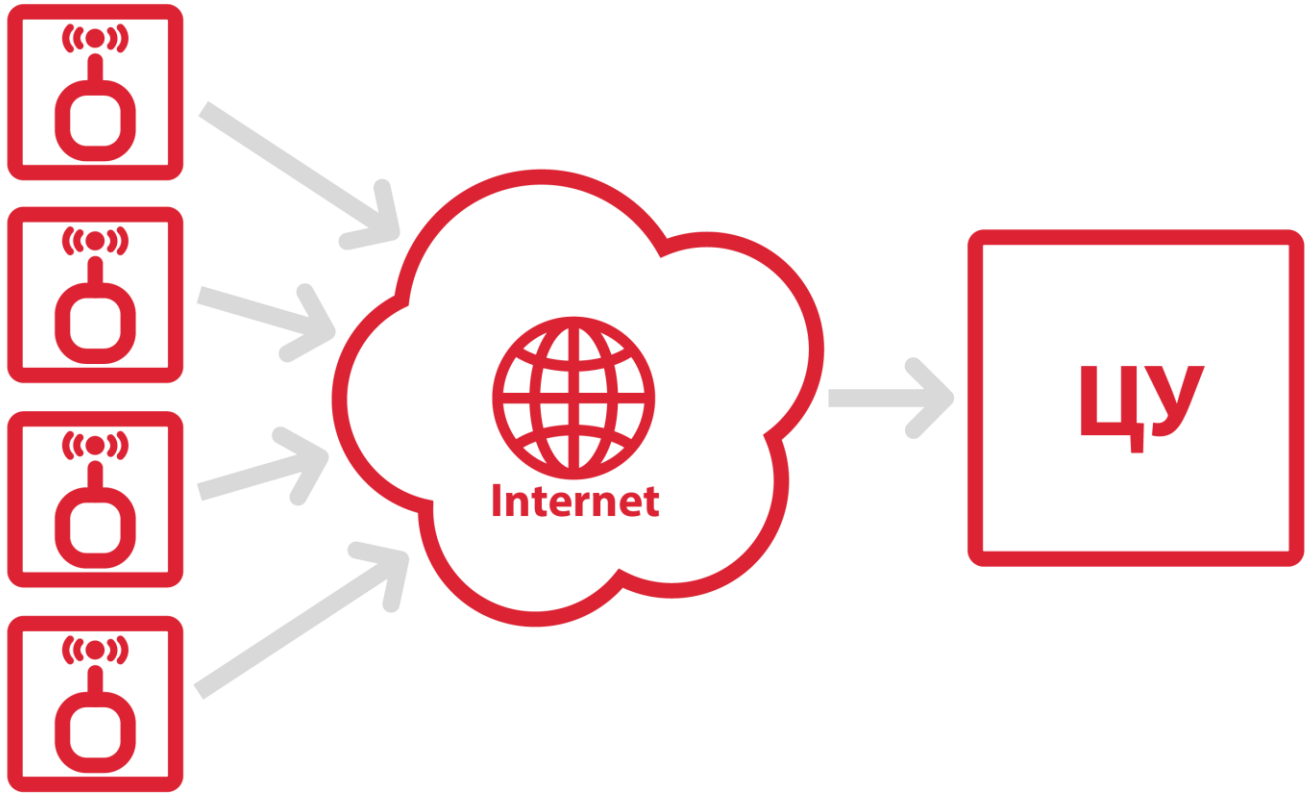
РУТОКЕН

XX международная научно-практическая конференция
«РусКрипто’2018»

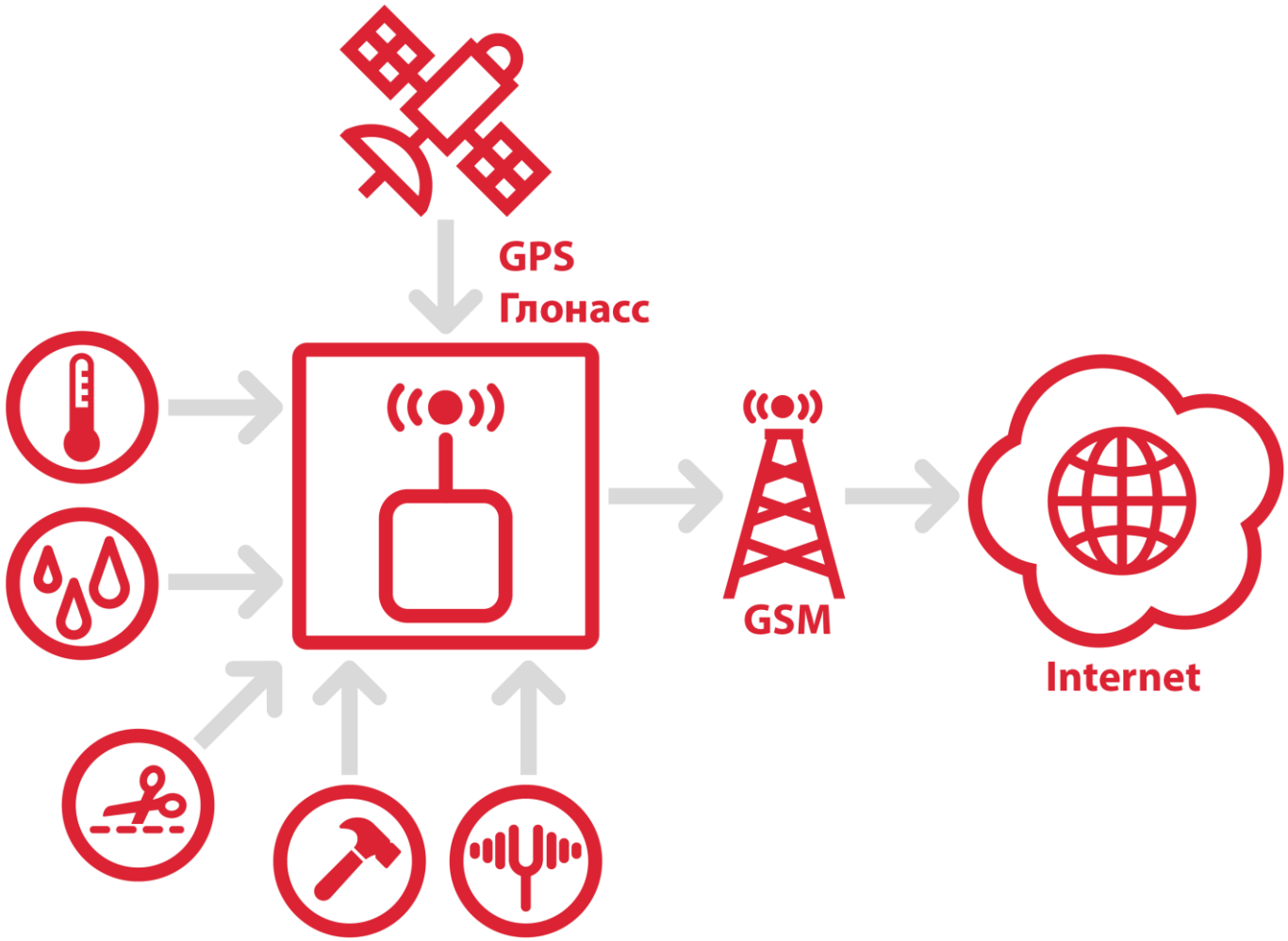
Практическое применение аппаратных криптографических средств в автономных телеметрических устройствах

Владимир Иванов,
компания «Актив»,
директор по развитию

Что было у заказчика?



Что было у заказчика?



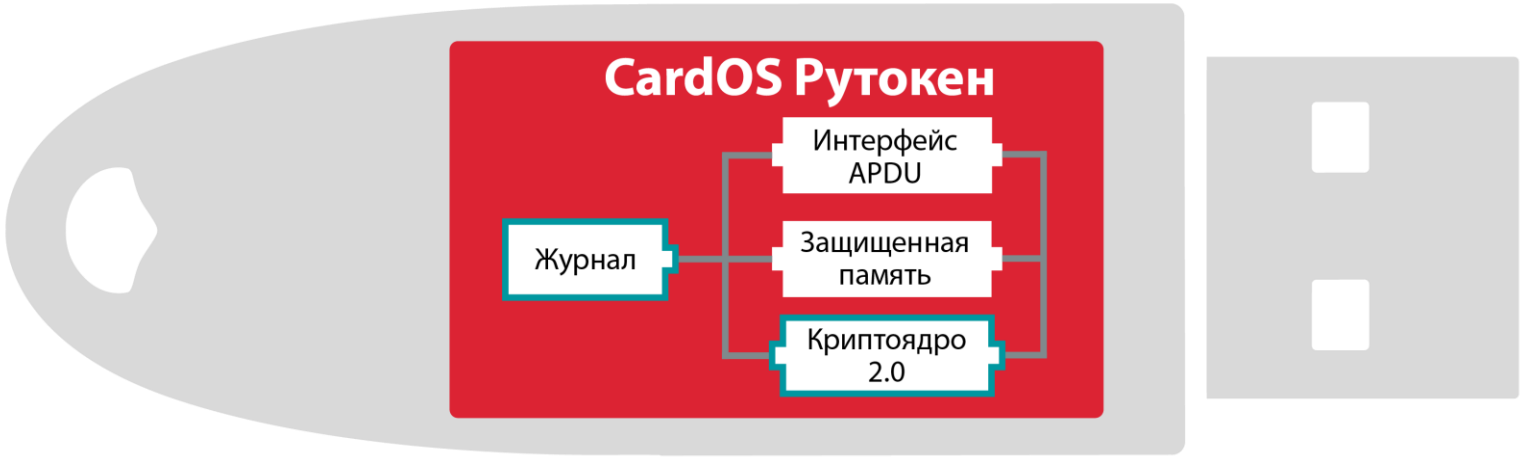
Что хотел заказчик?

- Взаимная аутентификация устройства и центра управления
- Конфиденциальность передаваемых данных и команд
- Целостность передаваемых данных и команд
- Защита от навязывания ложной информации
- Защита от replay-атак
- Сбор доказательной базы
- Юридическая значимость документов
- PKI

Что у нас было предложить?
Рутокен ЭЦП 2.0

- Аппаратная реализация электронной подписи
- Аппаратная реализация хеширования
- Генерация, хранение и использование криптографических ключей «на борту»
- Хранение данных

Архитектура Рутокен ЭЦП 2.0



Криптографические возможности Рутокен ЭЦП 2.0

Аппаратная реализация алгоритмов электронной подписи:

- ГОСТ Р 34.10-2001
- ГОСТ Р 34.10-2012 с длиной ключа 256 и 512 бит
- RSA с длиной ключа до 2048 бит

Аппаратная реализация алгоритмов хеширования:

- ГОСТ Р 34.11-94
- ГОСТ Р 34.10-2012

Аппаратная реализация симметричного шифрования:

- ГОСТ 28147-89

Выработка сессионных ключей (ключей парной связи) по схеме:

- VKO GOST R 34.10-2001 (RFC 4357)
- VKO GOST R 34.10-2012 (RFC 7836)
- расшифрование по схеме EC El-Gamal

Генерация последовательности случайных чисел требуемой длины.
Срок действия ключа до 3 лет в соответствии с документацией на СКЗИ.

Сертификация Рутокен ЭЦП 2.0

Сертификат № СФ/124-2771 удостоверяет, что СКЗИ Рутокен ЭЦП 2.0 соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, требованиям к СКЗИ и средствам электронной подписи классов КС1, КС2 и может использоваться для генерации и управления ключевой информацией, шифрования, хеширования и реализации функций электронной подписи (создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

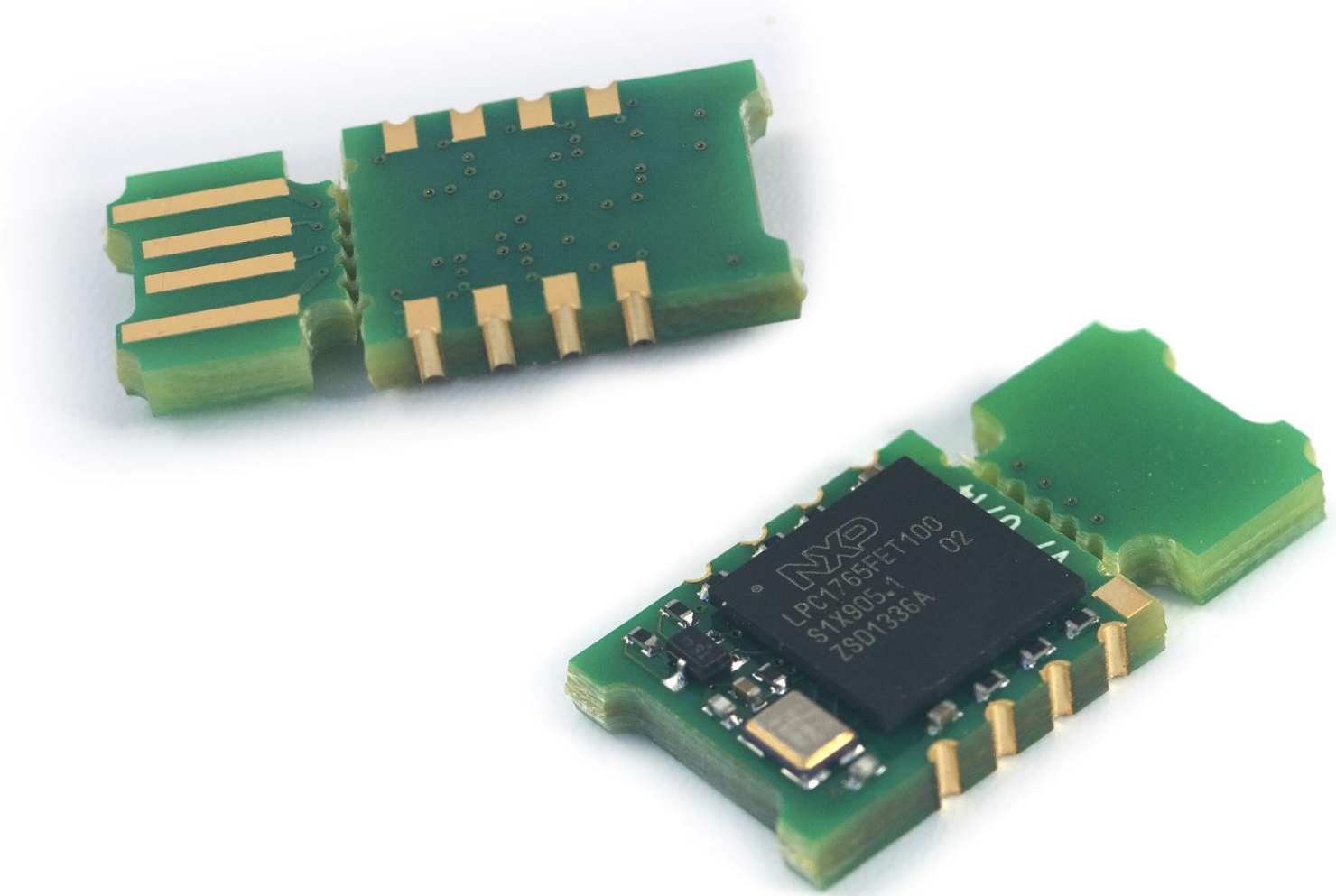
Рутокен ЭЦП 2.0 — сертифицированное ФСБ аппаратное средство для квалифицированной электронной подписи с новыми ГОСТ-ами.

Какие были ограничения?

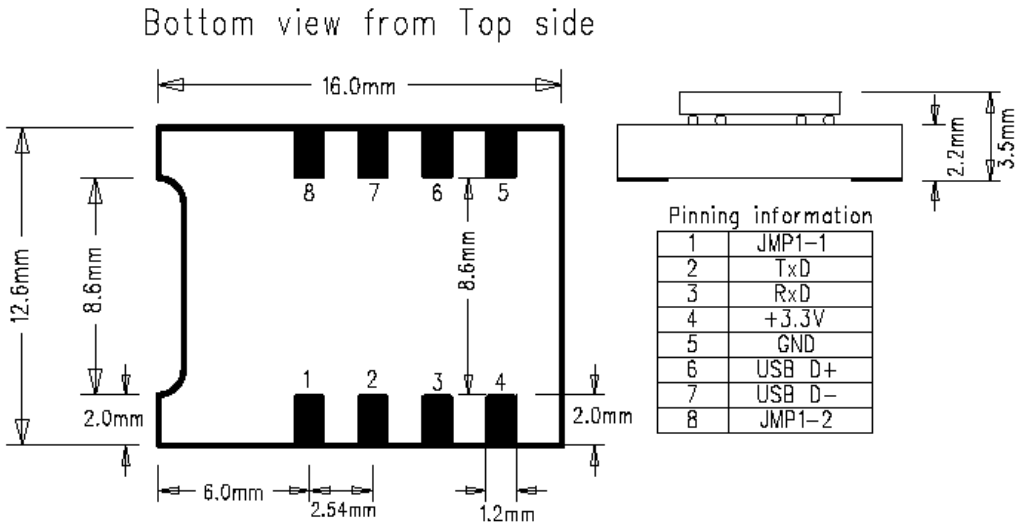
- Отсутствие поддержки USB-стека в операционной системе
- Отсутствие операционной системы
- Отсутствие интерфейса USB в основном контроллере
- Ограниченные ресурсы основного контроллера
- Межповерочный интервал 3 года (без обслуживания)
- Отсутствие у разработчиков заказчика опыта разработки криптографии

Что мы сделали?

- Убрали корпус
- Добавили UART – интерфейс
- Добавили несколько команд в ОС Рутокен
- Разработали интерфейсную библиотеку, не содержащую зависимостей
- Перепроектировали печатную плату
- Заменили постоянный USB-разъем временным (технологическим)
- Подготовили серийное производство
- Разработали технологическую упаковку (тубы)

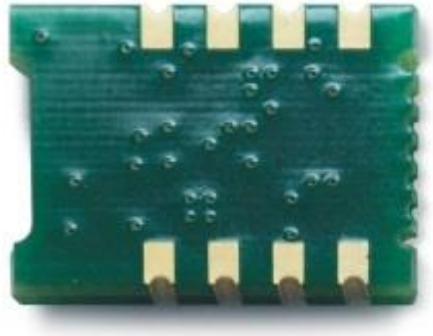

NXP
LPC1765FET100
S1X905.1
ZSD1336A
02

Что получилось?

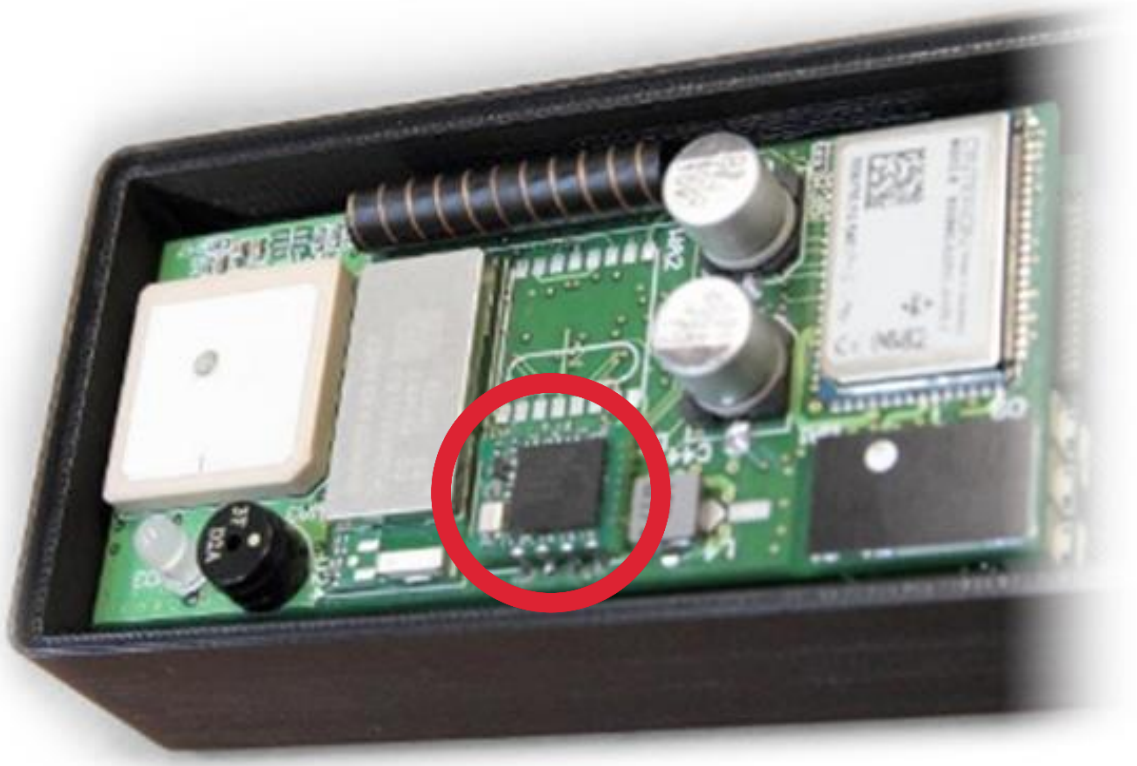


Pinning information

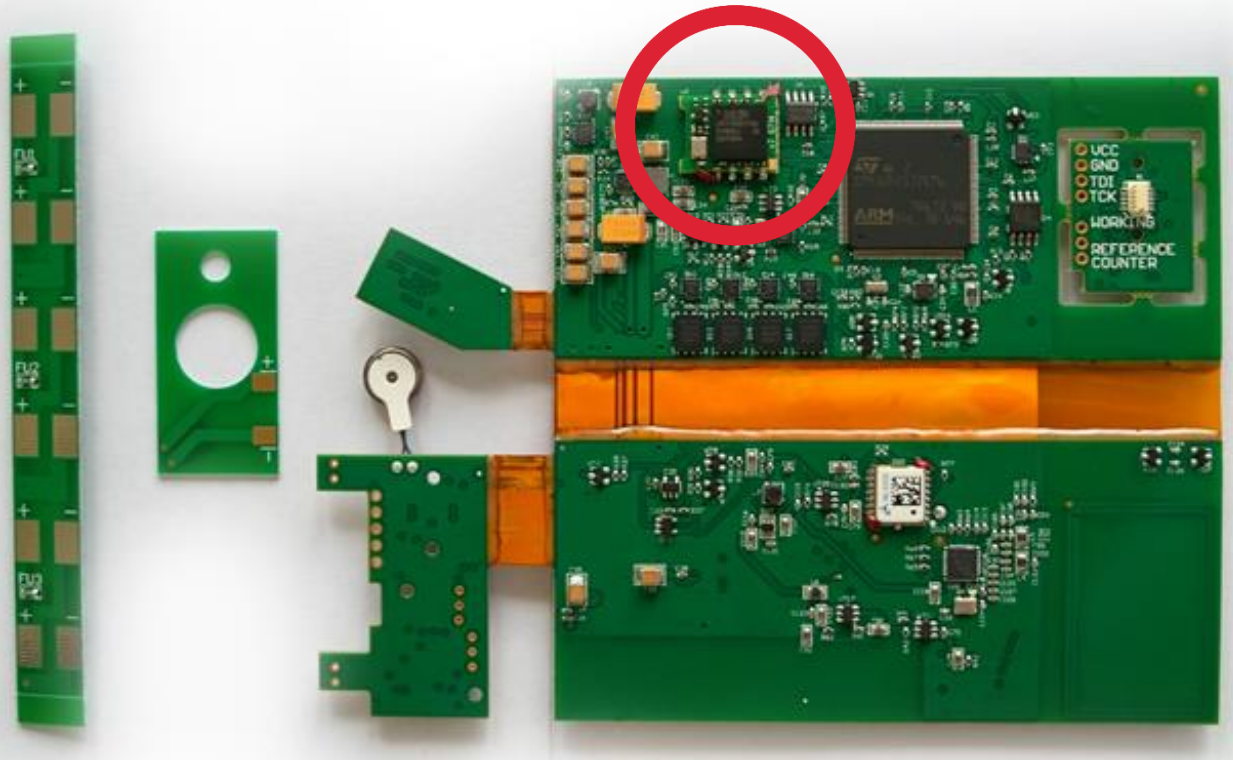
1	JMP1-1
2	TxD
3	RxD
4	+3.3V
5	GND
6	USB D+
7	USB D-
8	JMP1-2



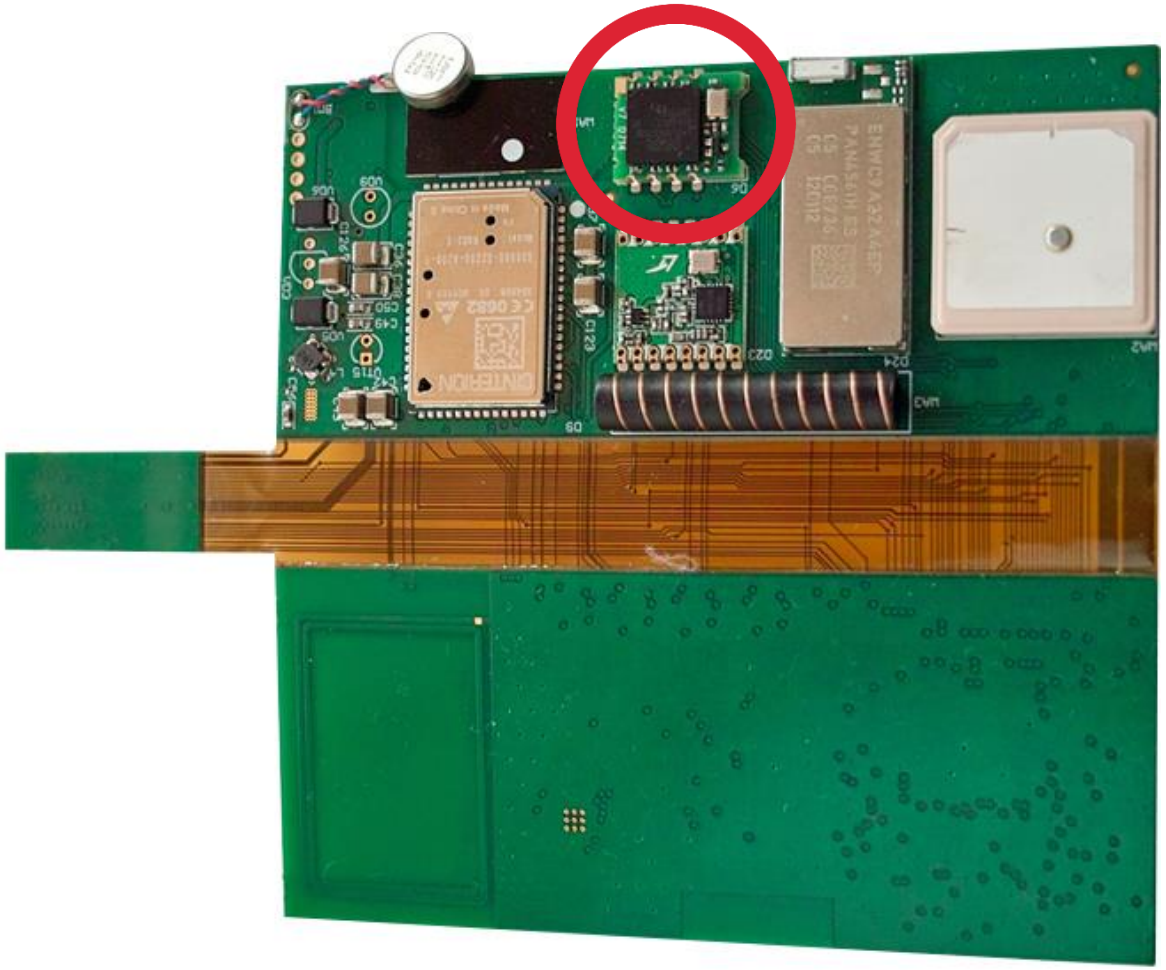
Что получилось?



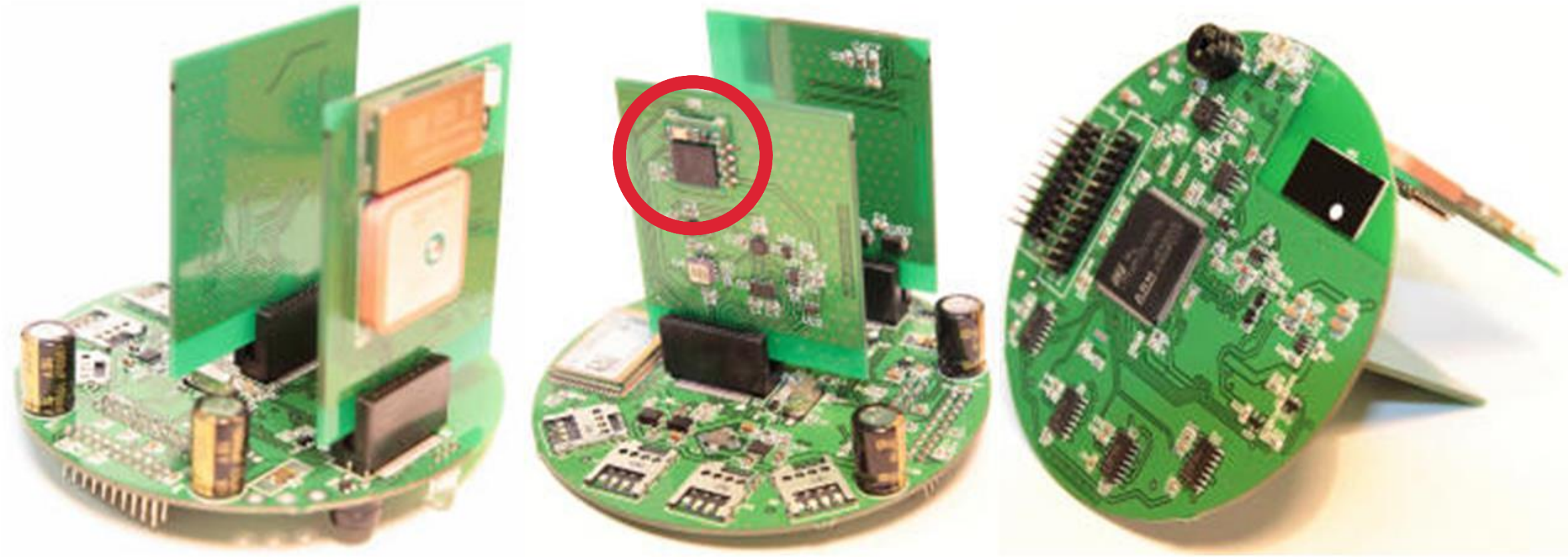
Что получилось?



Что получилось?



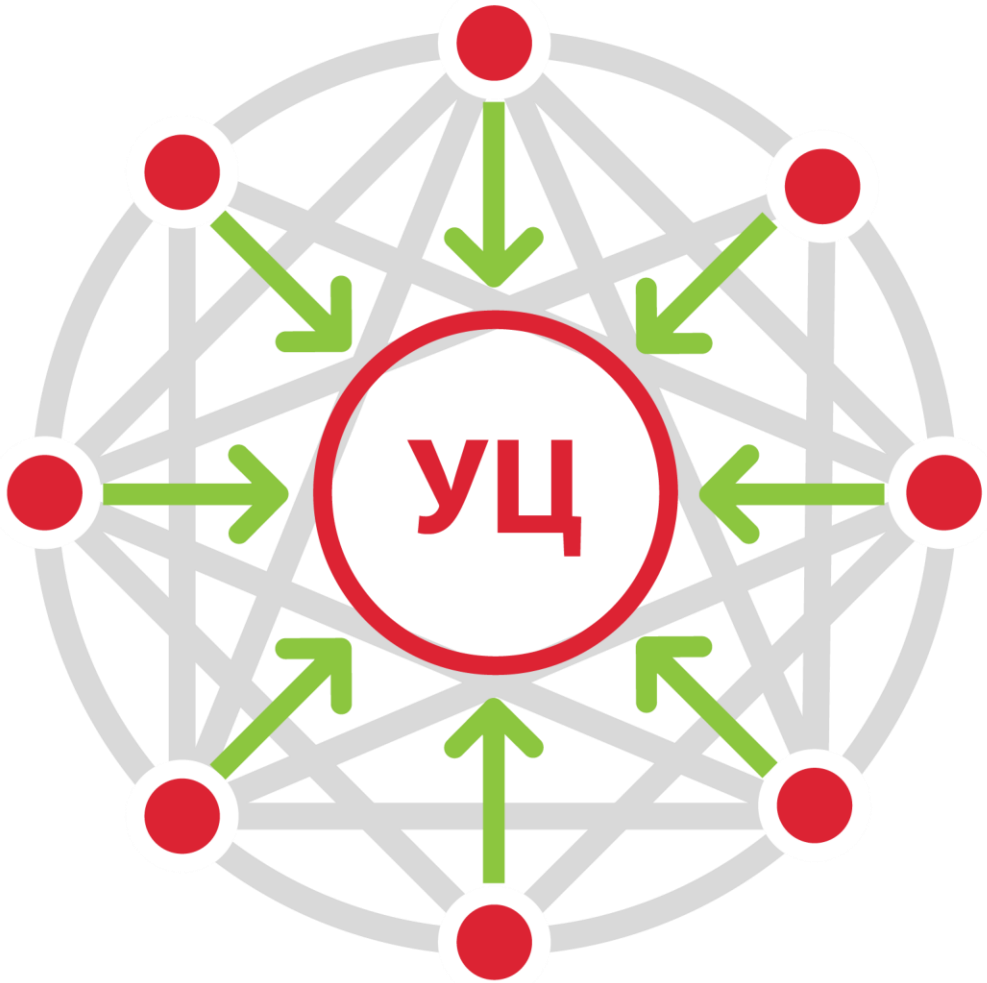
Что получилось?



Нужен ли PKI?

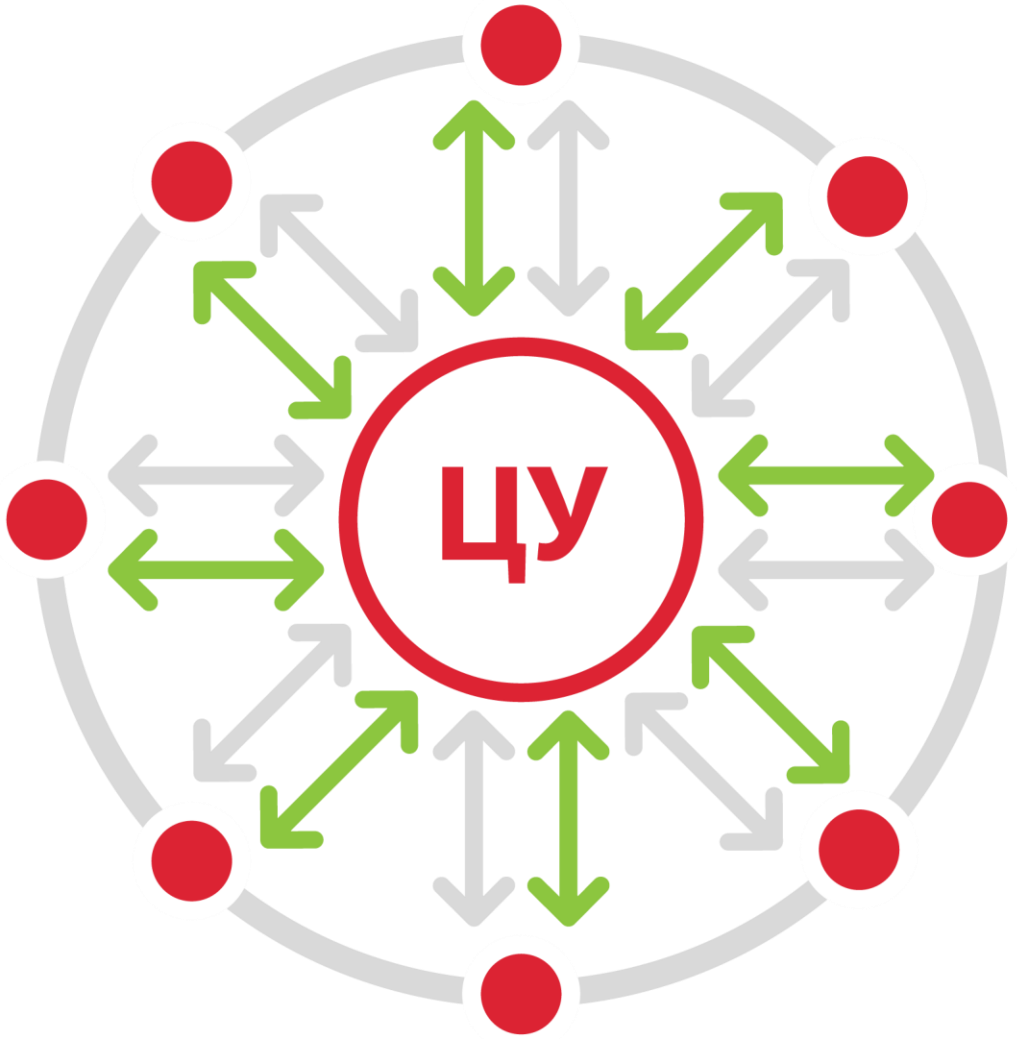
- Абоненты не доверяют друг другу
- Абоненты доверяют удостоверяющему центру
- Доверие обеспечивается за счет доверенной третьей стороны

Не наш случай! PKI не нужен!



Другая модель доверия

- Абонентам не нужно доверять друг другу
- Абоненты доверяют центру управления
- Коммуникации между абонентом и центром управления



Почему еще здесь не нужен PKI?

- Громоздкие ресурсоемкие библиотеки
- Большое количество зависимостей
- Громоздкие форматы данных
- Необходимость сервисов типа CRL и OCSP

Что будем использовать?

- «Сырая» подпись для имитозащиты и аутентификации
- «Белые списки» открытых ключей
- Имитозащита на основе HMAC или имитовставки
- Аппаратное шифрование ГОСТ 28147-89 на хранимых ключах или по VKO GOST
- Защита от replay-атак на основе меток времени от GPS/ГЛОНАСС и счетчиков

Чем хорош аппаратный модуль на базе Рутокен ЭЦП 2.0?

- Отлаженная серийная платформа
- Наличие USB (USB CCID) и UART интерфейсов
- Программный интерфейс APDU по ISO-7816
- Высокая надежность
- Высокая производительность
- Стройная понятная архитектура, удобная для разработчика
- Универсальность и кроссплатформенность программного обеспечения Рутокен
- Квалифицированная техподдержка
- Понятные перспективы сертификации

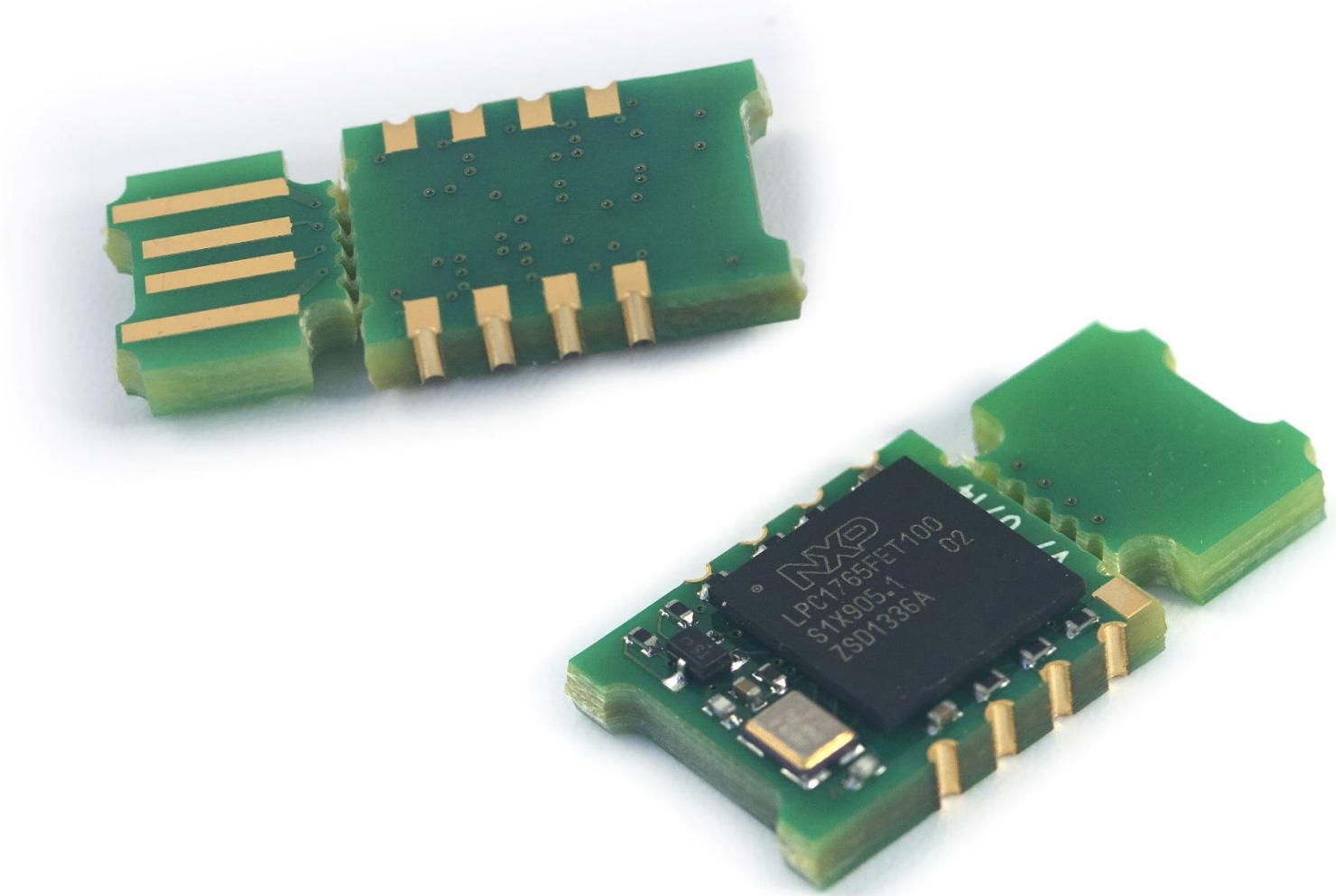
Развитие продукта!

- Новые интерфейсы
  - UART с максимальной скоростью до 8 Мбит/секунду
  - USB 2.0 с максимальной скоростью 480 Мбит/секунду
  - SPI с максимальной скоростью 25 Мбит/секунду
  - Параллельный интерфейс с максимальной теоретической скоростью до 80 Мбит/секунду
  - I^2C с максимальной скоростью до 1 Мбит/секунду

- Повышение производительности
  - 1,25 Мбайт/секунду хэширование на старых ГОСТ-ах
  - Шифрование на старых ГОСТ-а х в режиме гаммирования 2,1 Мбайт/секунду
  - Шифрование на старых ГОСТ-а х в режиме ECB 2,4 Мбайт/секунду

Возможные области применения

- Объекты критической инфраструктуры
- Телеметрические комплексы
- Системы фото- видео-фиксации и наблюдения
- Обеспечение сохранности грузов
- Мониторинг перевозки опасных грузов
- Детектирование выбросов/утечек опасных или загрязняющих веществ
- Контроль удаленных объектов


NXP
LPC1765FET100
S1X905.1
ZSD1336A
02

Вопросы