



SmartCard-Service

Акционерное общество «СмартКарт-Сервис»

127106, г. Москва, Алтуфьевское шоссе, д. 1

Телефон: +7 (495) 981-12-10, 8 (800) 100-31-64, факс: +7 (495) 981-12-11

E-mail: reception@scserv.ru, site: www.scserv.ru

Автоматизированное рабочее место инициализации криптомодулей «АРМ Инициализации»

Функциональное описание

Редакция 1

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ	3
Условные обозначения и сокращения.....	3
2. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ	4
2.1. Назначение и функциональные возможности АРМ.....	4
2.2. Необходимые технические и программные средства.....	4

1. ВВЕДЕНИЕ

Настоящее руководство предназначено для системных программистов и администраторов, ответственных за установку, настройку и проверку работоспособности программного обеспечения «АРМ Инициализации». Документ содержит сведения о функциональных возможностях программы и требованиях к аппаратному и программному окружению.

Программно-аппаратный комплекс (ПАК) «Инициализация ITSM» предназначен для выполнения базовой (первичной) инициализации криптомодулей типа СКЗИ ITSM в исполнении ИМ05-ITSM-B. Комплекс состоит из программного обеспечения «АРМ Инициализации» и аппаратного стенда, обеспечивающего одновременное подключение до 50 криптомодулей.

Условные обозначения и сокращения

Сокращение	Расшифровка
АРМ	Автоматизированное рабочее место
ПАК	Программно-аппаратный комплекс
СКЗИ	Средство криптографической защиты информации
УЦ	Удостоверяющий центр
CSR	Certificate Signing Request (Запрос на подпись сертификата)
DN	Distinguished Name (Отличительное имя)
OID	Object Identifier (Идентификатор объекта)
GUI	Graphical User Interface (Графический пользовательский интерфейс)

2. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

2.1. Назначение и функциональные возможности АРМ

АРМ Инициализации представляет собой программное средство с графическим пользовательским интерфейсом, разработанное для управления процессом инициализации криптомодулей. Все операции выполняются в защищенной среде, известной как «белая комната», для обеспечения безопасности и целостности криптографических операций.

Основные функциональные возможности программы включают:

- **Пакетная инициализация:** Одновременная работа с пакетом до 50 криптомодулей, подключенных к стенду.
- **Генерация ключей и запросов на сертификат (CSR):** Создание ключевых пар и формирование запросов на выпуск сертификатов непосредственно внутри криптомодулей.
- **Подписание CSR:** Использование ключа оператора, хранящегося на защищенном USB-токене JaCarta, для подписи сгенерированных запросов.
- **Загрузка сертификатов:** Загрузка в криптомодули корневых сертификатов Удостоверяющего центра и списков отозванных сертификатов.
- **Формирование отчетов:** Создание кратких и подробных отчетов по результатам каждой сессии инициализации для последующего анализа и аудита.
- **Запись в хранилище:** Сохранение в хранилище подписанных запросов на выпуск сертификатов и сертификата шифрования.
- **Повторная инициализация:** Возможность выборочной повторной инициализации криптомодулей, в которых произошел сбой.
- **Автоматизация:** Поддержка выполнения пользовательских сценариев (скриптов) до и после основного процесса инициализации.

2.2. Необходимые технические и программные средства

Для корректной работы АРМ Инициализации рабочая станция и окружение должны соответствовать следующим требованиям.

Компонент	Требование
Операционная система	Windows 10 или выше
Среда выполнения	.NET Runtime 8.0 или выше
Криптопровайдер	КриптоПро CSP 5.0 (рекомендуется последняя версия)
Утилиты	OpenSSL (openssl.exe)
USB-токен	JaCarta (для хранения ключа оператора)
ПО для токена	Единый клиент JaCarta
Драйверы	Специализированный драйвер для криптомодулей ИМ05-ITSM-B
Аппаратное обеспечение	Стенд инициализации (USB-хабы, с внешним питанием, обеспечивающие подключение для портов)