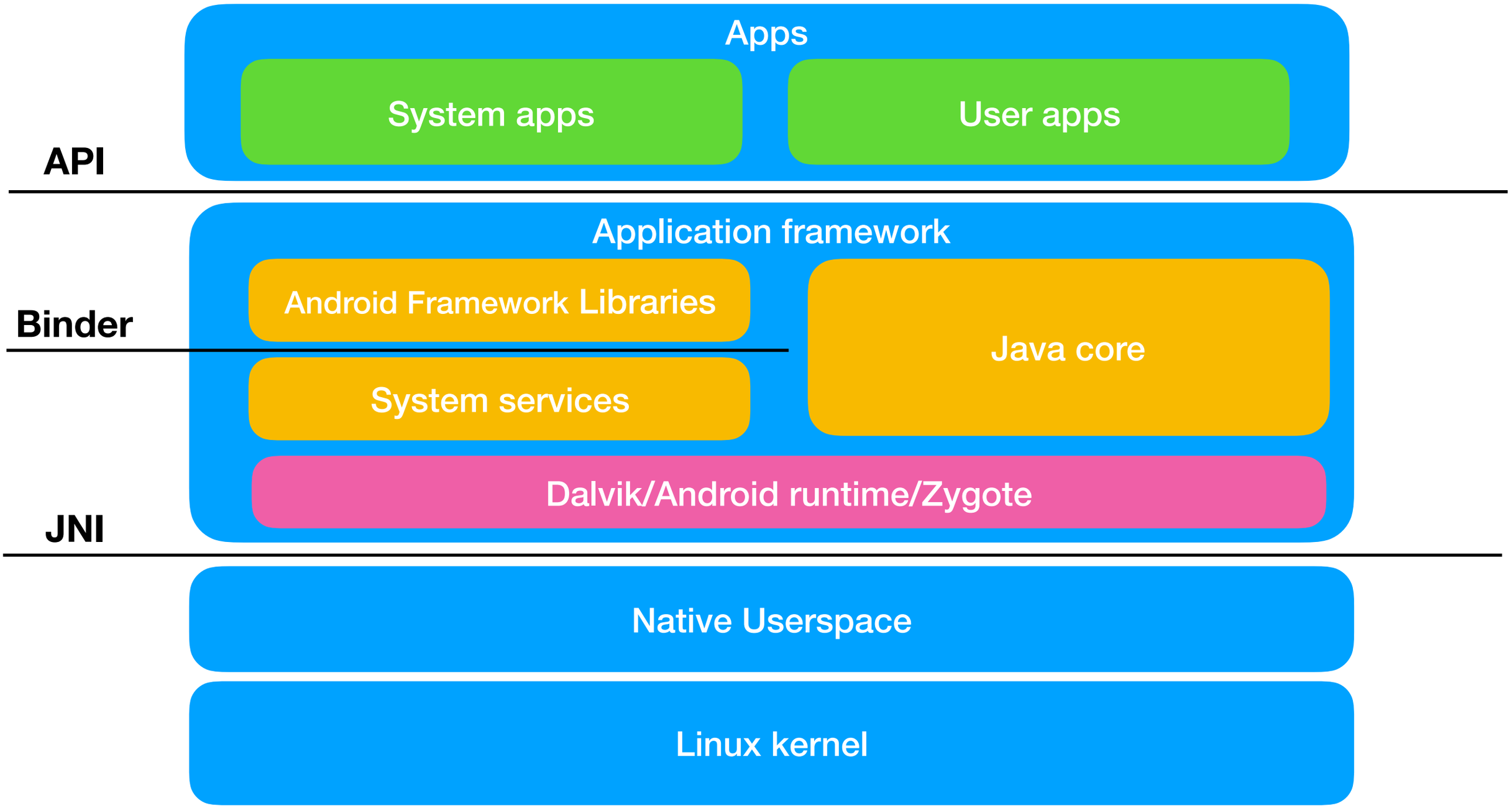
Взгляд из песочницы

Кирилл Филимонов
Mail.Ru Group

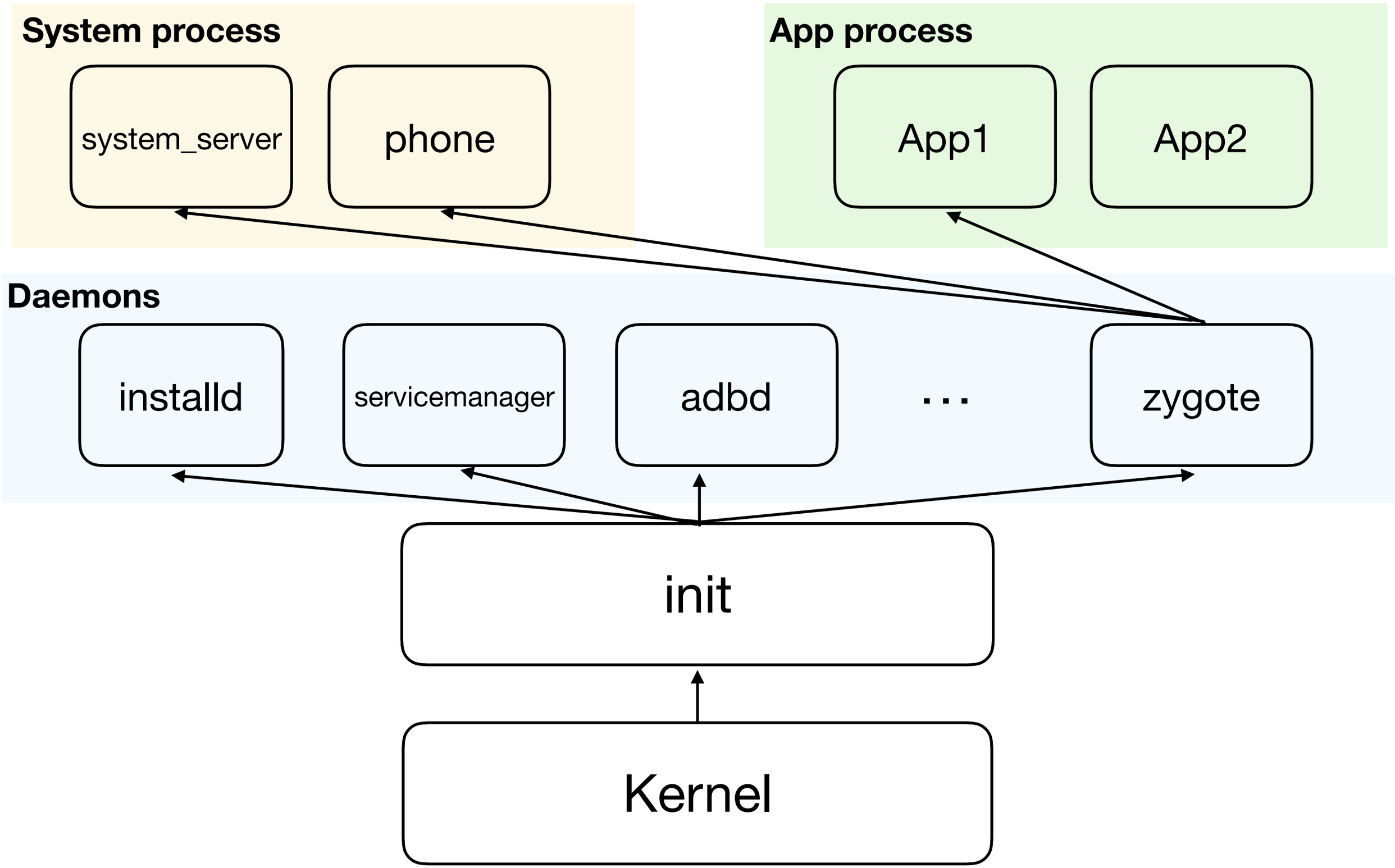
Структура ОС



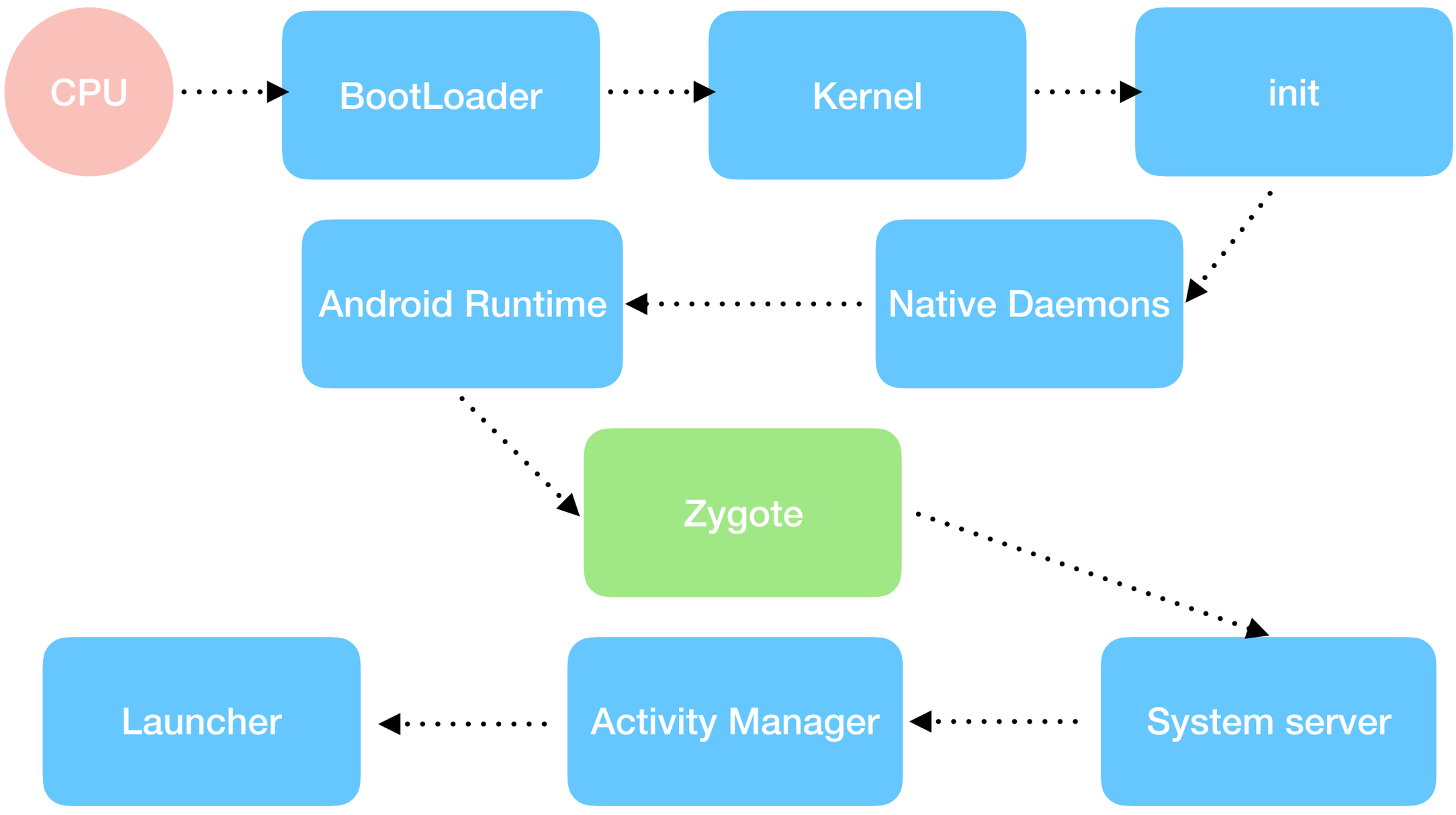
Linux kernel

- Binder
- Anonymous Shared Memory (ashmem)
- Wakelocks
- Low-Memory Killer
- Alarm
- Logger

Иерархия процессов



Запуск ОС


CPU
BootLoader
Kernel
init
Android Runtime
Native Daemons
Zygote
Launcher
Activity Manager
System server

Запуск ОС

BootLoader

- Поддержка основного оборудования (основные драйверы)
- Поиск и загрузка ядра
- Загрузка в режиме восстановления

Запуск ОС

Kernel

- Инициализация MMU и I/O
- Инициализация драйверов
- Инициализация демонов и поток ядра
- Монтирование корневой файловой системы
- Запуск пользовательского процесса init

Запуск ОС

init

- Ключевой процесс инициализации Android
- Выполнение app_process, запуск VM (Zygote)
- Запуск нативных демонов
- Запуск system_server

Запуск ОС

Zygote

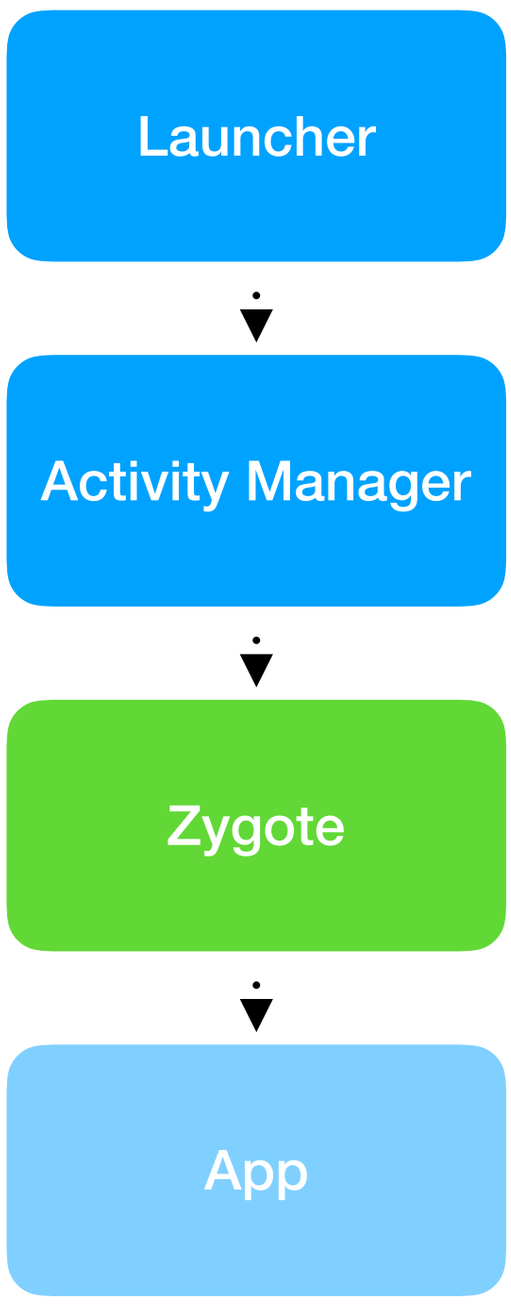
- Запуск Android runtime
- запуск VM
- Выполнение ZygoteInit
- Запуск профилировщика
- Регистрация сокета
- загрузка Java классов
- загрузка ресурсов
- запуск system_server (forkSystemServer)

Запуск ОС

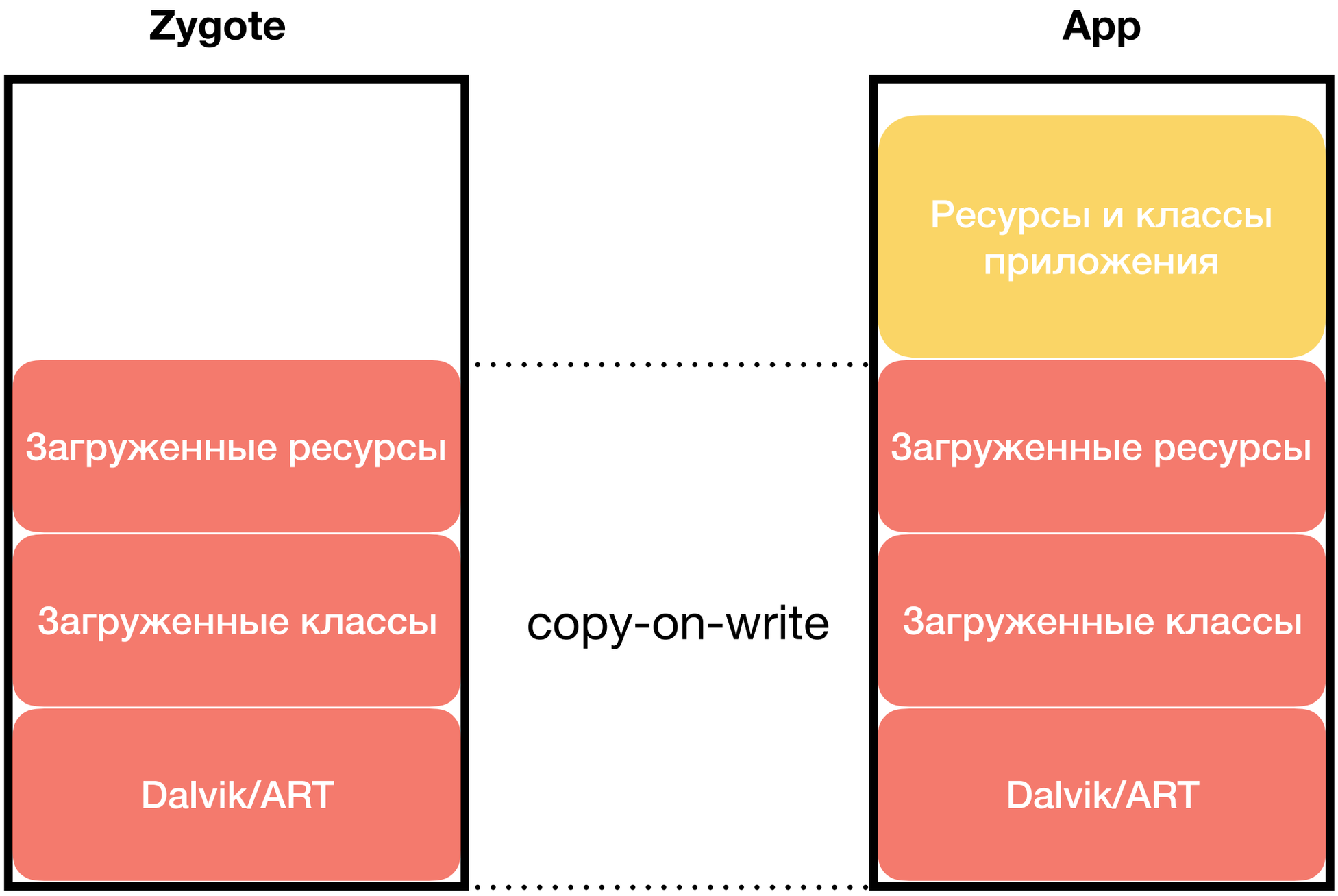
system_server

- инициализация сервисов
- регистрация в service manager
- запуск activity manager
- запуск package manager
- запуск window manager
- запуск power manager

Запуск приложения



Запуск приложения



Sandboxing

- Уникальные UID и GID
- Не изменяются
- Используется DAC
- Изолированное адресное пространство

IPC

Linux

- pipes
- message queue
- shared memory

Android

- binder

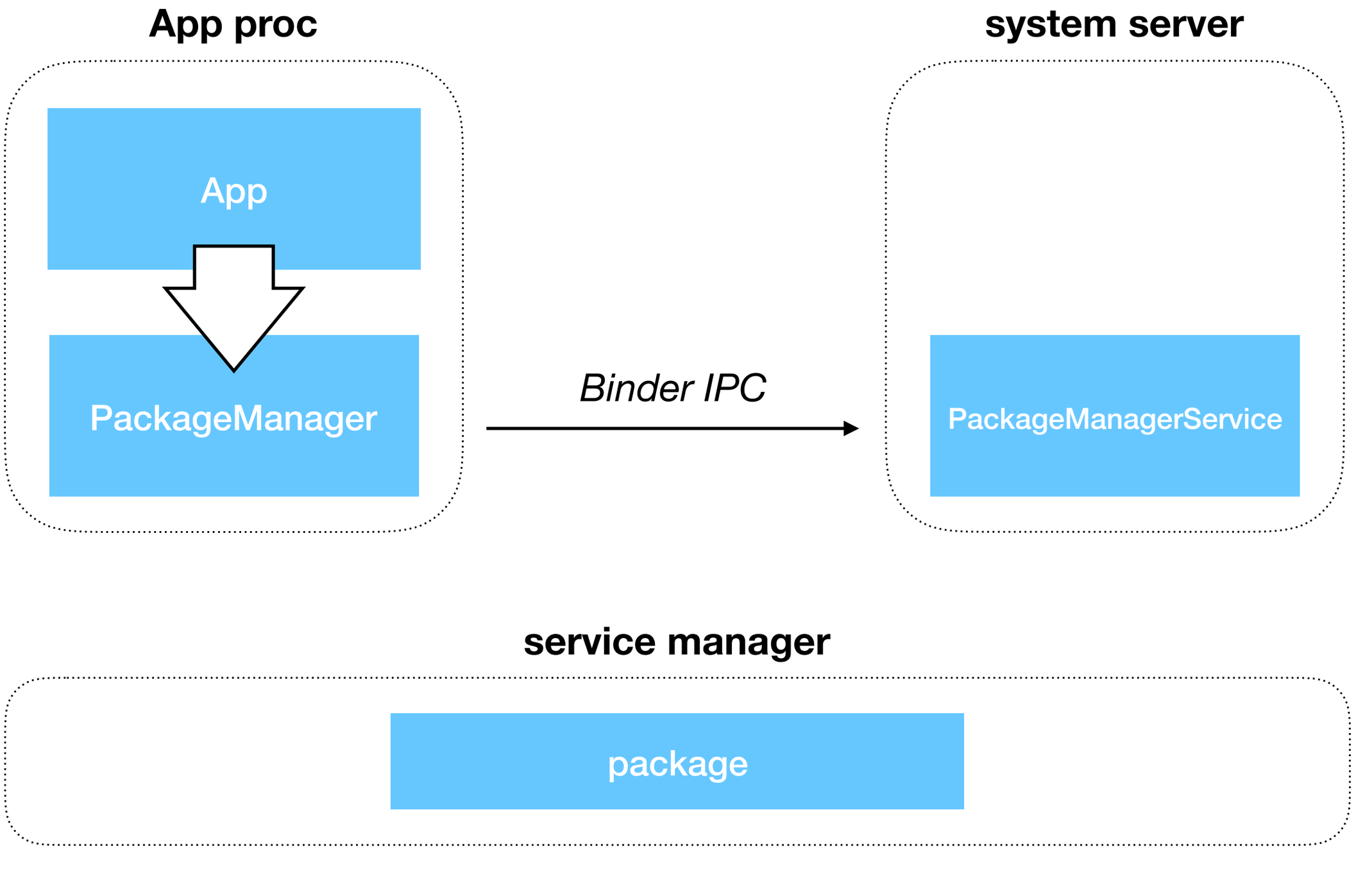
Binder

- Драйвер ядра для обеспечения IPC
- Легковесный RPC
- Пул потоков для обработки запросов
- Поддержка передачи файловых дескрипторов
- Синхронный и асинхронный вызов методов
- Синхронное взаимодействие между потоками

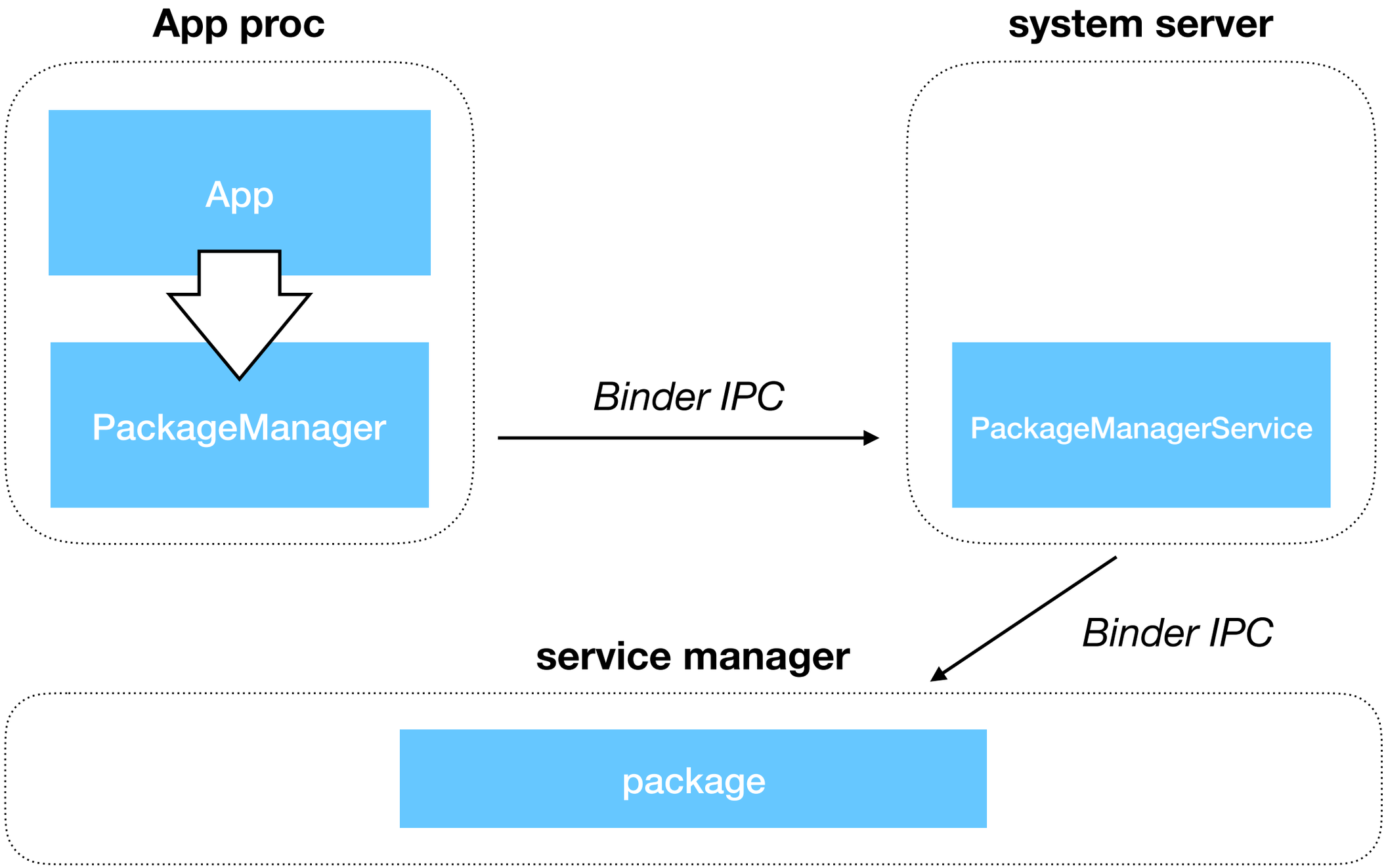
Package Manager

- Парсинг APK файлов
- Установка, обновление, удаление приложений
- Предоставляет информацию об установленных приложениях и разрешениях

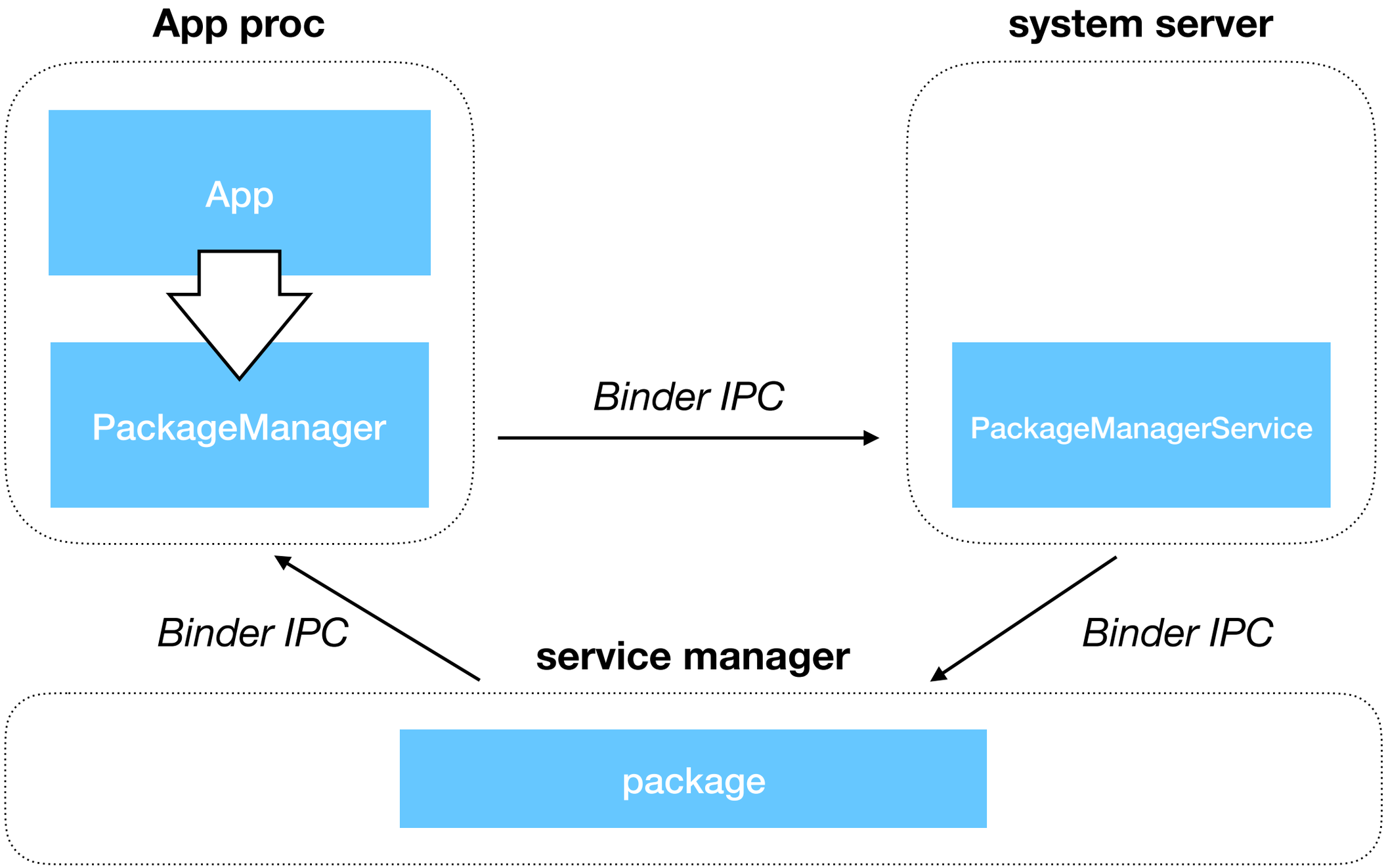
Взаимодействие со службами



Взаимодействие со службами



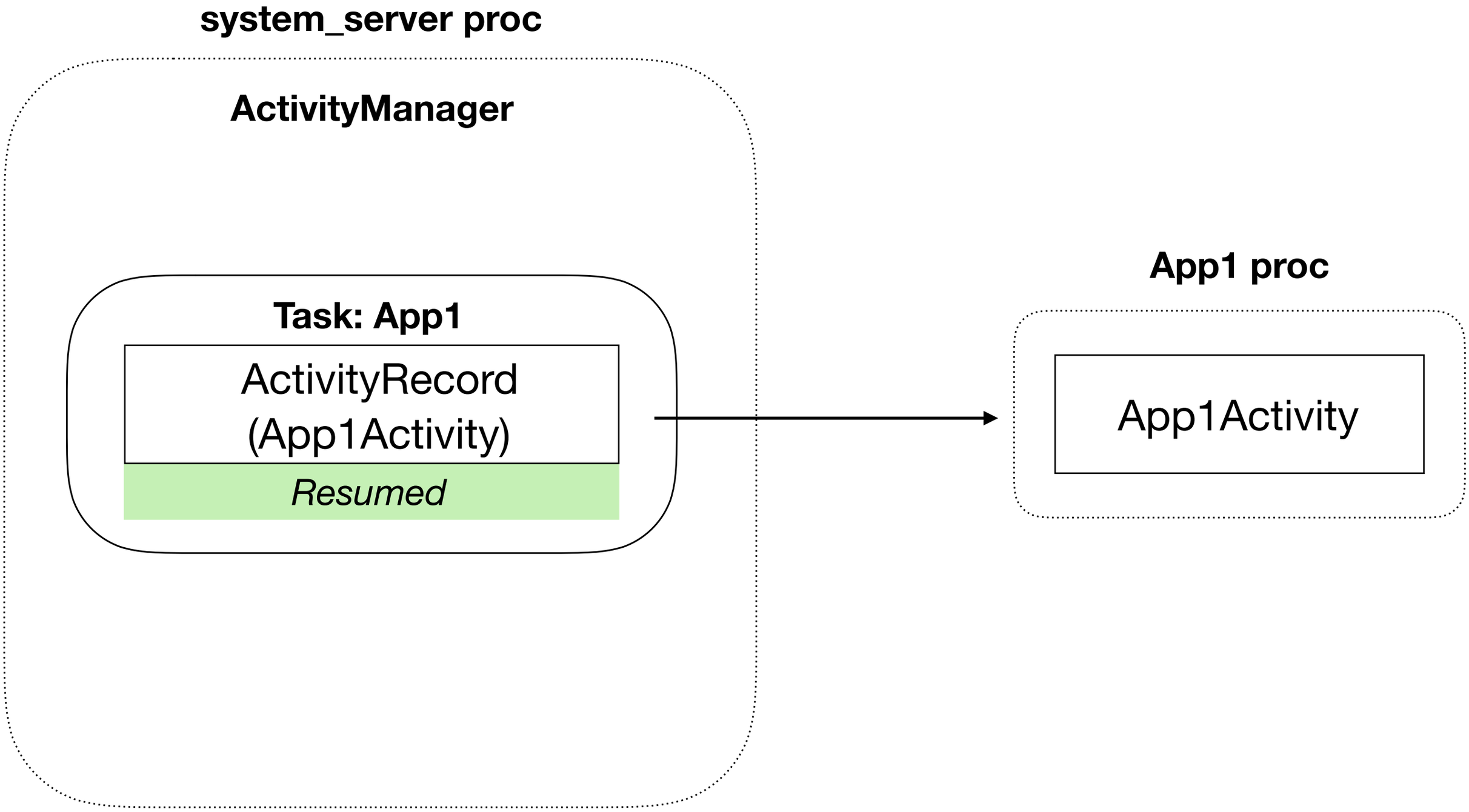
Взаимодействие со службами



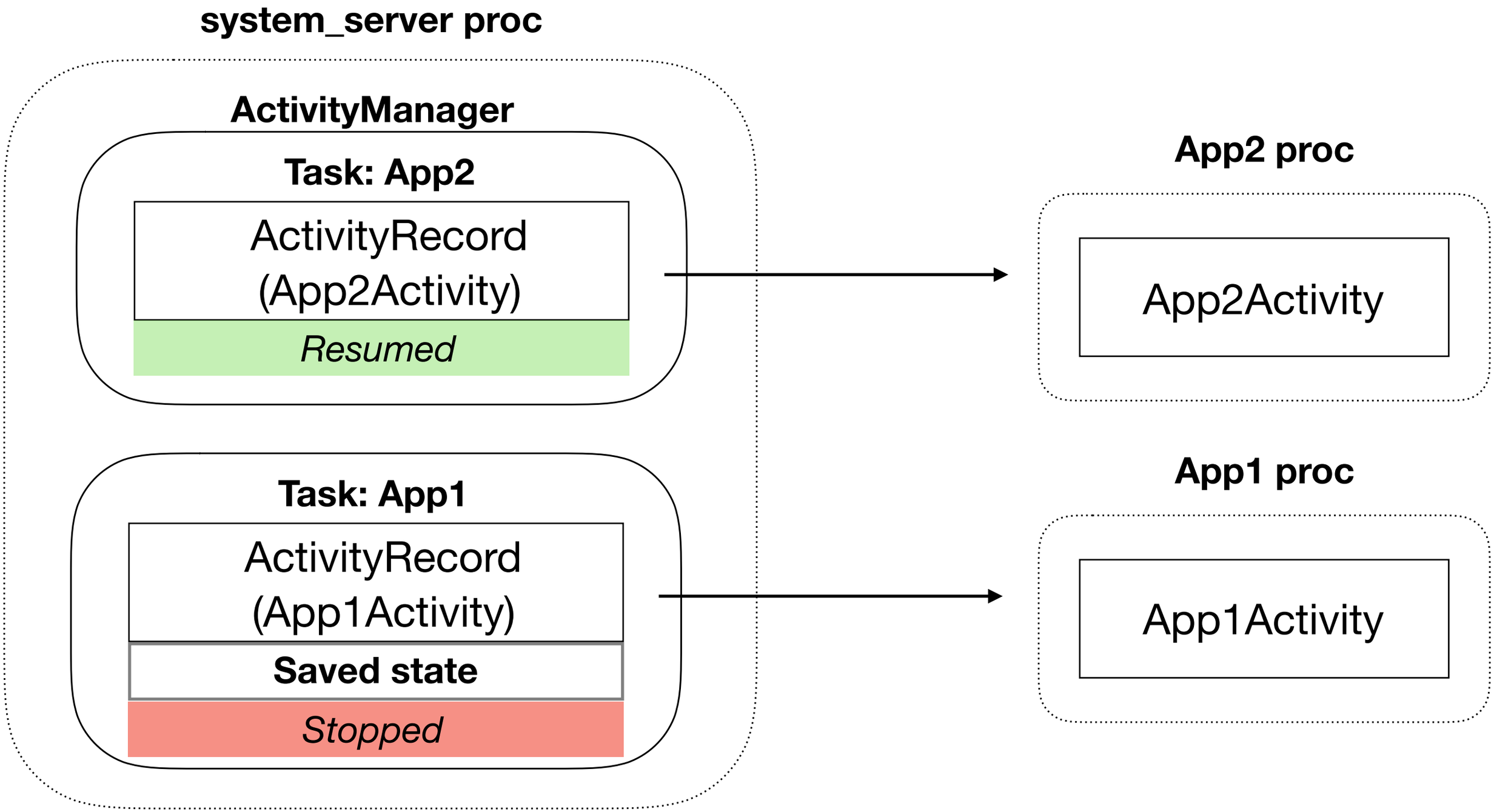
Activity Manager

- Запуск activity и service
- Получение поставщиков данных
- Рассылка интентов
- Обслуживание OOM adj
- Управление жизненным циклом
- Управление тасками
- Обработка ANR
- Разрешения

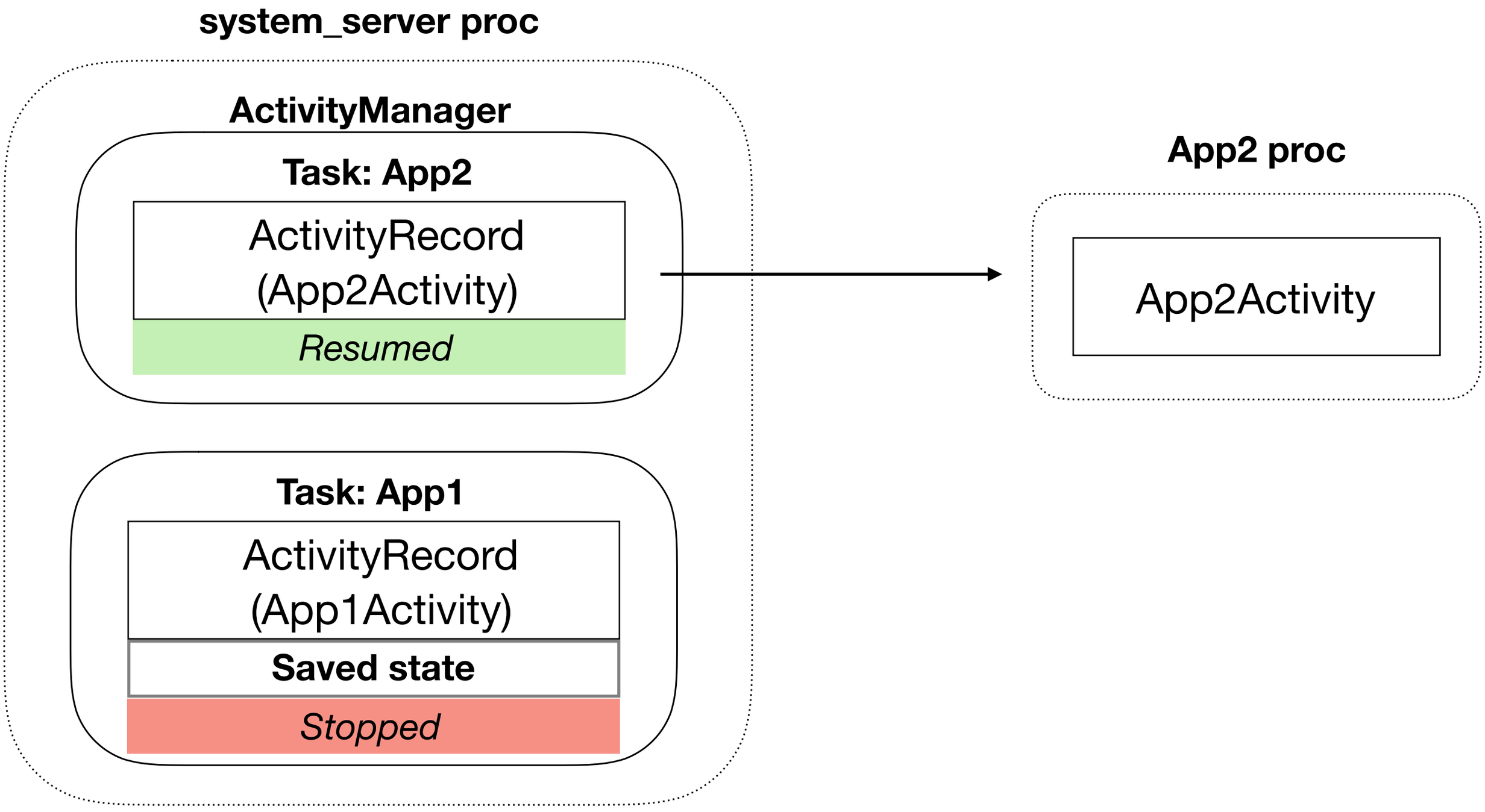
Activity


system_server proc
ActivityManager
Task: App1
ActivityRecord
(App1Activity)
Resumed
App1 proc
App1Activity

Activity


system_server proc
ActivityManager
Task: App2
ActivityRecord
(App2Activity)
Resumed
Task: App1
ActivityRecord
(App1Activity)
Saved state
Stopped
App2 proc
App2Activity
App1 proc
App1Activity

Activity


system_server proc
ActivityManager
Task: App2
ActivityRecord
(App2Activity)
Resumed
Task: App1
ActivityRecord
(App1Activity)
Saved state
Stopped
App2 proc
App2Activity

system_server proc

ActivityManager

Task: App2

ActivityRecord
(App1NewActivity)

Resumed

ActivityRecord
(App2Activity)

Saved state

Stopped

Task: App1

ActivityRecord
(App1Activity)

Saved state

Stopped

App1 proc

App1NewActivity

App2 proc

App2Activity

system_server proc

ActivityManager

Task: App1

ActivityRecord
(App1Activity)

Resumed

Task: App2

ActivityRecord
(App2Activity)

Saved state

Stopped

ActivityRecord
(App2Activity)

Saved state

Stopped

App1 proc

App1Activity

App1NewActivity

App2 proc

App2Activity

Service

system_server proc

ActivityManager

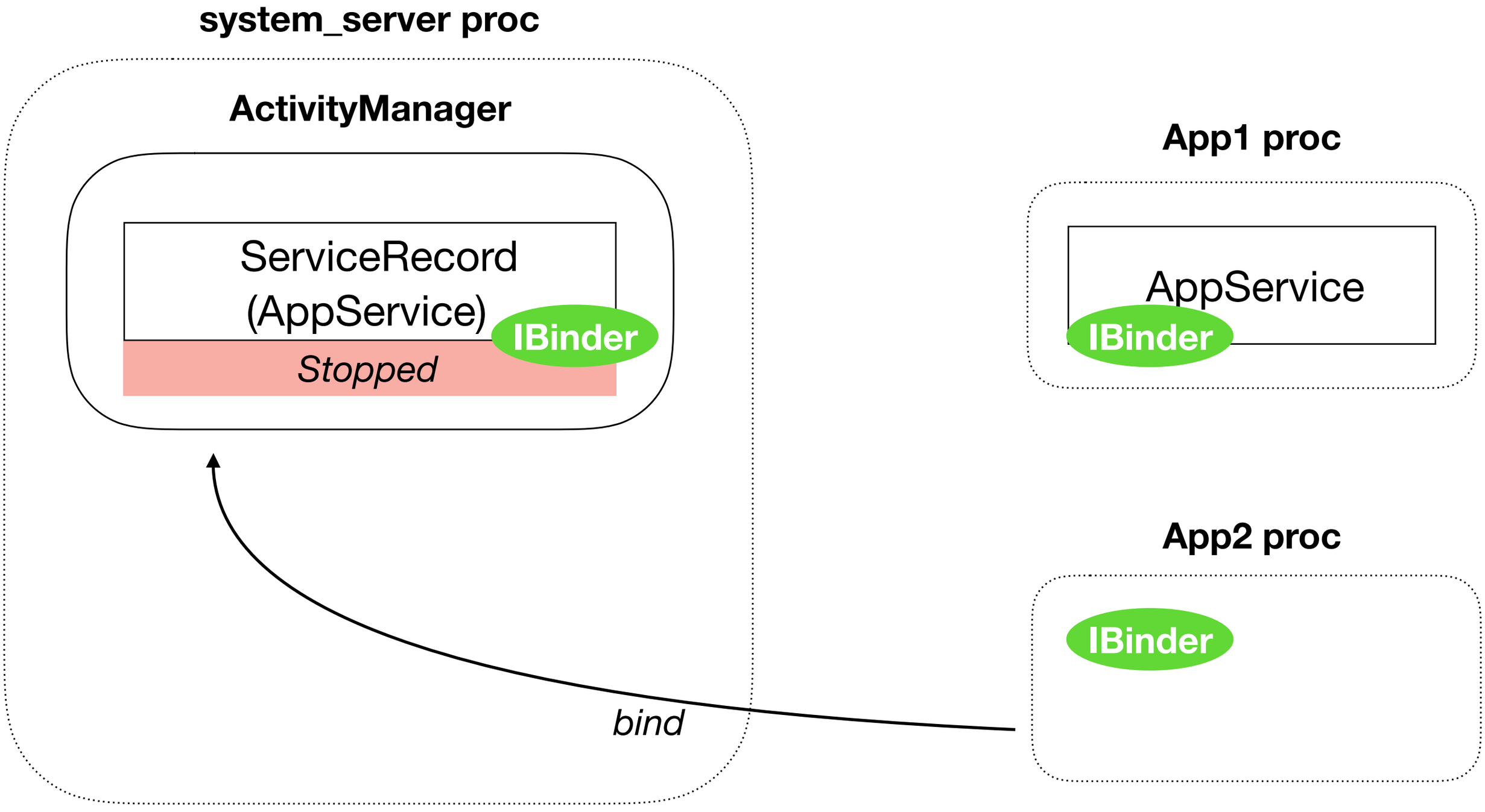
ServiceRecord
(AppService)

Stopped

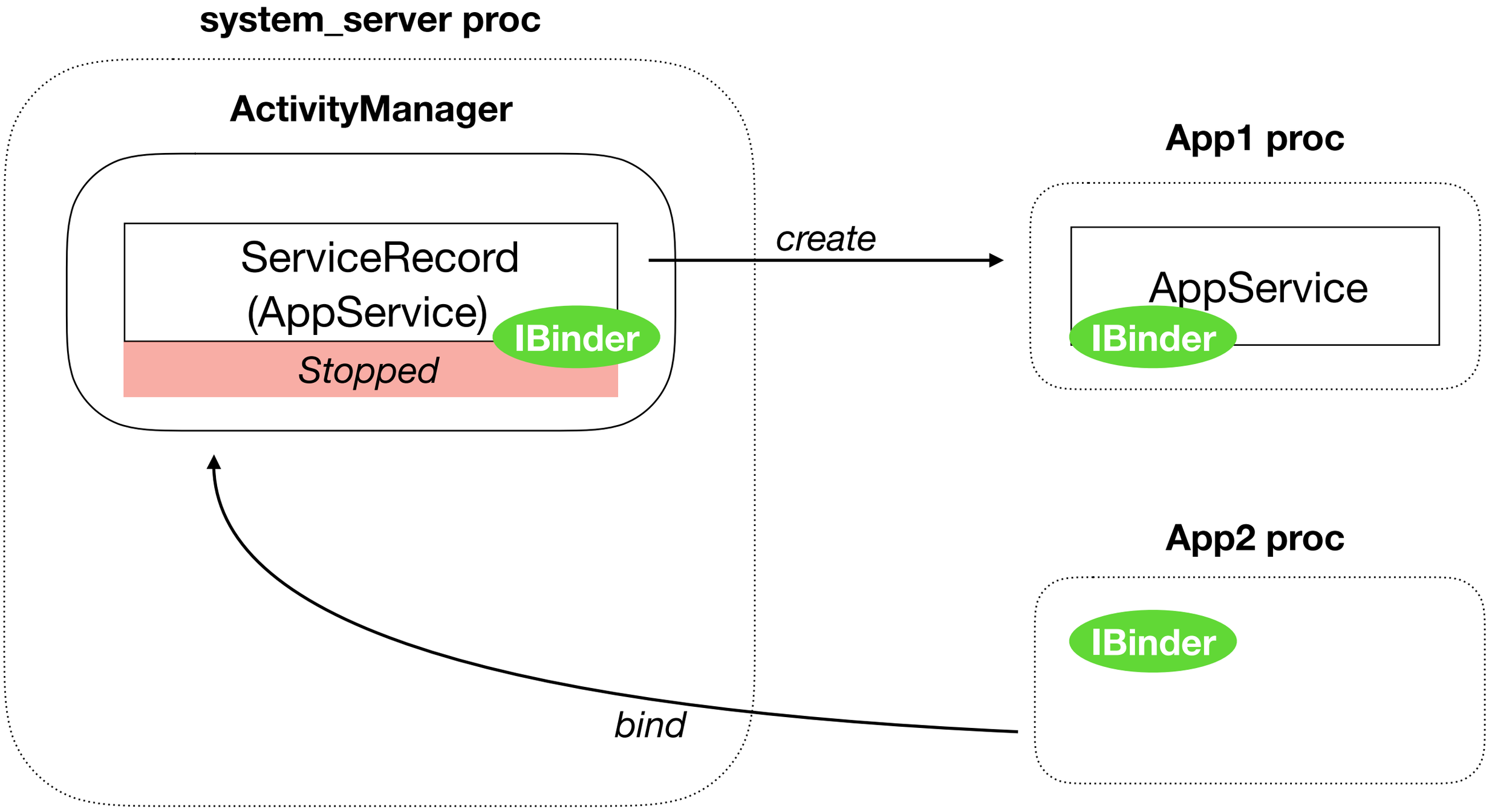
App1 proc

AppService

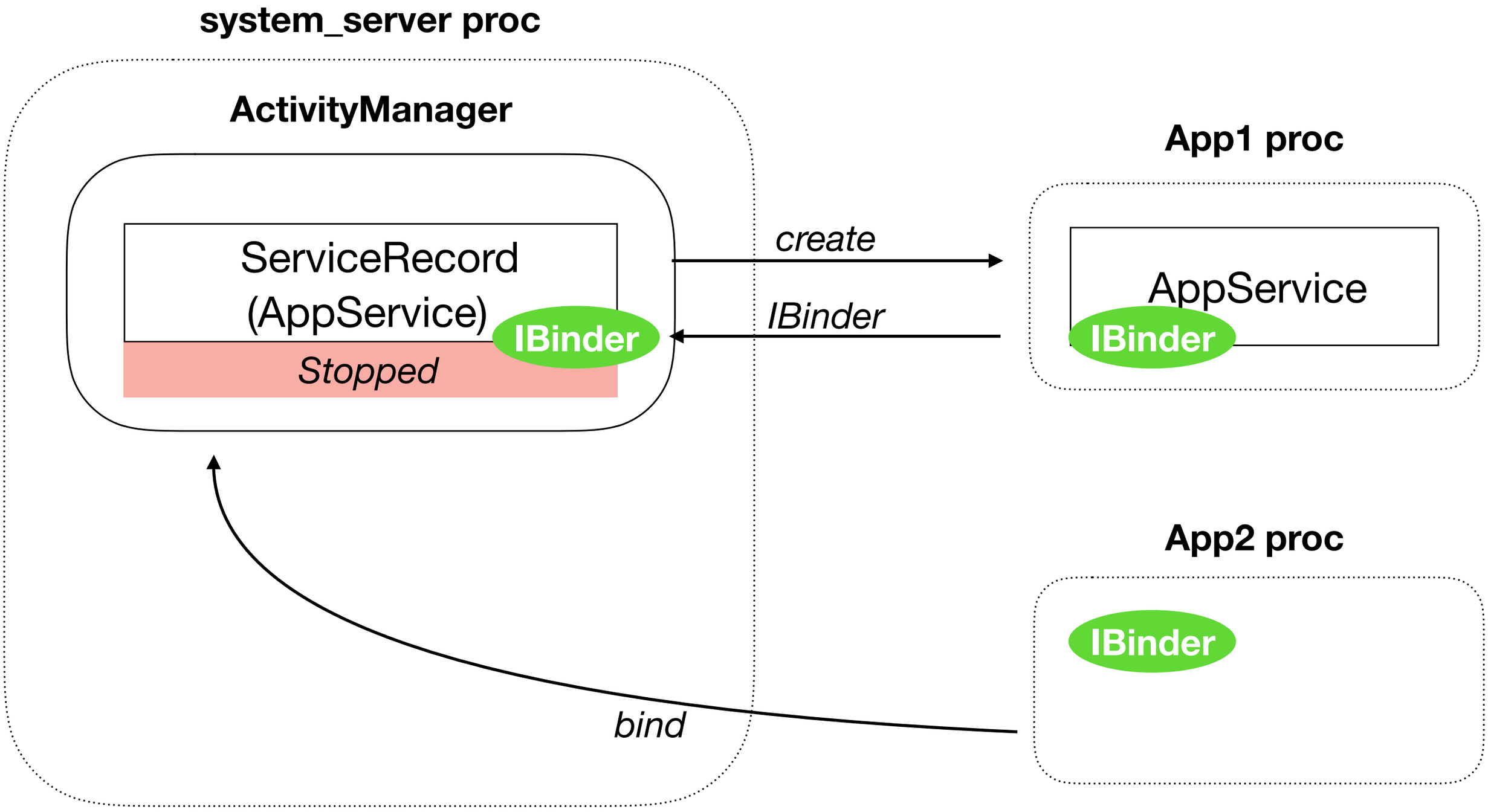
Binding


system_server proc
ActivityManager
ServiceRecord
(AppService)
IBinder
Stopped
App1 proc
AppService
IBinder
App2 proc
IBinder
bind

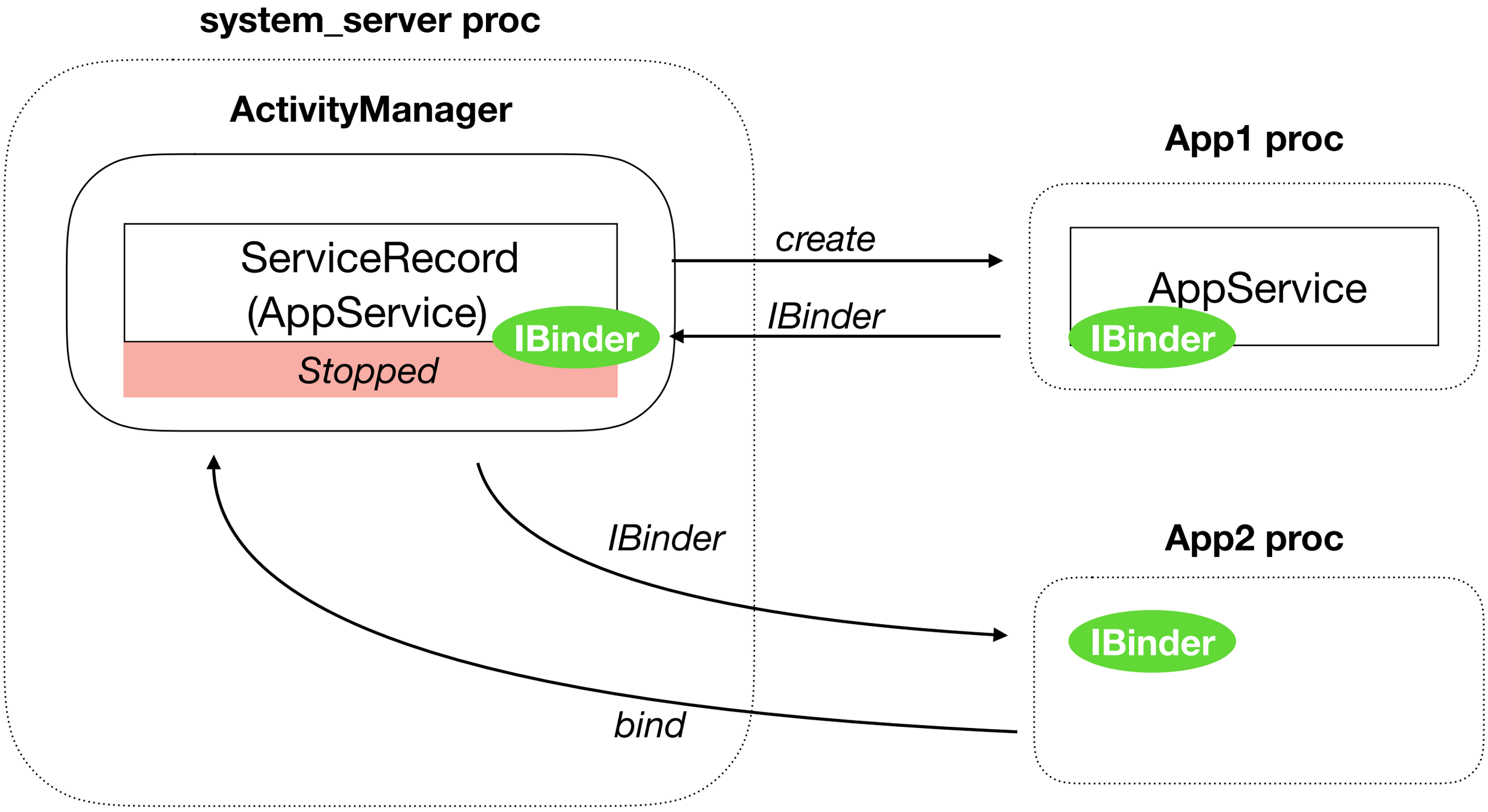
Binding


system_server proc
ActivityManager
ServiceRecord
(AppService)
IBinder
Stopped
create
App1 proc
AppService
IBinder
App2 proc
IBinder
bind

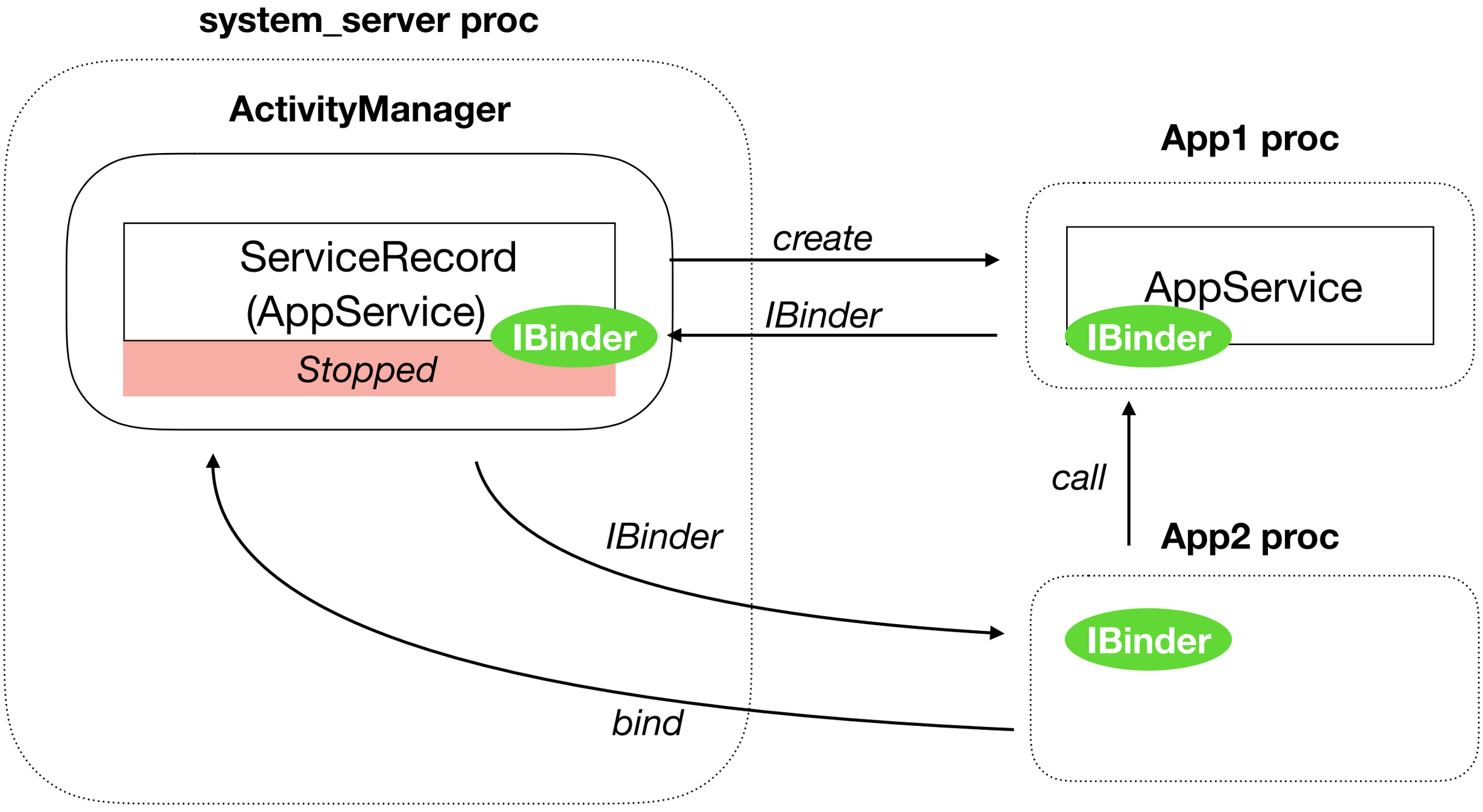
Binding


system_server proc
ActivityManager
ServiceRecord
(AppService)
Stopped
IBinder
create
IBinder
App1 proc
AppService
IBinder
App2 proc
IBinder
bind

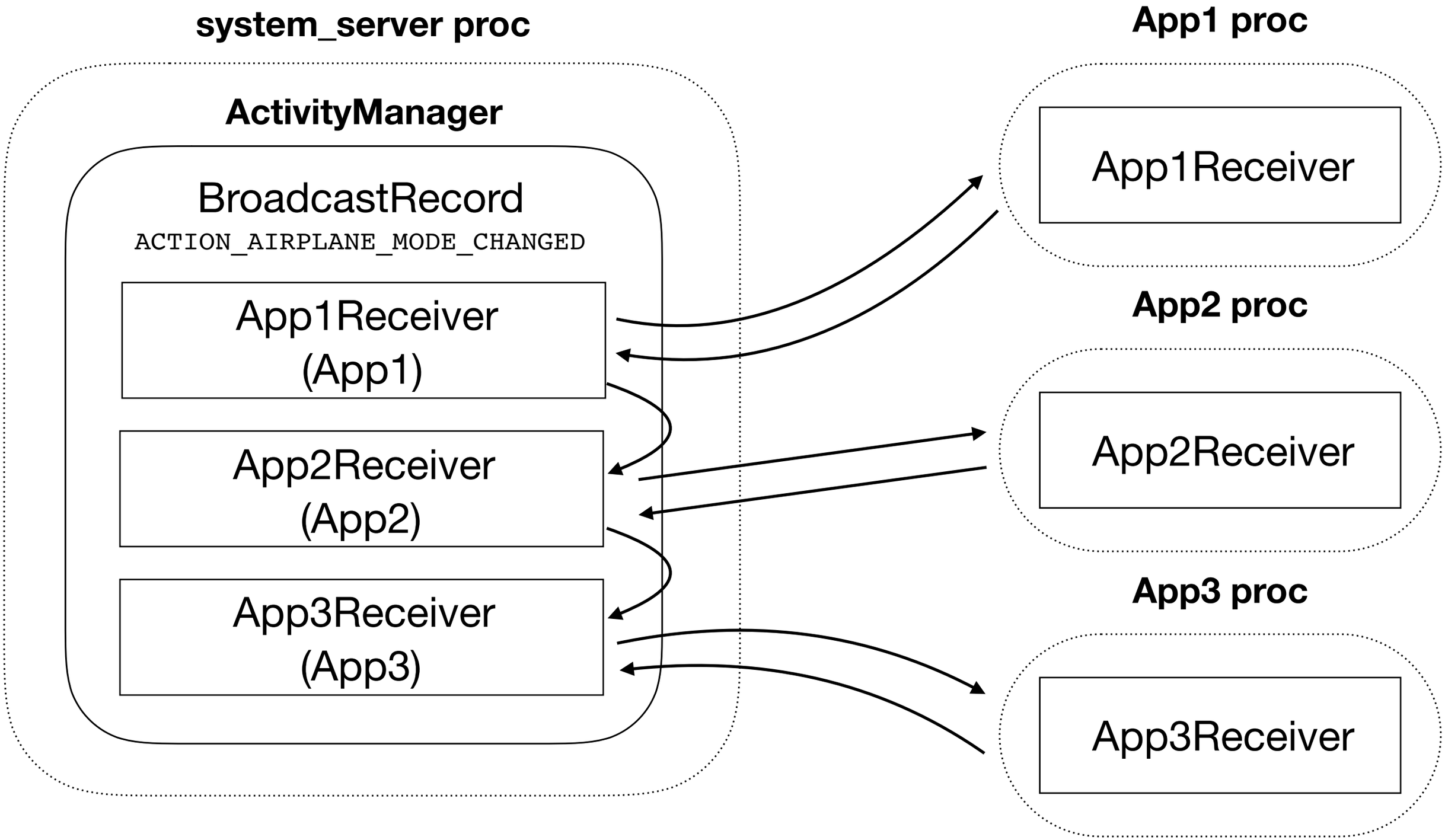
Binding


system_server proc
ActivityManager
ServiceRecord
(AppService)
Stopped
IBinder
create
IBinder
App1 proc
AppService
IBinder
IBinder
bind
App2 proc
IBinder

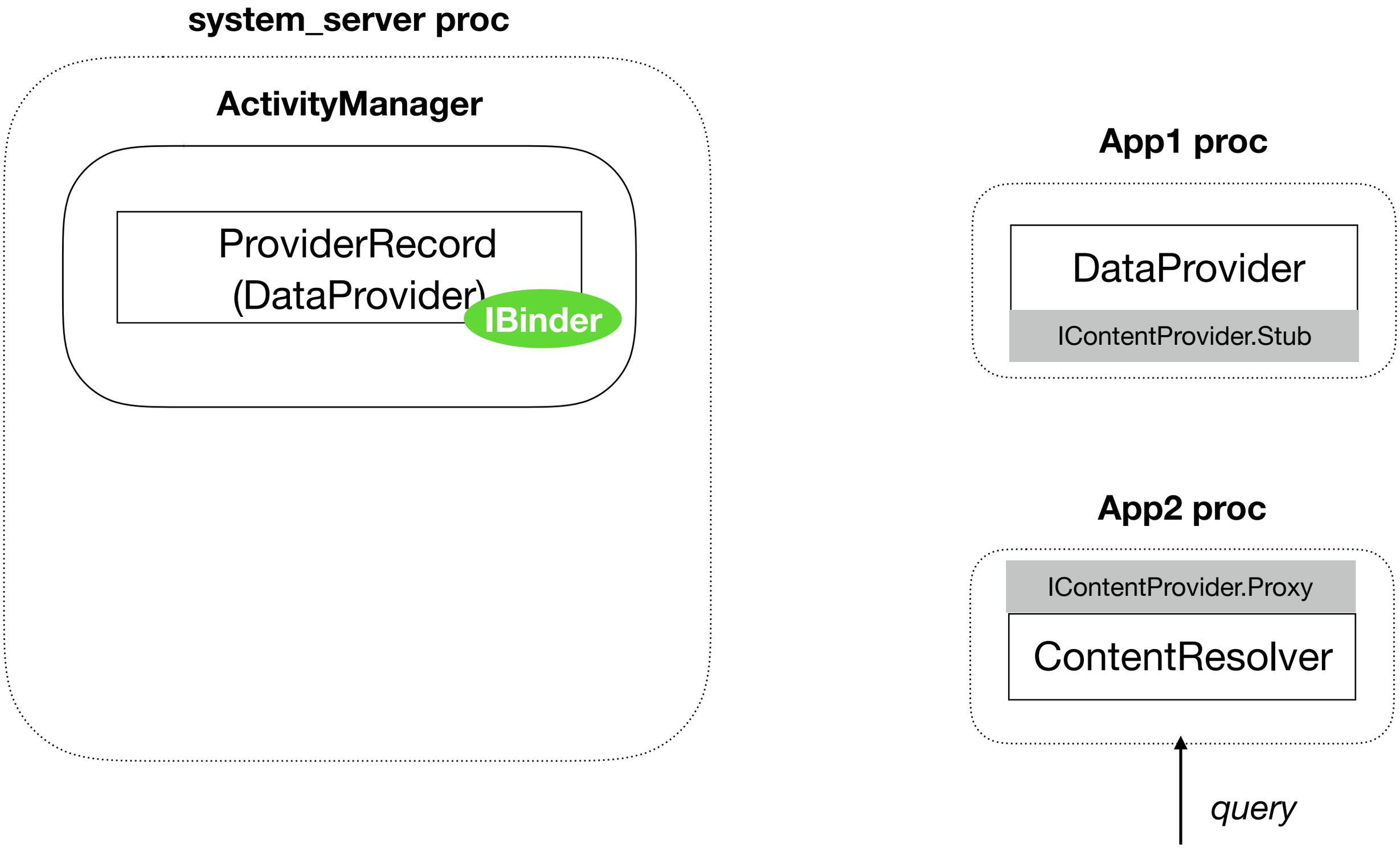
Binding


system_server proc
ActivityManager
ServiceRecord
(AppService)
Stopped
IBinder
create
IBinder
App1 proc
AppService
IBinder
call
App2 proc
IBinder
IBinder
bind

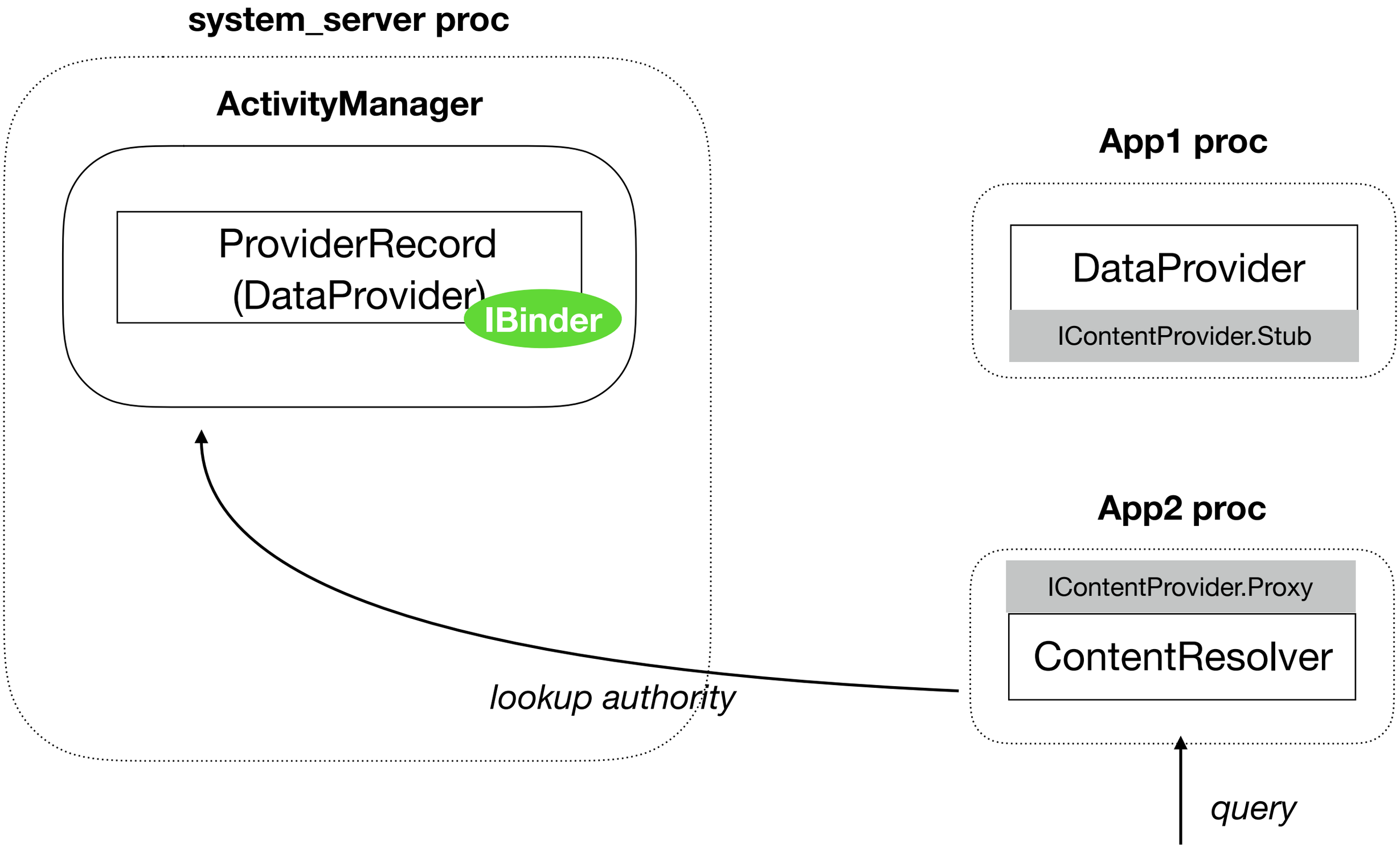
Broadcast Receiver



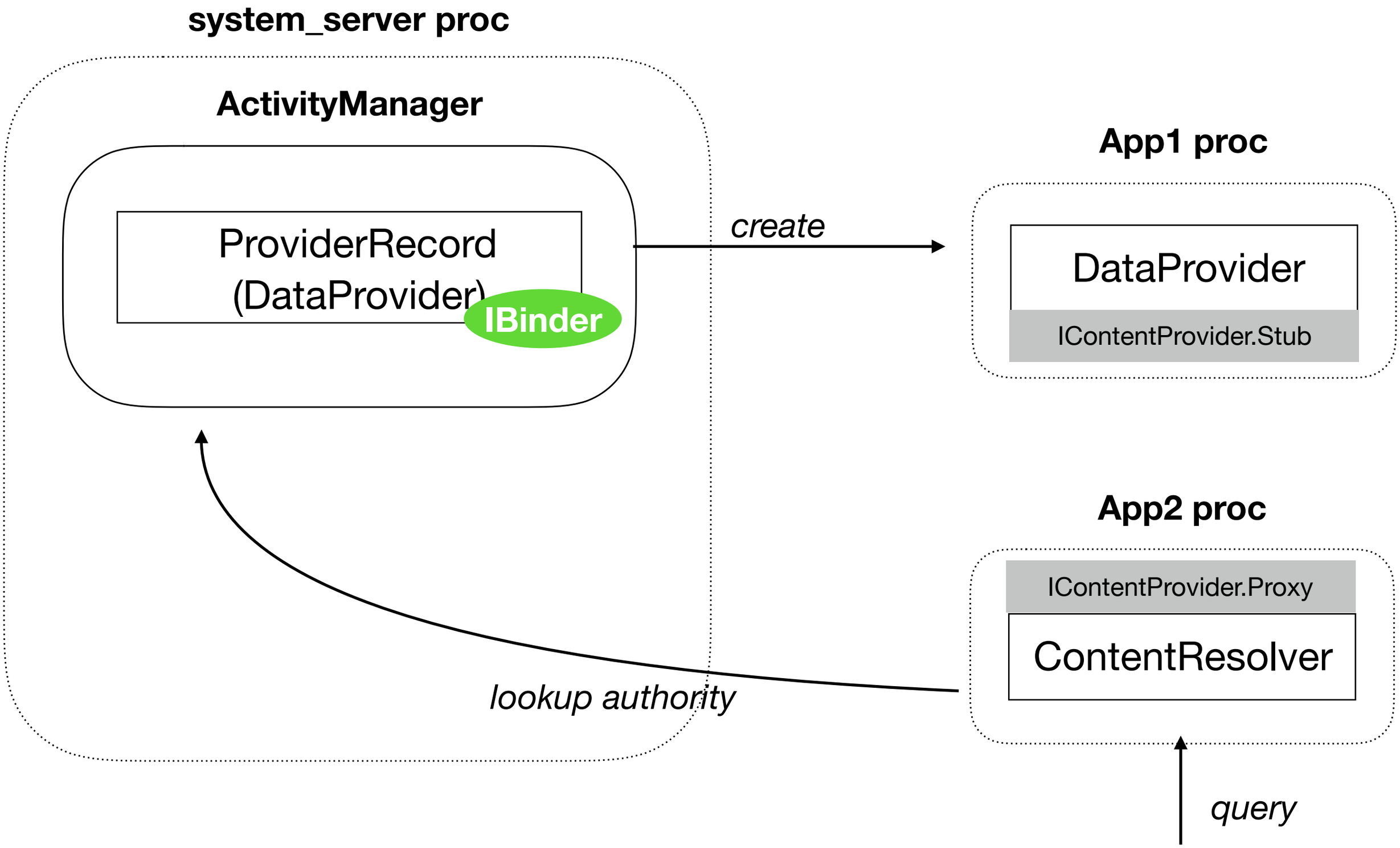
Content Provider



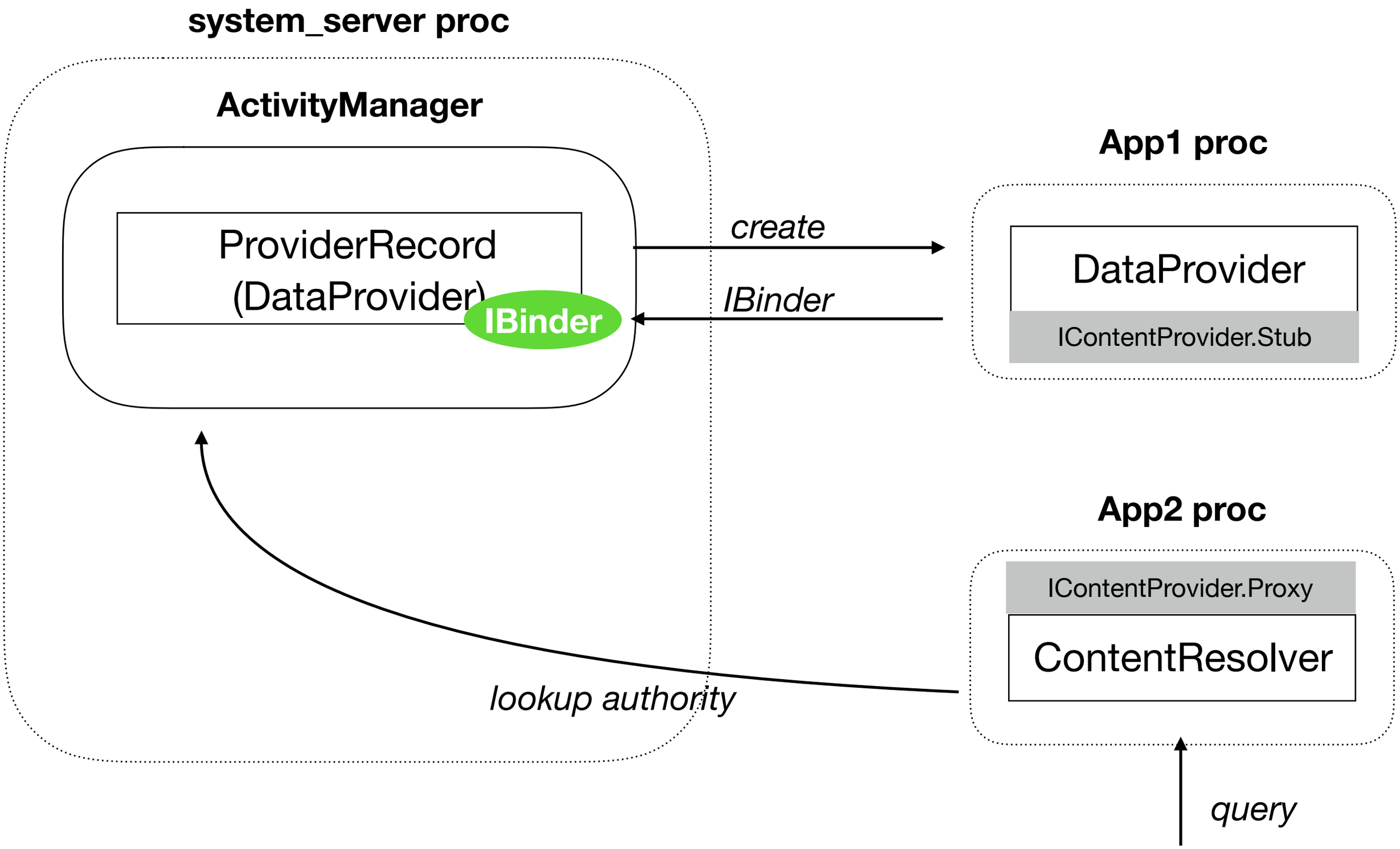
Content Provider



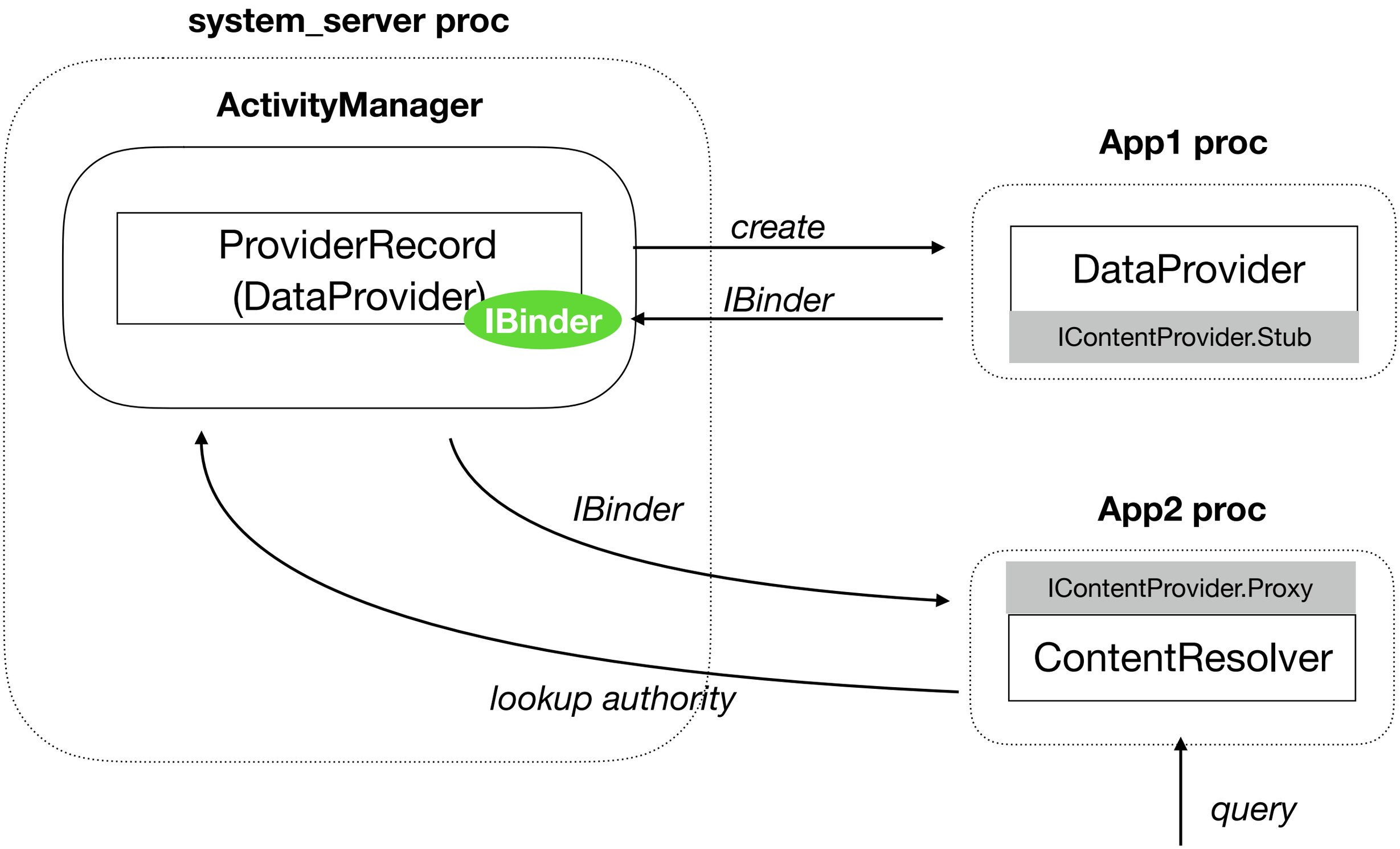
Content Provider



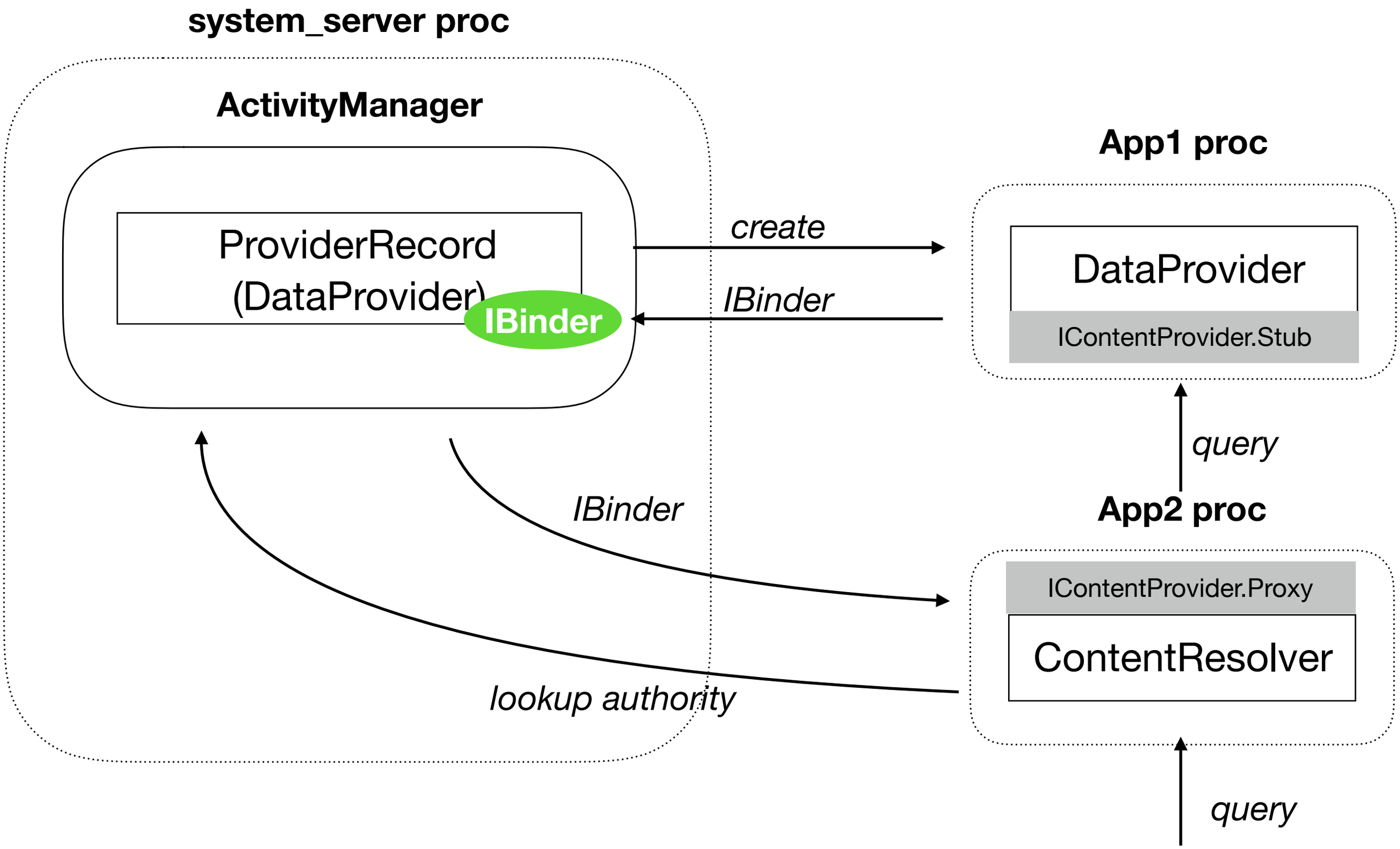
Content Provider



Content Provider



Content Provider



Android Permissions

Реализованы на разных уровнях

- Kernel

  Filesystem permissions

  Paranoid networking

- Native service

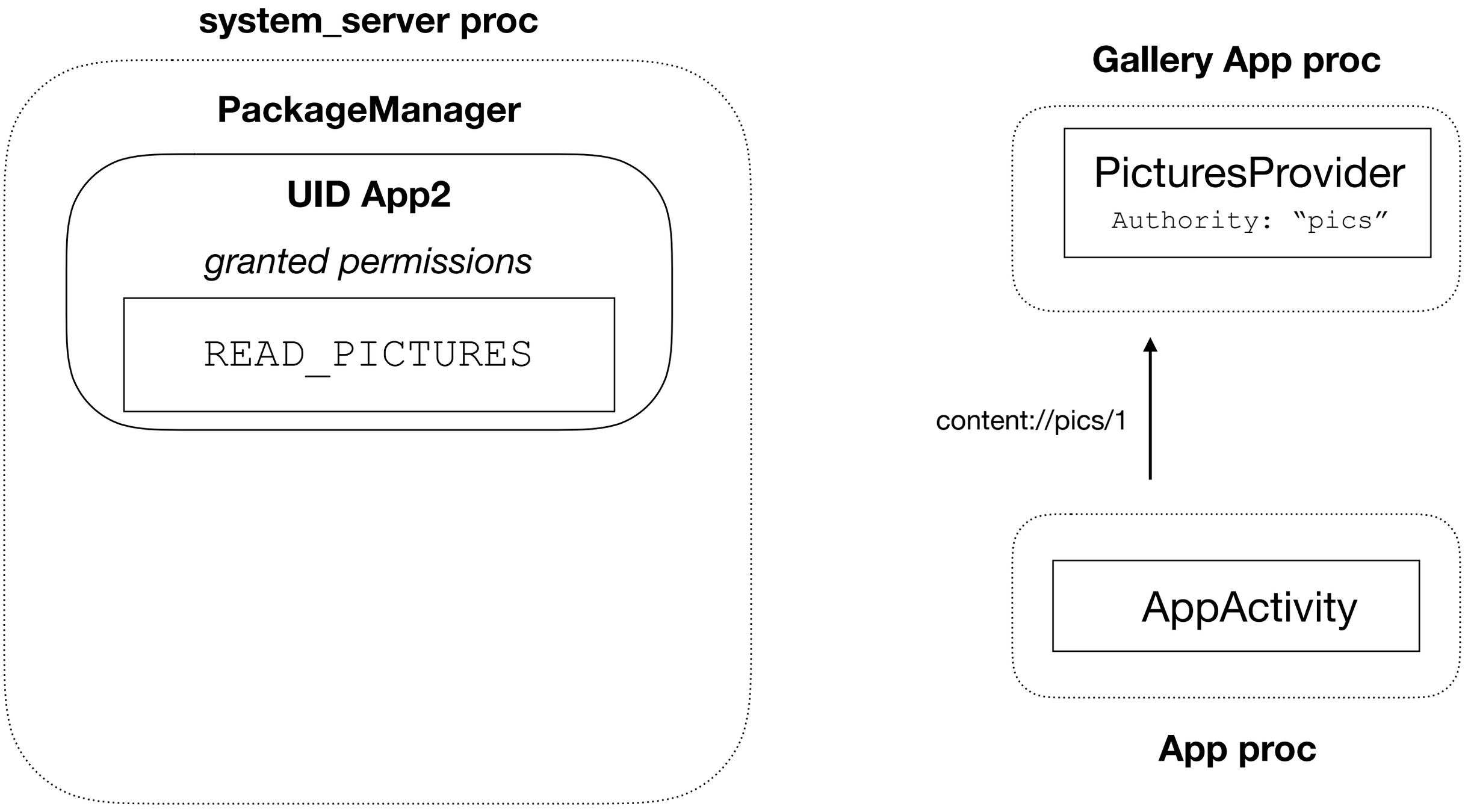
  Проверки на уровне UID и GID

- Framework

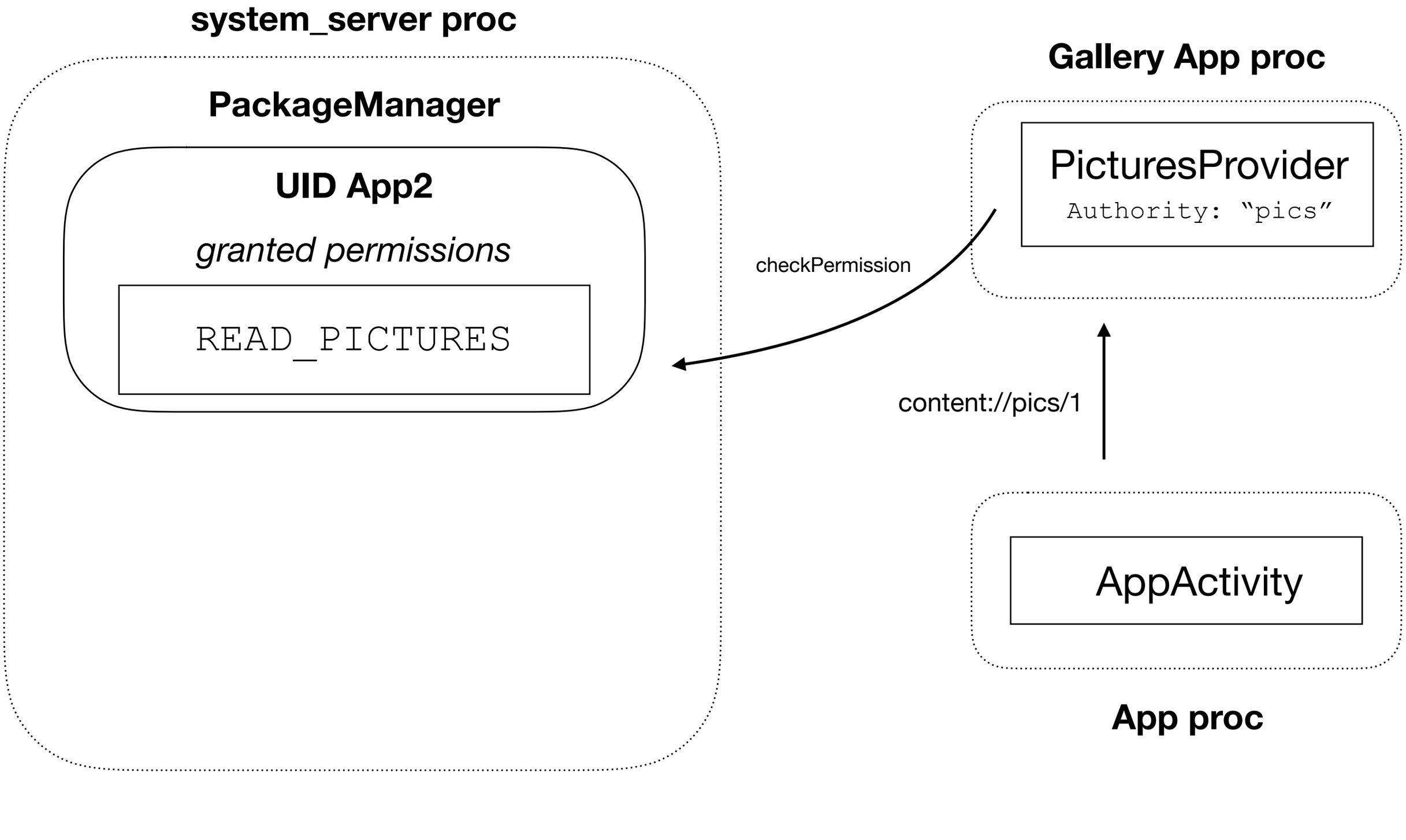
  PackageManager

  ActivityManager

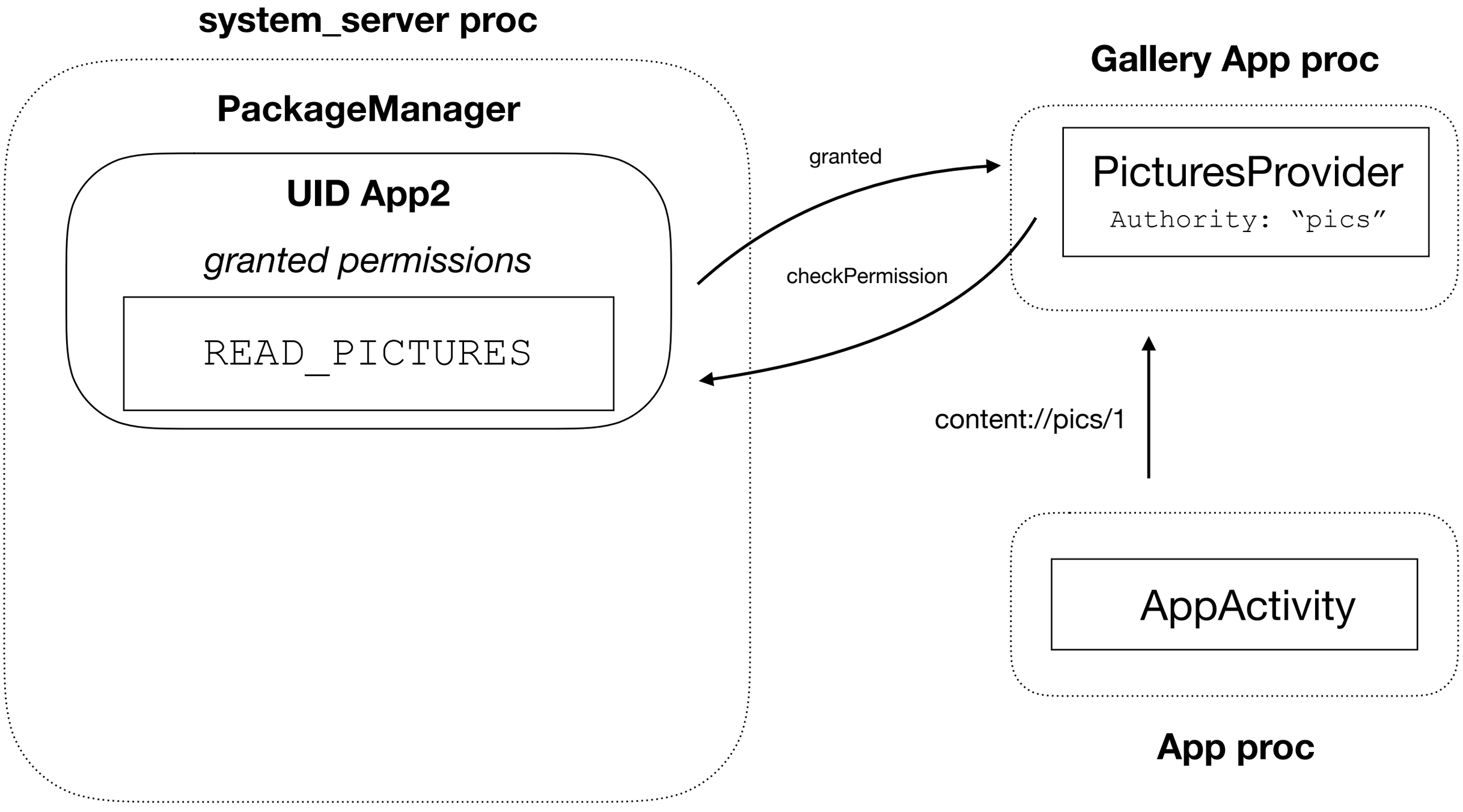
Android Permissions



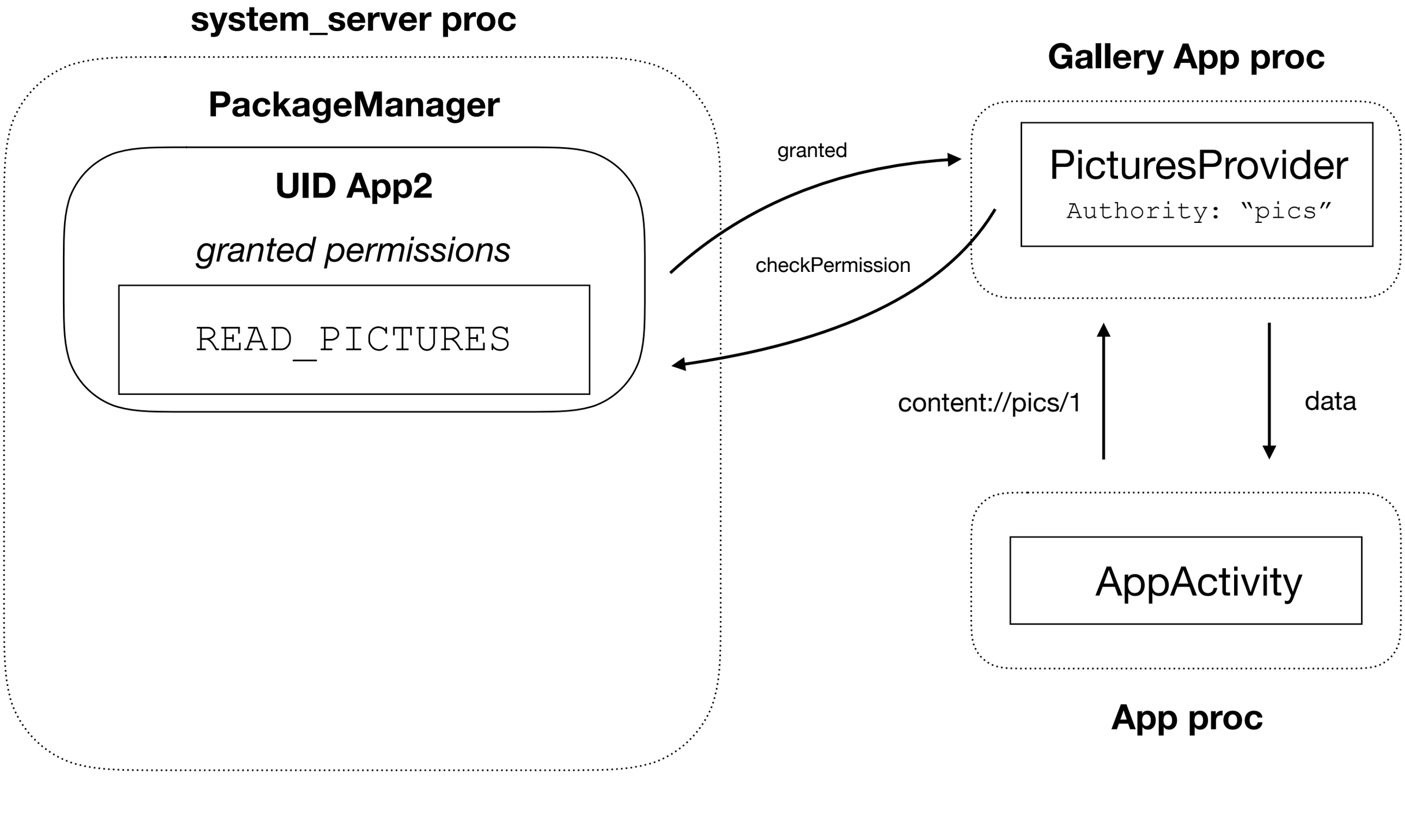
Android Permissions



Android Permissions



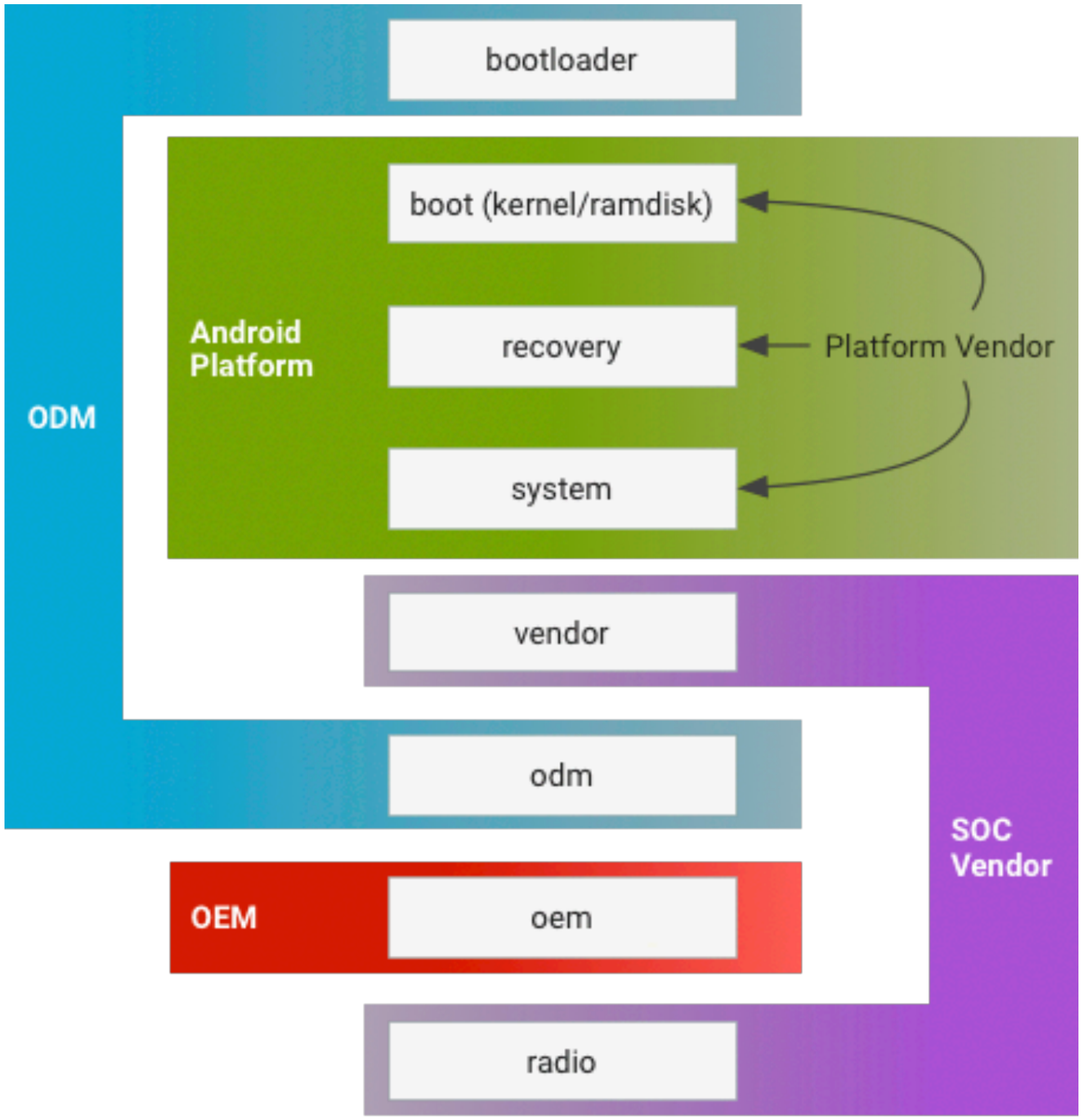
Android Permissions



Безопасность

- DAC (UID и GID)
- MAC (SELinux)
- Code signing

Android O


bootloader
boot (kernel/ramdisk)
Android Platform
recovery
Platform Vendor
system
ODM
vendor
odm
SOC Vendor
OEM
oem
radio

“Knowledge is power.”

–Francis Bacon

“Linux is obsolete.”

–Andrew Tanenbaum