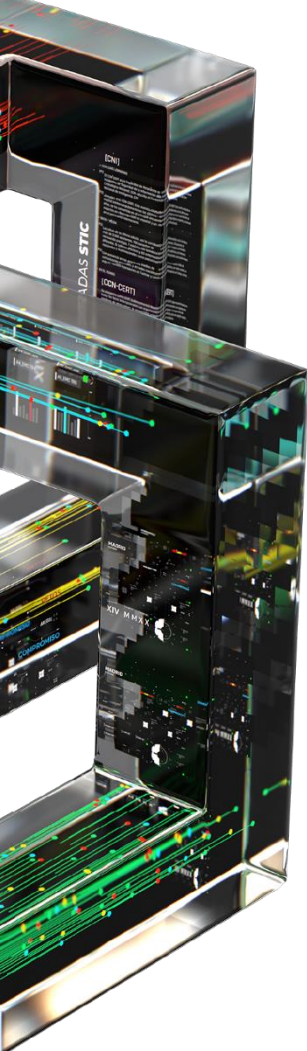




#XIVJORNADASCCNCERT

Android 11 user privacy on Samsung Enterprise devices





Isabel López Peral

Samsung Electronics Iberia S.A.U.

isabel.lopez@samsung.com

Agenda

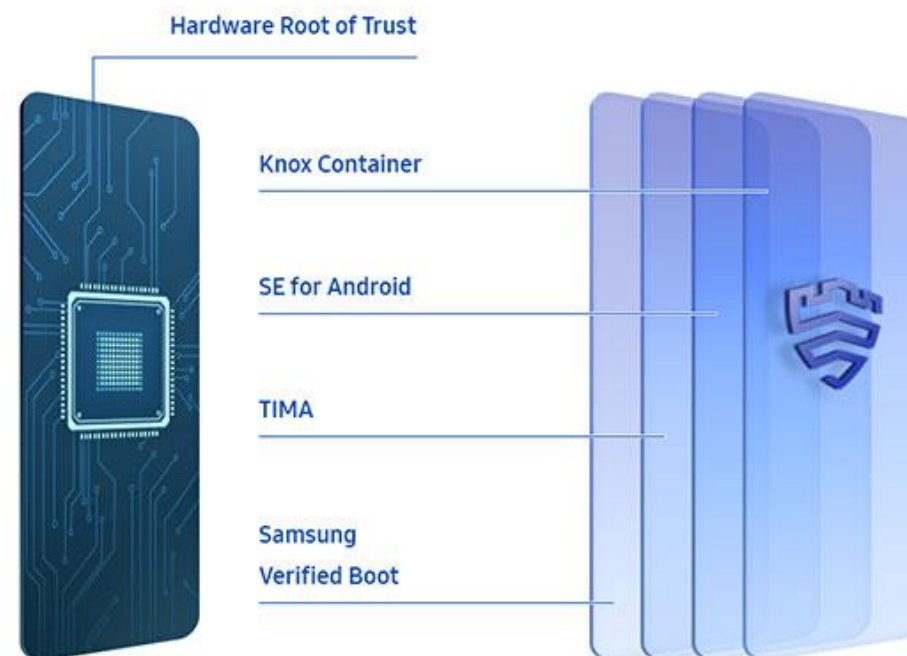
1. Samsung Knox Overview
2. CPSTIC Samsung approved products
3. Deployment scenarios for enterprise
4. User privacy in Android 11
5. Policy changes in Work Profile on Company Owned Device (WP-C)
6. Knox Separated Apps

Samsung Knox Overview

What is Knox?

Mainly consists of the Knox security platform on device and a series of Knox cloud solutions for IT

SECURE



Samsung Knox Overview

Knox Services

Comprehensive suite of enterprise mobility solutions for security, manageability and productivity



Deploy

Knox Configure

Quick & simple device setup and rebranding, out of the box

Knox Mobile Enrollment

Automated & enforced EMM enrollment, out of the box

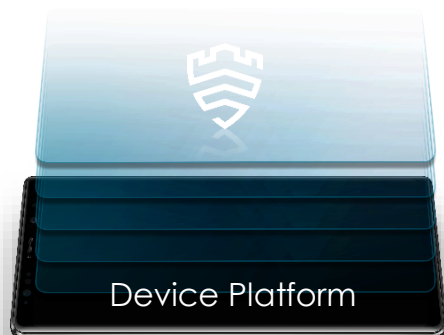
Manage

Knox Manage

Cross-platform EMM, highly optimized for Samsung devices

Knox E-FOTA

Versatile OS version control and management



Secure

Knox Platform for Enterprise

Multi-layered defense-grade security platform from the hardware up, designed for **enterprise**

including

Android Enterprise

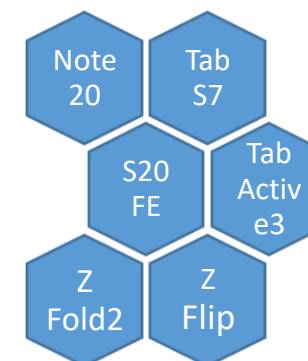
 **Secured by Knox** for **everyone**

CPSTIC Samsung approved products

Wide range of products qualified by CCN for ENS

Guía de Seguridad de las TIC CCN-STIC 1608

Name	Category	Manufacturer	Family	Type
Samsung Galaxy A51 (SM-A515F) Android 10	Protection of equipment and services	· Samsung Electronics Co., Ltd	Mobile devices	Producto Cualificado-ENS Alto
Samsung Galaxy S20+ 5G (SM-G986B), S20 5G (SM-G981B), S20 Ultra 5G (SM-G988B), S20+ 4G (SM-G985F), S20 4G (SM-G980F) Android 10	Protection of equipment and services	· Samsung Electronics Co., Ltd	Mobile devices	Producto Cualificado-ENS Alto
Samsung Galaxy Tab S6 (SM-T860, SM-T865) Android 10	Protection of equipment and services	· Samsung Electronics Co., Ltd	Mobile devices	Producto Cualificado-ENS Alto
Samsung Galaxy XCoverPro (SM-G715FN) Android 10	Protection of equipment and services	· Samsung Electronics Co., Ltd	Mobile devices	Producto Cualificado-ENS Alto



Mid-range device
qualified

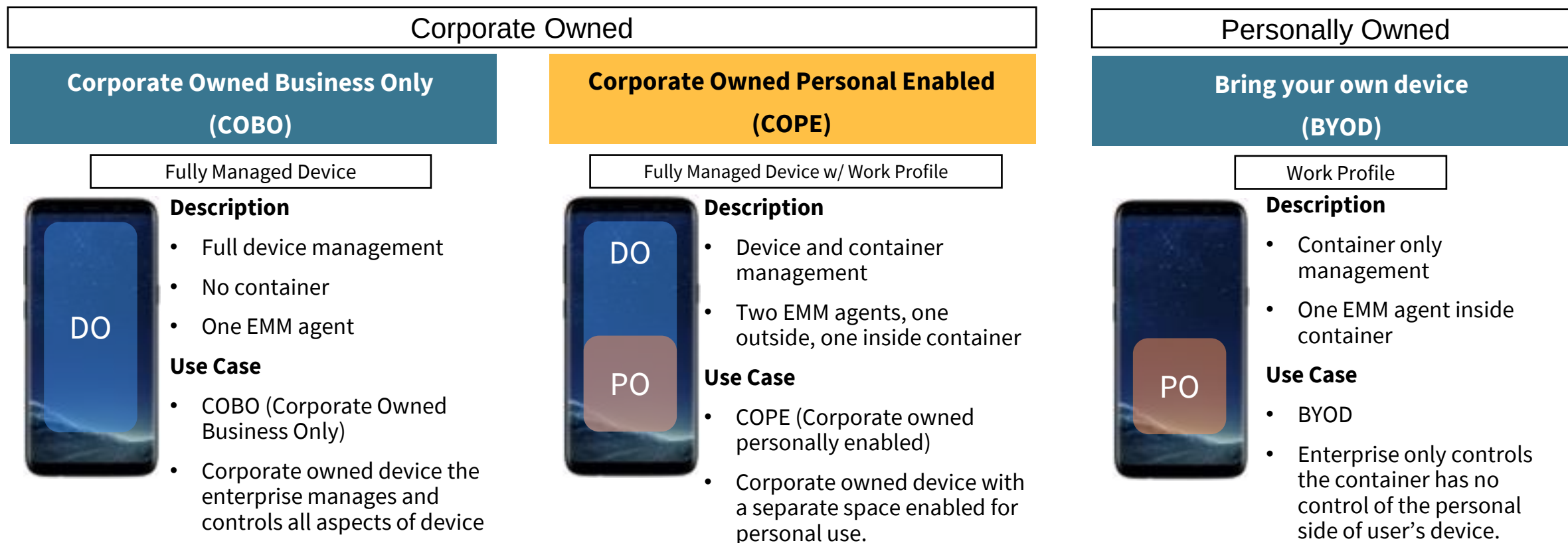
Three Generations of
Android OS Upgrades

Four years SMR for
EE models

<https://oc.ccn.cni.es/index.php/en/cis-product-catalogue/list-of-qualified-products>

Deployment Scenarios for Enterprise

Up to Android 10

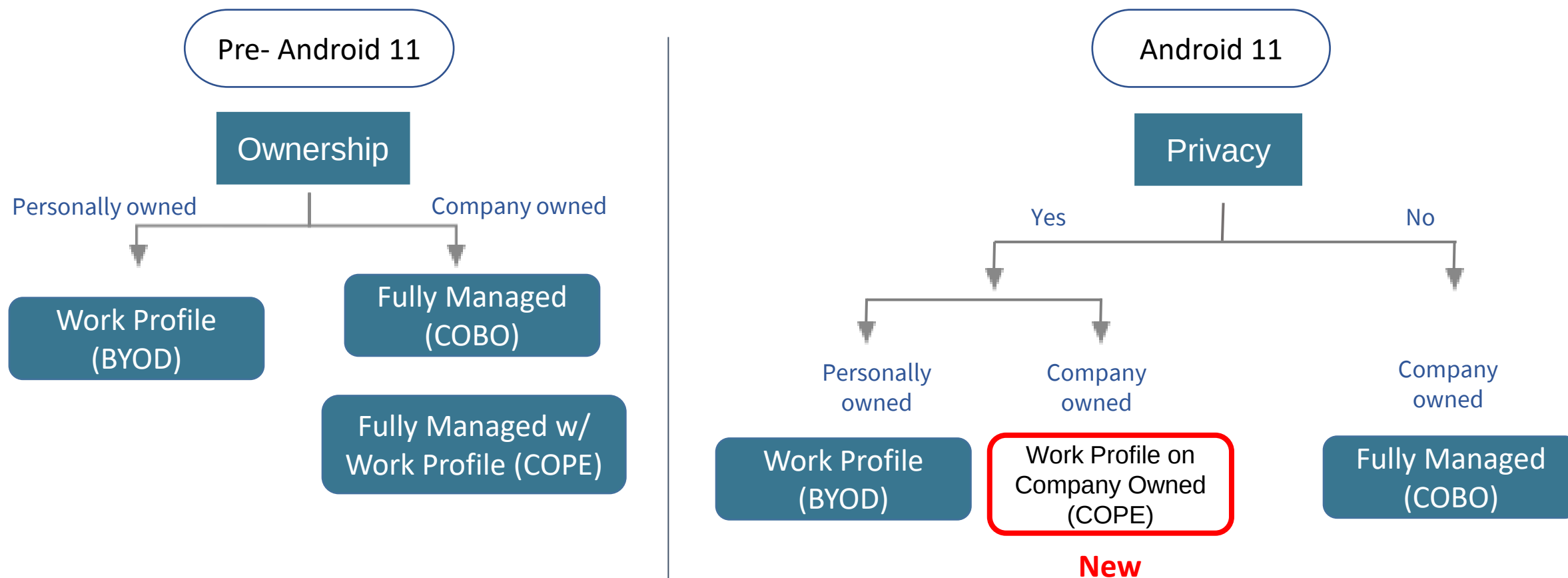


No user privacy required

User privacy is required as there is personal space

User privacy in Android 11

User privacy is a first order decision



User privacy in Android 11

Corporate Owned Personal Enabled (COPE)

Fully Managed Device w/ Work Profile



Description

- Device and container management
- Two EMM agents, one outside, one inside container

Use Case

- COPE (Corporate owned personally enabled)
- Corporate owned device with a separate space enabled for personal use.

- COPE scenario user privacy is required as there is a separate space for personal data
- Up to **Android 10** user privacy is not present because IT admin has full visibility and control on the personal space
- In **Android 11** Google establish user privacy for the Corporate Owned Personally Enabled (COPE) use case
- Device is recognized as Work Profile on Company Owned device (WP-C) during enrolment
- Profile Owner (PO) is enhanced to manage full device for a limited set of policies
- COPE mode in WP-C lacks of DO in personal space

Policy changes in WP-C

Capabilities now possible for core asset management

Device Management

- Wipe device
- Set password complexity
- Control system update policy
- Block screen capture
- Block external storage
- Block camera
- Block cross profile data sharing

App Management

- Set whitelist / blacklist of permissible apps

Connectivity Management

- Data roaming controls
- Block SMS usage
- Block BT controls
- Block Wi-Fi configuration
- Block tethering
- Block USB file transfer
- Block mobile networks
- Block air plane mode

Logging

- Only events happening inside the managed profile

KeyStore Management

- N/A



Policy changes in WP-C

Policies **NOT** available COPE in Android 11

Device Management

- Block end user ability to factory reset
- Disable Keyguard
- Reset Password for the device
- Enable/Disable backup service
- Disallow user from configuring user credentials

App Management

- Manage installed apps on personal side
- Control permissions on personal apps
- Block clearing personal app data and caches
- Ability to poll apps on personal side
- App restrictions for personal apps
- Grant privileged access to apps on the personal side (delegated scope)

Connectivity Management

- Configure personal side VPN
- Configure always on VPN on Personal side
- Set device wide DNS configurations
- Setting a Global Proxy
- Add an override APN
- Ability to block user from resetting network

Logging

- Bug report request
- Network logging

KeyStore Management

- View list of installed CA certificates
- Install user CA on Personal side
- Install certificate chain and corresponding private key
- Generate new public/private key pair
- Associate certificates with key pairs

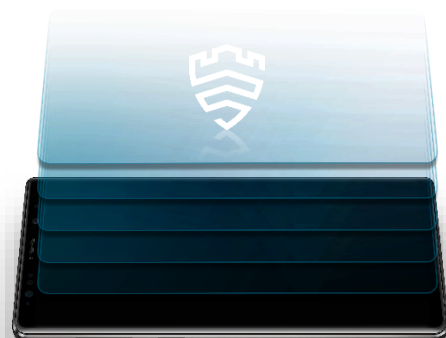


Policy changes in WP-C

New policies available - Expanded by K

- KPE provides more than 500 policies available
- Including Kiosk management for COSU (Corporate Security)
- setCCMode API now is available for enhance fundamentals Protection Profile) compliance
- For further information:

<https://docs.samsungknox.com/dev/knox-sdk/wpc-knox>



Knox Platform for Enterprise

Multi-layered defense-grade security

#XIVJORNADASCNCERT  Secured by Knox

Below is a list of the API methods allowed the personal profile of a company-owned device. If you don't see a particular method in this list, it is not allowed.

Class	Method
AdvancedRestrictionPolicy	allowBLE
AdvancedRestrictionPolicy	allowFirmwareAutoUpdate
AdvancedRestrictionPolicy	allowLocalContactStorage
AdvancedRestrictionPolicy	allowOnlySecureConnections
AdvancedRestrictionPolicy	allowRemoteControl
AdvancedRestrictionPolicy	allowUserSetAlwaysOn
AdvancedRestrictionPolicy	allowWifiScanning
AdvancedRestrictionPolicy	getCCModeState
AdvancedRestrictionPolicy	isBLEAllowed
AdvancedRestrictionPolicy	isFirmwareAutoUpdateAllowed
AdvancedRestrictionPolicy	isLocalContactStorageAllowed
AdvancedRestrictionPolicy	isOnlySecureConnectionsAllowed
AdvancedRestrictionPolicy	isRemoteControlAllowed
AdvancedRestrictionPolicy	isUserSetAlwaysOnAllowed
AdvancedRestrictionPolicy	isWifiScanningAllowed
AdvancedRestrictionPolicy	setCCMode
ApplicationPolicy	addAppPackageNameToBlackList
ApplicationPolicy	addAppPackageNameToWhiteList
ApplicationPolicy	addAppPackageNameToWhiteList
ApplicationPolicy	addAppPermissionToBlackList
ApplicationPolicy	addAppSignatureToBlackList

Knox Separated Apps

Solution overview

Companies typically need to separate official work apps from third-party business apps

Samsung offers **Separated apps** to install third-party business app

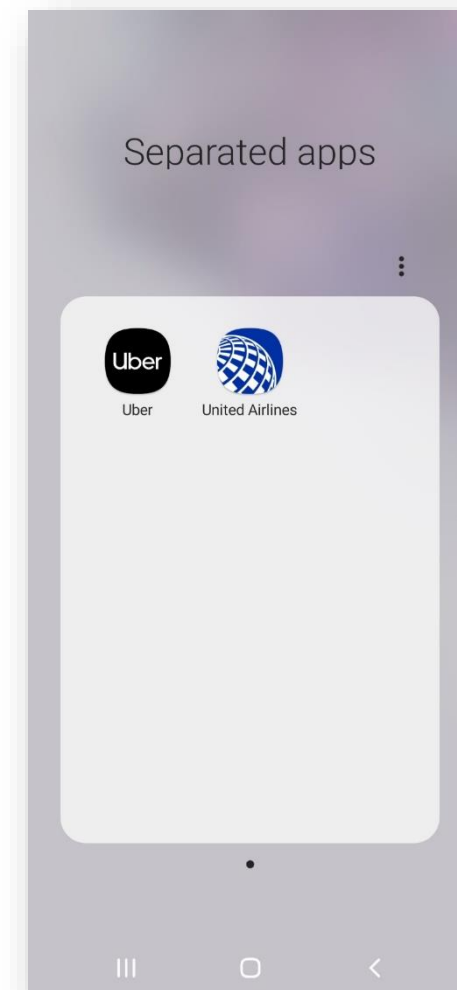
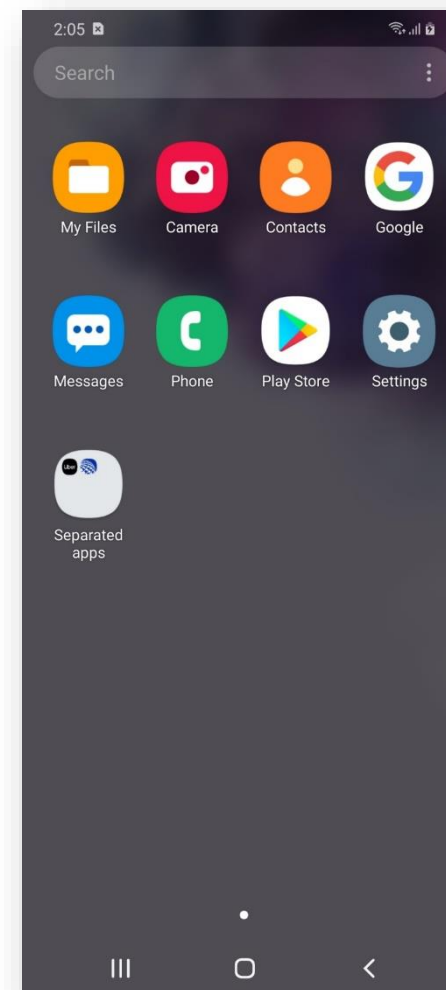
Separated apps isolates third-party apps in sandboxed folder. The third-party apps cannot intercommunicate with work apps or access confidential work data



Knox Separated Apps

Capabilities

- Admin has full control and visibility
- Admin can enable/disable app separation using Knox Service Plugin solution
- Admin can specify apps for separation and isolate non-work approved apps
 - Airline (United, Delta, Iberia, etc)
 - Taxi (Uber, myTaxi, etc)
- Apps will be installed via Managed Play
- Folder view for separated apps
- Default Policies
 - Bluetooth sharing is not allowed
 - Copy/Paste is not allowed
 - External SD card access is not permitted
 - VPN

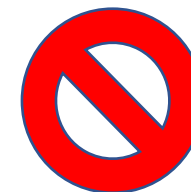


Knox Separated App

Key takeaway

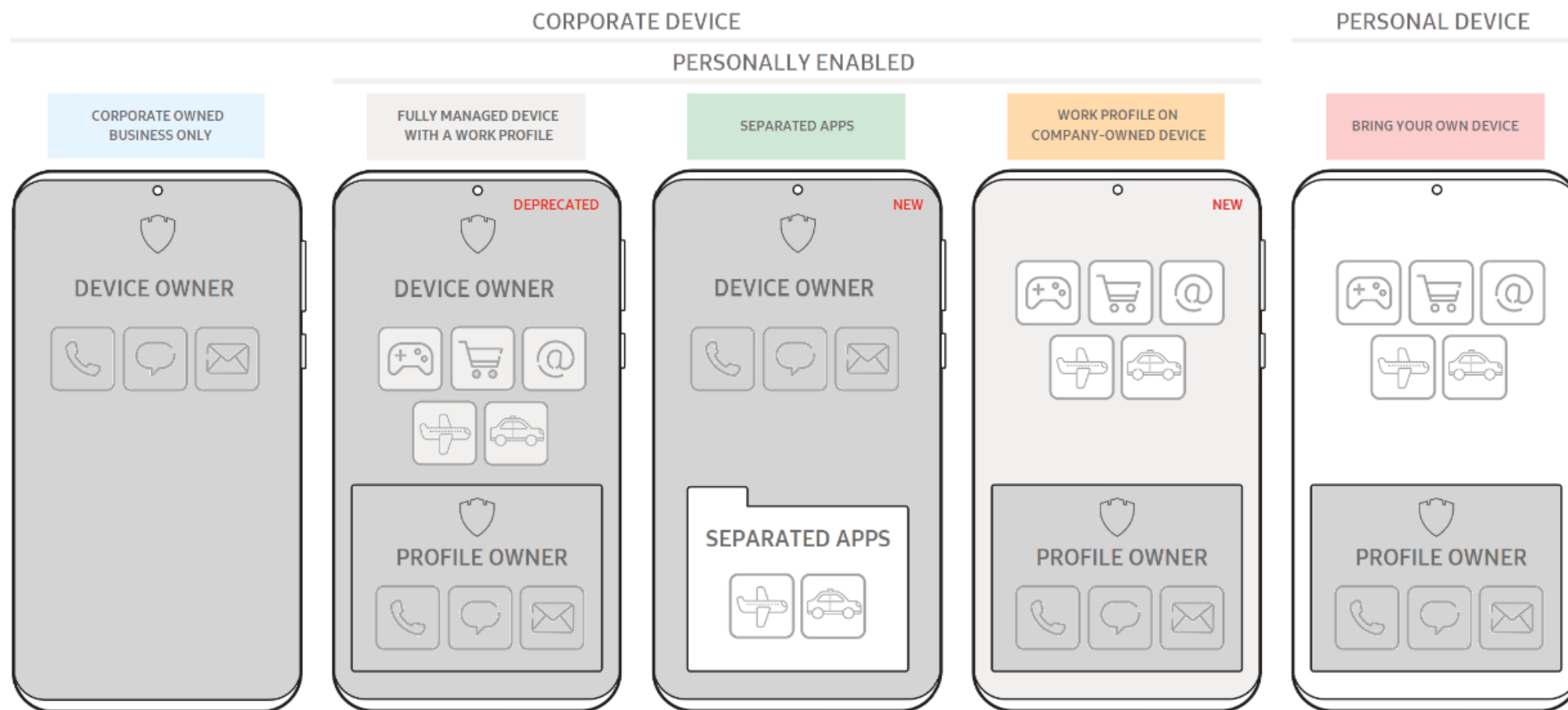


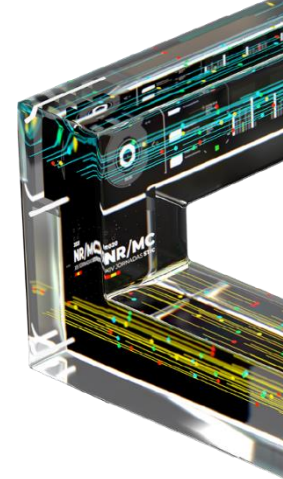
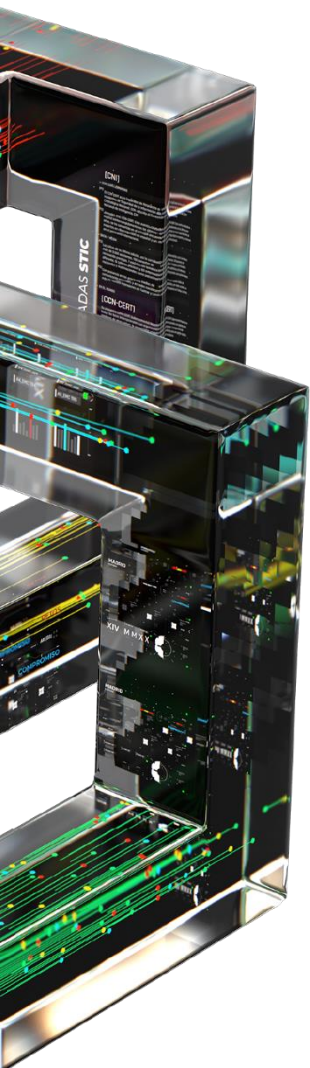
- Knox App Separation is a KPE premium feature on Fully Managed (DO) devices.
- Separated apps are isolated for security reasons.
- No access to sensitive work content.
- Allows IT admin to mitigate risks from one group of apps to another.



- Knox App Separation is **NOT** Fully managed with work profile (DO +PO)
- Knox App Separation is **NOT** original Knox Workspace (DA + container)
- Knox App Separation does **NOT** provide an privacy guarantees, i.e. It is **NOT** for personal apps and data.

In conclusion





MUCHAS GRACIAS

#XIVJORNADASCCNCERT