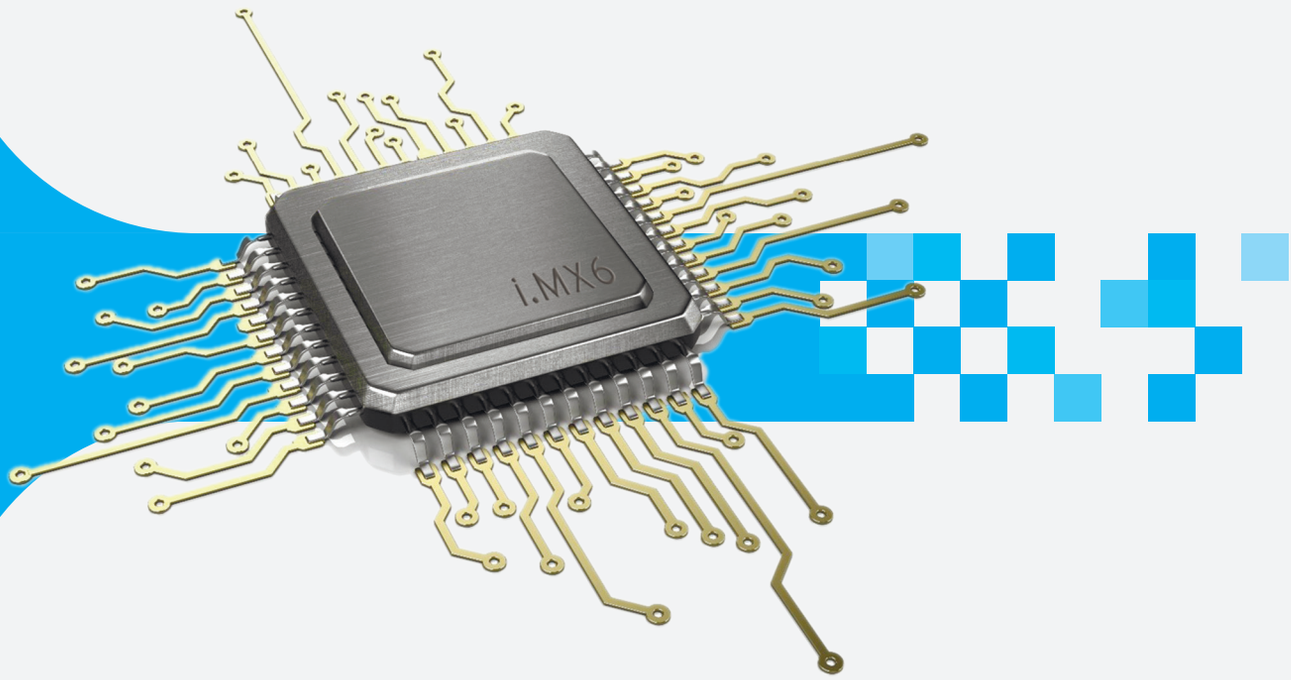
Доверенная платформа на ARM-процессорах i.MX6 с собственной TrustZone



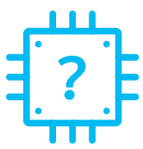
Trusted Security Module (TSM)

- Доверенная загрузка, ввод-вывод, визуализация
- Контроль ОС и исполняемых приложений
- Система дистанционного управления и мониторинга
- Сертификация (до сов. секретно)

Аладдин

Проблема доверия к импортной электронике

Мир электронных устройств, который нас окружает, условно можно разделить на два больших класса – это компьютеры и серверы, на которых мы работаем (на процессорах семейства x86 и др.), и множество носимой и встроенной электроники – гаджеты, бытовая, телекоммуникационная электроника, промышленная автоматика, автомобильная и др. встраиваемая электроника – всё это, как правило, построено на базе микропроцессоров архитектуры ARM.



Что особенного в современных ARM-процессорах?

1 Это "система на кристалле" (SoC – System on Chip) – т.е. в одном микроконтроллере, в одном корпусе содержатся и процессор, и память, и контроллеры внешних устройств для общения с внешним миром.

2 В процессорах ARM Cortex A (мультимедийная серия, использующаяся в смартфонах, планшетах, Smart-TV, принтерах, сканерах, платёжных, навигационных терминалах и пр.) и Cortex R (серия для промышленных контроллеров, АСУ ТП, встраиваемых и управляющих систем) появилась технология TrustZone (доверенная зона).

Что такое TrustZone?

Это аппаратное разделение (виртуализация) ARM-процессора на два изолированных друг от друга "мира" – Secure World и Normal World, позволяющее запущенным в них ОС и приложениям работать независимо друг от друга с использованием одного ядра процессора и набора периферии.

При загрузке процессора сначала загружается специализированная компактная **Secure OS**, находящаяся в Secure World и контролирующая все коммуникации процессора с внешним миром (контроллеры и периферию).

Она же формирует и профиль безопасности (доступные ресурсы, например, объём памяти, доступность внешней периферии и пр.) для "гостевой" (Guest/Rich OS), в которой будет работать "основная" ОС (iOS, Android, Sailfish, Linux, Windows и др.) в "нормальном" привычном для нас "мире" Normal World.

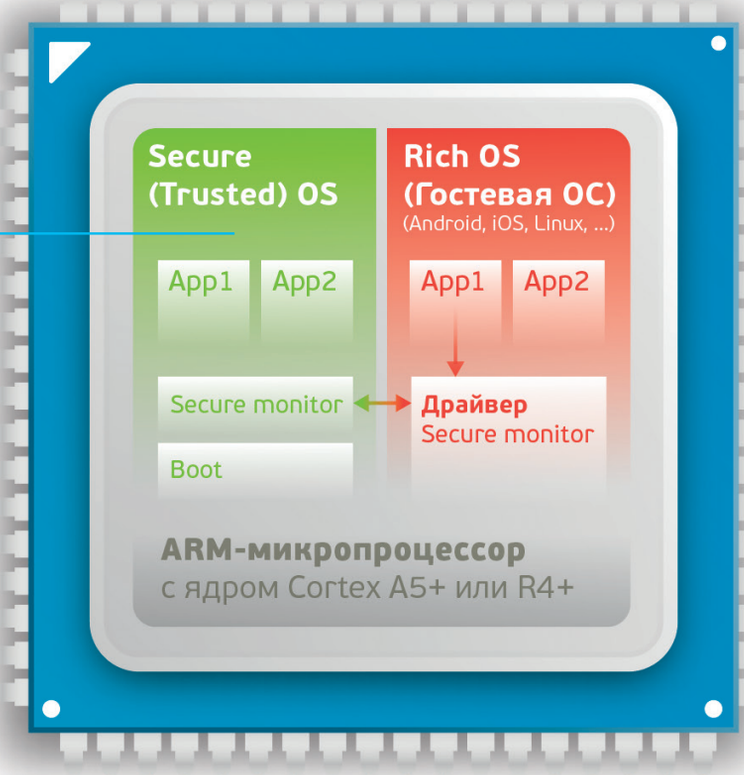
Несмотря на то, что эти два "мира" изолированы друг от друга, между ними есть **тесная связь** и возможность общения.

- Secure OS с загруженными в неё трастлетами (доверенные приложения) имеют неограниченные возможности и могут получить полный доступ ко всему – ко всей памяти, к ключам, к вводу-выводу и пр.
- Все ОС (включая сертифицированные), работающие в Normal World, в своём ядре имеют команды передачи управления на Secure OS. Делается это с помощью вызовов Secure Monitor Call (команды SMC#0 в ядре любой упомянутой ОС).

1 Загрузчик получает управление сразу после включения питания, стартует Secure OS

2 Secure OS загружает "гостевую" Rich OS

3 Secure OS может контролировать все приложения, и сама Rich OS узнать об этом не может



Управление обменом с периферией производится через TrustZone

В чём проблема?

1. Secure OS, работающая в TrustZone, имеет полный доступ ко всем ресурсам процессора, управляет всеми коммуникациями с внешним миром, загружается раньше "гостевой" ОС и полностью контролирует её работу.

2. Secure OS работает скрытно, так, что "гостевая" ОС "считает", что она работает на чистом "железе". На самом деле это не так – данные об объёме памяти, работе периферии она получает от Secure OS, команды и данные, пересылаемые периферийным устройствам, также проходят через Secure OS. *Кто мешает ей делать предобработку, например, менять GPS-координаты или сохранять копии документов в скрытой памяти?*

3. Secure OS и приложения из TrustZone могут скрытно и необнаруживаемо выполнять различные шпионские функции – включать микрофон, камеру, копировать вывод на экран, контролировать обмен данными, манипулировать информацией, красть криптографические ключи, отпечатки пальцев (с сенсора), ключи и пароли для доступа в государственные и корпоративные информационные системы и т.п.

4. Удалить вызовы Secure Monitor (команды SMC#0) из ядра "гостевых" ОС нельзя – они перестанут работать на этих процессорах, поскольку управлением режимами энергосбережения, загрузкой аппаратных ядер процессора, кэшем и пр. занимается именно Secure OS (как BIOS в системах на x86).

5. Удалить или заменить Secure OS в TrustZone практически невозможно (она "заперта" на секретном ключе), обнаружить – крайне сложно – только по косвенным признакам, например, по наличию команд SMC#0 в ядре "гостевой" ОС.

6. Написать свою Secure OS и загрузить её в импортный ARM-процессор – задача крайне нетривиальная, поскольку документация на аппаратный уровень процессоров, как правило, недоступна (особенно для российских компаний), ключи процессора для загрузки своей Secure OS нам также никто не даст.

7. ARM-процессоры с "открытой" TrustZone или без неё крайне небезопасны.

Aladdin Trusted Security Module (TSM)

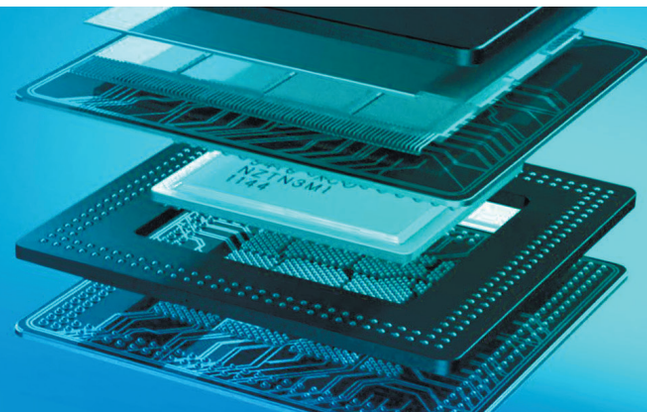
Что это такое?

1 **Это доверенная программно-аппаратная платформа с применением технологии TrustZone для импортных ARM-процессоров серии i.MX6** компании NXP/Freescale, которая позволяет заменить обычный загрузчик ОС на собственный доверенный, загрузить собственную реализацию Secure OS (TEE – Trusted Execution Environment) и обеспечить контроль над коммуникациями и процессами, загрузку и взаимодействие с любой "гостевой" системой (без внесения каких-либо изменений в неё или в используемые приложения).

2 **Aladdin TSM** включает в себя

- Модуль доверенной загрузки, реализующий функции электронного замка, удовлетворяющий* требованиям Профиля ФСТЭК России к средствам доверенной загрузки уровня BIOS второго класса защиты (до гостайны со степенью секретности "Совершенно Секретно").
- Модуль доверенного ввода и вывода для защищённых приложений, недоступного к перехвату средствами обычной ОС.
- Модуль СКЗИ и ЭП, реализующий набор российских криптоалгоритмов и протоколов, работает как трастлет в изолированной доверенной среде TrustZone с аппаратным доверенным хранилищем ключей. При этом все криптографические функции доступны приложениям в "гостевой" ОС через привычные вызовы библиотеки pkcs#11.
- Модуль централизованного управления, позволяющий с использованием системы JaCarta Management System (JMS) дистанционно управлять ключами и сертификатами, загрузкой трастлетов, безопасно обновлять "прошивку" процессора, загружать и анализировать журналы аудита и т.п.

* Находится в завершающей стадии сертификации.



Области применения

Мобильные устройства

Терминалы,
тонкие клиенты

Сетевое оборудование

Элементы Интернета
вещей (IoT, M2M) и т.п.

Ключевые особенности

- Загрузка ОС Linux и ОС на основе Linux, Android, Sailfish.
- Возможность встраивания в существующие разработки.
- Соответствие Профилю защиты ФСТЭК России на СДЗ 2 класса (ИТ.СДЗ.УБ2.ПЗ).
- Аутентификация пользователя до загрузки ОС (требование Профиля).
- Аутентификация по паролю или по паролю и USB-токену JaCarta.
- Проверка целостности объектов ОС перед загрузкой: ядро, Device Tree, файловые системы.
- Защита файлов ОС от непреднамеренного и преднамеренного изменений.
- Защита пользовательских данных от несанкционированного доступа.
- Журнал аудита событий безопасности.
- Удобный графический интерфейс, поддерживается управление с помощью компьютерной мыши и тачскрина.
- Механизм удалённого управления.
- Возможность локального и удалённого обновления.
- Встроенный инсталлятор — установка ОС из образов.

Работает совместно с Доверенной Средой (TEE)

- Запуск доверенных приложений (трастлетов) в защищённой песочнице.
- Доверенный ввод критических данных, недоступный к перехвату из основной ОС.
- Доверенная визуализация критических данных.
- Аппаратный контроль доступа к загрузочному носителю ОС.
- Доверенное хранение ключей и секретов.
- Реализация средства криптографической защиты информации и средства электронной подписи в виде трастлетов без дополнительных аппаратных устройств.

Для кого?

Aladdin TSM предназначен для:

- разработчиков электронных устройств;
- разработчиков программно-аппаратных комплексов;
- производителей электронной техники;
- интеграторов.

Отрасли:

- промышленная автоматизация;
- связь;
- транспорт;
- ЖКХ, умный город;
- мобильные терминалы;
- IoT.

Что это даёт?

Технология даёт возможности

1. Использовать (продолжать использовать) самую современную, надёжную и недорогую элементную базу там, где необходимо обеспечить высокий уровень безопасности, например, в КИИ, АСУ ТП, для навигационного и коммуникационного оборудования.

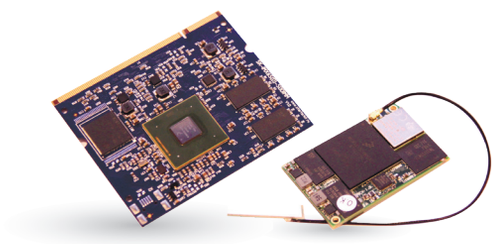
2. Активировать безопасный режим работы современных процессоров ARM i.MX6, загружая в их TrustZone российскую доверенную Secure OS с функциями "электронного замка", обеспечивающего:
   - доверенную загрузку, контроль целостности как Secure OS, так и любой "гостевой" ОС и всех файлов программ и данных;
   - защиту данных от НСД, утечки, искажения, перехвата;
   - контроль каналов и способов распространения защищаемых данных;
   - использование российской криптографии (для приложений это выглядит как крипто-сопроцессор);
   - соответствие требованиям российских регуляторов в области ИБ.

Примеры готовых устройств на базе i.MX6

Терминальные станции

Промышленные компьютеры

Процессорные модули



Процессорные платы, OEM-компьютеры

POS-терминалы

Планшетные компьютеры

Аладдин

+7 (495) 223 00 01
www.aladdin.ru
aladdin@aladdin.ru
129226, Москва, ул. Докукина, 16с1

Аладдин — ведущий российский вендор-разработчик и производитель ключевых компонентов для построения доверенной безопасной ИТ-инфраструктуры

https://t.me/aladdinrd https://vk.com/aladdinrd