**EMVCheck**

**v1.6**

**Руководство пользователя.**

**Оглавление**

[**Вступление.** 3](#_Toc2849725)

[**1.** **Установка программы** 4](#_Toc2849726)

[**2.** **Запуск программы.** 6](#_Toc2849727)

[**3.** **Настройки программы.** 7](#_Toc2849728)

[**4.** **Проверки.** 14](#_Toc2849729)

[**5.** **Просмотр отчета о проверке.** 16](#_Toc2849730)

[**6.** **Описание основных разделов проверок** 17](#_Toc2849731)

# **Вступление.**

EMVCheck – Данное средство позволяет банкам минимизировать усилия, связанные с подготовкой к сертификации эмитируемых карт в международных платежных системах, упростить выбор параметров карточных приложений при подготовке к выпуску новых карточных продуктов, а также выявить причины сбоев в работе уже выпущенных карт. При настройке параметров новых карточных продуктов EMVCheck помогает убедиться в работоспособности карты и проверить ее поведение при различных вариантах её персонализации. В случае возникновения у клиентов проблем при использовании выпущенных в обращение карт, EMVCheck помогает выяснять причины неработоспособности карт, возвращенных клиентами. EMVCheck также имеет функционал посылки некоторых скриптов на карту, с целью обновления информации и подсчета криптографии.

# **Установка программы**

Для установки EMVCheck, необходимо запустить установочный файл, который распакует программу в указанную директорию. Директория по умолчанию: “C:\Program Files (x86)\EMVCheck\EMVCheck-ВЕРСИЯ”. Каждая новая версия устанавливает программу в новый подкаталог, позволяя тем самым не терять заполненные пользователем базы ключей.

Ниже, на скриншотах представлен процесс установки.

Рис. 1 – Предупреждение.

Рис. 2 – Указание пути установки.

Рис. 3 – Завершение установки.

При установке имеется возможность создать иконку на рабочем столе и выбрать рабочую директорию. Для предотвращения путаницы в будущем, рекомендуется оставить директорию установки по умолчанию.

# **Запуск программы.**

Для запуска программы необходим ключ-флешка. После запуска программы, сразу открывается главная форма. На ней, после первого запуска или после смены ридера, необходимо настроить контактный и бесконтактный считыватели. Они располагаются в верхней части окна, на панели управления, во вкладке “Главная”.

Рис. 4 – Главная форма.

На главной форме присутствуют следующие элементы:

* Вкладка “Параметры” – на ней производится настройка словарей и ключей;
* Вкладка “Настройки” – на ней производятся некоторые настройки программы;
* Вкладка “Проверки” – на данной вкладке расположены кнопки для запуска различных проверок;
* Вкладка “Скрипты” – на данной вкладке расположены кнопки для посылки скриптов на карту;
* Вкладка “Дополнительно” – на данной вкладке расположены проверки CVV/PVV;
* Вкладка “Дерево транзакции” – на данной вкладке будет построен отчет о действиях с картой.
* Вкладка “Прочитанные теги” – на данной вкладке будут отображены теги карты, вычитанные во время работы с картой.

# **Настройки программы.**

Рис. 5 – Вкладка “Параметры”.

На вкладке “Параметры” расположены следующие элементы:

***Приложения*** – на данной форме, имеется возможность занести в базу новые приложения, чтобы программа смогла проверить их перебором, если PSE/PPSE отсутствует на карте.

Рис. 5.1 – Форма редактирования приложений.

Описание полей:

* AID – полный номер приложения, поле позволяет набирать цифры и буквы шестнадцатеричной системы;
* NAME – имя приложения, текстовое поле;
* Payment – название платежной системы, к которой относится приложение, текстовое поле.

***Теги терминалы*** – на данной форме, имеется возможность отредактировать теги, которые запрашивает карта. Можно изменять, как и значения по умолчанию, так и названия, и номера тегов. Для корректной работы программы, рекомендуется редактировать только значения тегов по умолчанию и добавлять новые, отсутствующие в базе, теги.

Рис. 5.2 – Форма редактирования тегов терминалов.

Описание полей:

* Tag – номер тега, шестнадцатеричный номер тега
* RID – первые 5 байт от номера приложения;
* Name – наименование тега;
* Value – значение тега, которое берется программой по умолчанию, шестнадцатеричное значение тега;
* Format – формат тега, используются форматы заданные спецификациями EMV;
* Length – длина тега, которая может задаваться диапазоном, значение длины задано целым десятичным числом, которое определяет количество байт в значении.

***Публичные ключи CA*** – на данной форме имеется возможность добавлять и редактировать публичные ключи для расшифровки сертификатов карты.

Рис. 5.3 – Форма редактирования открытых ключей.

Описание полей:

* RID – первые 5 байт полного номера приложения;
* IND – Индекс ключа, шестнадцатеричное значение;
* EXP – экспонента ключа, десятичное значение;
* DATE – дата окончания срока действия ключа в формате mmgg, поле необязательное.

***Чистые ключи*** – на данной форме имеется возможность добавлять и редактировать чистые значения ключей AC, MAC, ENC и др. необходимых для посылки скриптов, проверки PIN и подсчета криптографии. Check Value для чистых ключей подсчитывается автоматически.

Рис. 5.4 – Форма редактирования чистых ключей.

Описание полей:

* BIN – данное значение необходимо для автоматического выбора нужного keyset для проверки, десятичные цифры;
* MAC Length – длина MAC при подсчете, обычно либо 4, либо 8, но есть возможность выставить и другие значения; Задается для всех ключей;
* Derived MK KeySet – выставлен ли уже выведенный карточный ключ или его необходимо вывести;
* KEY AC – AC ключ, шестнадцатеричные цифры;
* KEY MAC – MAC ключ, шестнадцатеричные цифры;
* KEY ENC – ENC ключ, шестнадцатеричные цифры;
* KEY IDN – IDN ключ, шестнадцатеричные цифры;
* KEY DCVV – DCVV ключ, шестнадцатеричные цифры;
* KEY CVK – CVK ключ, либо CVVA и CVVB ключи, шестнадцатеричные цифры;
* KEY PVK – PVK ключ, либо PVVA и PVVB ключи, шестнадцатеричные цифры;
* Option – вывод ключа по опции A или B (подсчет SHA).

***Выбор и настройки HSM*** – на данной форме имеется возможность, при наличии, настроить используемый при проверках HSM Thales.

Рис. 5.5 – Форма настроек HSM Thales.

Описание полей:

* Адрес – адрес HSM;
* Порт – порт HSM;
* LMK ID – ID lmk ключа в шифратора;
* Тип ключа – TPK/ZPK/ZMK;

На данной форме выбирается шифратор, который будет использоваться при проверке.

Возможна работа с HSM в авторизованном/не авторизованном режиме. По кнопке “Настройки HSM – ключей” открывается форма редактирования ключей для HSM. Также имеется возможность проверки связи с HSM.

***Настройки SafeNet*** – на данной форме имеется возможность, при наличии, настроить используемый при проверках SafeNet.

Рис. 5.6 – Настройка SafeNet ключей.

 Форма ключей для SafeNet аналогична форме для чистых ключей. Добавляется только адрес и порт шифратора.



Рис. 6 – Вкладка “Настройки”.

На вкладке “Настройки” расположены следующие элементы:

***Спрашивать параметры транзакции*** – данная галка отвечает за запрос изменений, запрашиваемых картой данных, при проведении транзакции. К примеру, запрашиваемый PDOL будет отображен пользователю, с возможностью изменений значений в нем.

***Приводить биты в ключе*** – отвечает за то, чтобы при выводе ключей биты в ключе приводились к четному/нечетному числу.

***Криптография*** – здесь необходимо выбрать как будет считаться криптография – на чистых ключах, на HSM Thales или на SafeNet.

***Импорт настроек*** – данная кнопка позволяет импортировать ключи из старой версии программы.

***О программе*** – на данной форме расположен список изменений программы.

# **Проверки.**

На панели слева расположены кнопки проверок. Контактные проверки расположены одним блоком, бесконтактные разделены по платежным системам. Для запуска проверки, необходимо установить карту в необходимый считыватель и нажать на соответствующую кнопку проверки.

Рис. 7 – Проверки.

***EMV Generic*** – универсальная проверка контактной части карты. Криптография в этой проверке не подсчитывается.

***Verify Plaintext PIN*** – проверка открытого PIN.

***Verify Encipherment PIN*** – проверка шифрованного PIN.

***Offline/Online Transaction*** – эмуляция оффлайн/онлайн траназкций по карте, с проверкой криптографии.

Бесконтактные проверки названы соответственно, но они различаются форматом, в зависимости от платежной системы, поэтому разделены по платежной системе. На второй вкладке “Скрипты”, расположены кнопки для посылки скриптов на карту.

***Get Data*** – посылка команды Get Data на карту, для получения информации о данных в соответствующем теге. Имеется доступ к тегам, которые разрешены к чтению соответствующей спецификацией платежной системы.

***Pin Change*** – скрипт для смены PIN на карте.

***Put Data –*** скрипт для обновления данных в необходимом теге.

***PIN Unblock*** – скрипт для сброса счетчика PIN.

***Update Record*** – скрипт для обновления необходимой записи на карте.

Рис. 8 – Скрипты.

На вкладке “Дополнительно” расположены кнопки для проверки CVV/PVV на карте.

Рис. 9 – Вкладка “Дополнительно”.

***Загрузить отчет из файла*** – данная кнопка отвечает за удобный просмотр предыдущих проверок.

# **Просмотр отчета о проверке.**

После проверки, на главной форме будет сформирован отчет в виде дерева тегов с сопровождением дополнительной информацией.

Рис. 10 – Сформированный отчет.

 Все ошибки после проверки будут отмечены красным крестом. Все предупреждения будут помечены желтым восклицательным знаком. На вкладке “Прочитанные теги” есть возможность удобно просмотреть все теги, вернувшиеся картой в отсортированном по номеру, виде.

Рис. 11 – Прочитанные теги.

# **Описание основных разделов проверок**

* **PSE/PPSE** – если имеется на карте, то ответ карты в разобранном виде будет отображен в дереве. Включает в себя список приложений на карте;
* **Initiate Application Processing** – включает в себя операции Select и GPO;
* **Read Application Data** – в данном разделе отображаются все вычитанные записи;
* **Offline Data Authentication** – в данном разделе извлекается ключ карты и проводятся все возможные аутентификации (SDA/DDA) кроме CDA;
* **Start Transaction** – в данном разделе проводится посылка команд Generate AC (1 и 2), подсчитывается криптография и проводится CDA;
* **Get Data** – в данном разделе вычитываются все возможные теги, определенные платежными системами.