

OS DAY 2025

Механизмы изоляции при реализации «корня доверия». Интеграция с технологиями «корня доверия» в KasperskyOS

Антон Рыбаков,
руководитель группы
разработки функций
безопасности департамента
разработки KasperskyOS,
«Лаборатория Касперского»

Владимир Карантаев,
менеджер по анализу
эффективного
использования аппаратных
средств на базе
KasperskyOS,
«Лаборатория Касперского»



Владимир Карантаев

В ИТ и ИБ с 2002 года. Более 10 лет экспертной и прикладной деятельности в направлении Кибербезопасность АСУ ТП.

Соавтор и организатор первых киберучений национального уровня. Эксперт МЭК. Координатор Технологического комитета Альянса RISC-V. Лидер рабочей группы «Программно-аппаратные механизмы безопасности платформ на базе RISC-V».

К.т.н., автор экспертного курса лекций «Основы кибербезопасности РЗА энергосистем». Научный руководитель Центра практической кибербезопасности НТИ МЭИ, Кафедра РЗиАЭ.исполнения.



Антон Рыбаков

В 2007 году окончил Московский Университет Радиотехники, Электроники и Автоматики по специальности «Промышленная электроника».

Более 20 лет опыта в разработке системного и прикладного программного обеспечения, программно аппаратных комплексов, средств доверенной загрузки. Более 8 лет опыта в области построения доверенных сред исполнения.

Руководитель группы разработки функций безопасности KasperskyOS в «Лаборатории Касперского».



Владимир Карантаев

«Реализация доверенной среды исполнения на базе KasperskyOS – основа «Secure by Design»



Андрей Самоделов

«Корень доверия. Проектирование архитектуры системы управления ключами на основе Доверенного Хранилища в соответствии со спецификацией GP TrustedStorage».

Обзор источников требований и технологий Root of Trust (RoT, корень доверия)

Интегрированные функции безопасности – основа развития

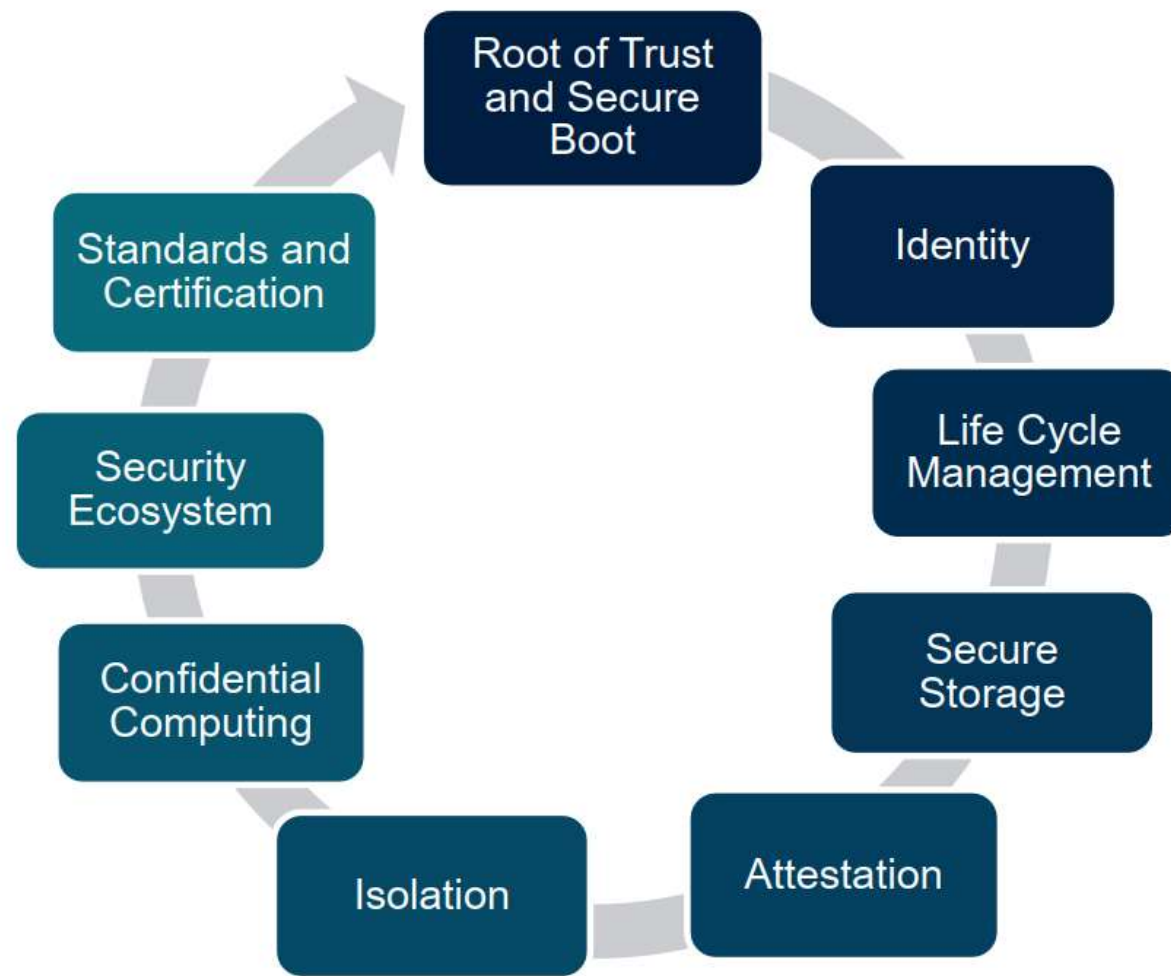
Доверенная система:

Система, для которой доказано (обосновано) соответствие целям безопасности при условии выполнения предположений безопасности. Примечание — доверенным может быть также элемент системы.

Конструктивный подход (к обеспечению информационной безопасности):

Подход, при использовании которого системе в процессе её создания с момента замысла придаются характеристики (свойства), которые должны обеспечивать соответствие целям безопасности, включая проверку такого соответствия.

Проект ГОСТ Р «Системы с конструктивной информационной безопасностью. Методология разработки»



Источник: Securing the Future of Open Source Computing

Аппаратная безопасность

Анализ угроз на стадиях жизненного цикла, включая:

- архитектуру системы команд (ISA);
- архитектурные принципы построения вычислительных систем общего и специального назначения;
- реализацию на микроархитектурном уровне.

Требования к жизненному циклу и процессам разработки микроцессорных систем/аппаратных средств – «Hardware **Secure** Development Lifecycle»:

- разработка и реализация требований к аппаратным механизмам безопасности;
- механизмы защищенной работы с памятью;
- реализация на уровне ISA аппаратного ускорения отечественных криптографических алгоритмов;
- противодействие бинарным уязвимостям на аппаратном уровне;
- противодействие атакам по побочным каналам;
- требования необходимо объединять с «отечественными маршрутами» разработки ЭКБ.



Источник: Securing the Future of Open Source Computing

Зарубежные аналоги:
NIST Hardware Security Program

NIST

(National Institute of Standards and Technology)

- Требования
- Система сертификация/оценки соответствия

ETSI (Smart Secure Platform)

IETF: Remote ATtestation ProcedureS (rats)

Требования к протоколам

TCG (Trusted Computing Group)

TPM 2.0 ISO/IEC 11889:2015

GlobalPlatform

PSA Certified

- Требования к RoT
- Системы сертификация/оценки соответствия
- Продукты для рынка
- Протоколы
- Open Source реализации требований к API

CHIPS Alliance

Open Compute Project (OCP)

Caliptra: RISC-V ядро VeeR EL2, RV32IMC

lowRISC

OpenTitan, RISC-V ядро Ibex, RV32IMCB

OpenTitan Earl Grey

OpenTitan Darjeeling

- Требования
- Разработка дизайнов аппаратных средств в проектах Open Source на основе открытых стандартов RISC-V
- Разработка встроенного ПО
- Разработка встроенного специального ПО

Common Criteria:

- Security IC Platform Protection Profile (PP-0035/PP-0055)
- Security IC Platform Protection Profile with Augmentation Packages (PP-0084)

Первый

- Аппаратные
- Программные

Второй

- Изменяемые/
Конфигурируемые
- Неизменяемые

Третий

По принципу изоляции:

- физически изолированный элемент безопасности, реализующий функции корня доверия;
- логическая или гибридная изоляция:
Обеспечивает логическую изоляцию в рамках SoC, с сохранением физической изоляции для ключевых security-блоков (OTBN, OTP);
- временная изоляция.

Четвертый:

Классификация корней доверия по функциональному назначению:

1. корень доверия для хранения;
2. корень доверия для измерений/оценки;
3. корень доверия для обновления ПО;
4. корень доверия для аутентификации;
5. корень доверия для шифрования;
6. корень доверия для безопасной загрузки;
7. корень доверия для доверенных исполняемых сред (TEE);
8. корень доверия для защиты цепочки поставок;
9. корень доверия для квантово-безопасной криптографии.

Варианты реализации корня доверия

Устройства с батарейным питанием: планшеты, смартфоны.

Устройства АСУ ТП:

- **IoT**-устройства на основе **MCU**
- устройства на основе Application CPU

Вариант 1

UDS (Unique Device Secret):

- ROM + OTP (One-Time Programmable) (варианты зависят от реализации, eFUSE и др.)
- PUF (SRAM PUF)+DICE.

Примеры:

- **NXP i.MX 8M**
- **RC 3588**
- **TI TDA4VH** и др.

Сценарии применения «корней доверия» 1, 3-8 (см. слайд 8).

Вариант 2

Отечественные:

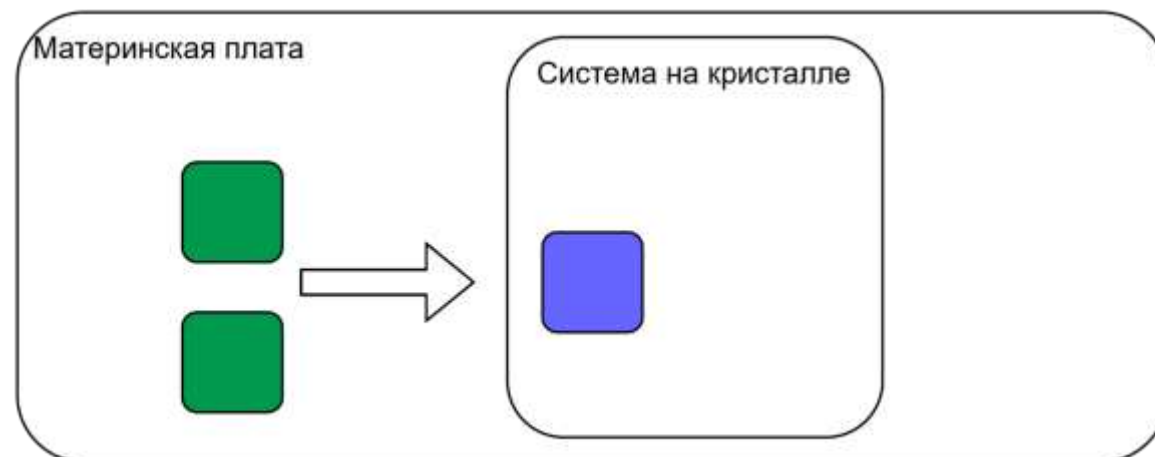
- Элвис «Доверенное ядро» в СнК Мсот 03 «СКИФ»

Зарубежные:

- RAMBUS
 - Коммерческое IP
 - Предсертифицированные в FIPS продукты

Проекты, реализуемые на основе открытых стандартов RISC-V в формате проектов Open Source :

- OpenTitan Darjeeling
- Caliptra



Вариант 3

Зарубежные

- Дискретные TPM (TPM 2.0):
 - Infineon TPM 2.0 (SLB 9665)
 - Fujitsu TPM 2.0 и д.р.

Сценарии применения «корней доверия» 1- 8 (см. слайд 8).

- SE:
 - Microchip ATECC608A (IoT TLS offload)
 - ST STSAFE-A110 (device identity)
 - Infineon OPTIGA Trust M (IoT provisioning)

- HSM:
Thales nShield HSM

Вариант 4

Проекты, реализуемые на основе открытых стандартов RISC-V в формате проектов Open Source :

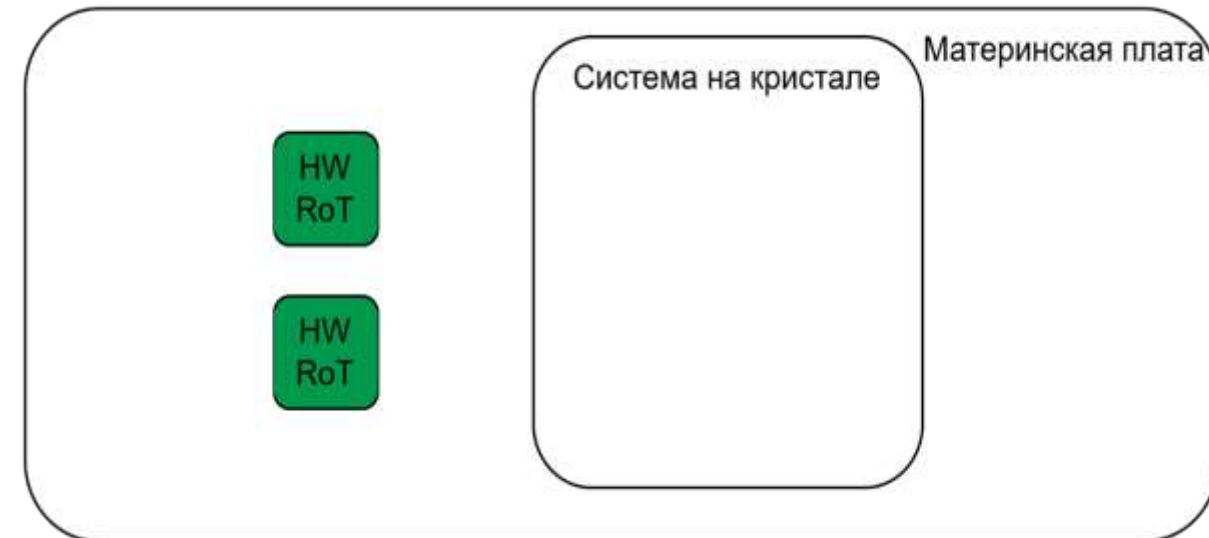
- OpenTitan Earl Grey

Сценарии применения «корней доверия» 1-8 (см. слайд 8), 9 в перспективе.

Отечественные

- SE
 - Аладдин
 - Актив
 - ИнфоТеКс: ViPNetSIESCore Nano
- HSM
 - ИнфоТеКс: ViPNetSIES Core

Сценарии применения «корней доверия» 1, 3-8 (см. слайд 8).



Варианты реализации корня доверия. Продолжение

Сценарии для «Облаков» — конфиденциальные вычисления:

- Серверы
- СХД

BMC: варианты реализации RoT:

- в виде отдельной микросхемы;
- в виде интегрированного в SoC BMC доверенного ядра.

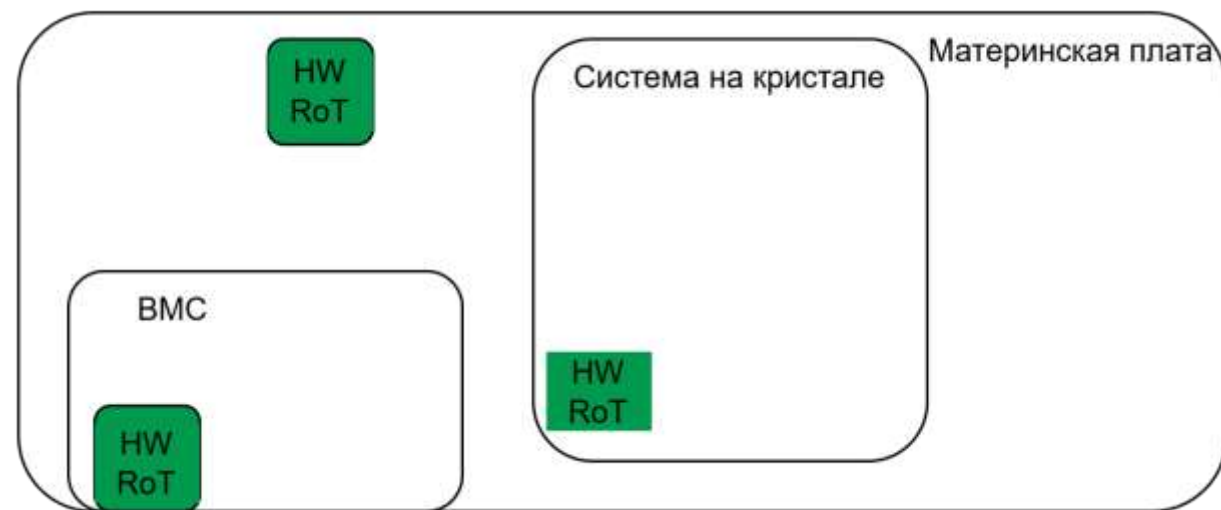
Проекты, реализуемые на основе открытых стандартов RISC-V в формате проектов Open Source:

- Open Compute Project (OCP) развивает спецификацию требований.

SoC для Серверов и СХД:

- OpenTitan Darjeeling
- Caliptra

Сценарии применения «корней доверия»: 1-9 по классификации со слайда 8



Возможности открытого стандарта RISC-V и Open Source

Открытый стандарт и проекты Open Source — предмет анализа и внимания.

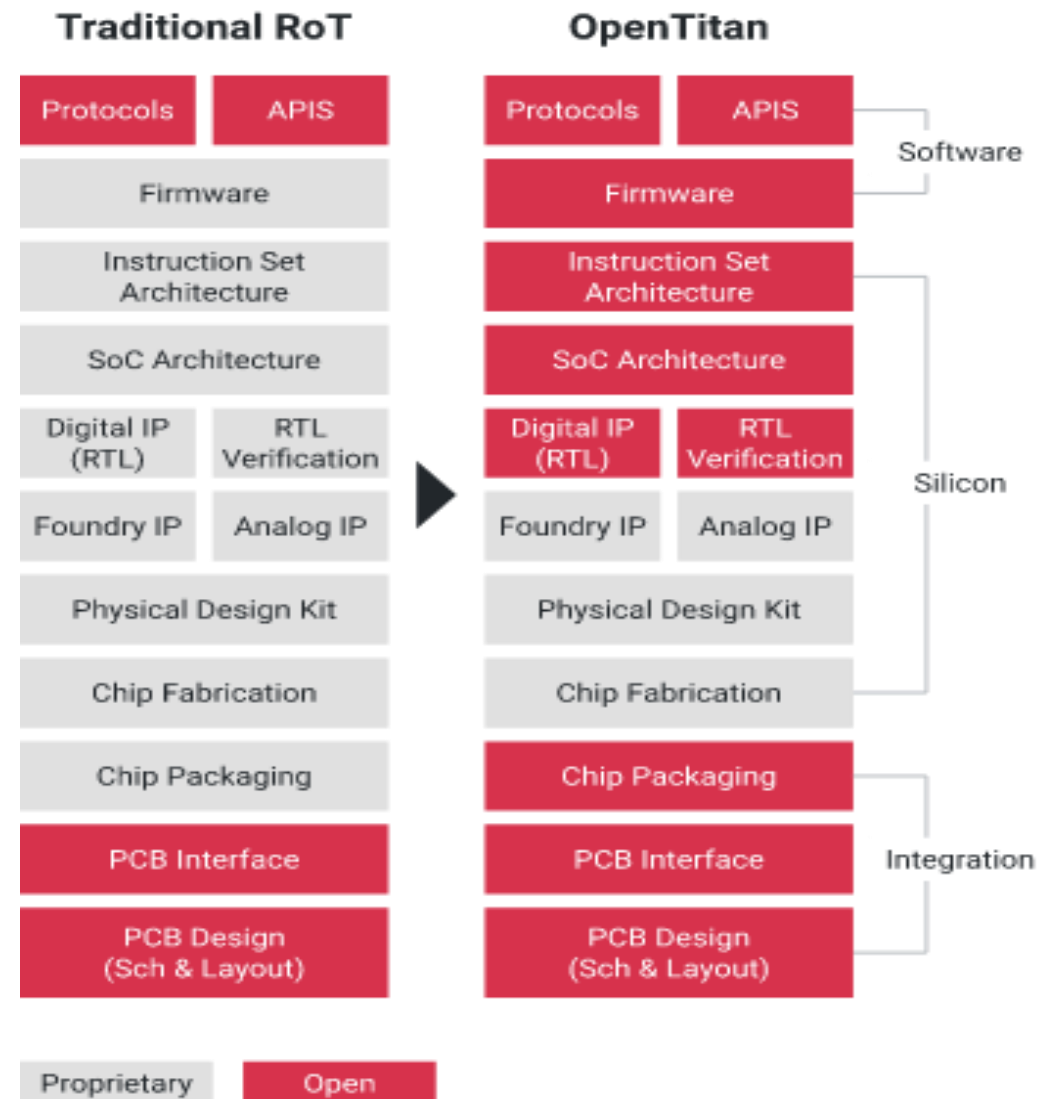
Открытая ISA. Возможность верификации, объем инструкций для реализации IP для ядра RoT будет сравнительно небольшим.

Микроархитектура. Возможность верифицировать код аппаратуры, так как он доступен или может быть предоставлен.

Возможность реализовать:

- аппаратное ускорение отечественных криптографических алгоритмов;
- механизмы изоляции, защищенной работы с памятью, противодействие атакам по побочным каналам.

Ускорение разработки ключевых технологий для построения защищенных ПАК и повышение доверия к результату.



Источник: https://embedded-recipes.org/2023/wpcontent/uploads/2023/10/Silicon_Root_of_Trust-Samuel-Ortiz.pdf

Уровень готовности проектов OpenTitan и Caliptra

	Open Titan		Caliptra
	OpenTitan Darjeeling	OpenTitan Earl Grey	
Тип	Отдельный чип	Secure Execution Environment в СнК	Отдельный Silicon RoT IP
ISA, Ядро	RISC-V ядро Ibex, RV32IMCB (harvard подобная архитектура)		RISC-V ядро VeeR EL2, RV32IMC
СС	Проекты ориентированы на соответствие EAL 4+ и выше. Формальная верификация на аппаратном уровне.		Проектируются с учетом самых высоких требований: EAL 6+. Формальная верификация на аппаратном уровне.
TCG (TPM)	RoT M, RoT I, DICE (Device Identifier Composition Engine)		
Изоляция	Аппаратный RBAC, ACL, разделение доменов		
Unique Device Secret	OTP, криптографический секрет.		OTP, SRAM PUF
Tape out	Подготовка к релизу	Да, 2023 год	Подготовка к tape out
ISO 21434	Да	Да	

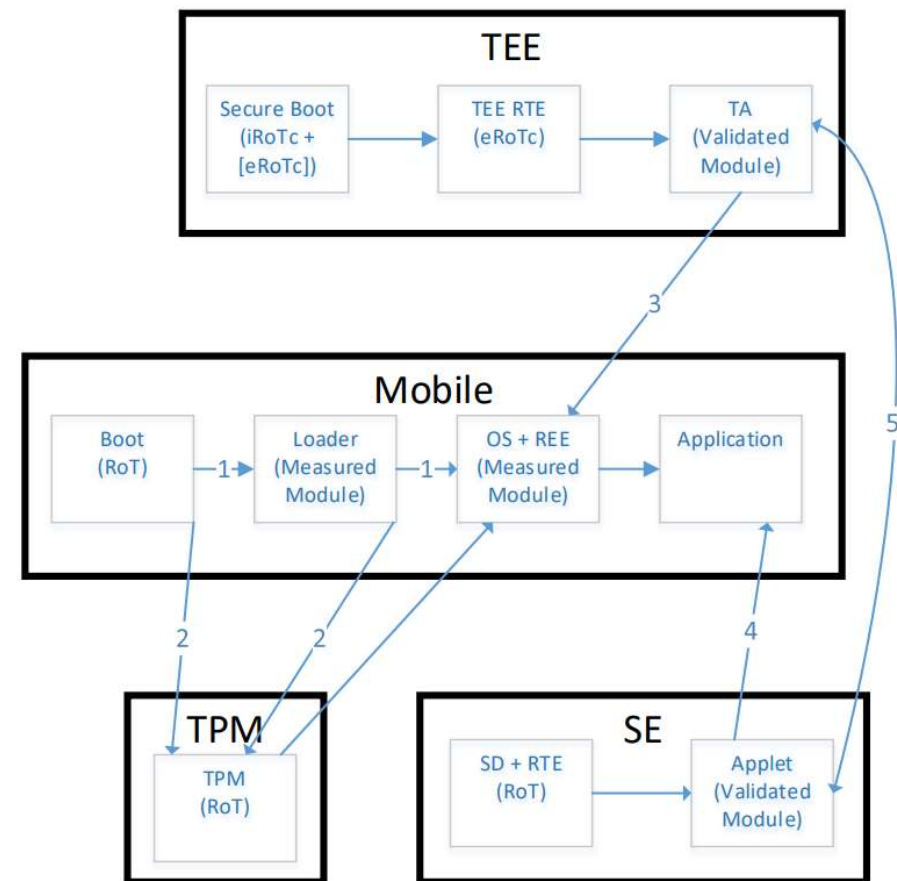
Технологии реализующие корень доверия

Конкретные реализации

- Secure Element — hardware roots of trust without the standard TPM interface.
- TPM:
 - В виде дискретного TPM (Отдельная микросхема)
 - fTPM — программная реализация, но с исполнением в средах с повышенными гарантиями защищенности.
 - vTPM — программная реализация.
- Корень доверия в виде IP, интегрированного в СнК — System on Chip's Root of Trust
- Корень доверия в виде отдельной микросхемы, интегрированной в SoM.

Обзор примеров использования показывает, что на практике могут применяться комбинации корней доверия, которые должны учитывать:

- влияние на себестоимость конечного изделия;
- сценарии использования ПАК и модель угроз;
- разработчик ОС должен поддержать необходимые варианты реализации.



Примеры использования корней доверия в устройстве

ГОСТ Защита информации. Корень доверия. Классификация. Термины и определения и Классификация

ГОСТ Защита информации. Корень доверия. Общие положения

ГОСТ Защита информации. Корень доверия. Сценарии использования

ГОСТ Защита информации. Корень доверия. Функциональные требования

ГОСТ Защита информации. Корень доверия. Требования к программному комплексу

ГОСТ Защита информации. Корень доверия. Классификация угроз

ГОСТ Защита информации. Корень доверия. Требования к безопасности/защищенности/доверенности

ГОСТ Защита информации. Корень доверия. Требования к оценке соответствия

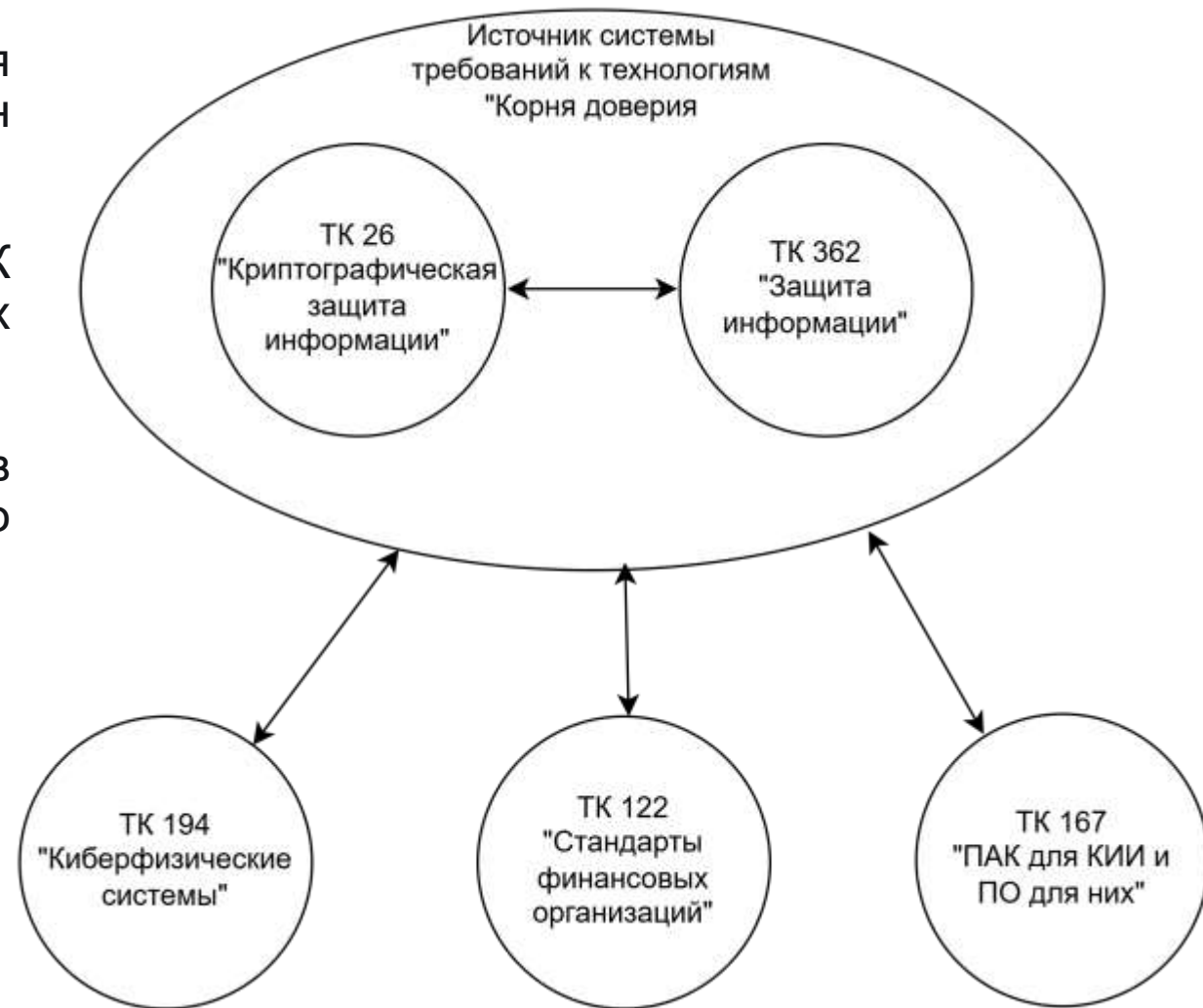
ГОСТ Защита информации. Корень доверия «Отраслевые профили»

Взаимодействия по реализации требований НТД

В 2025 году определить приоритетные для разработки ГОСТ, обеспечить внесение в «План стандартизации».

Синхронизировать с заинтересованными ТК РосСтандарта внесение изменений в НТД в зоне их ответственности.

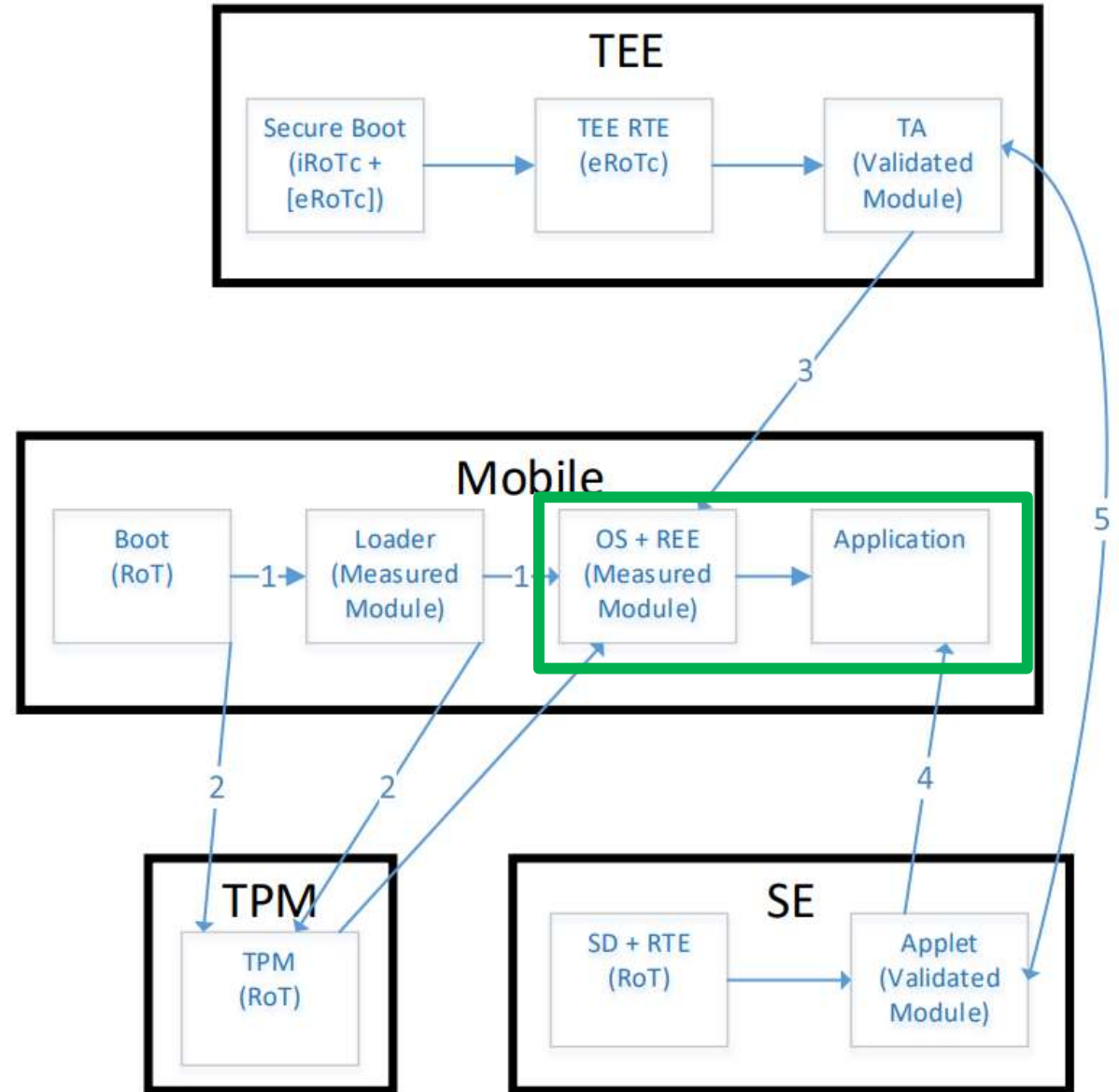
Синхронизировать планы по развитию НТД в сфере «аппаратной безопасности» с планами по развитию «отечественных маршрутов ЭКБ».



Взаимодействие с корнем доверия в KasperskyOS

Вызовы

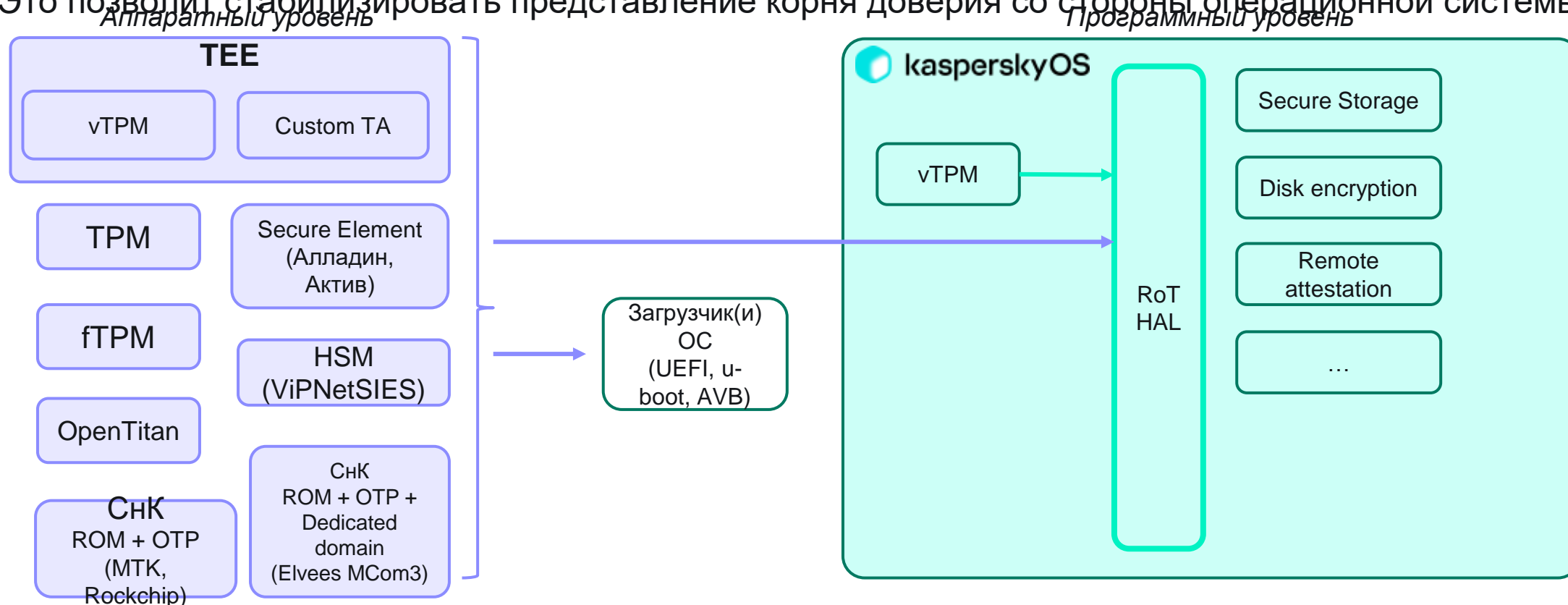
- Большое количество технологий RoT
- Гетерогенная структура в рамках одной ИС
- Безопасность



Задача

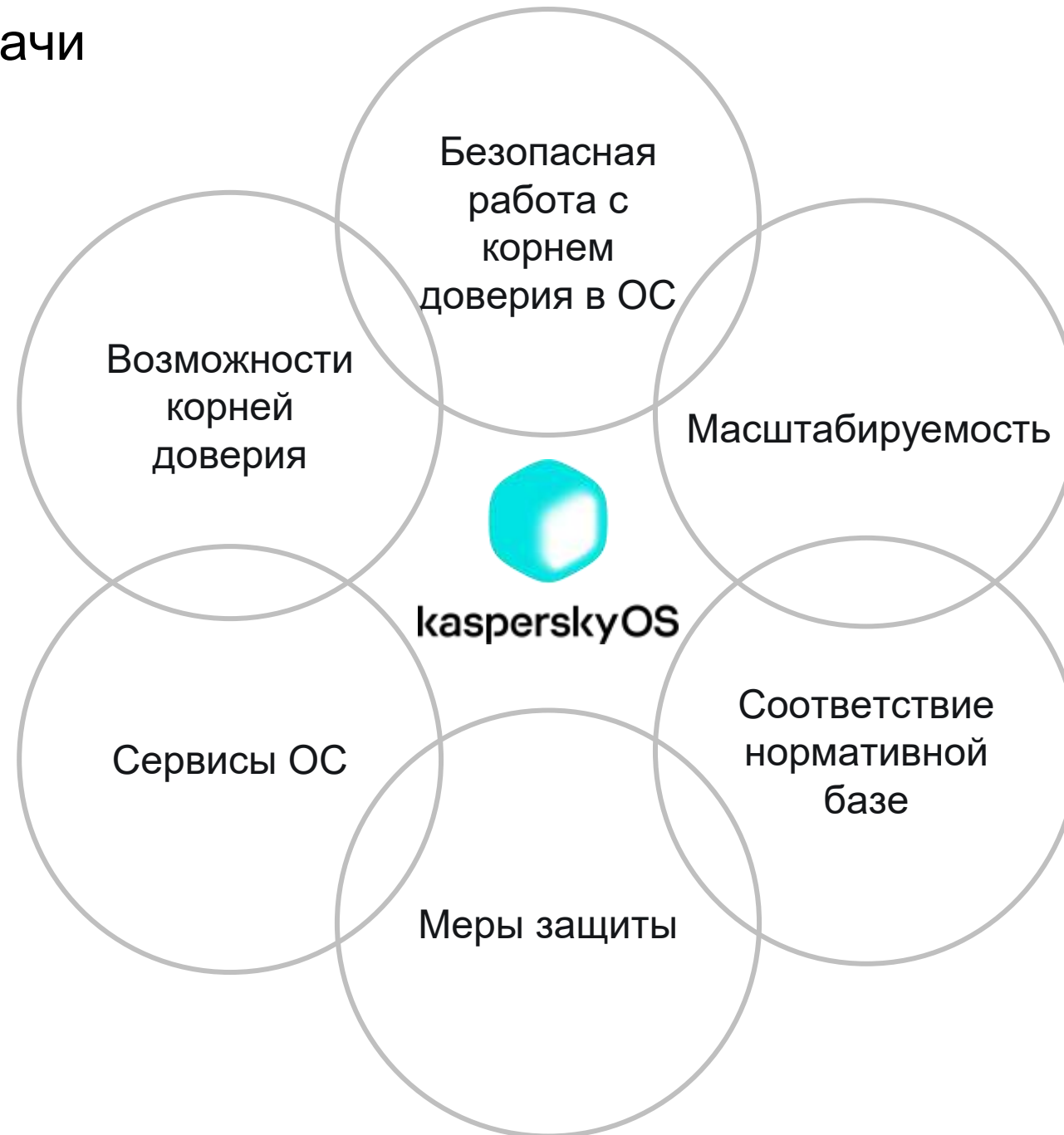
Необходимо создать **унифицированный HAL-интерфейс для организации корня доверия в KasperskyOS** — KasperskyOS Root of Trust (KRoT) HAL, который будет использоваться сервисами в KasperskyOS.

Это позволит стабилизировать представление корня доверия со стороны операционной системы



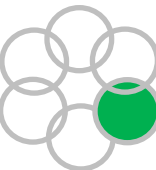
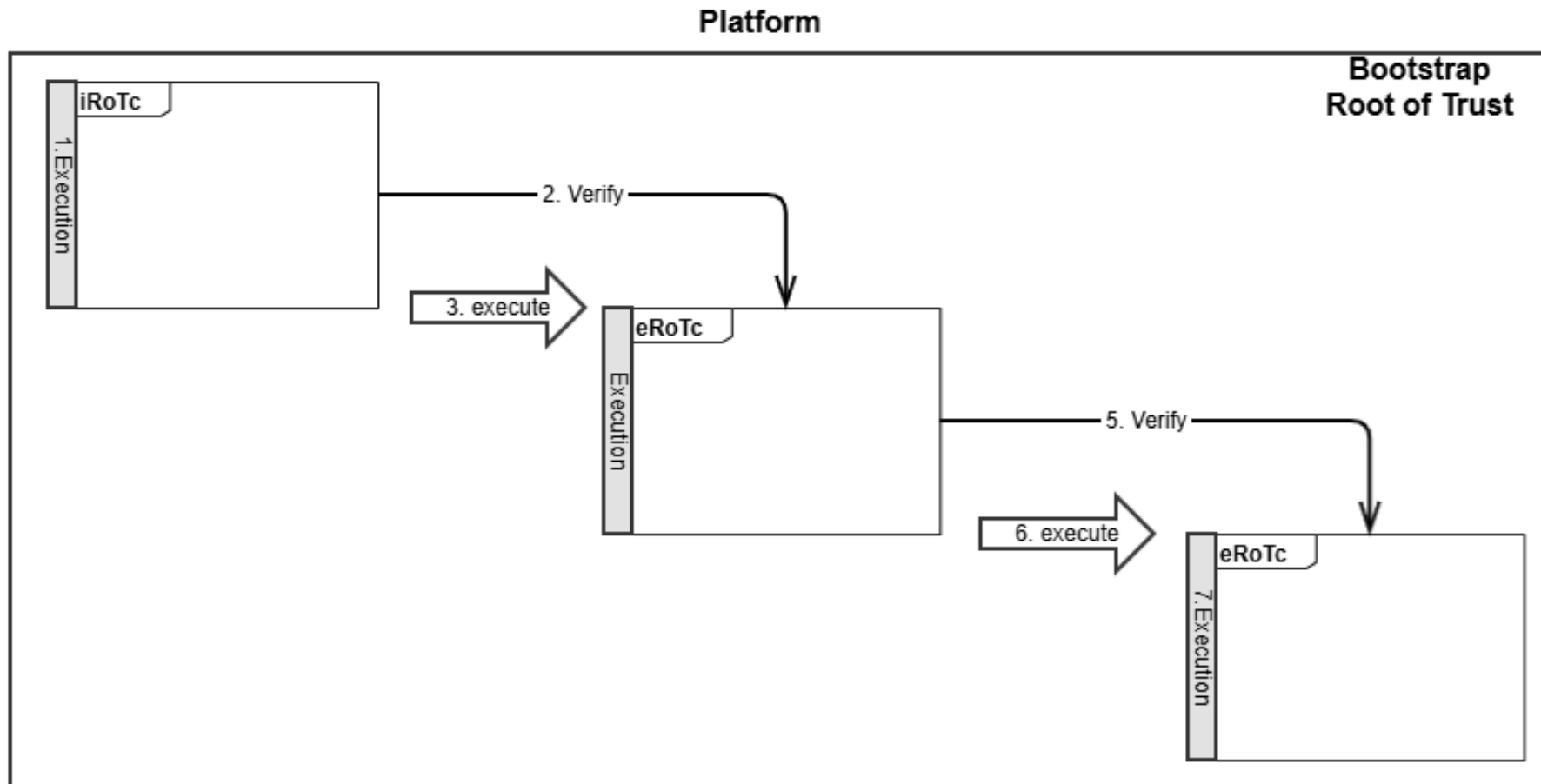
Root of Trust (RoT) is a source that can always be trusted within a cryptographic system. Because cryptographic security is dependent on keys to encrypt and decrypt data and perform functions such as generating digital signatures and verifying signatures, RoT schemes generally include a hardened hardware module. (Thales)

Декомпозиция задачи



Система требований к корню доверия

Стандарт Global Platform — Root of Trust Definitions and Requirements определяет понятие Bootstrapped Root of Trust.

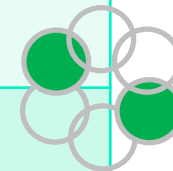


Система требований к корню доверия

Стандарт Global Platform — Root of Trust Definitions and Requirements

- определяет понятие Bootstrapped Root of Trust
- определяет набор сервисов корня доверия

Сервис	Детализация
4.1 Authentication Service	The Root of Trust for Authentication maintains one or more shielded locations for the purpose of securely storing and preserving the integrity of at least one credential [...]
4.2 Confidentiality Service	The Root of Trust for Confidentiality maintains shielded locations for the purpose of storing sensitive data, such as secret keys and passwords.
4.3 Identification (of a Root of Trust) Service	The Root of Trust for Identification maintains a shielded location for storing a secret value, such as a symmetric key or an asymmetric private key, for the purpose of establishing the identity of the Root of Trust [...]
4.4 Integrity Service	The Root of Trust for Integrity maintains shielded locations for the purpose of storing and protecting the integrity of non-secret critical security parameters and platform characteristics. Critical security parameters include, but are not limited to, authorization values, public keys, and public key certificates [...]
4.5 Measurement Service	The Root of Trust for Measurement provides the ability to reliably create platform characteristics [...]
4.6 Authorization Service	The Root of Trust for Authorization provides reliable capabilities to assess authorization tokens and determine whether or not they satisfy policies for access control [...]
4.7 Reporting Service	The Root of Trust for Reporting reliably reports platform characteristics. It provides an interface that limits its services to providing reports on its platform characteristics authenticated by a platform identity [...]
4.8 Update Service	The Root of Trust for Update verifies the integrity and authenticity of signed updates, and upon successful verification, authorizes the initiation of the update process. A platform may employ a Root of Trust for Update to update the code and data for Roots of Trust, including itself. Non-Root-of-Trust platform software may also utilize the Root of Trust for Update for updates [...]
4.9 Verification Service	The Root of Trust for Verification verifies the integrity and authenticity of signed objects. Objects may include, but are not limited to, public keys, code, and data [...]



Сопоставление сценариев в ОС и сервисов корня доверия

При разработке мер защиты KasperskyOS учитываются требования нормативной базы ФСТЭК (<https://bdu.fstec.ru/threat-section/defenses>)

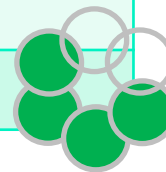
Группа мер защиты	Описание	Сценарии ОС
ОЦЛ	Обеспечение целостности	Контроль целостности/подлинности программных компонентов ОС и приложений
		Конфиденциальность ключей全盘ового шифрования
		Конфиденциальность ключей шифрования доверенного хранилища
ОПС	Ограничение программной среды	Контроль целостности/подлинности программных компонентов ОС и приложений
ОПО	ОПО Управление обновлениями программного обеспечения	Контроль целостности/подлинности программных компонентов ОС и приложений
		Конфиденциальность индексов защиты от отката версии
ИАФ	ИАФ Идентификация и аутентификация	Конфиденциальность уникальных идентификаторов устройства

Источник: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17>

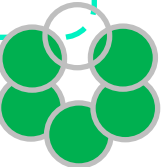
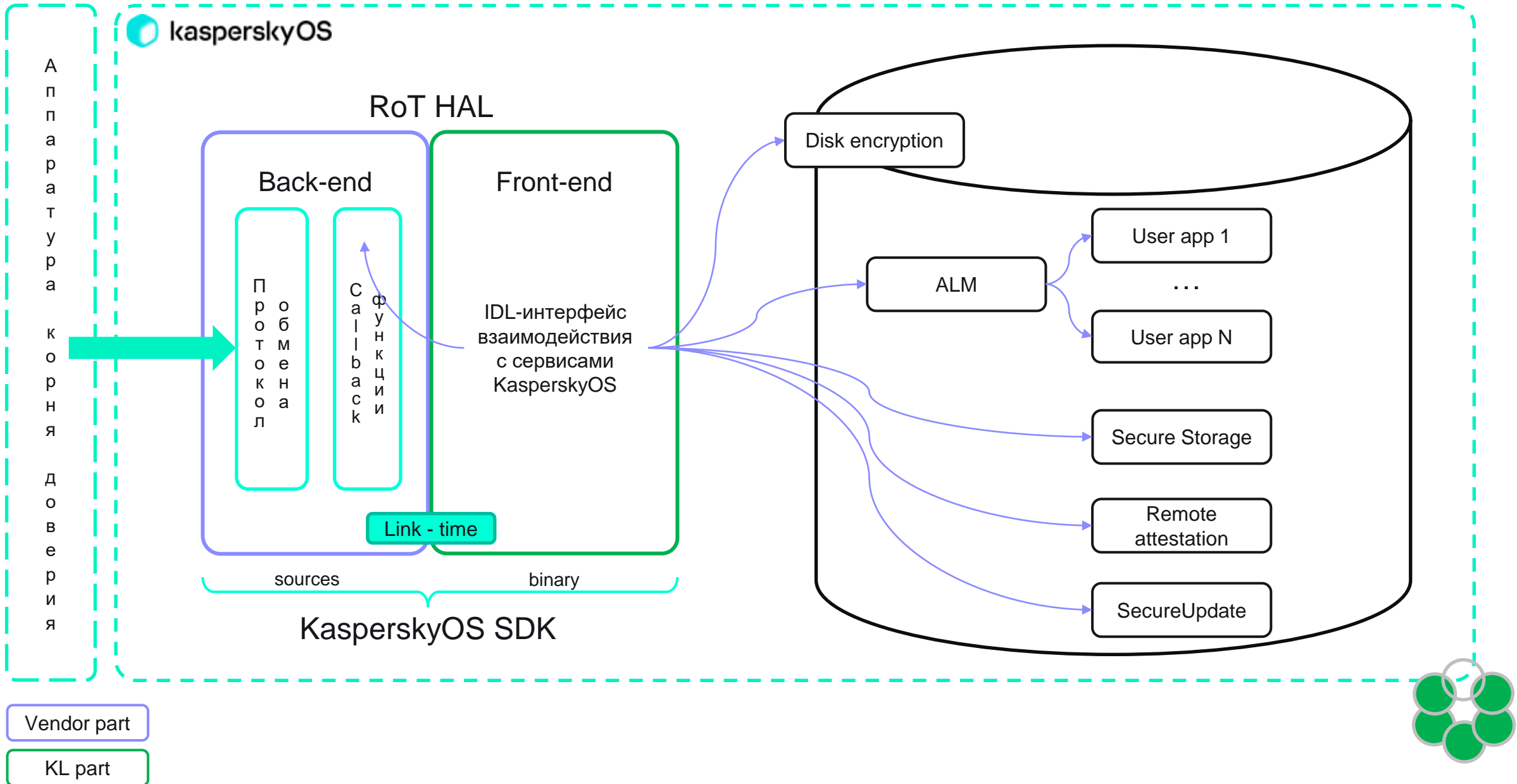
При реализации сценариев ОС опираемся на сервисы корня доверия из стандарта Global Platform

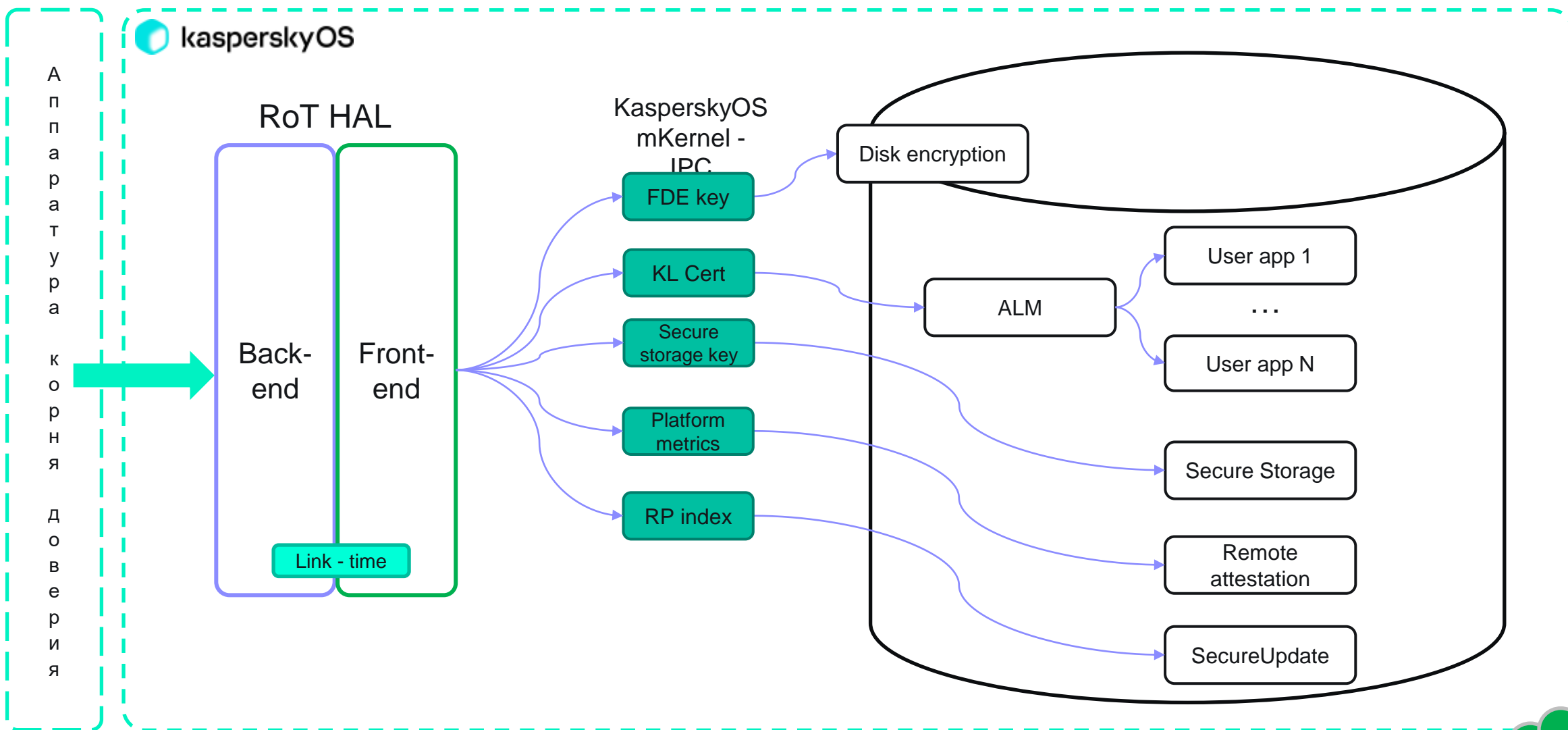
Сервис	Типы данных	Описание
Confidentiality	Ключи	Ключи симметричного шифрования для использования в сценариях платформенных сервисов (например ключ Secure Storage)
	Индексы защиты от отката	Индексы защиты от отката версии (для использования в сценариях обновления ОС, загрузчиков, ДСИ)
Integrity	Сертификаты	Сертификаты публичного ключа для проверки подписи (например - проверка цепочки загрузчиков, образа ОС в ходе Secure / Trusted Boot, сервисов ОС, пользовательских приложений)
	Списки отзыва	Список отозванных сертификатов для проверок образов обновления ОС, загрузчиков, ДСИ
Measurement	Уникальные идентификаторы	Уникальные идентификаторы для идентификации устройства, версии сборки и т.д. (например идентификатор устройства для облачной платформы)

Источник: https://globalplatform.org/specs-library/root-of-trust-definitions-and-requirements-v1-1-gp-req_025/

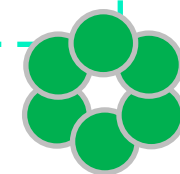


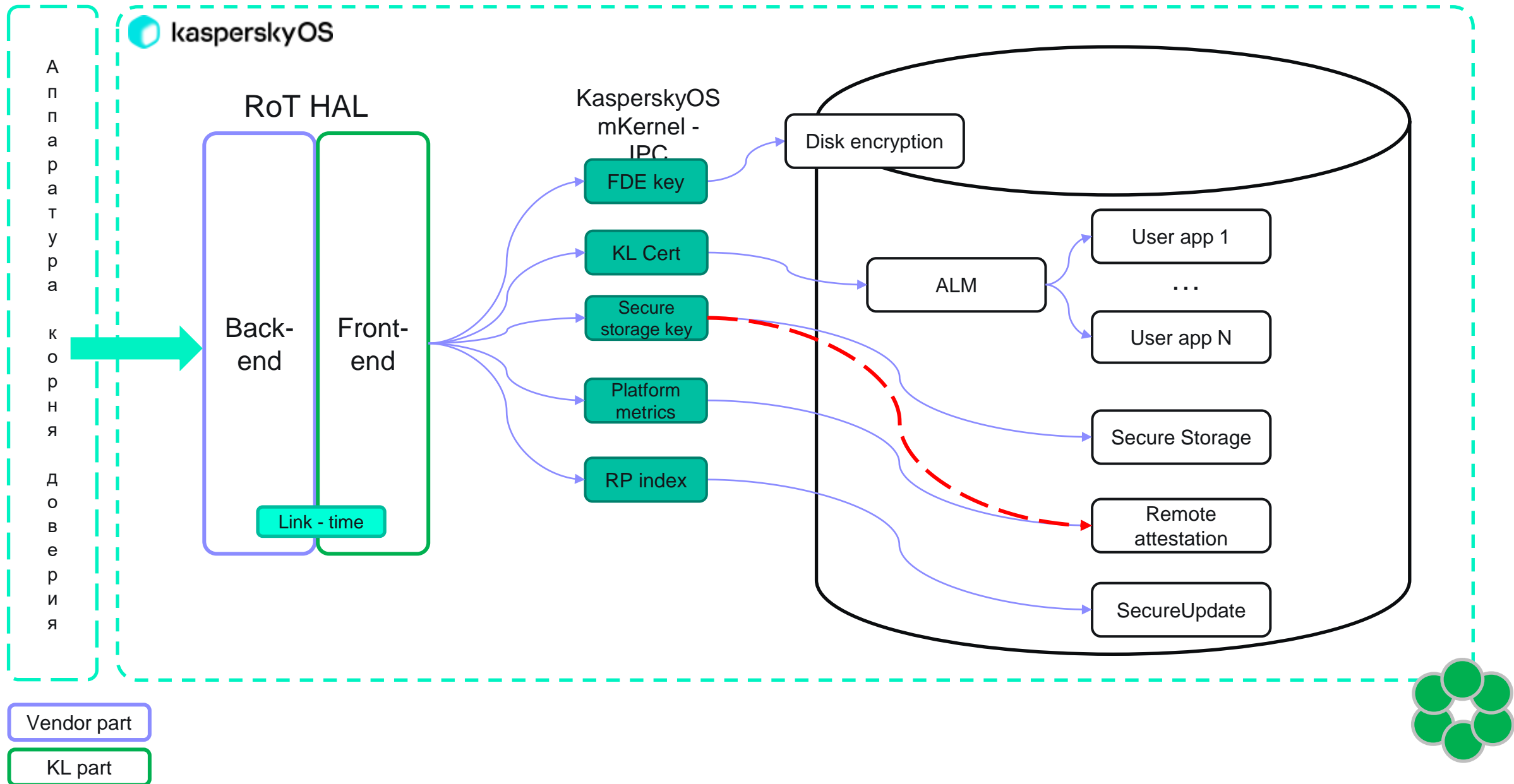
Верхнеуровневая архитектура решения — масштабируемость



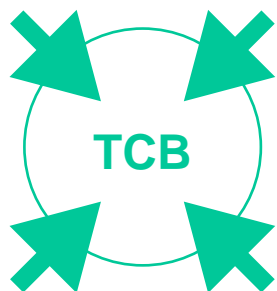


Vendor part
KL part





Minimization of trusted
code base

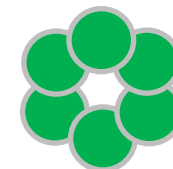
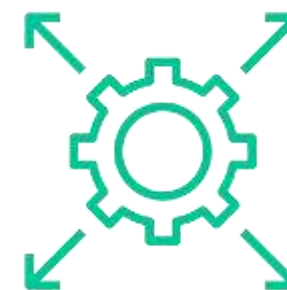


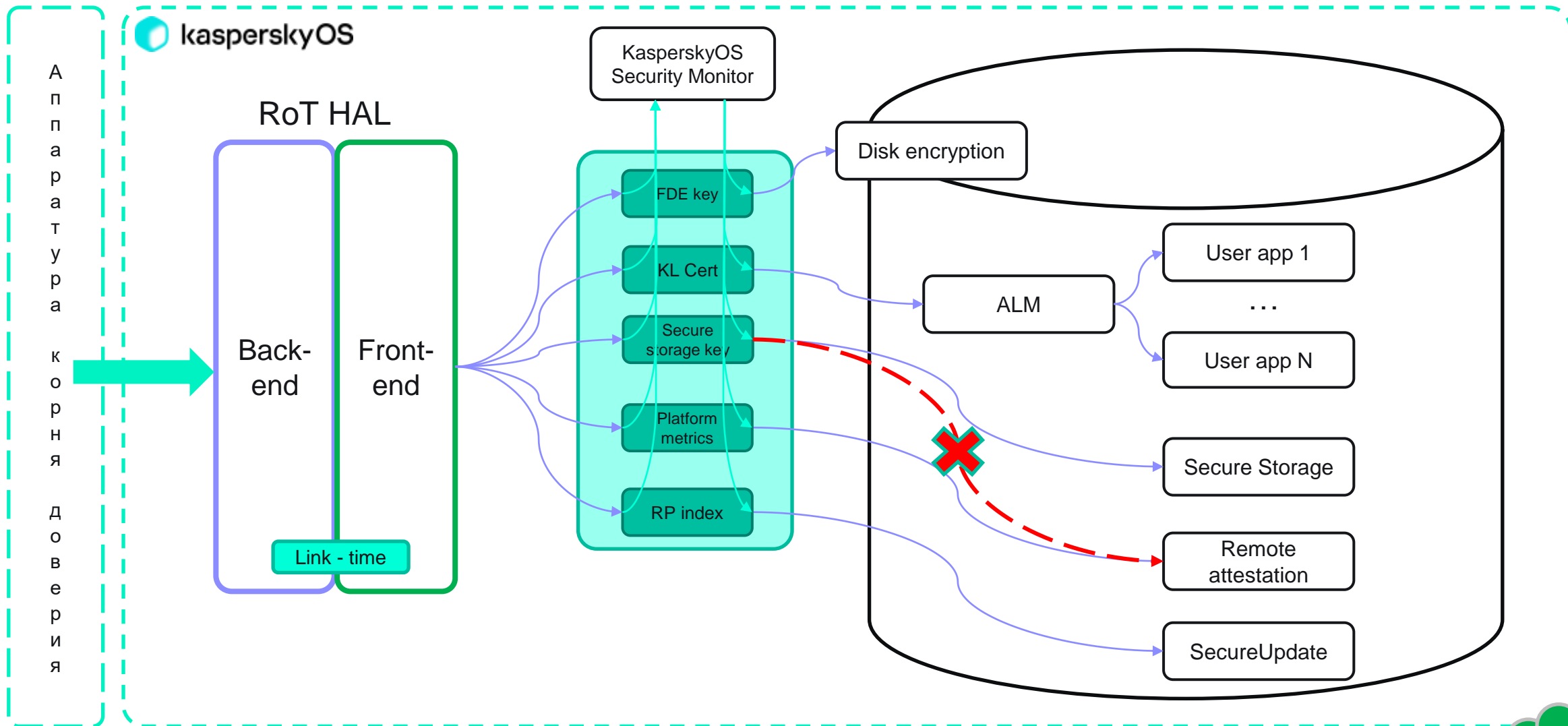
Microkernel design

Multiple Independent Levels
of Security (MILS)

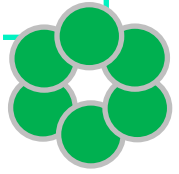


Flux Advanced Security
Kernel (FLASK)





Vendor part
KL part



Заключение

- Корень доверия — основа построения доверенных систем (trustworthy)
- Корень доверия — лежит в основе предположений о доверии, обеспечения целостности и подлинности ключевых элементов программной среды (ядра ОС, драйверов, системного и ключевого прикладного ПО)
- Открытый стандарт RISC-V для решения полного диапазона задач обеспечивает наименьшую совокупную стоимость владения
- Способен обеспечить технологическую основу для решения национальных задач, в т.ч. по безопасности и доверенной среде исполнения
- Актуальной задачей является разработка нормативно-технических требований к совокупности технологий, связанных с понятием «корень доверия»
- Приведены сценарии ОС общего назначения с опорой на корень доверия
- Приведена высокоуровневая архитектура интеграции корня доверия в KasperskyOS

Спасибо за внимание!



Пройдите опрос о KasperskyOS
и получите приз на стенде

Владимир Карантаев
Vladimir.Ge.Karantaev@kaspersky.com



Узнайте больше о разработке
под KasperskyOS

Антон Рыбаков
Anton.Rybakov@kaspersky.com

