СОВРЕМЕННЫЕ ПОДХОДЫ К ДОВЕРЕННОЙ ЗАГРУЗКЕ ОС НА ПРИМЕРЕ АВРОРА СДЗ ДЛЯ ПРОЦЕССОРОВ BAIKAL-M

Эльвира Хабирова, Константин Карасев

Открытая мобильная платформа

Основная деятельность

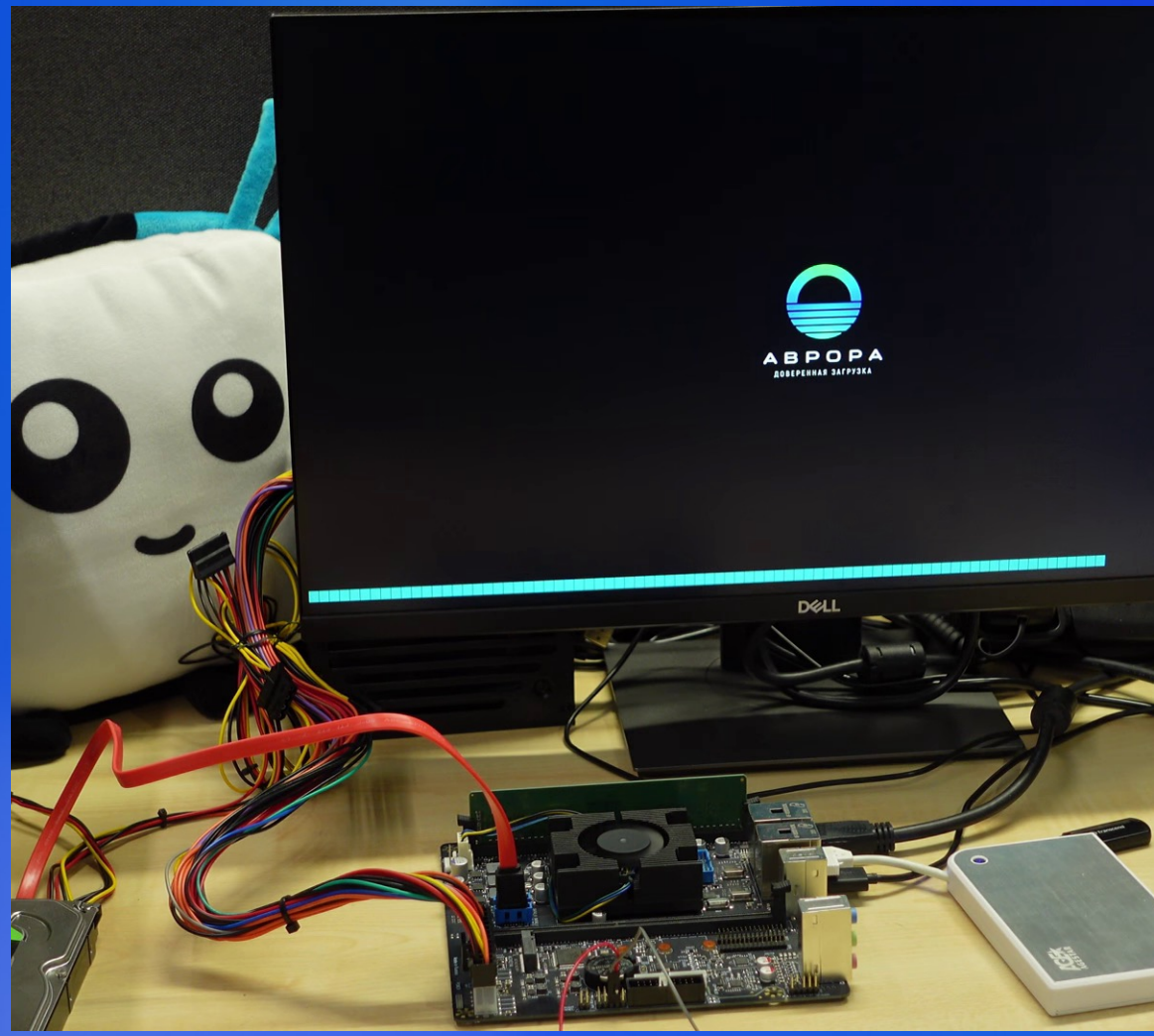
1. Разработка мобильной операционной системы
2. Разработка платформы управления Аврора Центр
3. Поддержка сообщества разработчиков ПО
4. Портирование ОС Аврора на новые аппаратные платформы

Общая информация:

- 200+ сотрудников
- Офисы в Москве, Иннополисе и Санкт-Петербурге
- ДЗО ПАО «РОСТЕЛЕКОМ»
- Активное участие в opensource проектах (glibc, linux kernel, ofono и др.)
- Образовательные программы на online-площадках и в ведущих ВУЗах страны

Аврора СДЗ (1/2)

- Программно-аппаратное средство доверенной загрузки
- Первое средство доверенной загрузки с корнем доверия **в самом кристалле** для отечественного СнК
- Поддержка загрузки различных ОС (Аврора / ALT Linux / Astra Linux / РЕД ОС и др.)



Загрузка Аврора СДЗ на плате Edelweiss

Аврора СДЗ (2/2)

- Доверенная загрузка с момента подачи питания на SoC до старта ядра ОС
- Инструменты подписи загрузчиков и ядра ОС для интеграторов и эксплуатантов
- Только отечественная ГОСТ-криптография
- Требования отечественных регуляторов, заложенные в архитектуру
- Внесено в Реестр отечественного ПО

АВРОРА

СРЕДСТВО ДОВЕРЕННОЙ ЗАГРУЗКИ

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВЫПИСКА

Из единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации

Порядковый номер реестровой записи: 13309

Дата формирования реестровой записи: 15.04.2022

Номер решения о включении сведений о программном обеспечении в соответствующий реестр: б/н

Существующие подходы к доверенной загрузке

- ПМДЗ
- АМДЗ
- АПМДЗ

Программные модули доверенной загрузки (ПМДЗ)

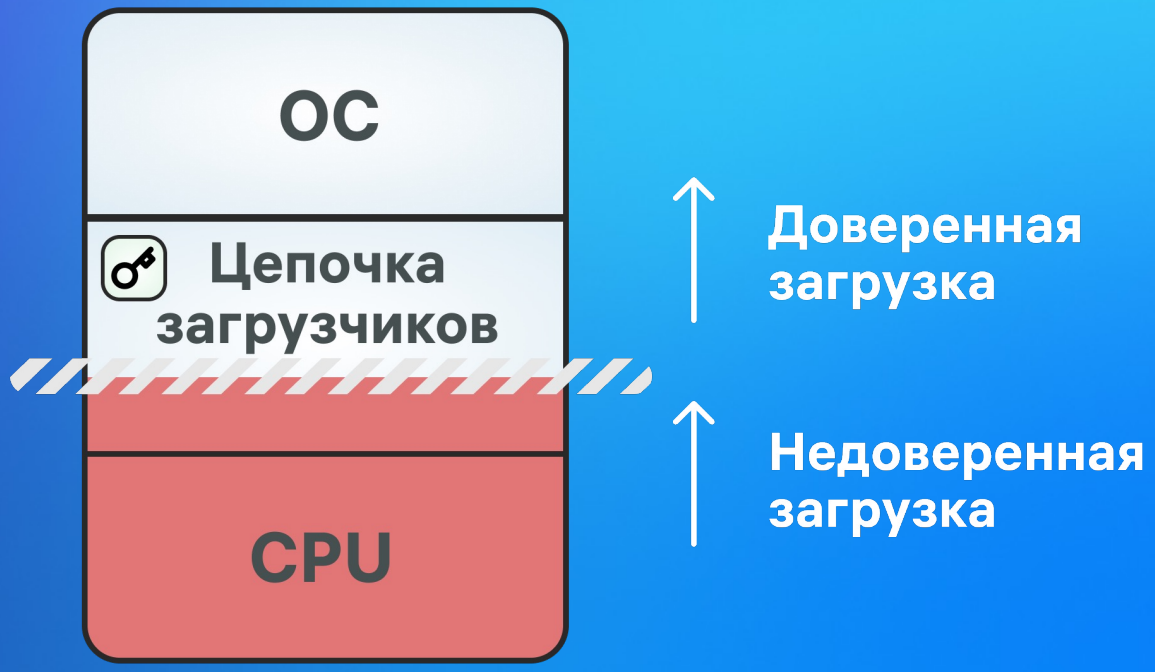
Замена базовой системы ввода вывода на модуль собственной разработки.

Плюсы:

- Невысокая стоимость по причине простоты и отсутствия аппаратной составляющей

Минусы:

- Корень доверия находится **не** в корне цепочки загрузки
- Может быть удален



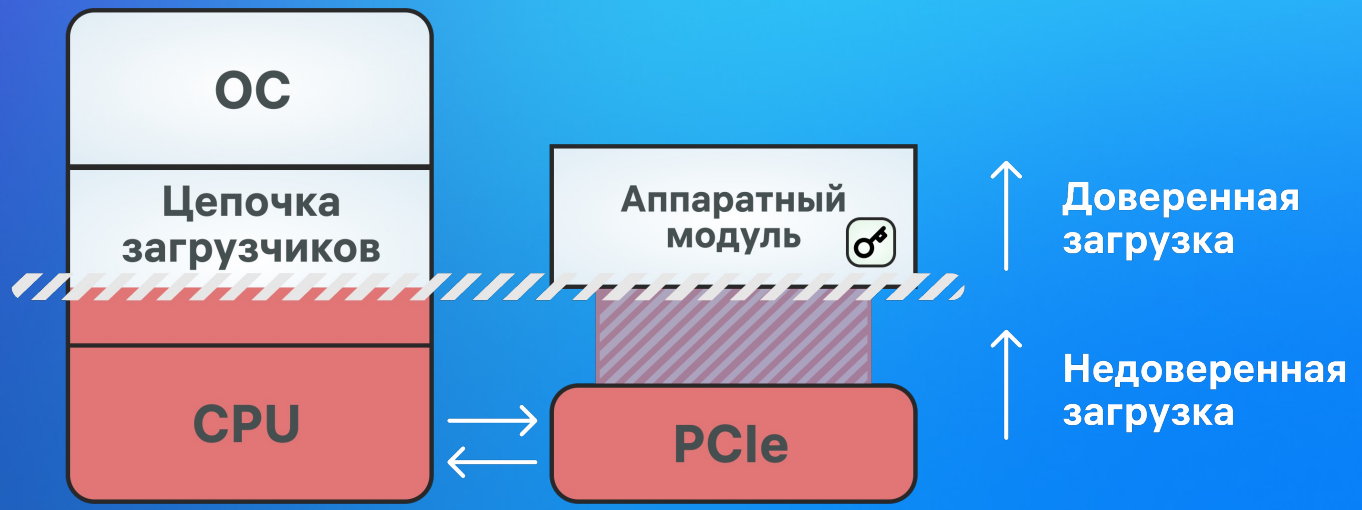
Аппаратные модули доверенной загрузки (АМДЗ)

Плюсы:

- Изоляция за счет нахождения на отчужденном аппаратном модуле

Минусы:

- Корень доверия находится **не** в корне цепочки загрузки
- Отчуждаем
- Размеры
- Стоимость
- Требуется свободный разъем материнской платы



Аппаратно-программные модули доверенной загрузки (АПМДЗ) с корнем доверия в кристалле

Плюсы:

- Корень доверия находится **в корне** цепочки загрузки
- Не требуется внешний аппаратный модуль
- Де-факто стандарт безопасности современных SoC (NXP, Qualcomm, Mediatek, ...)
- Неотчуждаемы

Минусы:

- Требуется поддержка со стороны производителя SoC

Байкал Электроникс — первый отечественный производитель SoC, который аппаратно заложил этот подход

Международные и отечественные стандарты

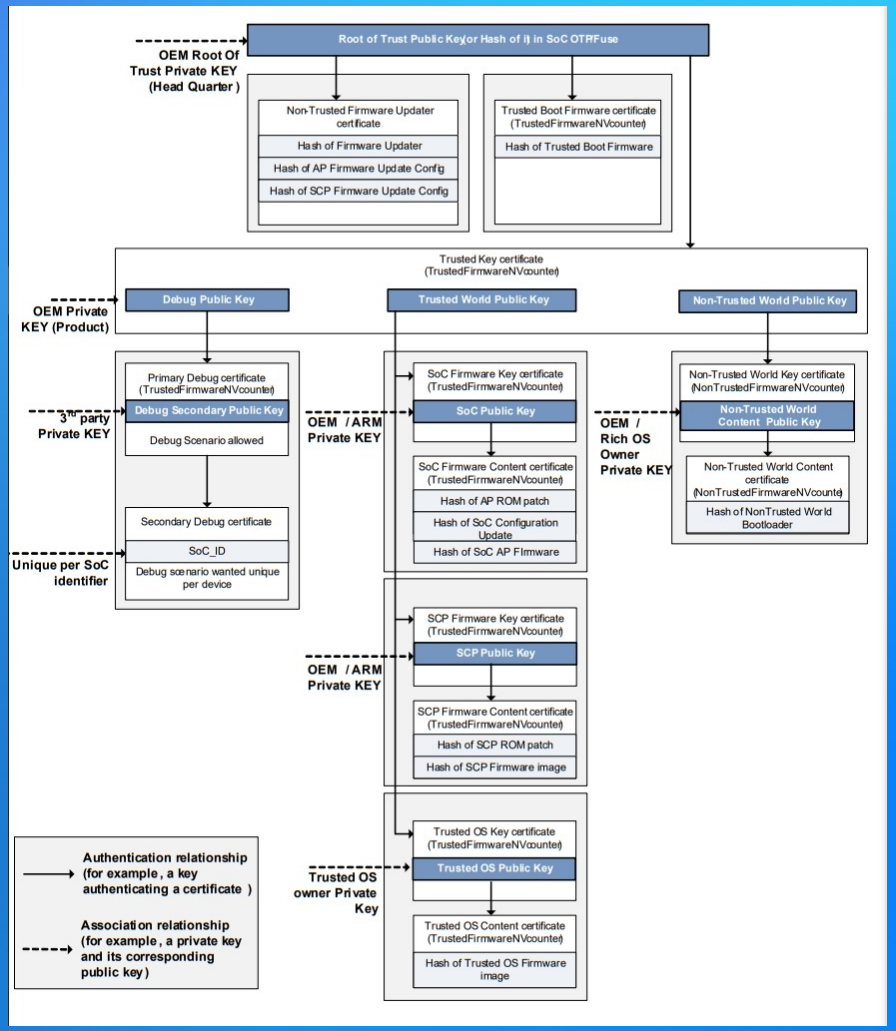
- ARM TBBR
- UEFI Secure Boot
- Профили защиты ФСТЭК
- ARM EBBR
- OpenTitan Security Model
- OCP Hardware Secure Boot
- OpenPower Secure Boot

Arm Trusted Board Boot (TBBR)

ARM DEN0006D

- Подробная спецификация, затрагивающая поведение Arm-платформы от подачи питания до перехода в UEFI/Linux
- Описывает подробности процедуры инициализации платформы и контроля целостности
- Предусматривает защиту от отката версии, обновления образов и отзыв ключей
- Основано на цепочке сертификатов
- Сложная ключевая схема
- Требуется криптография, соответствующая NSA suite B 128-bit

https://developer.arm.com/documentation/den0006/latest



Ключевая схема TBBR

UEFI Secure Boot

UEFI Specification 2.4+

- Описывает поведение в рамках UEFI, не привязан к платформе
- Ролевая модель не подразумевает разделения на пользователя и администратора
- Отсутствует защита от отката версии
- Отсутствует защита загрузочных записей UEFI от ОС

https://uefi.org/specifications

Профили защиты ФСТЭК

- Профиль защиты средства доверенной загрузки уровня загрузочной записи 6 класса защиты
- Профиль защиты средства доверенной загрузки уровня загрузочной записи 5 класса защиты
- Профиль защиты средства доверенной загрузки уровня платы расширения 4 класса защиты
- Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода 4 класса защиты

ФСТЭК ИТ.СДЗ.УБ4.ПЗ

Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода четвертого класса защиты

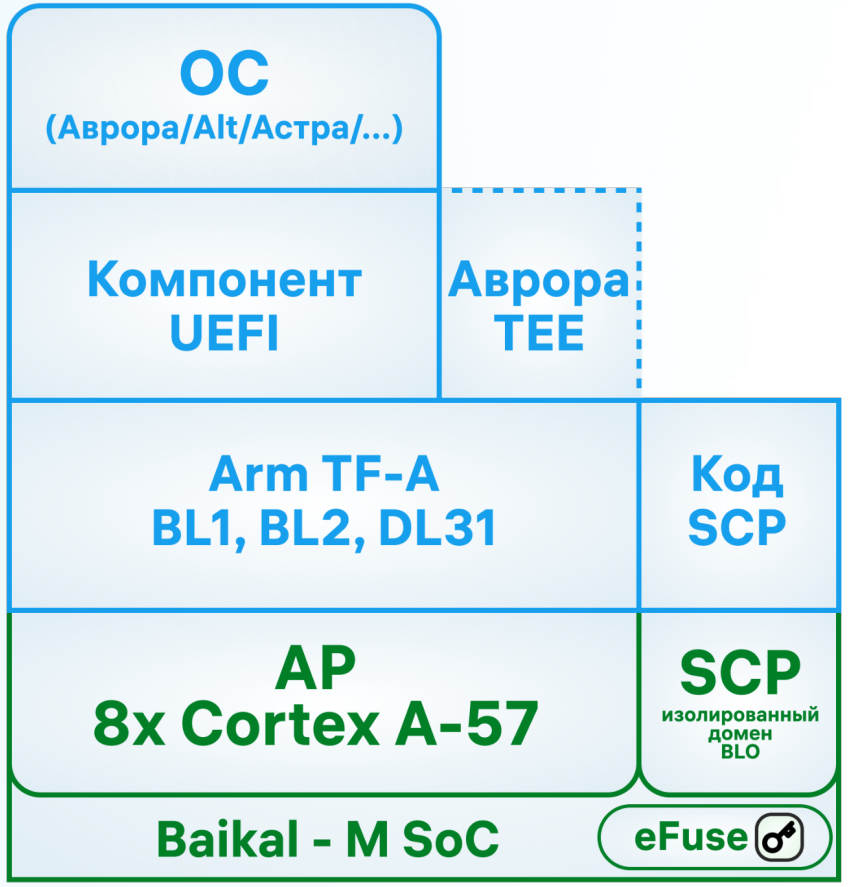
- Не привязан к конкретной платформе
- Предполагает встраивание в BIOS (UEFI)
- Требуется ролевая модель
- Требуется самотестирование функций СДЗ
- Требуется журналирование событий безопасности

Особенности Аврора СДЗ

- Корень доверия на кристалле
- Ключевая схема
- Схема загрузки
- Обновления
- Аврора TEE
- Требования регуляторов

Корень доверия на кристалле

- Доверенная загрузка начинается с неизменяемого кода, исполняющегося сразу после подачи питания
- Публичная часть ключей хранится в однократно-программируемой памяти (eFuse)
- В совокупности это делает включение доверенной загрузки необратимым
- eFuse также позволяет хранить значения для защиты от отката версии

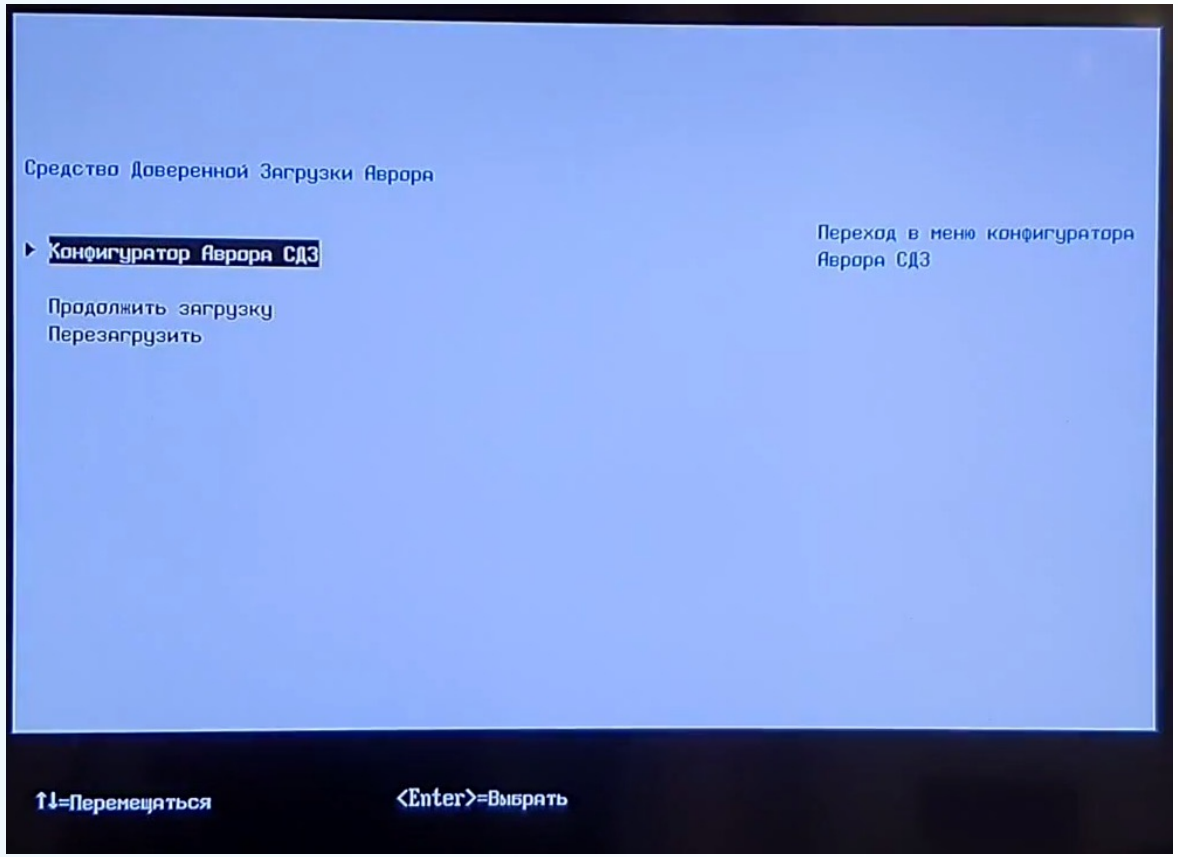


Технология eFuse используется в мире для хранения ключей более 10 лет.

Поддержка отечественных производителей SoC позволяет доверять таким решениям.

Расширение компонента UEFI

- UEFI не является корнем доверия, а лишь звеном в цепочке доверенной загрузки
- Через интерфейс UEFI доступны:
  - конфигурация СДЗ
  - операции над пользователями
  - операции над журналом событий безопасности
- Только через интерфейс администратора UEFI можно добавлять загрузочные записи



Ключевая схема

Иерархия ключей СДЗ состоит из следующих ключей:

- SCP — ключ верификации первичного загрузчика, прошивается в eFuse.
- Vendor — ключи верификации цепочки загрузчиков. Первичное внесение заверяется SCP key, возможна замена. Прошиваются в eFuse.
- Image — принадлежит вендору ОС. Используется для верификации образа ОС, публичная часть удостоверяется Vendor Key. Представлен в виде сертификата в образе ОС.

Используются **только алгоритмы ГОСТ** Р 34.10-2012 и ГОСТ Р 34.11-2012.

Ключевая схема

Вендор ОС:

- формирует ключ Image;
- подписывает образ ОС;
- передаёт вместе с публичным ключом Заказчику.

Заказчик:

- получает комплект поставки СДЗ и образ ОС;
- формирует ключи SCP и Vendor;
- подписывает образы СДЗ и ОС;
- передаёт на производство.

На производстве:

- производится партия устройств;
- производится внесение ключевой информации в СнК;
- производится прошивка образов загрузчиков и ОС.

Ключевая схема даёт максимальную гибкость процесса внесения ключей.
Ключи принадлежат заказчику и/или эксплуатанту.

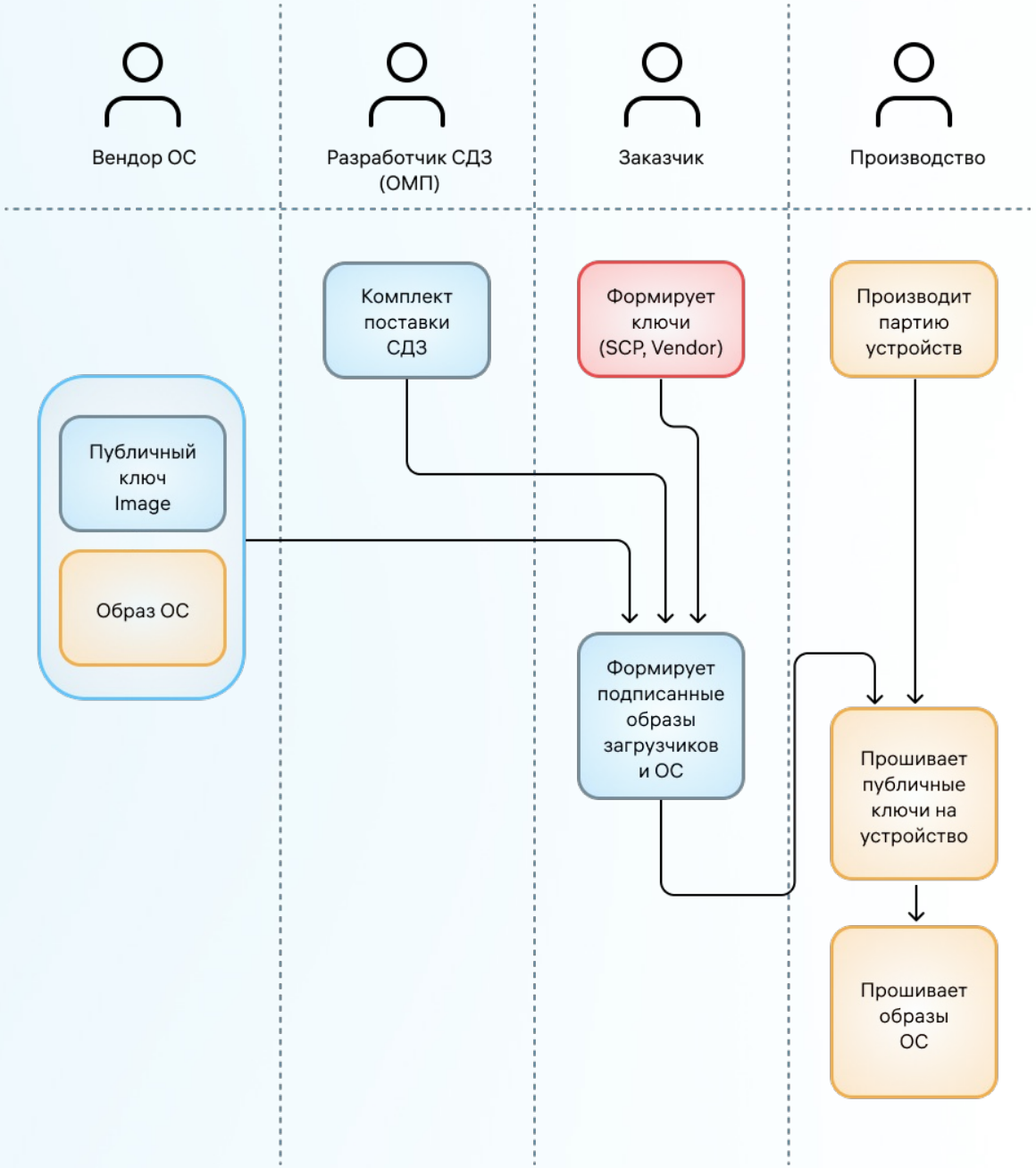


Схема загрузки

- Каждый компонент находится в контейнере и снабжён соответствующей подписью
- В ходе доверенной загрузки для каждого последующего контейнера проверяется его подпись

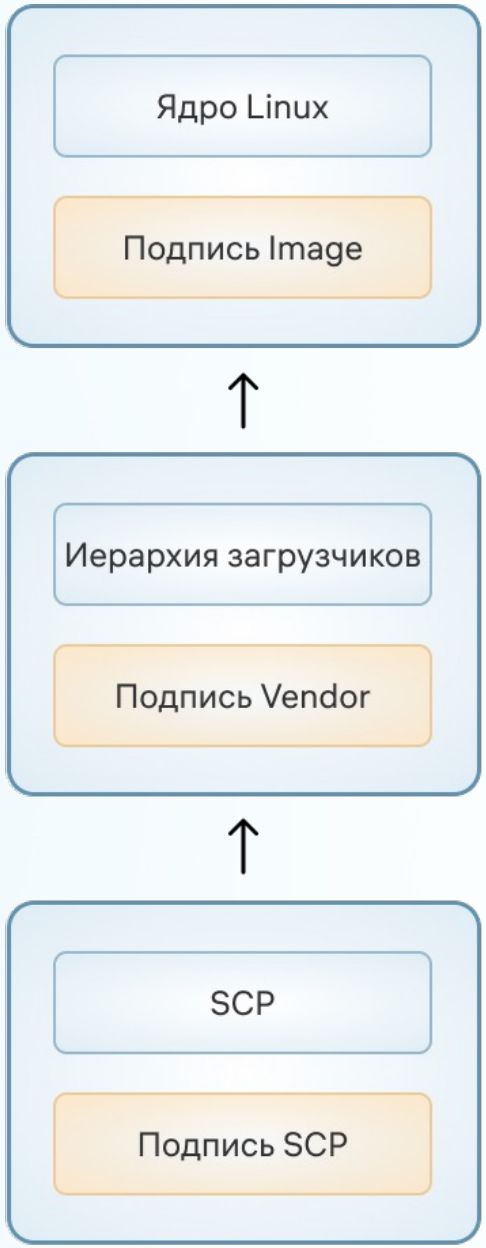
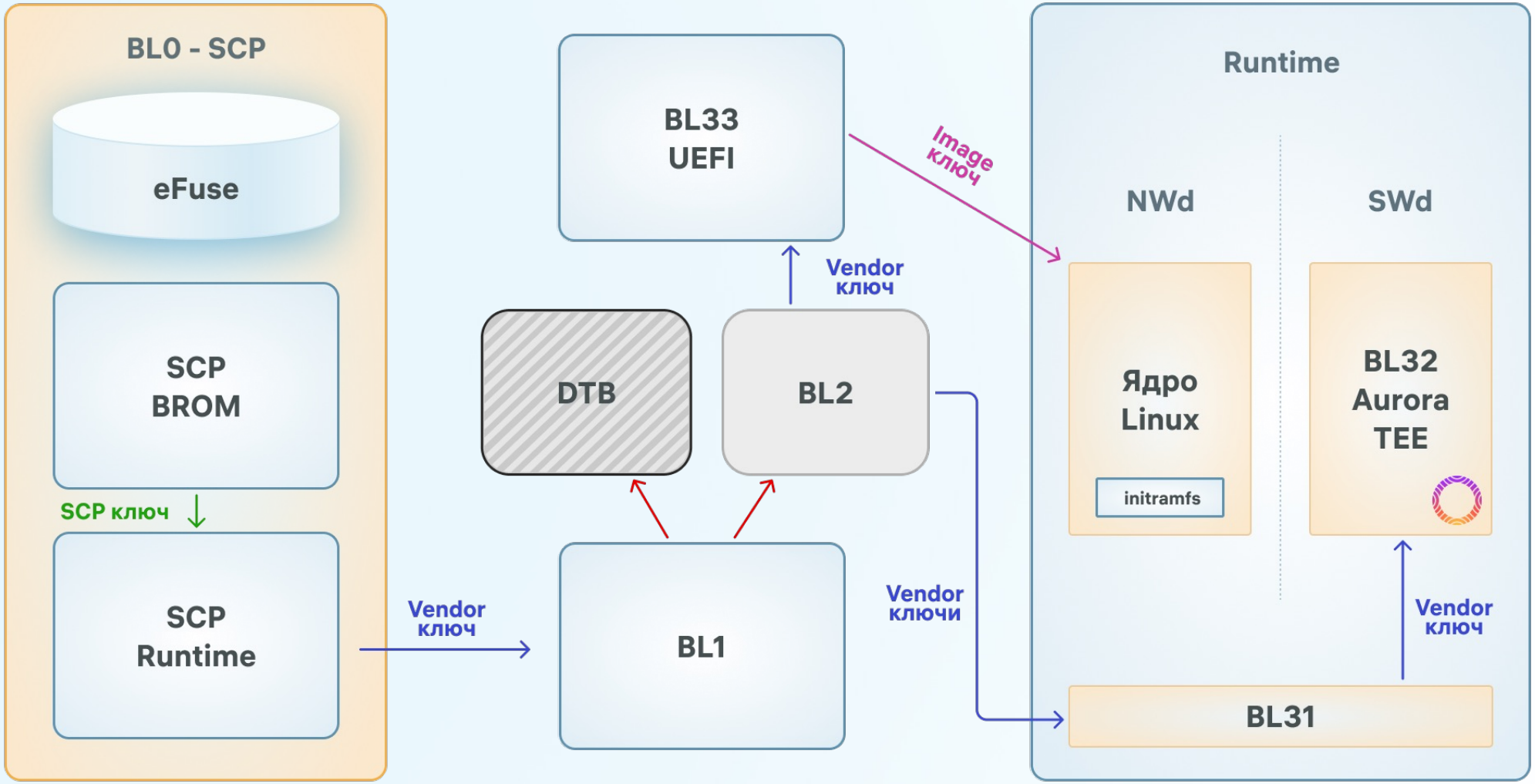
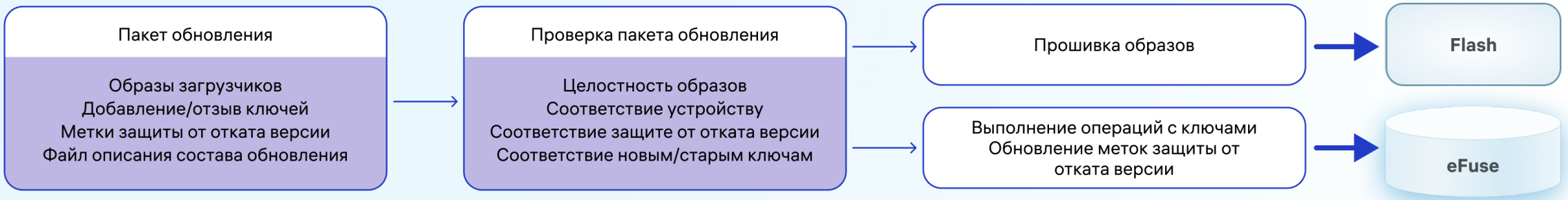


Схема загрузки



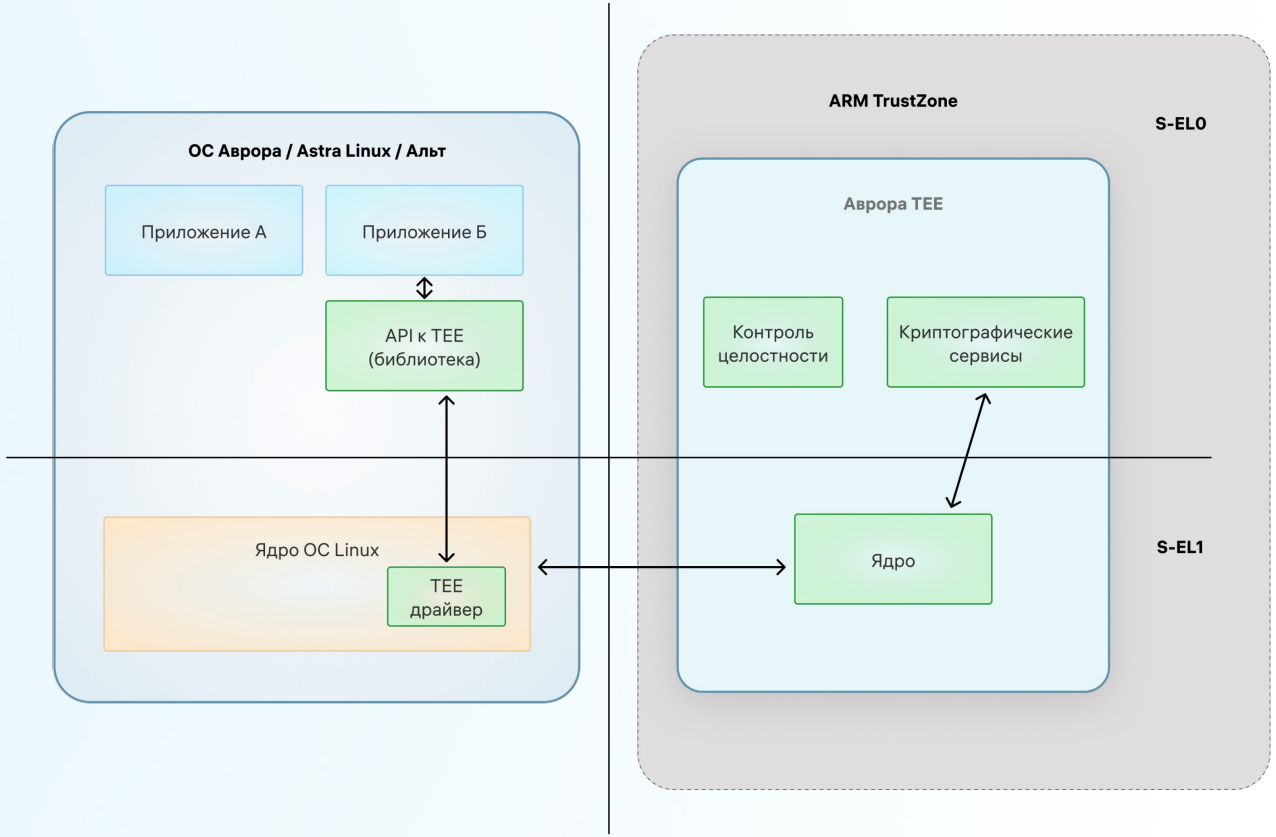
Система обновлений и управления ключами

- Позволяет обновлять полный набор образов загрузчиков Авроры СДЗ
- Интерфейс находится в оболочке UEFI
- Содержит множество проверок от случайных ошибок оператора
- Также позволяет одновременно добавлять и инвалидировать ключи, управлять метками защиты от отката версий



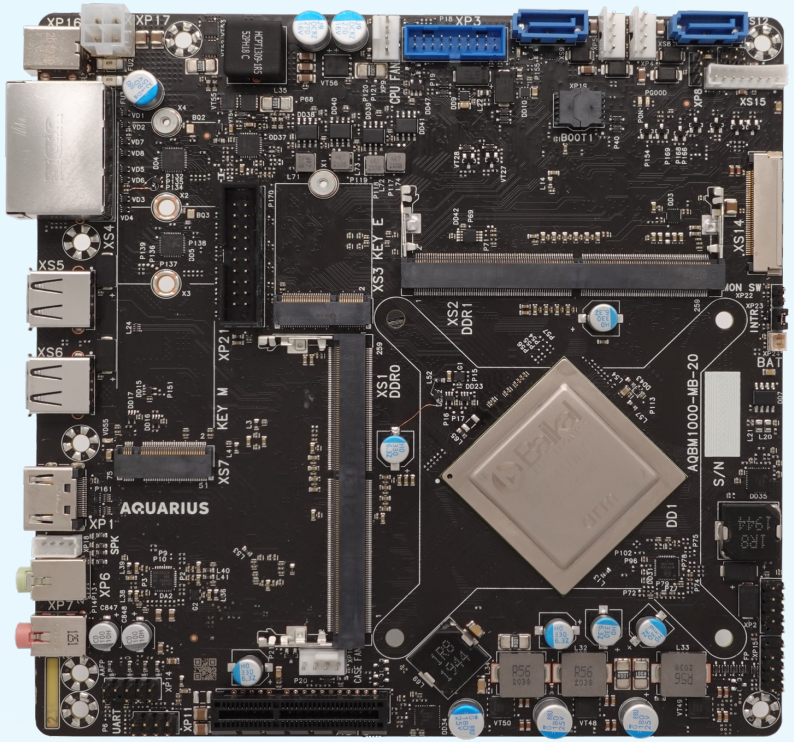
Интеграция с Аврора TEE

- Доверенная среда исполнения
- Исполняется в аппаратно-изолированной среде, режимы исполнения — S-EL0 / S-EL1
- Предоставляет криптографический сервис с хранилищем ключей (keystore) – аппаратно изолирован от основной ОС
- Осуществляет динамический контроль целостности исполняемого кода и данных основной ОС из Arm Trustzone (ATIC)
- Используется в Aquarius NS220 с 4 квартала 2021
- Впервые появляется на не-мобильном устройстве

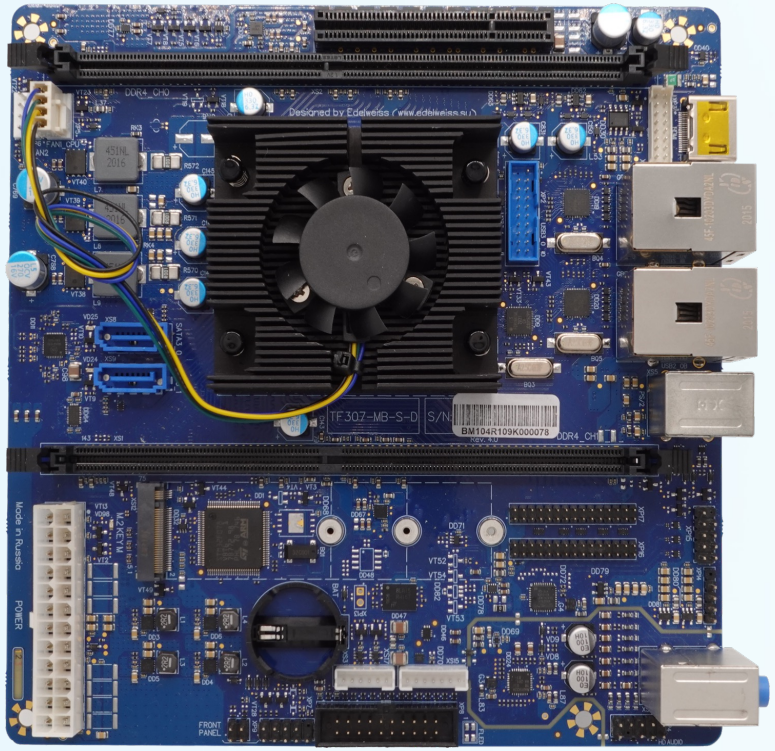


OS Day 2021. Константин Карасев, Открытая мобильная платформа. «Аврора TEE – доверенная среда исполнения для повышения защищенности операционных систем на базе ядра Linux»

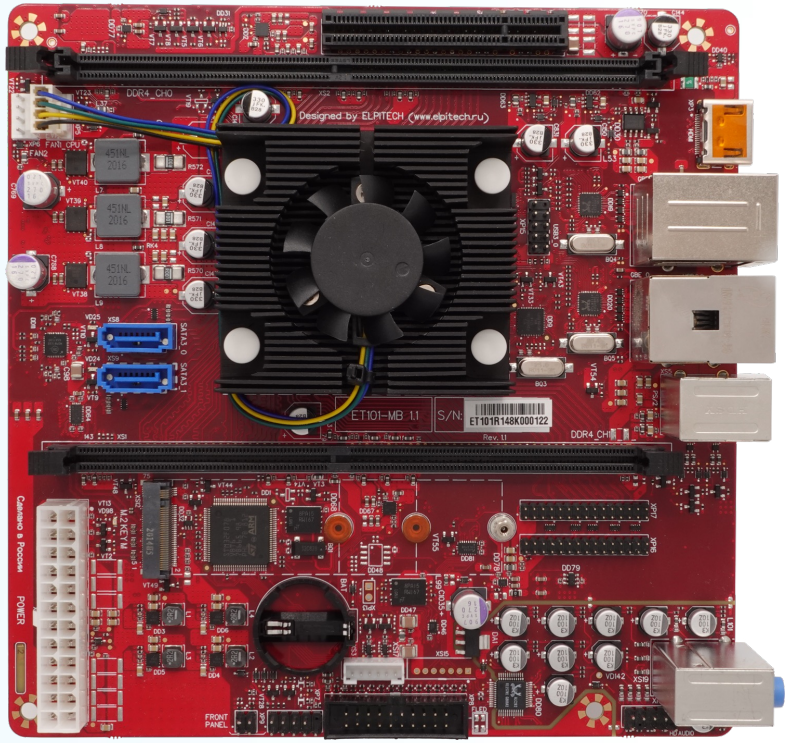
Поддерживаемые платы



Aquarius AQBM1000-MB-20



Edelweiss TF307-MB-S-C



Elpitech ET101-MB

Требования профиля безопасности

В архитектуру Аврора СДЗ заложено соответствие требованиям регулятора.

- Ролевая модель
- Самодиагностика
- Конфигурируемая идентификация и аутентификация
- Журналирование
- Метки времени

Вопросы?

omp.ru

auroraos.ru

info@omp.ru