Доверенная среда исполнения
Проект национального стандарта

Константин Карасев
архитектор Аврора TEE/Аврора СДЗ

ОТКРЫТАЯ МОБИЛЬНАЯ ПЛАТФОРМА

План доклада

- Предпосылки появления проекта стандарта
- Структура стандарта
- Текущий статус работ над стандартом
- Применение стандарта

Доверенная среда исполнения

- Изоляция вычислительных ресурсов и периферии для доверенных вычислений
- В целом, уменьшение поверхности атаки
- Дополнительный слой защиты в системе

При этом, возможность сэкономить (на стоимости и вычислительном ресурсе)

Как подтвердить доверенность?

- Спецификации GlobalPlatform TEE
- Задание по безопасности
- Профили защиты (ОС, СДЗ)
- Требования безопасности (с чего мы начали)
- Национальный стандарт

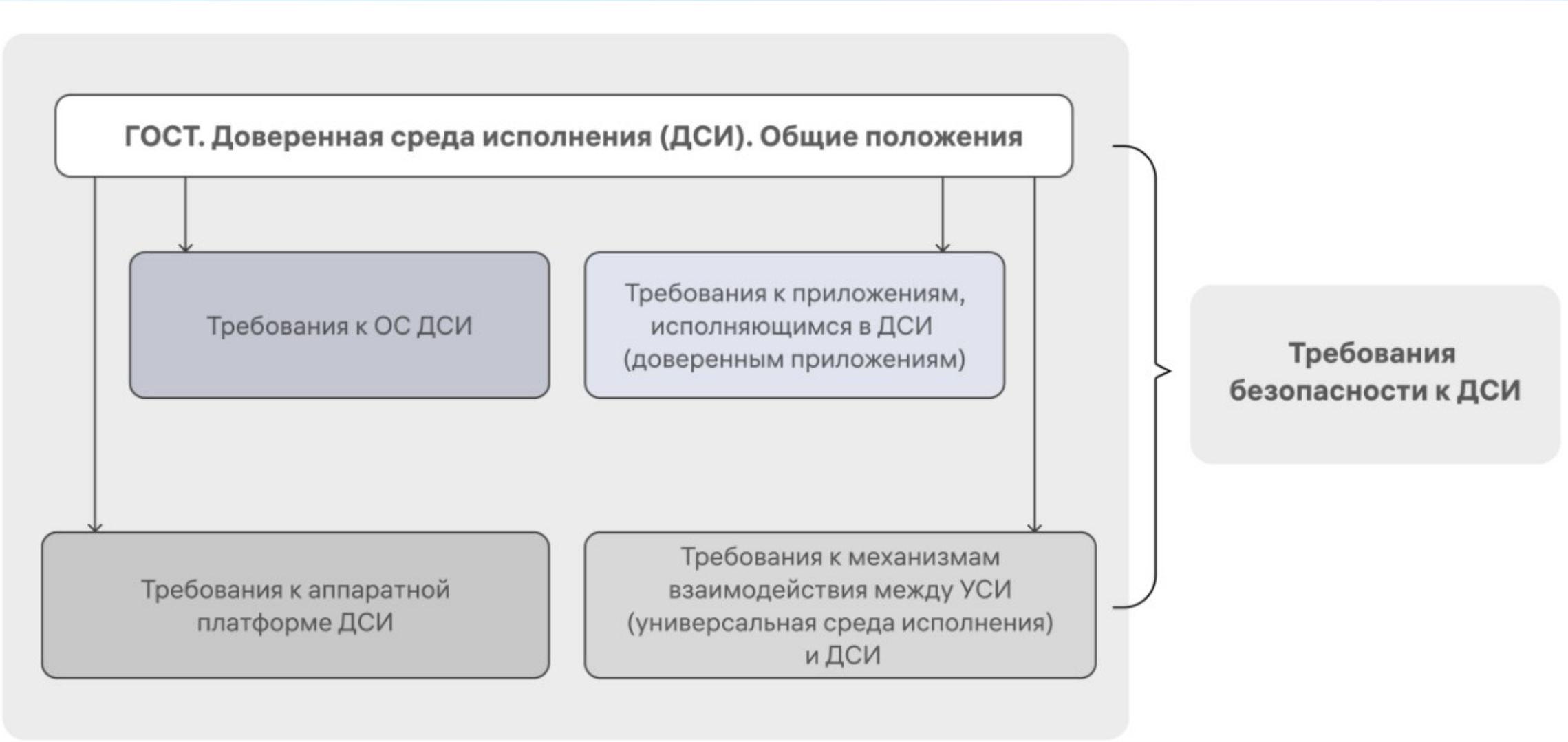
Необходимость стандарта

- Сложившаяся практика применения ДСИ в целях повышения безопасности ИТ-решений (стандарт de facto)
- Вовлеченность многих отраслей ИТ в построение ДСИ
- Широкий спектр технологий, применяемых для построения ДСИ
- Потребность в определении отличительных черт ДСИ, их стандартизации
- Совокупность всех обстоятельств сложившихся вокруг ДСИ требует наличия отдельного стандарта

Аудитория стандарта

- разработчики доверенных сред исполнения
- разработчики ПО, взаимодействующего с доверенными средами исполнения
- разработчики аппаратных платформ
- разработчики информационных систем

Структура стандарта



Проект стандарта определяет…

- Необходимый набор свойств ДСИ
- Цели применения ДСИ
- Архитектурные «рамки» построения ДСИ
- Особенности функционирования ДСИ
- Варианты аппаратной и программной архитектуры ДСИ
- Требования к ДСИ

Проект стандарта не ограничивает...

- Отрасли применения ДСИ (ПК, сервер, мобильное устройство)
- Выбор технологии для реализации ДСИ (ARM TrustZone, TPM, виртуализация)
- Выбор архитектуры процессора
- Список поддерживаемой периферии ДСИ
- Список сервисов ДСИ

Этапы подготовки стандарта

- Рабочая группа в подкомитете Технического комитета по стандартизации ФСТЭК
  - РГ 9, ПК 4, ТК 362 «Защита информации»
- Согласование в рабочей группе (7 участников)
- Рассмотрение в подкомитете, устранение замечаний
- Обсуждение и голосование за проект стандарта в ТК
- Публикация Росстандартом
- Ввод стандарта в действие

Рабочая группа

Компания	Основная деятельность
ООО «Открытая мобильная платформа»	Разработка ОС
Институт системного программирования РАН	Фундаментальные и прикладные исследования
АО «Аладдин Р. Д.»	Разработка СЗИ
АО «Байкал Электроникс»	Разработка микропроцессоров
ООО «ПК Аквариус»	Производство компьютерной техники
ООО «ЯДРО МИКРОПРОЦЕССОРЫ»	Разработка микропроцессоров
АО «ИнфоТеКС»	Разработка СКЗИ
ООО «КРИПТО-ПРО»	Разработка СКЗИ

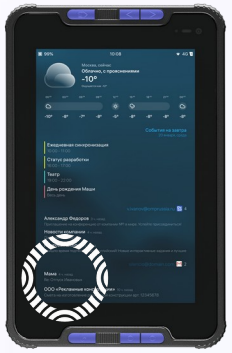
Статус подготовки стандарта

- Завершено согласование проекта в рабочей группе
- Подготовка документов к рассмотрению в ПК4
  - Сейчас
- Рассмотрение в подкомитете и устранение замечаний
  - Сентябрь 2024
- Голосование за проект стандарта в ТК
  - Март 2025
- Публикация Росстандартом
  - Июнь 2025

Следующие шаги разработки стандарта

- Требования к аппаратной платформе
- Требования к операционной системе ДСИ
- Требования к приложениям, исполняющимся в ДСИ (доверенным приложениям)
- Требования к механизмам взаимодействия между доверенной средой исполнения и универсальной средой исполнения
- Требования безопасности информации

Широкая линейка устройств с ОС Аврора

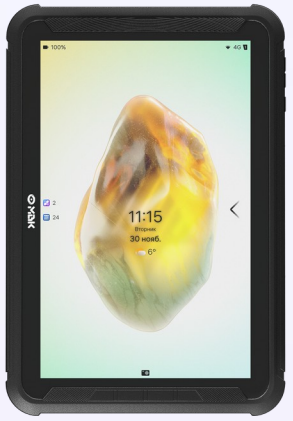


Aquarius
CMP NS208RH

Aquarius
NS M11

Aquarius
NS M12

Aquarius
CMP NS220



БайтЭрг
МВК-2020

QTech
QMP-M1-N-IP

F+
Lifetab Plus

Масштаб
TrustPhone T1

F+
R570E

Aquarius
CMP NS220RE

БайтЭрг
МВК-2021

F+
T1100

Yadro
KVADRA_T

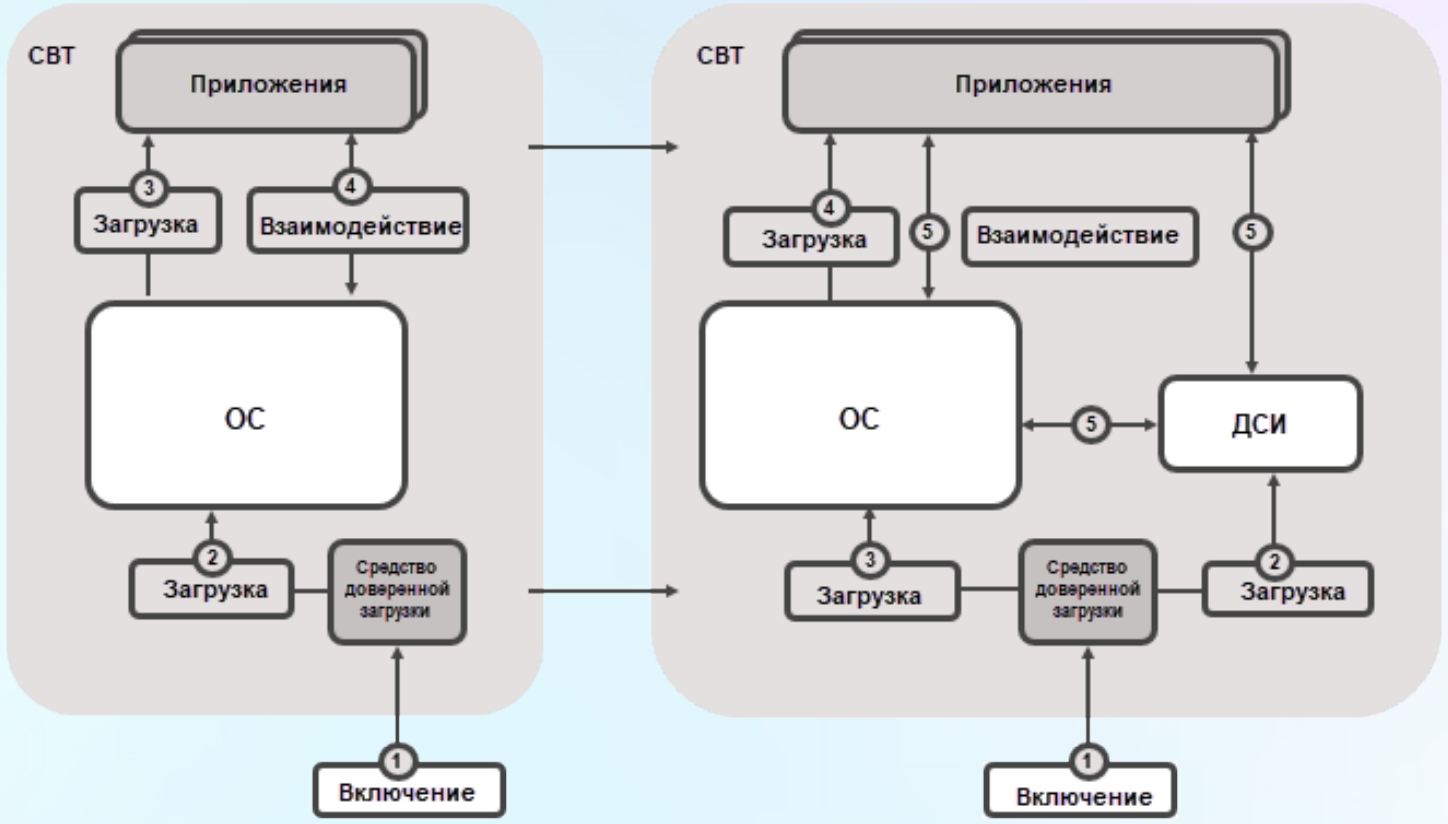
Применение ДСИ

- Управление ключами и криптографические операции
- TEE Keystore
- Финансовые сервисы
- Аутентификация пользователей
- Контроль целостности

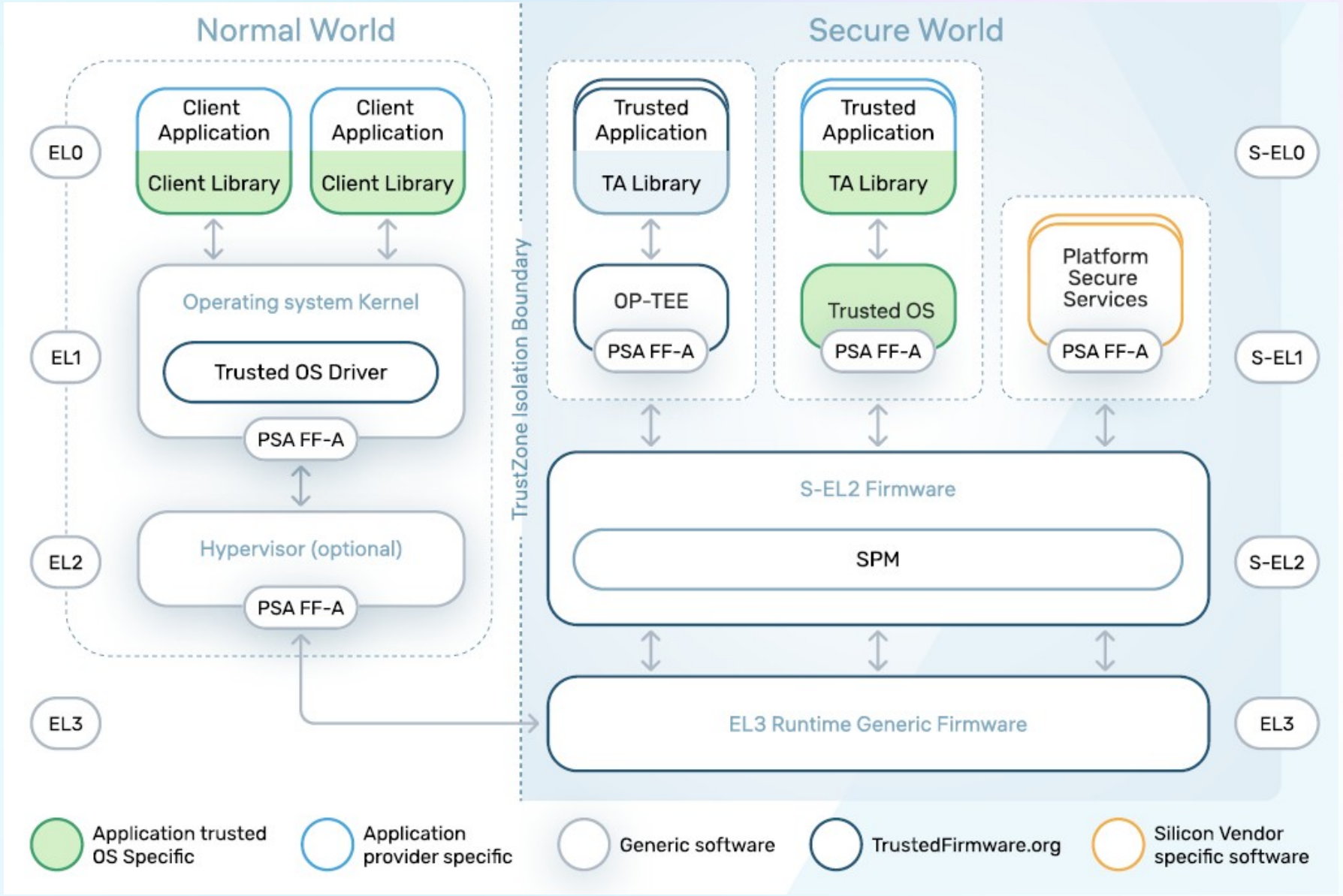
Всем спасибо за внимание!

ОТКРЫТАЯ МОБИЛЬНАЯ ПЛАТФОРМА

Аппаратные основы доверия



Аппаратные основы доверия



Программная архитектура

- Гибкий подход к проектированию
  - Полноценная операционная система
  - Библиотека
  - Отсутствие планировщика
- Изоляция сервисов внутри ДСИ от УСИ и друг от друга
- Целостность исполнения
- ДСИ не обязана парировать DoS

Программная архитектура (пример)