Zebra
DevCon 2023

ZEBRA

Getting your application ready for Android 13 and a Preview of Android 14

Pietro F. Maggi
Android Enterprise TSC - Google

Nicola De Zolt L.
Software Engineer- Zebra

Today's agenda

Zebra DevCon 2023

- Android 13 – Android 14
  - Performance, Privacy, Security
  - App Hibernation
  - Runtime Permissions Autogranting
  - XML Profiles
- Foreground Services
  - FGS restrictions
  - Direct Boot
- Scoped storage
- Package Visibility

Zebra
DevCon 2023

Android™ 13 / Android™ 14

Android 13 - Behavior changes

All Apps – d.android.com/about/versions/13/behavior-changes-all

Performance and battery

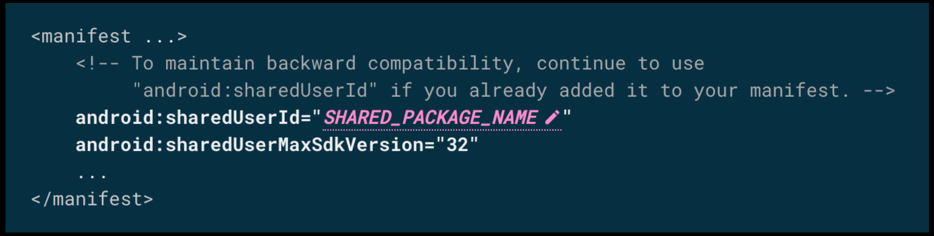
- Task Manager
- Battery Resource Utilization & Restricted App Stand-by Bucket

Privacy

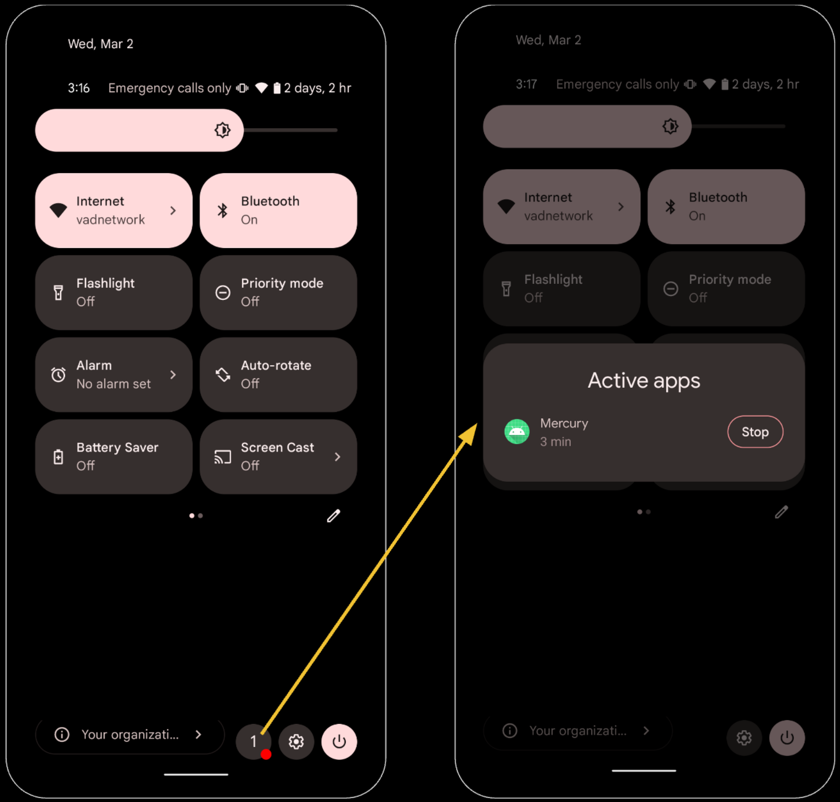
- Runtime permission for notifications

Security

- Migrate away from shared user ID



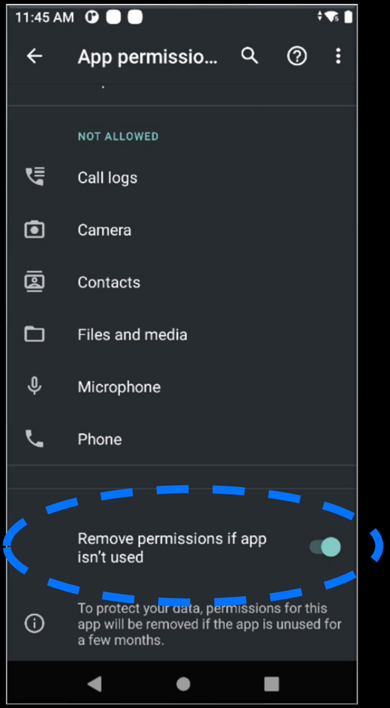
```
<manifest ...>
    <!-- To maintain backward compatibility, continue to use
         "android:sharedUserId" if you already added it to your manifest. -->
    android:sharedUserId="SHARED_PACKAGE_NAME"
    android:sharedUserMaxSdkVersion="32"
    ...
</manifest>
```



Zebra updates for Android 13 (and 11+)

Hibernation effects mitigation

- App hibernation (Android 11+) - https://developer.android.com/topic/performance/app-hibernation
  - Runtime Permissions reset mitigation is offered with the October 2023 LifeGuard Update

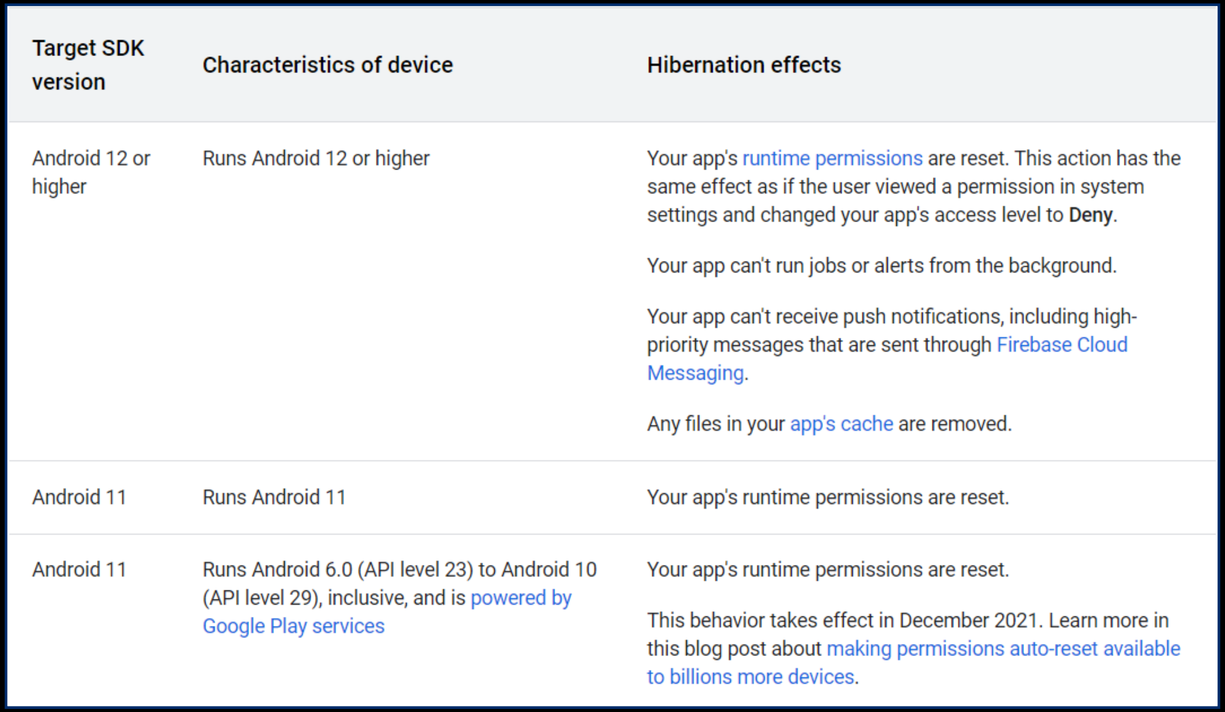


NOT ALLOWED

- Call logs
- Camera
- Contacts
- Files and media
- Microphone
- Phone

Remove permissions if app isn't used

To protect your data, permissions for this app will be removed if the app is unused for a few months.



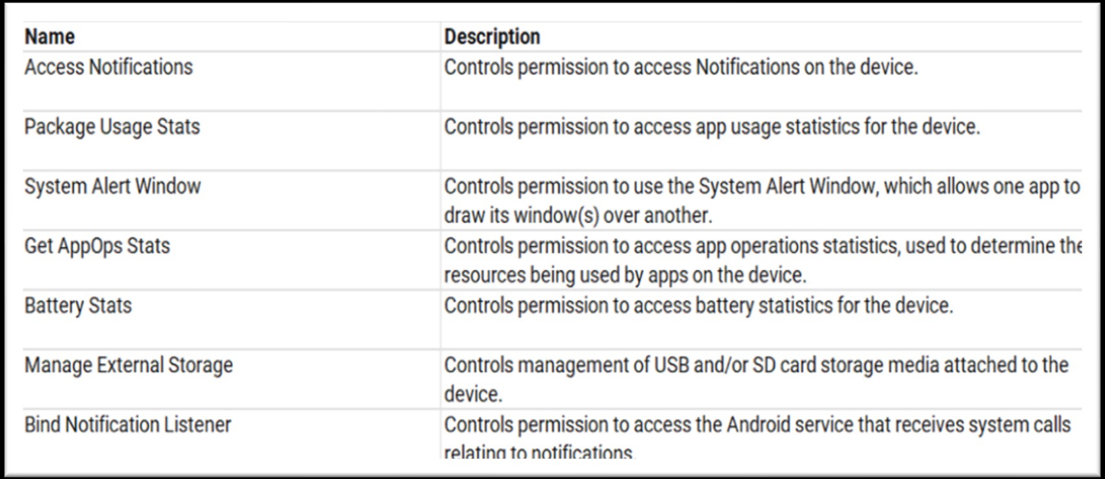
Target SDK version	Characteristics of device	Hibernation effects
Android 12 or higher	Runs Android 12 or higher	Your app's runtime permissions are reset. This action has the same effect as if the user viewed a permission in system settings and changed your app's access level to **Deny**. Your app can't run jobs or alerts from the background. Your app can't receive push notifications, including high-priority messages that are sent through Firebase Cloud Messaging. Any files in your app's cache are removed.
Android 11	Runs Android 11	Your app's runtime permissions are reset.
Android 11	Runs Android 6.0 (API level 23) to Android 10 (API level 29), inclusive, and is powered by Google Play services	Your app's runtime permissions are reset. This behavior takes effect in December 2021. Learn more in this blog post about making permissions auto-reset available to billions more devices.

Zebra updates for Android 13

StageNow's Runtime Permissions Autogranting

Zebra DevCon 2023

- In the beginning permissions were just *manifest-declared*
- Android 6 introduced *runtime permissions*
  - Users grant dangerous permissions to an app when it's running
  - **Zebra mitigated the impact** by introducing the *silent app install feature* for administrators
- «**Special**» runtime permission
  - Zebra preferred to limit the auto-granting mechanism,
  - A subset of dangerous permissions are not automatically granted ➔
  - Need an explicit granting by an Administrator (EMDK/ Stagenow **Access Manager** Permission Access Action)



Name	Description
Access Notifications	Controls permission to access Notifications on the device.
Package Usage Stats	Controls permission to access app usage statistics for the device.
System Alert Window	Controls permission to use the System Alert Window, which allows one app to draw its window(s) over another.
Get AppOps Stats	Controls permission to access app operations statistics, used to determine the resources being used by apps on the device.
Battery Stats	Controls permission to access battery statistics for the device.
Manage External Storage	Controls management of USB and/or SD card storage media attached to the device.
Bind Notification Listener	Controls permission to access the Android service that receives system calls relating to notifications

Zebra updates for Android 13

Continued Support for XML EMDK profiles

- The original plan was to deprecate XML support in Android 11 and Obsolete XML support in Android 13
  - – Developers and EMM vendors confirmed their desire to continue integrating with Mx
  - – Android™ 13 timelines too tight to commit for non-XML Mx integration
- Zebra decided to temporarily postpone obsoleting XML support in Android™13
  - – We will support backward compatibility
    - Legacy applications using XML-based EMDK will still run
  - – XML support is available in Android 13 through MX 11.9
  - – Beyond Mx 11.9 partners need to support non-XML integration
    - We are adding features without losing functionalities
  - – Targeting 2H2023 for EMDK support for non-XML-based output for device configuration
  - – Refer to https://techdocs.zebra.com/flux/about/ for any current and future updates

Android 14 - Behavior changes

All Apps – d.android.com/about/version/14/behavior-changes-all

Zebra
DevCon 2023

Core functionality

- Schedule exact alarms are denied by default
  Calendar and alarm clock apps should declare USE_EXACT_ALARM
- MTU is set to 517 for the first GATT client requesting an MTU
- New reason an app can be placed in the restricted standby bucket

Security

- Minimum installable target API level

```
INSTALL_FAILED_DEPRECATED_SDK_VERSION: App package must target at least SDK version 23, but found 19
```

- You can bypass this with adb if needed with the --bypass-low-target-sdk-block option

```
adb install --bypass-low-target-sdk-block FILENAME.apk
```

- On devices upgrading to Android 14, apps with a targetSdkVersion lower than 23 will remain installed

Android 14 - Behavior changes

Apps targeting Android 14 or higher

Zebra DevCon 2023

Core functionality

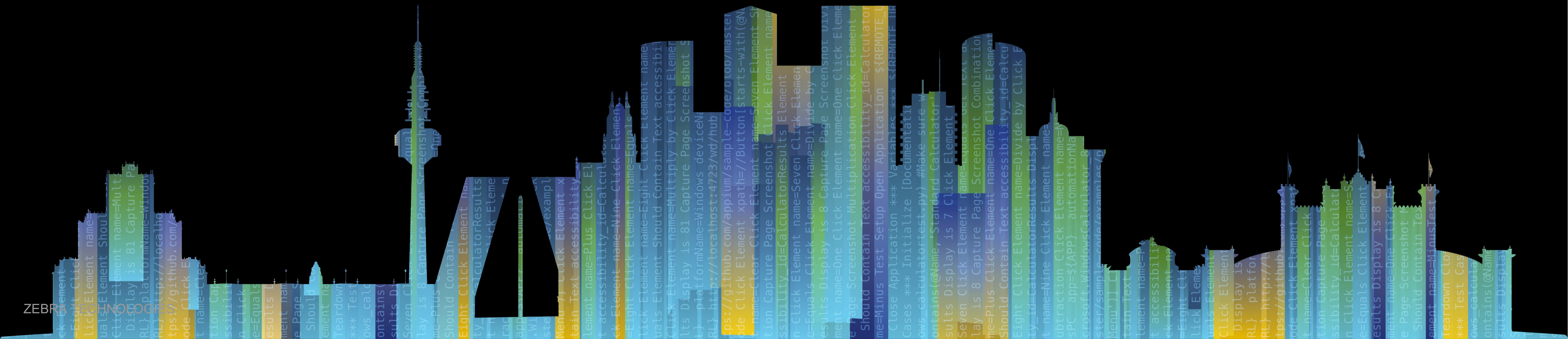
- Foreground service types are required
- Enforcement of `BLUETOOTH_CONNECT` permission in `BluetoothAdapter`
- `JobScheduler` reinforces callback and network behavior

Security

- Restrictions to implicit and pending intents
- Runtime-registered broadcasts receivers must specify export behavior
- Additional restrictions on starting activities from the background

Zebra
DevCon 2023

Foreground Service Restrictions



Why are Foreground Services Restrictions necessary?

To protect

- The user's privacy
- The device battery life

How

- Declaring foreground service types (multiple types can be combined)

Recommended alternative

- Jetpack WorkManager : d.android.com/workmanager

- `camera`
- `connectedDevice`
- `dataSync`
- `health`
- `location`
- `mediaPlayback`
- `mediaProjection`
- `microphone`
- `phoneCall`
- `remoteMessaging`
- `shortService`
- `specialUse`
- `systemExempted`

Why are Foreground Services Restrictions necessary?

Zebra
DevCon 2023

Steps

- Declare the service type

```
<manifest ...>
  <uses-permission android:name="android.permission.FOREGROUND_SERVICE" />
  <uses-permission android:name="android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK" />
    <application ...>
      <service
          android:name=".MyMediaPlaybackService"
          android:foregroundServiceType="mediaPlayback"
          android:exported="false">
      </service>
    </application>
</manifest>
```

- Add the new permission
- Include the foreground service type at runtime

```
Service.startForeground(0, notification, FOREGROUND_SERVICE_TYPE_LOCATION)
```

Zebra updates for FGS & Direct boot

Stagenow features

Zebra DevCon 2023

FGS Task Manager - How's Zebra supporting developers

- Preventing users to pull down the status bar
- Zebra MX API "UI Manager / Status Bar Disable" (Stagenow, EMDK)

FGS start-up

- Only foreground activities can start a FGS
- Exemption list - Respond to one of the following events
  - ACTION_BOOT_COMPLETED, ACTION_LOCKED_BOOT_COMPLETED, ACTION_MY_PACKAGE_REPLACED
  - Hint: Mark the FGS as android:***directBootAware***="true“
    Start the FGS immediately or you get *ForegroundServiceStartNotAllowedException*

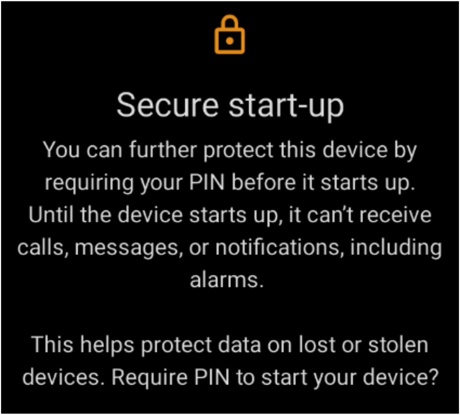
Zebra updates for FGS & Direct boot

Direct Boot - Impact on Developers

Zebra
DevCon 2023

- Additional security improvements in Android 13
  - Google removed support for Full Disk Encryption (FDE)
  - OEMs must now implement a File-based Encryption (FBE) filesystem
- Impact on developers: after a reboot, only a portion of the filesystem and system resources are available until the device is unlocked
- FDE / FBE behavior according to different Android versions:

Android 11, FDE,
Secure Startup prompt



Secure start-up

You can further protect this device by requiring your PIN before it starts up. Until the device starts up, it can't receive calls, messages, or notifications, including alarms.

This helps protect data on lost or stolen devices. Require PIN to start your device?

Android 13 PIN/Password/Pattern ON	~~FULL DISK ENCRYPTION~~	FILE-BASED ENCRYPTION
	~~Secure Start-up ON~~ ~~Apps prevented to run before 1st unlocking~~ ~~Normal mode after unlocking~~	**Direct-boot** mode on before 1st unlocking, Normal mode after unlocking ✓
	~~Secure Start-up OFF~~ ~~Normal mode (full data access) before and after unlocking~~	~~--No other choices--~~

Android 7 to 11 PIN/Password/Pattern ON	FULL DISK ENCRYPTION	FILE-BASED ENCRYPTION
	Secure Start-up ON ✗ Apps prevented to run before unlocking Normal mode after unlocking	**Direct-boot** mode on before 1st unlocking, Normal mode after unlocking
	Secure Start-up OFF ✓ Normal mode (full data access) before and after unlocking	--No other choices--

Zebra
DevCon 2023

Scoped Storage

Why is Scoped Storage necessary?

To protect

- The user's privacy

How

- Scoped storage changes the way apps store and access files on a device's external storage

Best practices guide

- Android storage use cases and best practices - d.android.com/training/data-storage/use-cases

Request all-files access (Google Play restricted)

- An app can request all-files access from the user by doing the following:
  - Declare the `MANAGE_EXTERNAL_STORAGE` permission in the manifest.
  - Use the `ACTION_MANAGE_ALL_FILES_ACCESS_PERMISSION` intent action to direct users to a system settings page where they can enable the following option for your app: *Allow access to manage all files.*

Zebra updates on Storage

Availability of public folders

- Google security tightening to data sharing use-cases
  - Started with Android 10 and the Scoped storage enforcement
  - Android 13 even increasing focus on users' privacy
- Security weaknesses like
  - Trusted files renaming
  - Files substituting
  - Improper app clean-up on uninstalling
  - are a threat to folders like
    - /enterprise/usr
    - /data/tmp/public
- Everything's still in place in Android 13
  - It's time however to review your apps' storage strategy!

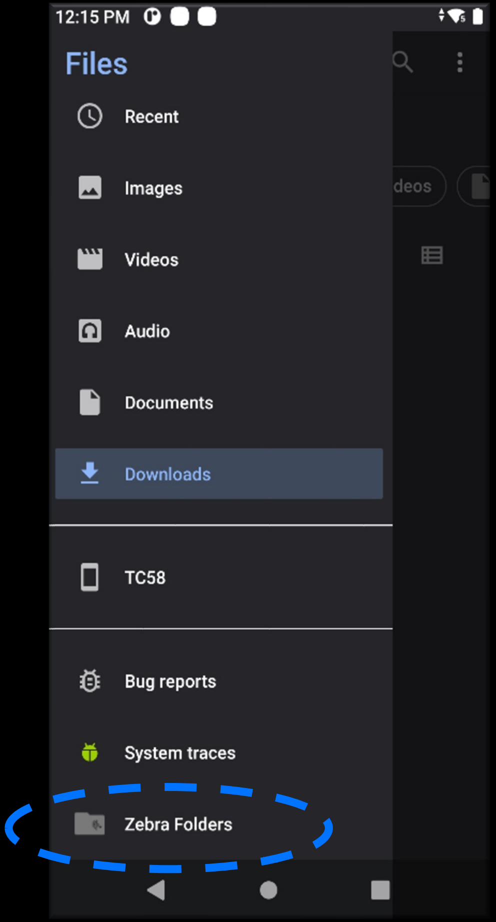
Apps Storage strategy: more time to review it!

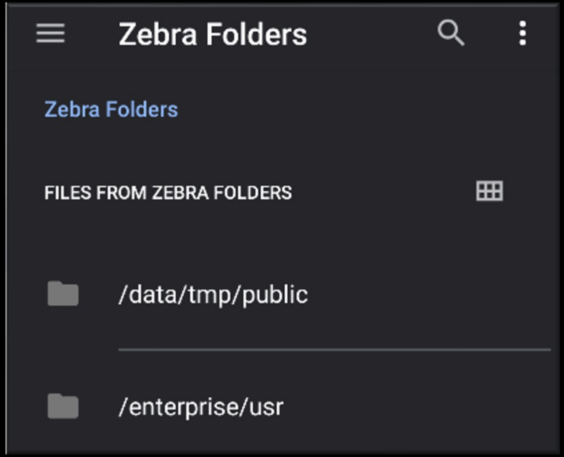
Zebra updates on Storage

File Browser app

Zebra has now released a new fully-featured File-browsing app to access the Zebra folders

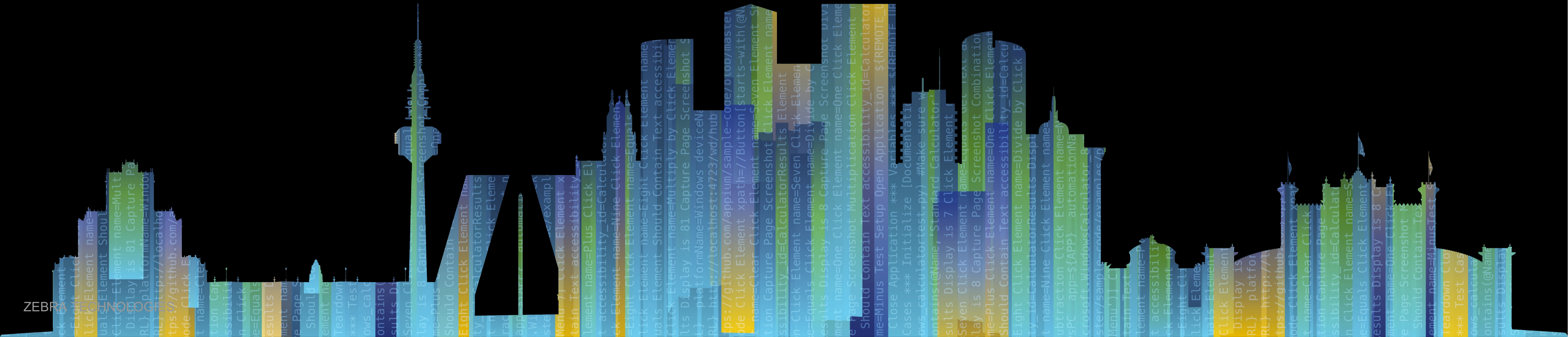
- Navigate to Settings / Storage
- Tap Documents & other
- Choose “Open with Files”
- The Zebra folders icon is found on the bottom-left side of the screen and gives access to /data/tmp/public and /enterprise/usr





Zebra
DevCon 2023

Package Visibility



Package Visibility

For app targets Android 11 (API level 30) or higher

Google Play considers the list of installed apps to be personal and sensitive user data

Types of apps that are visible automatically

- Your own app.
- Certain system packages, such as the media provider, that implement core Android functionality.
- The app that installed your app.
- Any app that launches an activity in your app using the startActivityForResult() method, as described in the guide about getting a result from an activity.
- Any app that starts or binds to a service in your app.
- Any app that accesses a content provider in your app.
- Any app that has a content provider that your app has been granted URI permissions to access.
- Any app that receives input from your app. This case applies only when your app provides input as an input method editor.

To query all apps (not recommended)

To allow your app to see all other installed apps, the system provides the QUERY_ALL_PACKAGES permission

Package Visibility

For app targets Android 11 (API level 30) or higher

Zebra DevCon 2023

For example: Accessing package information about the current Mainline modules

```
private fun mainlineVersion(context: Context): String? {
    val moduleProvider = "com.google.android.modulemetadata"

    return try {
            val pm = context.packageManager
            val packageInfo = pm.getPackageInfo(moduleProvider, 0)
            packageInfo.versionName
        } catch (e: PackageManager.NameNotFoundException) {
            null
        }
}

<manifest package="com.example.app">
    <queries>
        <package android:name="com.google.android.modulemetadata" />
    </queries>
    ...
</manifest>
```

Package Visibility

For app targets Android 11 (API level 30) or higher

Test package visibility issues

```
adb shell pm log-visibility --enable PACKAGE_NAME
```

Whenever packages are filtered out of a `PackageManager` object's return values, you see a message similar to the following in Logcat:

```
I/AppsFilter: interaction: PackageSetting{7654321 \
  com.example.myapp/12345} -> PackageSetting{...} BLOCKED
```

Questions

Zebra
DevCon 2023

ZEBRA

Thank You