Корни доверия

Требования
Архитектура
Реализация

Андрей Самоделов
Независимый эксперт
assamodelov@yandex.ru

Содержание

Общее описание корня доверия.

Определение корня доверия

Корень доверия – это максимально компактный привязанный к аппаратной платформе (вычислительному ядру) якорь цепочки доверия, представляющий собой программный, программно-аппаратный или аппаратный комплекс, который:

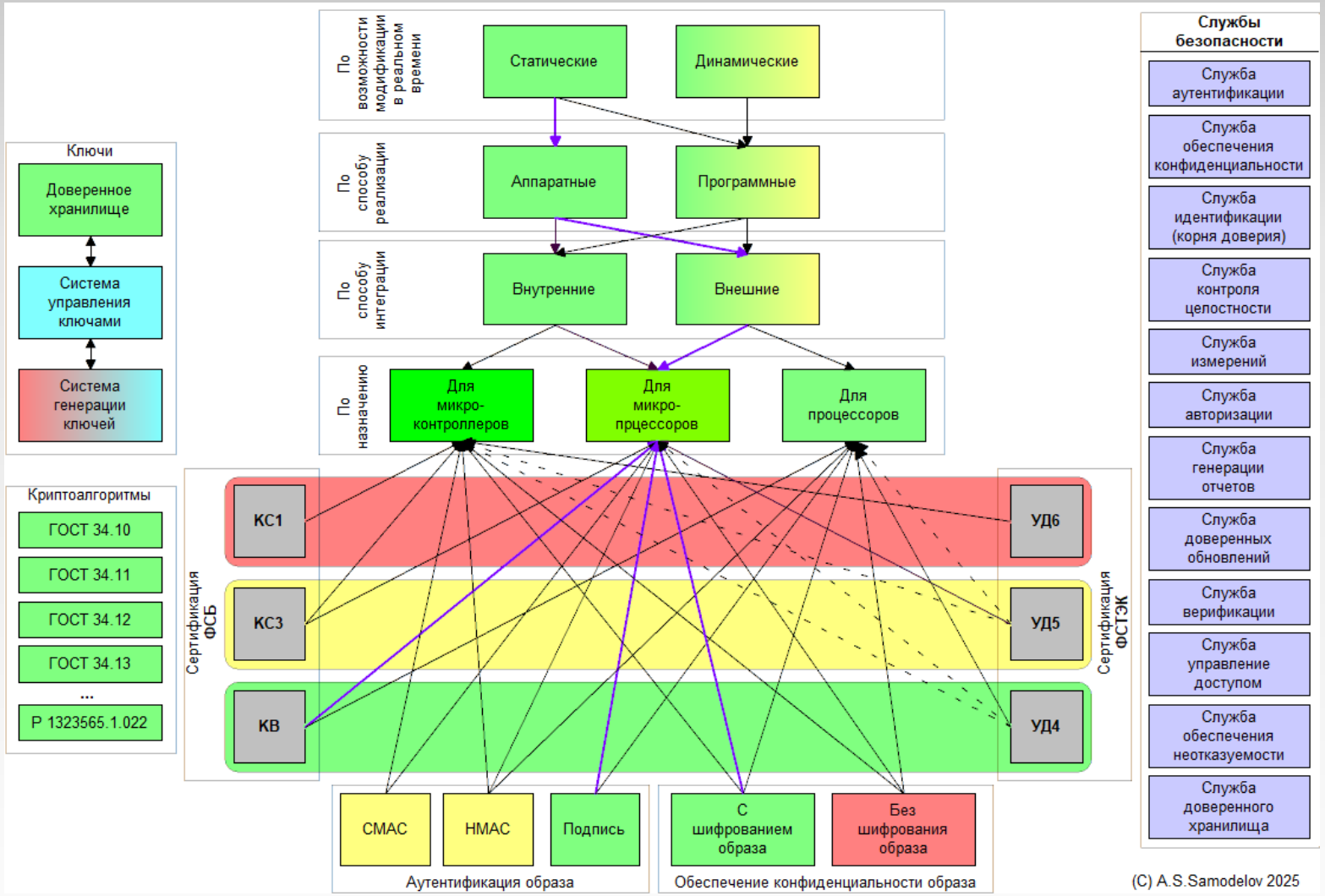
- *Работает предсказуемым образом (поскольку его неправильное поведение невозможно обнаружить) независимо от того, какое программное обеспечение выполняется на платформе, чтобы быть защищенным от программных атак,*
- *Защищен от физических атак во избежание необходимости доверять владельцу или пользователю платформы (которые в противном случае могли бы физически вмешаться в ее работу).*
- *Содержит, по крайней мере, минимальный набор функций, позволяющий описать характеристики платформы, которые влияют на ее надежность и безопасность (служба измерений),*
- *Инициализируется первым при холодной загрузке системы до начала выполнения какого-либо другого кода,*
- Обеспечивает загрузку и выполнение только доверенного кода (служба верификации),
- Обеспечивает доверенное хранение конфиденциальных (служба обеспечения конфиденциальности) и критичных (служба контроля целостности) данных,
- *Выполняет жестко определенную последовательность действий, приводящих к появлению в системе специфических служб безопасности и возникновению якоря цепочки доверия,*
- *Делает запись в системный журнал о завершении собственной инициализации, верифицирует следующий функциональный блок в цепочке доверия и, в случае успешной верификации, передает ему управление,*
- *Предоставляет одну или несколько служб безопасности.*

В случае, если верификация следующего блока кода прошла неуспешно, корень доверия делает соответствующую запись в системный журнал и дает команду на холодную перезагрузку системы.

Корень доверия может иметь счетчик инициализаций, в котором записывается номер инициализации и ее результат. При необходимости может быть введено пороговое значение последовательных неуспешных инициализаций, при достижении которого система блокируется и может быть выведена из состояния блокировки только производителем оборудования в специальных условиях.

В системе может быть несколько независимых корней доверия, привязанных к различным аппаратным платформа (вычислительным ядрам) и выполняющим специфические функции (предоставляющим специфические службы безопасности).

Классификация корней доверия



Корень доверия является сложным высоко интегрированным продуктом.
На рисунке показана многоуровневая диаграмма классификации корней доверия, отвечающая его функциональному назначению.
Основной задачей проектировщика корня доверия является выбор архитектуры, обеспечивающей выполнение функциональных и нефункциональных требований и минимально возможный размер, обеспечивающий простоту формальной верификации и последующей сертификации.

Общие требования GP к корню доверия

Общие требования к корню доверия

Требование 1. Вычислительное ядро, код и данные
Корень доверия **ДОЛЖЕН** состоять из вычислительного ядра и исполняемого кода (реализующего функции безопасности корня доверия), расположенных на единой платформе. Для доступа к корню доверия **МОГУТ** потребоваться дополнительные данные и/или ключ(и); в этом случае данные и/или ключ(и) **ДОЛЖНЫ** быть размещены на той же платформе, что и вычислительное ядро и исполняемый код.

Требование 2. Службы безопасности
Корень доверия **ДОЛЖЕН** предоставлять одну или несколько служб безопасности.

Требование 3. Необходимость сертификации
Поставщик/производитель **ДОЛЖЕН** разрабатывать корень доверия с учетом его последующего участия в сертификации платформы или устройства.

Требование 4. Уникальный идентифицируемый владелец
У корня доверия **ДОЛЖЕН** быть единственный идентифицируемый владелец.

Требование 5. Изменяемость
Код и/или данные корня доверия **ДОЛЖНЫ** быть неизменными, или их изменяемость **ДОЛЖНА** контролироваться только единственным идентифицируемым владельцем.

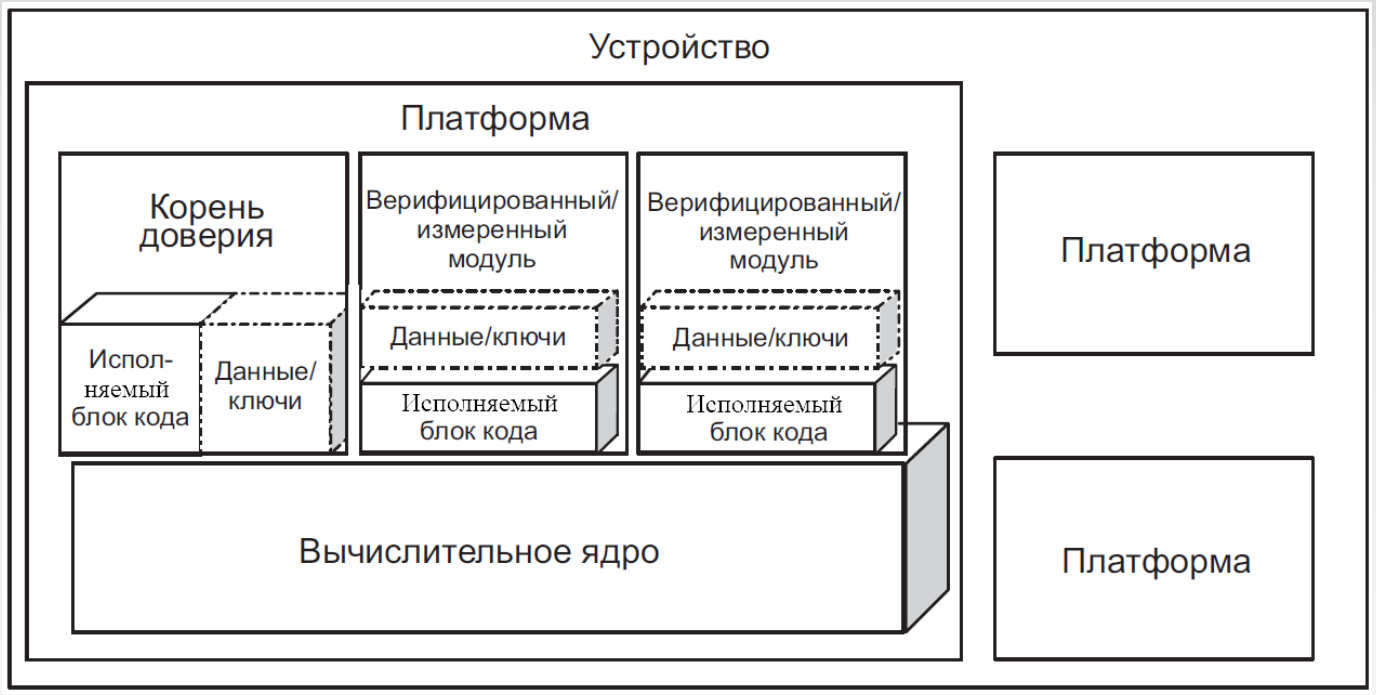
Требование 6. Передача права владения
Если корень доверия реализует механизм передачи права владения, разработанный первоначальным владельцем/поставщиком корня доверия, то текущий владелец корня доверия **ДОЛЖЕН** предоставить механизм для авторизации передачи прав владения новому владельцу.

Требование 7. Единственность корня доверия для платформы
Платформа **ДОЛЖНА** содержать один и только один корень доверия, возможно составной.

Требование 8. Последовательность загрузки
Корень доверия **ДОЛЖЕН** содержать код, который выполняется первым при инициализации вычислительного ядра во время холодной загрузки платформы.

Требование 9. Идентифицируемость производителя
Корень доверия **ДОЛЖЕН** иметь идентифицируемого производителя.

Незагружаемый корень доверия

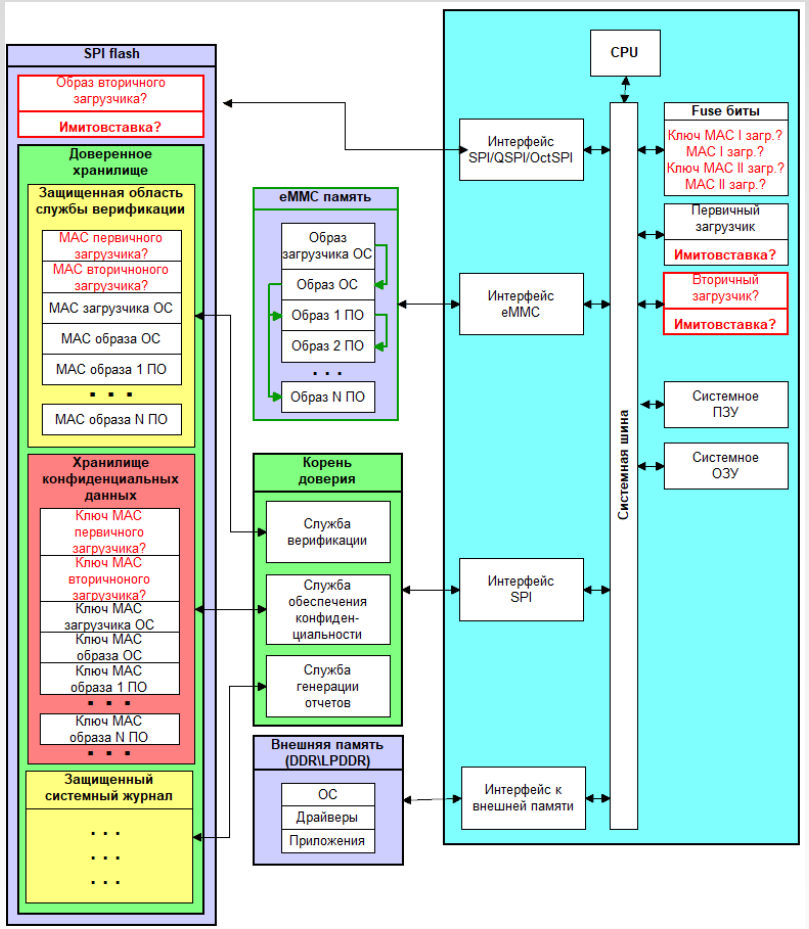


Незагружаемый корень доверия представляет собой монолитный блок кода и данных расположенный в загрузочном ПЗУ.

В состав кода незагружаемого корня доверия входит служба верификации, использующая жестко прошитый в устройство ключ проверки подписи, который используется для верификации как кода самого КД, так и кода последующего загружаемого образа.

Требования к незагружаемому корню доверия

Система с незагружаемым корнем доверия



Незагружаемый (необновляемый) корень доверия выполняется в виде изолированной подсистемы внутри СнК, состоящей из аппаратных модулей и встроенного ПО, или отдельного кристалла, снабженного собственным процессорным ядром и подключенного к центральной системе.

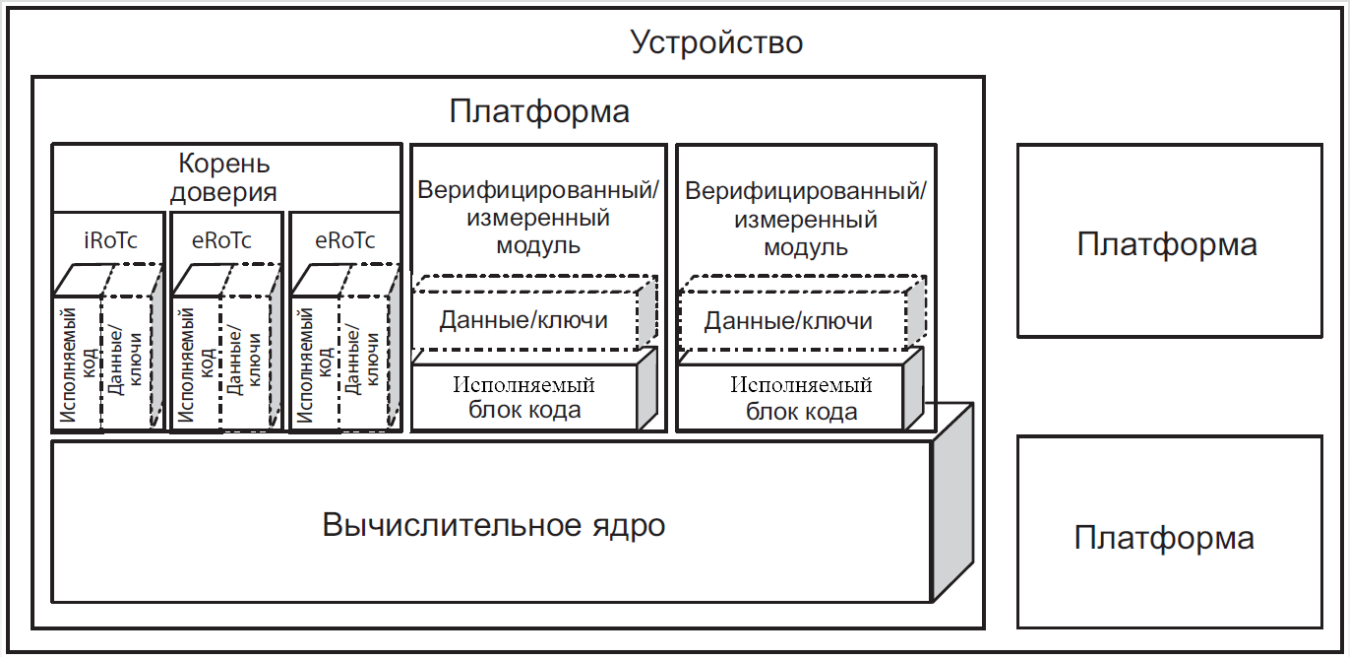
При реализации корня доверия в виде внешнего кристалла он должен обладать минимальным набором функций, необходимых для инициализации цепочки доверия

Активы незагружаемого корня доверия, как правило, хранятся в защищенной области внутри корня доверия.

Требование 10. Происхождение

Производитель платформы **ДОЛЖЕН** создавать и предоставлять корень доверия в собственном процессе производства.

Загружаемый корень доверия



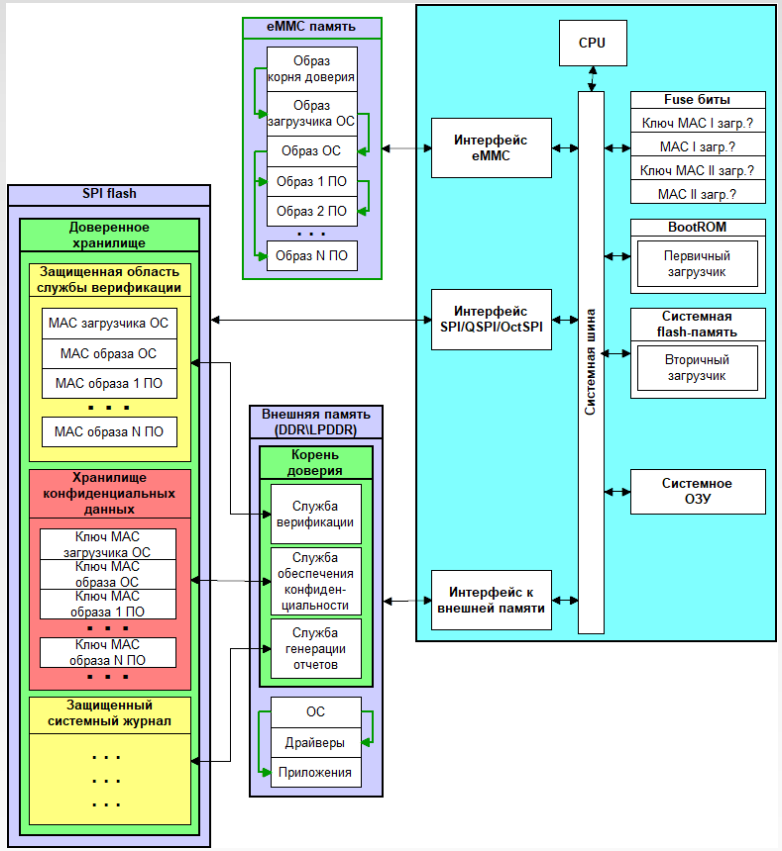
Загружаемый корень доверия представляет собой комплекс из нескольких блок кода и данных. Компоненты начального корня доверия iRoTc, как правило располагаются в загрузочном ПЗУ.

В состав кода iRoTc входит служба верификации, использующая жестко прошитый в устройство ключ проверки подписи, который используется для верификации кода iRoTc, кода расширенных компонентов eRoTc.

При использовании загружаемого КД верификация кода последующих загружаемых образов может производится на прикрепленных к образам сертификатах.

Требования к загружаемому корню доверия

Система с загружаемым корнем доверия



Загружаемый корень доверия состоит из начального компонента (iRoTc), расположенного в загрузочном ПЗУ (bootrom) и расширенных компонентов (eRoTc), загружаемых в процессе доверенной загрузки. iRoTc, по сути, является незагружаемым корнем доверия.

Расширенные компоненты корня доверия могут быть реализованы как службы доверенной ОС.

Требование 11. Происхождение (iRoTc)

Производитель платформы **ДОЛЖЕН** создавать и поставлять компонент начального корня доверия в процессе собственного производства.

Требование 12. Последовательность загрузки (iRoTc)

Начальный компонент корня доверия **ДОЛЖЕН** содержать код, который выполняется первым при инициализации вычислительного ядра во время холодной загрузки платформы.

Требование 13. Верификация (eRoTc)

Родительский компонент корня доверия (то есть либо начальный компонент корня доверия, либо другой eRoTc) перед первым выполнением eRoTc **ДОЛЖЕН** проверить целостность кода и данных расширенного компонента корня доверия. Компонент родительского корня доверия не сохраняет отчет о верификации кода и данных eRoTc.

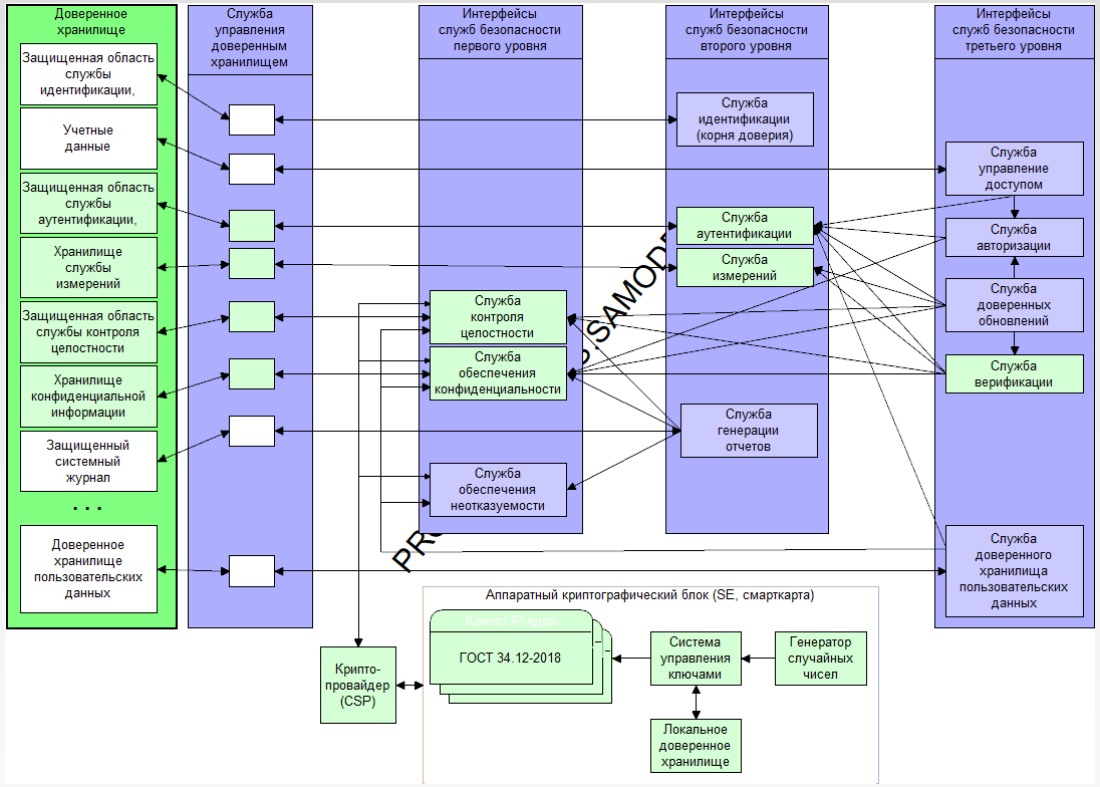
Требование 14. Расположение

iRoTc и все eRoTc, из которых состоит загружаемый корень доверия, **ДОЛЖНЫ** быть расположены на одной и той же платформе.

Службы безопасности корня доверия Global Platform

Архитектура служб безопасности корня доверия

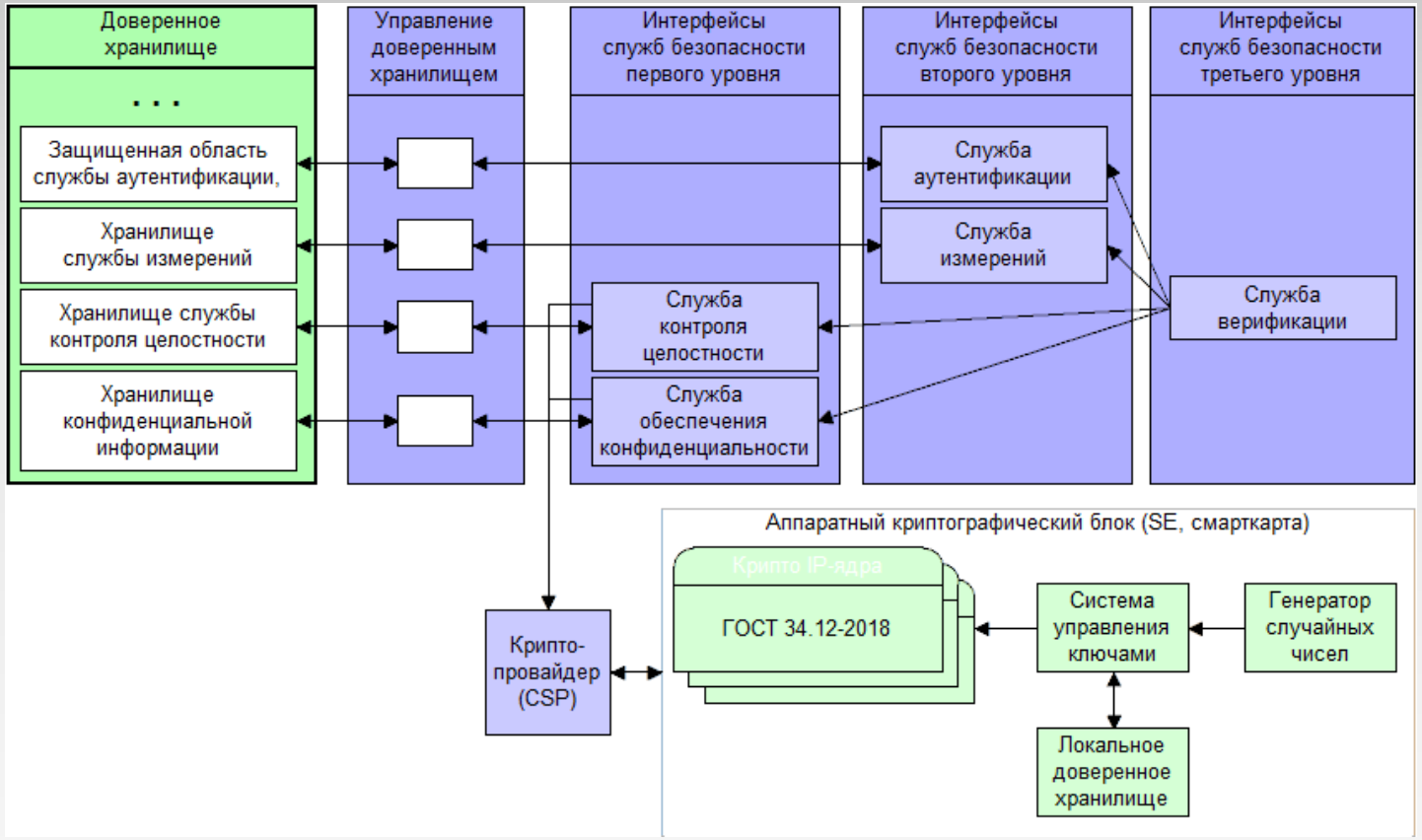
Диаграмма взаимосвязи служб безопасности корня доверия



Корень доверия **ДОЛЖЕН** предоставлять внешнему окружению одну, несколько или все службы безопасности:

- Служба идентификации корня доверия (RoT Identification Service);
- Служба аутентификации (Authentication Service);
- Служба авторизации (Authorization Service);
- Служба управления доступом (Access Control Service);
- Служба обеспечения конфиденциальности (Confidentiality Service);
- Служба контроля целостности (Integrity Service);
- Служба обеспечения неотказуемости (Non-repudiation Service);
- Служба измерений (Measurement Service);
- Служба генерация отчетов (Reporting Service);
- Служба доверенного хранилища (Trusted Storage Service);
- Служба доверенного обновления (Update Service);
- Служба верификации (Verification Service);
- Служба доверенного хранилища пользовательских данных

Минимальный корень доверия - корень доверия для верификации



В состав корня доверия для верификации будут входить следующие службы безопасности:

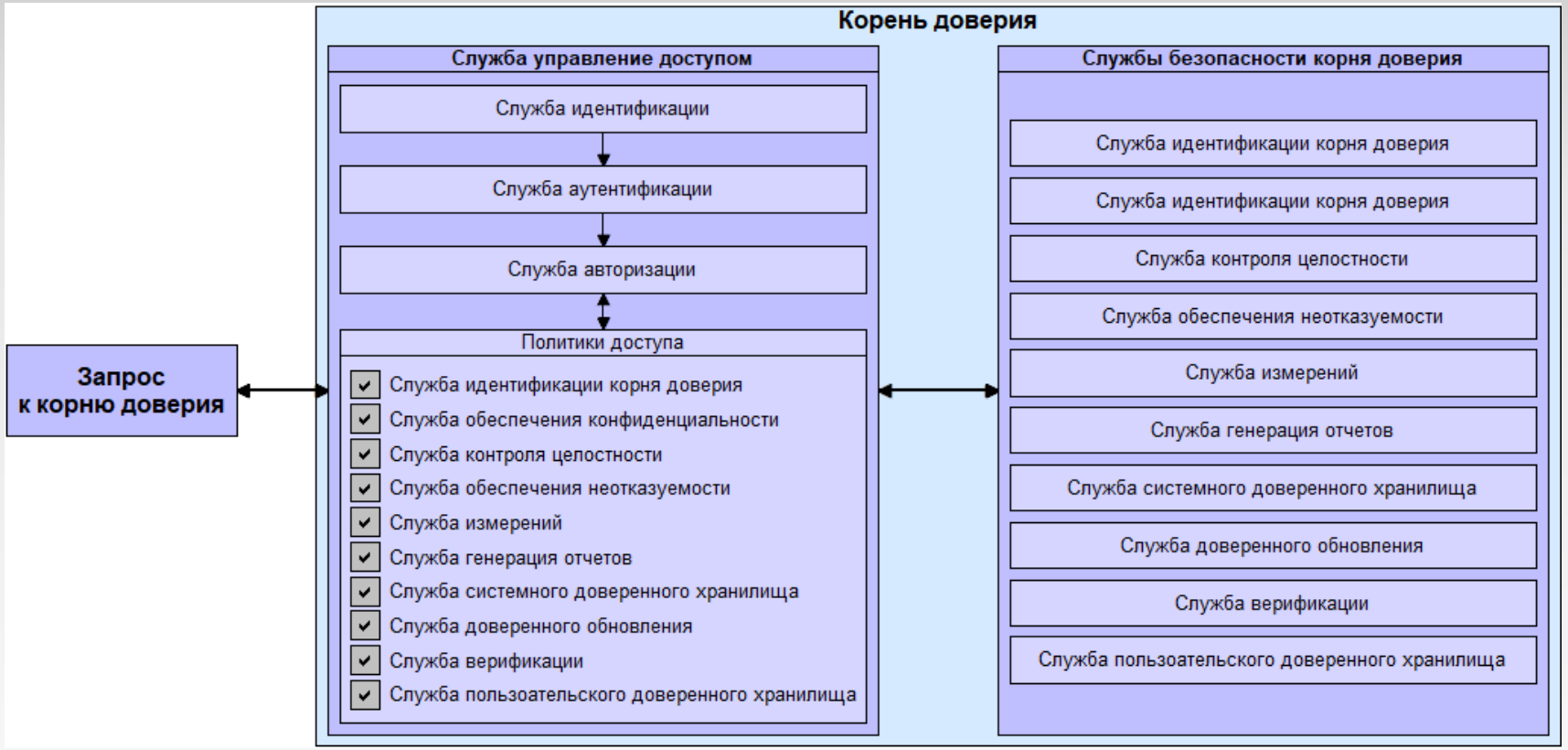
- **Служба аутентификации;**
- **Служба измерений;**
- **Служба контроля целостности;**
- **Служба обеспечения конфиденциальности;**

Эти службы могут быть реализованы либо как функции в коде службы верификации, либо как полноценные службы с соответствующими интерфейсами. Эти интерфейсы могут предоставляться внешнему окружению, наряду с интерфейсом службы верификации.

Прочие службы безопасности корня доверия могут быть, например, частью ОС и загружаться в процессе доверенной загрузки с использованием корня доверия для верификации.

Минимальный корень доверия должен предоставлять внешнему окружению всего одну службу безопасности – службу верификации. Именно с ее помощью осуществляется валидация загружаемого кода при построении цепочки доверия.
Такой корень доверия будет называться корнем доверия для верификации.

Контроль доступа к корню доверия с помощью политик



При необходимости, для доступа к корню доверия **МОЖЕТ** быть установлен набор пользователей с закрепленной за каждым из них политикой доступа к корню доверия.

Такой способ оказывается более экономным, чем реализация отдельного контроля доступа для каждой из служб безопасности

Требования Global Platform к службам безопасности корня доверия

Общие требования к службам безопасности

Требование 1. Интерфейс (ы) службы безопасности

Интерфейс (также называемый точкой входа) **ДОЛЖЕН** обеспечивать доступ для использования возможностей или функций службы безопасности корня доверия.

Требование 2. Сохранение целостности защищенных областей

Интерфейс службы безопасности должен обеспечивать надлежащий уровень защиты областей для сохранения целостности их содержимого.

Требование 3. Обеспечение конфиденциальности защищенных областей

Интерфейс службы безопасности может обеспечивать соответствующий уровень защиты областей для обеспечения конфиденциальности их содержимого.

Требование 4. Доступ к защищенным областям

Интерфейс службы безопасности должен обеспечивать соблюдение внутренней политики в отношении доступа к защищенным областям и их использования.

Требования к простым службам безопасности

Служба аутентификации

Требование 5. Хранилище службы аутентификации

Служба аутентификации **МОЖЕТ** поддерживать одну или несколько защищенных областей для хранения учетных данных, которые будут использоваться в протоколах аутентификации.

Требование 6. Контроль доступа к службе аутентификации

Служба аутентификации **ДОЛЖНА** поддерживать интерфейс для управления доступом и использованием содержимого защищенных областей.

Служба обеспечения конфиденциальности

Требование 7. Хранилище конфиденциальной информации

Служба обеспечения конфиденциальности **ДОЛЖНА** иметь одну или несколько защищенных областей для хранения секретных значений.

Требование 8. Контроль доступа к службе обеспечения конфиденциальности

Поскольку ряд значений являются секретными, служба обеспечения конфиденциальности **ДОЛЖНА** защищать их от несанкционированного раскрытия и использования

Служба идентификации (корня доверия)

Требование 9. Хранение данных службы идентификации

В службе идентификации **ДОЛЖНА** быть защищенная область для хранения секретных значений.

Требование 10. Доступ к службе идентификации

Служба идентификации **ДОЛЖНА** поддерживать интерфейс, позволяющий ей подтверждать подлинность того, что она авторизована для выполнения предоставляемых ею функций.

Требование 11. Протоколы аутентификации

Служба идентификации **ДОЛЖНА** поддерживать стандартные протоколы для аутентификации объекта корня доверия другими объектами.

Требование 12. Аутентификация объекта корня доверия

Владелец корня доверия **ДОЛЖЕН** подтвердить подлинность корня доверия, например, сертификатом публичного ключа, подписанного производителем или продавцом корня доверия.

Требования к простым службам безопасности

Служба контроля целостности

Требование 13. Хранилища службы контроля целостности

Служба контроля целостности **ДОЛЖНА** поддерживать защищенные области с целью хранения и защиты целостности несекретных, но критически важных настроек безопасности и характеристик платформы.

Требование 14. Доступ к службе контроля целостности

Служба контроля целостности **ДОЛЖНА** поддерживать интерфейс для защиты областей от несанкционированных модификаций.

Для подписанных сертификатов **МОЖЕТ** потребоваться дополнительный контроль целостности для защиты от несанкционированной замены в корнях доверия.

Служба измерений

Требование 15. Служба измерений

Служба измерений **ДОЛЖНА** надежно создавать характеристики платформы.

Служба измерений обычно не содержит защищенных областей для измерения.

Требования к составным службам безопасности

Служба авторизации

Требование 16. Служба авторизации

Служба авторизации **ДОЛЖНА** надежно оценивать токены авторизации и определять, соответствуют ли они политикам управления доступом.

Требование 17. Состав службы авторизации

Служба авторизации **МОЖЕТ** предоставлять те же услуги, что и служба аутентификации, служба контроля целостности или и та, и другая. В этом случае она также **ДОЛЖНА** удовлетворять требованиям, предъявляемым к каждой из этих служб.

Служба генерации отчетов

Требование 18. Служба генерации отчетов

Служба генерации отчетов **ДОЛЖНА** иметь возможность достоверно сообщать о характеристиках платформы, аутентифицированных с помощью ее идентификатора платформы, не подлежащим опровержению способом.

Требование 19: Составная служба генерации отчетов

Служба генерации отчетов **МОЖЕТ** предоставлять те же услуги, что и одна или несколько служб аутентификации, обеспечения конфиденциальности, идентификации, контроля целостности и измерений.

В этом случае она также **ДОЛЖНА** удовлетворять требованиям к каждой такой службе безопасности. Она может предоставлять функции этих служб в дополнение к функциям службы генерации отчетов или использовать эти службы из физически независимых фрагментов кода корня доверия.

Требование 20. Содержание отчетов службы

Служба генерации отчетов **ДОЛЖНА** обеспечивать актуальность отчетов о характеристиках платформы.

Требование 21. Свойство неотказуемости для отчетов

Служба генерации отчетов **ДОЛЖНА** поддерживать интерфейс, который ограничивает ее функции предоставлением отчетов, аутентифицированных неоспоримым образом.

Требования к составным службам безопасности

Служба доверенных обновлений

Требование 22. Служба доверенных обновлений

Служба доверенных обновлений **ДОЛЖНА** проверять целостность и подлинность подписанных обновлений и после успешной проверки разрешить запуск процесса обновления.

Требование 23. Составная служба доверенных обновления

Служба доверенных обновлений **МОЖЕТ** содержать службы безопасности корня доверия, к которым относятся служба аутентификация, служба авторизация, служба обеспечения конфиденциальности, служба контроля целостности и служба измерения, необходимые для выполнения обновления. В этом случае служба доверенных обновлений **ДОЛЖНА** удовлетворять требованиям, которые предъявляются к этим службам, даже если она не предоставляет доступ к функциям этих служб через интерфейс.

Служба верификации

Требование 24. Служба верификации

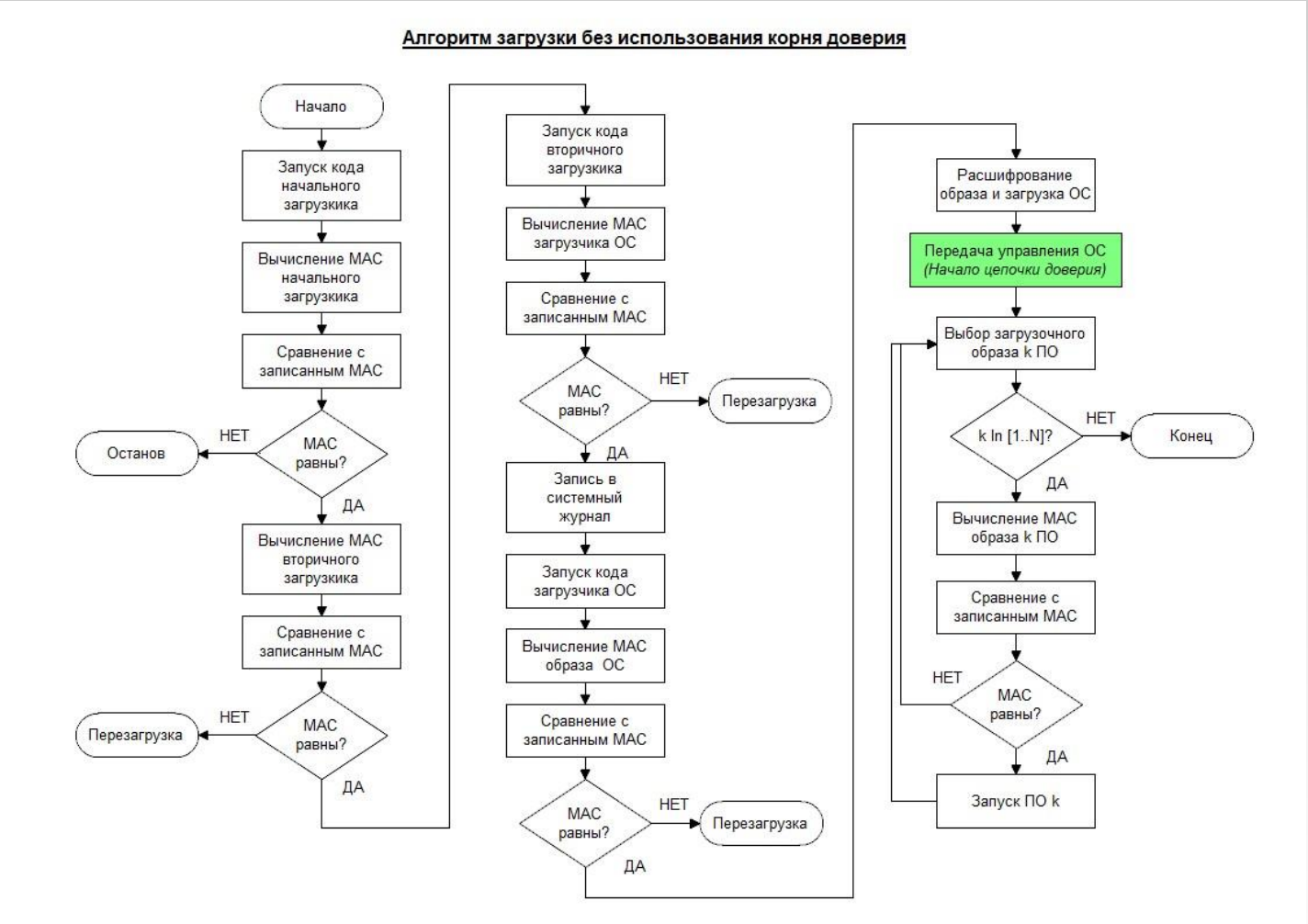
Служба верификации **ДОЛЖНА** проверять подлинность электронных подписей и целостность объектов, защищенных этими подписями.

Требование 25. Составная служба верификации

Служба верификации **МОЖЕТ** содержать любое подмножество служб безопасности корня доверия: аутентификации, обеспечения конфиденциальности, контроля целостности и измерений, необходимых для проверки подписи. В этом случае она **ДОЛЖНА** удовлетворять всем требованиям, которые предъявляются к каждой из этих служб, даже если она не предоставляет доступ к службам через интерфейс. Она **МОЖЕТ** предоставлять все эти функции в дополнение к службе верификации, или она **МОЖЕТ** использовать перечисленные службы.

Доверенная загрузка

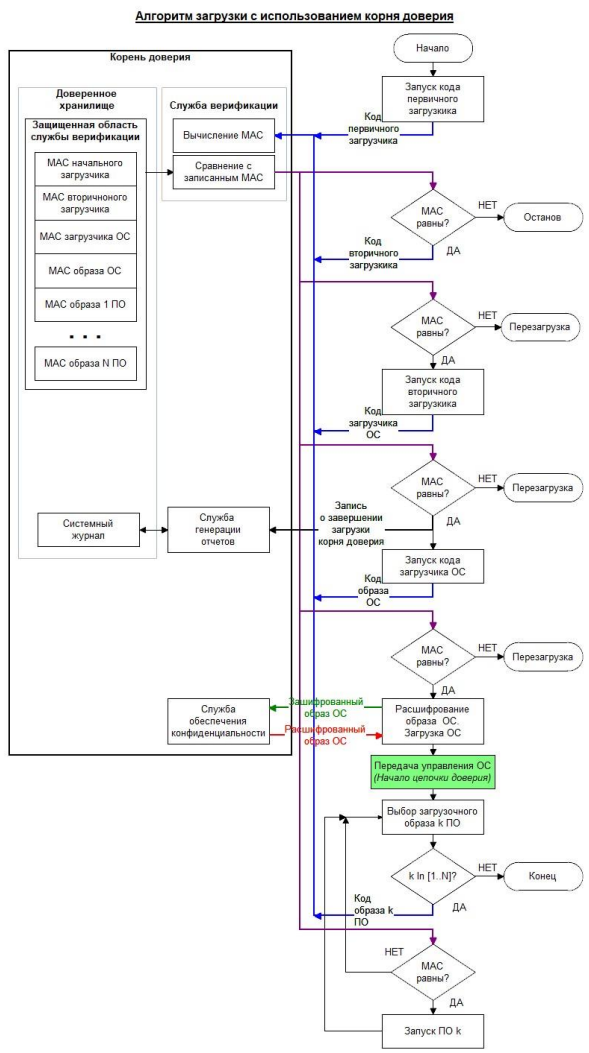
Алгоритм доверенной загрузки без корня доверия



Последовательность загрузки:

1. Верификация и выполнение первичного загрузчика, инициализация системных блоков микропроцессора;
2. Верификация и выполнение вторичного загрузчика, инициализация остальных блоков микропроцессора;
3. Верификация, загрузка и выполнение загрузчика ОС;
4. Верификация, загрузка и выполнение ядра ОС;
5. Верификация и загрузка драйверов;
6. Верификация, загрузка и выполнение прикладного ПО.

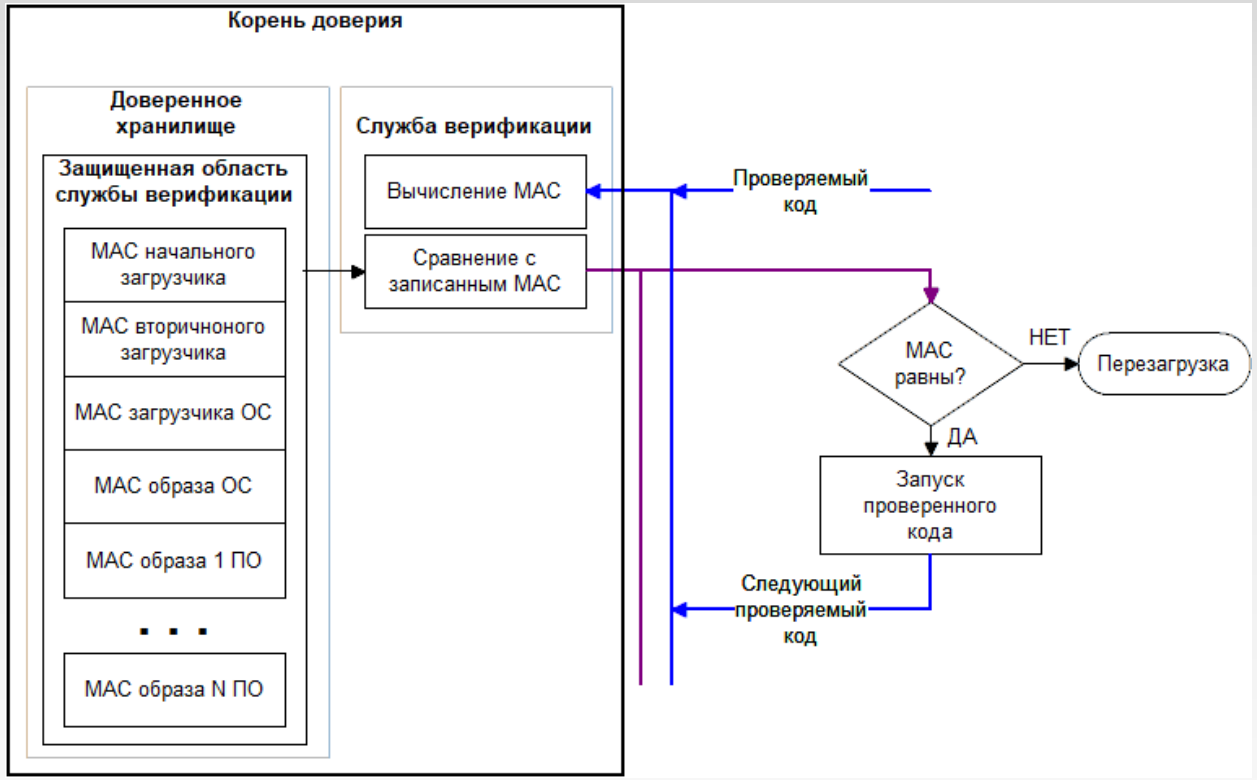
Алгоритм доверенной загрузки с корнем доверия



Алгоритм загрузки аналогичен рассмотренному выше.
Ключевой особенность является выделение наиболее критичного кода в виде отдельного модуля – корня доверия.
Это позволяет :

- Осуществить формальную верификацию кода и сертификацию корня доверия;
- Получить независимость корня доверия от кода ОС и прикладного ПО;
- Уменьшить поверхность атаки, за счет изоляции корня доверия от ОС и прикладного ПО
- Реализовать корень доверия в виде программно-аппаратного комплекса внутри СнК или в виде отдельной микросхемы;
- Повторно использовать сертифицированный корень доверия в последующих разработках без необходимости повторной сертификации.

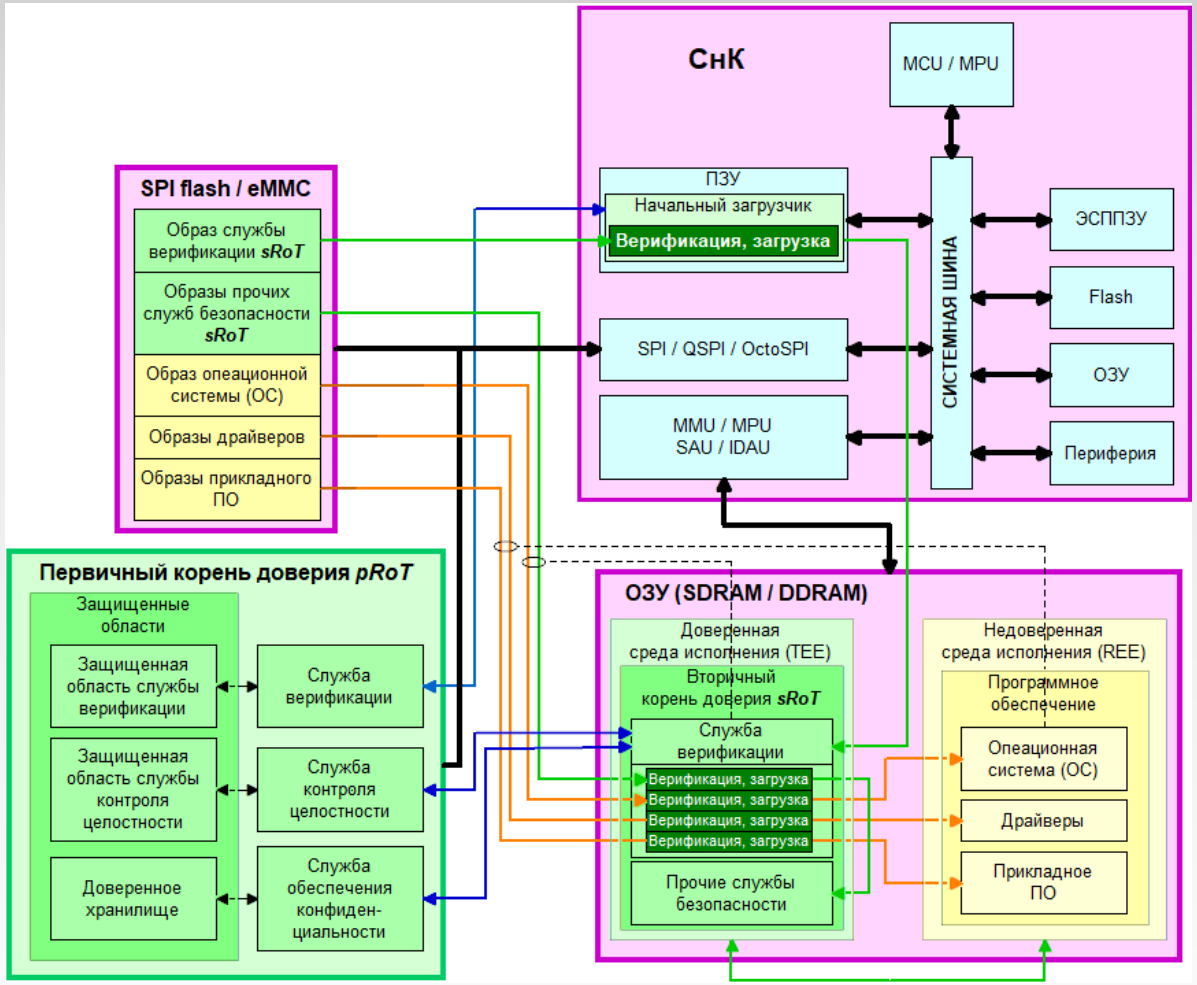
Алгоритм доверенной загрузки с корнем доверия



На диаграмме показана общая часть алгоритма доверенной загрузки с использованием корня доверия:

1. Проверяемый код отправляется службе верификации корня доверия;
2. Подсистемы измерений вычисляет хеш-функцию от принятого кода и имитовставку (MAC);
3. На основе идентификатора, передаваемого совместно с верифицируемым кодом, из доверенного хранилища с помощью подсистем контроля целостности и обеспечения конфиденциальности извлекается эталонное значение имитовставки и сравнивается с вычисленным;
4. Если значения совпадают, то происходит запуск верифицированного кода (в случае необходимости) отправка следующего кода на верификацию;
5. Если коды не совпадают, то происходят действия, определенные общим алгоритмом доверенной загрузки, например, запись результата верификации в системный журнал и перезагрузка системы.

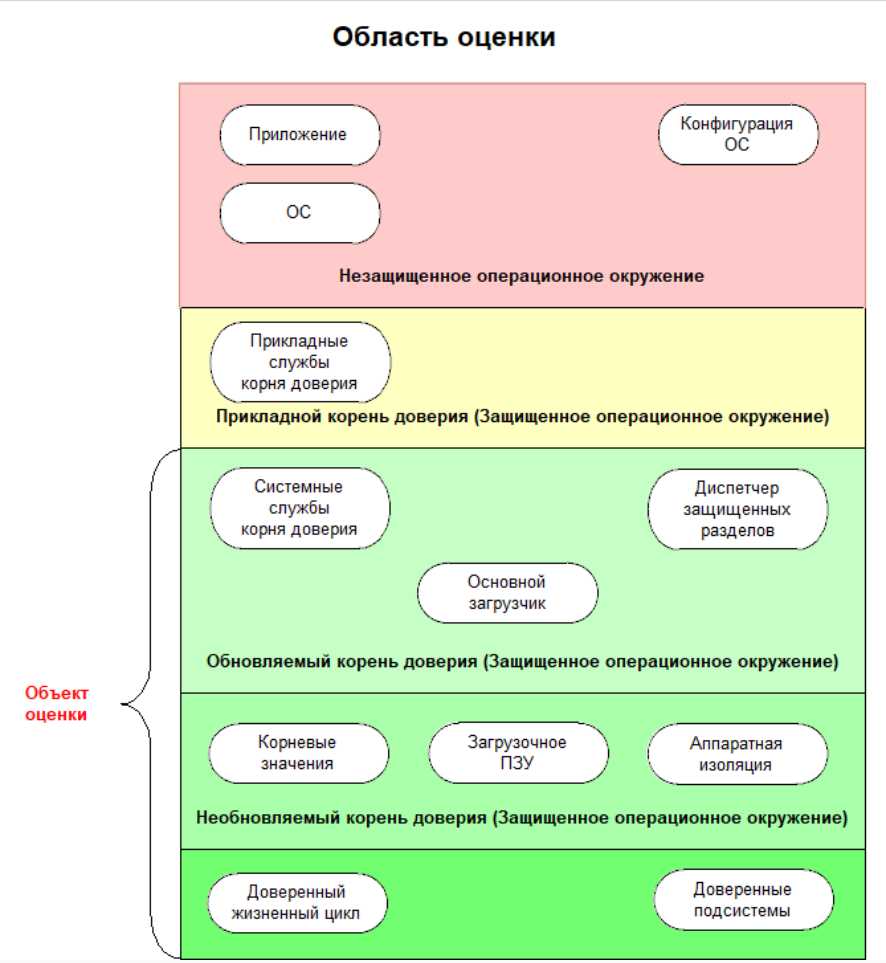
Доверенная загрузка с внешним корнем доверия



Внешний корень доверия выполняется максимально простым и компактным и содержит только базовую службу верификации и минимальное количество ключевой информации.
Поскольку внешний корень доверия не имеет доступа к глобальным коммуникационным интерфейсам (требование безопасности), то в рамках его функционирования не может быть поднят PKI и верификация осуществляется путем вычисления имитовставки на фиксированном ключе (ключах).
Основная задача внешнего корня доверия – верифицировать компоненты вторичного загрузчика (который может инициализировать интерфейсы, необходимые для поднятия PKI) и компоненты загружаемого корня доверия, прежде всего расширенную службу верификации, которая уже может осуществлять проверку аутентичности кода не только с помощью вычисления имитовставки, но и с помощью проверки электронной подписи в рамках стандартной процедуры с использованием сертификатов и удаленного УЦ.

Объект оценки для корня доверия

Общее описание объекта оценки для корня доверия



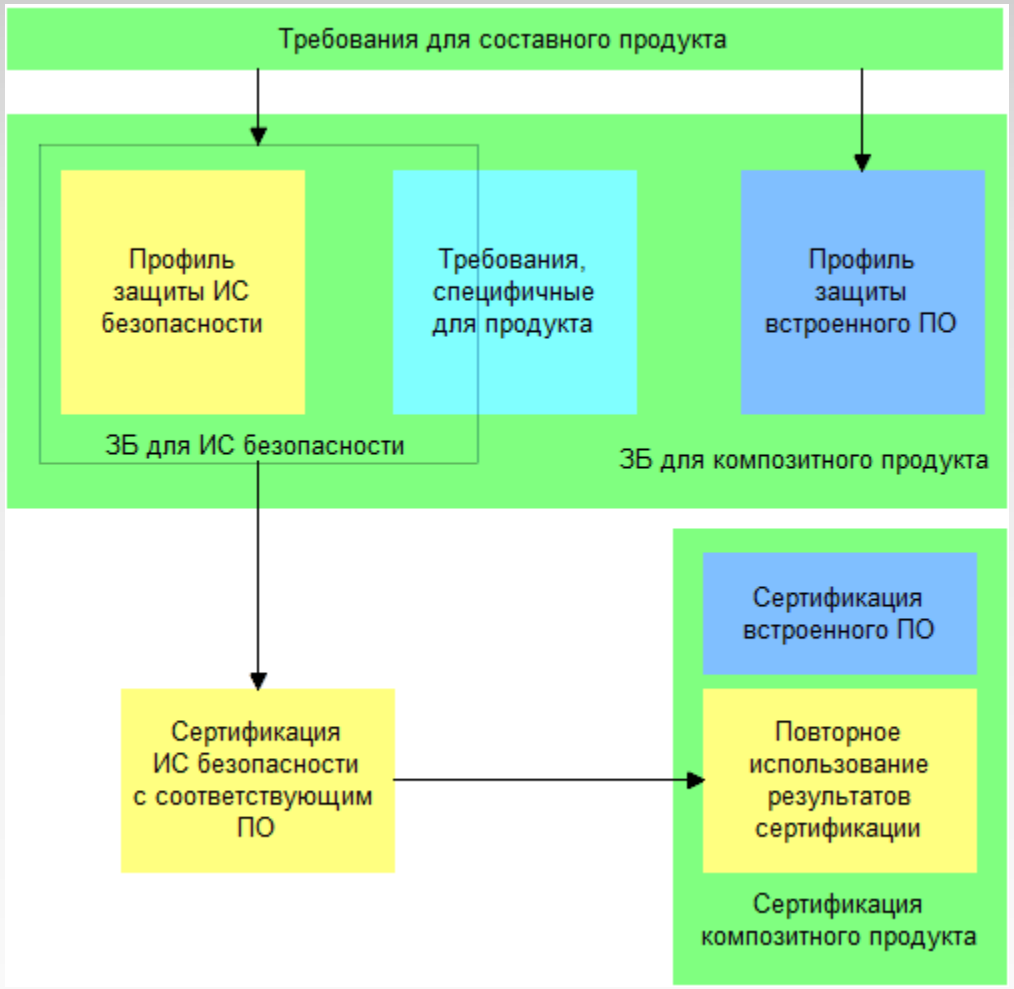
Объект оценки (ОО) корня доверия, включает в себя:

- Любое аппаратное, встроенное и прикладное программное обеспечение, используемое для обеспечения безопасности корня доверия микроконтроллера в составе:
  - Неизменяемый корень доверия MCU, например, загрузочное ПЗУ, такие параметры, как данные инициализации, аппаратные ключи и идентификаторы, аппаратное блоки изоляции, управление жизненным циклом системы безопасности и контроль за его выполнением (например, с помощью функции отладки, если она присутствует). Этот компонент не может быть обновлен.
  - Обновляемый корень доверия MCU, такой как платформа для изоляции программного обеспечения, защищающая более доверенное программное обеспечение от менее доверенного программного обеспечения, общие службы, такие как привязка к аппаратной платформе, первоначальная аттестация, общие криптографические службы, верификация обновлений встроенного ПО.
  - Доверенные подсистемы, используемые корнем доверия MCU, такие как подсистемы безопасности, доверенные периферийные устройства, SIM-карты или элементы безопасности (SE), включая как аппаратные, так и программные компоненты.
- Руководство по безопасному использованию MCU, обновляемое после поставки.

Объект оценки не содержит:

- Прикладной корень доверия
- Недоверенную среду исполнения (НДСИ, REE)
- Приложения, размещенные в НДСИ.

Структура профиля защиты корня доверия

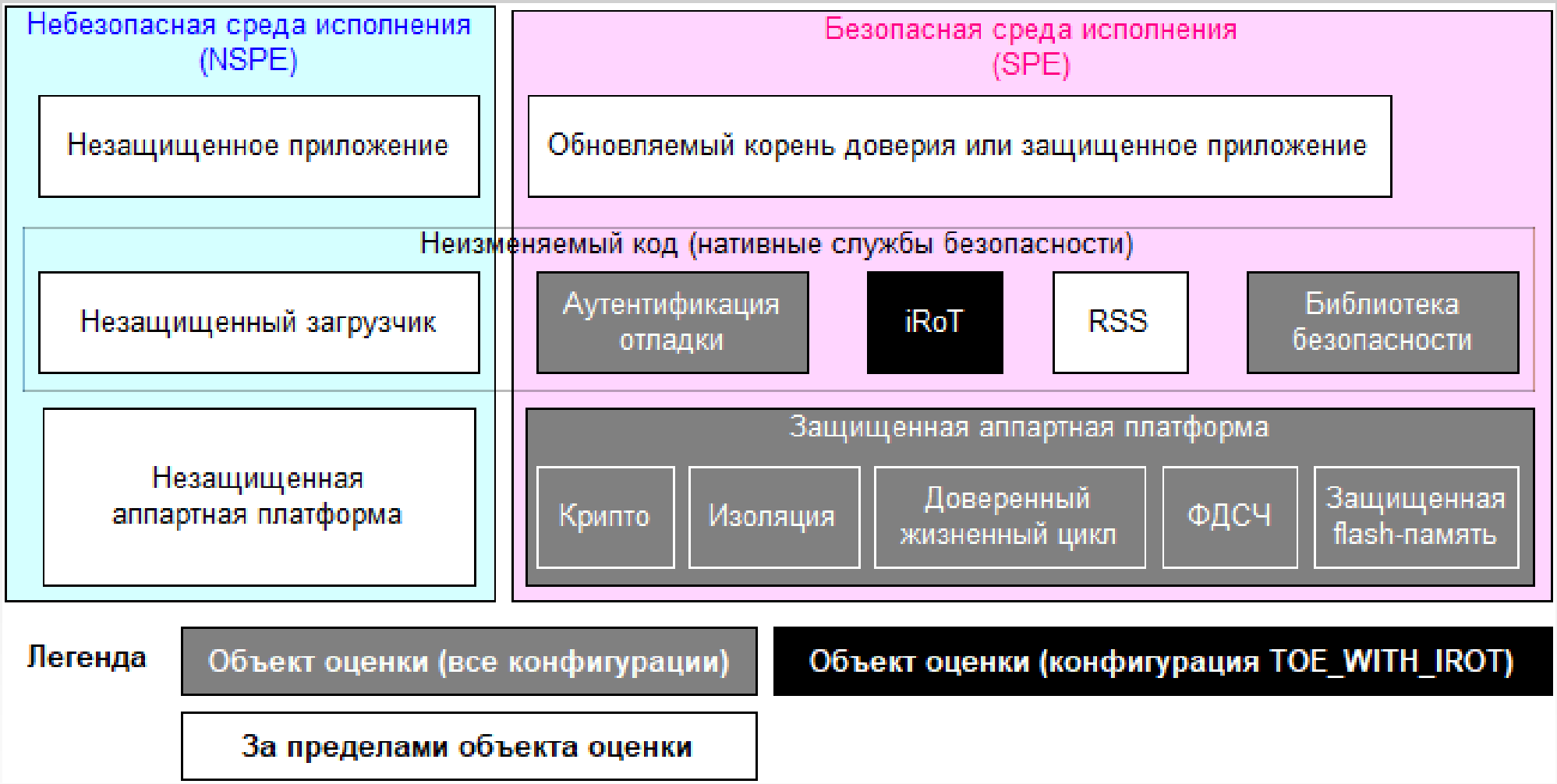


Производитель ОО поставляет ОО производителю композитного изделия. Интерфейсы, доступные после поставки производителем ОО, отличаются от интерфейсов для оперативного использования композитного изделия конечным потребителем (этап 7 слайд «Жизненный цикл…»). Этот интерфейс для конечного потребителя определяется разработчиком встроенного программного обеспечения ИС безопасности. Таким образом, руководящая документация, поставляемая производителем ОО, предназначена для разработчика встроенного программного обеспечения ИС безопасности и производителя композитного продукта. Термин «конечный потребитель» в данном случае означает пользователя композитного продукта на этапе 7 (слайд «Жизненный цикл…»).

На рисунке представлена взаимосвязь между сертификацией ИС безопасности со специализированным программным обеспечением и композитным продуктом, включающим встроенное программное обеспечение.

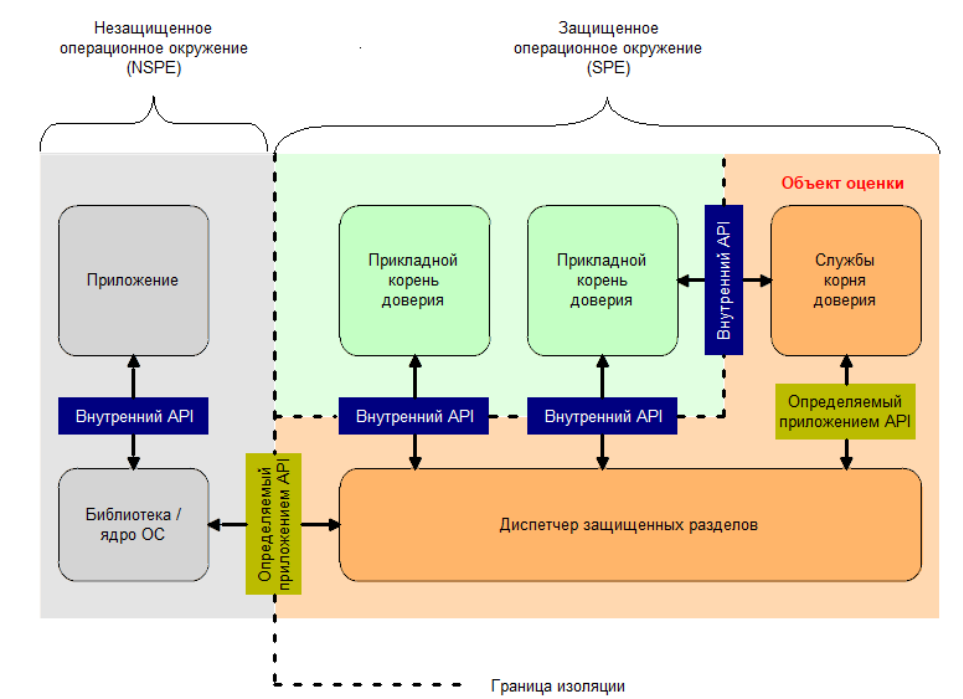
Объект оценки для корня доверия (микроконтроллера)

Общее описание объекта оценки



ПО объекта оценки корня доверия для микроконтроллера

Архитектура ПО корня доверия для микроконтроллера



Корень доверия микроконтроллера MCU RoT (ОО) встроен в устройство и работает совместно со стандартной незащищенной вычислительной средой, такой как ОСРВ.

Архитектура программного обеспечения ТОЕ определяет три различных класса компонентов:

- Корневые службы доверия, которые предоставляют службы безопасности для доверенной (ДСИ) и недоверенной (НДСИ) сред исполнения.
- Внутренние API-интерфейсы
- Базовые доверенные приложения, которые запускаются в ДСИ и получают доступ к его службам через внутренние API.

Архитектура программного обеспечения НДСИ также определяет три различных класса компонентов:

- Операционная система НДСИ, которая предоставляет клиентский API и отправляет запросы в ДСИ
- Клиентский API
- Приложения НДСИ, которые используют клиентский API для доступа к защищенным сервисам, предлагаемым MCU RoT, работающим на ДСИ.

Внешний программный интерфейс ОО включает в себя внутренний API (используемый приложением RoTs) и коммуникационный агент ДСИ. Протокол связи между НДСИ и ДСИ, используемый ниже уровня клиентского API, зависит от реализации.

Доверенная инсталляция в режиме "TOE_WITH_IROT"

Подготовка продукта осуществляется за три шага.
Поскольку статическая конфигурация безопасности программируется только на самом последнем этапе, то для того, чтобы выполнить полную установку с полностью активированной системой безопасности, необходимо выполнить три шага:
Шаг 1: Конфигурирование iRoT и DA. На этом шаге, с использованием TrustedPackageCreator создаются файлы конфигурации iRoT DA. В зависимости от выбранной конфигурации iRoT, автоматически обновляются файлы проекта (файлы компоновщика), а также статический сценарий обеспечения безопасности.
Шаг 2: Генерация образов кода и данных

- Образ кода генерируется командой, выполняемой в конце процесса компиляции проекта пользовательского приложения.
- Образ данных генерируется с помощью TrustedPackageCreator.

Шаг 3: Поставка. На этом шаге:

- Выполняется статический сценарий обеспечения безопасности.
- Образы кода и данных загружаются в пользовательскую flash память.
- Состояние продукта изменяется на “ПОСТАВКА” и конфигурационные данные записываются в область OB ключей.
- В завершение устанавливается окончательное состояние продукта (“ПОСТАВЛЕН”, “ЗАКРЫТАЯ_TZ”, “ЗАКРЫТЫЙ” или “ЗАБЛОКИРОВАННЫЙ”). Для защиты всего продукта, включая пользовательское приложение, окончательное состояние продукта должно быть установлено в “ЗАКРЫТЫЙ” или “ЗАБЛОКИРОВАННЫЙ”.

Доверенная инсталляция в режиме "TOE_WITHOUT_IROT"

Подготовка продукта осуществляется за три шага.
Поскольку статическая конфигурация безопасности программируется только на самом последнем этапе, то для того, чтобы выполнить полную установку с полностью активированной системой безопасности, необходимо выполнить три шага:
Шаг 1: Генерируются файлы конфигурации DA. В зависимости от пользовательского приложения Интегратора, на этом шаге должны быть сгенерированы дополнительные файлы конфигурации.
Шаг 2: Программирование байтов настройки. На этом шаге должны быть сконфигурированы: статическая защита безопасности, определение доверенной области и адрес загрузки в пользовательской flash памяти.
Шаг 3: Запись образа и поставка OB ключей. На этом шаге:

- Состояние продукта изменяется на “ПОСТАВКА” и конфигурационные данные записываются в область OB ключей.
- В завершение устанавливается окончательное состояние продукта (“ПОСТАВЛЕН”, “ЗАКРЫТАЯ_TZ”, “ЗАКРЫТЫЙ” или “ЗАБЛОКИРОВАННЫЙ”). Для защиты всего продукта, включая пользовательское приложение, окончательное состояние продукта должно быть установлено в “ЗАКРЫТЫЙ” или “ЗАБЛОКИРОВАННЫЙ”.

Сертификация ARM PSA (PSA Certified)

ISO/IEC 15408-3:2022 (ГОСТ Р ИСО/МЭК 15408-3-2013)

Объект оценки (ОО) PSA Certified

Компоненты

Предметом оценки ***PSA Certified***, или объектом оценки (***Target of Evaluation, TOE***), является комбинация аппаратных и микропрограммных компонентов, обеспечивающих соответствие устройства спецификации PSA. Рассматриваемое аппаратное обеспечение может представлять собой Систему-в-Корпусе (***System-in-Package, SiP***), Систему-на-Кристалле (***System-on-Chip, SoC***) интегрированные на печатную плату, или аналогичные конфигурации.

Аппаратное обеспечение также входит в сферу оценки безопасности, поскольку оно обеспечивает функции безопасности, такие как неизменяемое хранилище или защита отладки по JTAG, которые необходимы для обеспечения безопасной реализации требований PSA. Случай аппаратных ограничений систем на базе FPGA рассматривается в требованиях для ***PSA Certified Level 2 Ready***.

Компонентами платформы PSA, которые входят в сферу оценки безопасности, являются :

- Обновляемый PSA RoT, состоящий из подсистемы программной изоляции, защиты более доверенного ПО от менее доверенного ПО, общих служб, таких как служба привязка, служба начальной аттестации, общие криптографические службы, служба верификации обновлений ПО.
- Необновляемый PSA RoT, например код в Boot ROM, корневые активы и ID, аппаратная изоляция, управление доверенным жизненным циклом. Все эти компоненты являются необновляемыми.
- Доверенные подсистемы, используемые PSA RoT, такие как подсистемы безопасности, доверенные периферийные модули, SIM или SE, в состав которых входят программные и аппаратные компоненты.

Интерфейсы

Следующие интерфейсы представляют собой границу между ОО и его окружением и могут использоваться для взаимодействия с ОО и проведения атак:

- API между прикладным RoT и PSA RoT внутри SPE
- API между NSPE и SPE
- Интерфейс между PSA RoT внешними устройствами

Сертификация PSA Certified

Сертификация безопасности PSA Certified компонентов RoT позволяет провести лабораторную оценку компонентов защиты IP-ядер, таких как криптопроцессоры и подсистемы управления ключами (например, на основе PUF), которые встроены в корень доверия ИС (RoT).
Большинство ведущих мировых производителей кремниевой продукции внедрили систему PSA Root of Trust (PSA-RoT) и используют сертификат PSA, чтобы продемонстрировать надежность своих реализаций функций безопасности благодаря многоуровневой схеме PSA Certified.
Поставщики IP-ядер могут получить сертификат PSA на компоненты RoT, который подтверждает выполнение части требований PSA Certified Level 2, Level 3 или Level 4 iSE/SE. Это дает поставщикам IP-ядер возможность продемонстрировать с помощью сертификата PSA Certified надежность защиты, а также способ поддержать своих клиентов, которые хотят получить сертификат PSA на свои СнК, поскольку они смогут повторно использовать сертификаты IP-ядер.
Повторное использование результатов оценки компонентов для полной сертификации ИС по требованиям PSA Certified Level 2 и PSA Certified Level 3 упрощает процесс сертификации и ускоряет вывод продукции на рынок.

PSA Certified Level 1, 2, 2+SE

PSA Certified Level 1
для устройств, ПО и производителей ИС

- Демонстрирует **использование надежных принципов обеспечения безопасности**.
- **Основана на независимой оценке безопасности**, в ходе которой анализируется реализация функций безопасности.
- **Помогает уменьшить фрагментацию**, приводя в соответствие с основными глобальными руководящими принципами и нормативными документами. PSA обеспечивает соответствие между своим сертификатом L1 и требованиями других стандартов, таких как ETSI EN 303 645, NIST 8259A.
- **Повторное использование сертификации PSA для оценки соответствия рыночным стандартам**: сертификат PSA Certified Level 1 , может быть повторно использован в других отраслевых схемах сертификации, обеспечивая соответствие требованиям конечного рынка и вертикальных приложений. Альянс IoXt и UL признают сертификат PSA Root of Trust как способ ускоренного получения собственного сертификата

PSA Certified Level 2
для производителей ИС

Используется **независимое тестирование**, чтобы показать, что компонент безопасности PSA Root of Trust (PSA-RoT) может защитить от масштабируемых удаленных программных атак
Обеспечивается уровень **безопасности, подходящий для многих решений IoT для массового рынка**, подтвержденную независимой лабораторной оценкой. **Оценка занимает меньше времени** (и обходится дешевле), чем сертификация PSA Level 3, что может быть ключевым фактором в графике разработки продукта.

PSA Certified Level 2+ SE
для производителей ИС

Расширенная версия Level 2 с дополнительным подтверждением наличия усиленной физической защиты криптографических ключей и криптографических операций.

PSA Certified Level 3, 4

PSA Certified Level 3
для производителей ИС

- Является доказательством того, что **PSA-RoT** защищает от серьезных аппаратных и программных атак.
- Этот более высокий уровень предназначен для:
  - **IoT-решений, которые должны защищать ценные активы**;
  - Решений, особенно подверженных атакам из-за потенциальной экономической выгоды или ущерба бренду;
  - Решений, которые физически доступны и, следовательно, требуют защиты от аппаратных атак.
- Испытательная лаборатория проводит оценку по принципу "белого ящика", которая включает в себя анализ уязвимостей и тестирование на проникновение.
- Поддерживаемые профили защиты:
  - Профиль PSA-RoT Level 3 Protection Profile
  - Профиль защиты SESIP PSA-RoT Level 3 Protection Profile.

PSA Certified Level 3 + SE
для производителей ИС

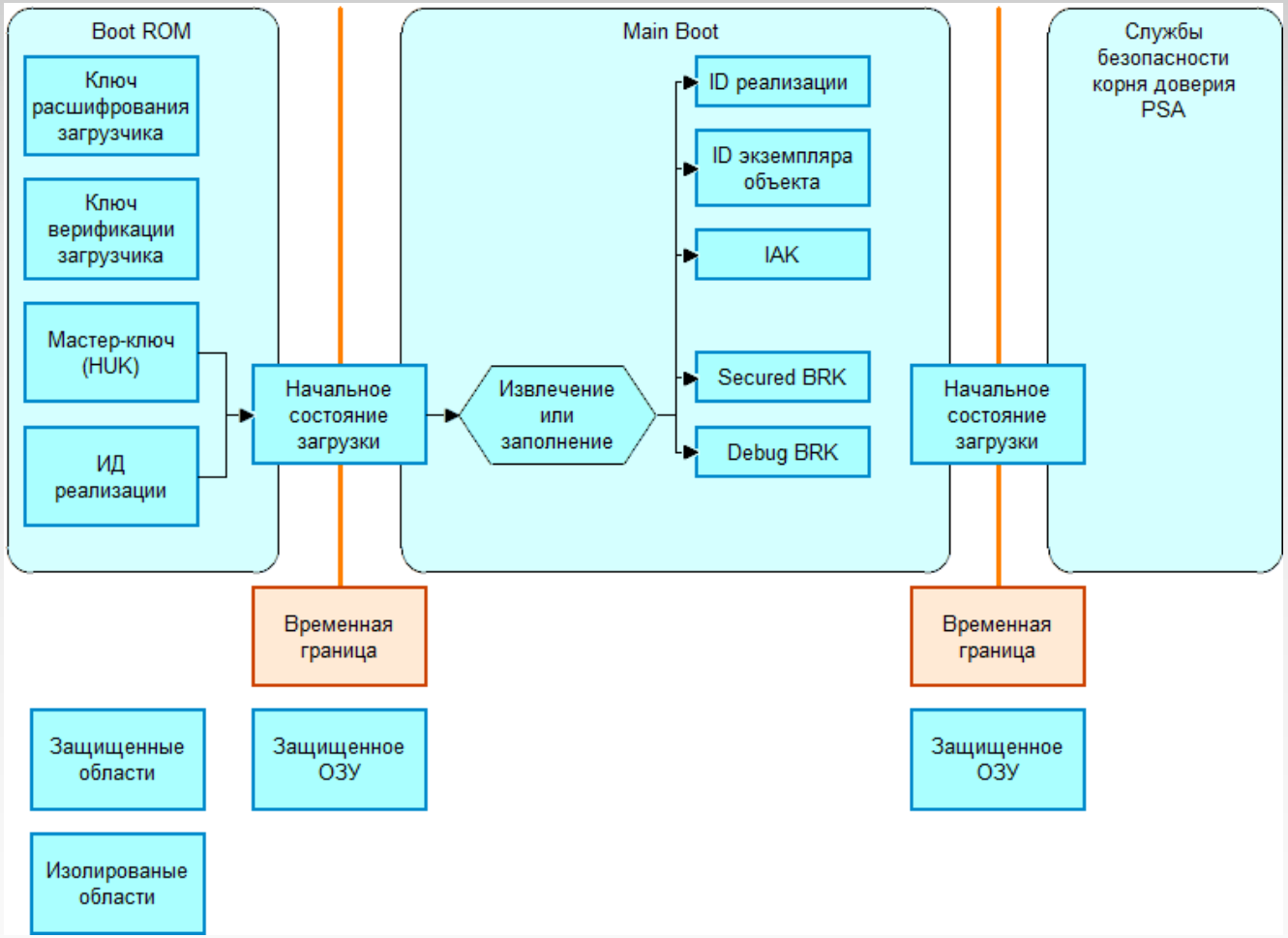
Расширенная версия PSA Certified Level 3 с дополнительным подтверждением наличия усиленной физической защиты криптографических ключей и криптографических операций.

PSA Certified Level 3
для производителей ИС ISE/ES

- **Повышенная устойчивость к атакам**: Продукты, сертифицированные на Level 4, предназначены для защиты от еще более серьезных потенциальных злоумышленников и угроз по сравнению с Level 3, что делает их пригодными для защиты особо важных активов или борьбы с изощренными противниками.
- **Испытания с высоким уровнем доверия**: Испытания для получения сертификатов Level 4 проводятся испытательными лабораториями с высоким уровнем доверия. При оценке соответствия используются строгие методики тестирования и испытательные стенды с самым современным оборудованием для оценки надежности продуктов.
- **Комплексное тестирование**: Процесс оценки включает в себя комплексные сценарии тестирования для доказательства устойчивости продуктов к аппаратным и программным атакам. Он может включать в себя оценку методом "белого ящика", анализ уязвимостей, тестирование на проникновение и другие передовые методы исследований.
- **Признание в отрасли**: Сертификат Level 4 означает высочайший уровень обеспечения безопасности в рамках системы сертификации PSA. Он доказывает способность продукта обеспечивать высокий уровень безопасности для критически важных приложений и сред.

Экосистема PSA

Активы, принадлежности и другие параметры PSA RoT



BRK (Binding Root Key) – привязка корневого ключа

HUK (Hardware Unique Key) – уникальный для устройства ключ, мастер-ключ

IAK (Initial Attestation Key) - ключ для первоначальной аттестации

Простейший четырехэтапный процесс PSA Certified

Платформа PSA Certified сводит разработку и внедрение системы безопасности к простому четырехэтапному процессу, снижая сложности и обеспечивая создание системы безопасности нужного уровня без чрезмерных затрат и увеличения сроков вывода на рынок.

Анализ: Выявление угроз, которые потенциально могут скомпрометировать устройство, и формирование набора требований к безопасности на основе выявленных рисков. PSA Certified предоставляет бесплатные редактируемые примеры, которые помогут разработать уникальную модель угроз для конкретного продукта..

Архитектура: Использование уникальных требований к безопасности для определения и выбора компонентов и спецификаций, которые позволят создать необходимый уровень безопасности для разрабатываемого продукта.

Реализация: Реализация доверенных компонент и встроенное ПО, используя высокоуровневые API-интерфейсы для обеспечения необходимого уровня безопасности и создания интерфейса к аппаратному корню доверия (RoT)..

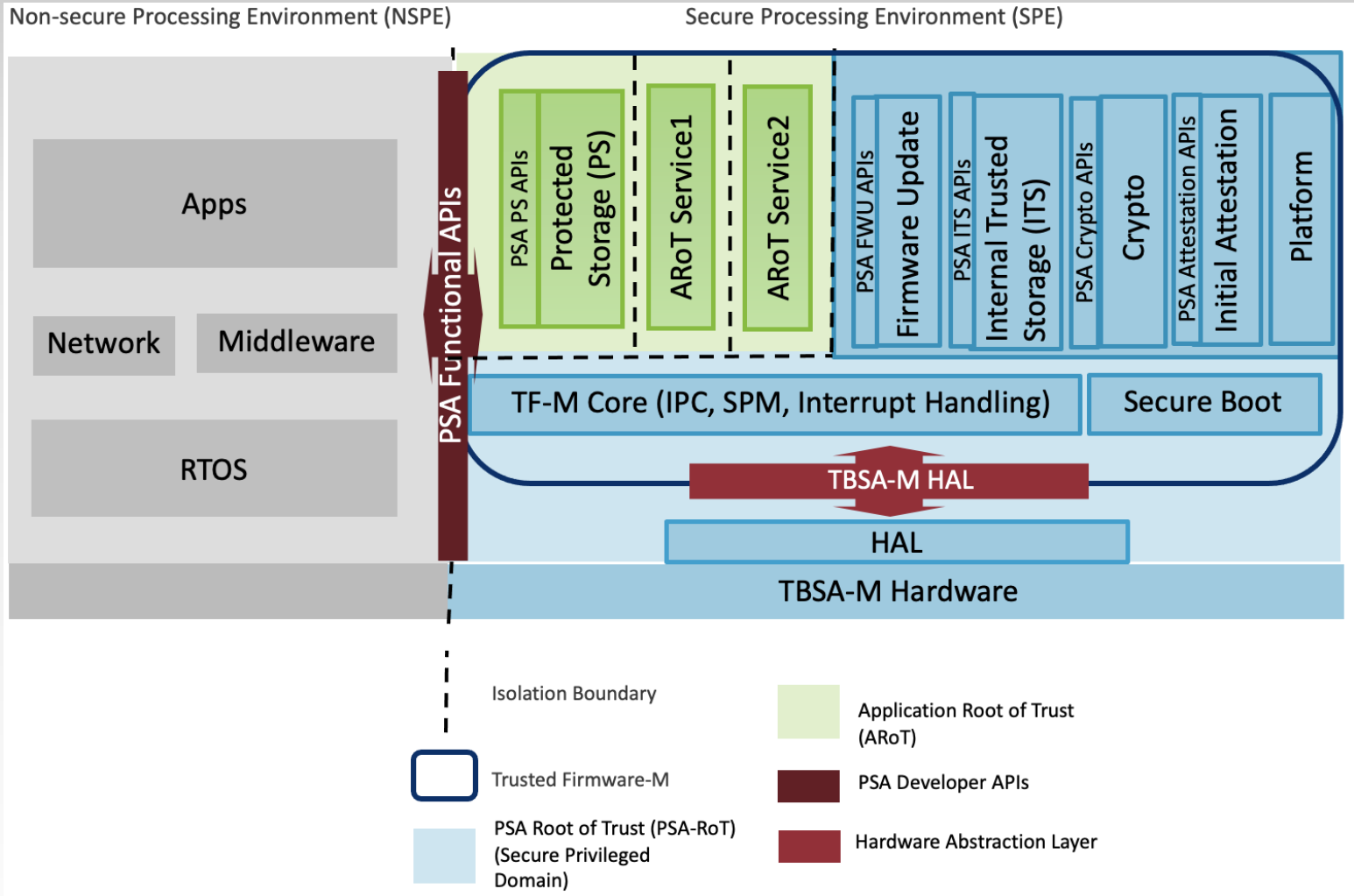
Сертификация: После независимой оценки безопасности проведение сертификацию устройства, платформы системного программного обеспечения или ИС и демонстрация приверженности передовым методам обеспечения безопасности.

Корни доверия TF-A и TF-M

Корень доверия TF-A

Одновременное выполнение защищенного и незащищенного кода в одном и том-же физическом блоке памяти, как это реализовано в расширениях ARM TrustZone-A, к безопасности никакого отношения не имеет, поэтому в данном исследовании не рассматривалось.

Корень доверия TF-M



TF-M Trusted FirmWare for Arm Cortex-M
TBSA-M Trusted Base System Architecture for Arm Cortex-M
PSA ARM Platform Security Architecture
PSA FWU PSA Firmware Update
ITS Internal Trusted Storage
IPC Inter Processors Communication
SPM Secure Partitions Manager

Корень доверия TF-M

Trusted Firmware-M (TF-M) реализует безопасную среду исполнения (Secure Processing Environment, SPE) для архитектур Armv8-M и Armv8.1-M (например в процессорах Cortex-M33, Cortex-M23, Cortex-M55, Cortex-M85) и двухъядерных платформах. Это эталонная реализация архитектуры безопасности платформы, соответствующая рекомендациям PSA Certified, позволяющим сертифицировать в рамках PSA Certified ИС, ОСРВ и устройства целиком.

TF-M основывается на изолирующей границе между небезопасной (Non-secure Processing Environment, NSPE) и безопасной (Secure Processing Environment, SPE) средой исполнения. Она может не ограничиваться использованием технологии Arm TrustZone для архитектур Armv8-M и Armv8.1-M. Для предшествовавших Armv8-M архитектурах требовалась физическая изоляция ядер.

TF-M содержит:

- Механизм доверенной загрузки (Secure Boot) для аутентификации образов небезопасной (NSPE) и безопасной (SPE) среды исполнения
- Ядро TF-M Core для управления изоляцией, обменом данными и выполнением кода внутри SPE и NSPE
- Криптографические службы безопасности, службы безопасности внутреннего доверенного хранилища (Internal Trusted Storage, ITS), защищенного хранилища (Protected Storage, PS), обновлений (Firmware Update) и аттестации (Attestation)

Корень доверия TF-M

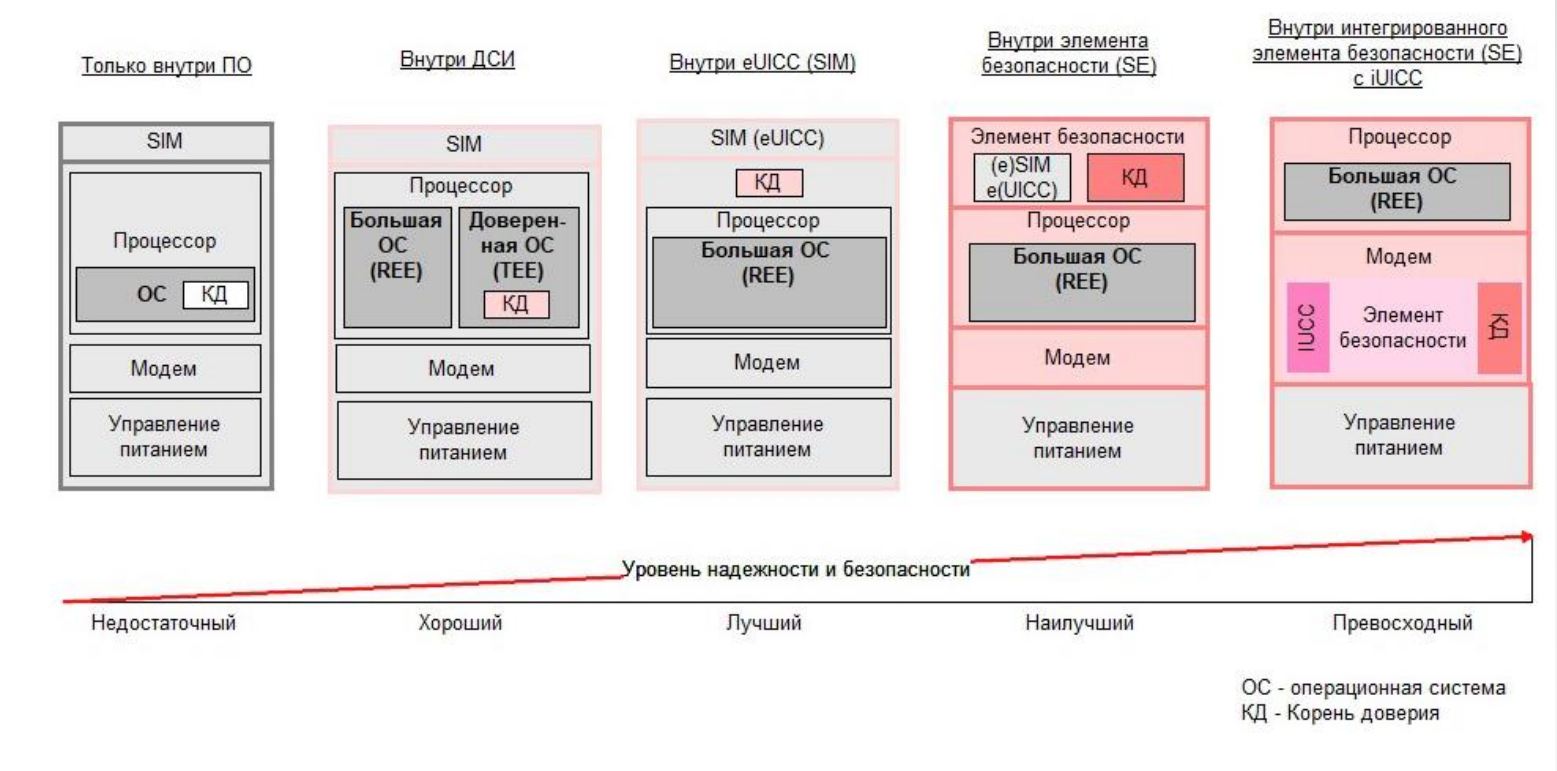
TF-M реализует спецификация PSA-FF-M, определяющую механизмы межпроцессорного обмена (IPC) и функции безопасности (SFN), обеспечивающие обмен данными между изолированными разделами прошивки. TF-M легко настраивается, позволяя пользователям включать в конечный продукт только необходимые службы и функции безопасности. Эталонный проект предоставляет пример базовой конфигурации Base Configuration, состоящей только из драйверов ядра TF-M и драйверов платформы и четыре предопределенных конфигурации, известных как профили TF-M Profiles. Профили TF-M Profiles и базовая конфигурация TF-M могут быть настроены для включения только необходимых служб и функций безопасности.

Приложения и библиотеки в небезопасной среде исполнения (Non-secure Processing Environment) могут использовать эти службы безопасности через стандартный набор функций из PSA Functional API. Приложения, работающие на устройствах с ядрами Cortex-M могут использовать службы TF-M для обеспечения безопасного соединения с граничными шлюзами и облачными сервисами IoT. Службы TF-M также защищают критически важные для платформы активы, такие как конфиденциальные данные, ключи и сертификаты. TF-M поддерживается большинством микроконтроллеров на базе Cortex-M v.8 и операционными системами реального времени (RTOS).

Термины TFM и TF-M равноправны и могут совместно использоваться в документации и коде, относящихся к Trusted Firmware M.

Архитектура корня доверия

Эволюция архитектуры корня доверия для мобильных устройств



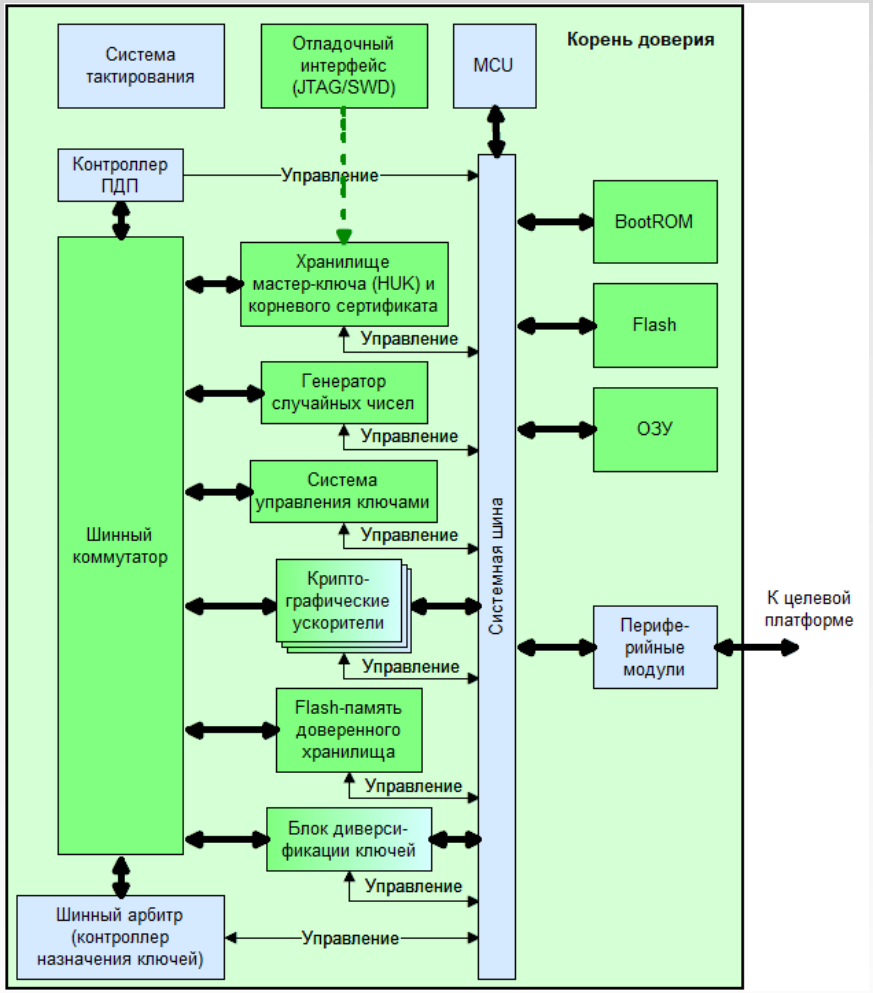
Корень доверия все дальше отодвигается от прикладного процессора к защищаемому объекту (коммуникационный интерфейс).

Это позволяет:

- увеличить надежность и защищенность решения,
- уменьшить поверхность атаки,
- избавиться от проблем совместимости с прикладным кодом,
- упростить сертификацию, ограничиваясь сертификацией аппаратной платформы.

Внешний корень доверия

Блок-схема внешнего корня доверия



Безопасность решения обеспечивается тем, что тракты прохождения ключей и данных разделены физически, а процессорный элемент только конфигурирует коммутатор источников и приемников ключевой информации и контроллер ПДП, обеспечивающий ее передачу.

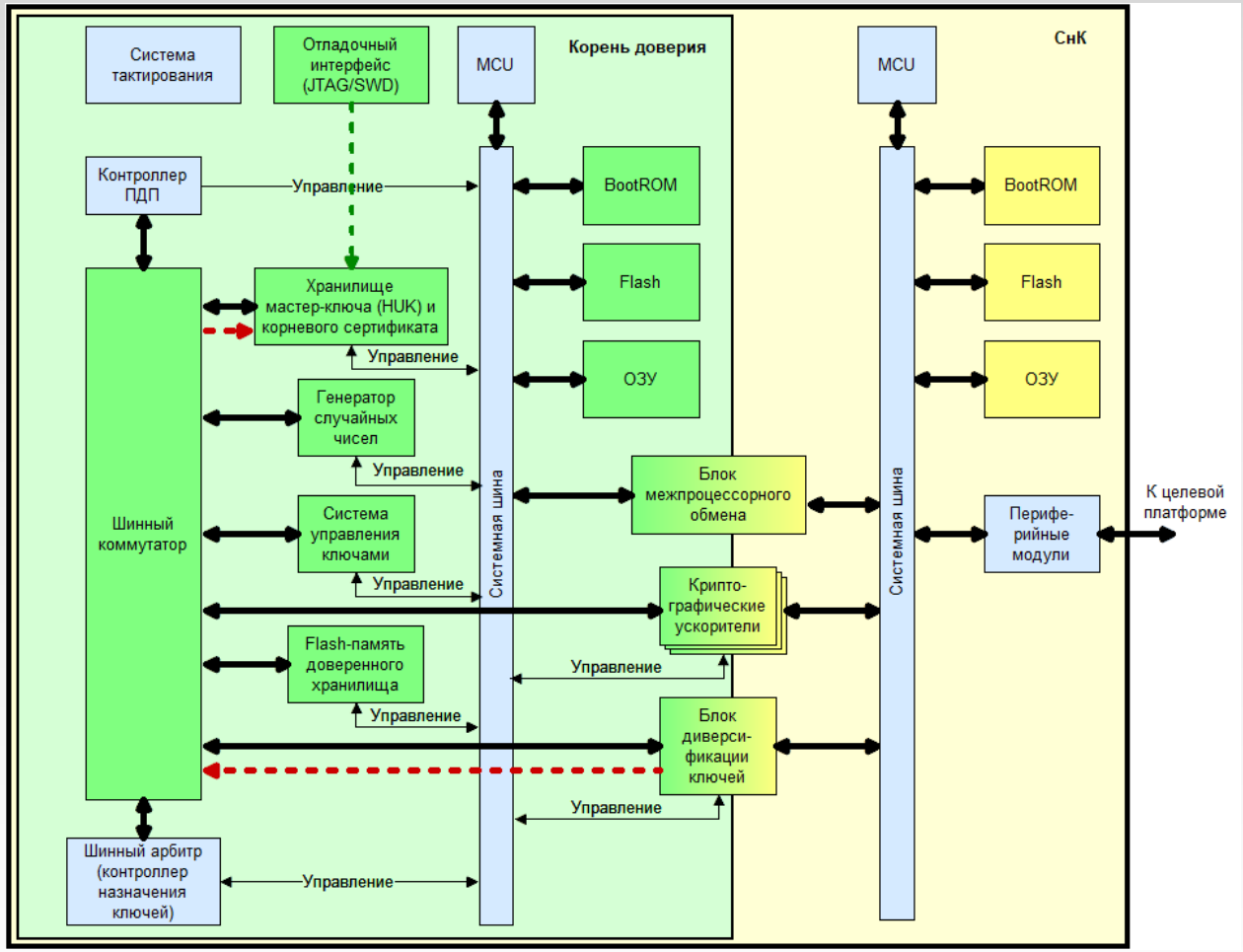
Требования:

Хранилище мастер-ключа и корневого сертификата **ДОЛЖНО** быть защищено от НСД, как физического, так и от ТУИ по каналам ПЭМИН;

Система диверсификации ключей **ДОЛЖНА** быть защищена от линейного и дифференциального криптоанализа.

Корень доверия в микроконтроллере

Блок-схема корня доверия в микроконтроллере



СнК микроконтроллера состоит из двух подсистем:

1. Коммуникационный процессор;
2. Корень доверия.

Каждая из подсистем управляется собственным вычислительным ядром.

Безопасность решения обеспечивается тем, что:

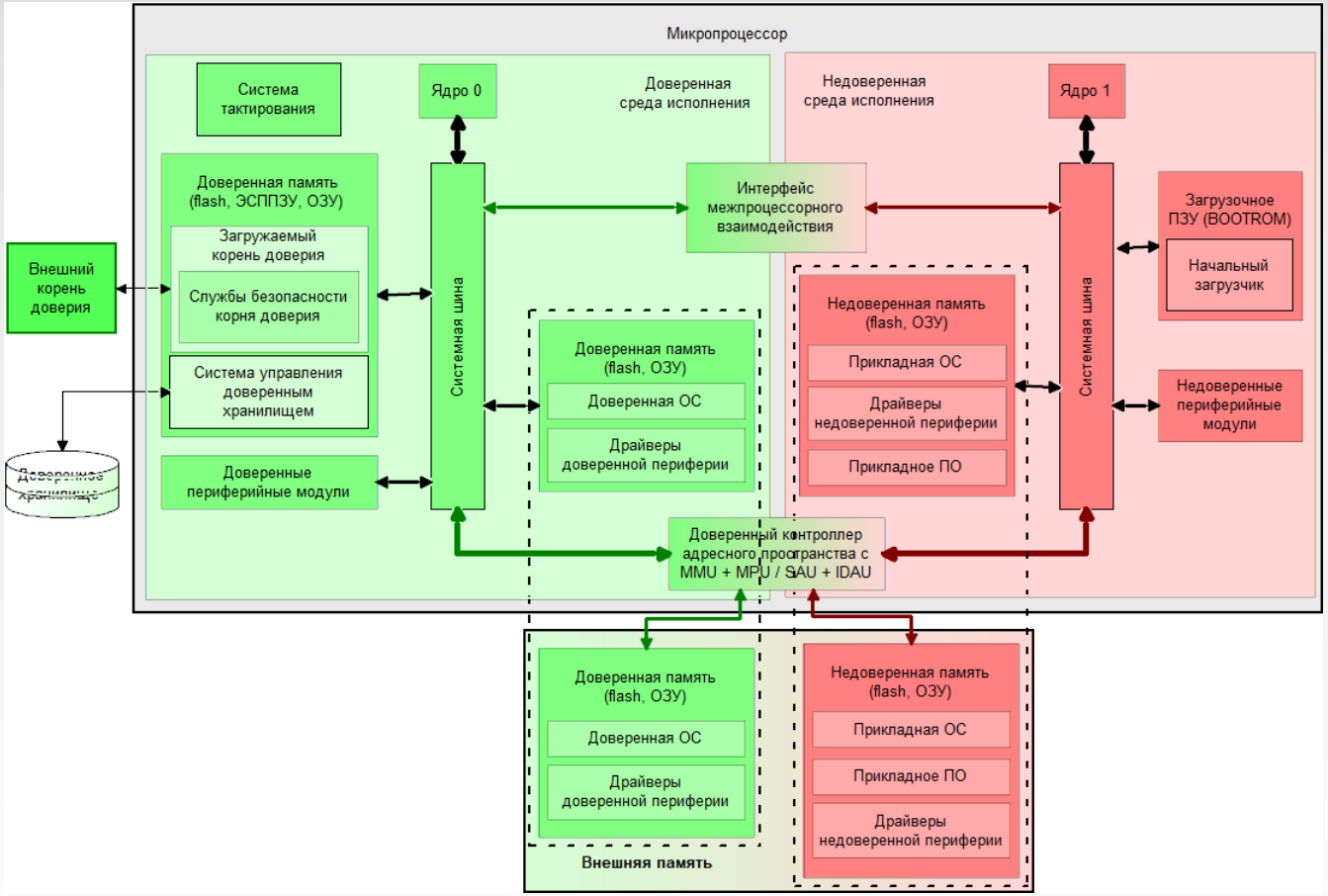
- тракты прохождения ключей и данных разделены физически и управляются различными ядрами,
- процессорный элемент корня доверия только конфигурирует коммутатор источников и приемников ключевых документов и контроллер ПДП, обеспечивающий ее передачу,
- обмен командами между корнем доверия и прикладного процессора осуществляется через блок межпроцессорного обмена,
- системные шины корня доверия и прикладного процессора разделены физически.

Требования:

1. Хранилище мастер-ключа и корневого сертификата должно быть защищено от физического НСД, так и от ТУИ по каналам ПЭМИН;
2. Система диверсификации ключей должна быть защищена от линейного и дифференциального криптоанализа.

Микропроцессоры со встроенными службами безопасности корня доверия

Блок-схема микропроцессора с встроенным корнем доверия



Возможна реализация загружаемых служб безопасности корня доверия на едином модуле памяти, управляемом системой разделения доступа, например, **ARM TrustZone**.

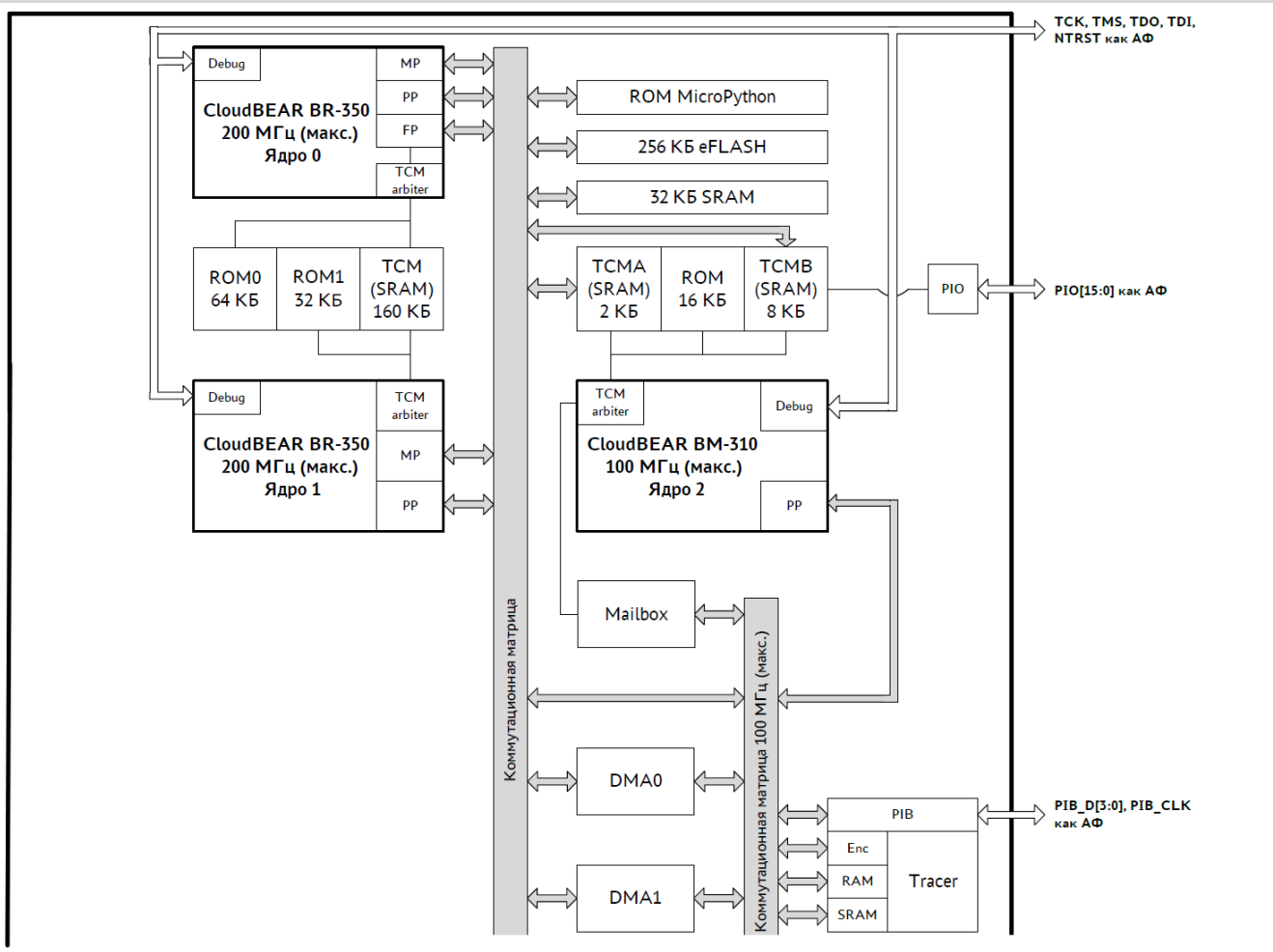
Для микроконтроллеров наиболее надежной и защищенной будет архитектура с физически разделенными блоками памяти. При этом ненужными становятся: доверенный и недоверенный контроллер внешней памяти и доверенный контроллер адресного пространства.

Для таких ядер, как **RISC-V**, возможно комбинированное решение с внутренней памятью для доверенной среды исполнения и внешней для недоверенной среды исполнения.

Примеры реализаций

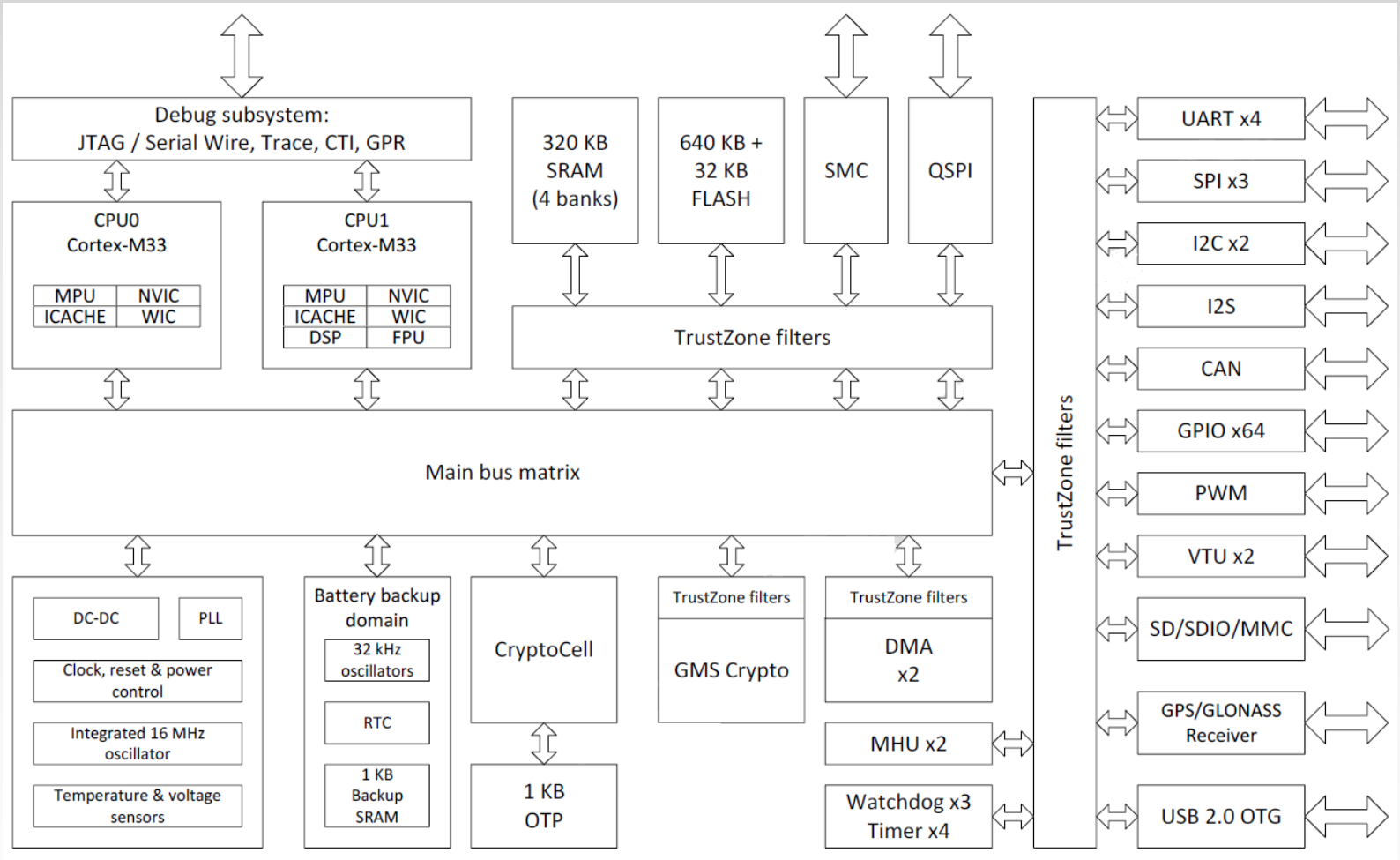
Микроконтроллер Baikal-U

Схема соединения ядер микроконтроллера Baikal-U



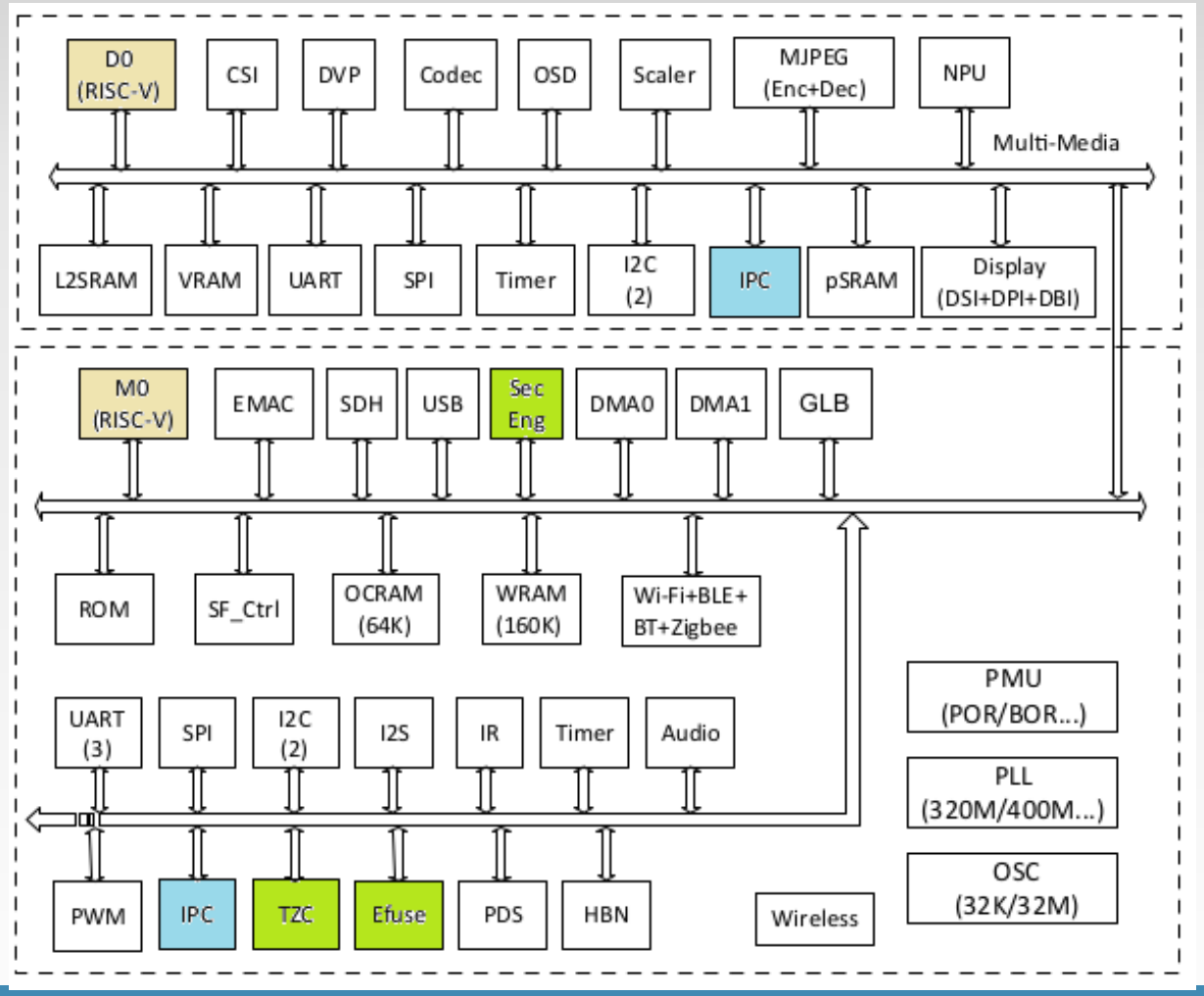
Микроконтроллер 1892ВМ268 ElIoT

Схема соединения ядер микроконтроллера 1892ВМ268 ElIOt



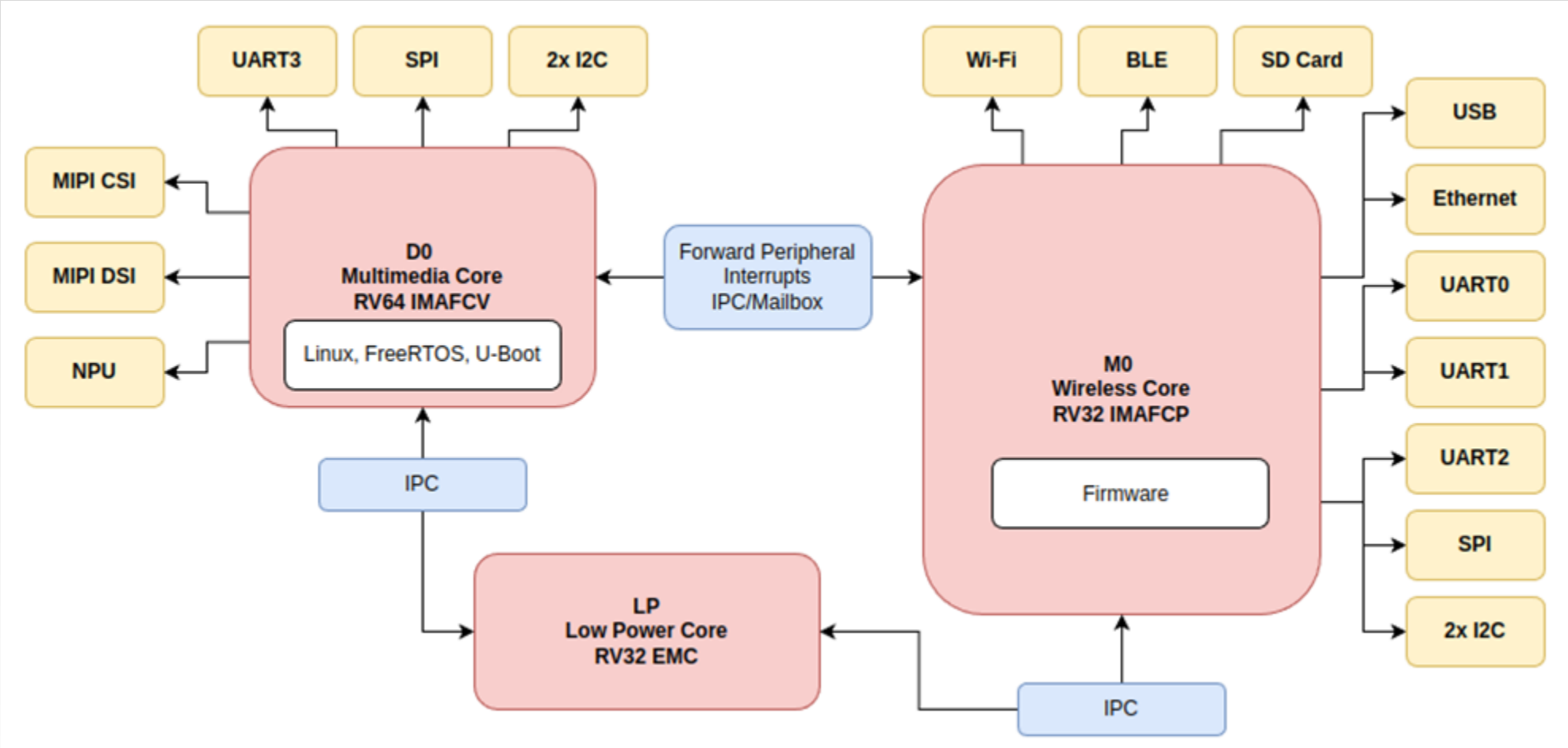
Промышленный беспроводной микроконтроллер

Блок-схема промышленного беспроводного микроконтроллера



Промышленный беспроводной микроконтроллер

Логическая схема соединения ядер промышленного беспроводного микроконтроллера



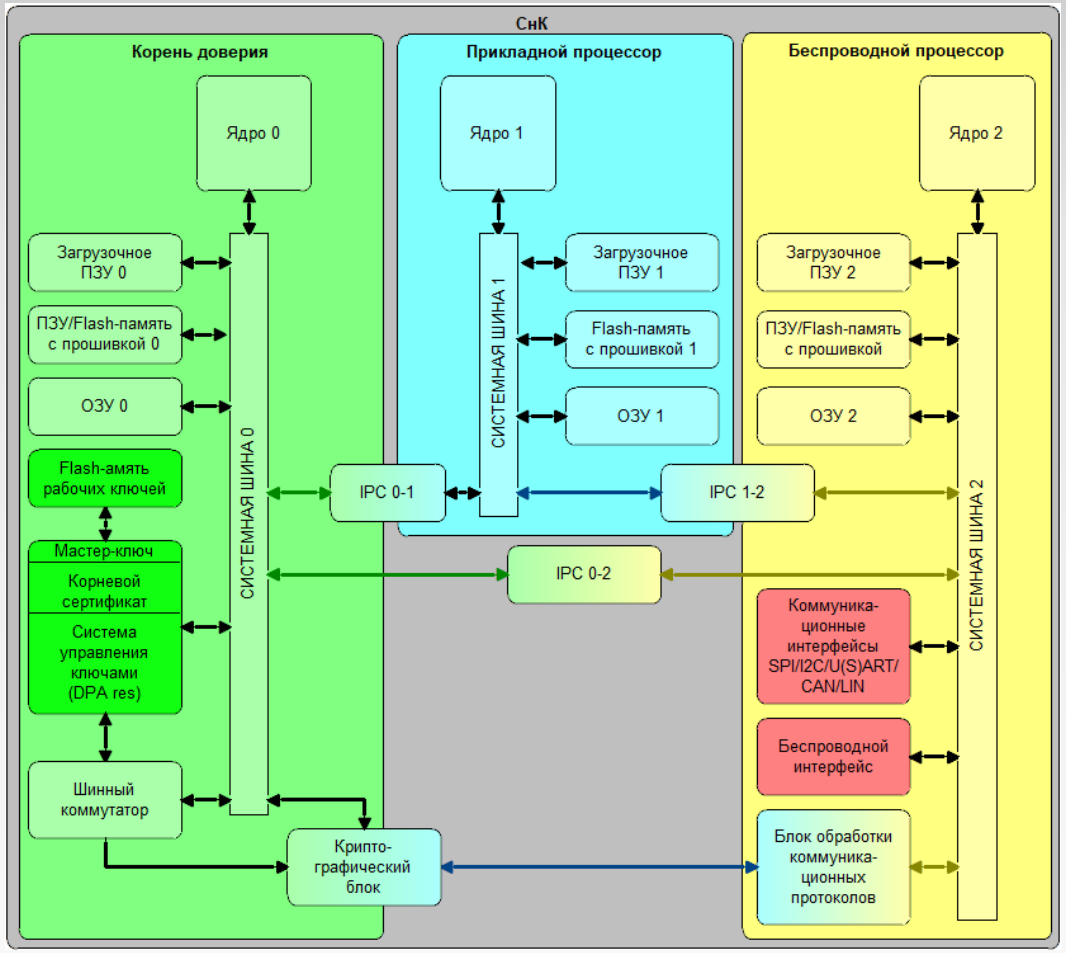
Промышленный беспроводной микроконтроллер

Спецификация беспроводного микроконтроллера

- Беспроводные протоколы (Tier-1)
  - Приемопередатчик 2.4 ГГц
    - ❖ Wi-Fi 802.11 b/g/n
    - ❖ Bluetooth 5.x Dual-mode (BT+BLE)
    - ❖ Zigbee / IEEE 802.15.4
  - Совместные Wi-Fi/Bluetooth/Zigbee
  - Интегрированный балун, УМ/МШУ
  - Поддержка внешних УМ/МШУ
- Микроконтроллер
  - Многоядерный RISC-V CPU:
    - ❖ 64-битное ядро C906 (D0) 480 MHz.
    - ❖ 32-битное ядро E907 (M0) 320 MHz;
    - ❖ 32-битное ядро E902 (LP) 160 MHz;
  - Поддержка XIP QSPI flash
- Аппаратный ускоритель AI NN
  - NPU BLAI-100 для обнаружения/распознавания Video/Audio
- Память
  - – Встроенная 32/64 Мбайт DRAM
  - – Поддержка до 128 Мбайт SPI-Nor Flash
  - – Поддержка до 256 Мбайт SPI-NAND Flash
- Безопасность
  - Доверенная загрузка; Доверенная отладка
  - XIP QSPI On-The-Fly AES расшифрование (OTFAD)
  - Изоляция критического ПО (TrustZone)
  - AES в режимах CBC/CCM/GCM/XTS
  - MD5, SHA-1/224/256/384/512
  - TRNG (физический датчик случайных чисел)
  - PKA (ускоритель публичного ключа) для RSA/ECC

Беспроводной микроконтроллер с корнем доверия

Общее описание беспроводного микроконтроллера с корнем доверия



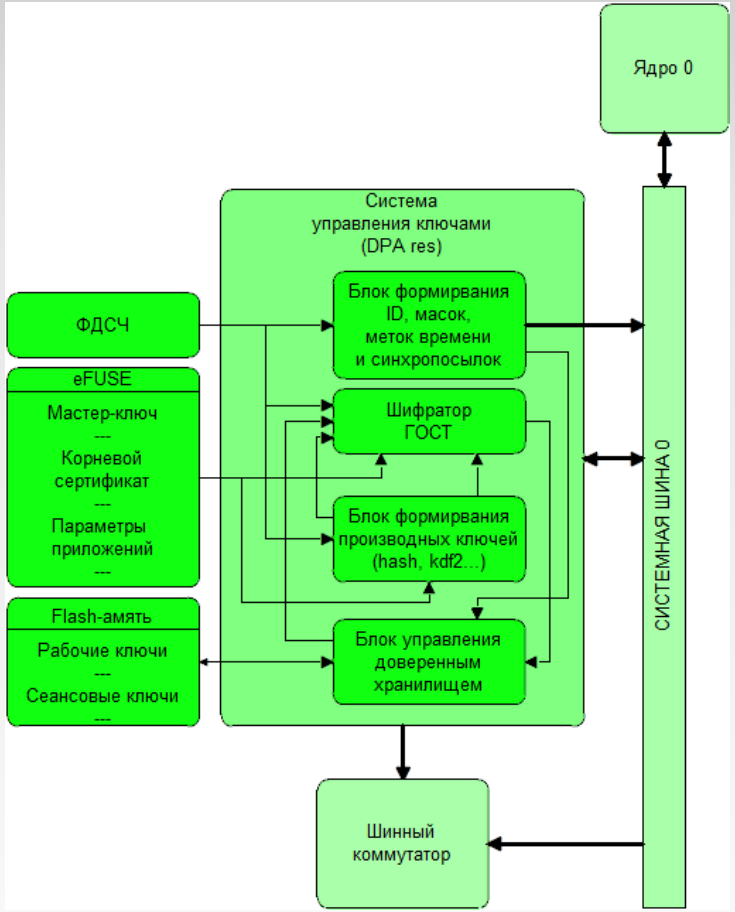
Микроконтроллер состоит из трех подсистем:

1. **Корня доверия**, отвечающего за верификацию программных модулей, хранение активов и выполнение криптографических операций;
2. **Прикладного процессора**, за выполнение пользовательских приложений, задач управления и реализации пользовательского HMI;
3. **Коммуникационного процессора,** отвечающего за взаимодействие с внешними устройствами по проводным и беспроводным интерфейсам, разбору и сборке пакетов обмена данными.

Между всеми тремя подсистемами организован попарный обмен данными и командами с помощью почтовых ящиков, качестве которых могут использоваться почтовые ящики или магазины регистров (FIFO).

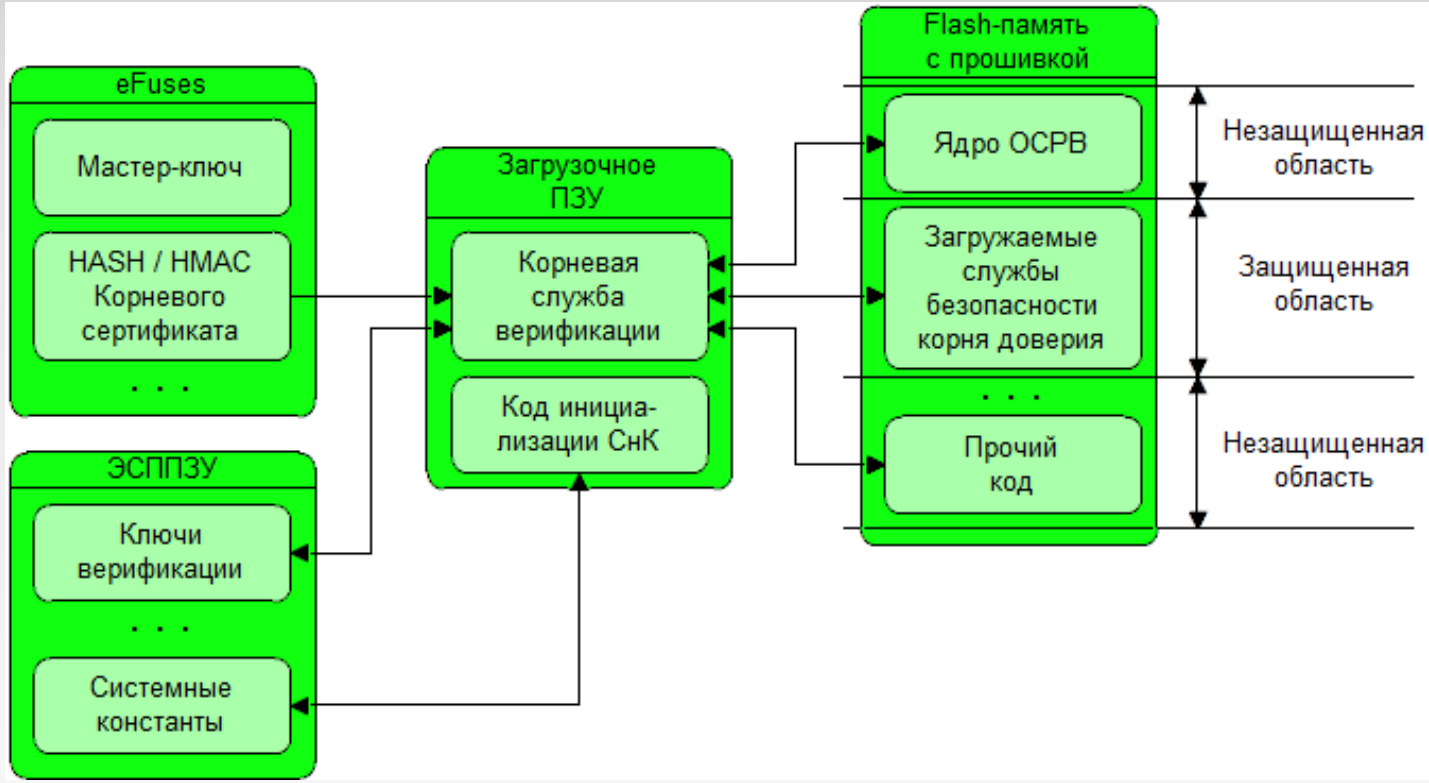
Безопасность выполнения криптографических операций гарантируется тем, что интерфейсы обмена данными и передачи ключей криптографического блока физически разделены и вынесены в разные подсистемы.

Система управления ключами корня доверия



Представленная на блок-схеме система управления ключами не имеет каких либо особенностей и обеспечивает поддержание полного жизненного цикла ключевых документов, масок, векторов инициализации и т.п.

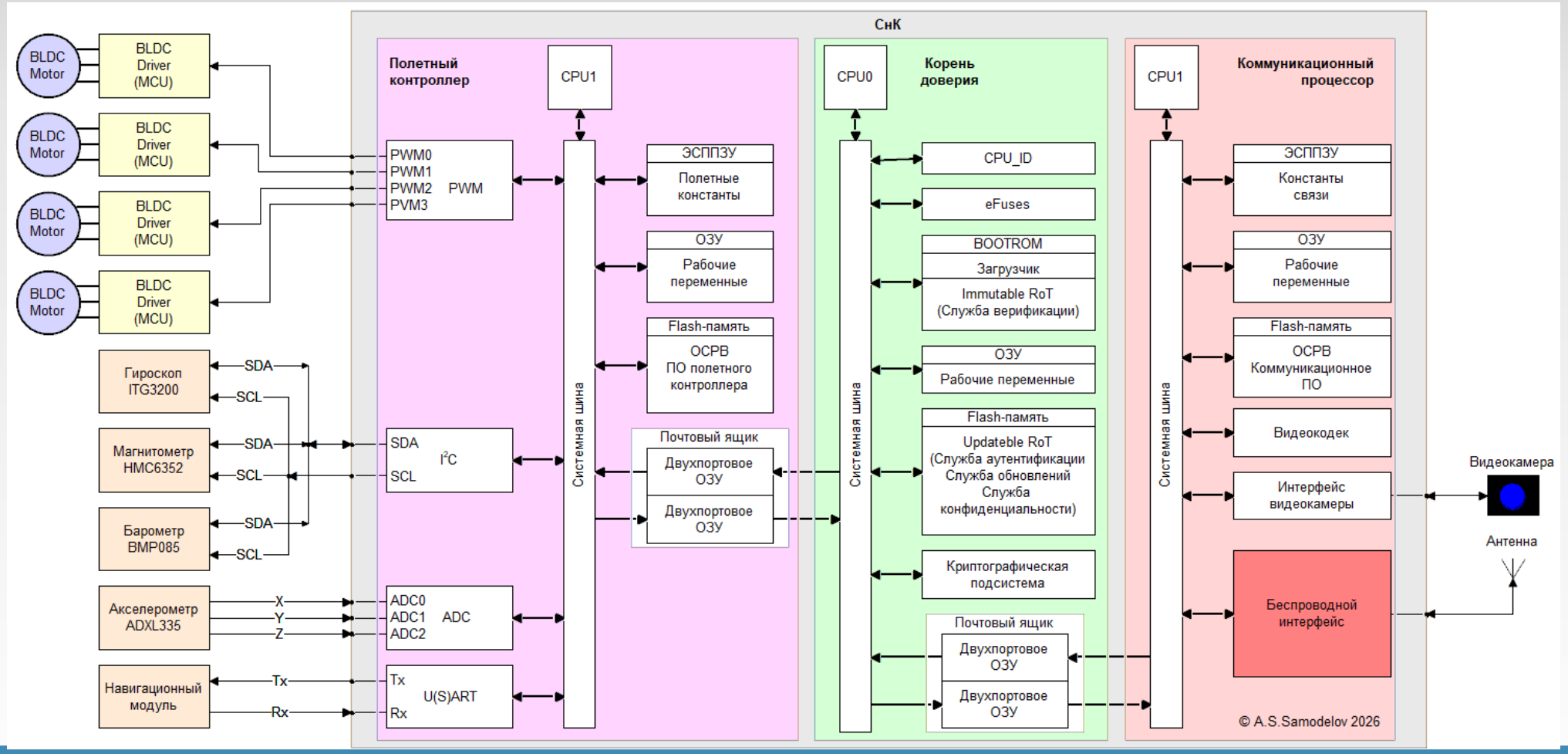
Развертывание корня доверия на микроконтроллере



На приведенной блок-схеме представлен механизм развертывания корня доверия (КД), начиная от аппаратного КД (Immutable RoT) и заканчивая службами безопасности расширенного корня доверия (Updatable RoT), запускаемыми под управлением ОС/ОСРВ.
Служба верификации iRoT выполняет верификацию подгружаемых компонент eRoT, гарантируя их аутентичность

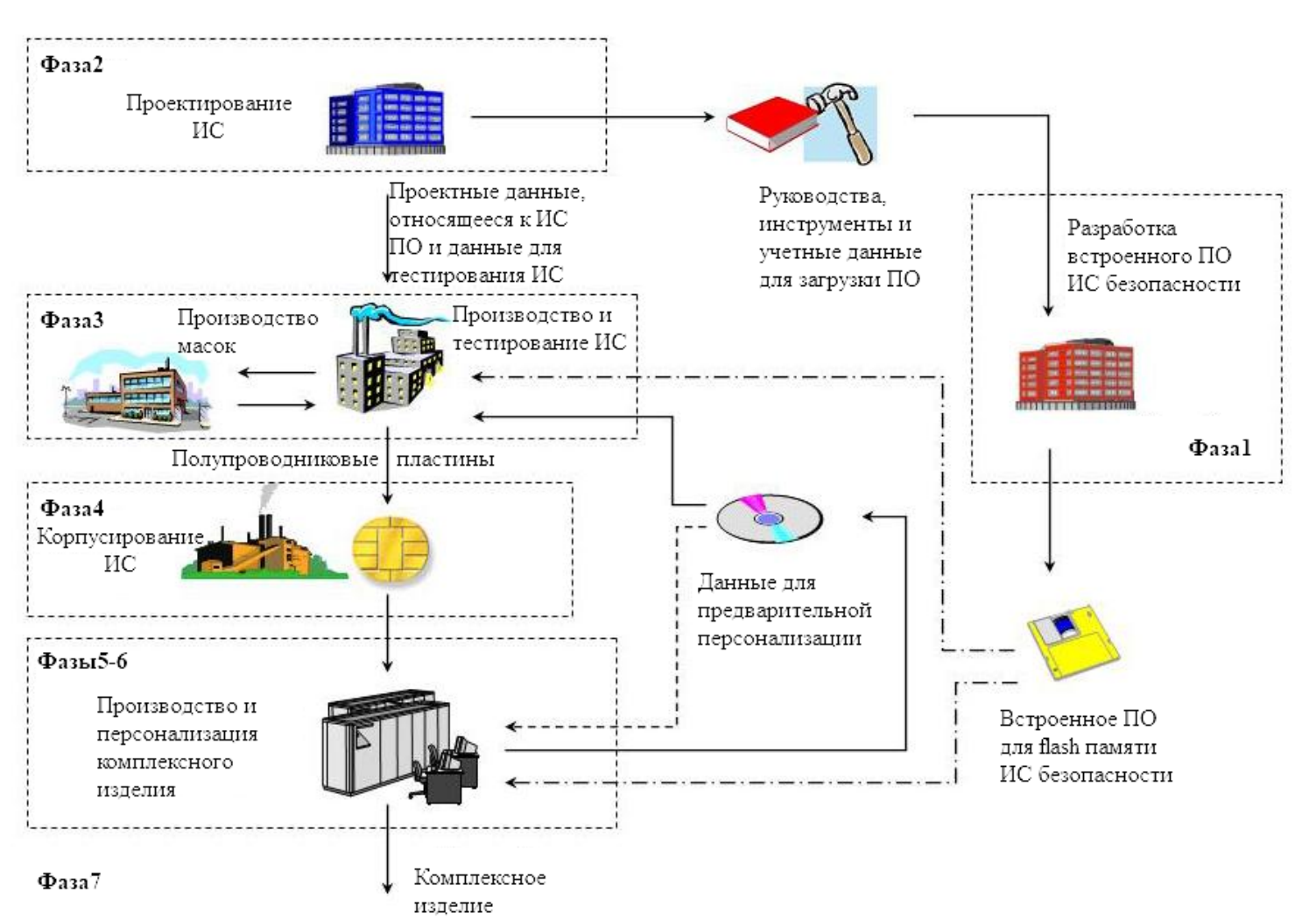
Защищенный микроконтроллер для БПЛА

Упрощенная блок схема доверенного микроконтроллера (СнК) для БПЛА
с функцией "свой-чужой" и защищенным беспроводным каналом обмена данными



Жизненный цикл корня доверия

Цикл проектирования и производства элемента безопасности корня доверия



В системе может быть несколько корней доверия, размещенных на разных аппаратных платформах, и предоставляющих различные службы. Часть из этих служб основанных, на криптографической обработке, и являющихся службами безопасности часто выполняют обособленно, на отдельном кристалле, подключенном к основной системе через коммуникационный интерфейс или в виде изолированного блока внутри кристалла процессора общего назначения.

Такой физически защищенный кристалл часто называют элементом безопасности (SE) или ИС безопасности

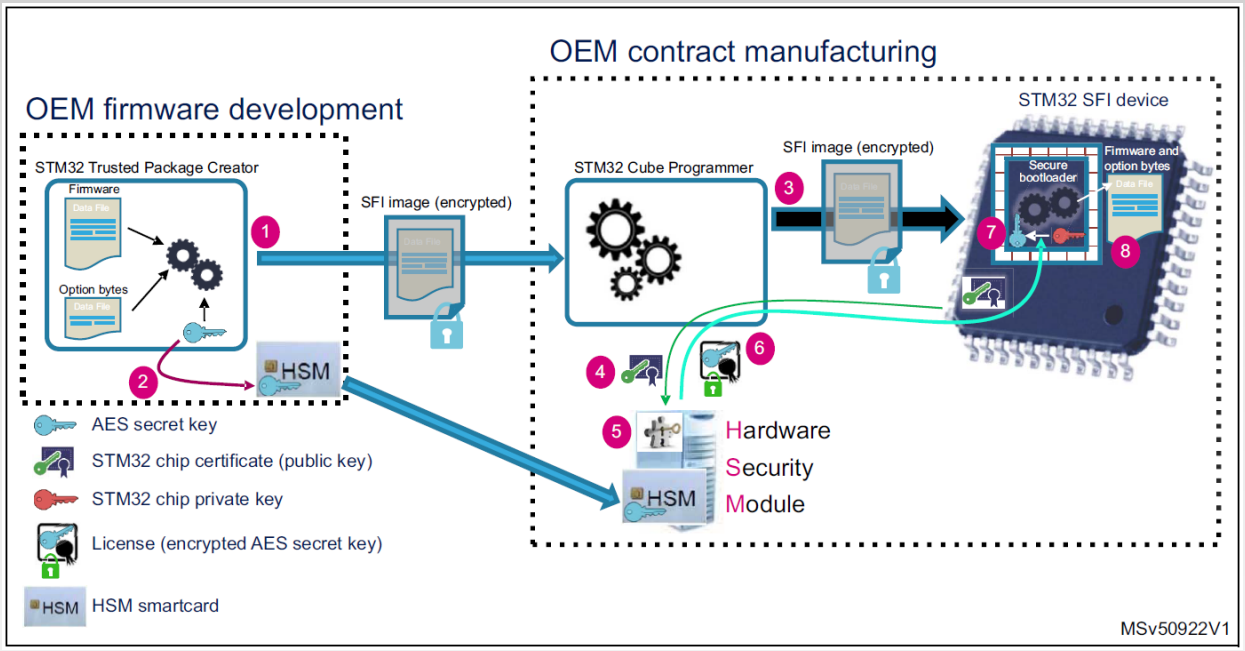
Жизненный цикл элемента безопасности корня доверия

Этап 1	Разработка встроенного ПО ИС безопасности	**Разработчик встроенного ПО для ИС безопасности** отвечает за: • разработку ПО для ИС безопасности; • спецификацию требований к предварительной персонализации ИС, хотя фактические данные для предварительной персонализации ИС появляются на Этапе 6 (или на Этапе 4 или 5).
Этап 2	Проектирование ИС безопасности	**Проектировщик ИС безопасности**: • проектирует ИС, • разрабатывает специализированное ПО для ИС, • предоставляет информацию, ПО и инструменты разработчику встроенного ПО для ИС безопасности и • получает ПО обеспечение для ИС безопасности от разработчика посредством надежных процедур доставки и проверки. На основе проектирования ИС, разработки специализированного ПО для ИС и встроенного ПО для защиты ИС проектировщик ИС: • создает базу данных ИС безопасности, необходимую для изготовления фотошаблонов ИС.
Этап 3	Производство и тестирование ИС безопасности	**Производитель ИС безопасности** несет ответственность за: • производство микросхемы на трех основных этапах: ○ изготовление микросхемы, ○ тестирование микросхемы, ○ предварительная персонализация микросхемы. **Производитель масок для ИС безопасности**: • создает фотошаблоны для изготовления микросхемы на основе информации из базы данных ИС безопасности.

Жизненный цикл элемента безопасности корня доверия

Этап 4	Корпусирование ИС	**Производитель корпусов ИС отвечает за:** • корпусирование и тестирование ИС.
Этап 5	Процесс завершения производства ИС безопасности	**Производитель композитного продукта несет ответственность за:** • процесс завершения производства и выходного тестирования ИС безопасности.
Этап 6	Персонализация ИС безопасности	**Специалист по персонализации отвечает за:** • персонализацию микросхемы безопасности и заключительные тесты.
Этап 7	Вывод из эксплуатации ИС безопасности	**Поставщик ИС безопасности несет ответственность за:** • доставку продукта ИС безопасности потребителю ИС безопасности и процесс вывода ИС безопасности из эксплуатации.

Обзор процесса доверенной инсталляции прошивки (SFI)

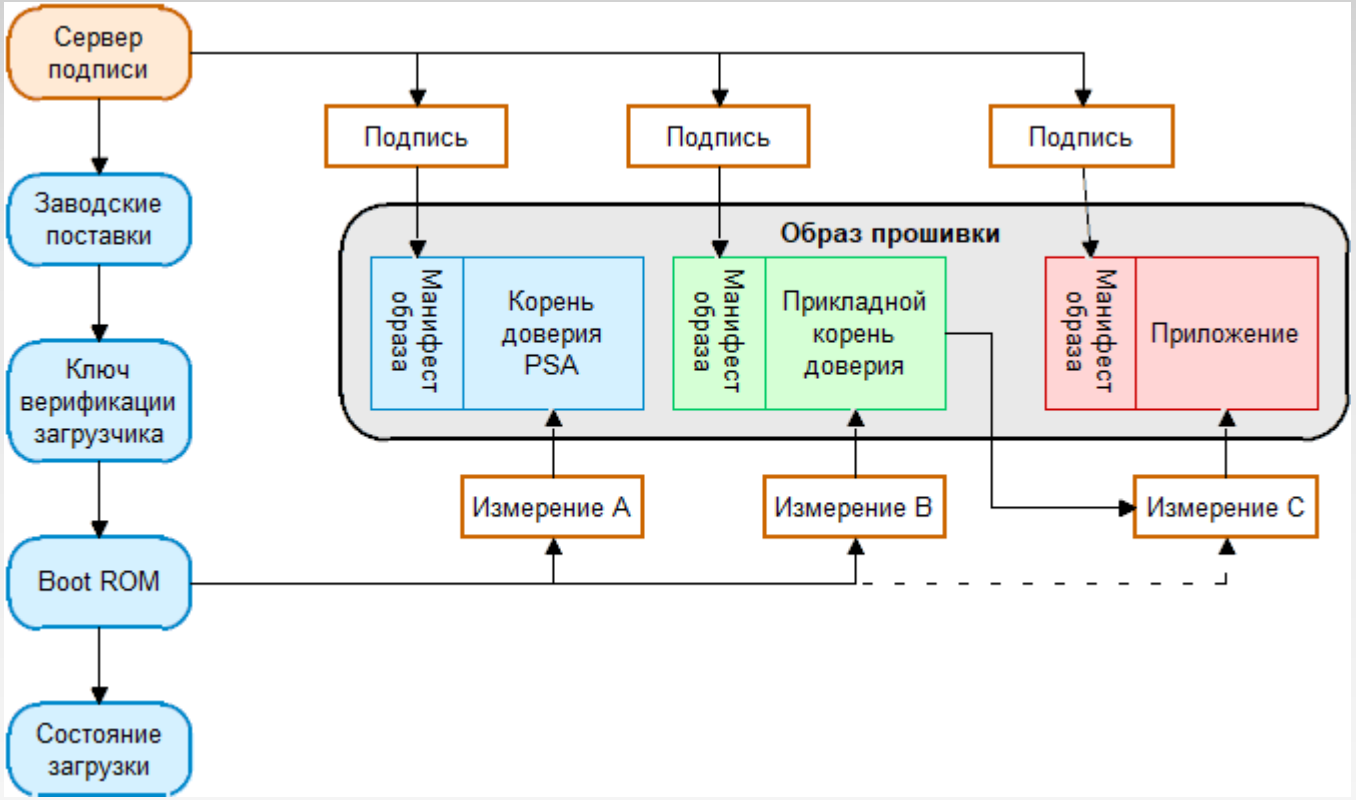


1. Получение (зашифрованного) образа SFI от Trusted Package Creator.
2. Генерация в HSM секретного мастер-ключа для экземпляра устройства.
3. Запуск процесса SFI.
4. Загрузка сертификата устройства.
5. Аутентификация устройства.
6. Предоставление лицензии.
7. Загрузка секретного мастер-ключа.
8. Программирование прошивки (Firmware) и байтов настройки (option bytes.

Доверенный загрузчик является стандартным загрузчиком с дополнительным функционалом безопасности. Если микроконтроллер сбрасывается в процессе загрузки секретного мастер-ключа, то перед повторным запуском SFI стираются все конфиденциальные данные.
В процессе SFI, доверенный загрузчик не позволяет никакому другому коду иметь доступ к пользовательской Flash памяти или ОЗУ.

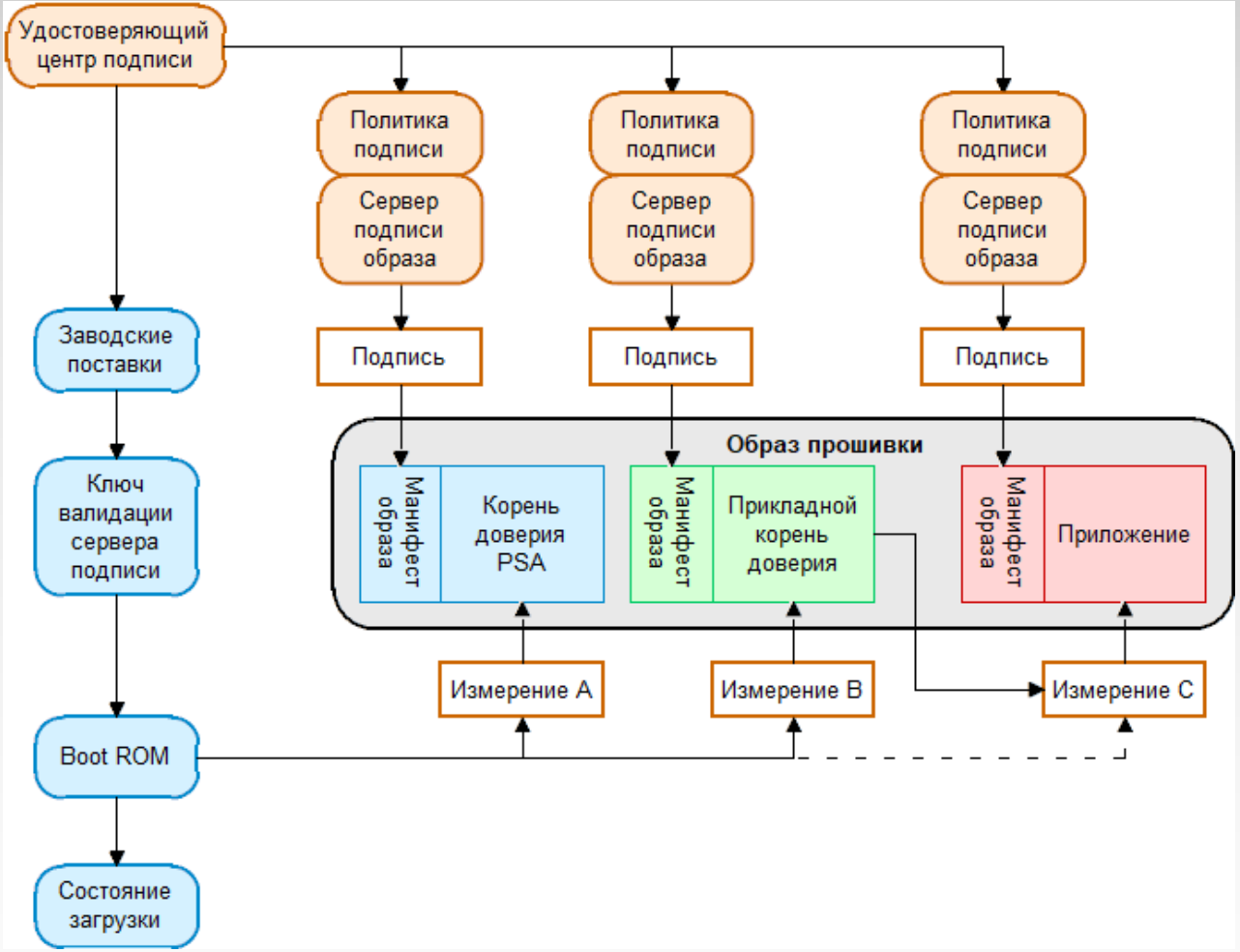
Примеры использования

Формирование и проверка подписи кода с одним сервером подписи



Сервер подписи формирует подпись для образов обновляемого корня доверия, прикладного корня доверия, ОС и пользовательских приложений.
Сертификат открытого ключа (или его хеш) записывается в область ПЗУ, доступную начальному загрузчику (Boot ROM).
Начальный загрузчик верифицирует образ необновляемого корня доверия и, возможно, прикладного корня доверия.
Прикладной корень доверия, как правило, уже имеет доступ к коммуникационным интерфейсам и может инициализировать дальнейшую верификацию загружаемых образов в духе стандартной PKI.

Формирование и проверка подписи кода с УЦ и несколькими серверами подписи



Удостоверяющий центр (УЦ) выпускает сертификаты ключей подписи и сертификаты ключей проверки подписи и передает сертификаты ключей подписи серверам подписи, которые могут принадлежать различным производителям ПО.
Серверы подписи формируют подписи для образов обновляемого корня доверия, прикладного корня доверия, ОС и пользовательских приложений.
Сертификат открытого ключа УЦ (или его хеш) записывается в область ПЗУ, доступную начальному загрузчику (Boot ROM).
Начальный загрузчик верифицирует образ сертификаты каждого из серверов подписи и на основание этих сертификатов проверяет подписи необновляемого корня доверия и, возможно, прикладного корня доверия.
Прикладной корень доверия, как правило, уже имеет доступ к коммуникационным интерфейсам и может инициализировать дальнейшую верификацию загружаемых образов в духе стандартной PKI.

Требования Российских регуляторов

Несмотря на новизну темы можно отметить ряд нормативных документов, имеющих прямое отношение к корням доверия:

1. Р 1323565.1.012-2017. Информационная технология КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации.
2. Приказ ФСТЭК России №76 от 02.06.2020 г. Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий.
3. Руководящий документ ФСТЭК России от 30 марта 1992 г. Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации.
4. ИТ.СДЗ.ПР4.ПЗ. Профиль защиты средства доверенной загрузки уровня платы расширения 4 класса защиты.
5. ГОСТ Р ИСО_МЭК 12207-2010 Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств.
6. ГОСТ Р 51904-2002 Программное обеспечение встроенных систем. Общие требования к разработке и документированию
7. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.
8. ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ. Часть 3. Компоненты доверия к безопасности.

Открытые вопросы

Имеется ряд вопросов, требующих дальнейшей проработки:

1. Корень доверия привязывается к аппаратной платформе. Для непрерывности цепочки доверия необходимо, чтобы сама платформа также была доверенной.
   Что такое «доверенная платформа»? В смысле ТК-362/ТК-167?
   Какие требования должны предъявляться к платформе, чтобы она могла считаться доверенной?
2. При использовании корня доверия в виде отдельного кристалла:
   Каким образом должна осуществляться привязка корня доверия к аппаратной платформе? (Взаимная аутентификация? Протокол? Способ хранения аутентификационных данных на аппаратной платформе? Привязка к отдельному ядру многоядерного кристалла?)
3. ***На каком этапе жизненного цикла SE, кем и каким образом должна производиться загрузка в него базовых активов? Какого масштаба должен быть актив: Кристалл? Устройство? Партия? Вендор? Интегратор?***
   Где и каким образом должны храниться ответные данные для активов SE?
4. ***Какие активы должны храниться на SE, какое максимальное время их жизни и какова процедура смены активов, в случае необходимости?***

Список литературы

Литература

1. Андрей Самоделов. Создание защищенных систем на базе технологии ARM TrustZone. Части 1–4. Компоненты и технологии. №№5–8. 2017.
2. Андрей Самоделов. Технология ARM TrustZone для архитектуры ARMv8-M. Компоненты и технологии. №9. 2019.
3. Андрей Самоделов. Расширения безопасности ARMv8-M Security Extensions. Требования к средствам разработки. Компоненты и технологии. №№10–11. 2019.
4. Андрей Самоделов. Аппаратная поддержка доверенной среды исполнения в микроконтроллерах и микропроцессорах с архитектурой ARMv.8A и ARMv.8M. Доклад на международной конференции RusCrypto-2020.
5. Андрей Самоделов. Повышение защищенности доверенного хранилища GPD Trusted Storage на основе технологии ARM TrustZone и особенностей архитектуры СнК с ядрами ARMv.8. Доклад на международной конференции РусКрипто-2021.
6. Андрей Самоделов. Корни доверия. Части 1-3. Электронные компоненты. №№8-10. 2025.
7. GP_REQ_025. GlobalPlatform Technology. Root of Trust Definitions and Requirements. Version 1.1. Public Release. June 2018.
8. NIST SP 800-164 Guidelines on Hardware-Rooted Security in Mobile Devices (Draft). National Institute of Standards and Technology. October 2012.
9. ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components
10. GPT_SPE_146. GlobalPlatform Technology. MCU Root of Trust Protection Profile. Version 1.0. Public Release. December 2022.
11. GPT_SPE_148. SESIP Profile for Secure External Memories v1.1. Sep 2024.
12. GPT_SPE_150. SESIP Profile for Secure MCUs and MPUs v1.1. May 2025.
13. GPT_SPE_151. SESIP Profile for DTSec Connected Diabetes Device Platforms v1.0. Jan 2024.
14. GPC_SPE_174. Secure Element Protection Profile and Extensions v2.0 Jul 2025
15. GP_FST_070 . Security Evaluation Standard for IoT Platforms (SESIP) Methodology v1.2. Jul 2023.
16. Smartcard IC Platform Protection Profile. Version 1.0. July 2001.
17. Security IC Platform Protection Profile with Augmentation Packages. Version 1.0. 13.01.2014

Спасибо за внимание!

Андрей Самоделов

Независимый эксперт

assamodelov@yandex.ru