

Программа для ЭВМ «АРМ Инициализации для Рутокен TLS»

Описание функций

В данном документе представлено описание функциональных характеристик программного обеспечения и информация, необходимая для установки и эксплуатации программного обеспечения.

1. Описание «АРМ Инициализации для Рутокен TLS»

Программа для ЭВМ «АРМ Инициализации для Рутокен TLS» — это программное обеспечение с графическим интерфейсом, предназначенное для подготовки к использованию и для администрирования устройств семейства Рутокен TLS (далее – Приложение).

Приложение при работе может работать параллельно с несколькими подключенными устройствами Рутокен TLS, подготавливая их к работе путем выполнения следующих действий:

- Обнаружение подключенных устройств Рутокен TLS;
- Форматирование (приведение в начальное состояние);
- Импортирование доверенных PKI-объектов на устройство;
- Импортирование служебной информации для установления TLS-соединения;
- Генерация служебных ключей и импорт соответствующих сертификатов открытых ключей на устройства;
- Импортирование одобренных образов прикладного программного обеспечения;
- Генерация и печать случайных PIN- и PUK-кодов;

Дополнительно, Приложение позволяет:

- Подготавливать токен Администратора АРМ;
- Обновлять образы одобренного программного обеспечения на Рутокен TLS без инициализации.

2. Установка

Для работы Приложения требуется подключение к базе данных (далее – БД). В составе Приложения поставляется сценарий для разворачивания БД (*create_db.sql*). Для разворачивания БД следует использовать указанный сценарий в СУБД.

В конфигурационном файле Приложения (*settings.ini*) следует указать учетные данные для подключения Приложения к БД в соответствующем разделе (*Database*):

[Database]

ConnectionString="Server=FQDN_Database;Database=DatabaseName;Uid=UserName;Pwd=UserPassword;"

Для инициализации устройств требуются:

- Подключение к БД;
- Подключенный токен Администратора АРМ.

3. Эксплуатация

3.1. Запуск

Для запуска приложения «АРМ Инициализации для Рутокен TLS» требуется запустить исполняемый файл *arminit*.

3.2 Доступные функции

3.2.1 Индикация подключенных устройств

При подключении устройств Рутокен TLS автоматически изменяется индикация подключенных готовых к инициализации устройств.

3.2.2 Настройка принтера

Программа для ЭВМ «АРМ Инициализации для Рутокен TLS» позволяет настраивать принтеры. Поддерживаются как аппаратные, так и виртуальные принтеры.

3.2.3 Подготовка токена Администратора АРМ

Программа для ЭВМ «АРМ Инициализации для Рутокен TLS» позволяет подготавливать токен Администратора АРМ.

3.2.4. Обновление образов доверенного программного обеспечения Рутокен TLS без инициализации

Программа для ЭВМ «АРМ Инициализации для Рутокен TLS» позволяет обновлять образы доверенного программного обеспечения Рутокен TLS без инициализации.

3.2.5. Сохранение информации о проинициализированных устройствах Рутокен TLS в БД.

Программа для ЭВМ «АРМ Инициализации для Рутокен TLS» позволяет сохранять информацию о проинициализированных устройства Рутокен TLS в БД.

3.2.6. Логирование операций в файл лога

Программа для ЭВМ «АРМ Инициализации для Рутокен TLS» позволяет логировать операции в файл лога.

3.3 Инициализация подключенных устройств Рутокен TLS

3.3.1 Выбор режима инициализации

Программа для ЭВМ «АРМ Инициализации для Рутокен TLS» позволяет выбирать режим инициализации подключенных устройств Рутокен TLS. Поддерживаются частичная и полная инициализации.

3.3.2 Выбор количества профилей на инициализируемых устройствах

Программа для ЭВМ «АРМ Инициализации для Рутокен TLS» позволяет выбирать количество профилей, создаваемых на инициализируемых устройствах Рутокен TLS. Поддерживается от одного до пяти профилей на одном устройстве.

3.3.3 Выбор импортируемых доверенных сертификатов корневых удостоверяющих центров

Программа для ЭВМ «АРМ Инициализации для Рутокен TLS» позволяет выбирать доверенные сертификаты корневых удостоверяющих центров для импорта на устройство. Поддерживаются сертификаты, закодированные в форматы DER и BASE64 (PEM) в соответствии со стандартом x.509 (RFC5280).

3.3.4 Выбор импортируемых одобренных образов программного обеспечения

Программа для ЭВМ «АРМ Инициализации для Рутокен TLS» позволяет выбирать одобренные образы программного обеспечения для импорта на устройство. Поддерживается до четырех импортируемых образов.

3.3.5 Выбор импортируемых сертификатов промежуточных удостоверяющих центров

Программа для ЭВМ «АРМ Инициализации для Рутокен TLS» позволяет выбирать сертификаты промежуточных удостоверяющих центров для импорта. Поддерживаются сертификаты, закодированные в форматы DER и BASE64 (PEM) в соответствии со стандартом x.509 (RFC5280). Для таких сертификатов должны строиться цепочки доверия, заканчивающиеся на импортируемых доверенных сертификатах корневых удостоверяющих центров.

3.3.6 Выбор импортируемых списков отозванных сертификатов (CRL)

Программа для ЭВМ «АРМ Инициализации для Рутокен TLS» позволяет выбирать списки отозванных сертификатов (CRL) для импорта. Поддерживаются списки, сформированные в соответствии со стандартом x.509 (RFC5280). Каждый CRL должен быть выпущен удостоверяющим центром, сертификат которого импортирован на устройство Рутокен TLS. Indirect CRL не поддерживаются.

3.3.7 Выбор или создание импортируемого списка реквизитов доверенных TLS-серверов

Программа для ЭВМ «АРМ Инициализации для Рутокен TLS» позволяет выбирать или создавать список реквизитов доверенных TLS-серверов для импорта. Поддерживаются CMS-конверты, сформированные в соответствии со стандартом CMS (RFC5652).

Формат данных для кодирования в CMS-конверт должен быть следующим:

ICMSC

Отображаемое имя №1;URI Web-ресурса для SNI №1;Доменное имя или IP-адрес TLS-сервера №1;Параметр видимости;Параметр интерфейса;

...

Отображаемое имя №N;URI Web-ресурса для SNI №N;Доменное имя или IP-адрес TLS-сервера №N;Параметр видимости;Параметр интерфейса;

Каждая строка должна заканчиваться последовательностью CRLF.

4. Удаление

Для удаления Приложения требуется удалить файлы Приложения и БД из файловой системы компьютера.