

САН (Certificate Authority Host)

Руководство пользователя

Версия САН 3.0.2

История изменений документа

Версия	Дата	Перечень изменений
1.0	29.08.2017	Первоначальная версия
1.1	25.09.2018	Добавлены пункты: «5»; «6» и «6.1»
1.2	03.04.2019	Изменена структура документа. Актуализированы пункты: «7»; «7.1»; «7.1.2»; «7.1.3». Добавлены пункты: «7.2»; «7.3»
1.3	23.10.2019	Добавлены пункты: «4»; «8.2». Актуализированы пункты: «7.1.2»; «7.1.3»; «7.1.3.1»; «7.2.1»; «7.2.1.1»; «7.2.1.2»; «7.2.2»; «8.1».
1.4	01.04.2020	Добавлены пункты: «6.2»

Содержание

1. Термины и определения	4
2. Введение	5
3. Краткое описание САН.....	6
4. Общая схема процесса обновления сертификатов	7
5. Вход/ выход в (из) системы.....	9
6. Создание пользователя	9
6.1. Удаление пользователя	10
6.2. Первый вход пользователя.....	11
7. Описание Web-интерфейса САН.....	12
7.1. Страница «General»	12
7.1.1. Статус состояния CAD	12
7.1.2. Взаимодействие с POS-терминалами	13
7.1.3. Работа с SAM-модулями	14
7.2. Страница «CAD and certificates»	16
7.2.1. Информация и инструменты для работы с CAD	16
7.2.2. Информация о сертификатах CAD	20
7.3. Страница «Settings»	22
8. Приложение	23
8.1. Файл ключей SAM-модулей.....	23
8.2. Коды ошибок САН.....	23

1. Термины и определения

CAH	(Certificate Authority Host) – сервер, обеспечивающий взаимодействие POS-терминала и CAD в процедуре начальной инициализации POS-терминала начальными сертификатами.
S/N	Серийный номер
SAM-модуль	Смарт-карта стандарта ISO 7816, используемая для генерации ключевых пар RSA для POS-терминала и заверения запроса на выпуск сертификата POS-терминала. Заверение (удостоверение) запроса осуществляется SAM-модулем путем вычисления MAC запроса. Расчет MAC выполняется на ключе, уникальном для каждого SAM-модуля; криптограммы ключей, зашифрованные на ZMK, загружаются в CAD для последующей проверки запросов на выдачу сертификатов POS-терминалу.
MAC-ключ SAM-модуля	MAC-ключ, используемый SAM-модулем для вычисления MAC запроса на выдачу сертификата публичного ключа POS-терминала.
POS-терминал	Электронное программно-техническое устройство, используемое для авторизации и проведения платежей по банковской карте.
CAD	Компонент УЗК. Представляет собой POS-терминал со специальным приложением, выполняющим функции удостоверяющего центра, выпускающего, перевыпускающего сертификаты публичных ключей POS терминалов.
КПХ	Касса-Пинпад-Хост. Режим работы POS-терминала, при котором взаимодействие POS-терминала с хостом (авторизации и другими) выполняется посредством собственных коммуникаций POS-терминала.
ПКХ	Пинпад-Касса-Хост. Режим работы POS-терминала, при котором взаимодействие POS-терминала с хостом (авторизации и другими) выполняется посредством коммуникаций ККМ.
ISL-сертификат	Сертификат, применяемый для установления защищенного соединения между POS-терминалом и подключенным к нему внешним пинпадом.
RKL-сертификат	Сертификат, применяемый для организации безопасной передачи ключей (мастер, KLK) из KDH в POS-терминал.
SSL-сертификат	Сертификат, применяемый для установления защищенного соединения между POS-терминалом и SSL-шлюзом.
Хэш сертификата	В отношении сертификата формата X.509 – расширение «Subject Key Identifier». В отношении ISL-сертификата – результат вычисления SHA-1 от сертификата.

2. Введение

Данный документ описывает web-интерфейс сервера САН и порядок работы с ним.

Данный документ предназначен для прочтения пользователем, осуществляющим работу с САН через web-интерфейс.

Данный документ не содержит информацию по установке, настройке и запуску сервера САН, а также требований к аппаратному и программному обеспечению.

3. Краткое описание CAN

CAN является программным продуктом, представляющим из себя сервер, обеспечивающий взаимодействие POS-терминала и CAD в процедуре начальной инициализации POS-терминала начальными сертификатами и удаленного обновления (выпуск, перевыпуск) сертификатов публичных ключей, хранящихся в POS-терминале.

Основные функции сервера CAN:

- Безопасное хранение криптограмм MAC-ключей SAM-модулей.
- Прием и обработка запросов, заверенных MAC-кодом, рассчитанным SAM-модулем, от POS-терминалов на выдачу сертификатов.
- Передача на CAD запроса на выдачу сертификата, MAC-кода запроса и криптограммы MAC-ключа SAM-модуля, найденной по S/N SAM-модуля.
- Прием от CAD и передача на POS-терминал двух сертификатов POS-терминала и сертификата CAD.

Взаимодействие пользователя с CAN осуществляется через web-интерфейс данного сервера.

4. Общая схема процесса обновления сертификатов

Общая логика процесса обновления сертификатов на POS-терминале состоит в следующем (Рисунок 1. Общая схема обновления (перевыпуска) сертификатов):

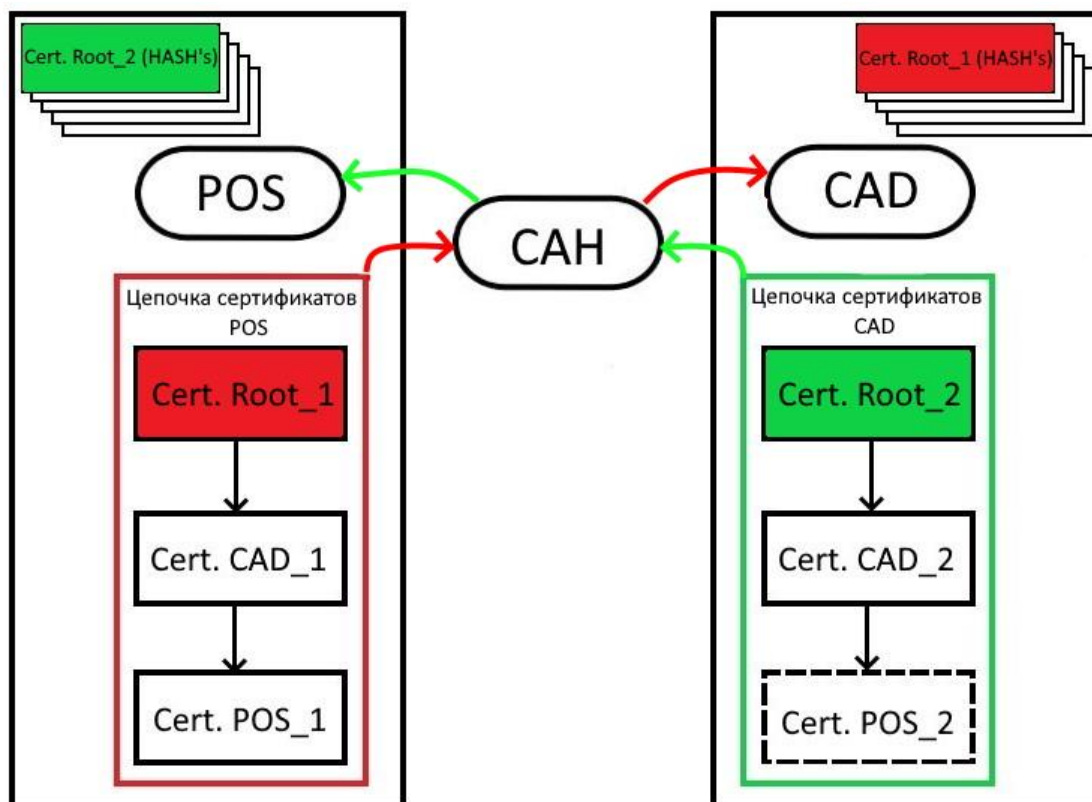


Рисунок 1. Общая схема обновления (перевыпуска) сертификатов

1. POS-терминал поочередно проверяет сертификаты, из загруженной в него цепочки сертификатов, на истечение срока действия;
2. За определенное время до истечения срока действия какого-либо из сертификатов в цепочке POS-терминала на CAH посылается запрос на обновление сертификатов. В запросе POS-терминал отправляет на CAH всю имеющуюся у него цепочку сертификатов, включая хэш-значения всех корневых сертификатов, прописанных в POS-терминале;

Примечание. Цепочка сертификатов CAD должна сходиться на одном из корневых сертификатов хранящихся в виде HASH-значений в коде POS-терминала. Цепочка сертификатов POS-терминала должна сходиться на одном из корневых сертификатов хранящихся в виде HASH-значений в коде CAD'а.

3. CAH проверяет цепочку сертификатов POS-терминала на сходимость к одному из сертификатов корневого УЦ, находящегося в БД CAH;
4. CAH формирует запрос для CAD на выпуск сертификата POS-терминала с том же самым публичным ключом, при положительном результате проверки;

ВАЖНО!

CAH передает запрос только тому CAD, который имеет один из корневых сертификатов, хэш-значения которых присутствуют в запросе от POS-терминала. Если в запросе от POS-терминала на CAH несколько хэш-значений корневых сертификатов, то выбирается тот CAD, в котором содержатся самые новые «свежие» корневые сертификаты.

5. CAD издает сертификат POS-терминала и передает на CAH всю, новую, цепочку сертификатов;

6. Полученную, новую, цепочку CAH передает POS-терминалу, дополнив её нужным корневым сертификатом.
7. Полученные от CAH новые сертификаты POS-терминал проверяет на целостность цепочки и сходимость к корневым сертификатам, прописанным в коде ПО POS-терминала, далее сохраняет их.

ВАЖНО!

Смена сертификатов корневого УЦ в POS-терминале инициируется при обнаружении факта того, что имеющаяся цепочка не сходится на сертификат корневого УЦ. Далее выполняется процедура обновления, описанная выше. Для смены в POS-терминале сертификата корневого УЦ необходимо предварительно загрузить в POS-терминал ПО, содержащее в коде ПО POS-терминала новый сертификат корневого УЦ в виде хэш-значения.

5. Вход/ выход в (из) системы

Вход в систему выполняется после авторизации пользователя путем ввода логина/ пароля на странице авторизации пользователя (Рисунок 2. Страница авторизации пользователя).

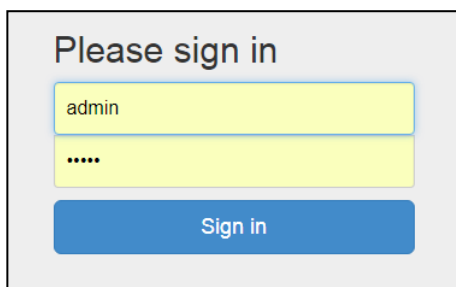


Рисунок 2. Страница авторизации пользователя

При первом запуске сервера, авторизация может быть выполнена под пользователем с ролью «**Administrator**», созданным системой по умолчанию со следующими данными:

Login (Логин): **admin**.

Password (пароль): **admin**.

При успешной авторизации открывается доступ к созданию других пользователей.

Выход пользователя осуществляется по нажатию кнопки



6. Создание пользователя

Выполнив авторизацию под пользователем с ролью «**Administrator**», отобразится окно регистрации нового пользователя, где нужно нажать кнопку «**Create**». Web-интерфейс системы CAH представляет собой страницу, содержащую следующие области (Рисунок 3. Кнопка "Create". Создание нового пользователя):

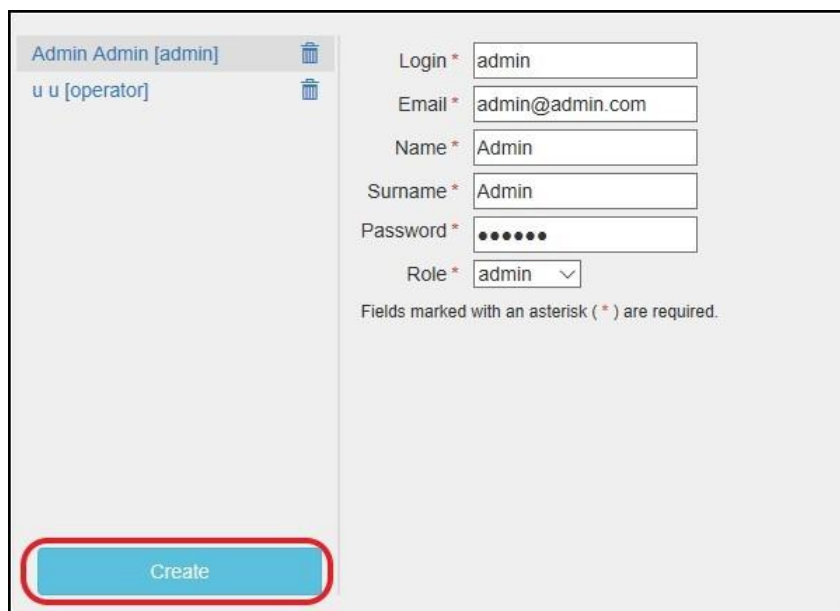


Рисунок 3. Кнопка "Create". Создание нового пользователя

Система создаст нового пользователя с пустыми параметрами, которые необходимо заполнить и нажать кнопку «**Save**» (Рисунок 4. Создание нового пользователя. Кнопка "Save".) для сохранения или «**Cancel**» для отмены.

- **Login** – логин для авторизации пользователя;

- **Email** – адрес электронной почты пользователя;
- **Name** – имя пользователя;
- **Surname** – фамилия пользователя;
- **Password** – пароль для авторизации пользователя. Требования к паролю:
 - длина пароля должна быть не менее 8 символов;
 - пароль должен содержать буквы, цифры и специальные символы;
 - запрет создания пароля, который (-ые) был установлен для пользователя, в течении года (12 месяцев) до этого.
- **Role** – указывается роль пользователя. Выбирается из раскрывающегося списка:
 - **admin** – данная роль позволяет создавать и удалять пользователей и менять пароль для уже созданных пользователей;
 - **operator** – данная роль позволяет выполнять регистрацию и блокировку SAM-модулей, также просматривать сводную информацию по зарегистрированным SAM-модулям.

The screenshot shows a web interface for creating a new user. On the left, there is a list of existing users: 'Admin Admin [admin]', 'u u [operator]', and 'User User [operator] *'. The main form has the following fields: 'Login *' with the value 'user', 'Email *' with 'user@inpas.ru', 'Name *' with 'User', 'Surname *' with 'User', 'Password *' with masked characters, and 'Role *' with a dropdown menu set to 'operator'. A red box highlights these fields, and a red arrow points from this box to the 'Save' button, which is also circled in red. Below the form, a note states: 'Fields marked with an asterisk (*) are required.' There is also a 'Cancel' button and a 'Create' button at the bottom left.

Рисунок 4. Создание нового пользователя. Кнопка "Save".

Максимальный срок действия паролей пользователей и администраторов – 90 дней.

После пяти не успешных попыток входа в систему учетная запись пользователя – блокируется.

При нажатии кнопки «**Save**» система выдаст сообщение о результате: «**Changes saved successfully**» – в случае успеха (Рисунок 5. Сообщение об успешном результате) или сообщение с описанием ошибки – в случае ошибки (Рисунок 6. Сообщение об ошибке).



Рисунок 5. Сообщение об успешном результате

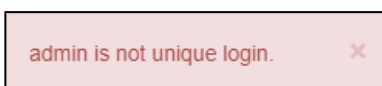


Рисунок 6. Сообщение об ошибке

6.1. Удаление пользователя

Для удаления пользователя необходимо нажать на иконку  рядом с именем пользователя, которого необходимо удалить.

Система запросит подтверждение на удаление (Рисунок 7. Запрос подтверждения на удаление пользователя).

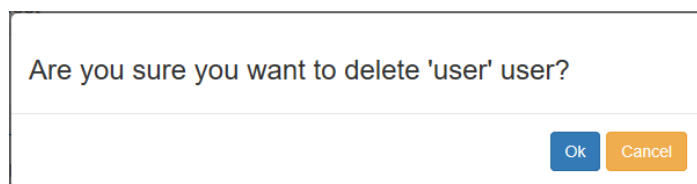


Рисунок 7. Запрос подтверждения на удаление пользователя

Нажать кнопку «**OK**» для подтверждения удаления или «**Cancel**» для отмены.

6.2. Первый вход пользователя

При первом входе пользователя, после регистрации администратором, система «**KDH**» запросит сменить пароль, установленный администратором, на новый.

В отобразившемся окне «**Change user password**» нужно заполнить следующие поля и нажать кнопку «**Save**» (Рисунок 8. Окно изменения пароля при первом входе пользователя в систему):

- **Current login:** - в данном поле указан логин изменяемого пользователя. Поле не доступно для редактирования;
- **Current password:** - в данное поле вводится текущий пароль пользователя (заданный администратором при создании пользователя);
- **New password:** - в данное поле вводится новый пароль. Обязательные условия при создании пароля:
 - минимальная длина пароля – 8 символов;
 - пароль должен содержать буквы, цифры и специальные символы;
 - запрет создания пароля, который (-ые) был установлен для пользователя, в течении года (12 месяцев) до этого.
- **Confirm password:** - в данное поле вводится идентичный пароль, введенному в поле «**New password:**», для подтверждения корректности ввода пароля.

После сохранения изменений система отобразит информационное сообщение «**New password saved successfully.**» и перейдет к странице авторизации (Рисунок 8. Окно изменения пароля при первом входе пользователя в систему).

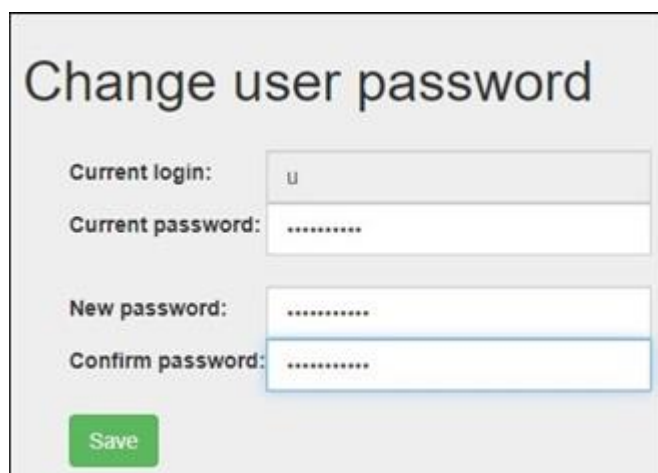


Рисунок 8. Окно изменения пароля при первом входе пользователя в систему

7. Описание Web-интерфейса CAH

Web-интерфейс системы CAH представляет собой три страницы:

1. «**General**» - на данной странице располагается информация о состоянии взаимодействия с CAD, POS-терминалами, также информация и инструменты для работы с SAM-модулями;
2. «**CAD and certificates**» - на данной странице располагается информация (сертификаты, hash корневых сертификатов POS-терминала) и инструменты для работы с CAD;
3. «**Settings**» - на данной странице располагаются настройки CAH.

7.1. Страница «General»

The screenshot shows the 'General' page of the INPAS Certificate Authority Host. The page has a top navigation bar with 'General', 'CAD and certificates', and 'Settings' tabs, and a 'Logout' button. The main content area is divided into three sections: 1. CAD status (idle), 2. Device list table, and 3. SAM list table. The device list table shows columns for Event time, SAM SN, Device SN, Vendor, Model, Device Type, CAD_ID, and IP. The SAM list table shows columns for SAM SN and Time loaded. The page also includes a bottom status bar with '1-40/31291' and '1-40/87'.

Рисунок 9. Web-интерфейс страницы «General»

Web-интерфейс страницы «General» представляет собой области:

- Статус состояния взаимодействия с CAD (область 1 на Рисунок 9. Web-интерфейс страницы «General»);
- Информация по взаимодействию с POS-терминалами (область 2 на Рисунок 9. Web-интерфейс страницы «General»);
- Информация и инструменты для работы с SAM-модулями (область 3 на Рисунок 9. Web-интерфейс страницы «General»);

7.1.1. Статус состояния CAD

В данной области (область 1 на Рисунок 9. Web-интерфейс) отображается информация о статусе взаимодействия CAH с CAD (передача запроса на сертификаты и получение сертификатов для POS-терминала). Статус может иметь следующие значения:

Idle – ожидание запроса от CAH;

Ok – запрос получен, обработан без ошибок (на CAH переданы сертификаты POS и CAD). После закрытия соединения с CAH переходит в статус **Idle**;

Error – ошибка в результате взаимодействия между CAH и CAD. После закрытия соединения с CAH переходит в статус **Idle**.

7.1.2. Взаимодействие с POS-терминалами

Данная область содержит следующие элементы (Рисунок 10. Взаимодействие с POS-терминалами).

1

Device SN

SAM SN

Event from

Event to

Device Type All

Status: All

2

Event time	SAM SN	Device SN	Vendor	Model	Device Type	CAD_ID	IP
✓ 29.03.19 13:48:15		325495206	Verifone	VX820	POS	25	/10.35.90.164:58645
✓ 29.03.19 13:18:19	10721E3D	325495206	Verifone	VX820	POS	24	/10.35.90.164:58412
✖ 20.11.20 12:50:45	10721E3D	325495206	Verifone	VX820	POS		/10.35.90.164:58293
✓ 18.11.20 17:57:28	1072733D	325495206	Verifone	VX820	POS	24	/10.35.90.164:63938
✓ 19.06.20 11:43:30	1072733D	325495206	Verifone	VX820	POS	24	/10.35.90.164:60083
✓ 19.06.20 9:43:17	03520797	PE11P87B50470	SUNMI	P1_4G-EU	POS	24	/192.168.88.27:47603
✓ 18.06.20 19:02:51	1072733D	55012859	PAX	S900-0GW-363-01LU	POS	24	/10.35.90.164:57227
✓ 18.06.20 18:30:48		55012859	PAX	S900-0GW-363-01LU	POS	25	/10.35.90.164:57018
✓ 18.06.20 18:27:17		55012859	PAX	S900-0GW-363-01LU	POS	25	/10.35.90.164:57007
✖ 18.06.20 18:25:03		55012859	PAX	S900-0GW-363-01LU	POS		/10.35.90.164:56999
✓ 26.03.19 16:46:08	1072733D	55012859	PAX	S900-0GW-363-01LU	POS	24	/10.35.1.105:34879
✓ 26.03.19 9:53:25	03520797	PE11P87B50470	SUNMI	P1_4G-EU	POS	24	/192.168.88.27:46185
✖ 26.03.19 9:33:51	03520797	PE11P87B50470	SUNMI	P1_4G-EU	POS	24	/192.168.88.27:43669
✓ 26.03.19 9:23:37	03520797	PE11P87B50470	SUNMI	P1_4G-EU	POS	24	/192.168.88.27:38752
✖ 26.03.19 8:35:15	03520797	PE11P87B50470	SUNMI	P1_4G-EU	POS	24	/192.168.88.27:49208
✖ 26.03.19 7:42:58	03520797	PE11P87B50470	SUNMI	P1_4G-EU	POS	24	/192.168.88.27:59842
✖ 26.03.19 7:28:02	03520797	PE11P87B50470	SUNMI	P1_4G-EU	POS	24	/192.168.88.27:58735
✓ 25.03.19 19:21:07		55012859	PAX	S900-0GW-363-01LU	POS	25	/10.35.90.164:60258
✓ 25.03.19 19:19:46		55012859	PAX	S900-0GW-363-01LU	POS	25	/10.35.90.164:60252
✓ 25.03.19 18:45:29	1072733D	55012859	PAX	S900-0GW-363-01LU	POS	24	/10.35.1.105:57667
✓ 25.03.19 18:36:26	1072733D	55012859	PAX	S900-0GW-363-01LU	POS	24	/10.35.1.105:57666

1-40/31291

Рисунок 10. Взаимодействие с POS-терминалами

- Фильтр** (область 1 на Рисунок 10. Взаимодействие с POS-терминалами) позволяет осуществлять поиск нужной информации, используя следующие параметры для фильтрации данных:
 - Device SN** - серийный номер POS-терминала;
 - SAM SN** - серийный номер SAM-модуля;
 - Event from** и **Event to** - диапазон дат. Позволяет вывести информацию за указанный период;
 - Device Type** - выполняет фильтрацию по типу оборудования. Возможные значения: «All» – отображается все оборудование; «POS» - отображаются только POS-терминалы; «PINPAD» - отображаются только пинпады.
 - Status** - Имеет значения: «All» – отобразить все запросы, «With errors» – отображать запросы только со статусом «ошибка».
- Информация по запросам от POS-терминалов** (область 2 на Рисунок 10. Взаимодействие с POS-терминалами) имеет табличное представление. Данные разбиты по следующим столбцам:
 - Результат обработки запроса от POS-терминала:**
 -  - успешно.
 -  - с ошибками.
 - Event time** - дата и время получения запроса сервером CAH от POS-терминала.
 - SAM SN** - серийный номер SAM-модуля.
 - Device SN** - серийный номер POS-терминала, от которого получен запрос.

- **Vendor** - вендор POS-терминала, от которого получен запрос.
- **Model** - модель POS-терминала, от которого получен запрос.
- **Device Type** - тип оборудования: «POS», «PINPAD».
- **CAD_ID** – отображается идентификатор устройства CAD со страницы «CAD and certificates», на которые отправился запрос от POS-терминала.

Примечание. Если столбец «CAD_ID» пуст – ошибка возникла до того, как данные отправились конкретному устройству. Если столбец «CAD_ID» имеет значение, то запрос уже отправился конкретному CAD. Результатом будет либо ошибка, возвращенная CAD, либо успешно обработанный запрос (см. документ «[Общий справочник кодов ошибок RKL.pdf](#)»).

- **IP** - IP-адрес и порт POS-терминала, с которого получен запрос.

7.1.3. Работа с SAM-модулями

Данная область содержит следующие элементы (Рисунок 11. Информация по SAM-модулям):

SAM SN	Time loaded
98765432	03.10.16 13:46:50
07732793	03.10.16 16:20:31
14468597	03.10.16 16:44:26
17883493	06.10.16 16:00:10
04468597	14.02.17 17:28:38
07883493	14.02.17 17:50:54
02583797	06.06.17 14:31:49
02583997	06.06.17 14:31:49
02583697	06.06.17 14:31:49
02583897	06.06.17 14:31:49
02584097	06.06.17 14:31:49
04468599	07.09.17 14:19:13

Рисунок 11. Информация по SAM-модулям

- **Фильтр** (область 1 на Рисунок 11. Информация по SAM-модулям) позволяет осуществлять поиск нужной информации, используя параметры:
 - **SAM SN** - серийный номер SAM-модуля;
 - **Status** – выполняет фильтрацию по включенным/ отключенным SAM-модулям. Возможные значения: «All» – отображаются все SAM-модули; «ON» - отображаются только те SAM-модули, для которых разрешена выдача сертификатов; «OFF» - отображаются только те SAM-модули, для которых запрещена выдача сертификатов.
- **Информация по SAM-модулям** (область 2 на Рисунок 11. Информация по SAM-модулям). Содержит информацию по SAM-модулям, для которых на сервер CAH загружены криптограммы MAC-ключей. Имеет табличное представление. Данные разбиты по следующим столбцам:

- **SAM SN** - серийный номер SAM-модуля;
- **Time loaded** - дата и время загрузки криптограммы MAC-ключа SAM-модуля;
- **Включение/ отключение выдачи сертификатов SAM-модулю:**
 -  - данная пиктограмма означает, что для данного SAM-модуля разрешена выдача сертификатов, при нажатии на неё выполняется смена пиктограммы на , запрещая выдачу сертификатов для данного SAM-модуля;
 -  - данная пиктограмма означает, что для данного SAM-модуля запрещена выдача сертификатов, при нажатии на неё выполняется смена пиктограммы на , разрешая выдачу сертификатов для данного SAM-модуля.



- (область 3 на Рисунок 11. Информация по SAM-модулям) - инструмент для загрузки файла с криптограммами MAC-ключей SAM-модулей.

7.1.3.1. Загрузка списка криптограмм MAC-ключей

Для загрузки криптограмм MAC-ключей SAM-модулей необходимо выполнить следующие шаги:



- Нажать на инструмент .
- В открывшемся окне указать файл со списком MAC-ключей SAM-модулей и нажать кнопку «Открыть».

Примечание. Список криптограмм MAC-ключей SAM-модулей представляет из себя текстовый файл в формате «*.CSV». Данный файл генерируется утилитой «Персонализатор SAM-модулей» при записи информации (приложение, сгенерированные ключи) на SAM-модули. Формат и структура файла подробно описаны в приложении (8.1 Файл ключей SAM-модулей).

Система выполнит загрузку MAC-ключей из указанного файла и выведет сообщение «**SAM keys were loaded**» – в результате успешной загрузки, или сообщение с описанием ошибки – в результате неуспешной загрузки.

Данные из загруженного файла будут добавлены в таблицу с информацией по SAM-модулям.

7.2. Страница «CAD and certificates»

На данной странице располагается информация (сертификаты, hash корневых сертификатов POS-терминала и CAD) и инструменты для работы с CAD.

Web-интерфейс страницы «CAD and certificates» представляет собой области:

- Информация и инструменты для работы с CAD (область 1 на Рисунок 12. Web-интерфейс страницы «CAD and certificates»);
- Информация о сертификатах CAD (область 2 на Рисунок 12. Web-интерфейс страницы «CAD and certificates»);

Devices cad:

1

ID	Cad IP Adress	Cad IP port	Cad status	Cad state	Default Cad	KCV ZMK	Last success time connect to cad
21	10.35.1.166	1803	SWITCH_OFF		false		13.03.2019 12:01:08
22	10.35.1.164	1803	SWITCH_OFF		false		13.03.2019 12:00:08
24	10.35.1.40	1803	ACTIVE		true	C631E8	03.04.2019 11:52:10
Last error							
Root certificate hashes [(...E619B3/ISL_ROOT), (...2EFA61/X509_ROOT)]							
25	10.35.1.174	1803	ACTIVE		true	0AC9A3	03.04.2019 11:52:10

Edit rows

Certificates:

2

- ISL_ROOT(id = 239)
- ISL_CAD(id = 240)
- X509_ROOT(id = 117)
- X509_RKL(id = 347)
- X509_SSL(id = 348)

Certificate X.509 content:

Subject: EMAILADDRESS=root_rkl.ca@inpas.ru, C=RU, L=Moscow, OU=Security Department, O=INPAS COMPANY, CN="ROOT RKL CA"

Issuer: EMAILADDRESS=root_rkl.ca@inpas.ru, C=RU, L=Moscow, OU=Security Department, O=INPAS COMPANY, CN="ROOT RKL CA"

Serial number: 13338564992C39DE0355F9A8510A13EA

Valid from: 18.11.2015 00:00:00

Valid to: 18.11.2020 00:00:00

Public key: D87CA68CBCEC679276785A9FD17F42EDAFAFFA0A

Public key algorithm: D87CA68CBCEC679276785A9FD17F42EDAFAFFA0A

Subject key identifier: 92E394DEAE7CDBC55DB2219E3C51C418F52EFA61

Issuer key identifier: 92E394DEAE7CDBC55DB2219E3C51C418F52EFA61

Days to expire: 594

Export Certificate

Рисунок 12. Web-интерфейс страницы «CAD and certificates»

7.2.1. Информация и инструменты для работы с CAD

Данная область содержит следующие элементы (Рисунок 13. Область работы с CAD):

Devices cad:

1

ID	Cad IP Adress	Cad IP port	Cad status	Cad state	Default Cad	KCV ZMK	Last success time connect to cad
21	10.35.1.166	1803	SWITCH_OFF		false		13.03.2019 12:01:08
22	10.35.1.164	1803	SWITCH_OFF		false		13.03.2019 12:00:08
24	10.35.1.40	1803	ACTIVE		true	C631E8	03.04.2019 11:52:10
Last error							
Root certificate hashes [(...E619B3/ISL_ROOT), (...2EFA61/X509_ROOT)]							
25	10.35.1.174	1803	ACTIVE		true	0AC9A3	03.04.2019 11:52:10

Edit rows

2

Рисунок 13. Область работы с CAD

- **Фильтр** (область 1 на Рисунок 13. Область работы с CAD) позволяет осуществлять поиск нужной информации используя следующий параметр для фильтрации данных:

- **Search** – указывается значение для поиска CAD и нажимается кнопка ;

-  - в раскрывающемся списке указываются, по какому критерию будет выполняться поиск CAD. Для этого нужно снять/ установить флаг в чек бокс с названием нужного столбца.

- **Информация и инструменты для работы с CAD** (область 2 на Рисунок 13. Область работы с CAD) имеет табличное представление. Данные разбиты по следующим столбцам:

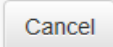
- **ID** – персональный идентификатор, присвоенный CAD при регистрации в CAH;
- **Cad IP Address** – IP-адрес CAD, указанный при регистрации в CAH;
- **Cad IP port** – порт CAD, указанный при регистрации в CAH;
- **Cad status** – отображается статус подключения CAD. Возможные значения:
 - **Active (Активен)** – последняя попытка получения с CAD обновленных сертификатов для POS-терминала была успешной;
 - **Switch Off (Выключен)** – временно выключен через интерфейс CAH, запросы на него не посылаются;
 - **No connection (Нет подключения)** – отсутствует соединение с CAD;
 - **Not ready (Не готов)** – физическое подключение с устройством есть, однако не удалось получить с CAD сертификаты, либо в ответ на периодический ring-запрос «is alive» не получен ответ нужного формата.

В CAH есть механизм отслеживания статусов, подключенных CAD. Для каждого CAD со статусом «**No connection (Нет подключения)**» или «**Not ready (Не готов)**» система предпринимает попытки выполнить команду регистрации CAD. В случае успеха CAD переводится в статус «**Active (Активен)**». На CAD, находящиеся в статусе «**Active (Активен)**», периодически отсылается ring-запросы «is alive» с целью заблаговременного перевода CAD в статус «**No connection (Нет подключения)**» или «**Not ready (Не готов)**»;

- **Cad state** – состояние устройства CAD. Возможные значения: «**Established (Штатная работа)**»; «**Warning (Предупреждение)**»; «**Error (Ошибка)**».
- **Default Cad** – отметка указывает, что данный CAD может быть использован для первичного издания сертификатов POS-терминалу со “старым” ПО, при котором в запросе от POS-терминала не содержится информации о корневых сертификатах, на которых должна сходиться цепочка сертификатов POS-терминала. Возможные значения: «**False**», «**True**»;

Примечание. «**Default CAD**» – издает сертификаты POS-терминалам со “старым” ПО, только с применением цепочки сформированной на “старом” корневом сертификате УЦ. Т.е. CAD с признаком «**Default CAD**» должен уметь гарантированно выдавать сертификаты POS-терминалам со “старым” ПО на известном для “старого” ПО сертификате.

- **KCV ZMK** – контрольная сумма ключа ZMK, на котором CAD может расшифровать криптограмму MAC-ключа SAM-модуля при издании новых сертификатов POS-терминала;
- **Last success time connect to cad** – дата и время последнего успешного получения с CAD обновленных сертификатов для POS-терминала;
- **Last error** – код ошибки, полученный в последнем ответе с CAD. Если последний ответ от CAD не содержал ошибку, в данной строке ничего не отображается;
- **Root certificate hashes** – значения hash всех корневых сертификатов, на которых CAD может проверить присланную POS-терминалом цепочку.

- Кнопка «Edit rows»  - включает режим редактирования списка CAD. В режиме редактирования возможно выполнить следующие действия: «Добавить новый CAD», «Редактировать CAD», «Удалить CAD». Выйти из режима редактирования списка CAD, возможно, нажав кнопку «Cancel» .

7.2.1.1. Режим редактирования списка CAD

Для перехода в режим редактирования списка CAD нужно нажать кнопку «Edit rows»



(Рисунок 14. Режим редактирования списков CAD).

Devices cad:



ID	Cad IP Address	Cad IP port	Cad status	Cad state	Default Cad	KCV ZMK	Last success time connect to cad	
21	10.35.1.166	1803	SWITCH_OFF		false		13.03.2019 12:01:08	 
22	10.35.1.164	1803	SWITCH_OFF		false		13.03.2019 12:00:08	 
24	10.35.1.140	1803	ACTIVE		true	C631E8	03.04.2019 17:05:10	 
25	10.35.1.174	1803	NO_CONNECTION		true		03.04.2019 16:30:10	 

Рисунок 14. Режим редактирования списков CAD

В режиме редактирования возможно добавить, отредактировать и удалить нужный CAD. Для выполнения каждого из этих действий существует специальная кнопка:



- при нажатии на данную кнопку система запросит подтверждение на удаление CAD. После подтверждения система выполнит удаления выбранного CAD;



- при нажатии на данную кнопку отображается окно редактирования CAD (Рисунок 15. Окно редактирования CAD).

Edit cad with id 21
✕

Cad ip address
(format: xxx.xxx.xxx.xxx) *

Cad ip port
(range 1-65535) *

Status *

Is default device

☐





Рисунок 15. Окно редактирования CAD

Редактирование параметров CAD: «Cad IP address», «Cad IP port», «Is default device», доступно только для CAD в статусе «Switch Off (Выключен)». После нажатия кнопки «Save changes», выполняется проверка уникальности адреса, попытка установить соединение и получить с CAD данные.

При переводе CAD из статуса «Active (Активен)», «No connection (Нет подключения)» или «Not ready (Не готов)» в статус «Switch Off (Выключен)» вся информация об этом CAD удаляется из БД CAH.

При ручном переводе CAD в статус «Active (Активен)» - активация CAD (доступно только для CAD в статусе «Switch Off (Выключен)», «No connection (Нет подключения)» или «Not ready (Не готов)») выполняется попытка установить соединение и получить с CAD данные. По результатам проверки CAD переходит в статус «Active (Активен)», «No connection (Нет подключения)» либо «Not ready (Не готов)».

Для сохранения изменений нужно нажать кнопку «Save changes». Для отмены внесенных изменений нужно нажать кнопку «Cancel».

7.2.1.2. Регистрация нового CAD

«New row» - при нажатии на данную кнопку отображается окно для регистрации нового CAD в системе CAH (Рисунок 16. Окно регистрации нового CAD).

The image shows a dialog box titled "Add a new CAD". It has four input fields: "Cad ip address" with the value "10.35.1.41" and a format hint "xxx.xxx.xxx.xxx"; "Cad ip port" with the value "1806" and a range hint "range 1-65535"; "Status" with a dropdown menu showing "ACTIVE"; and "Is default device" with a checked checkbox. At the bottom right, there are two buttons: "Save changes" and "Cancel".

Рисунок 16. Окно регистрации нового CAD

Примечание. Для издания, переиздания сертификатов POS-терминалам с “новым” ПО, CAD должен иметь собственную цепочку сертификатов, сходящуюся на одном из корневых сертификатов хранящихся в виде HASH-значений в коде POS-терминала. Следовательно, в POS-терминале с “новым” ПО должна быть собственная цепочка сертификатов, сходящаяся на одном из корневых сертификатов хранящихся в виде HASH-значений в коде CAD’а.

В отобразившемся окне нужно указать IP-адрес и порт CAD (параметры: «Cad IP address», «Cad IP port»), указать статус подключения CAD (параметр «Status») и установить флаг в чек бокс, если CAD может быть использован для первичного издания сертификатов POS-терминалу со “старым” ПО (параметр «Is default device»).

Примечание. Для первичного издания сертификатов POS-терминалам со “старым” ПО, «Default CAD» должен иметь собственную цепочку сертификатов, сходящуюся на корневом сертификате, который загружен (присутствует) в POS-терминале со “старым” ПО.

Для сохранения внесенных данных регистрируемого CAD нужно нажать кнопку «**Save changes**»

Save changes

. Для отмены регистрации CAD нужно нажать кнопку «**Cancel**»

Cancel

ВАЖНО!

CAD'ы со "старым" ПО не поддерживаются, т.к. не поддерживают новый формат команд. CAD со "старым" ПО может только выпускать сертификаты, перевыпуск сертификатов – **недоступен**.

После задания адреса и нажатия кнопки «**Save changes**» проверяется уникальность заданного адреса:

- Если по заданному адресу уже зарегистрирован CAD, отобразится соответствующее сообщение об ошибке, новый CAD не будет зарегистрирован;
- Если адрес уникален, то будет выполнена попытка получить данные с регистрируемого CAD. Если попытка получения данных завершилась неуспешно, отображается соответствующее предупреждение и запрос подтверждения добавления CAD. При необходимости зарегистрировать CAD, несмотря на ошибку получения с него данных, такой CAD регистрируется со статусом «**No connection (Нет подключения)**» или «**Not ready (Не готов)**» в зависимости от результата выполнения попытки получить с него данные;
- Если данные с CAD были успешно получены, CAD регистрируется со статусом «**Active (Активен)**».

7.2.2. Информация о сертификатах CAD

Данная область содержит следующие элементы (Рисунок 17. Область информации о сертификатах CAD):

Certificates:

ISL_ROOT(id = 239)

ISL_CAD(id = 240)

X509_ROOT(id = 117)

X509_RKL(id = 347)

X509_SSL(id = 348)

Certificate X.509 content:

Subject:	EMAILADDRESS=root_rkl.ca@inpas.ru, C=RU, L=Moscow, OU=Security Department, O=INPAS COMPANY, CN="ROOT RKL CA"
Issuer:	EMAILADDRESS=root_rkl.ca@inpas.ru, C=RU, L=Moscow, OU=Security Department, O=INPAS COMPANY, CN="ROOT RKL CA"
Serial number:	13338564992C39DE0355F9A8510A13EA
Valid from:	18.11.2015 00:00:00
Valid to:	18.11.2020 00:00:00
Public key:	D87CA68CBCEC679276785A9FD17F42EDAFEFFA0A
Public key algorithm:	D87CA68CBCEC679276785A9FD17F42EDAFEFFA0A
Subject key identifier:	92E394DEAE7CDBC55DB2219E3C51C418F52EFA61
Issuer key identifier:	92E394DEAE7CDBC55DB2219E3C51C418F52EFA61
Days to expire:	593

Export Certificate

Рисунок 17. Область информации о сертификатах CAD

Примечание. При регистрации CAD отправляет на CAH полную собственную цепочку сертификатов, вплоть до сертификата (сертификатов) корневого УЦ (хранящихся в виде HASH-значений в коде CAD'a).

- **Дерево сертификатов** (область 1 на Рисунок 17. Область информации о сертификатах CAD) отображает данные о сертификатах, полученные от выбранного CAD:
 - Формат сертификата («X.509», «ISL»);
 - Тип сертификата («ROOT», «RKL», «SSL», «CAD»);
 - Внутренний «id» сертификата (присваивается, когда сертификат сохраняется в БД CAH).
- Подробная информация по выбранному сертификату, полученная от выбранного CAD (область 2 на Рисунок 17. Область информации о сертификатах CAD):
 - **ISL:**
 - **Issuer ID** – идентификатор издателя сертификата;
 - **Serial number** – серийный номер;
 - **Create date** – дата и время создания сертификата;
 - **Expire date** – дата и время окончания действия сертификата;
 - **Key id** – идентификатор ключа;
 - **Device model** – модель устройства;
 - **Device serial number** – серийный номер устройства;
 - **Days to expire** – количество дней до окончания действия сертификата.
 - **X.509:**
 - **Subject** – сведения о субъекте, которому выдан сертификат;
 - **Issuer** – сведения о издателе сертификата;
 - **Serial number** – серийный номер;
 - **Valid from** – дата и время начала действия сертификата;
 - **Valid to** – дата и время окончания действия сертификата;
 - **Public key** – значение публичного ключа;
 - **Public key algorithm** – алгоритм для публичного ключа;
 - **Subject key identifier** – собственный ключ;
 - **Issuer key identifier** – идентификатор ключа издателя;
 - **Days to expire** – количество дней до окончания действия сертификата.
- Кнопка «**Export Certificate**» (область 3 на Рисунок 17. Область информации о сертификатах CAD) позволяет выгрузить нужный сертификат из системы:
 - **ISL** – выгружается в бинарном виде;
 - **X.509** – выгружается в формате PEM.

В зависимости от изменения количества дней до окончания действия сертификата, меняется статус состояния сертификатов (Рисунок 18. Статус состояния сертификатов):



Рисунок 18. Статус состояния сертификатов

- **Норма** – до истечения срока действия сертификата осталось больше времени, чем указано в параметре «**Minimum days for expire certificate**» (страница «**Settings**»);

- **Предупреждение** – до истечения срока действия сертификата осталось меньше времени, чем указано в параметре «**Minimum days for expire certificate**» (страница «**Settings**»), но сертификат ещё не истек. Напротив сертификата отображается предупреждающая пиктограмма  ;
- **Ошибка** – сертификат истек. Напротив сертификата отображается предупреждающая пиктограмма  .

7.3. Страница «Settings»

На данной странице возможно выполнить следующие настройки (Рисунок 19. Страница "Settings").

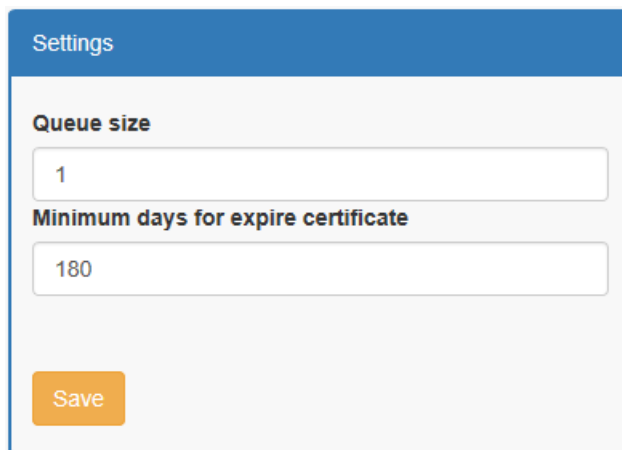


Рисунок 19. Страница "Settings"

Queue size (максимальный размер очереди POS-терминалов) – при достижении указанного в параметре значения САН каждому обратившемуся POS-терминалу сразу сообщает о невозможности обновить сертификаты.

Minimum days for expire certificate (Минимальное количество дней до истечения эмитентских сертификатов) – указывается минимальное количество дней до окончания действия сертификатов (как собственных сертификатов CAD, так и корневых, на которые сходятся цепочки сертификатов CAD). Для сертификатов, у которых осталось меньшее количество дней, чем указано в параметре, отображается предупреждение. Использование данного параметра предотвращает издание POS-терминалу сертификата на CAD, если в результирующей цепочке POS-терминала окажется сертификат, который скоро истечет, т.к. сразу после получения такой цепочки POS-терминал снова запросит обновление тех же самых сертификатов. Минимальное значение параметра – 180 дней.

8. Приложение

8.1. Файл ключей SAM-модулей

Данный файл формируется автоматически с помощью программы «Персонализатор SAM».

Структура файла:

№	Обозначения	Название	Тип
1	S/N_SAM_модуля	Идентификатор SAM-модуля (CPLC)	HEX
2	Криптограмма_MAC_ключа	HEX-символьное представление криптограммы (32 HEX-символа для 3DES двойной длины)	HEX
3	KCV_MAC_ключа	Проверочное значение MAC-ключа. Игнорируется.	HEX
4	KCV_ZMK_ключа	Контрольная сумма ключа ZMK, на котором зашифрован MAC-ключ SAM-модуля.	HEX

Формат TXT, разделитель полей «;».

Файл может содержать несколько строк, разделенных 0xDD, 0x0A или их комбинацией.

Пример файла со списком ключей SAM-модулей:

```
1072733D;D2BD71F4564A1C13A06BA9B8CA5B178A;7B8358;c631e8
10721E3D;D2BD71F4564A1C13A06BA9B8CA5B178A;7B8358;c631e8
```

8.2. Коды ошибок САН

Код ошибки	Текст ошибки	Пояснение
00	Успешное завершение	Успех
03	Неизвестный серийный номер	Не найден терминал по указанному идентификатору
12	Неверный Stan	Нет STAN
30	Неверный формат запроса	Нет полей 61, 48, 42; Некорректные поля 48 и 61; Нет информации о вендоре и модели терминала; Нет тега FF10; Нет тэгов необходимых для выполнения операции, например, 0A
76	Сертификат не прошел проверку	Сервер САН не смог удостовериться в подлинности POS-терминала (нарушена целостность цепочки сертификатов; истек срок действия одного из сертификатов в цепочке; в БД в числе доверенных не найден корневой сертификат из цепочки POS-терминала)
77	Запрашиваемый ключ не найден или выключен	SAM модуль не найден или выключен
78	Ошибка KCV	Не прошла проверка сессионного KCV или KCV ключа
80	Ключ не передается	
81	Устройство не в состоянии READY	
82	Сервер сертификатов занят. Повторите позднее	Сервер САН вернул ответ о своей загруженности (в очередях на CAD скопилось такое кол-во POS-терминалов, которое не позволит обработать очередной запрос от нового POS-терминала в ожидаемое POS-терминалом время)
83	Сертификаты не обновлены (83). Обратитесь в Банк	Для переданных POS-терминалом данных (информации о корневых сертификатах) не найден ни

		один CAD, способный издать/переиздать хотя бы один сертификат POS-терминала
89	Неверный терминал	---
96	Системная ошибка	Системная ошибка сервера в процессе обработки запроса