



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»

Руководство по установке и настройке

Редакция 1

Москва
2026

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ.....	3
Условные обозначения и сокращения	3
2. УСТАНОВКА ПРОГРАММЫ.....	4
2.1. Состав дистрибутива	4
2.2. Подготовка к установке.....	4
2.3. Порядок развертывания АРМ	5
3. НАСТРОЙКА ПРОГРАММЫ	6
3.1. Аппаратная настройка стенда инициализации	6
3.2. Настройка параметров приложения	6
3.3. Настройка сессионных параметров.....	7
3.4. Работа с сертификатами	8

1. ВВЕДЕНИЕ

Настоящее руководство предназначено для системных программистов и администраторов, ответственных за установку, настройку и проверку работоспособности программного обеспечения «АРМ Инициализации». Документ содержит пошаговые инструкции по развертыванию и конфигурированию.

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. УСТАНОВКА ПРОГРАММЫ

Процесс установки АРМ Инициализации не требует запуска специализированного инсталлятора и заключается в подготовке системного окружения и копировании файлов программы на рабочую станцию.

2.1. Состав дистрибутива

Дистрибутив АРМ Инициализации поставляется в виде набора файлов и каталогов, содержащих все необходимые для работы компоненты. Основные элементы дистрибутива:

- Исполняемый файл программы (например, ArmInitialization.exe).
- Файлы конфигурации.
- Необходимые библиотеки (DLL), включая библиотеку для работы с модулем «Криптон».

2.2. Подготовка к установке

Перед развертыванием АРМ необходимо убедиться, что на рабочей станции установлено все требуемое программное обеспечение. Установку следует производить с правами администратора.

1. **Установка .NET Runtime:** Загрузите и установите среду выполнения .NET 8.0 (или более позднюю версию) с официального сайта Microsoft.
2. **Установка КриптоПро CSP:** Установите КриптоПро CSP версии 5.0. В процессе установки убедитесь, что выбраны компоненты, включающие утилиты csptest.exe и certmgr.exe. Дополнительно скачайте из личного кабинета КриптоПро и скопируйте утилиту cryptcp.x64.exe в каталог установки КриптоПро CSP (обычно C:\Program Files\Crypto Pro\CSP\).
3. **Установка OpenSSL:** Установите дистрибутив OpenSSL, убедившись, что путь к исполняемому файлу openssl.exe будет доступен для программы.
4. **Установка «Единый клиент JaCarta»:** Установите программное обеспечение «Единый клиент JaCarta» для обеспечения корректной работы с USB-токеном оператора.
5. **Установка драйвера криптомодуля:** Установите специализированный драйвер для криптомодулей ИМ05-ITSM-B. **Это обязательный шаг**, без которого операционная система не сможет распознать подключаемые криптомодули как USB-устройства.

2.3. Порядок развертывания АРМ

Развертывание программы выполняется путем простого копирования файлов.

1. Создайте на локальном диске рабочей станции каталог для размещения программы (например, C:\ARM_Init\).
2. Скопируйте все файлы и каталоги из дистрибутива в созданный каталог.
3. Для удобства запуска создайте на рабочем столе ярлык для исполняемого файла ArmInitialization.exe.

После выполнения этих действий программа готова к первому запуску и настройке. При первом запуске, если файлы конфигурации отсутствуют, АРМ автоматически создаст их со значениями по умолчанию.

3. НАСТРОЙКА ПРОГРАММЫ

Настройка APM Инициализации включает в себя как аппаратную подготовку стенда, так и конфигурирование самого программного обеспечения. Корректная настройка является ключевым условием для успешной и стабильной работы комплекса.

3.1. Аппаратная настройка стенда инициализации

Стенд инициализации состоит из USB-хабов, которые позволяют в совокупности подключить до 50 криптомодулей. Для обеспечения стабильной идентификации каждого устройства необходимо выполнить процедуру **локализации слотов**.

***Важно:** Все USB-хабы должны быть подключены к соответствующим USB-портам рабочей станции **до загрузки операционной системы**. В противном случае ранее настроенная схема расположения слотов может быть нарушена, что потребует повторной локализации.*

Процедура локализации слотов выполняется в настройках приложения и заключается в привязке каждого физического USB-порта на хабах к определенной позиции на графической схеме в главном окне программы. Это позволяет однозначно идентифицировать криптомодуль, в котором произошла ошибка в процессе инициализации. Рекомендуется физически промаркировать хабы и кабели для сохранения порядка подключения.

3.2. Настройка параметров приложения

Параметры приложения являются постоянными (консервативными) и сохраняются между сеансами работы. Доступ к ним осуществляется через соответствующий раздел меню в интерфейсе программы. При первом запуске создаются настройки по умолчанию, которые необходимо отредактировать.

Параметр	Описание
Пути к утилитам	Указываются полные пути к исполняемым файлам криптоутилит: csptest.exe, certmgr.exe, cryptcp.x64.exe (КриптоПро) и openssl.exe (OpenSSL).

Путь к архиватору	Задается путь к утилите-архиватору, используемой для создания пакетов инициализации.
Шаблон имени архива	Определяет маску для имен файлов архивных пакетов.
Ключ инициализации (DN)	Отличительное имя (Distinguished Name) сертификата, используемого для подписи.
Локализация слотов	Интерфейс для выполнения привязки физических USB-портов к графической схеме.

3.3. Настройка сессионных параметров

Сессионные (динамические) параметры задаются перед каждым сеансом инициализации и определяют специфику конкретной операции. Окно настройки состоит из нескольких вкладок.

1. Папки и файлы:

- **Пути к сертификатам:** Указываются каталоги, содержащие файлы корневых сертификатов, сертификатов УЦ и списков отозванных сертификатов (CRL). Если каталог пуст, соответствующие сертификаты не загружаются.
- **Путь к скриптам:** Каталог со сценариями, которые могут выполняться до или после инициализации.
- **Доверяемые OID:** Строка с идентификаторами объектов (OID), которые будут добавлены в сертификат.

2. Параметры ключей:

- **Номер и тип ключа:** Задаются KeyNumber (0-255) и KeyType (2 или 3, по умолчанию 3).
- **Использование ключа:** Определяются параметры Key Usage и Enhanced Key Usage, а также их критичность.
- **Пользовательские расширения:** Строка с кастомными расширениями, передаваемая банком.
- **Источник гаммы:** Выбирается источник случайных данных для генерации ключей — либо **внешний файл**, либо аппаратный генератор «Криптон».

3. Параметры CSR:

- **DN генерируемого сертификата:** Задается маска для формирования отличительного имени (DN) сертификата, которая может включать макрос для подстановки серийного номера устройства.

- **Пароль контейнера оператора:** Вводится пароль для доступа к закрытому ключу оператора на токене JaCarta. Этот пароль **не сохраняется** и должен вводиться при каждом сеансе.
- **DN подписывающего сертификата:** Отличительное имя сертификата оператора, который будет использован для подписи CSR.

4. Выбор криптомодулей:

- На этой вкладке отображается список всех подключенных и распознанных криптомодулей. Оператор может выбрать все модули или только некоторые из них для проведения инициализации.

3.4. Работа с сертификатами

Для выполнения операций APM требует наличия нескольких типов сертификатов:

- **Сертификат оператора:** Закрытый ключ и сертификат находятся на USB-токене JaCarta. Сертификат должен быть импортирован в хранилище сертификатов Windows на рабочей станции с помощью «Единого клиента JaCarta» и утилит КриптоПро.
- **Сертификат инициализации:** Должен быть заранее импортирован в хранилище сертификатов «Личные» на локальном компьютере.
- **Сертификаты УЦ:** Корневые и промежуточные сертификаты Удостоверяющего центра, а также списки отозванных сертификатов (CRL) предоставляются банком и должны быть размещены в каталогах, указанных в сессионных настройках.