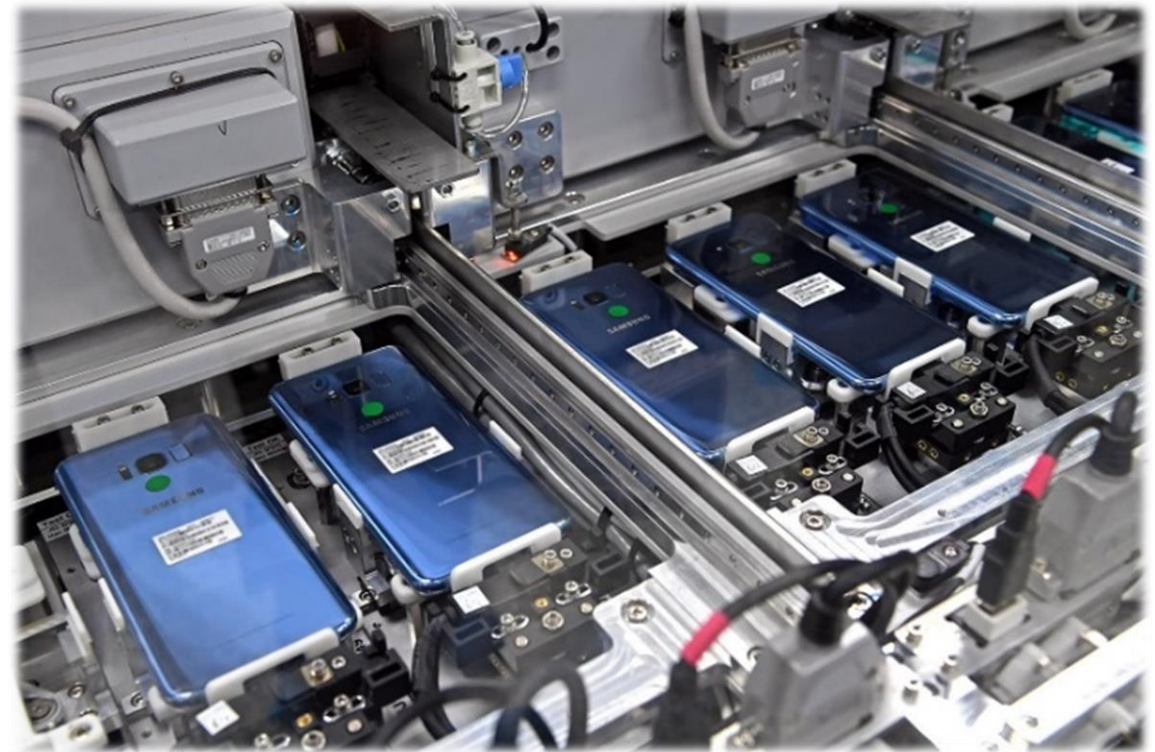
FCS_CKM.1 Cryptographic key generation

Example DAR requirements

Data-At-Rest Protection

From the Hardware and up

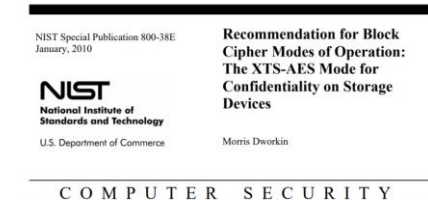
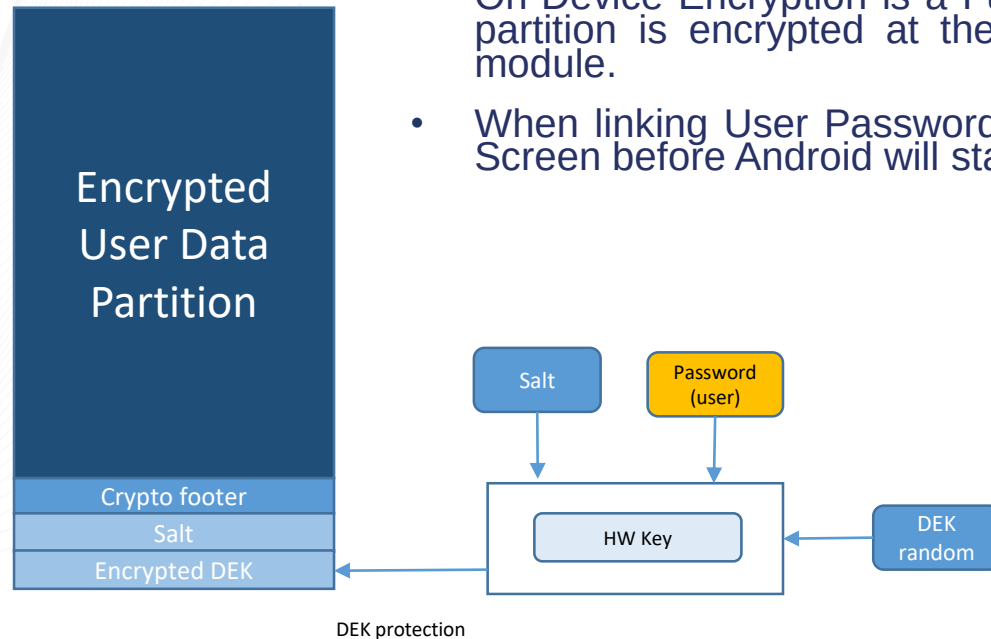
- Hardware-backed security
 - REK (Root Encryption Key) Hardware fused
 - Trusted Execution Environment (TEE)
 - SPU (Security Processing Unit) SoC sub-system
- Hardware operation
 - Certified Flash Memory Protection
- User Password binding



Data-At-Rest Protection

Implementation: Full-Disk Encryption

- On-Device Encryption is a Full-Disk Encryption solution for Android devices where the user data partition is encrypted at the block level. This is implemented with the dm-crypt Linux kernel module.
- When linking User Password to the key protection, the user must authenticate to the Boot Lock Screen before Android will start.



The 512-bit value is decrypted and passed to DM-Crypt/FMP, where half is used for the DEK and half as the XTS tweak key

```

00 00 00 0F 00 00 00 11 00 00 00 00 3C 00 0E 00 04 00 4A 00 10 00 4E 00 40 00 5E 00 10 00  | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
9E 00 10 00 AE 00 10 00 BE 00 04 00 CE 00 10 00 D2 00 40 00 E2 00 10 00 22 01 10 00 32 01 10 00  | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
42 01 10 00 52 01 10 00 62 01 00 00 01 01 E9 A4 5A 18 85 D8 2A 87 1A 04 1A 09 A4 FE E0 58 C2 DB  | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
33 79 66 60 CD 07 23 29 6D 3A B6 AD E1 FE A8 FC 1A D2 34 81 83 A8 C5 E7 94 81 3F D6 8F E8 FC 97  | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
E1 29 ED D8 CD 6E 42 8C D1 47 ED 7C 69 C6 6A 43 84 D1 E5 3E FD 77 A9 0A B8 1F 94 ED 3A C5 FC 28  | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
36 CB 87 8B 0E C4 5B 10 0E 36 BD E5 E2 16 49 3A 56 50 E9 D2 C8 AD 95 F1 B6 CF 36 0C EA 0D 3F 45  | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
AA 4D A9 75 E5 42 A6 D8 04 5B FB BA 15 EE 00 00 02 01 CE CB 2D 89 BC 27 7D 1E 40 8D AD 0D 1E BA  | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
45 F5 FD 50 AF 3F 41 13 CC 21 11 0E 2F D5 E2 47 1A CB 28 37 1A 77 FE BC 62 54 C9 EE 43 39 8E 68  | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
7B 75 0A A1 B9 62 3D 3F 01 91 01 AC AD 5F 03 6B 2B 9D BD 4B 50 72 29 6C 5E 0A 67 99 39 A1 86 58  | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
A3 1B 88 91 E0 E7 A0 80 03 E6 E9 C3 9C 1C C9 61 D8 63 1E 9A CB 7C E4 DD A2 B2 DB DB A5 F6 F6 72  | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
AD 65 5C E5 7C 4D 89 0B 8A C6 28 E1 9E 0C EF 1D 06 41 02 00 02 33 D9 48 4F D5 12 E6 10 BC F0 0C  | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
50 28 02 00 02 33 D9 48 4F D5 12 E6 10 BC F0 0C 50 28 00 00 00 00 00 00 00 00 00 00 00 00 00  | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

Crypto footer including ODE DEK protected

01	ODE info footer start
CE...F5	Salt
FD...1B	ODE DEK protected

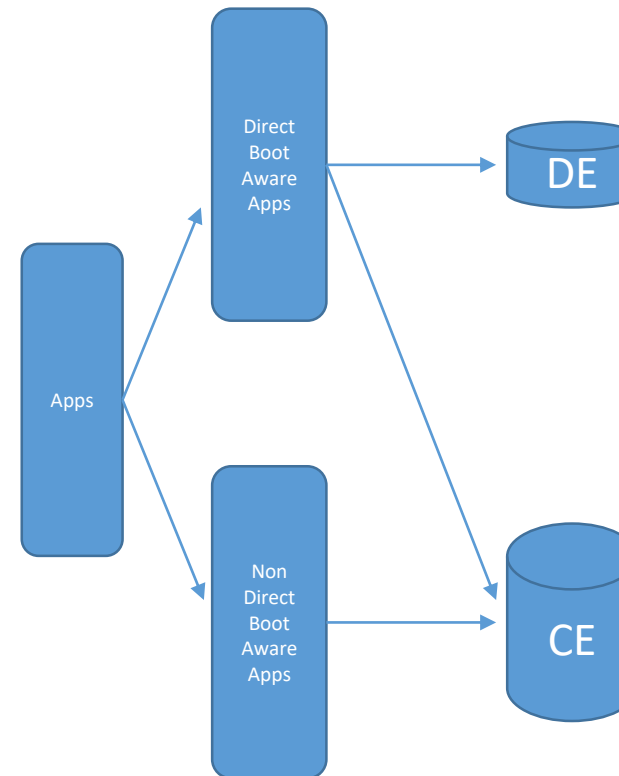
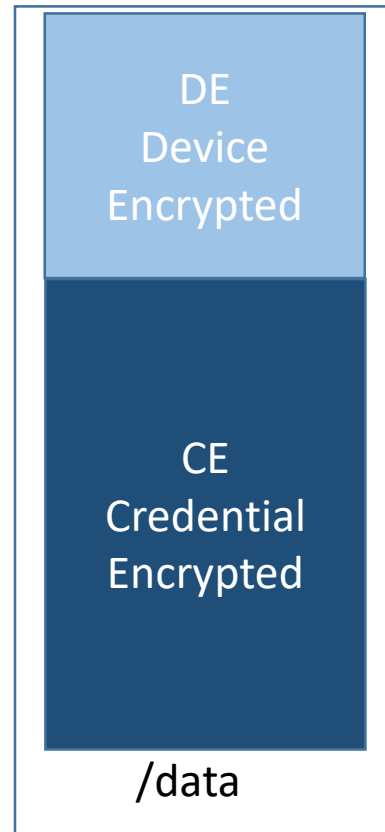
Data-At-Rest Protection

Implementation: File-Based Encryption

- File-Based Encryption is a per-file encryption solution for Android devices where each file is encrypted with a unique key
- To leverage this per-file encryption, several storage areas are created on the device, each area using different area Keys: DE and CE
- The **Device Encrypted** files' unique file key will be derived from a DE MasterKey and the UserPassword is not involved in the process. The **Credential Encrypted** files' unique file key will be derived from a CE MasterKey and the UserPassword **IS** involved in the process.

Data-At-Rest Protection

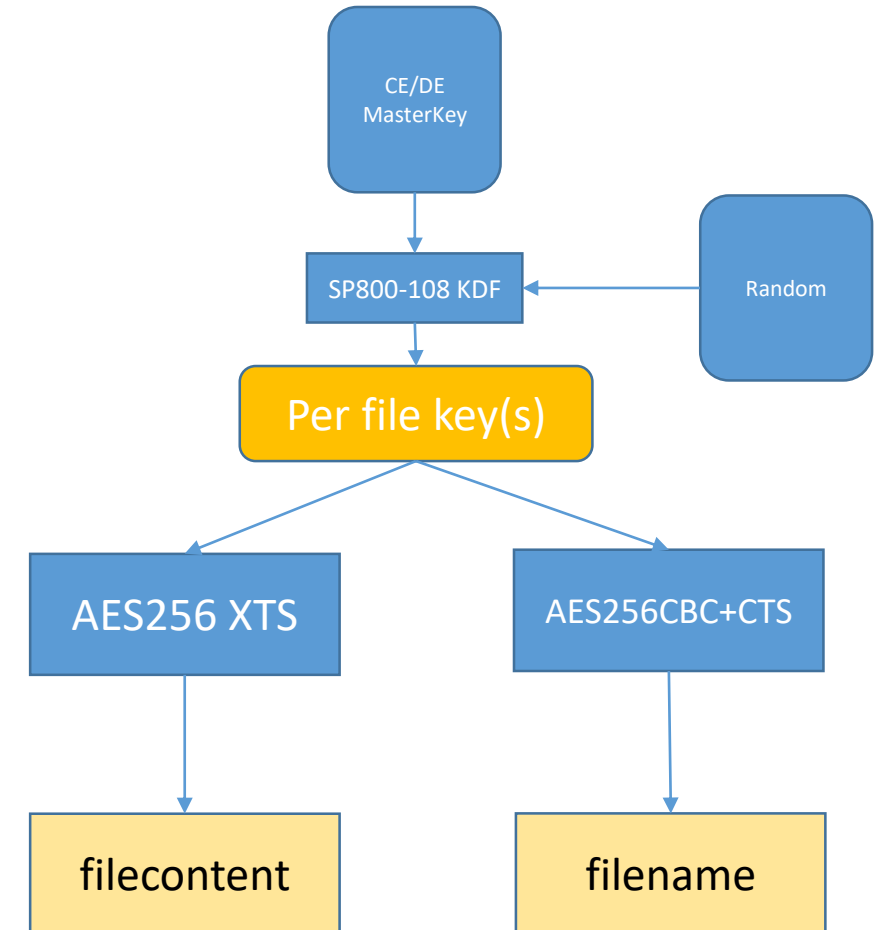
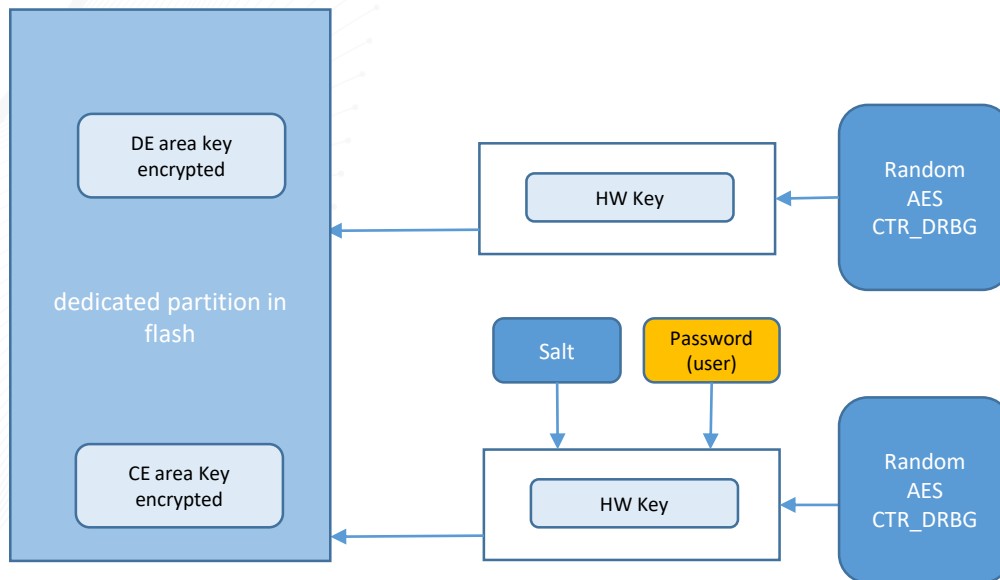
Implementation: File-Based Encryption



- With DE and CE encrypted storage areas there is no user interaction needed after reboot to run some apps
- Direct Boot allows apps to operate within a limited context before the device is unlocked

Data-At-Rest Protection

Implementation: File-Based Encryption



FBE overview

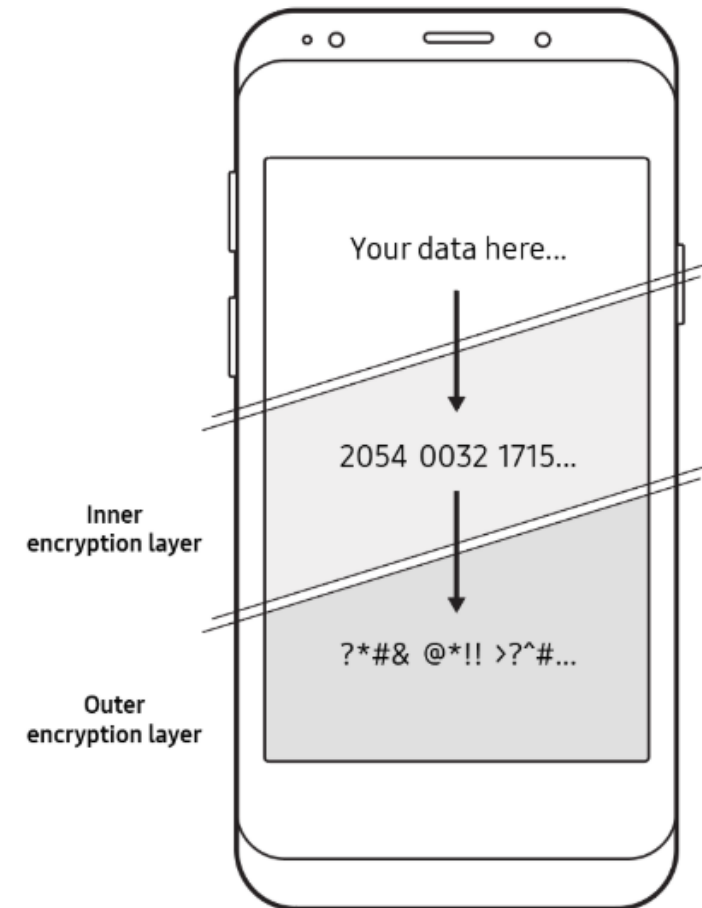
What is DualDAR and why is it beneficial?

Concept

- Knox DualDAR is a DAR protection solution providing redundancy and 3rd party integration of data encryption software.
- Knox DualDAR extends the built-in Android File Based Encryption (FBE) framework, protecting classified data using two layers of encryption.

- DATA AT REST CAPABILITY PACKAGE

The use of multiple layers, implemented with components meeting the CSfC* vendor diversity requirements, reduces the likelihood that a single vulnerability can be exploited to reveal protected information.



* Commercial Solutions for Classified Program of National Security Agency (NSA)

What is DualDAR and why is it beneficial?

DualDAR Requirements



DATA AT REST CAPABILITY PACKAGE of National Security Agency

- Capability Packages of the CSfC Program provide how to implement secure solutions using COTS* products
- DAR CP mitigates the risk to data from unauthenticated access when the device is powered-off or unauthenticated

* Commercial Off-the-Shelf

What is DualDAR and why is it beneficial?

Data types and device state

RED, GRAY, and BLACK

- Red data is unencrypted classified data being processed by the EUD*. After a user successfully authenticates to the outer and inner layers of DAR encryption.
- Gray data contains classified information that has been encrypted once.
- Black data contains classified information that has been encrypted twice. An EUD* is considered black when the device is powered-off and/or unauthenticated and the stored data has been encrypted with both the outer and inner layers of DAR encryption.



**Data at Rest
Capability Package**



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



* End User Device

What is DualDAR and why is it beneficial?

Samsung DualDAR

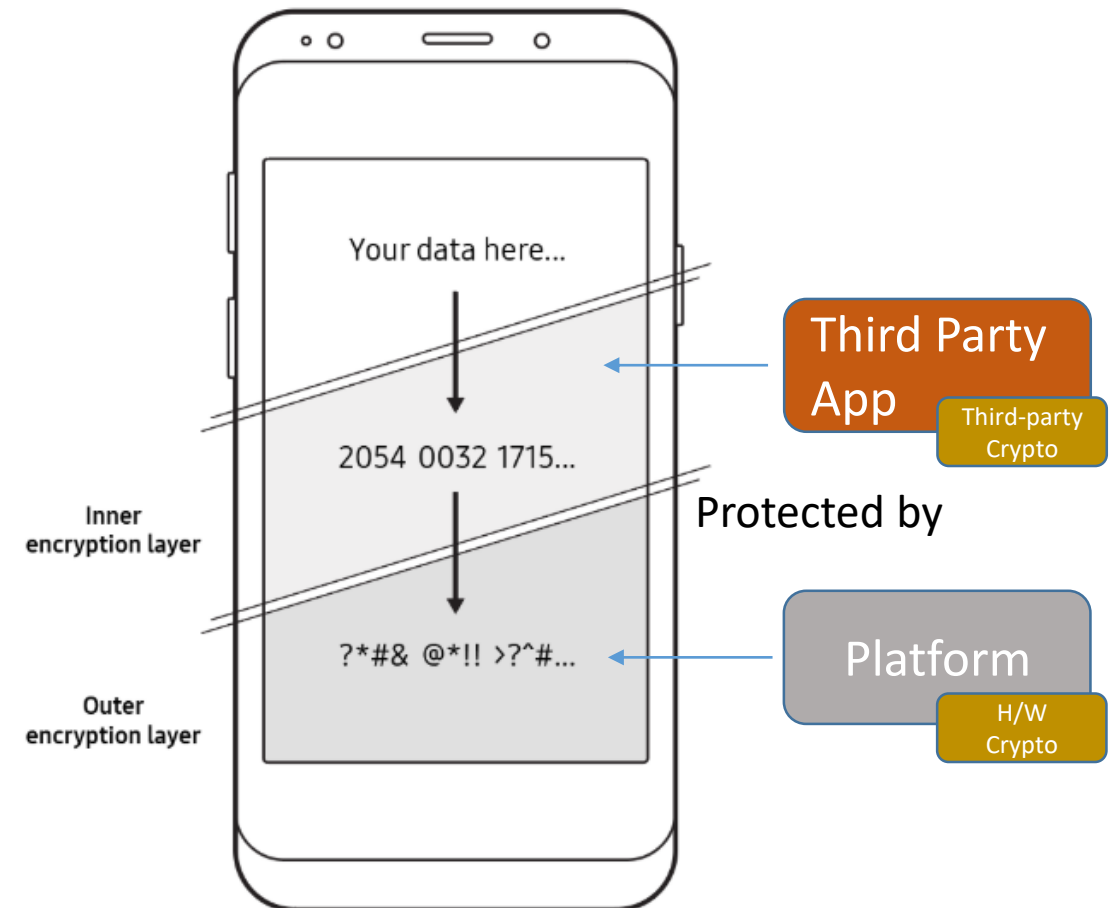
The DualDAR solution provides two layers of encryption and key generation for all data placed inside the Workspace.

Outer layer:

- The outer layer of the DualDAR solution is the standard Samsung FBE implementation discussed earlier.

Inner layer:

- Is based on a framework that allows an independent third party to install a separate cryptographic module.
- When **no** third party module is installed, a separate inner layer of encryption is secured by a Samsung cryptographic module that is included with the Galaxy Samsung devices.

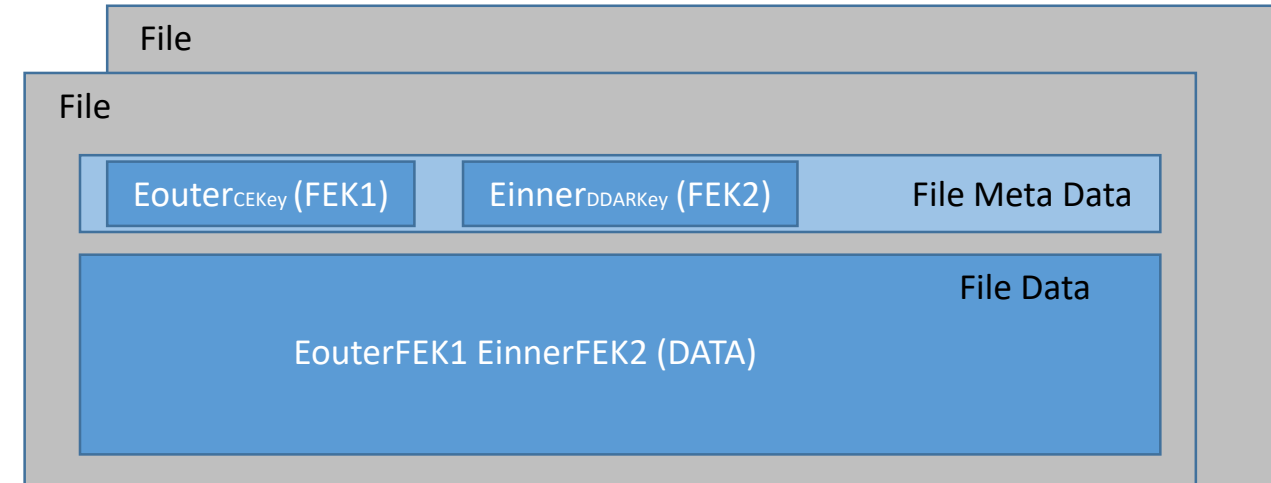


What is DualDAR and why is it beneficial?

How DualDAR encryption works

In a Workspace configured for DualDAR, secure data availability is as follows:

- Access to app data inside the container is only available when the container is unlocked, that is when the user is actively using the container.
- When the container, or device is locked, the container encryption keys are evicted from memory following a timeout.
- In a data lock state, the device remains powered-on but the user is locked out of both the Workspace and device. All classified data is protected in Credential Encrypted (CE) storage within the Workspace. CE storage is not available until the user provides both their device and Workspace credentials.



- From an app point of view, the DualDAR Workspace functions as CE storage.
- The Knox framework prevents apps from writing data to non-DualDAR protected DE storage.
- An specific app aware of both CE and DE storage, and needs to write unclassified content to DE storage can be whitelisted to be allowed to write to DE storage.

Knox DualDAR features and architecture

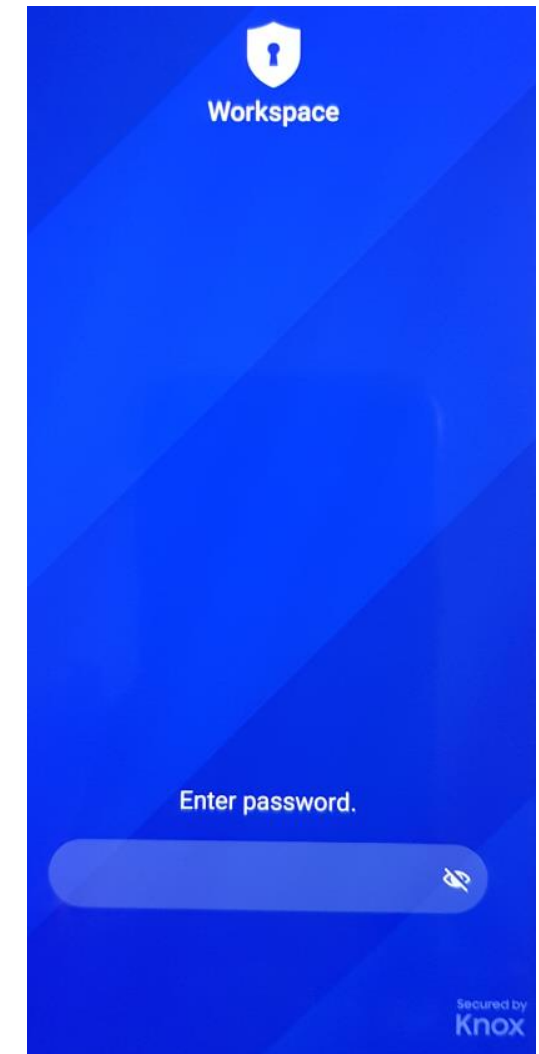
Features

- Dual Authentication Model for DualDAR Workspace
- Timed Exposure
- Access Control to prevent Enterprise Apps from writing Classified Data to Unprotected Storage (DE)
- Dual Layer Protection

Knox DualDAR features and architecture

Dual Authentication

- To access DualDAR protected data, the user must authenticate into each layer of the device and Workspace separately.
- It is required of the end user to provide the first password to authenticate to the device and the second password to authenticate to the Knox Workspace.
- IT admin can set password policies independently for each password
- Encryption keys are evicted from memory



Knox DualDAR features and architecture

Encryption keys eviction from memory

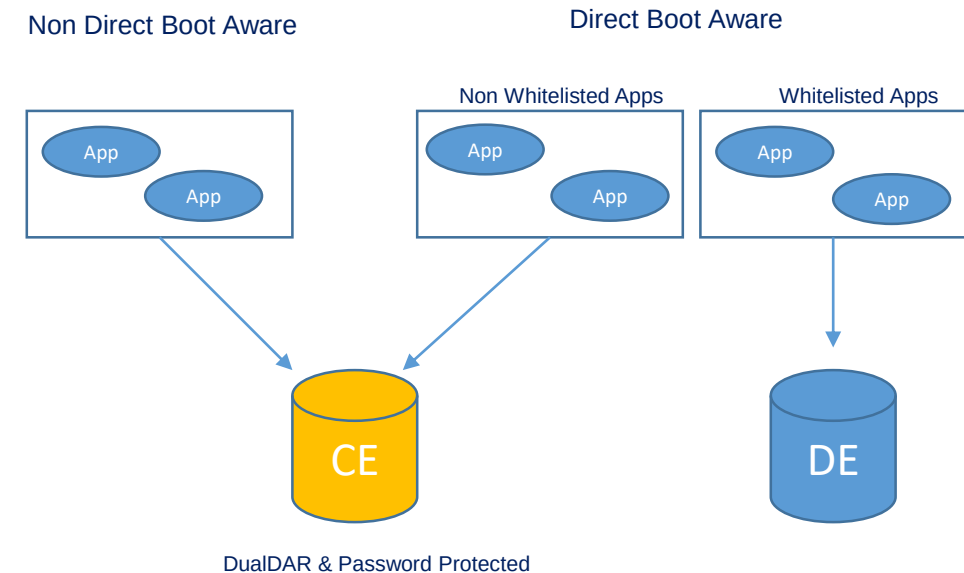
- There are two Keyguards used to protect access to Classified Data in Workspace CE Storage
 - Device Keyguard
 - Workspace Keyguard
 - The password used for each Keyguard is used to protect the encryption key for each layer:
 - Device Password for Outer
 - Workspace Password for Inner
- When Workspace is in a lock state, or the device is locked as a whole, the Inner Layer keys are evicted from memory.

Knox DualDAR features and architecture

Access Control for Enterprise Apps

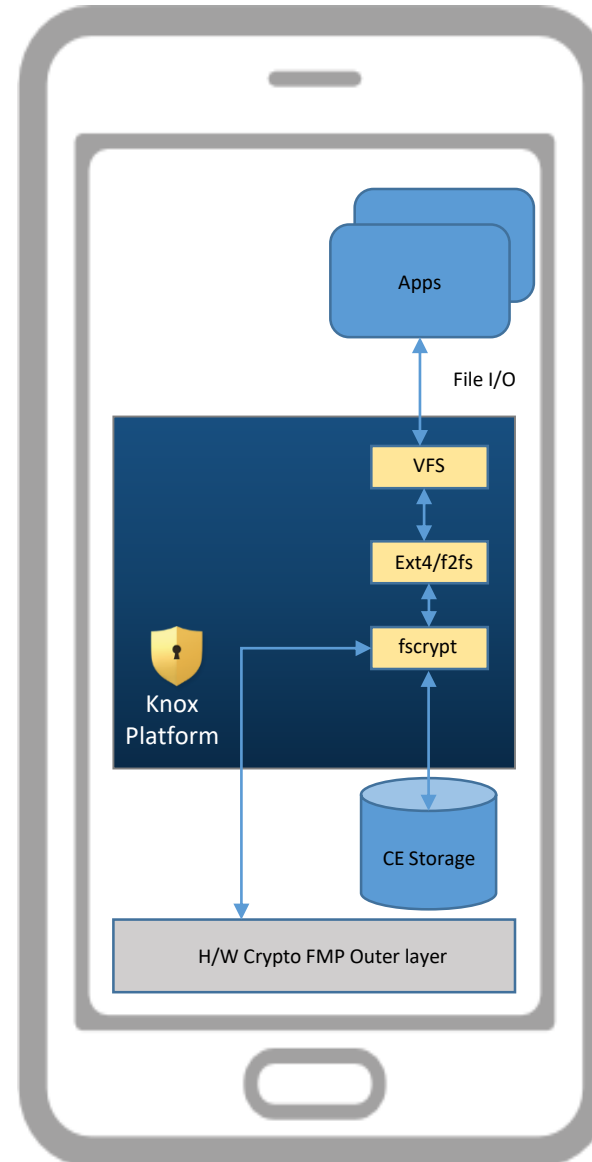
Device Encrypted Storage

- With DualDAR enabled, work apps cannot write to Device Encrypted Storage by default
- That mitigates the risk of a malicious app writing classified content to DE storage without explicit IT admin approval.
- To allow writes to DE storage, a package whitelist can be created and the 'DE restriction' settings must be set to False.



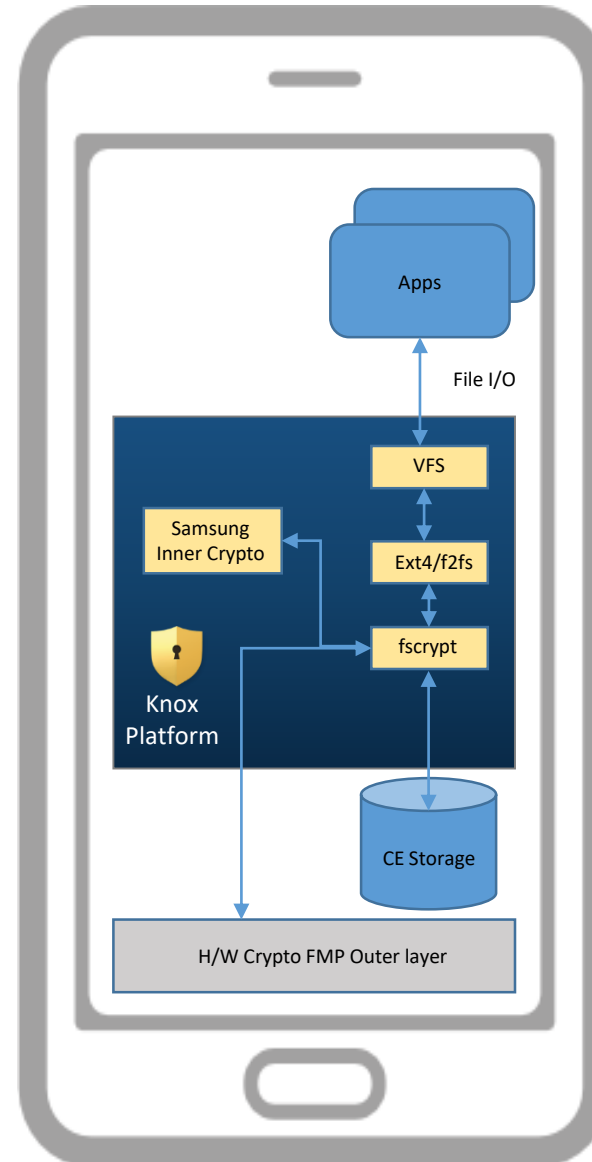
Knox DualDAR features and architecture

Software Architecture



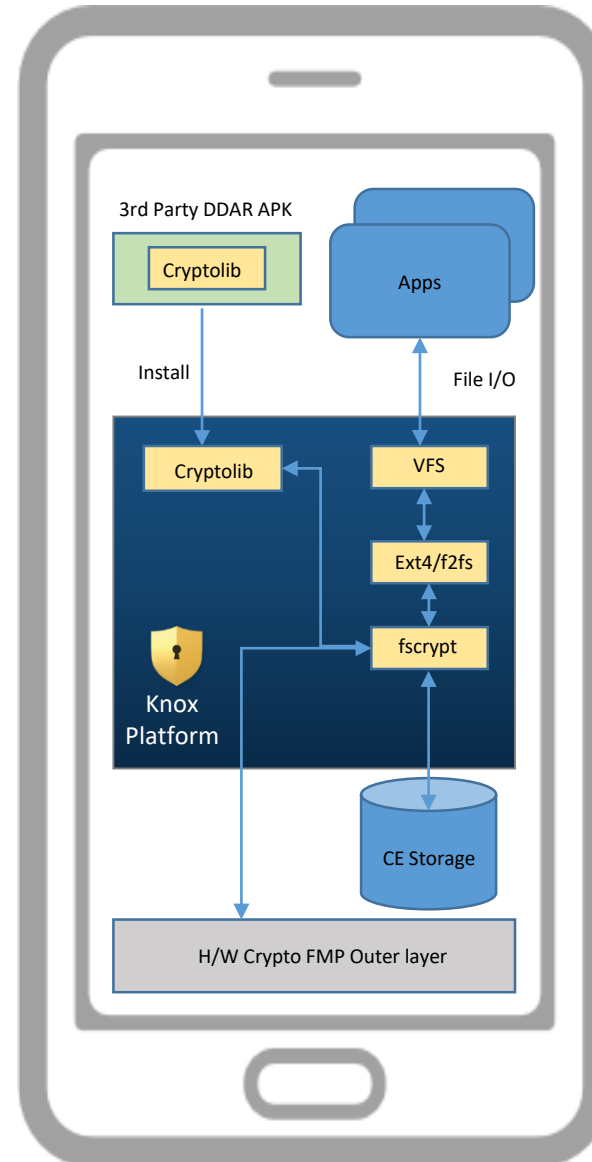
Knox DualDAR features and architecture

Software Architecture



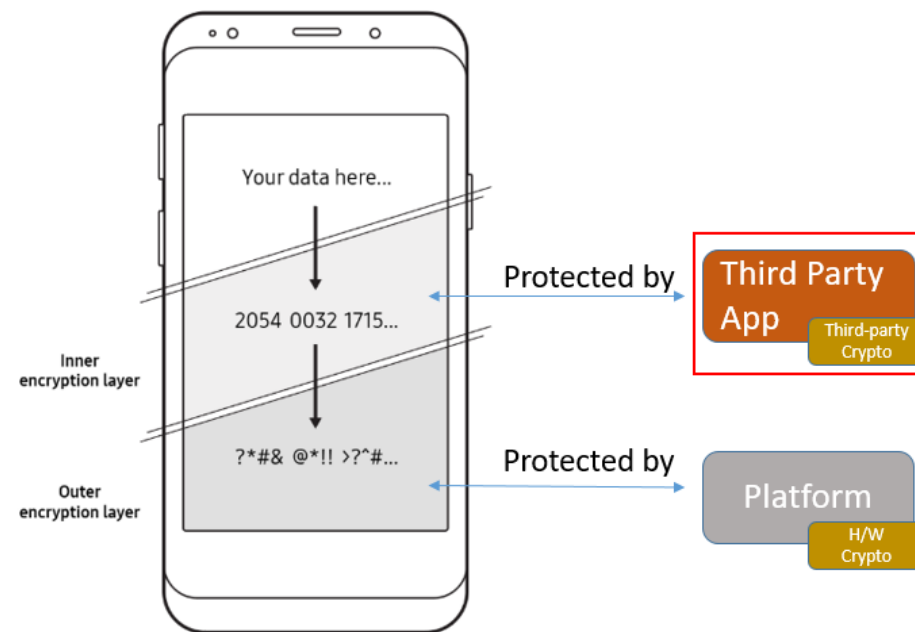
Knox DualDAR features and architecture

Software Architecture



Knox DualDAR features and architecture

Inner Layer of Encryption by 3rd party: second layer of encryption



- The platform must activate a KPE DualDAR license before an APP can invoke the APIs and receive platform callbacks.

Knox DualDAR features and architecture

Inner Layer of Encryption by 3rd party: Second layer implementation, Knox SDK

SAMSUNG Knox SDK API reference

Map Knox API level to SDK version ☐ Filter by Knox API level: 1

PACKAGE INDEX | CLASS INDEX

com.samsung.android.knox
com.samsung.android.knox.accounts
com.samsung.android.knox.application
com.samsung.android.knox.bluetooth
com.samsung.android.knox.browser

com.samsung.android.knox.ddar

Provides classes that:

- Enable creation and configuration of a workspace(container) with Dual DAR protection.
- Enable third party applications to provide an implementation for an independent second layer of encryption.

Classes

DualDARClient

This class is used by privileged application to invoke Dual DAR platform apis and receive platform callbacks.

DualDARPolicy

This class supports MDM(EMM) to create a workspace(container) protected with Dual DAR and provides APIs to access and set Dual DAR configurations.

DualDARPolicy.DUAL_DAR_VERSION_CODES

Enumeration of the currently known DUAL DAR version codes.

<https://docs.samsungknox.com/devref/knox-sdk/reference/com/samsung/android/knox/ddar/package-summary.html>

Knox DualDAR features and architecture

Inner Layer of Encryption by 3rd party: Second layer implementation, Native SDK

SAMSUNG Mobile Device Management Native SDK

Main Page	Namespaces	Classes	Files
Class List	Class Index	Class Members	

ddar > abstract_crypto >

ddar::abstract_crypto Class Reference

Base class for dual-dar crypto implementation. [More...](#)

```
#include <ddar.h>
```

List of all members.

Public Member Functions

virtual bool	prepare (context *context, metadata *md)=0 Callback to initialize ephemeral cache.
virtual bool	encrypt (metadata *md, void *pt, void *ct, unsigned long page_offset, int page_len)=0 Callback when a file is currently being written to the disk.
virtual bool	decrypt (metadata *md, void *ct, unsigned long page_offset, int page_len)=0 Callback when a file is currently being read from the disk.

Detailed Description

Base class for dual-dar crypto implementation.

Additional Information here:

developer.samsungknox.com

https://docs.samsungknox.com/devref/knox-sdk/reference/native/html/classddar_1_1abstract_crypto.html

Knox DualDAR features and architecture

Inner Layer of Encryption by 3rd party: Certification

Application Software Protection Profile (ASPP)
Extended Package: File Encryption:
Mitigating the Risk of Disclosure of Sensitive Data on a System



10 November 2014
Version 1.0

Protection Profile for Application Software



Version: 1.1
2014-11-05
National Information Assurance Partnership

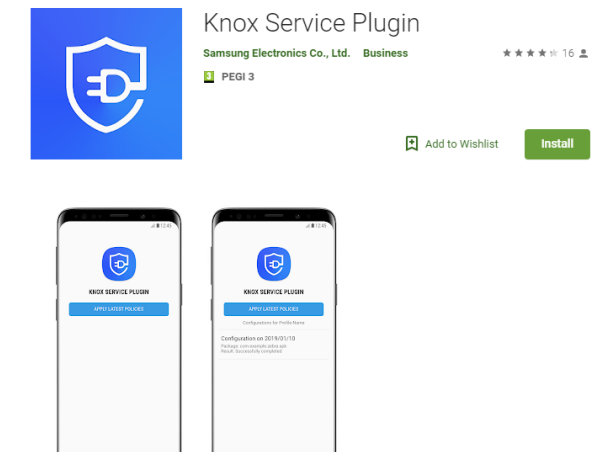
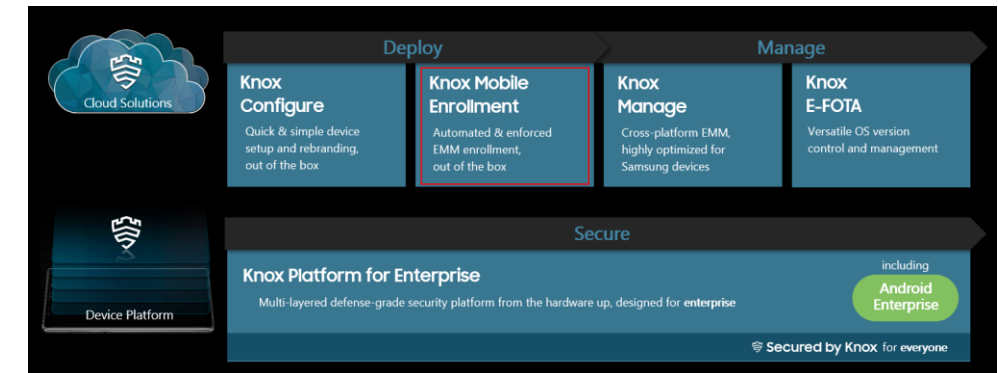
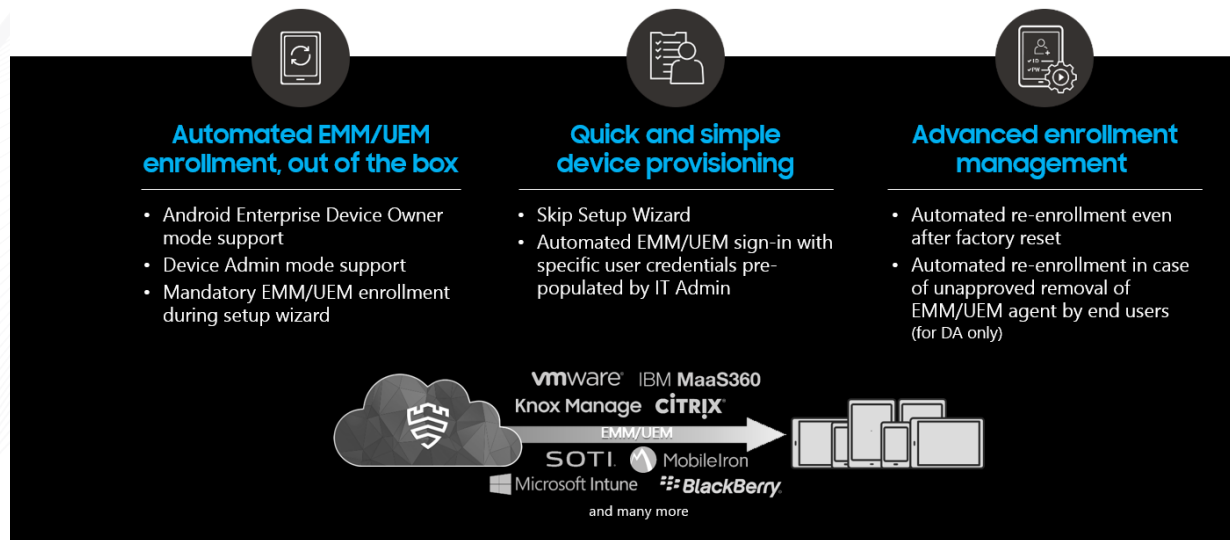
Main Protection Profiles for a Inner Layer of Encryption Certification

Deployment of a DualDAR Workspace

Tools

Knox Mobile Enrollment

Makes device enrollment easier for both IT admins and device users



- IT admins can use DualDAR features the moment they're released.
- Through the Knox Service Plugin (KSP) and Knox Mobile Enrollment (KME), IT admins can create DualDAR workspace containers and configure policies

Deployment of a DualDAR Workspace

Knox Mobile Enrolment (KME)

Use your 3rd Party App for

inner layer crypto

or by using default...

Samsung Crypto, using File Kernel Software Crypto

Algorithm: AES XTS 256 for File Encryption

and

TEE with Hardware Backed Protection for Key Management

Algorithm: PBKDF2, AES GCM 256



Deployment of a DualDAR Workspace

Knox Service Plugin (KSP)

Work profile policies (Profile Owner)

<APPLICATION CONFIGURATION

- > Work profile configuration (Premium)
- > RCP policy (Premium)
- > VPN policy (Premium)
- > Firewall policy (Premium)
- > Restrictions in work profile (Premium)
- > Advanced restrictions in work profile (Premium)
- > Password Policy (Premium)
- > Application management policies (Premium)
- > Device Admin whitelisting (Premium)
- > Enterprise Billing policy (Premium)
- > Universal Credential Manager policy (Premium)
- > Dual Data-at-rest (DAR) Encryption (Premium)
- > Certificate management policies (Premium)
- > Network Platform Analytics (NPA) (Premium)

▼ Dual Data-at-rest (DAR) Encryption (Premium)

- Enable Dual DAR controls Disable ▼ ⓘ
- Data lock timeout type No lock-out ▼ ⓘ
- Data lock timeout value (in minutes) 1 ⓘ
- Restrict access to device encrypted (DE) storage Disable ▼ ⓘ
- List of apps allowed to access DE storage ⓘ

Deployment of a DualDAR Workspace

Create a Workspace with your MDM as usual



Thank you!



COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

**XIII
JORNADAS
STIC
CCN-CERT**

ccn-cert
centro criptológico nacional