

Aladdin embedded PKI Starter Kit

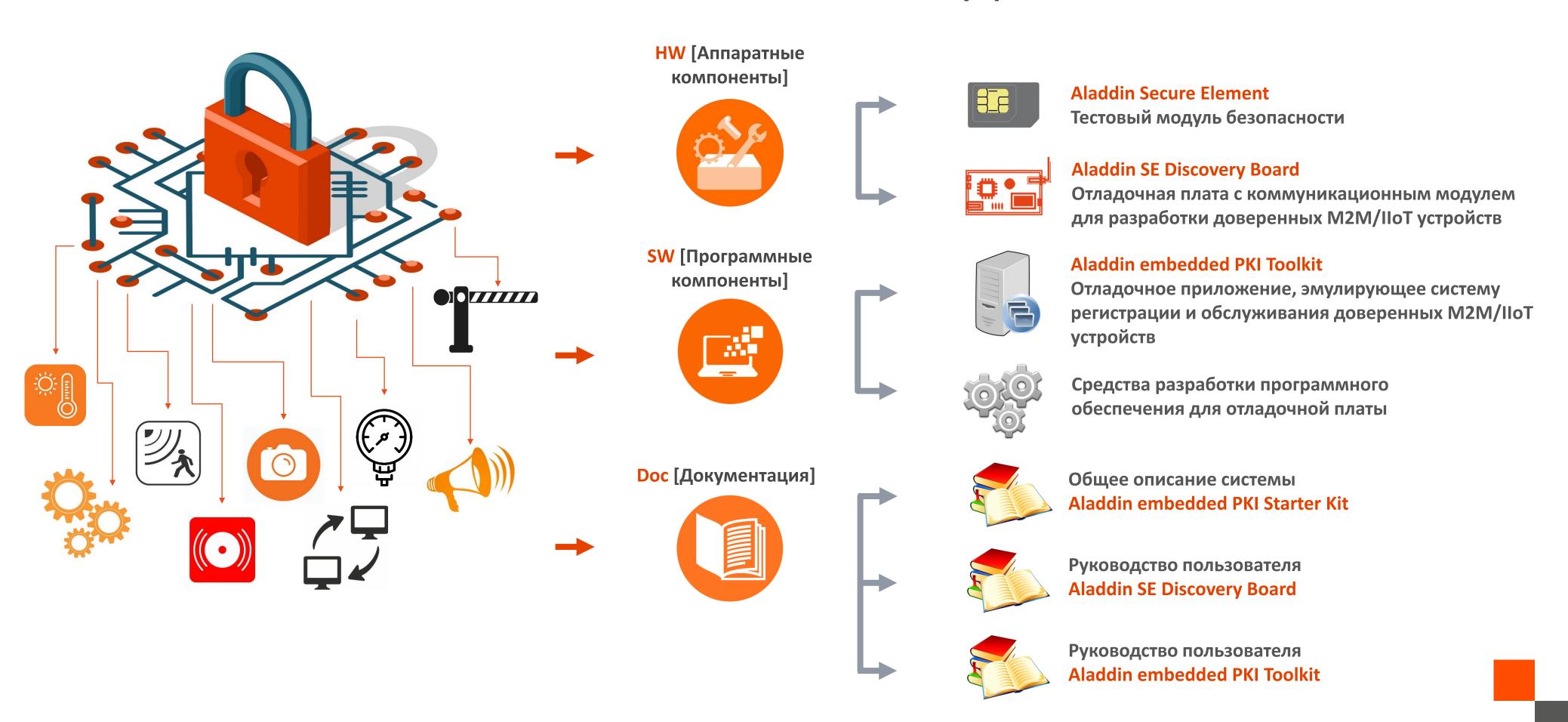
Технологическая платформа разработки доверенных устройств и систем управления

Общее описание



Aladdin ePKI Starter Kit

Aladdin embedded PKI - технологическая платформа разработки доверенных M2M/IIoT устройств и Starter Kit



Назначение



Быстрая разработка и отладка устройств промышленного назначения для критической информационной инфраструктуры. Создание систем управления на основе цифровых двойников.



Встраивание модуля безопасности в устройства для достижения высокого уровня безопасности в процессах аутентификации, шифрования данных, хеширования и выполнения других криптографических операций.

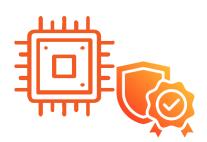


Макетирование устройств и систем с использованием средств криптографической защиты информации, включая оконечные устройства и сервисы управления.



Сертификация в ФСБ и ФСТЭК.

Решаемые задачи



Идентификация и аутентификация компонентов систем. Защита от модификации устройств или их элементов, подтверждение подлинности взаимодействующих сторон. Допуск к выполнению действий.



Защита целостности программного обеспечения и данных. Проверка на предмет изменения данных, полученных при передаче.



Обеспечение конфиденциальности информации. Защита информации как внутри систем, так и при построении внешних каналов передачи данных. Шифрование передаваемой информации. Защита от несанкционированного доступа к средствам защиты данных.

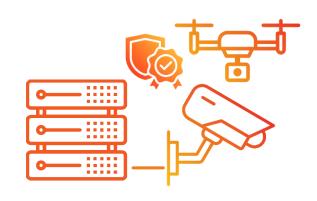


Неотказуемость от информации. Обеспечение гарантии того, что отправитель информации не сможет впоследствии заявить, что он не отправлял её.

Возможности и сферы применения



Электроника, энергетика, добыча, переработка, строительство, пищевая промышленность. Создание устройств и систем, обслуживающих технологические процессы.



Телекоммуникации, беспилотная авиация, охрана. Создание доверенных систем управления. Встраивание аппаратных модулей безопасности в оборудование наблюдения, связи и передачи информации.



Контрольно-измерительное и медицинское оборудование. Встраивание аппаратных модулей безопасности для обеспечения гарантии неизменности и подлинности данных, а также неотказуемости от предоставленной информации.



Финансовый сектор. Создание систем для обеспечения конфиденциальности и целостности информации, защиты каналов обмена данными, аутентификации пользователей и обезличивания персональных данных.



Логистика. Встраивание аппаратных модулей безопасности в системы контроля маршрута, состояния груза, подлинности данных отправления.

Пользователи



Компании-разработчики промышленных устройств и решений для В2В рынка. В платформе заложены и используются современные принципы и протоколы построения доверенных устройств и систем.



Системные интеграторы, которым требуются технологии защиты каналов обмена информацией с использованием сертифицированных аппаратных модулей безопасности. Платформа позволяет моделировать конечные системы, используя реальные процессы.



Ритейлеры для использования в качестве демонстрационного или вспомогательного оборудования.



Учебные заведения, которые обучают проектированию устройств и систем, преподают курсы информационной безопасности.

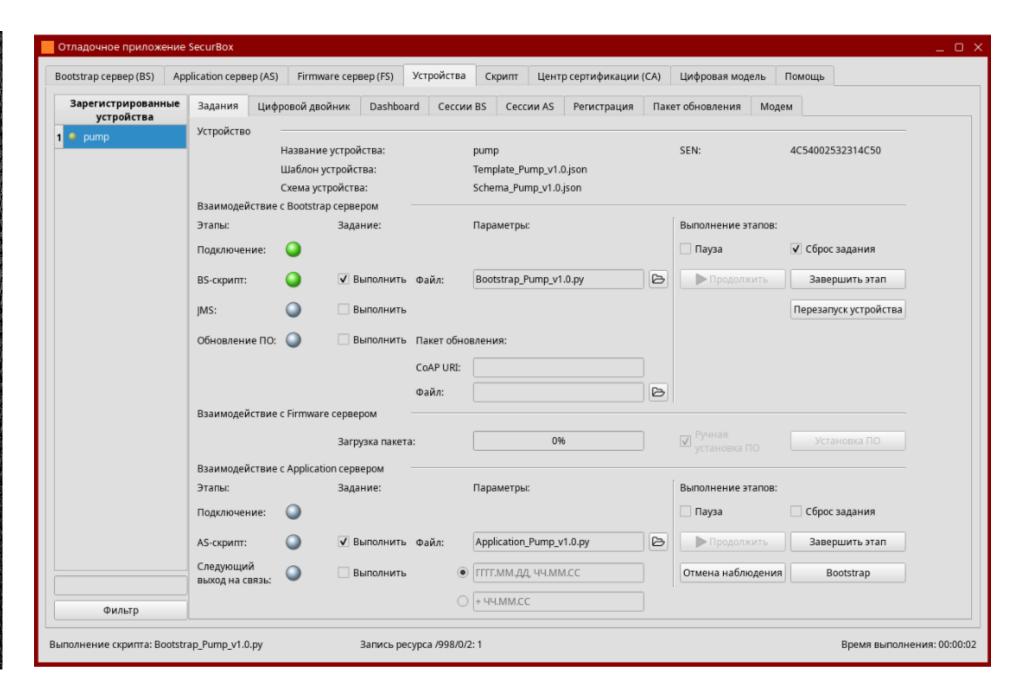
Поставка

Комплект для разработки доверенных устройств с использованием аппаратного модуля безопасности

Модели безопасности. Выполнен на базе специализированеного зазвишейного мекроингровора. Повновите принети премя, отном и сструмента. Поддержавел респремента руковительного должного потакта.

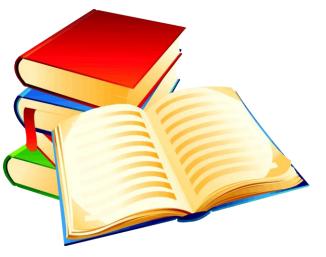
 Отлаганена питат с комуникацичным моделе, пределазнения для разраблега предраменного объестием ИКМ-ИСП с уструмента для и моделения и предраменного должного должн

Отладочное приложение под Linux, эмулирующее систему регистрации и обслуживания доверенных устройств https://aladdin-rd.ru/





Библиотеки для встраивания модуля безопасности и демо-проекты для отладочной платы https://aladdin-rd.ru/



Документация и обучение https://aladdin-rd.ru/

Основные преимущества

Aladdin embedded PKI Starter Kit - компактная технологическая платформа, содержащая все необходимые компоненты для разработки доверенных M2M/IIoT устройств и систем на основе ePKI

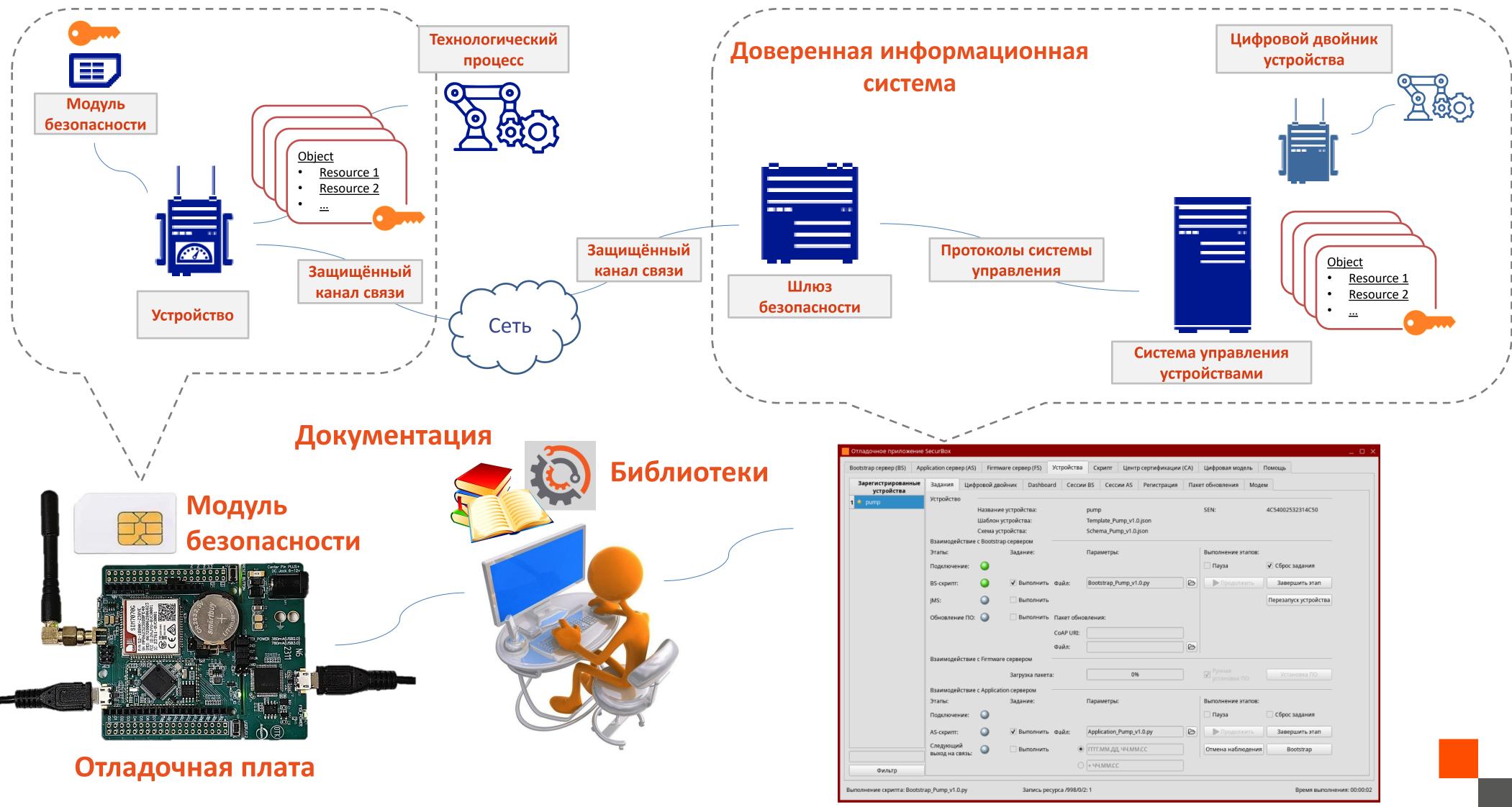


- Архитектуру доверенной информационной системы на основе ePKI.
- Устройства любого прикладного назначения с использованием объектной модели данных управляемого технологического процесса.
- Серверы управления устройствами, включая: сервер безопасности, сервер приложения, сервер обновления программного обеспечения устройств, скрипты управления устройствами с использованием технологий и принципов построения доверенной информационной системы.
- Средства защиты каналов связи с использованием аппаратного модуля безопасности.
- Цифровые двойники устройств для организации удалённого управления.

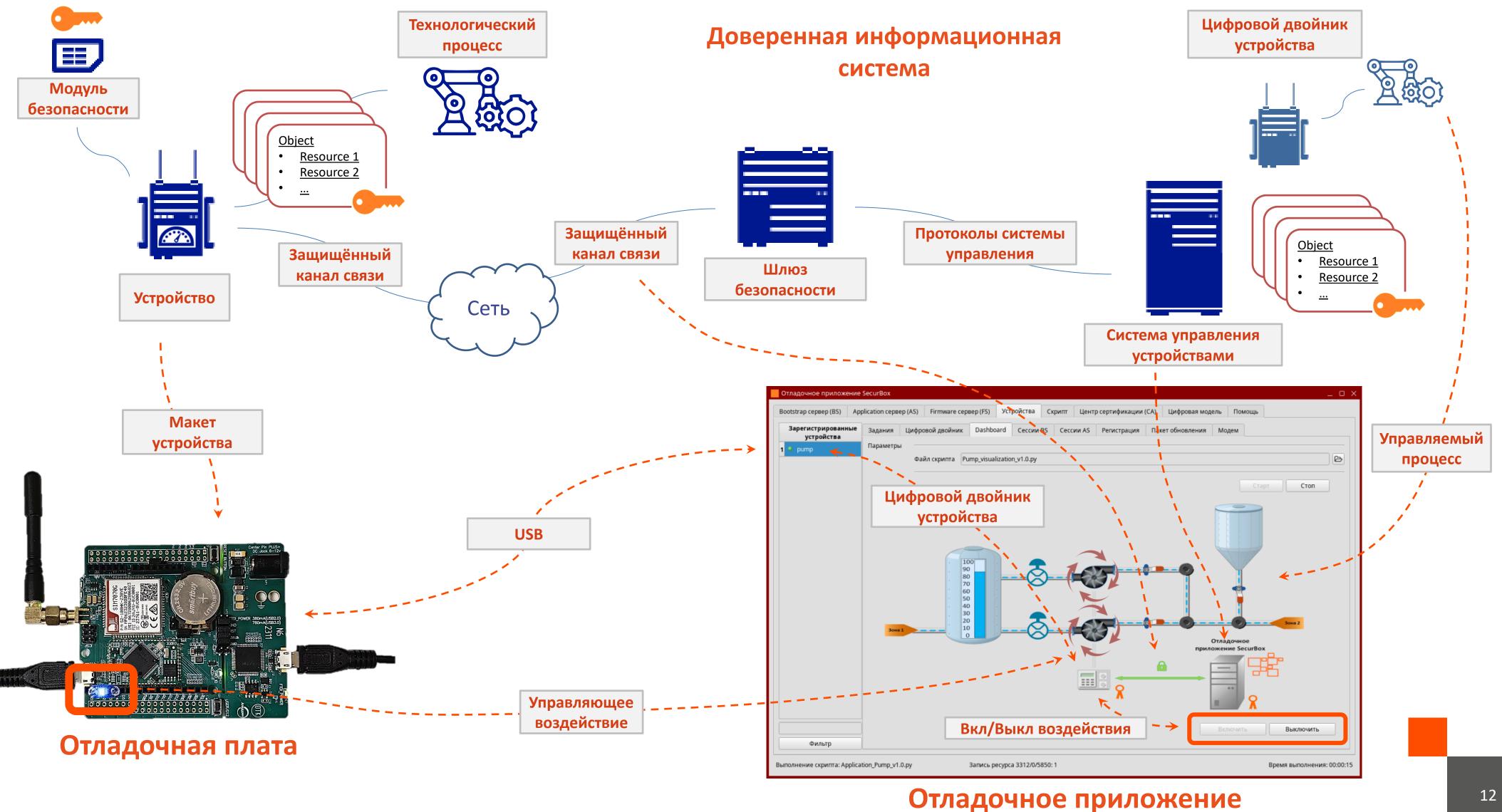
Использование платформы



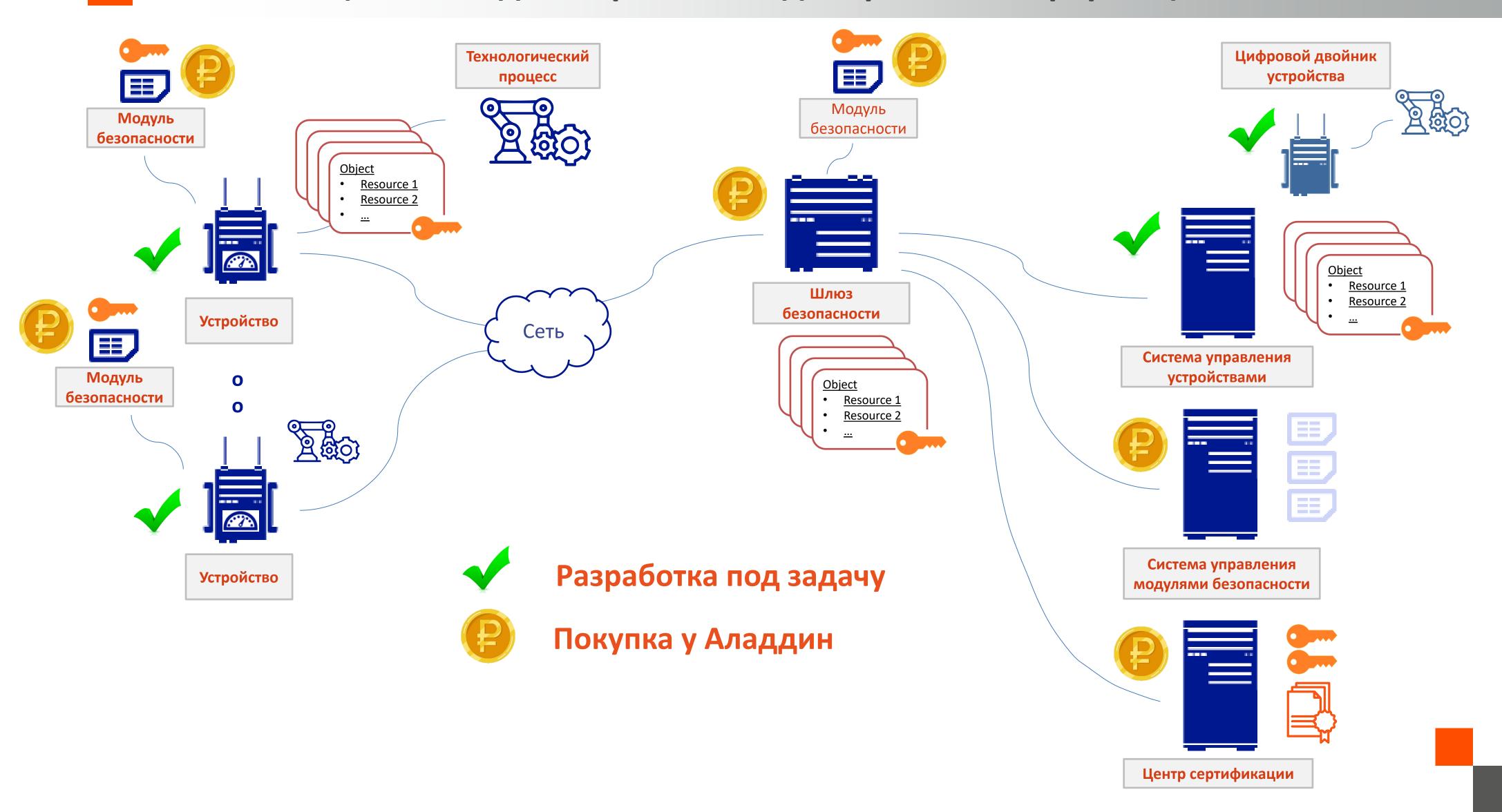
Как разрабатываем с помощью платформы



Как моделируем процессы с помощью платформы



Конечная цель – создание реальной доверенной информационной системы

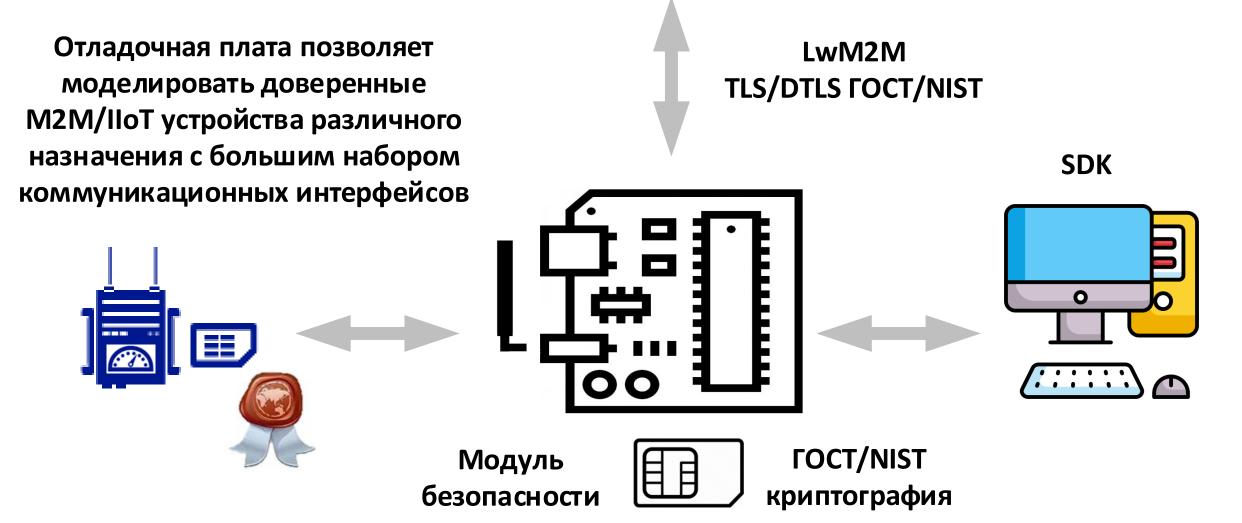


Технические характеристики



Платформа моделирует ePKI систему с поддержкой спецификации LwM2M

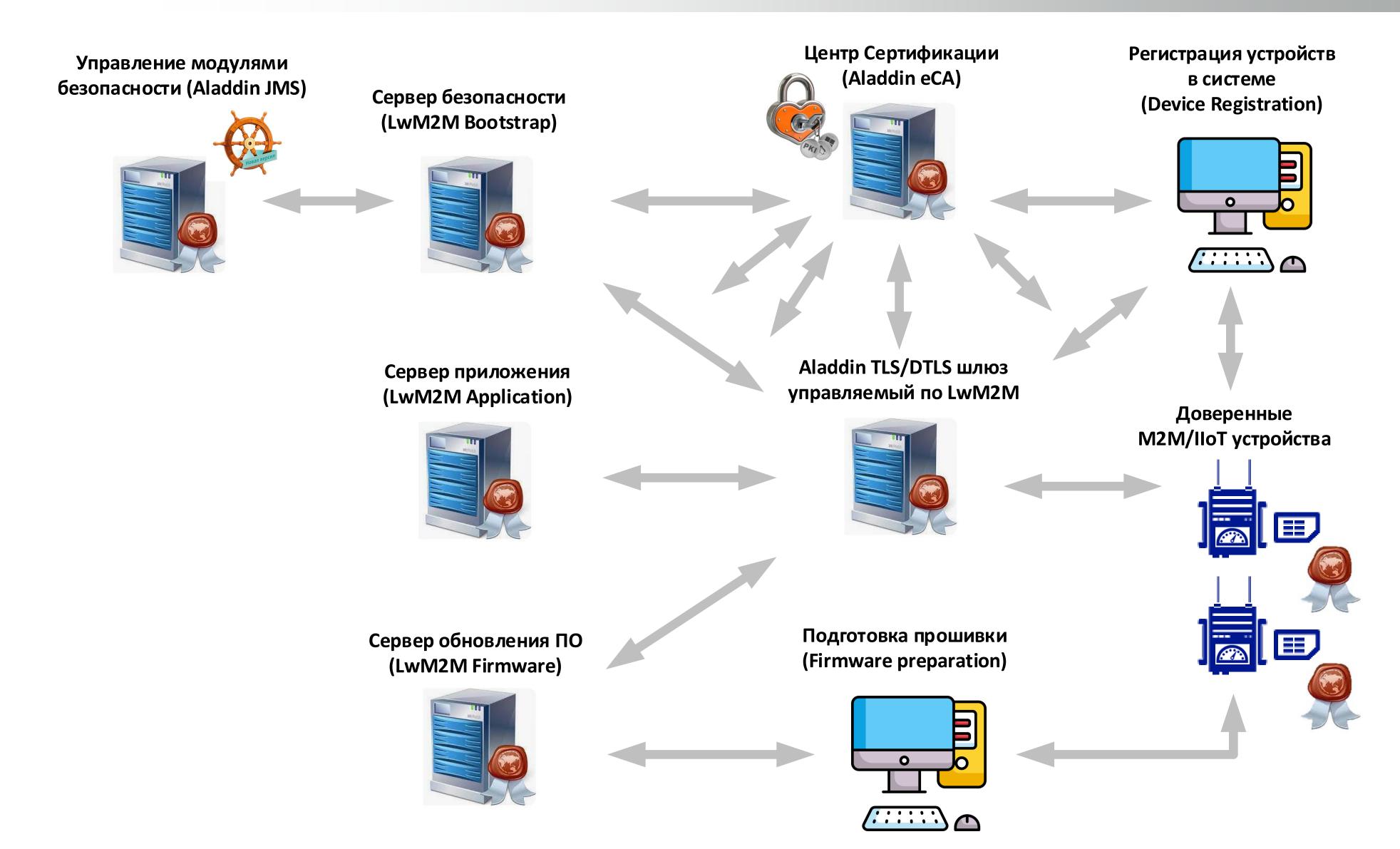




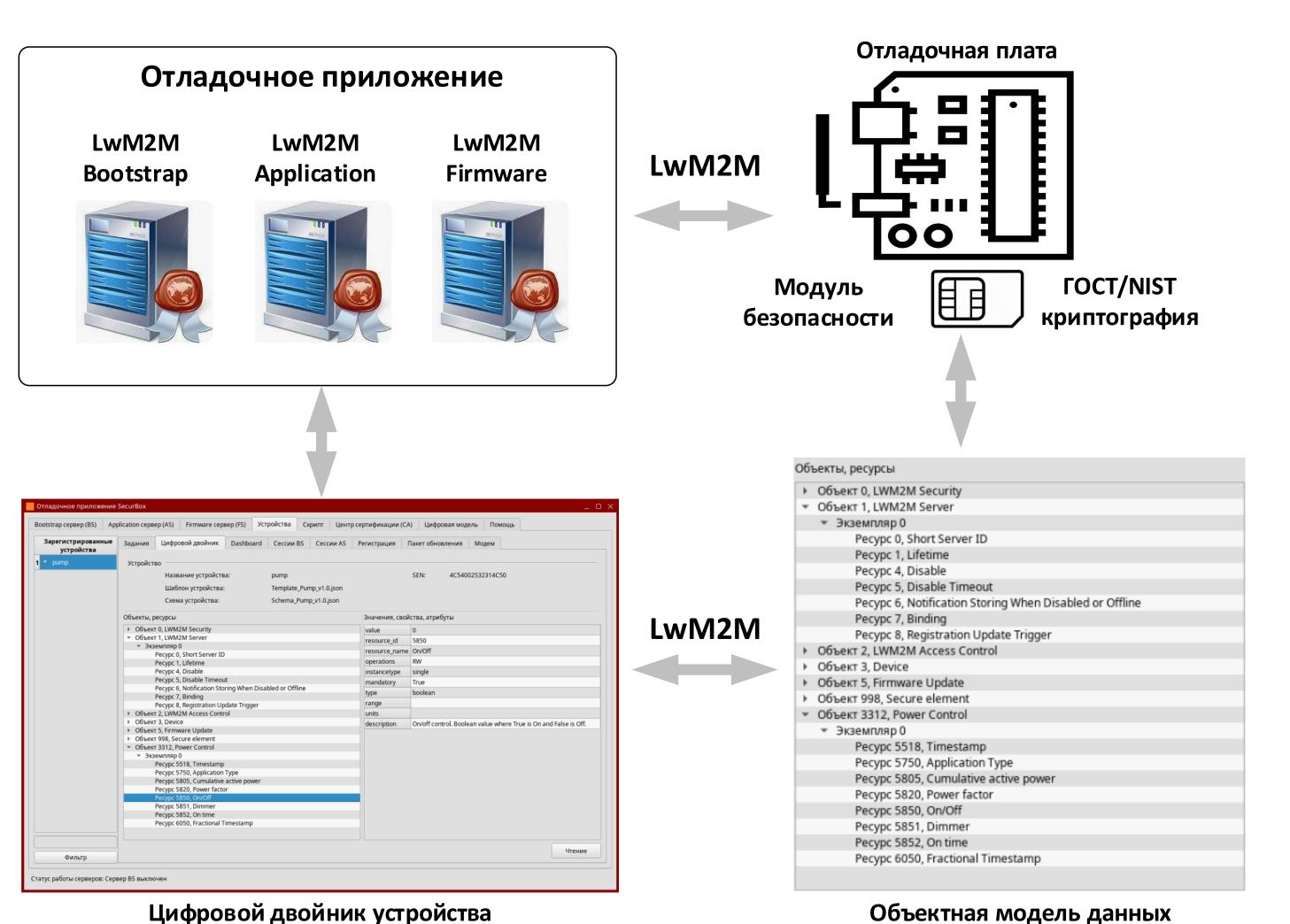
SDK содержит набор библиотек TLS/DTLS ГОСТ/ NIST, LwM2M, которые поддерживают работу с модулем безопасности

Для быстрого старта разработки поставляются готовые демо-проекты, использующие эти библиотеки, и скрипты управления для LwM2M серверов

Взаимодействие компонентов ePKI/LwM2M системы



Цифровой двойник. Работа с объектной моделью данных устройства



в отладочном приложении

Проектирование доверенных устройств любого прикладного назначения с использованием аппаратного модуля безопасности и объектной модели данных

Проектирование и отработка удалённого безопасного управления доверенным устройством с использованием цифрового двойника

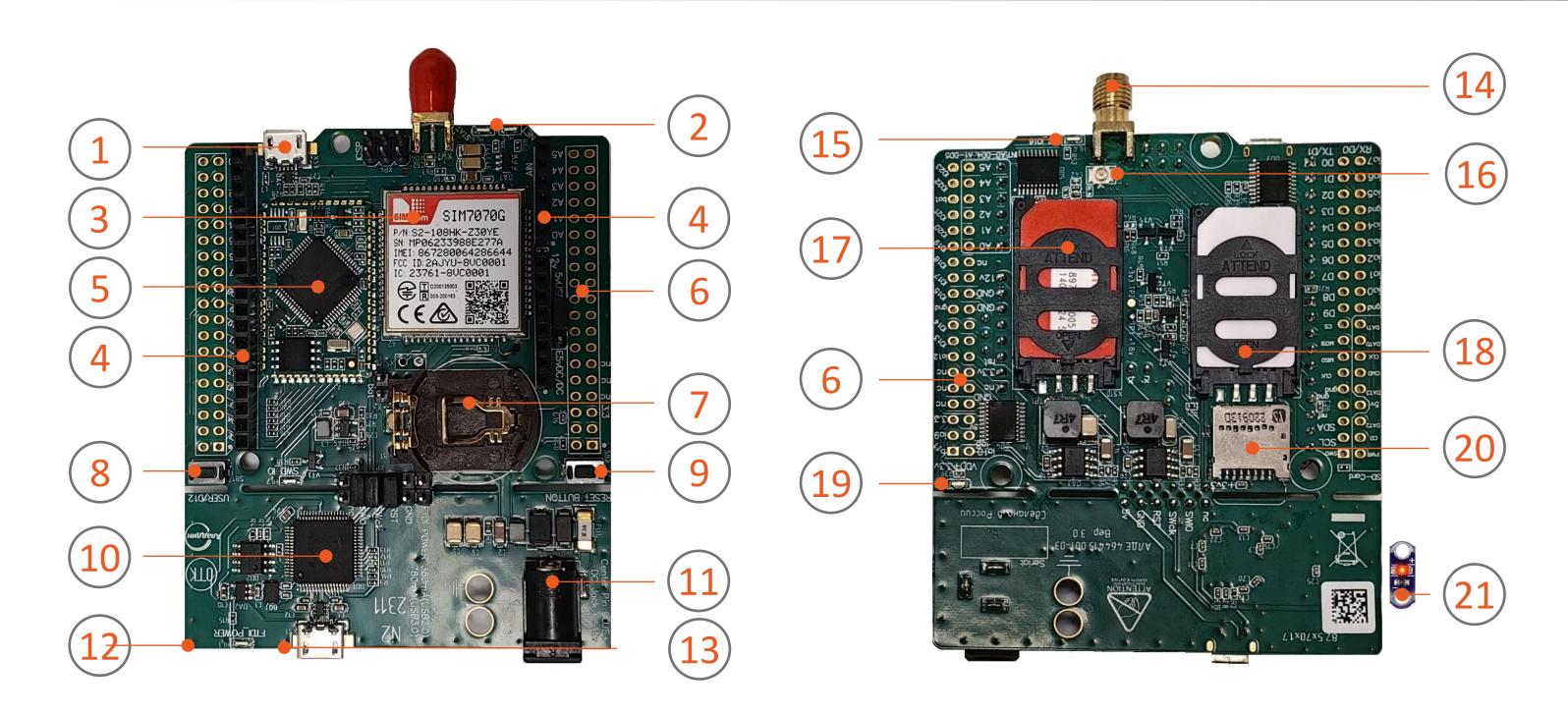
Объектная модель данных устройства

Отладочная плата с широким набором интерфейсов. Импортозамещение





Расположение основных элементов на отладочной плате



- 1.Основной разъём Micro-USB
- 2.LED индикаторы STAT, NET коммуникационного модуля
- 3. Коммуникационный модуль SimCOM 7070G
- 4. Контактная группа Arduino для подключения плат расширения
- 5. Модуль с основным микроконтроллером
- 6. Контактная группа ST Morpho для подключения плат расширения
- 7. Разъём для подключения литиевой батареи CR2032

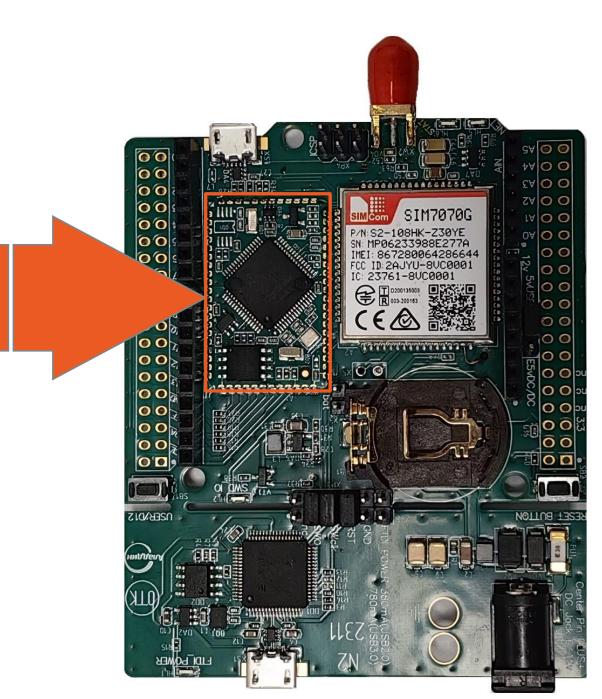
- 8. Пользовательская кнопка USER
- 9. Кнопка RESET
- 10. Микроконтроллер отладчика FTDI 2219-C
- 11.Разъём питания 7V-12V VIN
- 12.LED индикатор питания FTDI
- 13. Micro-USB разъём отладчика
- 14. Разъём SMA для GSM антенны

- 15.Пользовательский LED индикатор
- 16.Разъём U.FL-R-SMT-1 для ГЛОНАСС/GPS антенны
- 17.Разъём 2FF для eSIM карты
- 18.Разъём 2FF для модуля безопасности
- 19.LED индикатор VDD+3.3V
- 20.Разъём карты MicroSD
- 21. Микро-плата с LED индикатором

Аппаратные возможности интеграции основных микроконтроллеров



Модуль JC-4-Base, содержащий основной микроконтроллер отладочной платы, выполнен в виде отдельной универсальной платы для поверхностного монтажа. Разработаны и созданы пять базовых вариантов исполнения JC-4-Base на микроконтроллерах: GigaDevice GD32F427, Atmel ATSAML 11E16A, NXP LPC55S69 JEV98K, Nuvoton M2351SIAAE, Элвис 1892BM2. В зависимости от требований заказчика в рамках отдельного проекта под выбранный микроконтроллер на партию отладочных плат может быть произведён модуль JC-4-Base и портировано встраиваемое программное обеспечение.

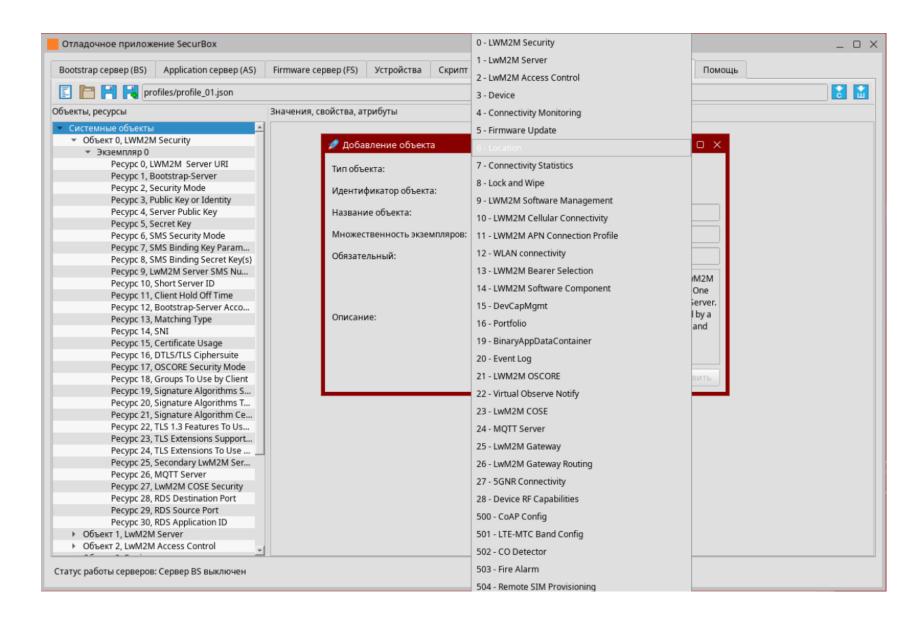


Моделирование процессов реальной системы

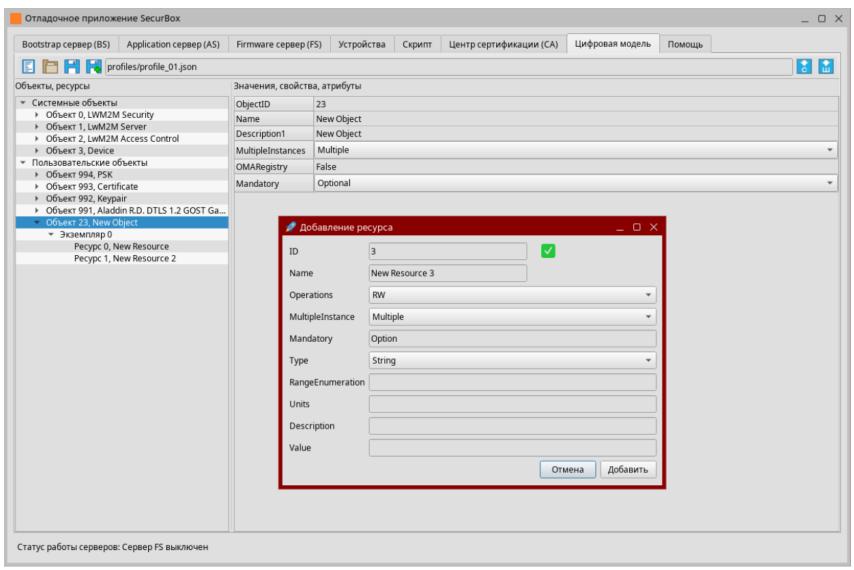


Разработка объектной модели устройства





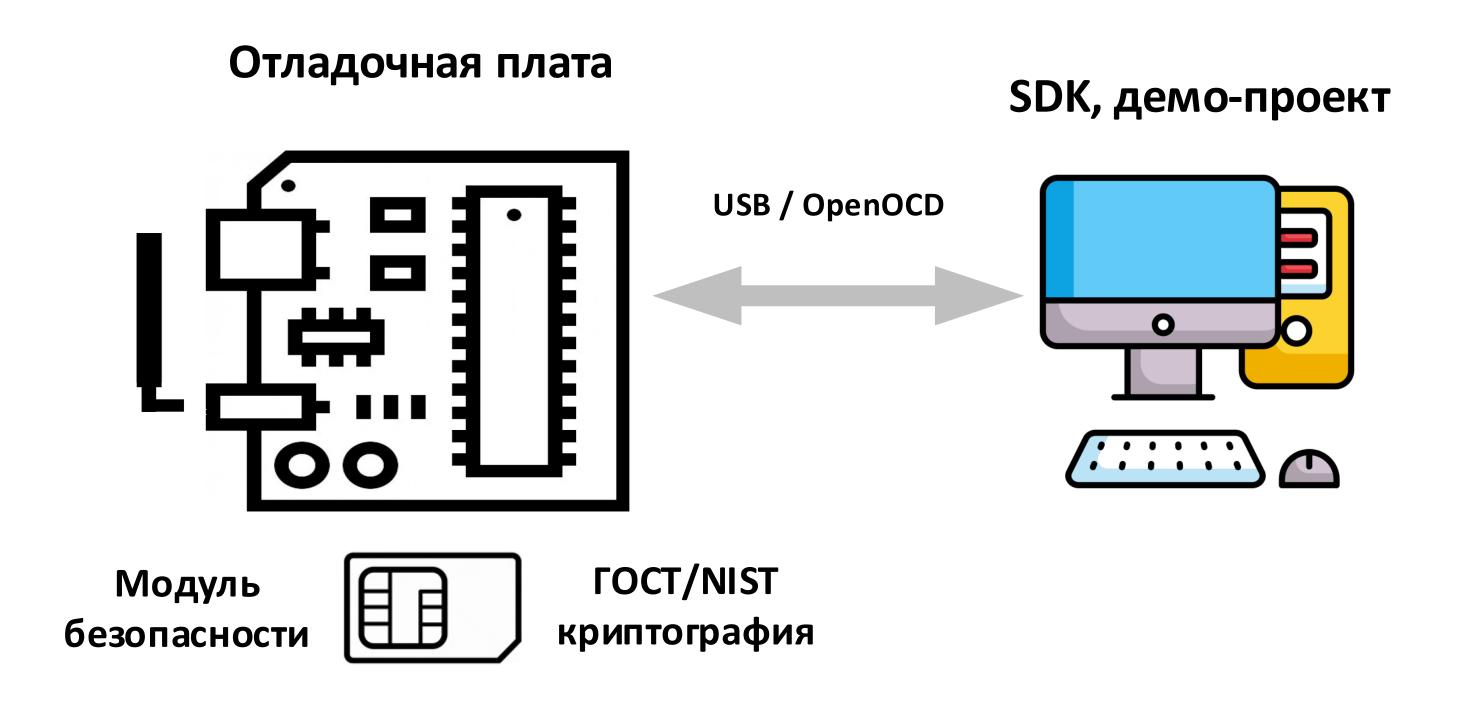
Отладочное приложение содержит библиотеку обязательных системных и стандартных объектов, описанных в спецификации LwM2M, и некоторые объекты из репозитория ОМА OMA LWM2M Object editor



Отладочное приложение позволяет создавать собственные объекты с необходимым набором ресурсов для разработки объектной модели устройства любого прикладного назначения

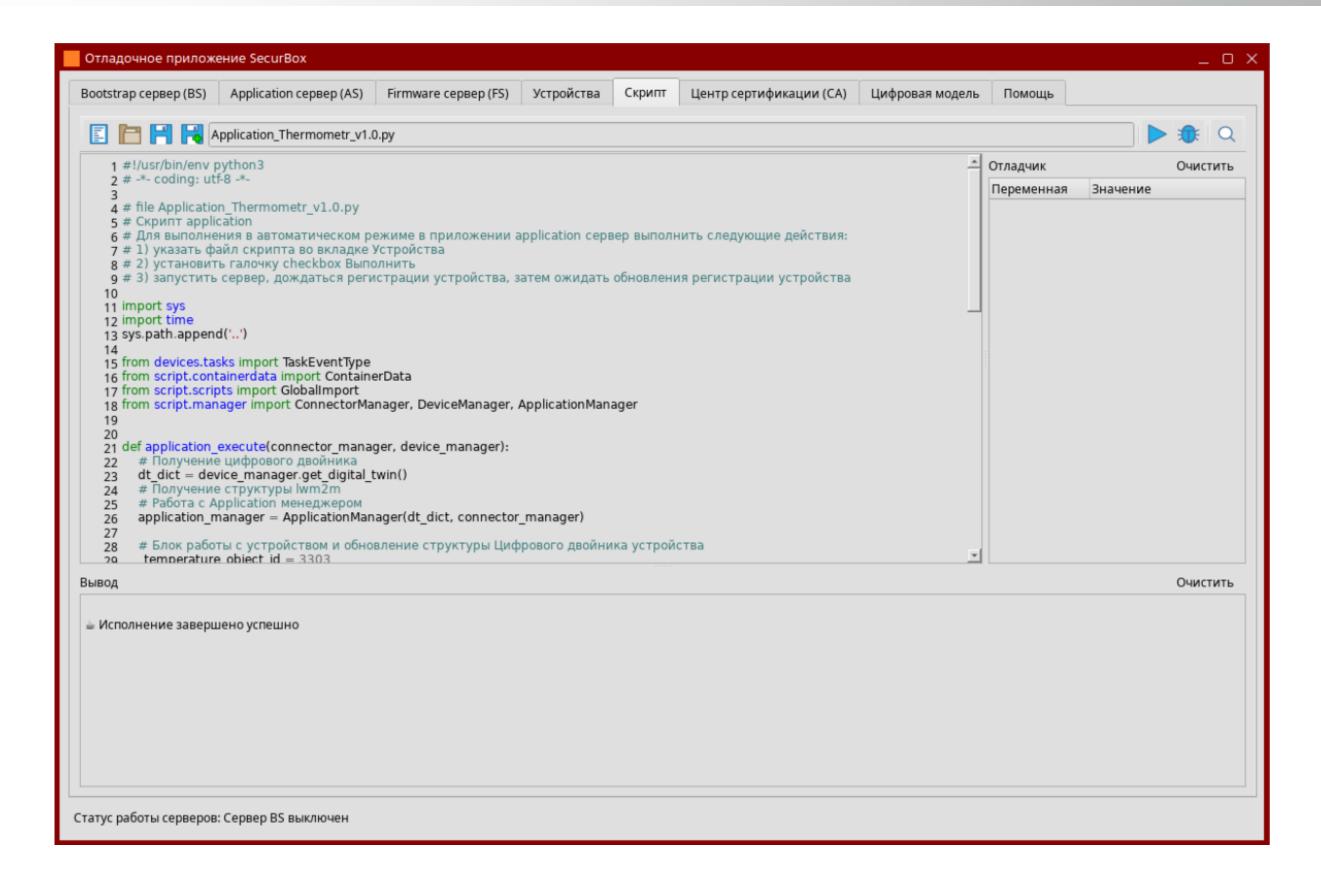
Подготовка и загрузка прошивки устройства





Разработка скриптов взаимодействия компонентов системы

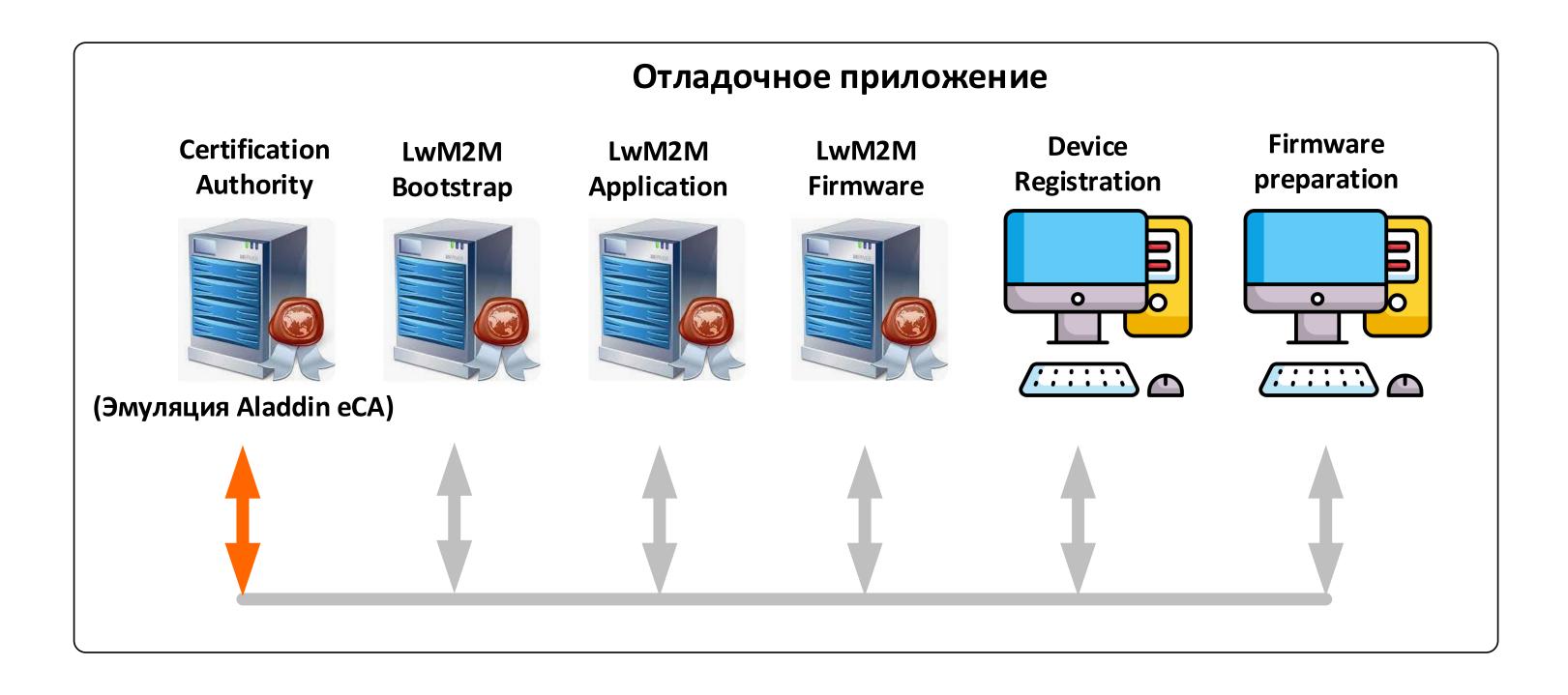




Отладочное приложение позволяет создавать на Python скрипты взаимодействия компонентов моделируемой системы и отлаживать их в пространстве общих переменных в среде отладочного приложения

Генерация и распределение ePKI сертификатов подсистем

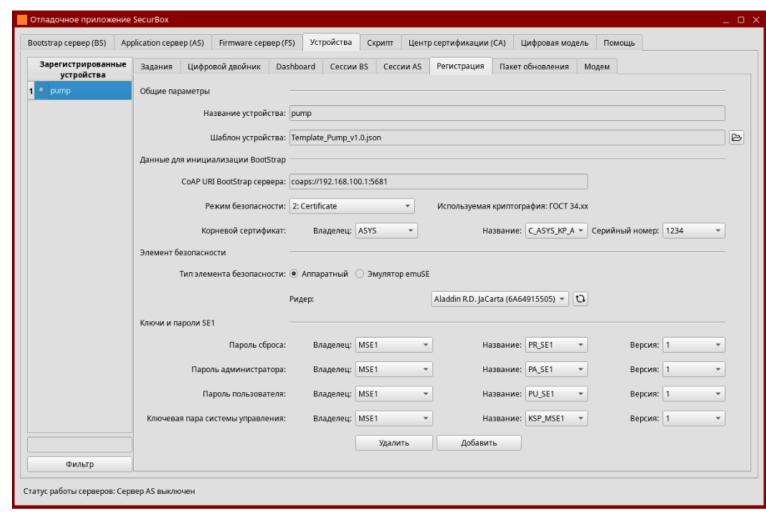




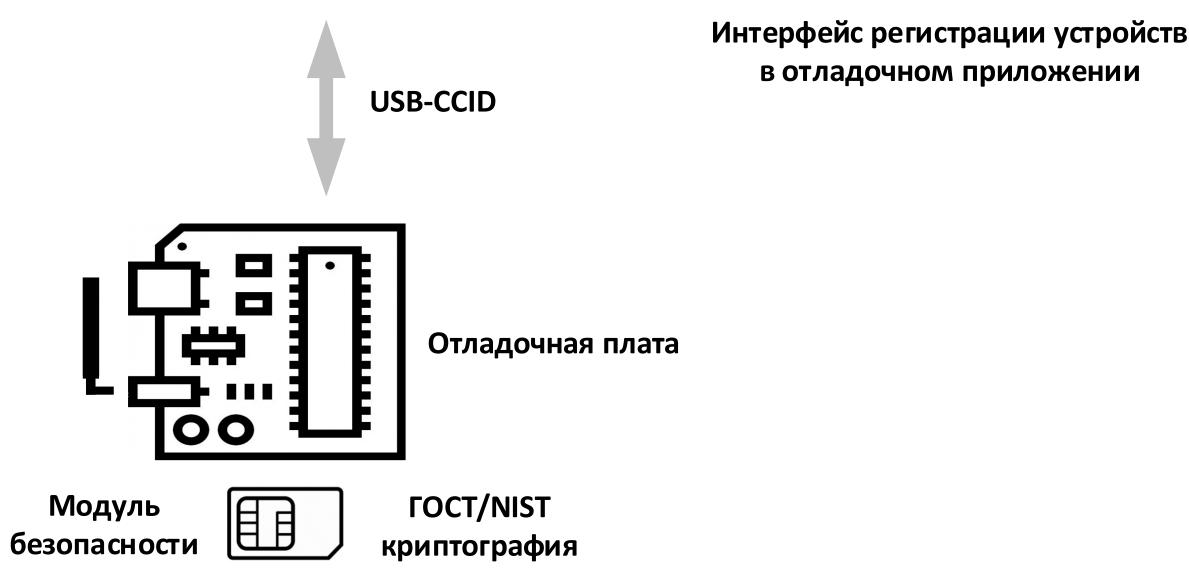
Регистрация устройства в системе





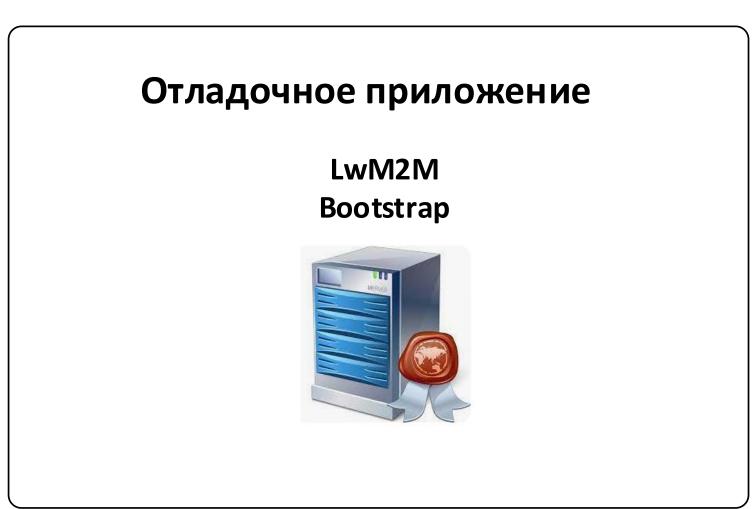


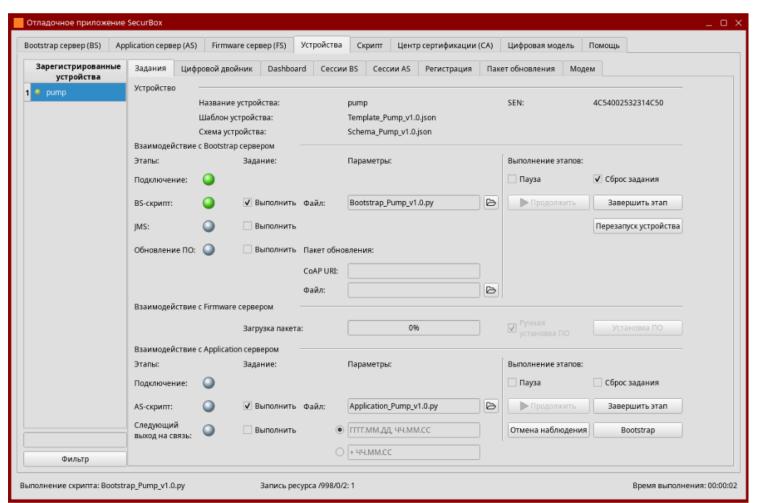
в отладочном приложении

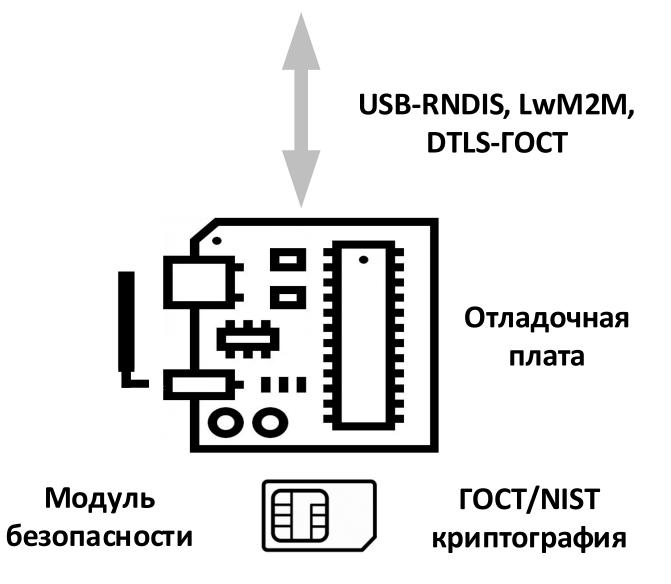


Конфигурация устройства. Взаимодействие с Bootstrap сервером







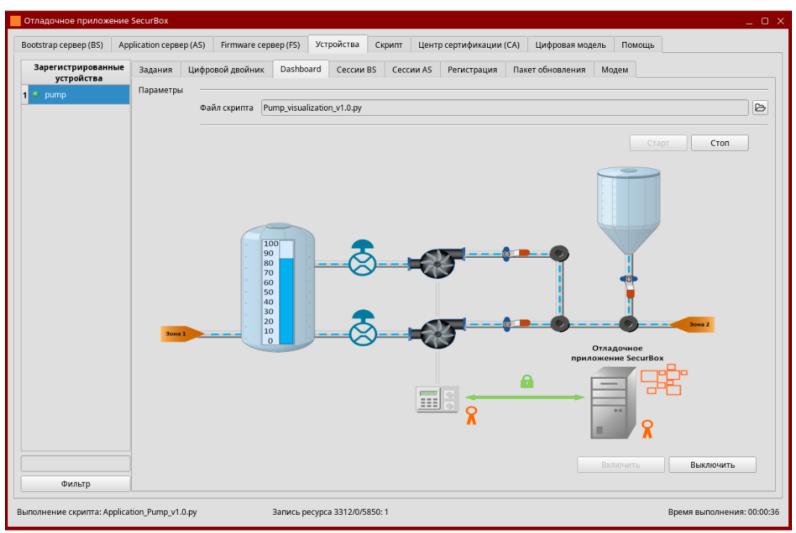


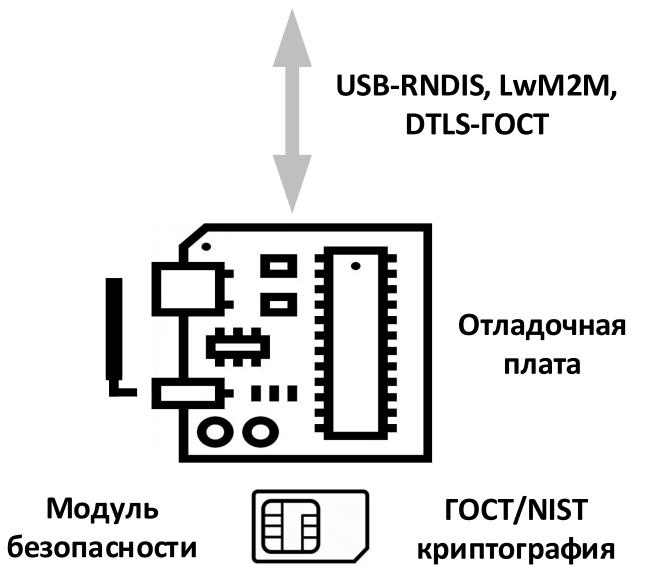
Интерфейс назначения заданий взаимодействия с серверами в отладочном приложении

Прикладное обслуживание. Взаимодействие с Application сервером



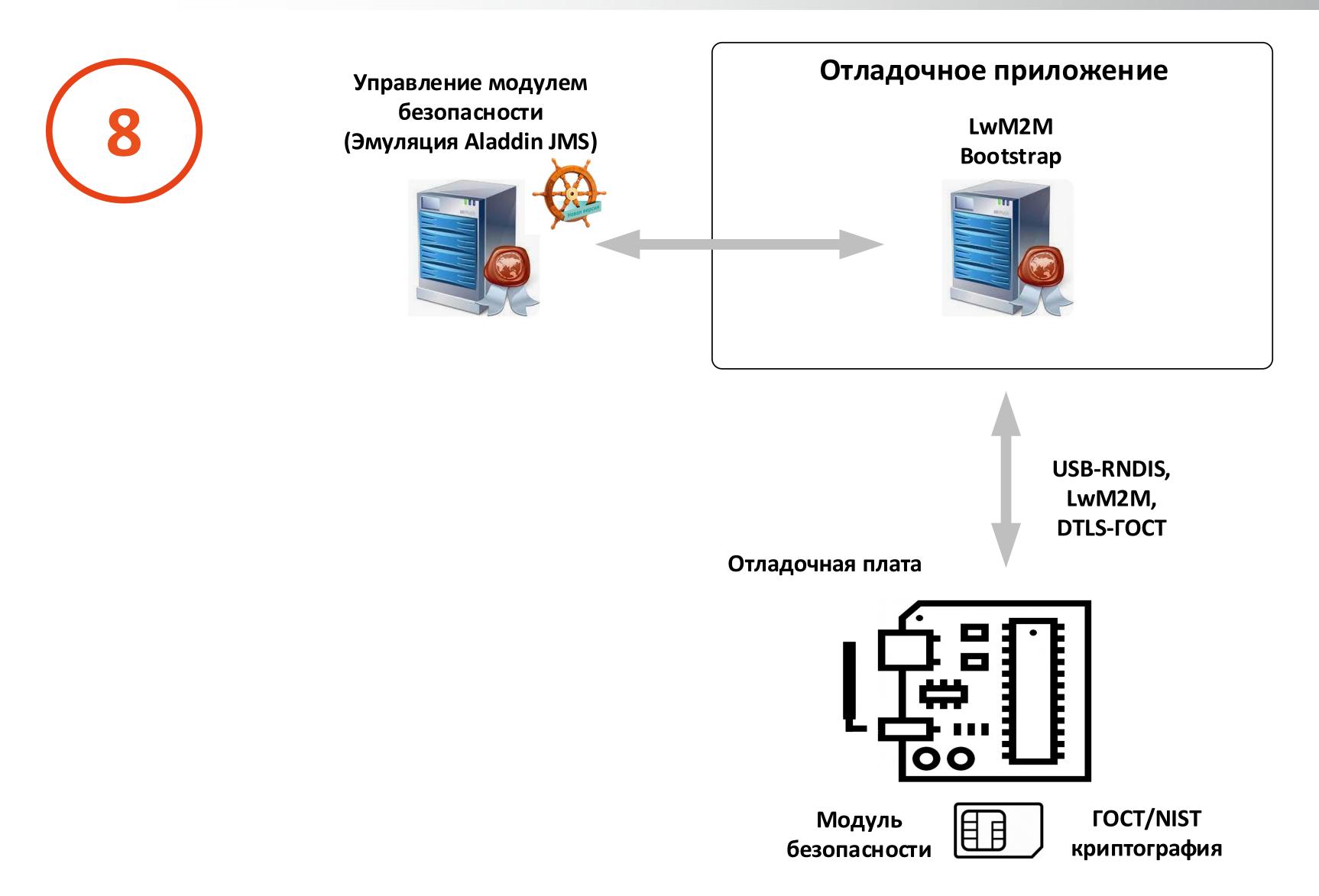






Интерфейс отображения прикладного применения системы в отладочном приложении

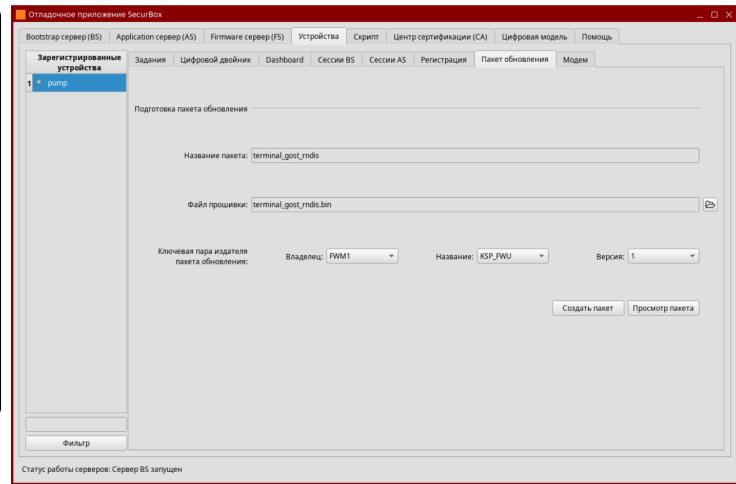
Смена цифрового сертификата устройства

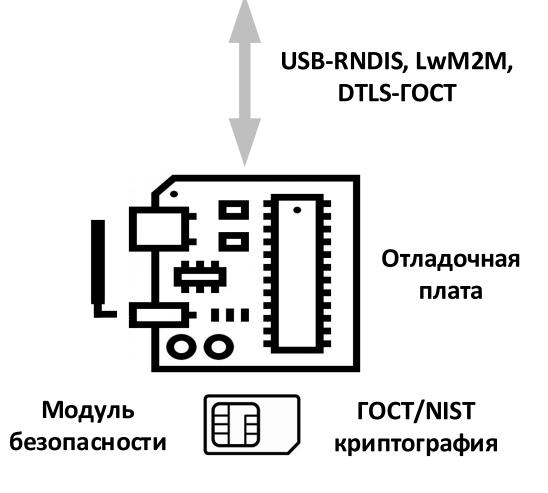


Удалённое доверенное обновление программного обеспечения

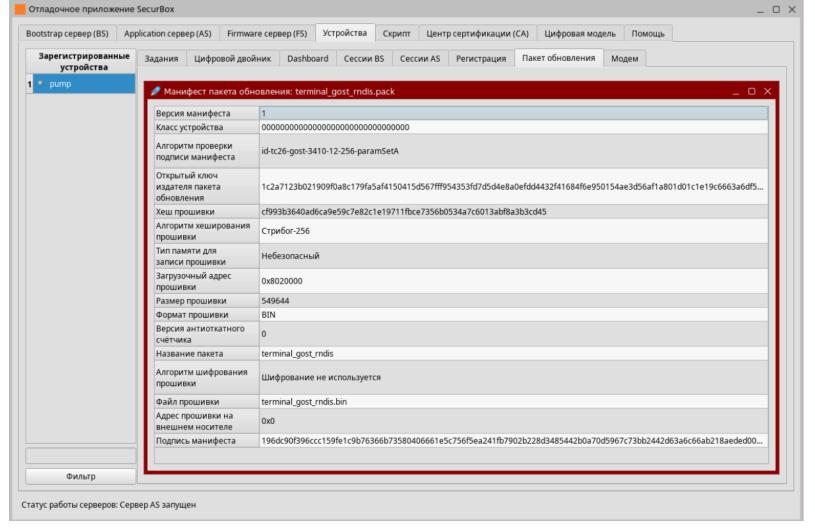








Интерфейс подготовки пакета обновления встраиваемого программного обеспечения в отладочном приложении

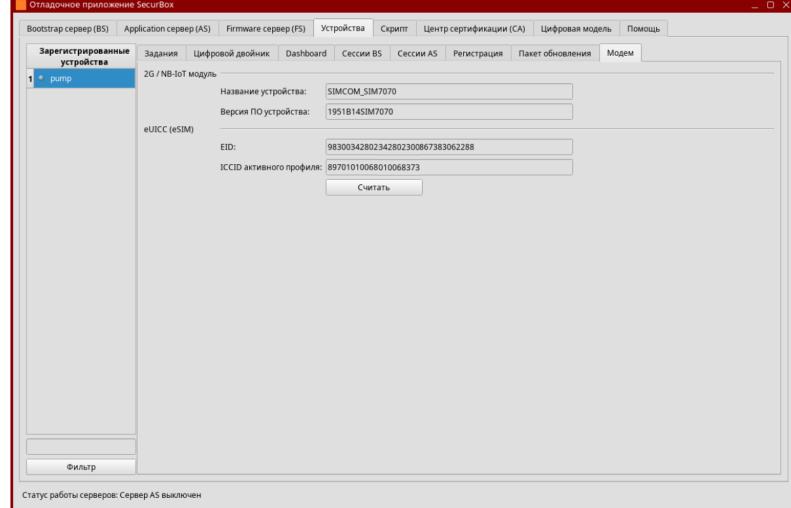


Окно просмотра манифеста пакета обновления встраиваемого программного обеспечения в отладочном приложении

Работа через мобильную сеть







Ethernet, LwM2M, DTLS-ГОСТ

Отладочная плата

USB-CCID

Woбильный оператор

eSIM
2G, 3G, LTE, NB-IoT
2G, 3G, LTE, NB-IoT

2G, 3G, LTE, NB-IoT

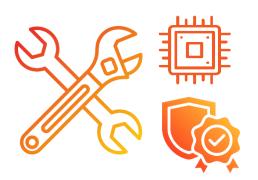
COCT/NIST криптография

Интерфейс просмотра параметров коммуникационного модуля и eSIM в отладочном приложении

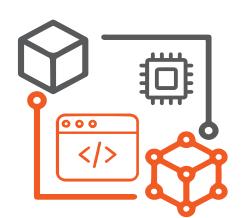
Ключевые особенности платформы



Платформа может применяться для создания перспективных доверенных устройств и систем для таких сфер, как: электроника, энергетика, добыча, переработка, строительство, пищевая промышленность, телекоммуникации, беспилотная авиация, охрана, контрольно-измерительное оборудование, медицина, финансовый сектор, логистика и др.



Платформа содержит необходимые инструментальные средства для разработки доверенных устройств, использующих сертифицированные аппаратные модули безопасности. Функции безопасности заложены в основу проектирования и поддерживаются на всех этапах создания доверенных устройств и систем (Secure-by-Design).



Платформа позволяет разрабатывать и отлаживать программное обеспечение устройств на основе цифровых моделей. Отладочное программное обеспечение платформы реализует службы управления безопасностью и прикладными процессами с использованием цифровых двойников, современных протоколов и принципов построения доверенных систем.



Программное обеспечение платформы поставляется как в скомпилированном виде, так и в исходных кодах. В состав платформы входит отладочная плата с широким набором интерфейсов. Вместе с платформой поставляется подробная документация. Таким образом, платформа является наглядным пособием для обучения, демонстрации и выполнения лабораторных работ по специальностям, которые затрагивают темы автоматических систем управления технологическими процессами, системной интеграции и информационной безопасности.

Термины

M2M – межмашинное взаимодействие, обмен данными между устройствами и системами без прямого участия человека.

M2M устройство – устройство, которое может собирать и передавать информацию о состоянии своего окружения и взаимодействовать с другими устройствами или системами через информационную сеть без прямого участия человека.

ПоТ – промышленный Интернет вещей, подключение и взаимодействие M2M устройств промышленного назначения через сеть, в том числе и Интернет.

M2M/IIoT система — система M2M устройств и сервисов промышленного назначения, взаимодействующих через сеть, в том числе и Интернет.

Доверенное устройство – доверенная электронная компонентная база + доверенное ПО + доверенная цепочка производства и поставки.

Доверенная информационная система — информационная система, состоящая, преимущественно, из доверенных устройств и систем, соответствующая требованиям обеспечения технологической независимости, функциональности, надёжности и защищённости.

Криптография — это область теоретических и прикладных исследований, которая связана с разработкой и применением методов криптографической защиты информации. Криптография использует математические методы для обеспечения выполнения криптографических операций.

Криптографическая защита — использование криптографии для защиты оборудования, программного обеспечения и каналов передачи данных. **Модуль безопасности** — программно-аппаратное устройство, выполняющее функции криптографической защиты информации.

Цифровая модель изделия — система математических и компьютерных моделей, а также электронных документов изделия, описывающая структуру, функциональность и поведение вновь разрабатываемого или эксплуатируемого изделия на различных стадиях жизненного цикла, для которой на основании результатов цифровых и (или) иных испытаний выполнена оценка соответствия предъявляемым к изделию требованиям.

Цифровой двойник изделия — система, состоящая из цифровой модели изделия и двусторонних информационных связей с изделием (при наличии изделия) и (или) его составными частями.

еРКІ — РКІ для встраиваемых систем. РКІ — инфраструктура открытых ключей, представляющая собой совокупность технологий, стандартов, ролей и политик, необходимых для создания, управления, распространения, использования, хранения и отзыва цифровых сертификатов.

TLS/DTLS - криптографические протоколы, обеспечивающие защищённый обмен данными между сервером и клиентом.

<u>LwM2M</u> - протокол управления M2M/IIoT устройствами и обеспечения взаимодействия с сервисами. Используется в платформе для синхронизации цифрового двойника устройства с данными устройства, проектируемого на базе отладочной платы.

ГОСТ – Государственные Стандарты Российской Федерации.

NIST - Национальный Институт Стандартов и Технологии (США), вместе с Американским Национальным Институтом Стандартов (ANSI) участвует в разработке стандартов и спецификаций к программным решениям, имеющим коммерческое применение по всему миру.

CCID – протокол для подключения смарт-карты к компьютеру через кард-ридер с использованием интерфейса USB.

RNDIS - протокол для создания виртуального канала Ethernet между устройством и компьютером при подключении через USB.

Аладдин - будь собой в электронном мире!



Спасибо!

Дмитрий Белов

Руководитель направления M2M AO "Аладдин Р.Д."

<u>D.Belov@aladdin.ru</u>

+79161028511

www.aladdin-rd.ru

