Разработка устройства для доверенного сеанса связи: S-Terra СПДС-USB-01

Заказчик

Компания «С-Терра СиЭсПи» — российский разработчик и производитель средств сетевой информационной безопасности. Решения компании для построения виртуальных частных сетей (VPN) обеспечивают защиту межсетевых взаимодействий, беспроводных и мультисервисных сетей, гарантируют безопасность работы удаленных и мобильных пользователей.

Задача

Разработать и подготовить к постановке на производство специальный загрузочный носитель (далее — СЗН) СПДС-USB-01, который представляет собой USB-устройство для построения среды доверенного сеанса в рамках системы С-Терра «Пост»: http://www.s-terra.ru/products/catalog/s-terra-post/

СПДС-USB-01 должен предоставлять следующие возможности:

- Доступ к криптографическому контроллеру, работающему по стандарту ISO-7816-3
- Доступ к носителю данных посредством интерфейса USB Mass Storage
- Управление доступом к разделам на носителе данных в зависимости от результатов аутентификации
- Возможность загрузки IBM ПК-совместимых компьютеров с устройства

– Скорость передачи данных по USB на уровне флеш-накопителей мировых производителей

Необходимо разработать библиотеку для предоставления программисту API управлением устройством через USB CCID в операционной системе Linux. Также требуется разработать комплекс программного обеспечения, которое будет выполняться на контроллере и на ПК. ПК должен проводить постпроизводственное тестирование и начальную инициализацию устройства: создание паролей и прав, запись образов операционной системы в устройство.

Решение

1. Аппаратное обеспечение

За основу программного обеспечения были взята библиотека AT91LIB компании Atmel. Решение было построено на основе чипа с процессором ARM Cortex M3.

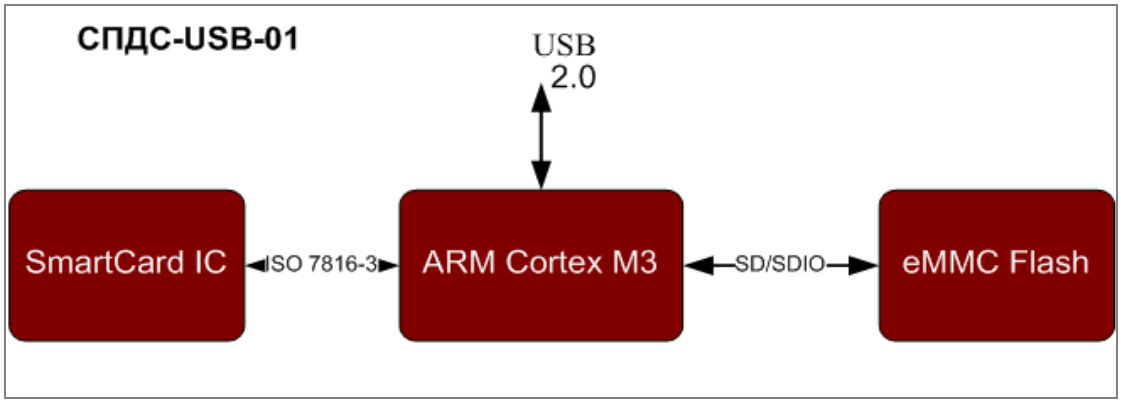

Рис.1. Структурная схема устройства

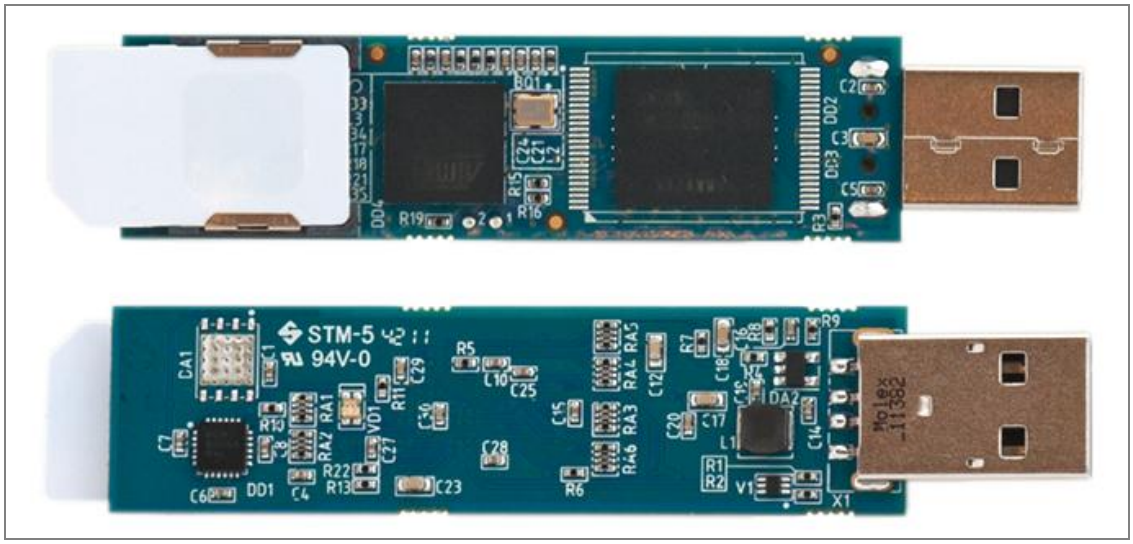

Рис.2. Аппаратная платформа устройства

2. Программное обеспечение

С учетом требований заказчика была разработана следующая архитектура реализации ПО:

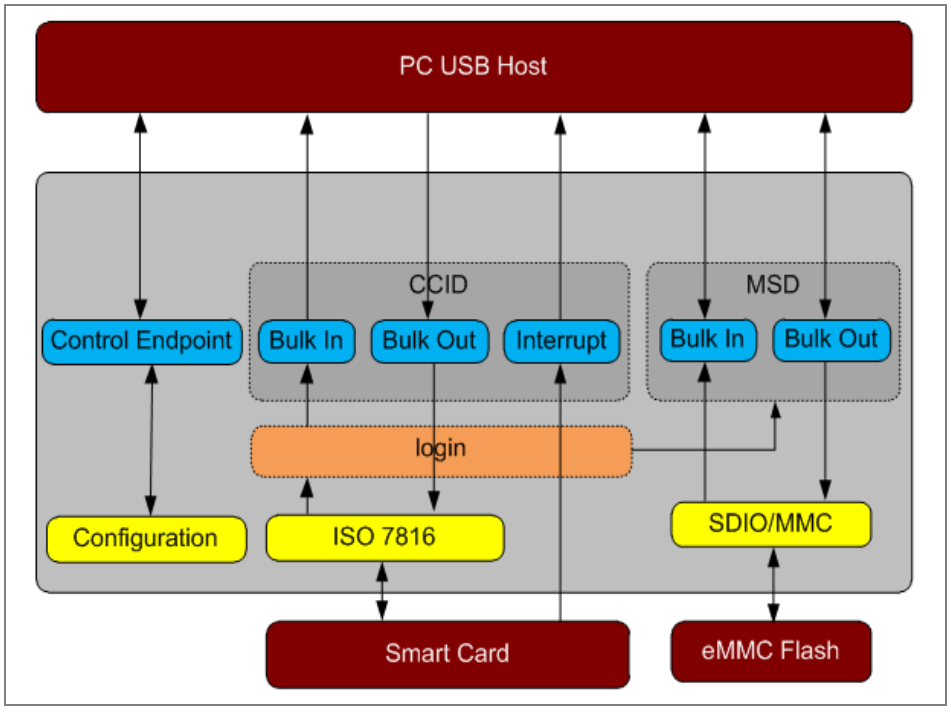

Рис.2. Архитектура ПО

Основные модули ПО:

1. USB CCID предоставляет доступ к смарт-карте (смарт-чипу) через интерфейс ISO7816.
2. USB MSD предоставляет доступ к содержимому eMMC согласно правам пользователя, который авторизовался через USB CCID.
3. Login проверяет ответы смарт-карты по интерфейсу ISO7816 и в соответствии с ними выставляет права на доступ к данным в MSD-инфраструктуре.

Для инициализации устройства была использована операционная система Debian 6.0, библиотеки usblib и libsysfs. На их основе были разработаны три библиотеки:

1. libinitsbs предоставляет функции авторизации и записи данных в устройство.
2. libsbs предоставляет функции общения со смарт-картой (сброс, создание файловой системы, создание пользователя, авторизация, удаление пользователя, блокировка и др.).
3. Библиотека libsysfsdev.

Преимущества

- Принципиально новая технология (среда построения доверенного сеанса, СПДС), которая лежит в основе работы устройства, позволяет отказаться от дорогостоящих и сложных в эксплуатации пакетов защиты типа security suite, NAC, DLP и др.
- Данные на устройстве защищены крипто-чипом (смарт-картой): пользователь проходит строгую двухфакторную аутентификацию, реализована криптографическая защита трафика и данных
- Устройство обеспечивает изолированное сетевое соединение с сервером приложений и доверенную загрузку целостной информационной среды
- Операционную систему можно загружать напрямую с устройства
- Продукты защиты сертифицированы ФСТЭК России и ФСБ России