Повышение защищенности доверенного хранилища GPD Trusted Storage на основе технологии ARM TrustZone и особенностей архитектуры СнК с ядрами ARM v.8

Андрей Самоделов
Системный аналитик,
«Лаборатория Касперского»

kaspersky

Содержание

Цели доклада

В докладе рассмотрены результаты исследований и проектирования архитектуры системы управления ключами на основе Доверенного Хранилища в соответствии со спецификацией GP Trusted Storage.

Для повышения защищенности операций с хранилищем используется СнК с кластером ядер ARM Cortex-A v.8 и расширениями безопасности ARM TrustZone (ARM TZ). Такая архитектура позволяет изолировать среду исполнения общего назначения для запуска пользовательских приложений (Non-Secure World ARM TZ, REE) от доверенной среды исполнения для выполнения особо критичных (например, криптографических) операций (Secure World ARM TZ, TEE).

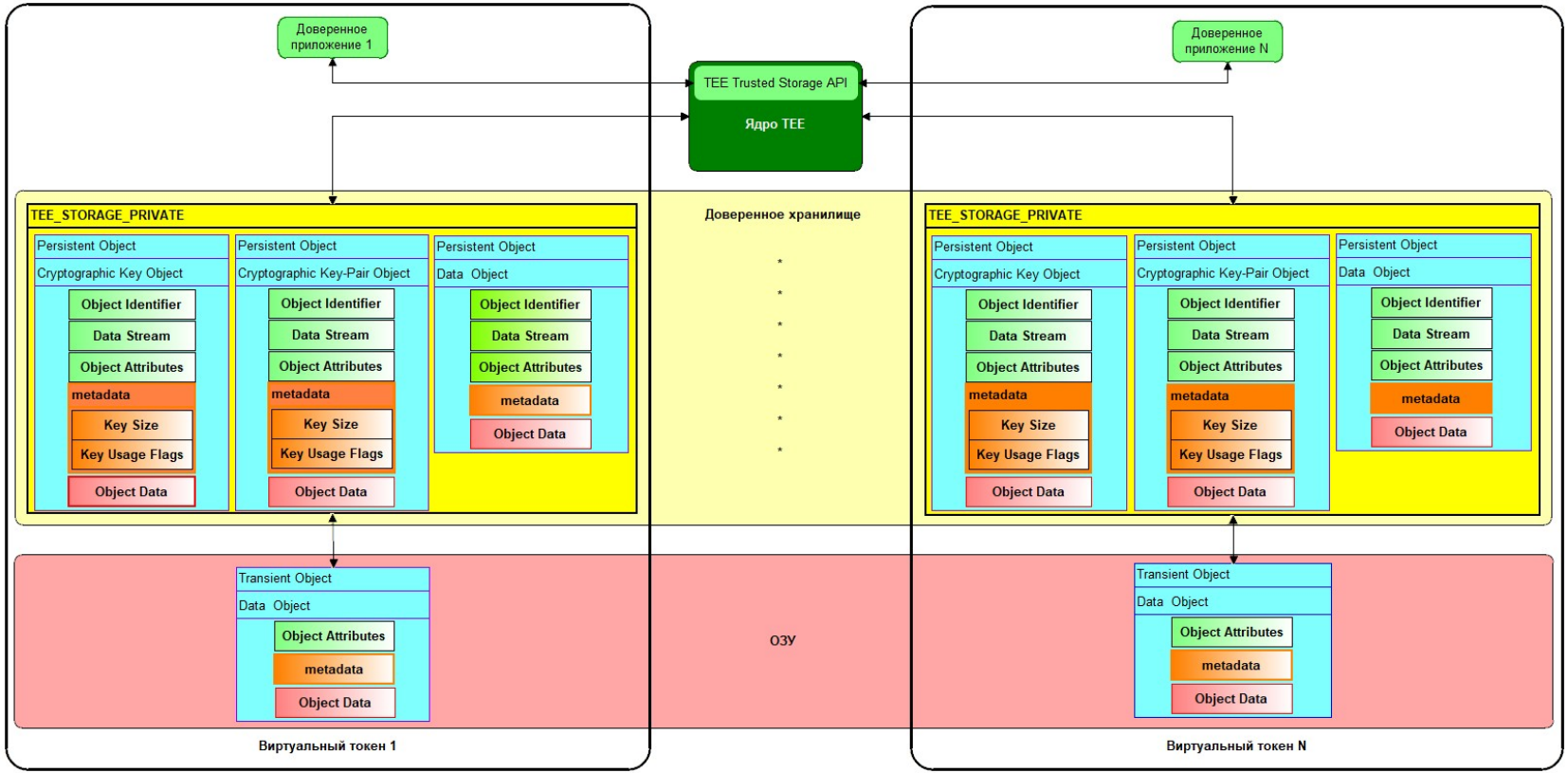
С целью получения еще большей защищенности решения, в архитектуру процессора добавлен дополнительный изолированный контур (ИК), который предназначен для генерации ключей, доверенного хранения/экспорта/импорта системных криптографических ключей, а также изоляции самих системных ключей и операций с их участием от TEE. Обмен данными между ИК и TEE происходит с помощью выделенной области (двухпортовой) памяти (почтовый ящик).

Предлагаемый подход может служить для уменьшения времени разработки ПО для ПАК СЗИ и, в дальнейшем, упрощения сертификации.

Объектная модель Доверенного Хранилища в соответствии со спецификацией GP Trusted Storage[1]

[1] Использована полная спецификация Доверенного Хранилища, приведенная в Разделе 5 «Trusted Storage API for Data and Keys» документа «GlobalPlatform Technology. TEE Internal Core API Specification Version 1.2.1» (GPD_TEE_Internal_Core_API_Specification_v1.2.1_CC.pdf)

Блок-схема Доверенного Хранилища



kaspersky

Принципы функционирования Доверенного Хранилища

В соответствии со спецификацией GP Trusted Storage Доверенное Хранилище состоит из виртуальных токенов, которые включают в себя:

- доверенное приложение (трастлет);
- раздел на внешнем хранилище (SD/MMC/eMMC/SSD/HDD…) с объектами хранения (контейнерами);
- буферную область памяти для промежуточных операций с объектами хранения.

Каждое доверенное приложение (криптографическим способом) привязывается к собственному разделу Доверенного Хранилища.

Объекты хранения делятся на 3 типа:

- объект (контейнер) криптографического ключа;
- объект (контейнер) криптографической ключевой пары;
- объект данных.

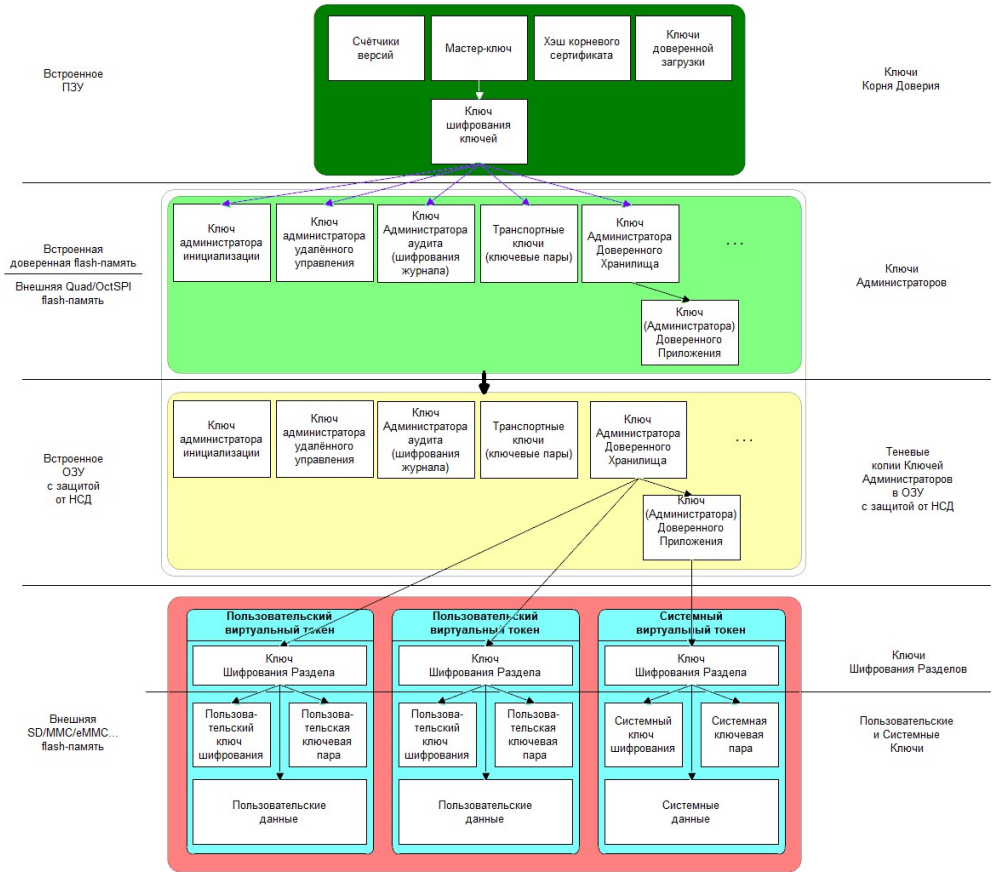
В состав каждого типа объекта входят:

- идентификационная информация;
- метаданные;
- сами хранимые активы.

Для объектов ключей/ключевых пар в состав метаданных входит информация о длине ключей и алгоритмах, в которых соответствующие ключи могут использоваться.

Ключевая структура решения

Ключевая структура решения



Для защиты пользовательских (и системных) данных необходима определенная ключевая структура, позволяющая осуществлять администрирование устройства и гарантирующая целостность и конфиденциальность хранимой информации.

Для рассматриваемой архитектуры ключевая структура состоит из пяти уровней:

1. Ключи Корня Доверия
2. Ключи Администраторов и Транспортные Ключи
3. Теневые копии Ключей Администраторов в ОЗУ с защитой от НСД
4. Ключи Шифрования Разделов
5. Пользовательские и Системные Ключи

Ключи уровней 2, 4 и 5 зашифрованы на ключах вышележащих уровней.
Ключи уровня 3 располагаются в ОЗУ под масками с контрольными суммами.

kaspersky

Ключевая структура решения

Корень доверия

Ключевая структура решения построена по иерархическому принципу.
В основе иерархии лежит симметричный мастер-ключ (Hardware Unique Key, HUK), который хранится
во внутреннем ПЗУ, входящем в состав изолированного контура. Мастер-ключ программируется в заводских условиях при изготовлении процессора и является неизвлекаемым секретом.

На основе мастер-ключа (для уменьшения нагрузки на него и возможности повторной инициализации устройства) при первичной инициализации устройства генерируется ключ шифрования ключей
(Key Encryption Key, KEK), длина которого определяется используемым алгоритмом шифрования и требованиями локальных регуляций.

Оба этих ключа, совместно с ключами доверенной загрузки и хешем корневого сертификата (публичного ключа корневого сертификата), образуют корень доверия (Root of Trust, RoT) всего устройства.

Ключевая структура решения

Ключи первого уровня иерархии

К ключам первого уровня иерархии относятся:

- Ключ Администратора инициализации;
- Ключ Администратора удаленного управления
- Ключ Администратора аудита (ключ шифрования журнала аудита);
- Транспортные ключи (ТКШ)/ключевые пары (ТКП);
- Ключ Администратора Доверенного Хранилища (КШАДХ);
- Ключи (Администраторов) Доверенных Приложений (КШАДП).

Ключи первого уровня иерархии зашифрованы на ключе KEK и могут хранится либо в накристальной flash-памяти, доступной только для ИК, либо во внешней flash-памяти, доступной только через периферийный интерфейс ИК.
Ключи (Администраторов) Доверенных Приложений зашифрованы на Ключе Администратора Доверенного Хранилища и могут использоваться совместно с КШАДХ для защиты системных данных, что повышает степень их защищенности.

Ключи второго уровня иерархии

При наличии в составе СнК ОЗУ с защитой от несанкционированного доступа (НСД), один или несколько ключей первого уровня иерархии могут быть (с помощью специальной команды) расшифрованы и размещены под маской и с контрольными сумами в ОЗУ с защитой от НСД. Это позволяет повысить общую производительность, например, в операциях с доверенным хранилищем и уменьшить общую нагрузку на ключ KEK.

В случае использования ОЗУ с защитой от НСД в его составе должен присутствовать блок гарантированной очистки ОЗУ при наступлении события НСД с (встроенным) автономным источником питания, с емкостью, достаточной для полного выполнения операции.

Ключевая структура решения

Ключи третьего уровня иерархии

К ключам третьего уровня иерархии относятся:

- Ключи Шифрования Разделов Доверенного Хранилища (КШРДХ).

Ключи шифрования Разделов Доверенного Хранилища зашифрованы на Ключах Шифрования Администраторов Доверенного Хранилища (КШАДХ) и/или на Ключах Шифрования (Администраторов) Доверенных Приложений (КШАДП) и хранятся в зашифрованном виде в заголовках Разделов Доверенного Хранилища.

Раздел Доверенного Хранилища может принадлежать:

- Реальному пользователю, для хранения ключей (ПКШ)/ключевых пар (ПКП) и произвольных данных (ПД).
- Виртуальному пользователю, в качестве которого может выступать любое из приложений, для хранения ключей, начальных настроек и прочих критичных для приложения данных.

Ключевая структура решения

Ключи четвертого уровня иерархии

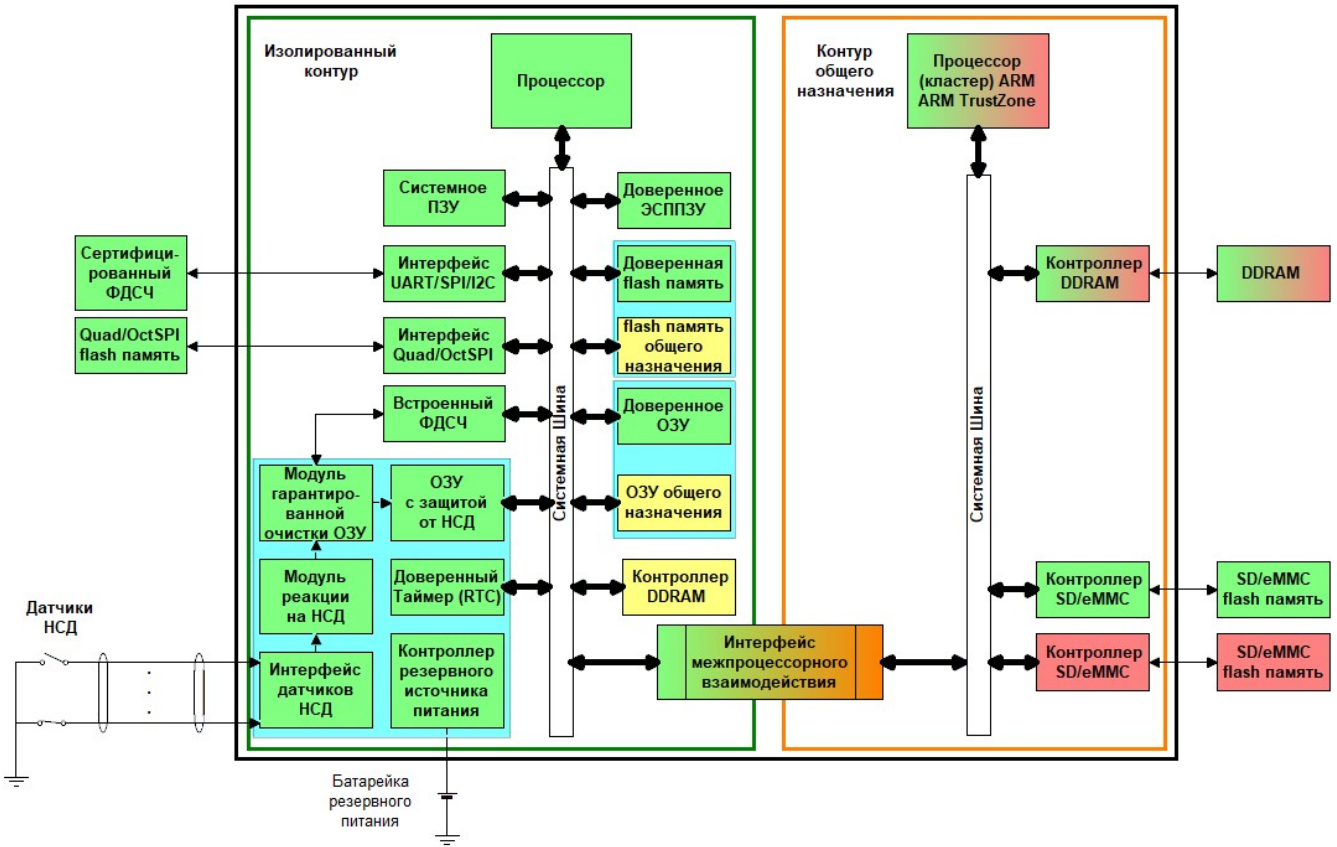
К ключам четвертого уровня иерархии относятся:

- Пользовательские ключи/ключевые пары, хранящиеся в Разделах Доверенного Хранилища.

Все ключи и произвольные данные внутри Раздела Доверенного Хранилища зашифрованы на уникальном для каждого раздела Ключе Шифрования Раздела Доверенного Хранилища (КШР), который хранится в заголовке раздела зашифрованным на Ключе Шифрования Администратора Доверенного Хранилища (КШАДХ).
Для Разделов Доверенного Хранилища, привязанных к Доверенным Приложениям, для шифрования КШР может использоваться уникальный для каждого приложения Ключ (Администратора) Доверенного Приложения КШАДП.

Архитектура процессора для реализации Доверенного Хранилища с повышенной степенью защищенности

Упрощенная блок-схема процессора



kaspersky

Функции процессора

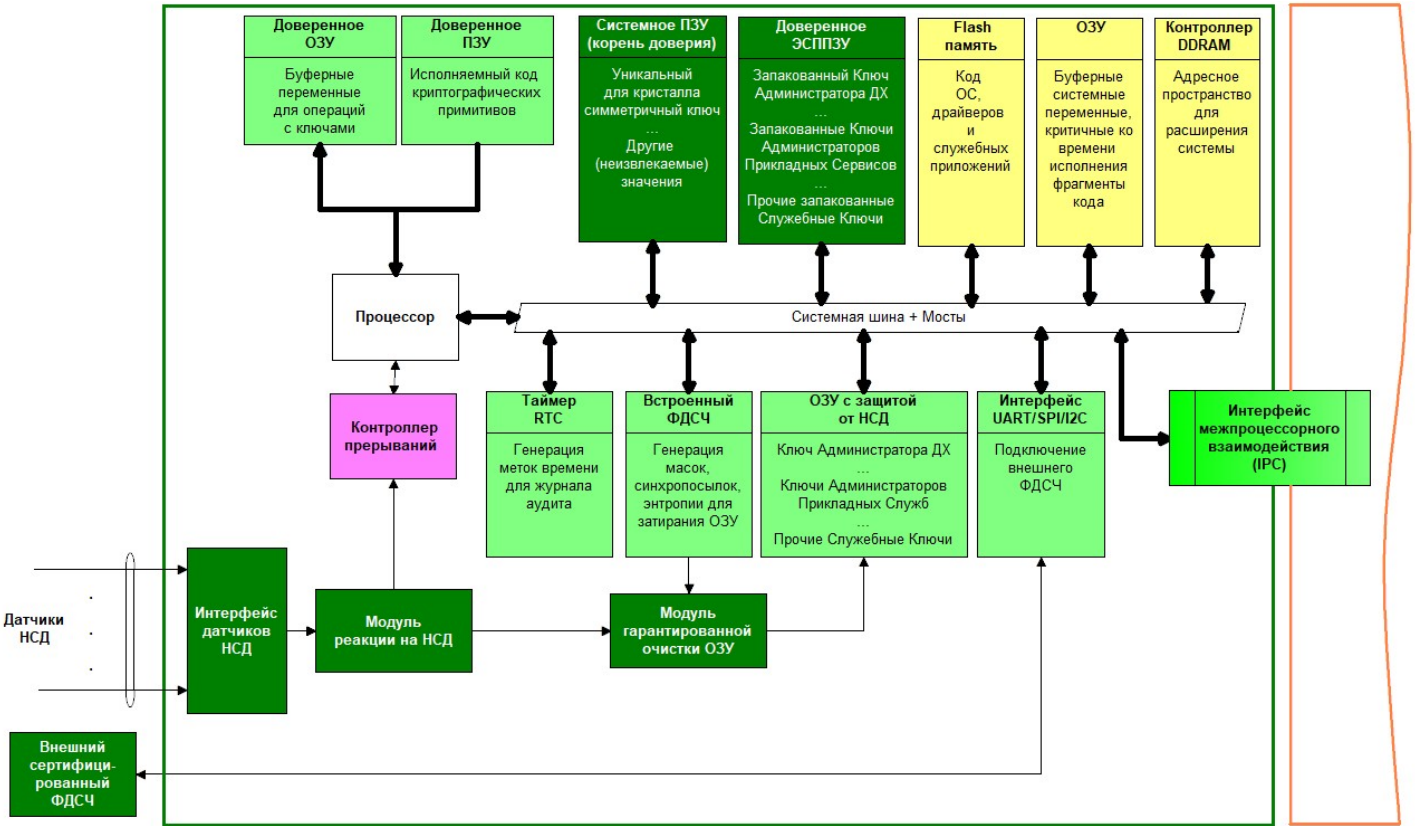
Процессор состоит из Контура Общего Назначения (КОН), выполненного на базе процессорного кластера с архитектурой ARM Cortex-A v8 и Изолированного Контура (ИК) который может быть выполнен на произвольном ядре, в зависимости от требований к производительности и энергопотреблению. Кластер ARM Cortex-A никаких особенностей не имеет.

В состав ИК входят:

- системное ПЗУ для хранения корневых секретов (мастер-ключ, КШК);
- доверенное ЭСППЗУ для хранения ключей первого уровня (ключей администраторов);
- flash-память, разделенная на доверенную область (для хранения кода крипто-примитивов) и область общего назначения (для хранения остального кода);
- ОЗУ, разделенное на доверенную область (для манипуляций с ключами) и область общего назначения (для выполнения остальных операций);
- контроллер DDRAM для расширения системы (опционально);
- ОЗУ с защитой от НСД для хранения теневых копий системных ключей с целью повышения производительности криптографических операций;
- встроенный ФДСЧ для генерации синхропосылок, масок, УИД и меток времени;
- интерфейс к внешнему сертифицированному ФДСЧ для генерации ключей;
- интерфейс к внешнему носителю (QSPIFlash) для хранения контейнеров с системными ключами;
- почтовый ящик для обмена данными с ARM-кластером.

Программно-аппаратная архитектура Изолированного Контура

Блок-схема Изолированного Контура



kaspersky

Функции Изолированного Контура

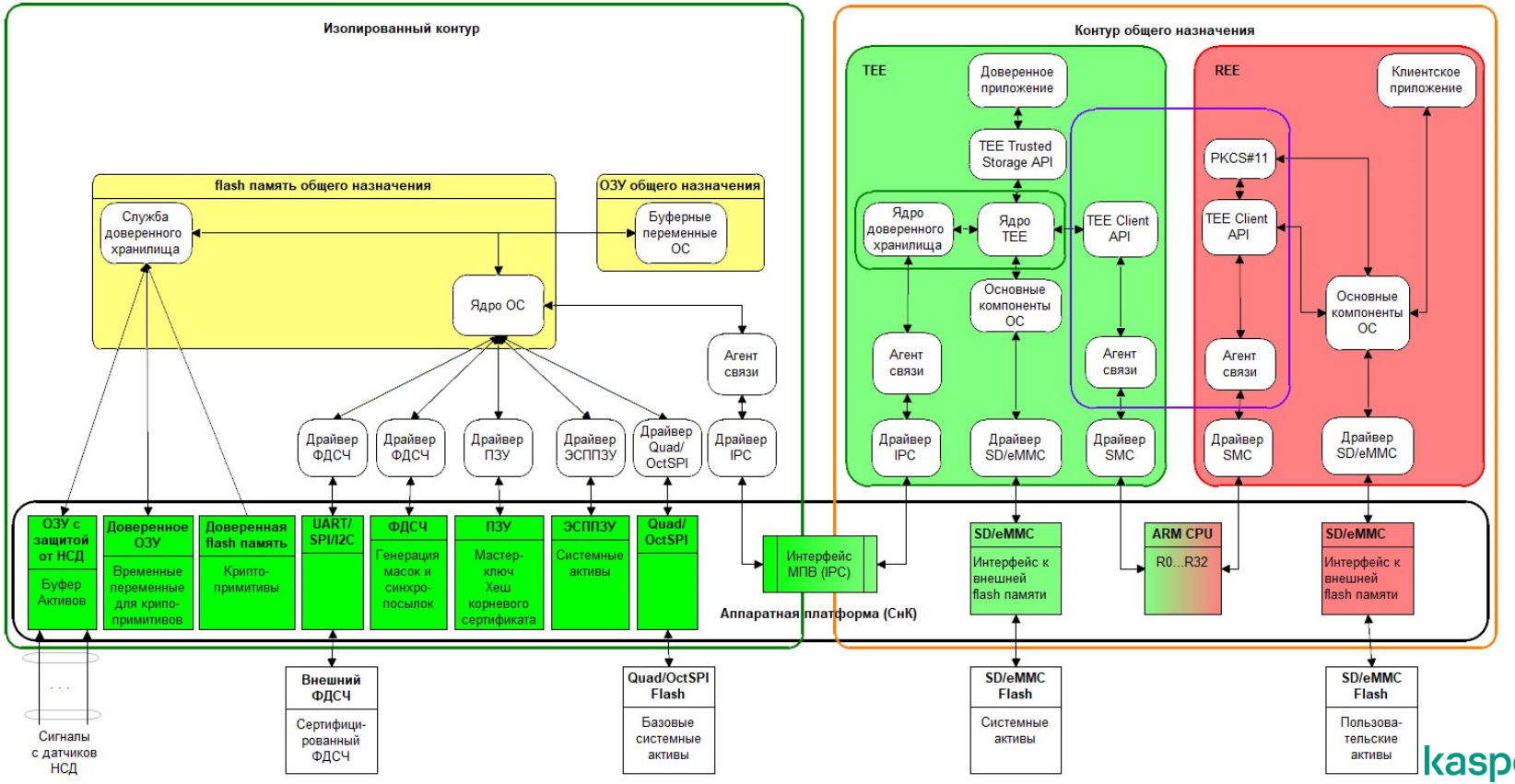
Изолированный Контур предназначен для реализации функционала Корня Доверия (Root-of-Trust, RoT) и выполняет следующие типы операций:

- генерация масок и синхропосылок (векторов инициализации, IV);
- генерация Уникальных Идентификаторов (УИД);
- генерация ключей шифрования/ключевых пар Администраторов (КШАxx/КПАxx);
- генерация Пользовательских Ключей Шифрования (ПКШ) и Ключевых Пар (ПКП);
- запаковка и распаковка ключей/ключевых пар (например, по алгоритму Magma_MGM);
- распаковка и размещение Ключей Администраторов в ОЗУ с защитой от НСД;
- гарантированное удаление Ключей Администраторов из ОЗУ с защитой от НСД при наступлении события НСД;
- управление (создание, чтение, модификация, удаление) системным разделом Доверенного Хранилища, размещенным в ЭСППЗУ и/или на микросхеме Quad/OctSPI flash, памяти, подключенной к Изолированному Контуру;
- ведение защищенного журнала критичных операций и событий на внешнем носителе.

Поскольку архитектура ИК не содержит компонент (например, криптосопроцессоров), подлежащих обязательной сертификации, то для ее реализации возможно использование зарубежных фабрик по производству кристаллов. Кроме того, это снижает риски, связанные с экспортно-импортными ограничениями.

Программно-аппаратная архитектура Доверенного Хранилища

Полная программно-аппаратная блок-схема Доверенного Хранилища с повышенной степенью защищенности



kaspersky

Программная архитектура решения

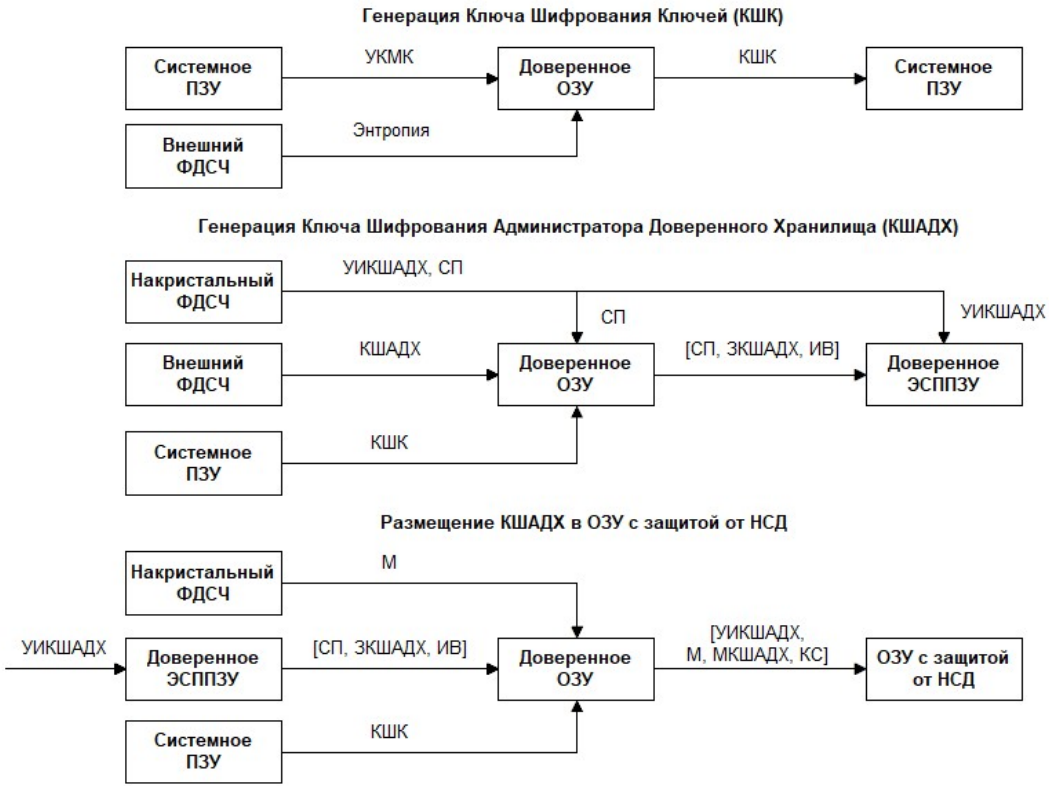
С точки зрения программной архитектуры решение состоит из трех операционных окружений:

- среды исполнения общего назначения (REE), исполняющейся на ARM-кластере в режиме Non-Secure World, в которой функционирует универсальная ОС, коммуникационные приложения, а также (пользовательские) приложения, не связанные с обработкой критичных данных;
- доверенной среды исполнения (TEE, ARM TZ), исполняющейся на ARM-кластере в режиме Secure World, в которой функционирует защищенная ОС с надстройкой GP Trusted Execution Environment и использующими ее API доверенными приложениями, и предназначенной для выполнения основных операций над пользовательскими данными/с использованием пользовательских ключей;
- изолированной среды исполнения, исполняющейся в Изолированном Контуре и предназначенной для реализации полнофункциональной системы управления ключами.

Обмен данными между REE и ARM TZ (TEE) происходит с помощью вызова инструкции SMC и формирования необходимых блоков данных в разделяемых областях памяти.
Обмен данными между ARM TZ (TEE) и ИК с целью повышения защищенности происходит через буферное (двухпортовое) ОЗУ (почтовый ящик), адресное пространство которого находится за пределами адресного остального пространства. Доступ к почтовому ящику происходит через наборы регистров, отдельные для ИК и ARM TZ.

Примеры сценариев

Инициализация Доверенного Хранилища



Обозначения:

УКМК – Уникальный для Кристалла Мастер-Ключ

КШК – Ключ Шифрования Ключей

КШАДХ – Ключ Шифрования Администратора Доверенного Хранилища

УИКШАДХ – Уникальный идентификатор КШАДХ

ЗКШАДХ – Зашифрованный КШАДХ

МКШАДХ – Маскированный КШАДХ

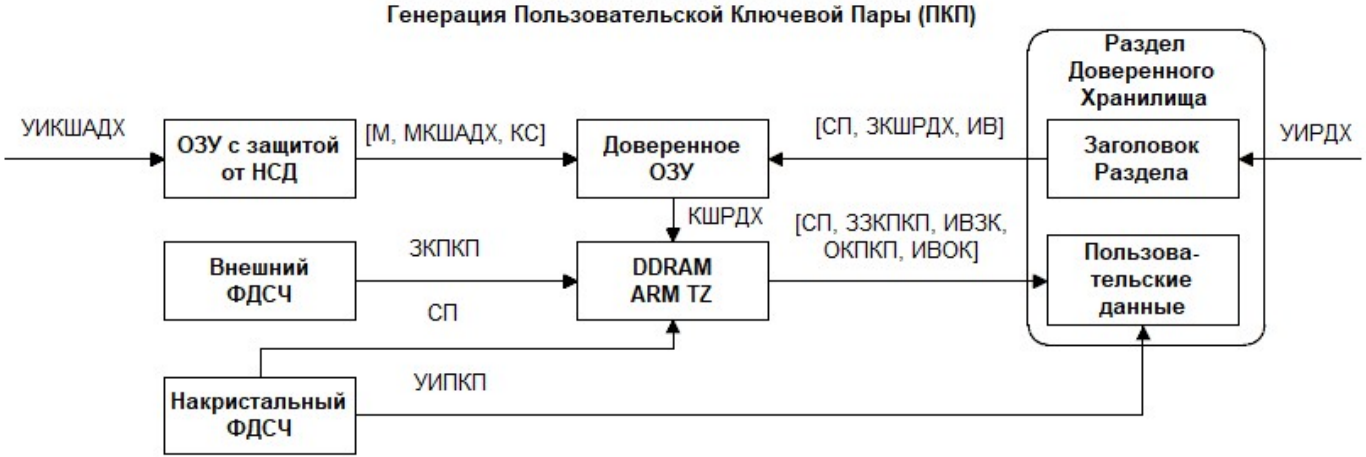
СП – Синхропосылка (вектор инициализации, IV)

ИВ – Имитовставка (код аутентификации, CMAC)

КС – Контрольная сумма (CRC16/CRC32)

kaspersky

Генерация пользовательской ключевой пары



Обозначения:

(М)КШАДХ – (Маскированный) Ключ Шифрования Администратора Доверенного Хранилища

УИКШАДХ – Уникальный идентификатор КШАДХ

(З)КШРДХ – (Зашифрованный) Ключ Шифрования Раздела Доверенного Хранилища

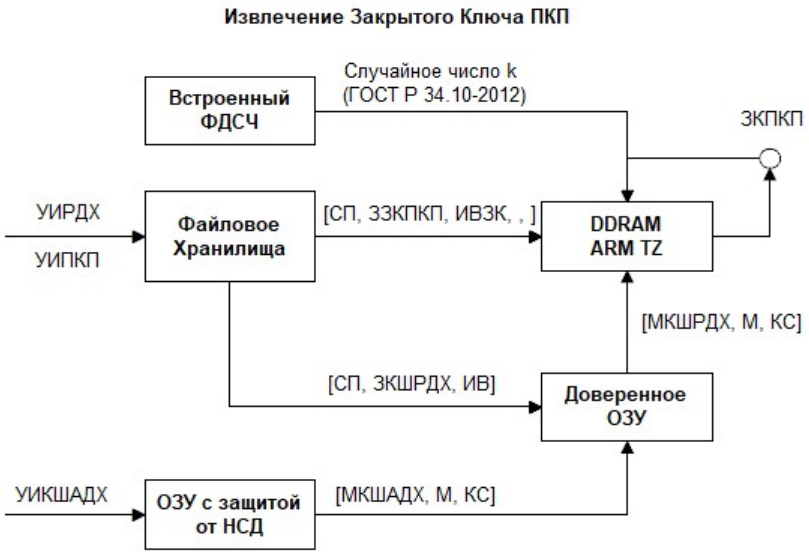
(З)З(/О)КПКП – (Зашифрованный) Закрытый (/Открытый) Ключ Пользовательской Ключевой Пары

СП – Синхропосылка (вектор инициализации)

ИВ(ЗК/ОК) – Имитовставка (для Закрытого/Открытого Ключа)

КС – Контрольная сумма (CRC16/CRC32)

Формирование электронной подписи



Обозначения:

УИПКП – Универсальный идентификатор пользовательской ключевой пары

УИРДХ – Универсальный идентификатор раздела доверенного хранилища (идентификатор пользователя)

УИКШАДХ – Универсальный идентификатор ключа шифрования администратора доверенного хранилища

З(М)КША(/Р)ДХ – Зашифрованный (маскированный) ключ шифрования администратора (/раздела) доверенного хранилища

(З)ЗКПКП – (Зашифрованный) закрытый ключ пользовательской ключевой пары

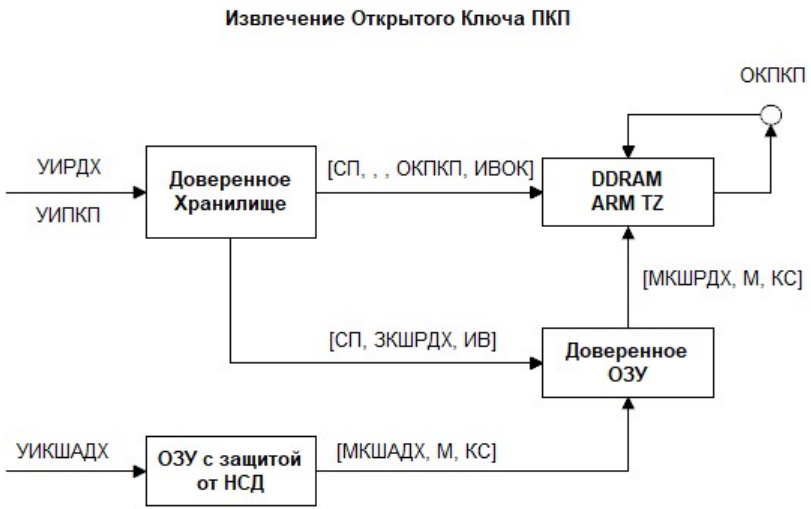
СП – Синхропосылка

ИВ(ЗК) – Имитовставка (закрытого ключа)

М – Маска

КС – Контрольная сумма (CRC16/CRC32)

Экспорт сертификата открытого ключа



Обозначения:

УИПКП – Универсальный идентификатор пользовательской ключевой пары

УИРДХ – Универсальный идентификатор раздела доверенного хранилища (идентификатор пользователя)

УИКШАДХ – Универсальный идентификатор ключа шифрования администратора доверенного хранилища

З(М)КША(/Р)ДХ – Зашифрованный (маскированный) ключ шифрования администратора (/раздела) доверенного хранилища

ОКПКП – Открытый ключ пользовательской ключевой пары

СП – Синхропосылка

ИВ(ОК) – Имитовставка (открытого ключа)

М – Маска

КС – Контрольная сумма (CRC16/CRC32)

kaspersky

Открытые вопросы

- Востребованность архитектуры на рынке СЗИ.
- Регламент инициализации кристалла: где, кем, в каких условиях будет формироваться корень доверия[1] (т.е. будут записываться начальные неизвлекаемые секреты)?
- Возможность реализации внутреннего сертифицированного ФДСЧ (с учетом производства кристаллов за пределами РФ).

[1] Один из вариантов первичной инициализации СнК (SoC) с использованием аппаратных модулей защиты (HSM) в условиях контрактного производства рассмотрен в документе MicroSemi (MicroChip) «Secure Production Programming Solution (SPPS) User Guide» (spps.pdf)

kaspersky

Спасибо!

Андрей Самоделов
Системный аналитик

Andrey.Samodelov@kaspersky.com