



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

Утверждаю

Генеральный директор

АО «СмартКарт-Сервис»

_____ В.А. Васильев

«_____» _____ 20____ г.

Удостоверяющий центр CA.RUS

Руководство пользователя (ca-center)

Москва

2024

Оглавление

Руководство пользователя (ca-center).....	1
1. Настройка конфигурационного файла ПО сервера, рабочих станций и дополнительных утилит3	
1.1. Настройка конфигурационного файла ПО сервера	3
1.2. Настройка конфигурационного файла ПО рабочих станций	4
1.3. Настройка конфигурационного файла ПО дополнительных утилит	5
2. Описание работы ПО сервера	5
2.1. Режим генерации RSA ключей в HSM	5
2.2. Режим загрузки RSA ключей в HSM и БД.....	6
2.3. Режим инициализации журнала аудита.....	6
2.4. Режим генерации сертификатов CA для загрузки в EPP	6
2.5. Режим сервера (основной)	6
3. Описание работы ПО рабочих станций	7
3.1. Пользовательский интерфейс	7
4. Описание работы ПО дополнительных утилит	8
4.1. Режим создания штрих-кода CSR хоста	8
4.2. Режим считывания штрих-кода с результатом подписи сертификата хоста	8
4.3. Режим считывания идентификатора карты с отображением на экран.....	8

1. Настройка конфигурационного файла ПО сервера, рабочих станций и дополнительных утилит

Перед началом работы необходимо настроить конфигурационный файл приложения на каждой машине, использующей компоненты приложения (сервер, рабочая станция).

Настройка состоит из общей настройки (предназначенной для обеспечения корректного взаимодействия между компонентами системы администратором), и тонкой настройки (предназначенной для управления доступным функционалом системы).

Внимание!

Тонкую настройку не рекомендуется выполнять без консультаций или непосредственного участия разработчика системы.

ПО поставляется с конфигурационным файлом «по умолчанию», который требуется поменять в соответствии с нуждами развертывания системы.

Также посмотреть пример конфигурационного файла с комментариями о назначении и допустимых значениях каждого поля можно в файле «app.config-descr.json».

Внимание!

Обращаем внимание, что формат файла с комментариями не может быть обработан ПО и представлен только для информации.

1.1. Настройка конфигурационного файла ПО сервера

1.1.1. Общая настройка конфигурационного файла ПО сервера

Необходимо актуализировать следующие поля для персонализации системы и обеспечения ее связности:

- Все значения в секциях [cert_subject](#), вложенных в секцию [key_load](#) – это описывает информацию, содержащуюся в сертификатах данного СА.
- [hsm/server_connection/endpoints](#) – список одновременно используемых HSM (используется первый, если не успешно – выполняется переход к следующему). Здесь необходимо указать тип ([type](#)), ip-адрес ([ipAddress](#)) и порт ([port](#)) HSM устройств.

При необходимости можно изменить следующие поля на усмотрение администратора:

- [ca-srzd/log/path](#) – путь записи логов системы.
- [ca-srzd/database/root](#) – путь хранения базы данных системы.
- [ca-srzd/server/port](#) – tcp/ip порт сервера (должен совпадать с портами сервера настроенным на рабочих станциях).
- Все значения [duration_years](#) – длительность действия выпускаемого сертификата.
- Все значения [expiry_date](#) – дата окончания выпускаемого сертификата для загрузки в EPP.
- Все пути к файлам в секции [key_generation](#) (должны совпадать с путями в секции [key_load](#)).
- Все пути к файлам в секции [key_load](#) (должны совпадать с путями в секции [key_generation](#)).

Внимание!

Не рекомендуется менять остальные поля без консультации с разработчиком системы.

1.1.2. Тонкая настройка конфигурационного файла ПО сервера

Тонкая настройка проводится посредством консультаций или непосредственного участия разработчика системы.

1.2. Настройка конфигурационного файла ПО рабочих станций

1.2.1. Общая настройка конфигурационного файла ПО рабочих станций

Необходимо актуализировать следующие поля для персонализации системы и обеспечения ее связности:

- [ca-awsd/server_connection/ipAddress](#) – ip-адрес машины сервера.
- Все значения в секции [channels](#) для всех типов ерр-клавиатур в секции [ca-awsd/epp/epp_config](#). Необходимо указать имя канала ерр в ОС ([name](#)), например «ttyUSB51». Имя должно быть постоянным при всех перезапусках ОС, для этого могут понадобиться соответствующие настройки в самой ОС. Имена не должны быть одинаковыми.
Общее число каналов должно быть от одного до 8 включительно.
- [ca-awsd/printer/external_print_args_mask_linux](#) – команда для отправки pdf-документа на печать. В данной команде не рекомендуется менять ничего кроме имени принтера, также можно указать печать на принтер «по умолчанию».

При необходимости можно изменить следующие поля на усмотрение администратора:

- [ca-awsd/log/path](#) – путь записи логов системы.
- [ca-awsd/server_connection/port](#) – tcp/ip порт сервера (должен совпадать с портом сервера настроенным на сервере).
- [ca-awsd/http-server/port](#) – tcp/ip порт ННТР сервера пользовательского интерфейса (должен совпадать с портом ННТР-сервера при запуске web-браузера).
- [ca-awsd/printer/temp_dir](#) – путь записи промежуточных файлов для печати.
- [ca-awsd/authenticator/enabled](#) – указывает использовать ли устройство авторизации доступа. Если нет – доступ разрешен всегда. Если есть – доступ разрешен, если в устройстве присутствует идентификатор (например, карта доступа) авторизованного пользователя.
- [ca-awsd/authenticator/allow_shutdown_when_authenticator_disabled](#) – актуально, если устройство авторизации доступа не используется. Указывает, активна ли кнопка выключения ПК рабочей станции.
- [ca-awsd/authenticator/allow_shutdown_server_when_authenticator_disabled](#) – актуально, если устройство авторизации доступа не используется. Указывает, активна ли кнопка выключения ПК сервера.
- [ca-awsd/authenticator/authorized_ids](#) – актуально, если используется устройство авторизации доступа. Указывает список строковых номеров идентификаторов (например, карт доступа), которым доступны основные операции на рабочей станции.
Для определения идентификатора карты можно воспользоваться специальной командой [-readcardid](#) ПО дополнительных утилит (ca-utils).
- [ca-awsd/authenticator/authorized_ids_shutdown](#) – актуально, если используется устройство авторизации доступа. Указывает список строковых номеров идентификаторов (например, карт доступа), которым доступна кнопка выключения ПО рабочей станции.
Для определения идентификатора карты можно воспользоваться специальной командой [-readcardid](#) ПО дополнительных утилит (ca-utils).

- `ca-awsd/authenticator/authorized_ids_shutdown_server` – актуально, если используется устройство авторизации доступа. Указывает список строковых номеров идентификаторов (например, карт доступа), которым доступна кнопка выключения ПО сервера. Для определения идентификатора карты можно воспользоваться специальной командой `-readcardid` ПО дополнительных утилит (`ca-utils`).

Внимание!

Не рекомендуется менять остальные поля без консультации с разработчиком системы.

1.2.2. Тонкая настройка конфигурационного файла ПО рабочих станций

Тонкая настройка проводится посредством консультаций или непосредственного участия разработчика системы.

1.3. Настройка конфигурационного файла ПО дополнительных утилит

1.3.1. Общая настройка конфигурационного файла ПО дополнительных утилит

При необходимости можно изменить следующие поля на усмотрение администратора:

- `ca-utils/log/path` – путь записи логов системы.
- `ca-utils/read_barcode/default_out_path` – путь записи считанных штрих-кодов по умолчанию, если не указан в параметрах команды.
- `ca-utils/gen_barcode/default_out_pathname` – путь и имя файла сгенерированного изображения штрих-кода по умолчанию, если не указан в параметрах команды.

Внимание!

Не рекомендуется менять остальные поля без консультации с разработчиком системы.

1.3.2. Тонкая настройка конфигурационного файла ПО дополнительных утилит

Тонкая настройка проводится посредством консультаций или непосредственного участия разработчика системы.

2. Описание работы ПО сервера

Перед началом работы проводится конфигурация ПО.

Далее ПО сервера может быть запущено в одном из пяти режимов:

- режим генерации RSA ключей в HSM;
- режим загрузки RSA ключей в HSM и БД;
- режим инициализации журнала аудита;
- режим генерации сертификатов CA для загрузки в EPP;
- режим сервера (основной).

2.1. Режим генерации RSA ключей в HSM

Данный режим активируется выполнением приложения сервера (`ca-srvd`) с параметром `-grsa`.

В данном режиме приложение сервера генерирует при помощи модуля HSM и сохраняет в файлы RSA ключи. Приватная часть ключей не секретная и зашифрована LMK модуля HSM.

Список и параметры ключей, которые требуется сгенерировать, указывается в конфигурации в секции [ca-srvd/key_generation](#).

Если файлы ключей уже существуют, файлы не будут перезаписаны и ПО завершится с ошибкой.

Возможен повторный запуск данного режима с другим набором ключей в конфигурации, если он не пересекается с уже существующими файлами ключей.

При первичном развертывании системы эта команда выполняется первой.

При восстановлении ПО, при наличии ранее созданных RSA ключей, эта команда не требуется.

2.2. Режим загрузки RSA ключей в HSM и БД

Данный режим активируется выполнением приложения сервера (ca-srvd) с параметром [-lrsa](#).

В данном режиме приложение сервера загружает в БД и в HSM-модули RSA ключи, созданные командой [-grsa](#) с использованием модуля HSM с тем же LMK.

Список и параметры ключей, которые требуется загрузить, указывается в конфигурации в секции [ca-srvd/key_load](#).

При первичном развертывании системы эта команда выполняется второй.

При восстановлении ПО, при наличии ранее созданных RSA ключей, эта команда выполняется первой.

В случае, если загружаемые данные уже присутствуют в БД, ПО завершится с ошибкой.

2.3. Режим инициализации журнала аудита

Данный режим активируется выполнением приложения сервера (ca-srvd) с параметром [-iauditjournal](#).

В данном режиме приложение сервера проверяет наличие журнала аудита и проверяет его на целостность, или создает журнал с нуля, если он не существует.

При первичном развертывании системы эта команда выполняется третьей.

При восстановлении ПО, при наличии ранее созданных RSA ключей, эта команда выполняется после команды [-lrsa](#).

В случае, если журнал аудита не находится в целостном состоянии или невозможно его проверить (требуется связь с HSM и ключи, загруженные в нем командой [-lrsa](#)), ПО завершится с ошибкой.

2.4. Режим генерации сертификатов СА для загрузки в EPP

Данный режим активируется выполнением приложения сервера (ca-srvd) с параметром [-geppcerts](#).

В данном режиме приложение сервера генерирует и подписывает сертификат, с использованием модуля HSM, для дальнейшей загрузки их в EPP-клавиатуру.

Список и параметры сертификатов, которые требуется сгенерировать, указывается в конфигурации в секции [ca-srvd/gen_epp_certs](#).

Эта команды выполняется после команды [-auditjournal](#).

В случае, если создаваемые сертификаты уже присутствуют в БД, ПО завершится с ошибкой.

2.5. Режим сервера (основной)

Данный режим активируется выполнением приложения сервера (ca-srvd) без параметров, или в режиме фонового процесса.

В данном режиме приложение сервера находится в режиме ожидания запросов от приложений рабочих станций и обрабатывает их.

Запуск ПО в данном режиме необходимо осуществлять только после начальной настройки системы (предварительно должны быть выполнены команды `-grsa` (по необходимости), `-lrsa`, `-auditjournal`, `-geppcerts`).

При поступлении запроса на подпись сертификата хоста приложение выдает рабочей станции подписанный сертификат хоста и подписанные сертификаты CA-центра, указанные в секции конфигурации `ca-srvd/bank_cert_signature` (для тестового (`test`) или промышленного (`production`) режима, в соответствии с параметрами запроса).

Для каждого хоста будут создаваться сертификаты с новыми серийными номерами.

При поступлении запроса на подпись сертификата ключа EPP-клавиатуры, приложение выдает рабочей станции подписанный сертификат EPP и подписанные сертификаты CA-центра, указанные в секции конфигурации `ca-srvd/epp_cert_signature` (для тестового (`test`) или промышленного (`production`) режима, в соответствии с параметрами запроса).

Для каждой EPP-клавиатуры будут создаваться сертификаты EPP с новыми серийными номерами и сертификаты CA-центра, ранее сгенерированные на этапе ввода ПО в эксплуатацию командой `-geppcerts`.

Таким образом, в EPP-клавиатуру загружаются сертификаты CA-центра с одинаковым серийным номером.

3. Описание работы ПО рабочих станций

Единственный режим работы приложения рабочей станции (`ca-awsd`) активируется выполнением приложения рабочей станции (`ca-awsd`) без параметров, или в режиме фонового процесса.

В данном режиме приложение рабочей станции находится в режиме ожидания запросов от пользовательского интерфейса, обрабатывает их, управляет подключенным оборудованием (таким как принтер, сканнер штрих-кодов, еpp-модули).

Пользователю отдельно демонстрируется режим, в котором находится приложение в текущий момент (промышленный/тестовый, авторизованный/не авторизованный).

Основные операции доступны в авторизованном режиме. Для выполнения дополнительных операций, таких как, например, выключение ПО рабочей станции и выключение ПО сервера могут потребоваться дополнительные полномочия, в соответствии с настройками и использованным идентификатором пользователя, если его использование включено в конфигурации.

Режим диагностики доступен всегда.

3.1. Пользовательский интерфейс

Пользовательский интерфейс отображается в полноэкранном режиме без возможности покинуть его и представлен следующими основными экранами взаимодействия:

- **Главное меню.** Здесь пользователь может выбрать задачу (подготовка EPP, подпись сертификата хоста, диагностика, перевод системы в тестовый или наоборот промышленный режим), а так же выполнить выключение ПО рабочей станции или ПО сервера.
- **Меню диагностики.** Здесь пользователь может проверить работоспособность подключенного оборудования и серверной части системы.
- **Меню подписи сертификата хоста.** Пользователю будет предложено выбрать тип требуемого сертификата (PKCS7, X.509), и поднести штрихкод с данными CSR банка в формате PEM. После успешного выполнения процедуры, автоматически будут распечатаны сгенерированные сертификаты. При необходимости повторить печать будет доступна кнопка повторной печати.
- **Меню подготовки EPP.** Пользователь сможет выбрать до 8 подключенных EPP любого типа для одновременной подготовки. Потребуется указать тип EPP-клавиатуры и канал,

на котором она подключена. Время исполнения каждой операции для EPP может сильно варьироваться и зависит от внутренних процессов работы EPP.

По завершении пользователь получит успешный статус операции и серийный номер успешно обработанной EPP.

Покинуть меню подготовки EPP можно только при отсутствии EPP в процессе обработки.

При покидании меню подготовки EPP и следующем входе в него – предыдущие статусы подготовки EPP сохраняются, что полезно при случайном выходе, когда не удалось запомнить серийные номера обработанных EPP.

4. Описание работы ПО дополнительных утилит

ПО дополнительных утилит (ca-utils) может быть запущено в следующих режимах:

- режим создания штрих-кода CSR хоста;
- режим считывания штрих-кода с результатом подписи сертификата хоста в файл;
- режим считывания идентификатора карты с отображением на экран.

4.1. Режим создания штрих-кода CSR хоста

Данный режим активируется выполнением приложения дополнительных утилит (ca-utils) с параметром `-gbarcode`.

Параметры данной команды имеют вид:

`-gbarcode [-infile:<input-file-pathname>] [-outfile:<output-file-pathname>]`

Если не указан параметр `- outfile`, то изображение штрих-кода сохраняется по пути и под именем по умолчанию (см. конфигурационный файл).

В данном режиме приложение дополнительных утилит считывает данные CSR хоста в формате PEM из входного файла (infile) и записывает в выходной файл (outfile) изображение штрих-кода с данными CSR в формате bmp для последующей печати его на принтере самостоятельно.

4.2. Режим считывания штрих-кода с результатом подписи сертификата хоста

Данный режим активируется выполнением приложения дополнительных утилит (ca-utils) с параметрами семейства `-rbarcode:<barcode-name>`.

Параметры данной команды имеют вид:

`-rbarcode [-file:<output-file-pathname>] <-type:<barcode-file-type>>`

Где тип формата файла штрих-кода (barcode-file-type) – один из списка:

- pem (предназначен для хранения сертификатов любого типа);
- cer (предназначен для хранения сертификатов типа x509);
- p7b (предназначен для хранения сертификатов типа PKCS#7).

Если не указан параметр `-file`, то штрих-код сохраняется под именем `YYYYMMDDHHMMSS.<расширение, зависящее от типа формата файла>` состоящим из даты и времени в путь по умолчанию (см. конфигурационный файл).

В данном режиме приложение дополнительных утилит предложит поднести штрих-код к считывателю и сохранит его данные в файл в требуемом формате.

Для отмены операции воспользуйтесь комбинацией (CTRL+C).

4.3. Режим считывания идентификатора карты с отображением на экран

Данный режим активируется выполнением приложения дополнительных утилит (ca-utils) с параметром `-readcardid`.

Параметры данной команды имеют вид:

`-readcardid`

В данном режиме приложение дополнительных утилит предложит приложить карту к считывателю начнет циклически считывать идентификатор карты и отображать его на экране, до завершения приложения (CTRL+C).