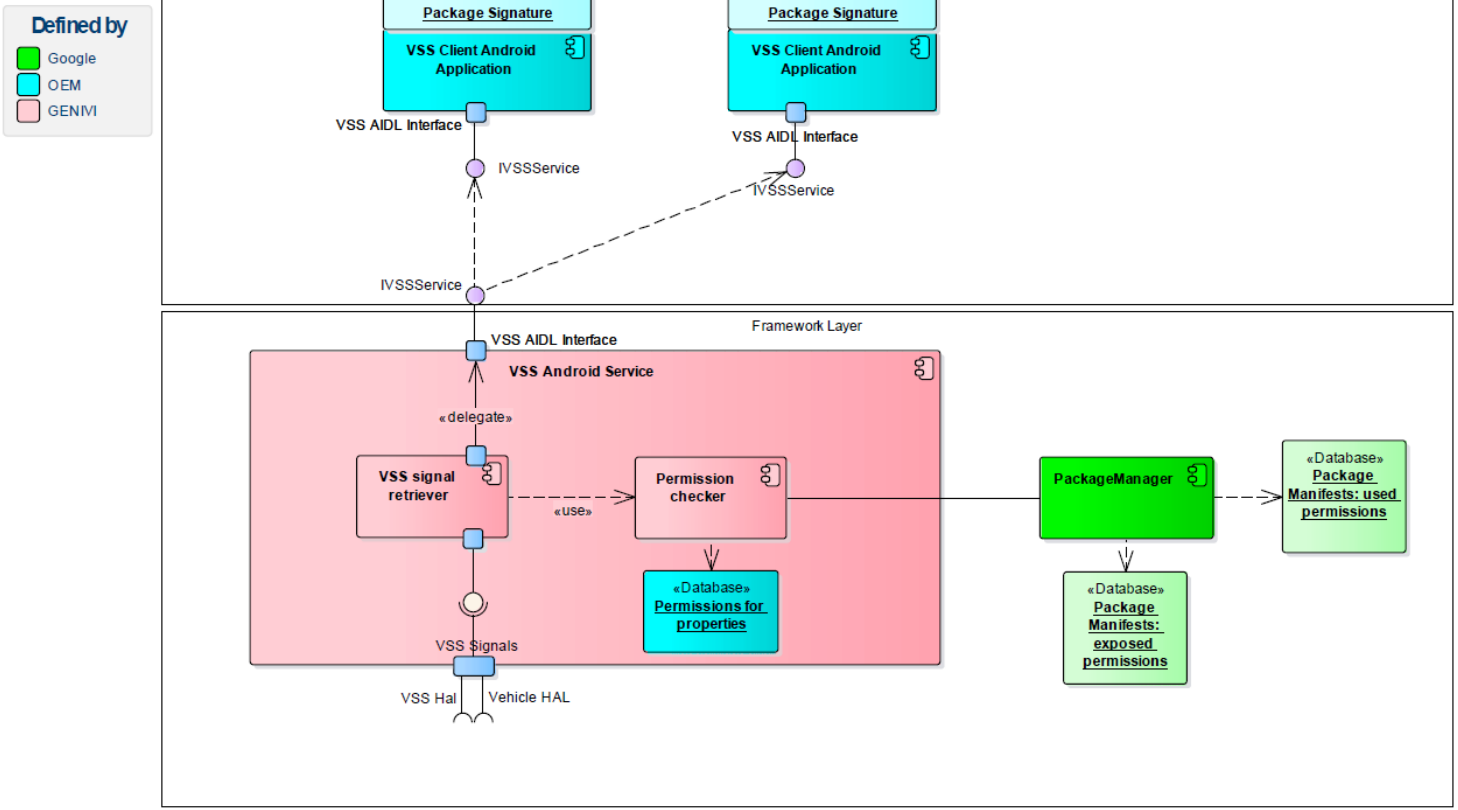
Android custom permission service

Stefan Wysocki

Senior Software Engineer
Tieto
stefan.wysocki@tieto.com

tieto

Overview



Overview

- Exposed permissions can be configured to be available for system applications or signed with the same key as platform or VSS Android Service
- This allows OEMs to staticaly control the apps that will use the VSS signals by signing the application with needed key
- User is able to see and grant permission by itself for given packages in runtime

Permission control

- Permissions **can*** be granted automaticaly when package signed with specific key
  - If not signed, permission would not be granted
- Permission enforcement for accessing - up to implementation:
  - throw an security exception
  - return dummy value
- When installed:
  - User is able to see the permissions during installation (needs to be implemented by a App Store, if Play Store is not an option)

https://developer.android.com/guide/topics/manifest/permission-element android:protectionLevel

Advantages

- Mechanism already known for Android application developers, existing in the platform
- Permission database well known and secured across Android
- Easy certification process for apps. By declaring used permissions, OEM could see it all „at glance” by checking the Application AndroidManifest.xml
- Additional „harness” for app developers to not accidentaly exceed their permissions

Disadvantages

- Not able to „specialize” the properties. Different signing keys for different purpouses and access levels
- No temporary permissions granted for specific sessions

Stefan Wysocki

Senior Software Engineer
Tieto
stefan.wysocki@tieto.com