



Enterprise considerations with Android M and N

DevTalk – 22nd February 2017

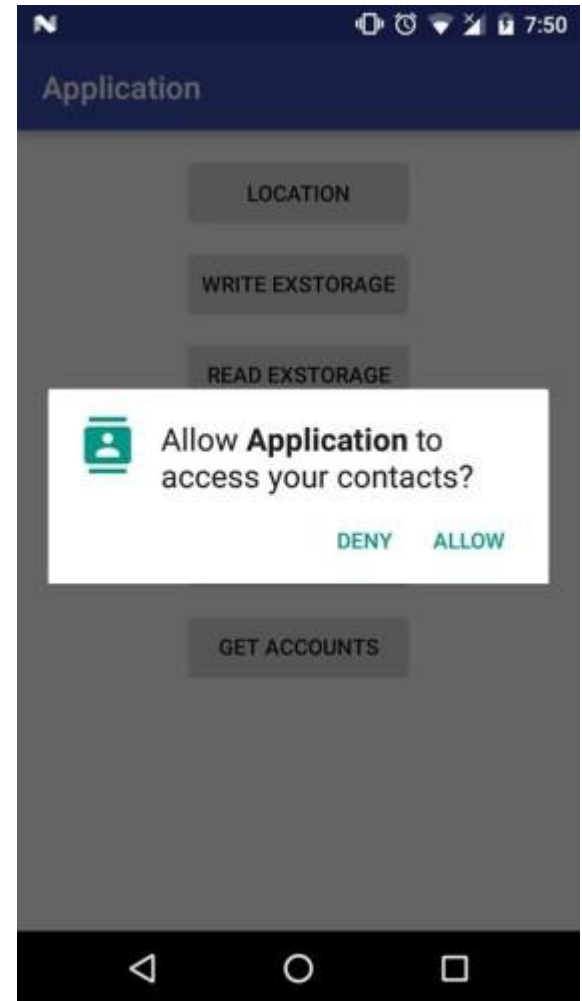
Darryn Campbell

Agenda:

- Android M Enterprise considerations:
 - Dynamic runtime permissions
 - Doze mode & enhanced 'N' doze mode
 - Locking down the new M features (demo)
 - Encryption & adoptable storage
 - Enterprise Android, formally AFW (demo)
- Android N Enterprise considerations:
 - Multi window
 - Notification enhancements
 - Tile API
 - Webview changes
 - Hardware backed attestation



Looks like a
good way for
users to break
applications



What are your options?

1. Continue to target API 22

- Pros: It just works
- Cons: No access to APIs at level 23 or higher including enterprise COSU. User is still able to revoke the permission

2. Implement Google's runtime model (check for permissions, request permissions from user)

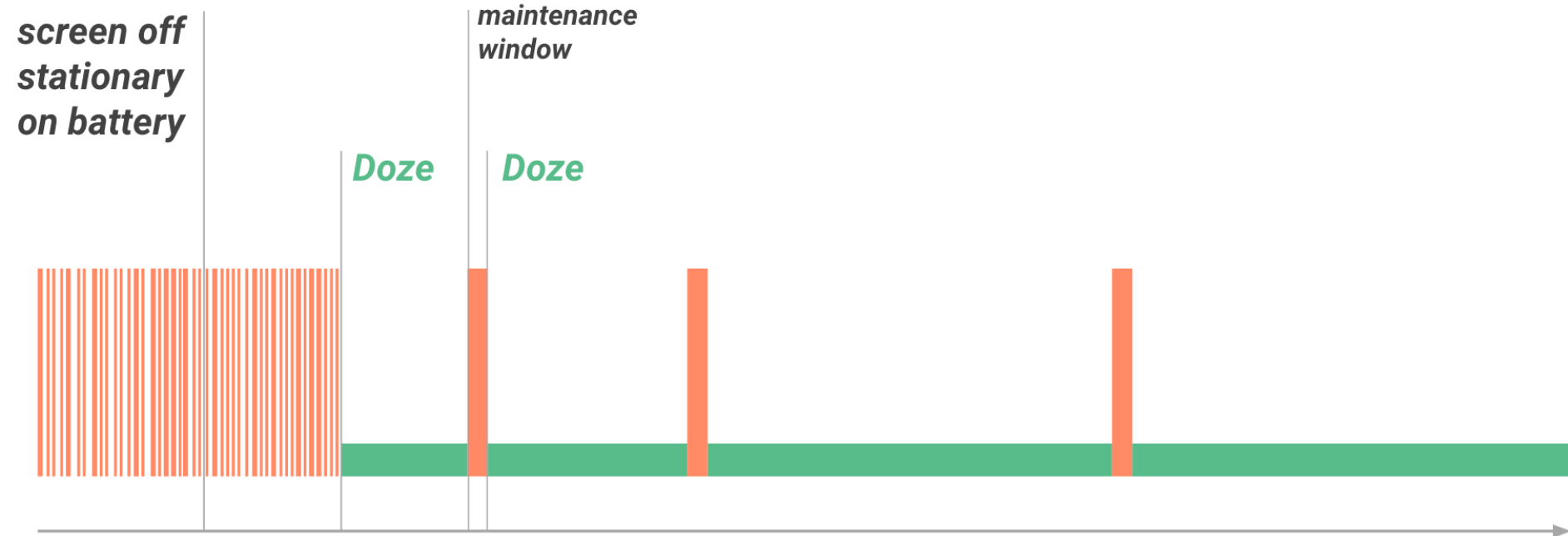
- Pros: Conforms with recommended Google practices
- Cons: Requires user to allow permission or adds overhead to the provisioning step

3. Use an MX AppManager profile to install the application (either through StageNow or EMDK)

- Pros: Permissions are automatically granted
- Cons: Not suitable for development when you are debugging your app

Recommendation: A combination of 2 and 3 to debug and deploy respectively. Lock down the app permissions dialog.

Note: Google managed devices can specify the policy through the DPC



Thanks but my battery already lasts a shift, I'd rather sync my data.

Impacted:

- GSM devices only. AOSP devices are unaffected.
- Push solutions that do not depend on GCM / FCM
- Applications using Alarms to schedule jobs

How can I test?

- https://developer.android.com/training/monitoring-device-state/doze-standby.html#testing_doze_and_app_standby

What can I do?

- Transition to GCM / FCM (GMS only)
- Whitelist applications (Network & wake locks only):
 - `adb shell dumpsys deviceidle whitelist +com.yourcompany.yourapp`
 - Usually a manual process, Play store may reject your app if it is not suitable for Whitelisting (<https://developer.android.com/training/monitoring-device-state/doze-standby.html#whitelisting-cases>)
 - Would include Enterprise Play Store?



**GREAT NEW
FEATURES!!**
How do I turn
them off?

- New copy / paste
 - Google assistant on the toolbar
- User revoking app permissions
- Long press on notifications to bring up options
- Notification shade
- System UI tuner

DEMO

- What is it?
- Why?
- How to enable?
- How to provision?



Doesn't Zebra
already have
encryption?



Interaction with Encrypt Manager – Adoptable Storage

<http://techdocs.zebra.com/emdk-for-android/6-0/mx/encryptmgr/>

Two modes:

1. Full Storage Card Encryption Mode

- Matches what Adoptable Storage is with the same limitations
- Can be provisioned via StageNow
- Duplicates Android functionality so potential for future deprecation

2. Folder Encryption Mode

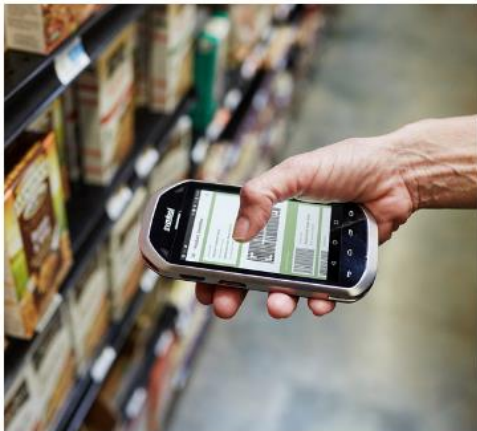
- Supports encryption in /data and on the Storage Card
- Allows a common encrypted implementation in common with non-Marshmallow devices in your deployment

Note: Encryption Manager will not be aware that an adopted SD card is encrypted, the two are mutually exclusive.

Interaction with MX Power Manager - Marshmallow

Reset Action	Emulated storage cards	Physical storage cards	Adopted storage cards	Enterprise partition
Reboot	Retained	Retained	Retained	Retained
Full Device Wipe	Wiped	Wiped	Wiped	Wiped
Factory Reset	Wiped	Retained	Wiped	Wiped
Enterprise Reset	Wiped	Retained	Wiped	Retained

Learn how Android empowers businesses to mobilize and transform.



Make better decisions

Gain insight on in-store customer behavior, product performance, and inventory trends. Android helps you to better understand your business and make more strategic decisions.



Improve the patient experience

Equip your doctors and nurses with a range of purpose-built devices that helps them better serve patients from the time they check-in to their recovery at home.

See what's possible



Streamline efficiency

Improve efficiency by creating modernized workflows for machine monitoring and maintenance, manufacturing processes, distribution, and receiving.

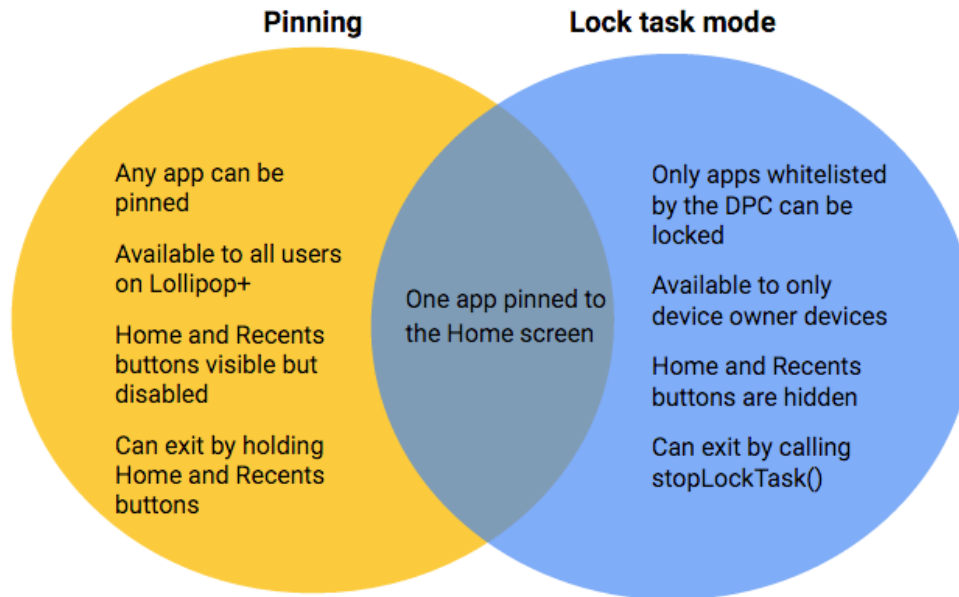
See what's possible

Recap:

- Android for Work started with 5.0 (lollipop). Announced at Google I/O 2014
- Initially targeted BYOD (Bring your own device) use cases
 - Separation of 'Work' mode from personal applications
 - 'Work profile' owned by a "Profile Owner" which would be a device policy controller (DPC)
- Enhancements for COPE (Corporate owned, personally enabled)
 - Expectation that device or profile will owned by a DPC
 - DPC is acting as device owner (DO) or profile owner (PO)
- Enhancements for COSU (Corporate owned, single use) [6.0+]
 - Expectation that these devices will only have a device owner (DO)
 - Typical Zebra device use cases
 - Non-Zebra single use Android devices could be a payment terminal or airport check-in.
- DO provisioning via NFC prioritized by Google (also possible via adb)

Enterprise Android enhancements in Marshmallow:

- COSU support (Corporate Owned – Single Use).
 - Managed configurations with bundle data types
 - Lock Task Mode in addition to lollipop's consumer oriented 'Pinning'



DEMO

- Multi-Window Support
- Notification Enhancements
- Doze on the Go
- Data Saver
- Tile API
- Number Blocking
- New Emojis 😊
- WebView enhancements, now using Chrome (on GMS)
- Enterprise updates (incremental)
- Hardware backed keystore



With multi-window,
my employees'
efficiency has
doubled!

- App Shortcuts
- Image Keyboard Support
- “Professional” Emoji 😊😊😊
- Storage Manager Intent



**Adoptable storage
enables me to store
more emoji!**