Архитектура модели безопасности ОС Аврора

Окошкин Дмитрий
Руководитель группы разработки

ОТКРЫТАЯ МОБИЛЬНАЯ ПЛАТФОРМА

О докладчике

- разработка и поддержание жизненного цикла приложений в ОС Аврора
- изолированное окружение исполняемого кода
- механизм подписи разделов, приложений и их данных
- проверка устанавливаемого контента приложения
- системный API

План презентации

- Что такое ОС Аврора
- Архитектура безопасности ОС Аврора
- Новая концепция доверенных источников приложений в Аврора 5
- Дальнейшее развитие

ОС Аврора

ОПЕРАЦИОННАЯ СИСТЕМА

Пятое поколение

Современный мобильный функционал
с фокусом на безопасности и эргономике

АВРОРА
СВОЯ СИСТЕМА

Более 5 лет

в промышленной эксплуатации

ЭКОСИСТЕМА ПРИЛОЖЕНИЙ

Более 100 партнеров

создают свои решения
для ОС Аврора

МОБИЛЬНЫЕ СЕРВИСЫ И MDM

Аврора Центр

Управление парком устройств
Push-сервис, сервис обновлений,
магазин приложений

СРЕДСТВА РАЗРАБОТКИ

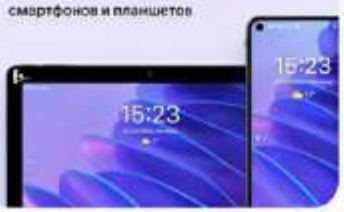
Аврора SDK

для Windows, MacOS и Linux

МОДЕЛЬНЫЙ РЯД

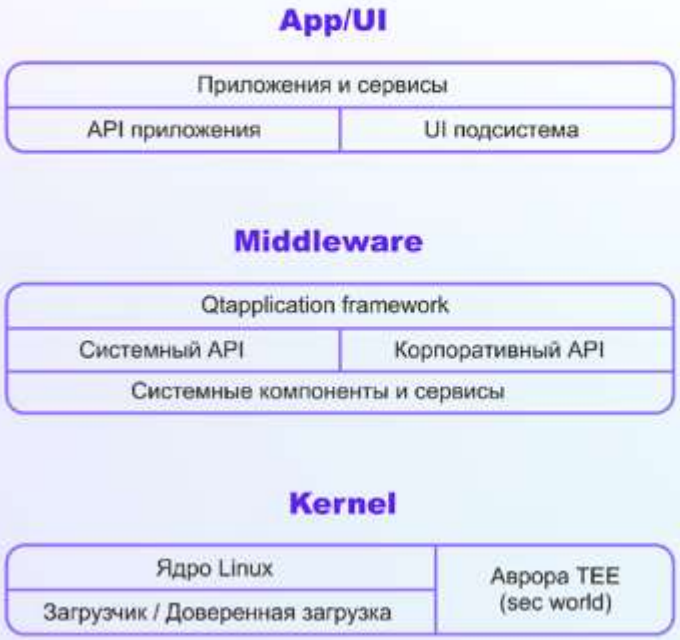
10+ устройств

смартфонов и планшетов



ОС Аврора - Архитектура

- Linux ядро
- GNU/Linux userland
- Wayland
- Systemd
- Qt Framework
- Flutter
- Пакетный менеджер RPM
- Более 1800 закрытых и open-source пакетов



Категории угроз и направления атак

- Физический доступ
- Сетевое взаимодействие
- Исполнение недоверенного кода и обработка недоверенного контента

Физический доступ

- Доверенная загрузка (Trusted boot)
- Шифрование домашнего каталога
- Шифрование краты памяти
- Криптохранилище Аврора TEE

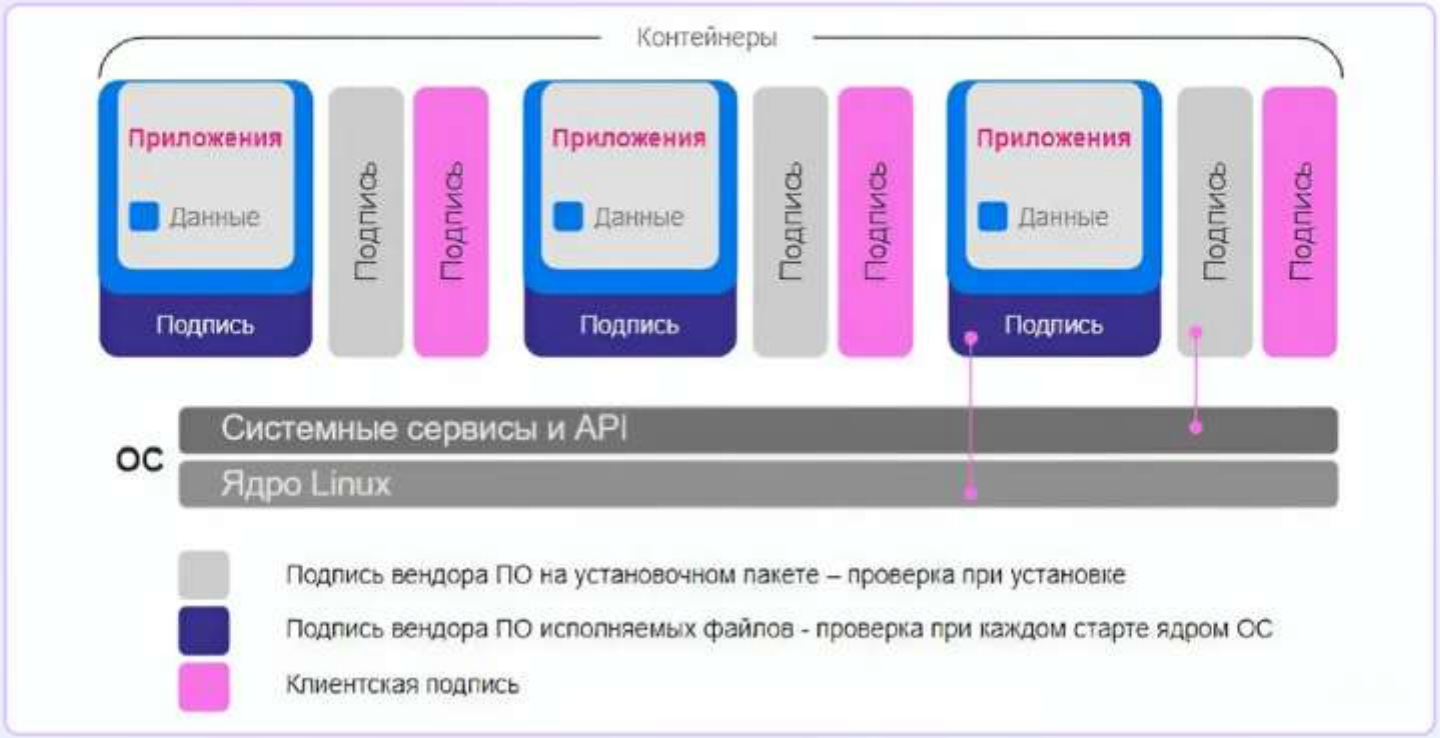
Сетевое взаимодействие

- Доверенный VPN
- Crypto API
- WPA2-Enterprise
- Firewall

Архитектура безопасности приложений

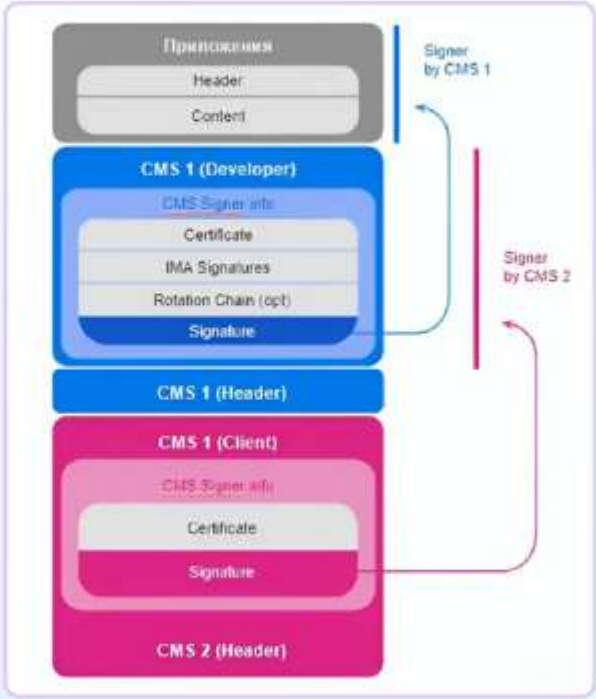
- В ОС Аврора реализована **многоуровневая система безопасности**, которая не требует сложной ручной настройки, а работает сразу **«из коробки»**
- Все системы безопасности направлены на противодействие следующим угрозам — физический доступ, сетевое взаимодействие и **исполнение недоверенного кода**, обработка недоверенного контента
- Особое внимание уделяется возможности построения **замкнутой программной среды**, исключающей попадание и запуск недоверенного программного обеспечения в среде ОС Аврора

Общая модель безопасности



Подпись пакета приложения в ОС Аврора

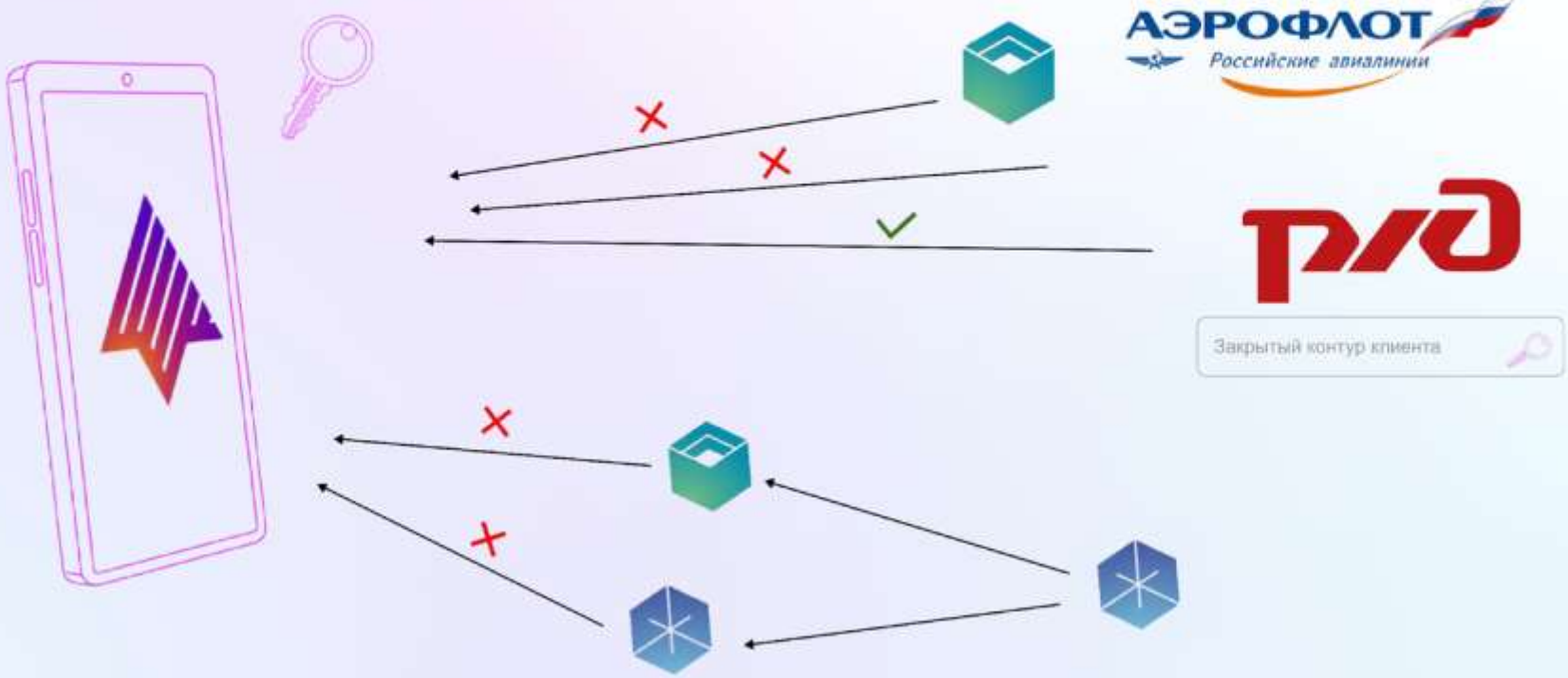
- **IMA (Integrity Measurement Architecture)** – подсистема ядра Linux для обеспечения динамического контроля целостности
- Подписи интегрированы в RPM пакет: **расширенные атрибуты** восстанавливаются при установке пакета
- Поддержка **алгоритмов ГОСТ**
- IMA **запрещает выполнение неподписанных** или некорректно подписанных исполняемых файлов и динамических библиотек



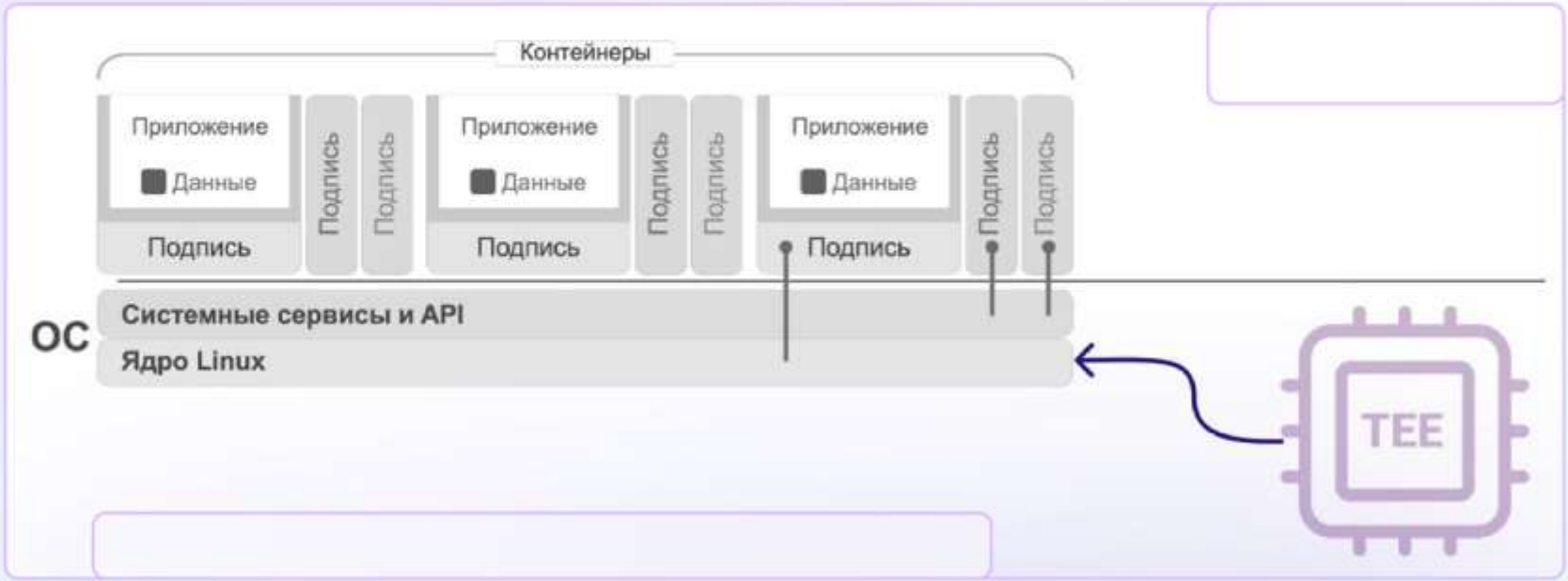
Профили валидации пакета

- **Regular** - базовый профиль для разработки стандартных приложений
- **Extended** - расширенный профиль, содержит больше разрешенных системных компонентов, используемых для разработки не только обычных приложений, но и например, VPN-клиентов
- **MDM** – профиль для MDM клиентов
- **Antivirus** - этот профиль наследует regular и используется для разработки антивирусного ПО
- **Auth** - профиль используется для разработки ПО предоставляющее функционал аутентификации на устройстве
- **Market** - профиль для разработки приложений типа Магазин

Обеспечение замкнутой среды проектов



Аврора TEE


Контейнеры
Приложение
Данные
Подпись
Подпись
Подпись
Приложение
Данные
Подпись
Подпись
Подпись
Приложение
Данные
Подпись
Подпись
Подпись
ОС
Системные сервисы и API
Ядро Linux
TEE

Эшелонированная защита ОС Аврора от исполнения недоверенного кода

Предотвращение запуска

- Подпись пакетов
- Динамический контроль целостности исполняемых файлов (IMA)
- Валидация используемого API

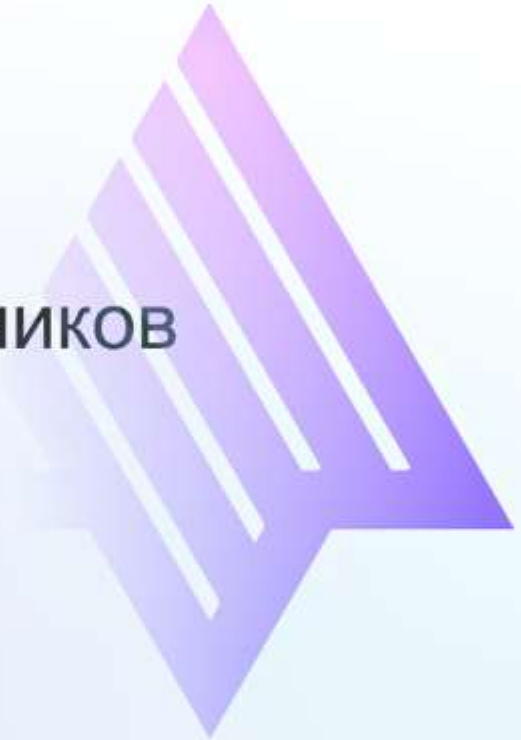
Ограничение исполнения

- Изоляция по namespace
- Разрешения приложений
- Запрет небезопасных системных вызовов
- Запрет выполнения JIT кода под суперпользователя
- Хранилище ключей в Аврора TEE
- Включение механизмов защиты на уровне компилятора

Реагирование на последствия

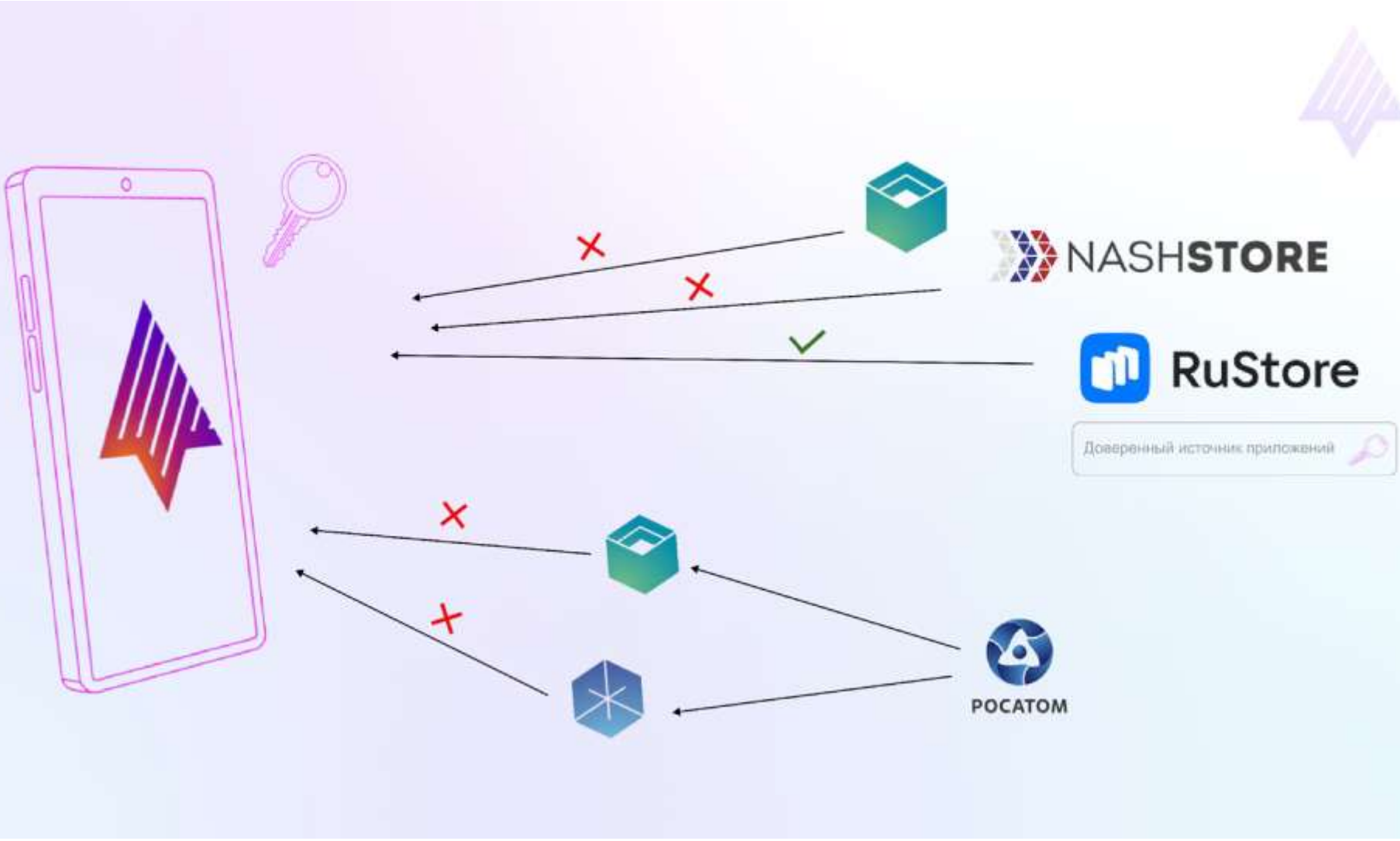
- Сервисы Securityd и Integrityd
- Доверенная загрузка (Secure Boot)
- ATIC (Aurora Trusted Integrity Checker)
- Kernel Self Protection

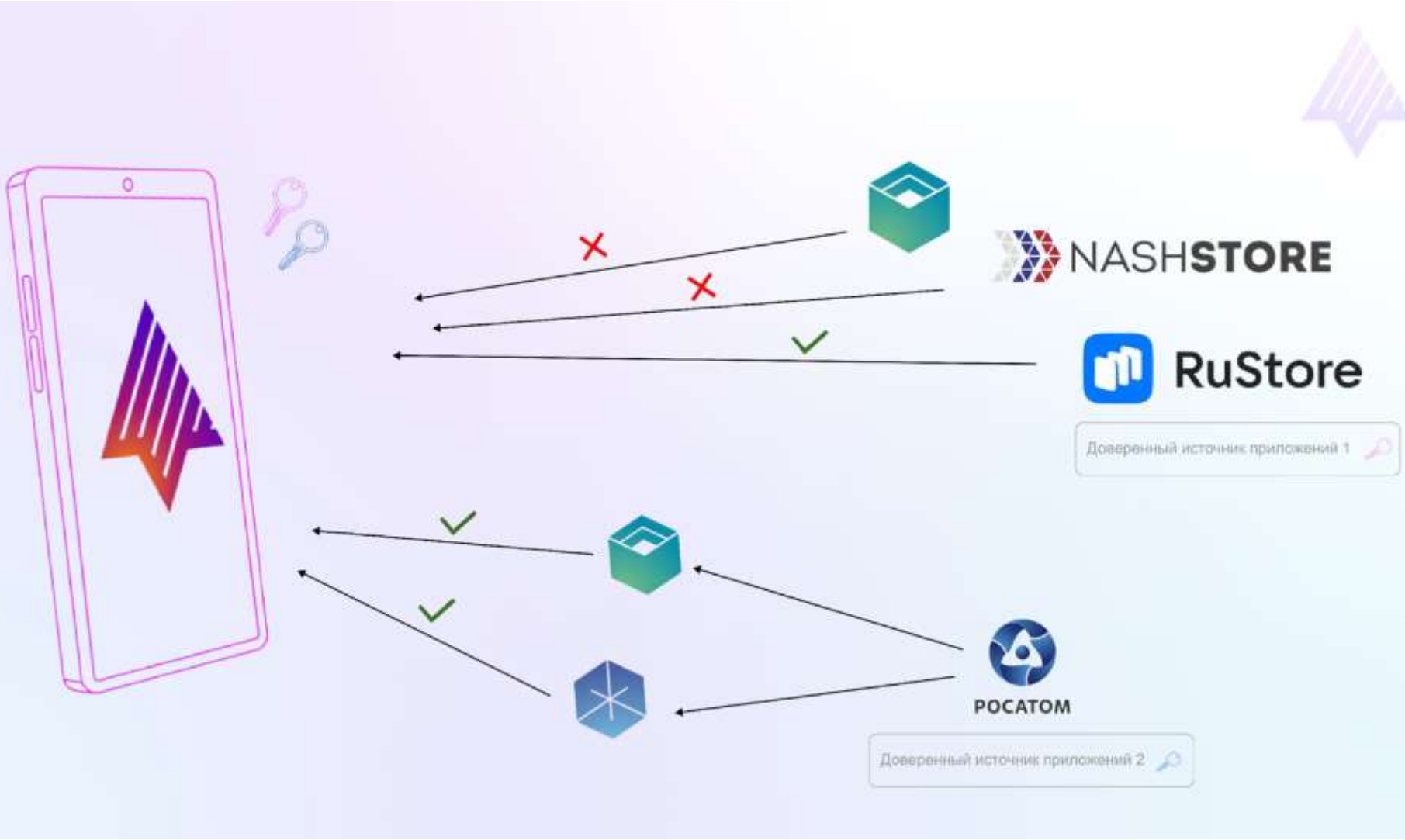
Концепция доверенных источников в Аврора 5

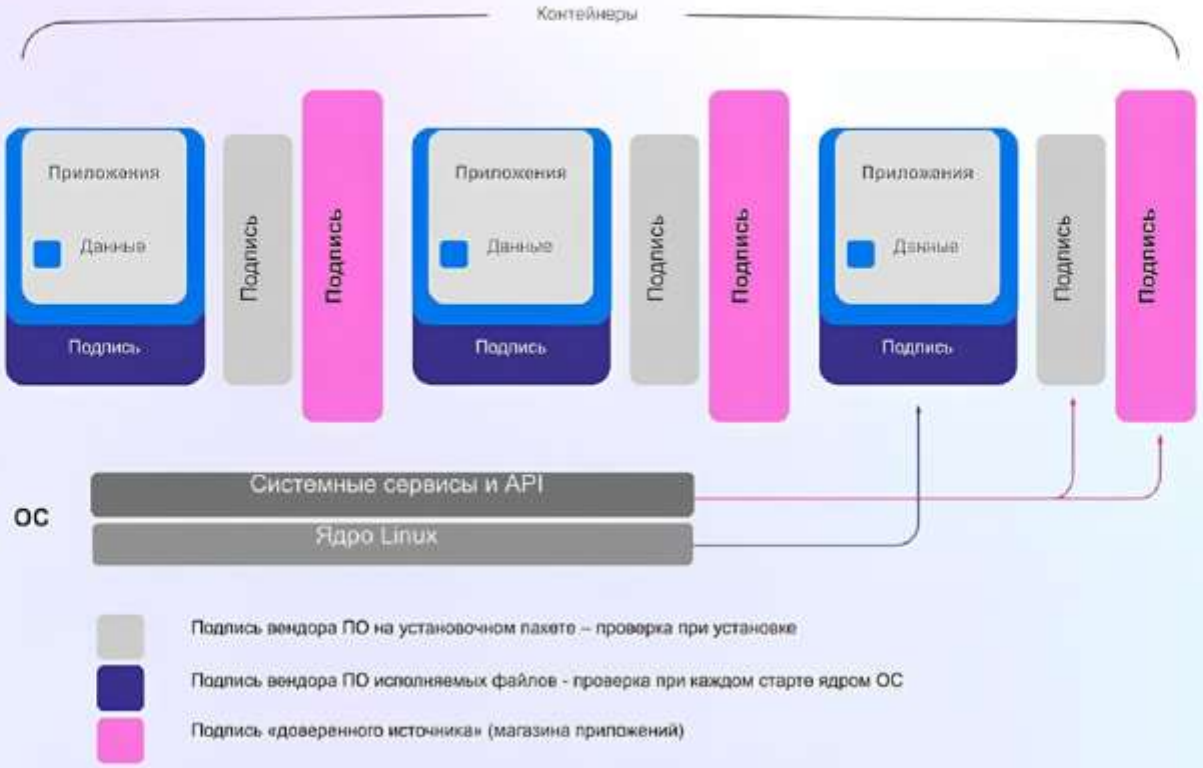


Наши цели - которые были поставлены при проектировании механизма доверенных источников

1. **Сохранить и усилить** возможности контроля замкнутости среды
2. **Устранить** недоработки механизма клиентской подписи
3. **Быть готовыми** к глобальным магазинам приложений


NASHSTORE
RuStore
Доверенный источник приложений
РОСАТОМ


NASHSTORE
RuStore
Доверенный источник приложений 1
РОСАТОМ
Доверенный источник приложений 2

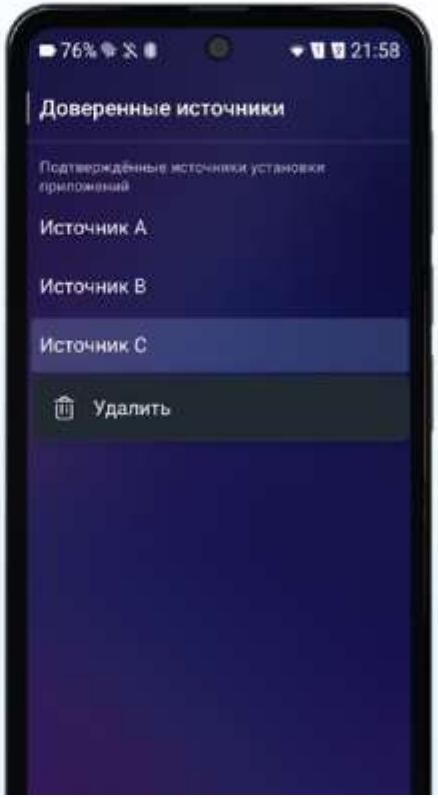

Контейнеры
Приложения
Данные
Подпись
Подпись
Подпись
Приложения
Данные
Подпись
Подпись
Подпись
Приложения
Данные
Подпись
Подпись
Подпись
ОС
Системные сервисы и API
Ядро Linux
Подпись вендора ПО на установочном пакете – проверка при установке
Подпись вендора ПО исполняемых файлов - проверка при каждом старте ядром ОС
Подпись «доверенного источника» (магазина приложений)

На устройстве может быть **несколько источников**, которым доверяет администратор устройства

Что было невозможно при механизме клиентской подписи

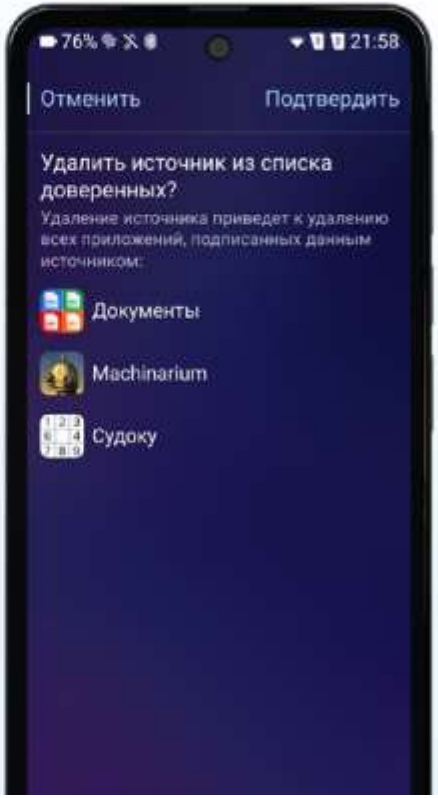
На устройстве могут находиться приложения **только из доверенных источников**

Список приложений на устройстве определяется гибким перечнем источников, которым доверяет владелец устройства



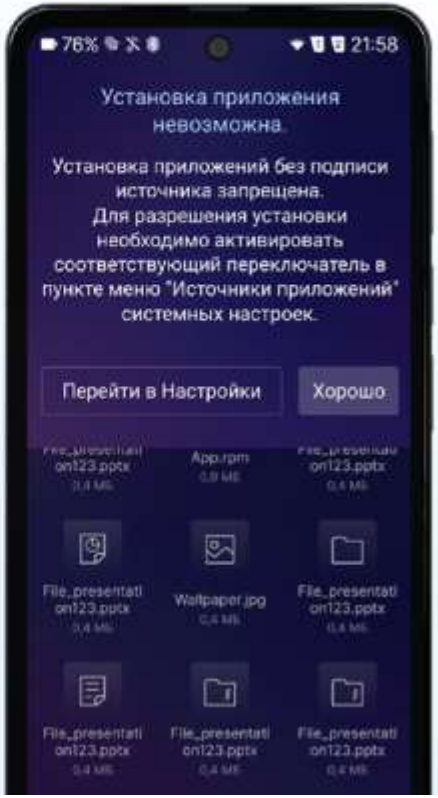
На устройстве могут находиться приложения **только из доверенных источников**

Список приложений на устройстве определяется гибким перечнем источников, которым доверяет владелец устройства



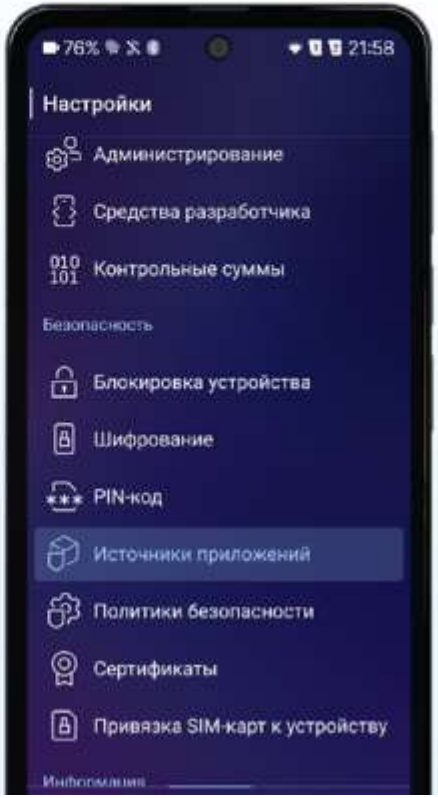
Подпись источника является **обязательной**

За исключением, если администратор
явно разрешил установку пакетов
без подписи источника в настройках администратора



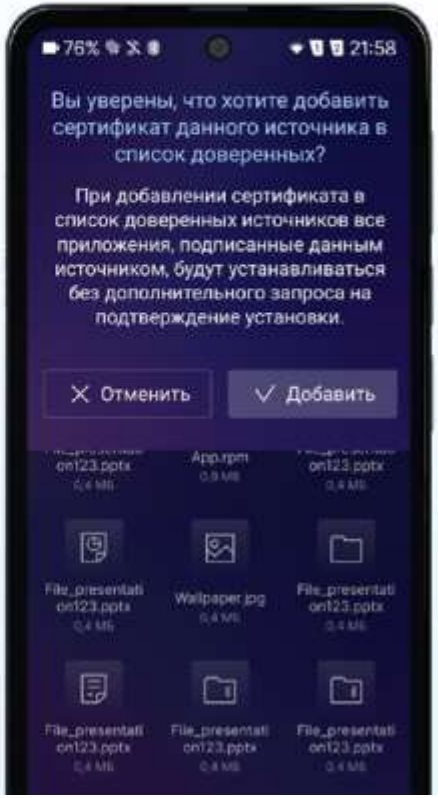
Управление списком источников доступно **только администратору** устройства

Это позволяет сохранить сценарии использования ОС Аврора в закрытом контуре



Доверие к источнику приложения, а не к каналу поставки

Только подпись определяет источник приложения. Это дает пространство для корпоративных витрин приложений.



API для сторонних магазинов с точки зрения безопасности

Market API

+ Необходим ключ разработчика магазина приложений

+ Для использования API пользователь должен принять разрешение

± Позволяет создавать децентрализованные глобальные магазины приложений

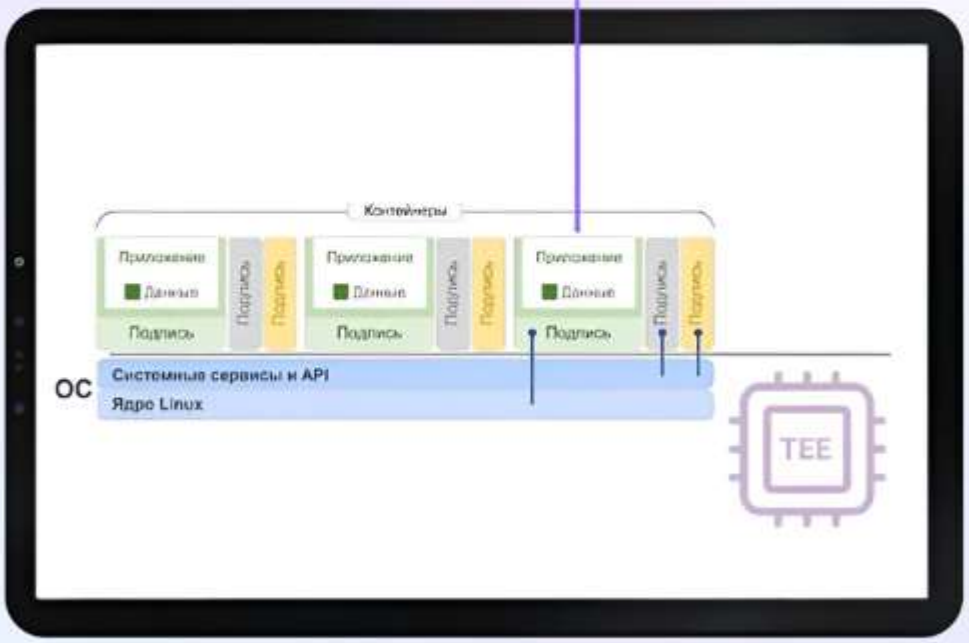
+ Нет требований к реализации серверной части глобального магазина приложений

+ Магазин приложений подписывает пакет ключём и сертификатом источника.
Сертификат выпускается ОМП

Дальнейшее развитие

1. Публичный API для локальной и удаленной **аттестации**
2. Групповое ограничение **разрешений** для приложений из определенных источников
3. Per-user приложения

Аттестация



Сервер приложения

Сервер аттестации

Заключение

1. Платформа Аврора - это **современная мобильная операционная система** и сервисы для корпоративного рынка

2. ОС Аврора имеет **эшелонированную целостную модель безопасности**, которая постоянно развивается

3. ОС Аврора активно **развивается** и реагирует на новые обстоятельства

Спасибо!

ОТКРЫТАЯ
МОБИЛЬНАЯ
ПЛАТФОРМА