конференция РусКрипто

Реализация доверенной среды для мобильных устройств на базе стандартов TEE и Secure Element

Михаил Дударев, БИФИТ

О себе

Михаил Дударев - эксперт в области технологий Java Card и безопасности мобильных устройств, технический консультант Global Platform.

О нас

- jCardSim - реализация Java Card с открытым исходным кодом, получившая самую престижную мировую премию для разработчиков программного обеспечения Oracle Duke’s Choice Awards 2013.
- Кем используется
  - Thales, Yubico, BMW, Audi
  - SimplyTapp (Android HCE)
  - В университетах всего мира для обучения Java Card

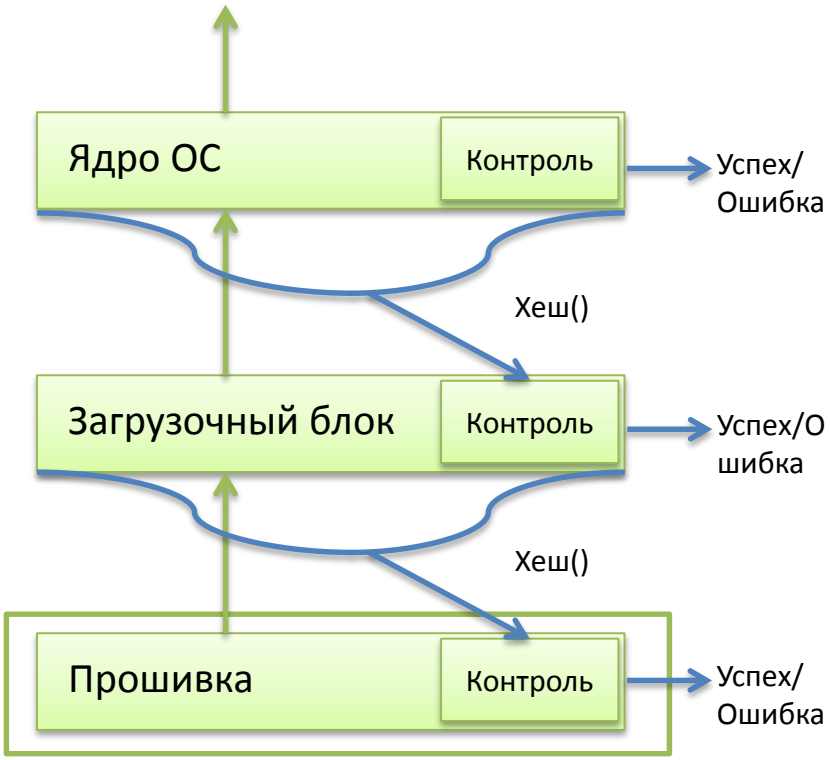
Краткое содержание

- Стандарт Trusted Execution Environment
- Архитектура Secure Element и ее реализация на платформе Java Card
- Secure Element и NFC
- Android HCE и его применение
- Samsung Knox как пример реализации доверенной среды – плюсы и минусы

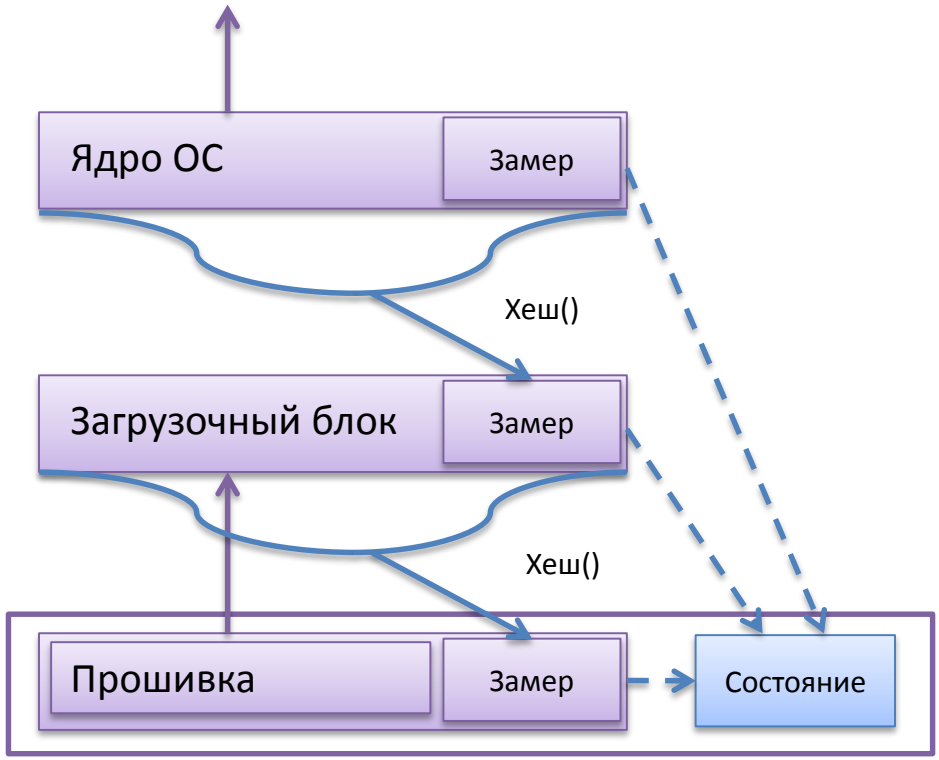
Основные принципы построения доверенной среды

- Контроль целостности платформы
- Защищенное хранилище
- Изолированная среда исполнения
- Идентификация устройства
- Аутентификация устройства
  - Удаленная аттестация

Контроль целостности платформы. Процесс загрузки

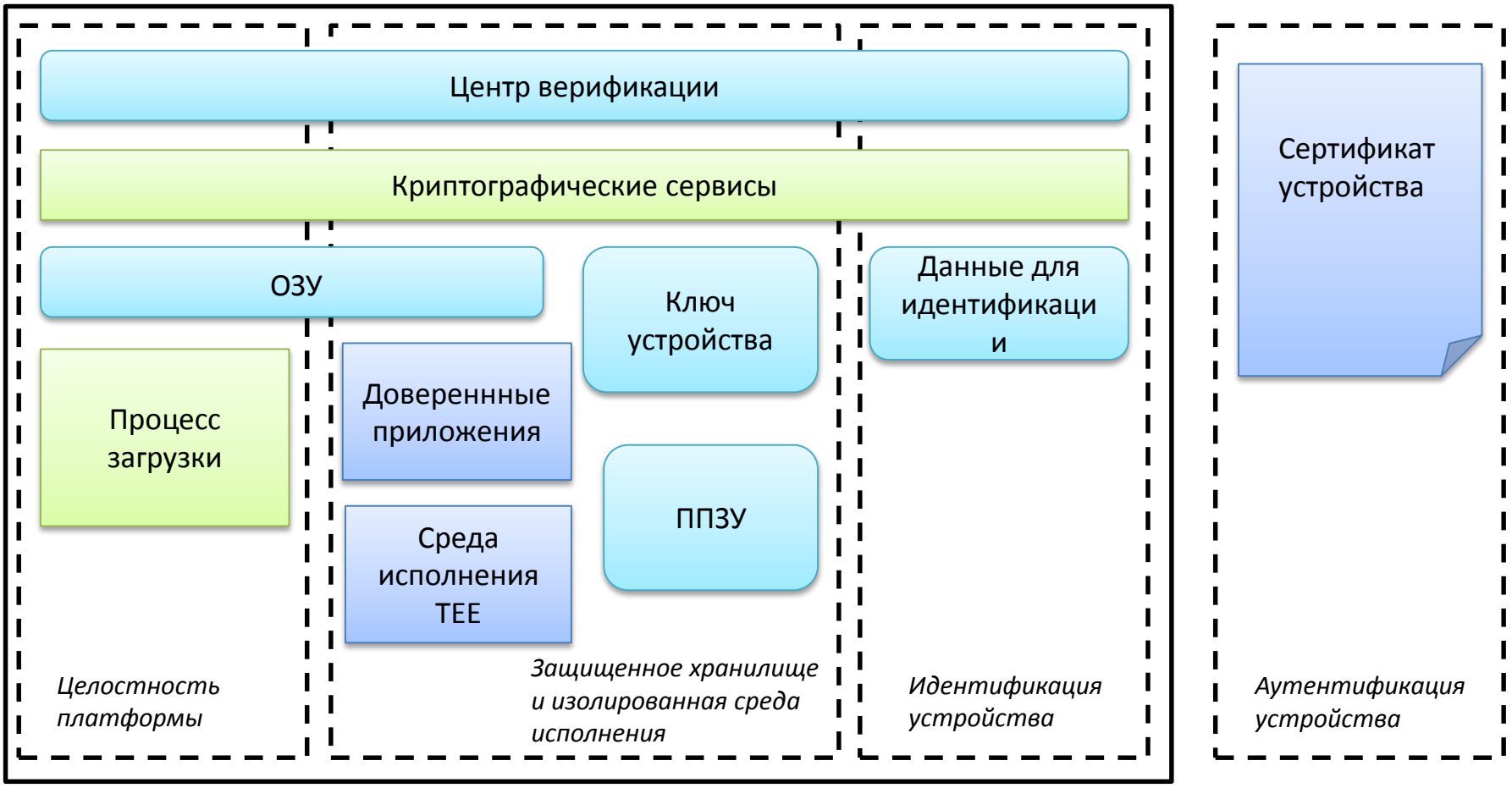


Загрузка в гарантированно доверенной конфигурации

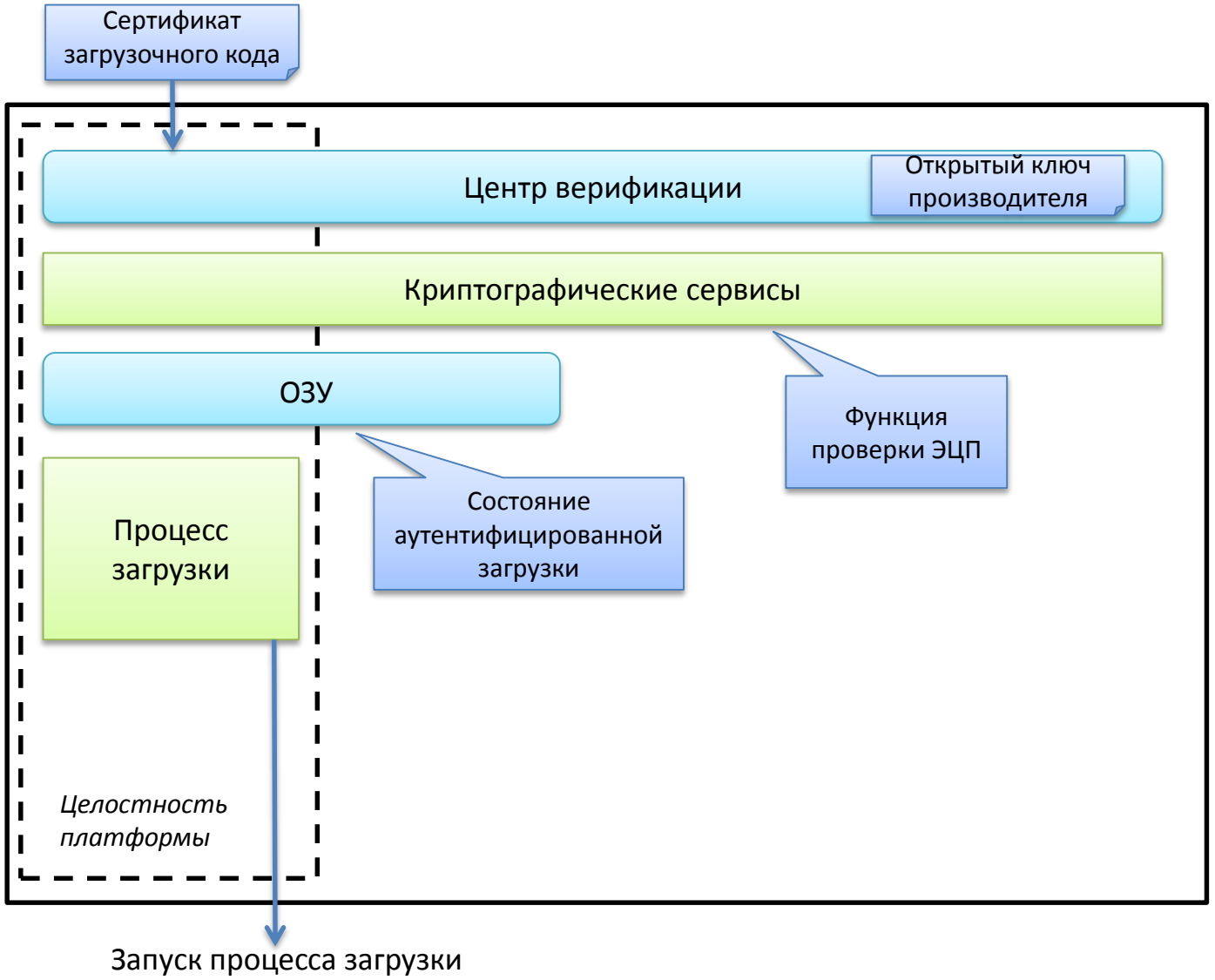


Загрузка в любой конфигурации

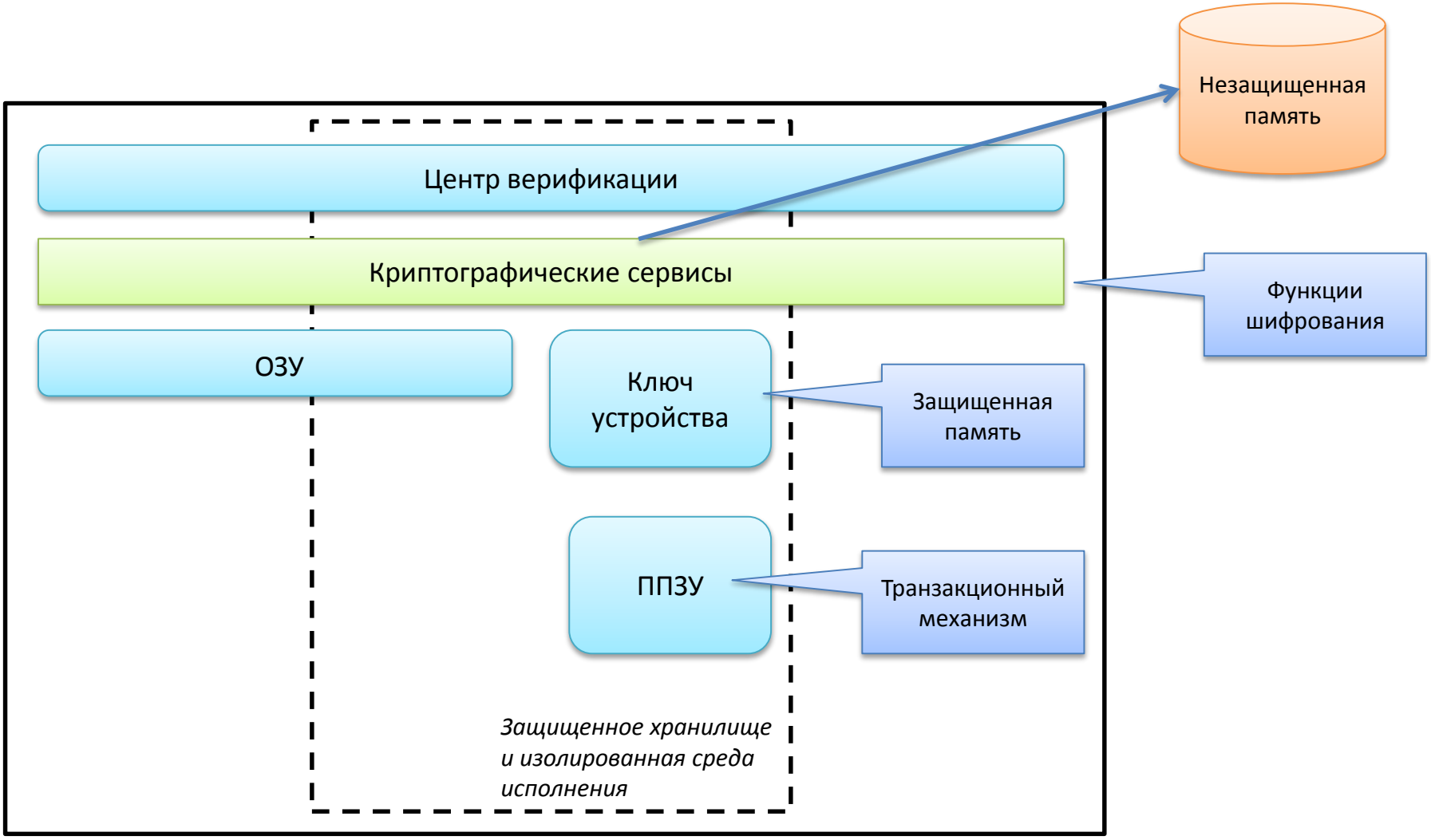
Основные принципы построения доверенной среды (TEE)



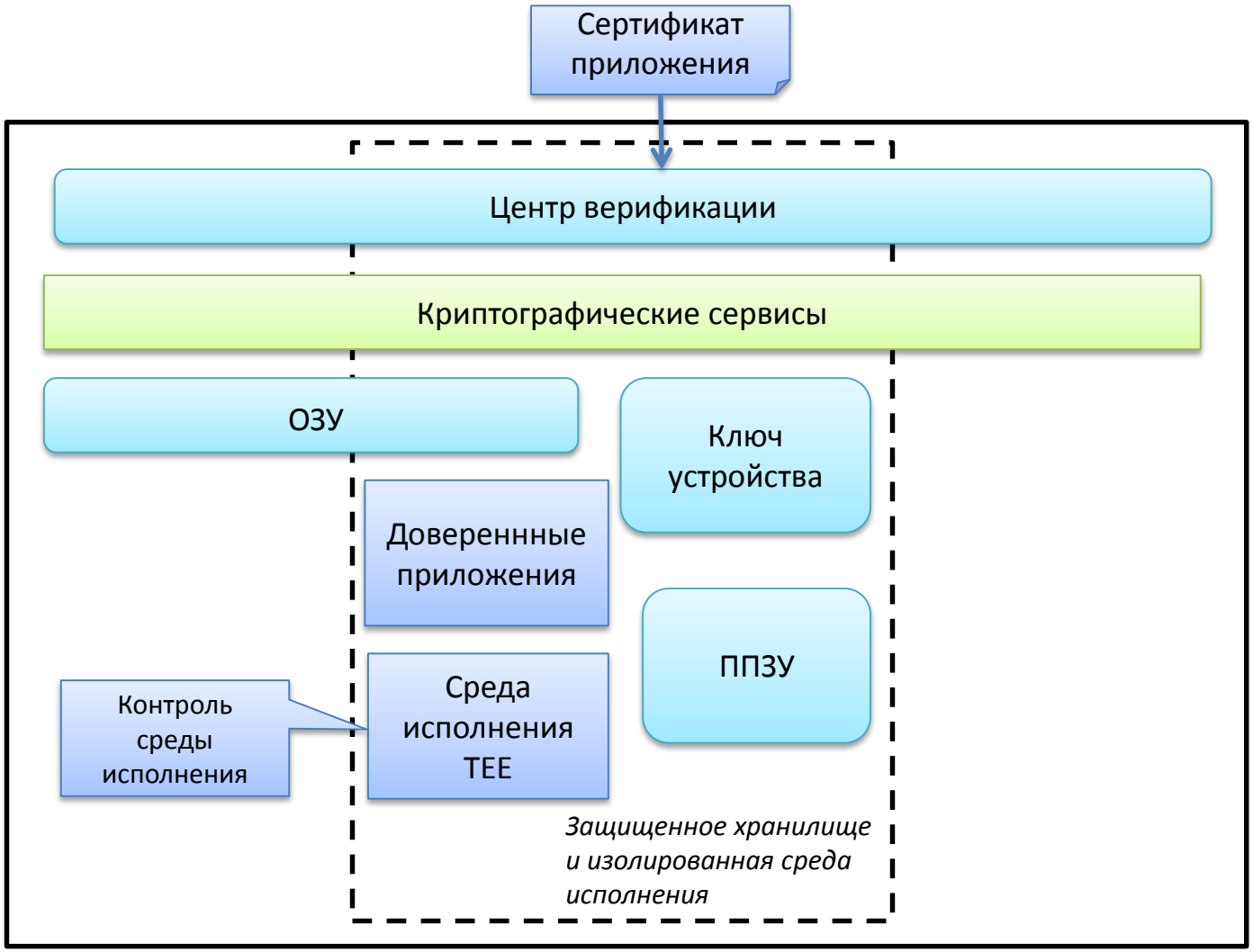
Контроль целостности платформы



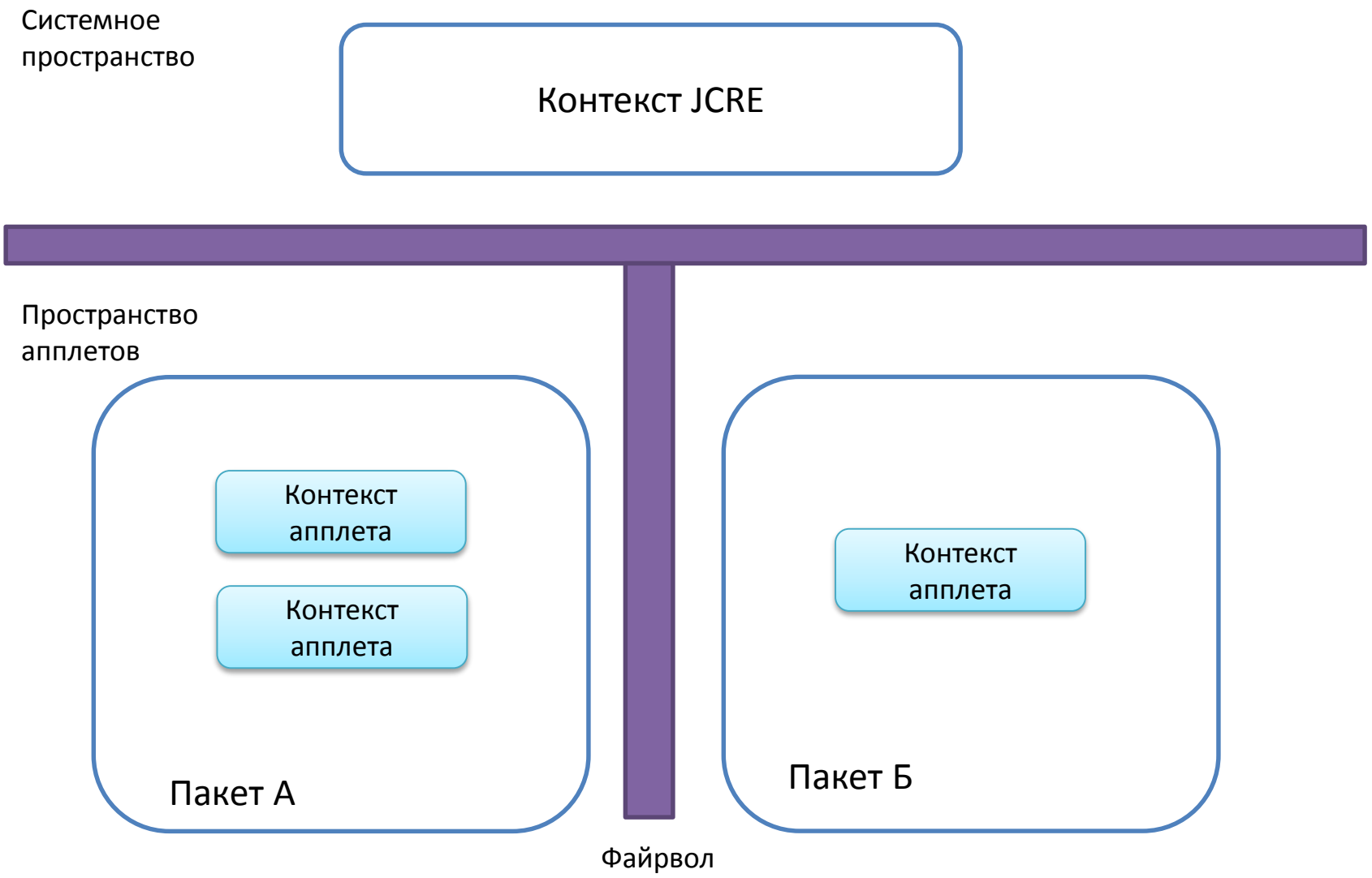
Защищенное хранилище



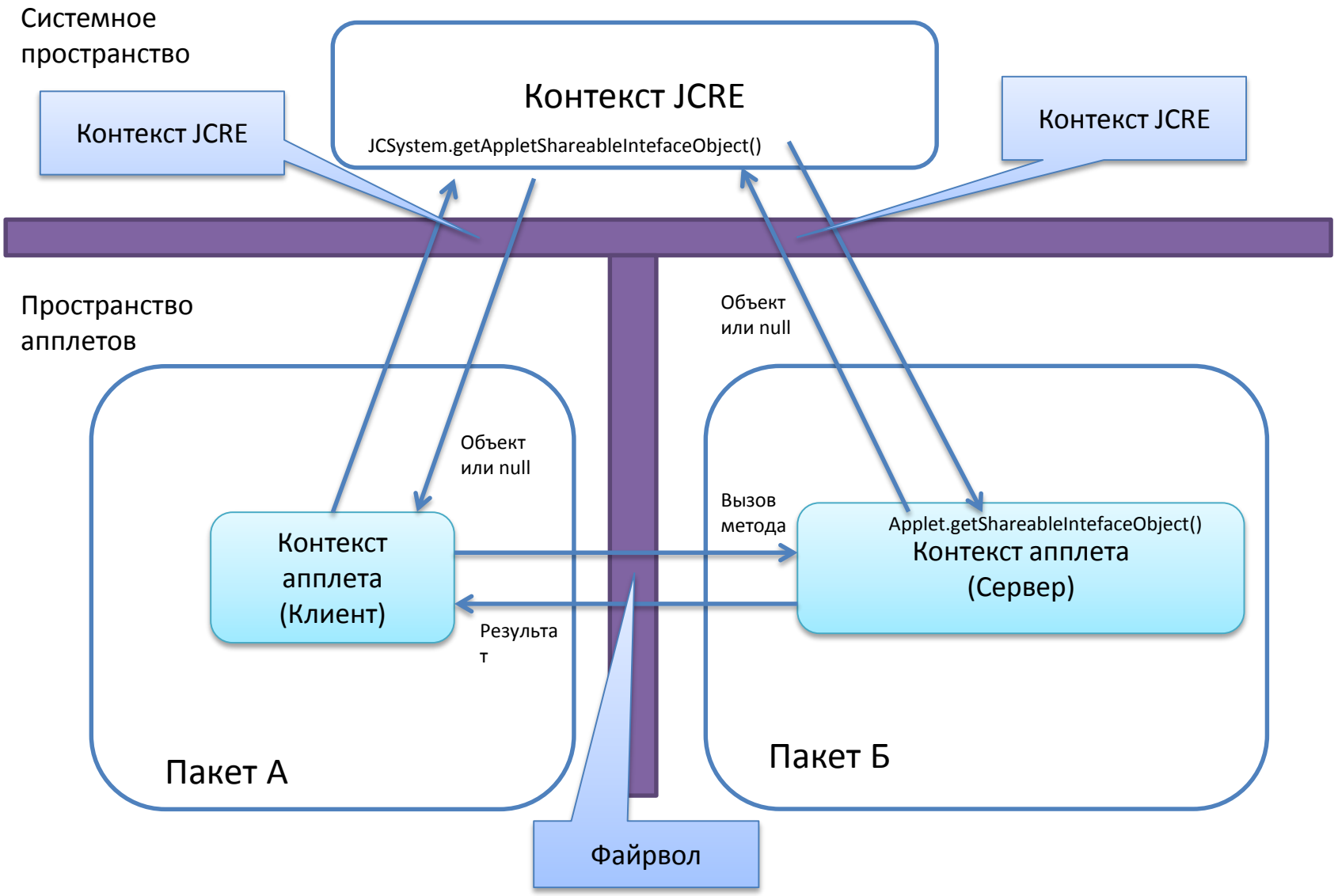
Изолированная среда исполнения



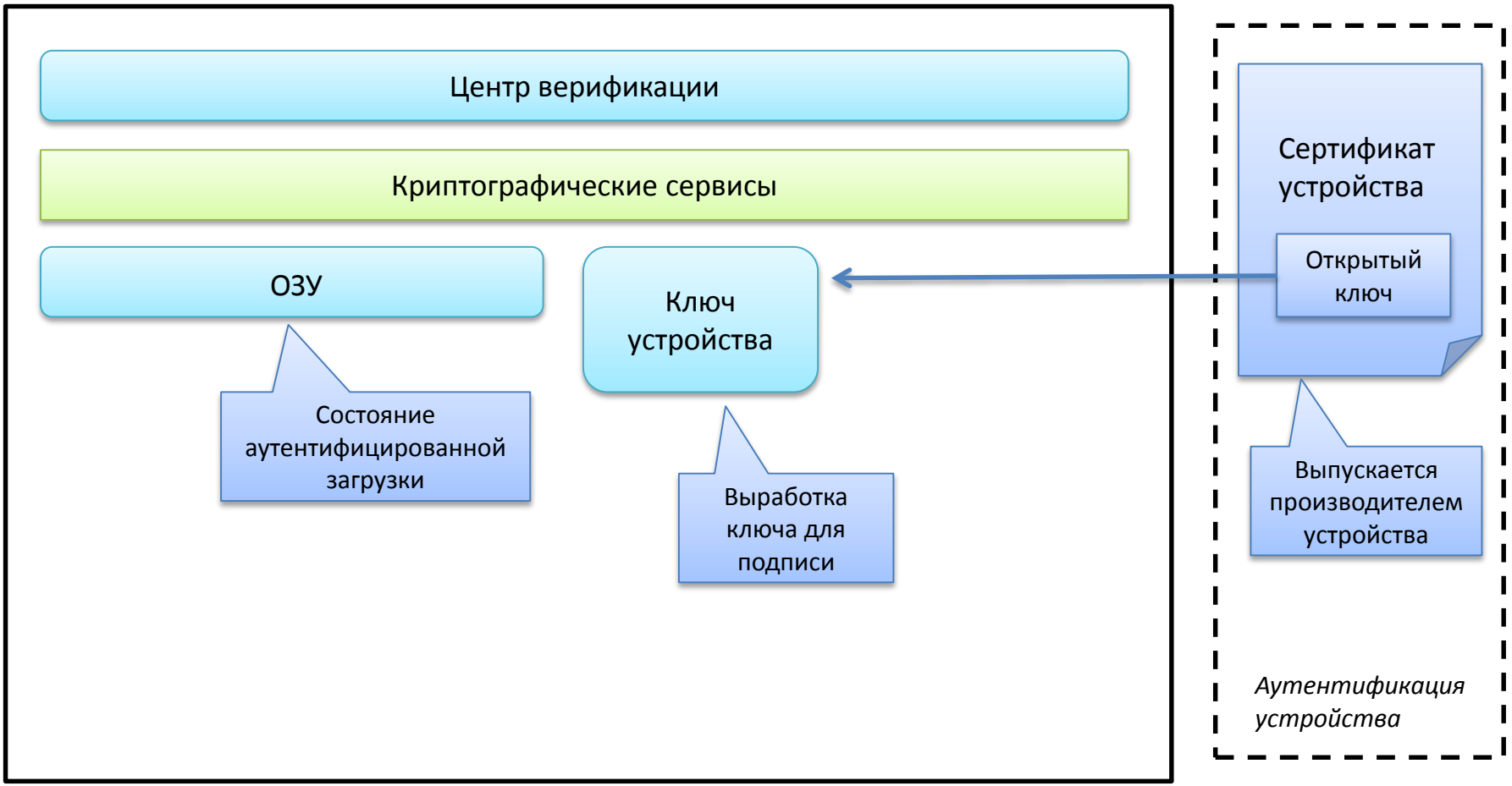
Среда исполнения Java Card



Среда исполнения Java Card

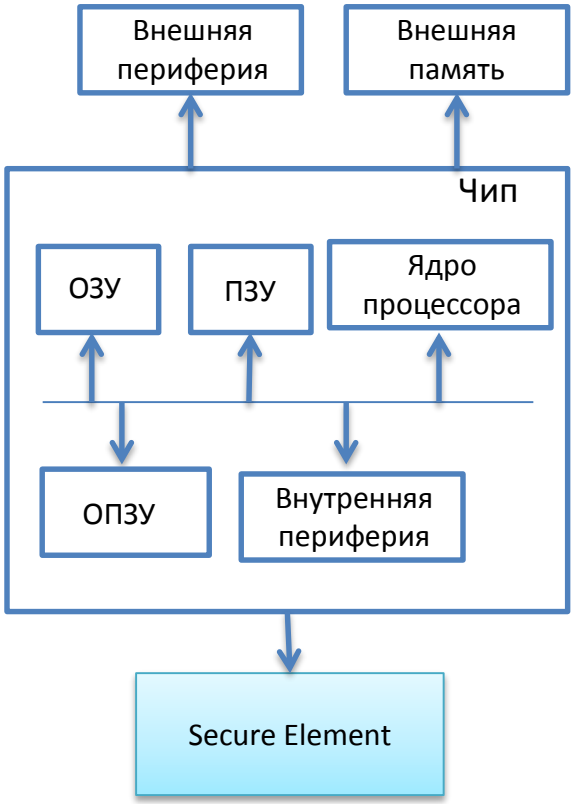


Аутентификация устройства и удаленная аттестация

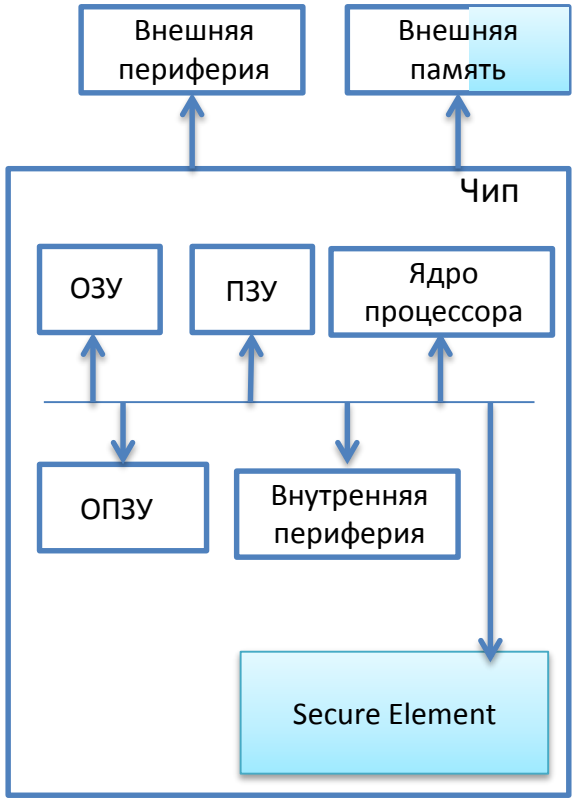


Программная архитектура TEE

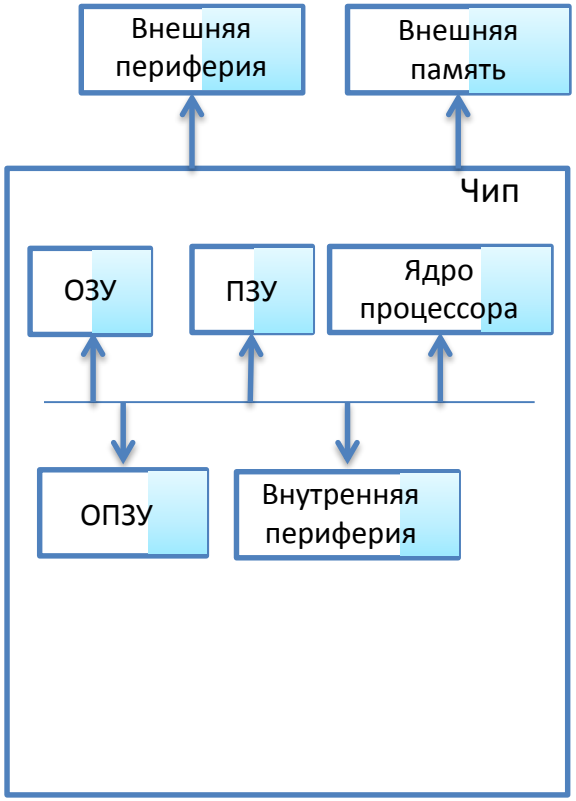
Варианты реализации



Внешний Secure Element
(TPM, Java Card)

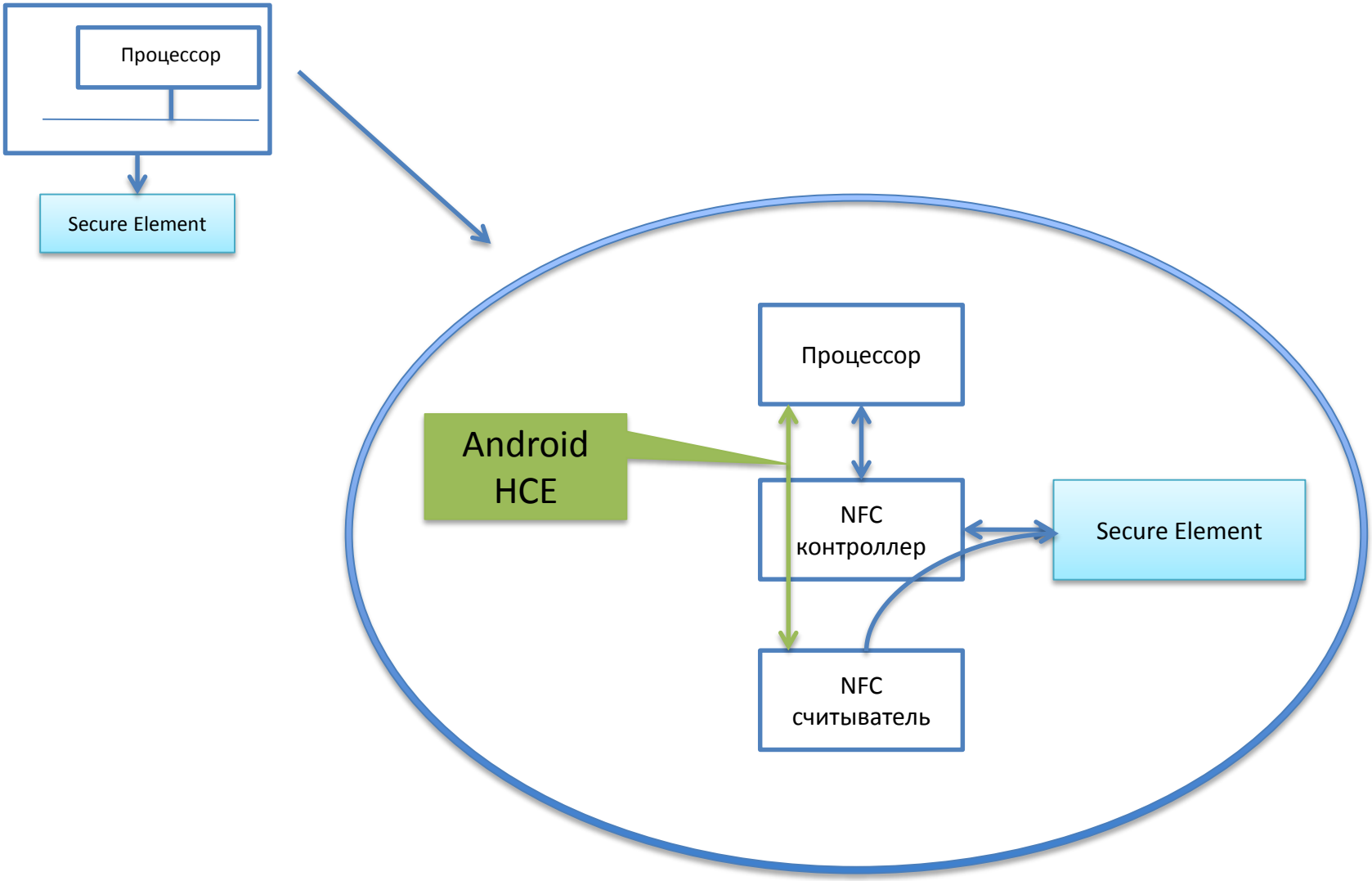


Встроенный Secure Element
(Java Card)



Защищенная среда процессора
(TrustZone, M-Shield)

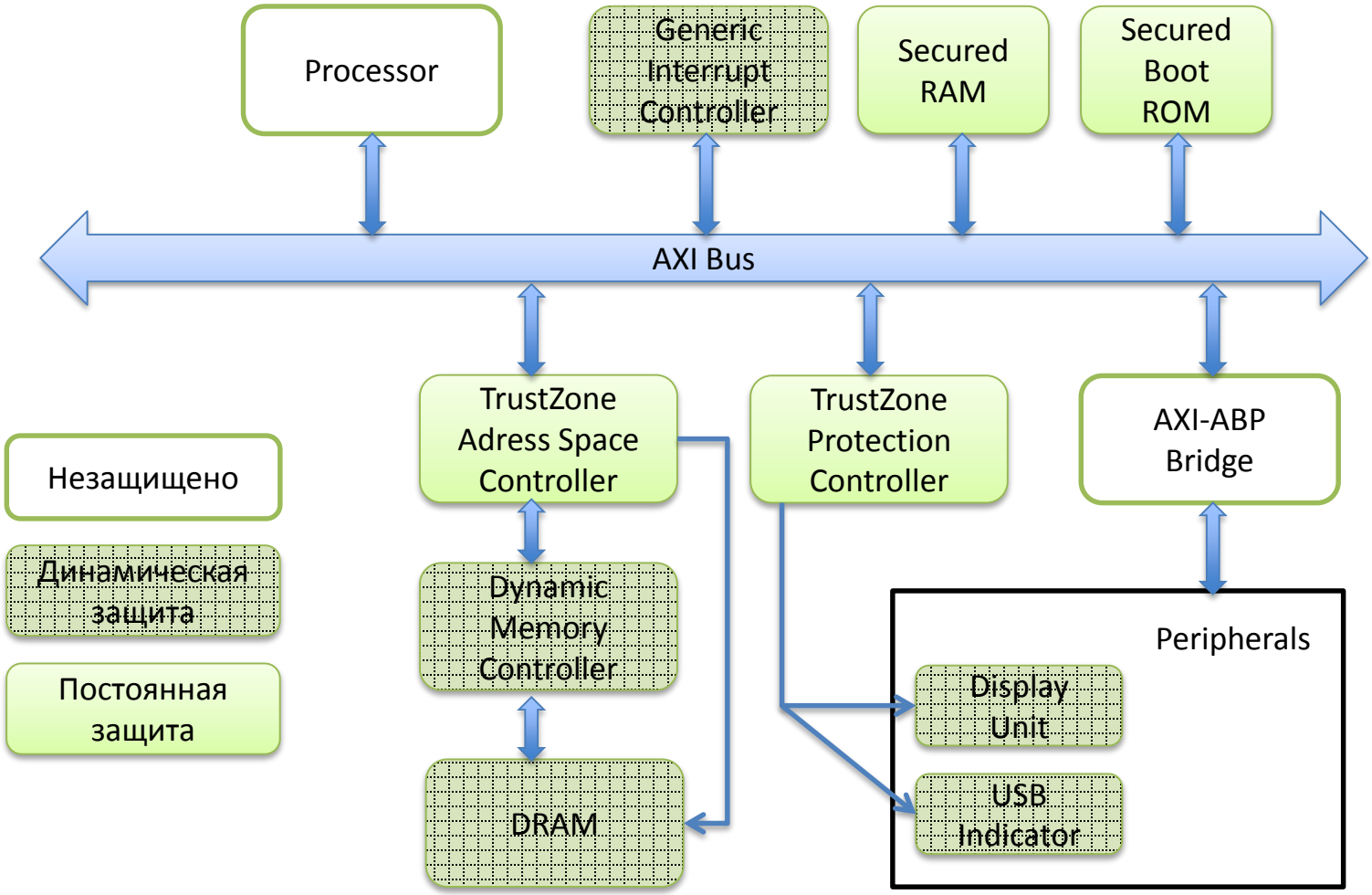
NFC и Secure Element



ARM TrustZone

- ARM Cortex-A57
- ARM Cortex-A53
- ARM Cortex-A17
- ARM Cortex-A15
- ARM Cortex-A9
- ARM Cortex-A8
- ARM Cortex-A7
- ARM Cortex-A5
- ARM1176

ARM TrustZone



Samsung Knox

- Основан на ARM TrustZone

- Отсутствует выделенный Secure Element
- Закрытая экосистема дистрибьюции приложений
- Многочисленный ошибки и уязвимости, связанные с превышением привилегий у недоверенного кода

Выводы

- На текущий момент единственной хорошо изученной и формально описанной реализацией доверенной среды является Java Card
- Необходимо создать отечественную модель безопасности для Java Card с учетом требований регуляторов
- Гармонизация и стандартизация API Java Card для работы с российской криптографией
- Реализация набора тестов для проверки корректности реализации российской криптографии в Java Card

Документация и полезные ссылки:

- Global Platform (http://www.globalplatform.org)
- ARM TrustZone (http://www.arm.com/products/processors/technologies/trustzone)
- TEE Emulator (https://github.com/Open-TEE)

Email: dudarev@bifit.com

Twitter: MikhailDudarev

СПАСИБО!