

TVCAS

<https://tvcas.com>

<https://t.me/tvcas>

Представленная здесь CAS относится к единому алгоритму шифрования [SimulCrypt](#). Для возможности использования смарткарт TVCAS совместно с абонентским оборудованием, реализована поддержка Conax (в будущем Irdeto). Мною были протестированы и успешно работают модули, изображённые ниже...



Работают они все одинаково, отличие только в этикетке. Смарткарты шарятся в oscam/wicard, однако, реализован счётчик запросов, который позволяет открывать не более 2 каналов одновременно. При превышении лимита карта уходит в not found. Лимит в 2 канала обусловлен тем, что в природе существуют приставки, позволяющие в момент просмотра одного канала, записывать другой.

ХАРАКТЕРИСТИКИ TVCAS

1. Максимально гарантированное количество абонентов ограничено скоростью работы базы данных и составляет 50000 (больше не тестировалось);
2. Количество кодируемых каналов — не ограничено;
3. Смарткарты самодельные на [PIC16F688](#) (в идеале -I/ST в корпусе TSSOP14). (с версии 2.0 поддерживаются SilverCard);
4. Максимальное количество реализуемых пакетов телепрограмм(классы) — 8;
5. Интеграция с биллингом — через файл выгрузки CSV;
6. **Простое API для управления подписками смарткарт.** Реализуется через GET-запрос с заранее установленным API-ключём в файле config.php. Пример:

```
GET http://mytvcas.local/api.php?  
api_key=mysecretkey123&serial_no=2100000000&set[name]=Петрова%20Зинаида&set[info]=Зелёная%2038-  
5&set[pair]=0&set[start]=1234567890&set[finish]=1234567890&set[access_criteria]=00000001
```

Параметры **set[x]** необязательны. В случае их полного отсутствия, в ответ будет возвращена информация по карте в формате json. Если-же был передан один или

несколько параметров **set[x]** , то сначала в базе будут изменены эти поля, а затем прочитана и возвращена информация об этой карте. Т.е. json-ответ будет содержать информацию уже изменённую, в соответствии с запросом.

Пример ответа API:

```
{"serial_no":"2100000000","name":"Ivan Petrov","info":"Zeleenaya street 123-234","access_criteria":"01010101","pair":"0","start":"1586693700","finish":"1589285580"}
```

Ответы ошибок API:

NOT_VALID_API_KEY – api_key не соответствует установленному в config.php

SMARDCARD_NOT_FOUND – карта не найдена в БД TVCAS;

UNKNOWN_SET_PARAMETER – один или несколько параметров неизвестны;

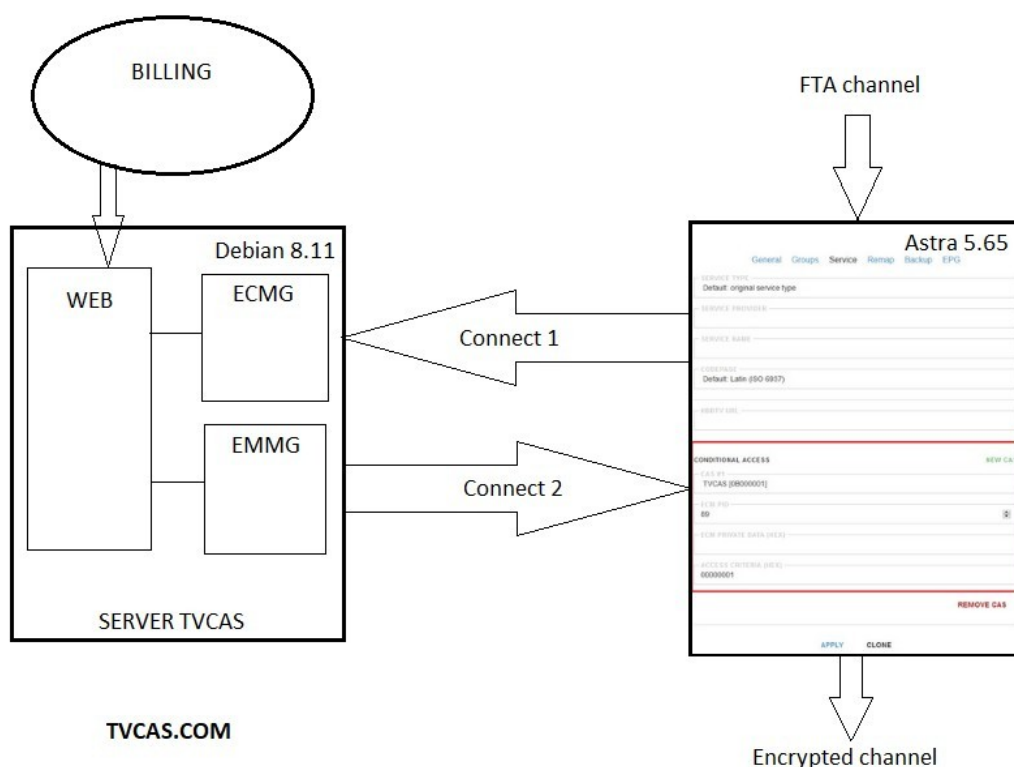
ACCESS_CRITERIA_ERROR – access_criteria отличается от шаблона 11111111 (восемь знаков — допустимы «нули» и «единицы»);

PAIR_ERROR – pair отличается от шаблона (может быть 1 или 0);

START_ERROR – время отличается от формата UNIX (10 цифр)

FINISH_ERROR – время отличается от формата UNIX (10 цифр)

Структурная схема TVCAS



Принцип работы

Между скремблером MUX (на схеме Astra 5.65) и TVCAS устанавливаются два соединения — MUX подключается к расшаренному порту ECMG (**connect 1**), а EMMG подключается к порту MUX-а (**connect 2**).

Connect 1 необходим для передачи ECM-пакета. MUX генерирует ключи CW1 и CW2, отдаёт их генератору ECMG, а тот в ответ передаёт зашифрованный пакет (ECM), который впоследствии инклюдируется в поток с определённым PID-ом. В этом зашифрованном пакете содержится три основных параметра: текущее время, ключи (CW1 и CW2) и Access Criteria (в рамках данной CAS — это признак пакета программ). ECM-пакет предназначен для **всем** смарткартам.

```
PID: 89 (0x0059) [= ]
transport_scrambling_control: 0 (0x00) [= No scrambling of TS packet payload]
adaptation_field_control: 1 (0x01) [= no adaptation_field, payload only]
continuity_counter: 3 (0x03) [= (sequence ok)]
Payload: (len: 184)
==> pointer_field: 0 (0x00)
==> Section table: 128 (0x80) [= DVB CA message section (EMM/ECM)]
Data-Bytes:
0000: 00 80 70 34 70 32 64 21 73 23 94 50 78 96 b0 9f ..p4p2d!s#.Px...
0010: 3e ec 43 32 f7 cc cb 26 9b 68 52 f7 bd 8f ae d5 >.C2...&.hR.....
0020: c6 d9 3d da cc cc 58 68 95 f2 a0 14 47 cd d8 e3 ..=...Xh....G...
0030: 3d 28 fa f9 11 b0 25 7e ff ff ff ff ff ff ff ff =(....&~.....
0040: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
0050: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
0060: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
0070: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
0080: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
0090: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
00a0: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
00b0: ff ff ff ff ff ff ff ff .....
=====
```

ECM-пакет системы TVCAS

Connect 2 служит для передачи EMM-пакетов. EMMG генерирует пакеты для каждой смарткарты (если её статус активен) и передаёт в MUX. Таким образом, каждый EMM-пакет предназначен только конкретной **своей** смарткарте.

```
PID: 90 (0x005a) [= ]
transport_scrambling_control: 0 (0x00) [= No scrambling of TS packet payload]
adaptation_field_control: 1 (0x01) [= no adaptation_field, payload only]
continuity_counter: 7 (0x07) [= (sequence ok)]
Payload: (len: 184)
==> pointer_field: 0 (0x00)
==> Section table: 130 (0x82) [= DVB CA message section (EMM/ECM)]
Data-Bytes:
0000: 00 82 70 3b 00 00 00 7d 2b 75 07 70 32 64 10 18 ..p;...}+u.p2d..
0010: f1 e0 69 44 99 d8 96 43 fc c3 f4 8f a5 93 85 0f ..iD...C.....
0020: 9e be 96 78 00 00 00 00 00 00 00 00 00 00 00 00 ...x.=.....@....
0030: 6b fd 35 5c ea bb 9c c5 32 54 b3 d2 bf 04 b4 ff k.5\....2T.....
0040: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
0050: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
0060: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
0070: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
0080: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
0090: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
00a0: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
00b0: ff ff ff ff ff ff ff ff .....
=====
```

serial number card (points to 0000-0007)

encrypted data (points to 0008-003f)

EMM-пакет системы TVCAS

Данные криптируются алгоритмом, схожим на [ГОСТ Р](#). В нём используется [сеть Фейстеля](#) и многораундовый битовый сдвиг. В алгоритме (файл `/cas/bin/gost.php`) тайного ничего нет, напротив, согласно [Принципа Керкгоффса](#), работа криптоустойчивых систем должна быть известна. Секретом здесь является лишь КЛЮЧ. Без него расшифровать пакет не представляется возможным. Ключи находятся в базе данных сервера TVCAS и на запрограммированных смарткартах. Если со смарткартами всё безопасно — фьюзами установлена защита от чтения кода и памяти, то с сервером куда сложнее — побеспокойтесь о безопасности ключей, начиная от персонала, заканчивая использованием для этой цели локальной машины без выхода в Интернет!

Установка сервера.

Установку TVCAS-сервера рекомендуется производить на [Debian 8.11](#) с PHP5. На более современных релизах, вероятно, придётся корректировать работу с базой данных MariaDB.

```
# пакеты, необходимые после установки ОС

apt-get install mc sudo apache2 php5 libapache2-mod-php5 mysql-server
php5-mysql
```

1. При установке пакета **mysql-server** зададим пароль к БД. Например tvmastercas

2. Добавить в файл `/etc/sudoers` следующие строки:

```
www-data ALL=(ALL) NOPASSWD: /usr/bin/perl

www-data ALL=(ALL) NOPASSWD: /var/www/html/cas/bin/ecmg.php

www-data ALL=(ALL) NOPASSWD: /var/www/html/cas/bin/emmg.php

www-data ALL=(ALL) NOPASSWD: /bin/kill

www-data ALL=(ALL) NOPASSWD: /bin/rm

www-data ALL=(ALL) NOPASSWD: /usr/bin/tail

# перезапускаем сервис sudo
service sudo restart
```

3. Добавить в файл `/etc/crontab` следующие строки (не забываем про перенос каретки [ENTER] в конце строки):

```
*/1 * * * * root /var/www/html/cas/bin/cronlmin.php &
```

4. Качаем и распаковываем на сервер файлы
(строки ниже актуальны также для обновления системы):

```
rm -rf /var/www/html

wget https://tvcas.com/downloads/tvcas2.tar.gz

tar -C /var/www -xf tvcas2.tar.gz

rm tvcas2.tar.gz
```

5. Создаём и импортируем базу данных MySQL:

```
mysql -uroot -ptvmastercas

> CREATE DATABASE tvcas DEFAULT CHARACTER SET UTF8;

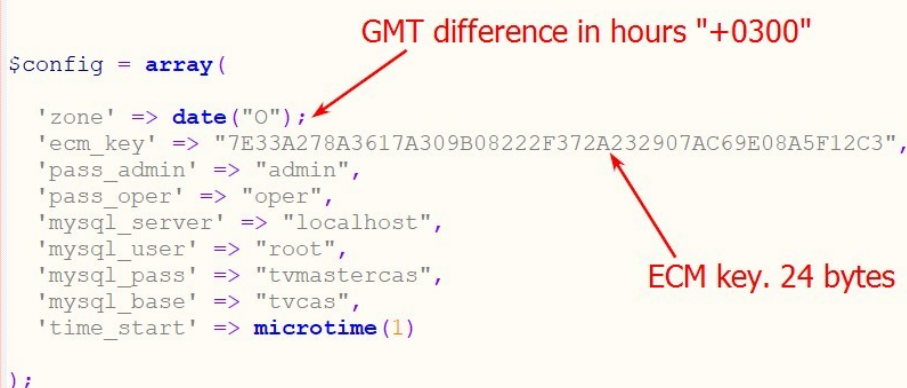
> exit

mysql -uroot -ptvmastercas tvcas < /var/www/html/tvcas.sql

rm /var/www/html/tvcas.sql
```

WEB-ИНТЕРФЕЙС имеет две точки входа. Вход для **администратора** системы (<http://xx.xx.xx.xx/cas, admin/admin>), здесь доступны логи, создание новых смарткарт, генераторов и вход для **оператора** системы (<http://xx.xx.xx.xx/, oper/oper>) — панель с базовыми функциями просмотра/управления.

Пароли к пользователям можно изменить в файле **/var/www/html/includes/config.php**:



```
$config = array(

    'zone' => date("O");
    'ecm_key' => "7E33A278A3617A309B08222F372A232907AC69E08A5F12C3",
    'pass_admin' => "admin",
    'pass_oper' => "oper",
    'mysql_server' => "localhost",
    'mysql_user' => "root",
    'mysql_pass' => "tvmastercas",
    'mysql_base' => "tvcas",
    'time_start' => microtime(1)

);
```

/var/www/html/includes/config.php

Если ваш PHP настроен на местный часовой пояс (файл `php.ini`), то параметр `zone` оставляем как есть. Если нет, то, например, для Москвы (Europe/Moscow) `'zone' => «+0300»`. Обратите внимание на параметр `ecm_key`. Во избежание дублирования ключей у разных операторов, при каждом скачивании с-

tvcas.com, в архиве он будет другой! (отключил 04.02.2020. меняйте ключи самостоятельно) Хотя ничего не мешает использовать лично сгенерированный ключ. Важно, чтобы он был в hex длиной 24 байта. В любом случае, рекомендую этот ключ сохранить в надёжном месте под паролем, потому как от его сохранности зависит безопасность системы в будущем.

The screenshot shows the TVCAS Admin Panel interface. At the top, there is a navigation bar with links: Admin Panel, My Smartcards, ECM Generators, EMM Generators, Logs, and Exit. A search bar for smartcards is also present. Below the navigation bar, there are buttons for 'Add new', 'Add multiple', 'Export CSV', and 'Import CSV'. The main area contains a table with columns: #, serial_no, name, info, access_criteria, type, start, finish, edit, and OPER. The table lists six smartcards with their respective details. At the bottom of the table, there is a footer with the text: 'Localtime: 07:21:40 (+0300). Page generated at 0,036 sec. ©2018-2019 Copyright by TVCAS.COM'. Below the screenshot, the text 'Админка TVCAS — Смарткарты' is displayed.

#	serial_no	name	info	access_criteria	type	start	finish	edit	OPER
1	210-000-000-0	Ivan Petrov	Moscow, Pupkina st. 3-5	11111111	1	16.09.2019 at 19:17	16.10.2019 at 19:17	Today at 07:17	[Icons]
2	210-000-000-1	Alexandr Zel	Moscow, Zelenaya st. 23/2-9	11111111	1	16.09.2019 at 19:17	16.10.2019 at 19:17	Today at 07:17	[Icons]
3	210-000-000-2	Marina Sreblo	Moscow, Lenina st. 1	11111111	1	16.09.2019 at 19:17	16.10.2019 at 19:17	Today at 07:18	[Icons]
4	210-000-000-3	Vasya Nalivaykin	Moscow, Siniya st. 10-256	00000000	1	16.09.2019 at 19:17	16.10.2019 at 19:17	Today at 07:19	[Icons]
5	210-000-000-4	Mr. V.Putin	Moscow, Krasnaya square 1	11111111	1	16.09.2019 at 19:17	16.10.2019 at 19:17	Today at 07:20	[Icons]
6	210-000-000-5	Ms. Eva Brown	Moscow, Sovetskaya 3-25	11111111	1	16.09.2019 at 19:17	16.10.2019 at 19:17	Today at 07:21	[Icons]

Для наглядности, в установленной «из коробки» системе уже добавлены несколько карт и по одному генератору ЕСМ и ЕММ. ЕММ-ключи для каждой карты также генерируются уникальными при каждой загрузке архива с сайта. (отключил 04.02.2020. меняйте ключи самостоятельно) Создание и программирование карт оставим на потом, а сейчас посмотрим как связать между собой сервер TVCAS и Astra 5.65. Кстати, версия 5.64 тоже будет работать, но там есть нюансы с клонированием ЕММ, поэтому рекомендую именно 5.65.

Настройка ASTRA

The screenshot shows the ASTRA web interface. The 'Settings' tab is selected and highlighted with a red circle. A dropdown menu is open, showing various configuration options. The 'CAS' option is highlighted with a red circle and a mouse cursor. The background shows a list of streams on the left and right, including '_FOX HD', '_NGC HD', 'TK Витебск HD', '_National Geographic', and 'Камера коридор'.

- Interface
- General
- Users
- HLS
- HTTP Play
- HTTP Authentication
- Softcam
- CAS**
- Servers
- Groups
- Edit Config
- License
- Restart

CAS
TVCAS

NAME
TVCAS

SUPER CAS ID (HEX)
0B000001

☒ Start Stream ID with 1

ECMG CHANNEL ID
1

ECMG ADDRESS
192.168.2.26

ECMG PORT
43000

CRYPTO PERIOD
10

address
port our ECMG on TVCAS-server
[for connect 1]

every 10 seconds a key is requested from the smartcard

ECMG PROTOCOL
Default: TCP

port Astras for [connect 2]

ECMG PORT
41000

ECMG PID
90

this PID will be EMM-packets in stream

ECMG PRIVATE DATA (HEX)

not work in Astra 5.64

☒ EMM Clone (duplicate EMM packets to all streams)

☐ Remove

Dashboard Sessions Settings Log

General Groups **Service** Remap Backup EPG

SERVICE TYPE
Default: original service type

SERVICE PROVIDER

SERVICE NAME

CODEPAGE
Default: Latin (ISO 6937)

HBBTV URL

CONDITIONAL ACCESS

CAS #1
TVCAS [0B000001]

ECM PID
89

ECM PRIVATE DATA (HEX)

ACCESS CRITERIA (HEX)
00000001

press NEW CAS

select our CAS

this PID will be EMM-packets in stream

what packages does the channel belong to

NEW CAS

REMOVE CAS

APPLY CLONE

Коснёмся параметра **ACCESS CRITERIA**. Как упоминалось выше, он отвечает за пакетирование. Каждая цифра — это свой пакет. Таким образом, если у вас всего три пакета, то используйте, например, три его последние цифры. При вводе поддерживаются «0» и «1». На рисунке выше канал принадлежит «первому» пакету, если бы мы ввели 01010101, то канал принадлежал бы «первому», «третьему», «пятому» и «седьмому» пакетам.

После проделанных настроек, Astra необходимо перезапустить, т.к. созданный EMM-порт открывается только при её старте.

Если вы всё сделали правильно, то на вкладках генераторов в панели администратора увидим коннекты.

Admin Panel
My Smartcards
ECM Generators
EMM Generators
Logs
Exit

Add new

#	id	info	port	peers	touch_time	timeout	Create	Moder	OPER
1	23	MY NEW ECMG	43000	Today at 14:41:14 - 192.168.2.40:52498, cw=0, ecm=0 [log]	Today at 14:41:08	60	16.09.2019 at 16:23:23	16.09.2019 at 19:14:47	

Localtime: 14:41:16 (+0300). Page generated at 0,003 sec.
©2018-2019 Copyright by TVCAS.COM

Astra

Admin Panel
My Smartcards
ECM Generators
EMM Generators
Logs
Exit

Add new

#	id	info	host	port	timeout	client_id	touch_time	stream_time_open	datagram_time_last	datagram_count	queue_size	OPER
1	11	MY NEW EMMG	192.168.2.40	41000	60	0x0b000001	Today at 14:43:02	Today at 14:43:02	Today at 14:43:22	2	6	

Localtime: 14:43:27 (+0300). Page generated at 0,002 sec.
©2018-2019 Copyright by TVCAS.COM

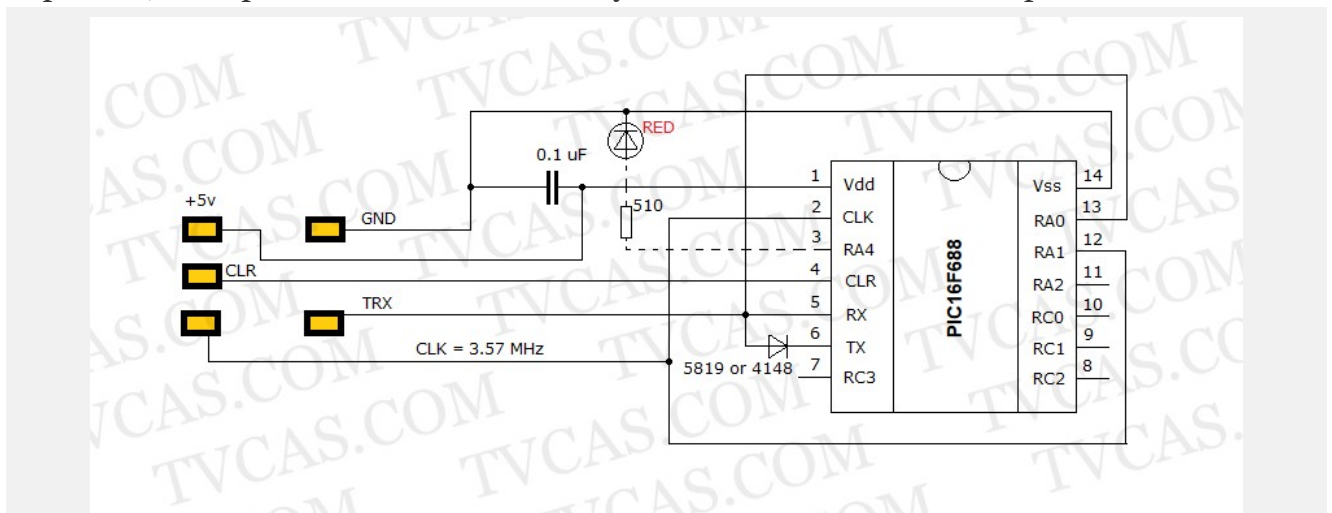
Astras ip and port

EMM

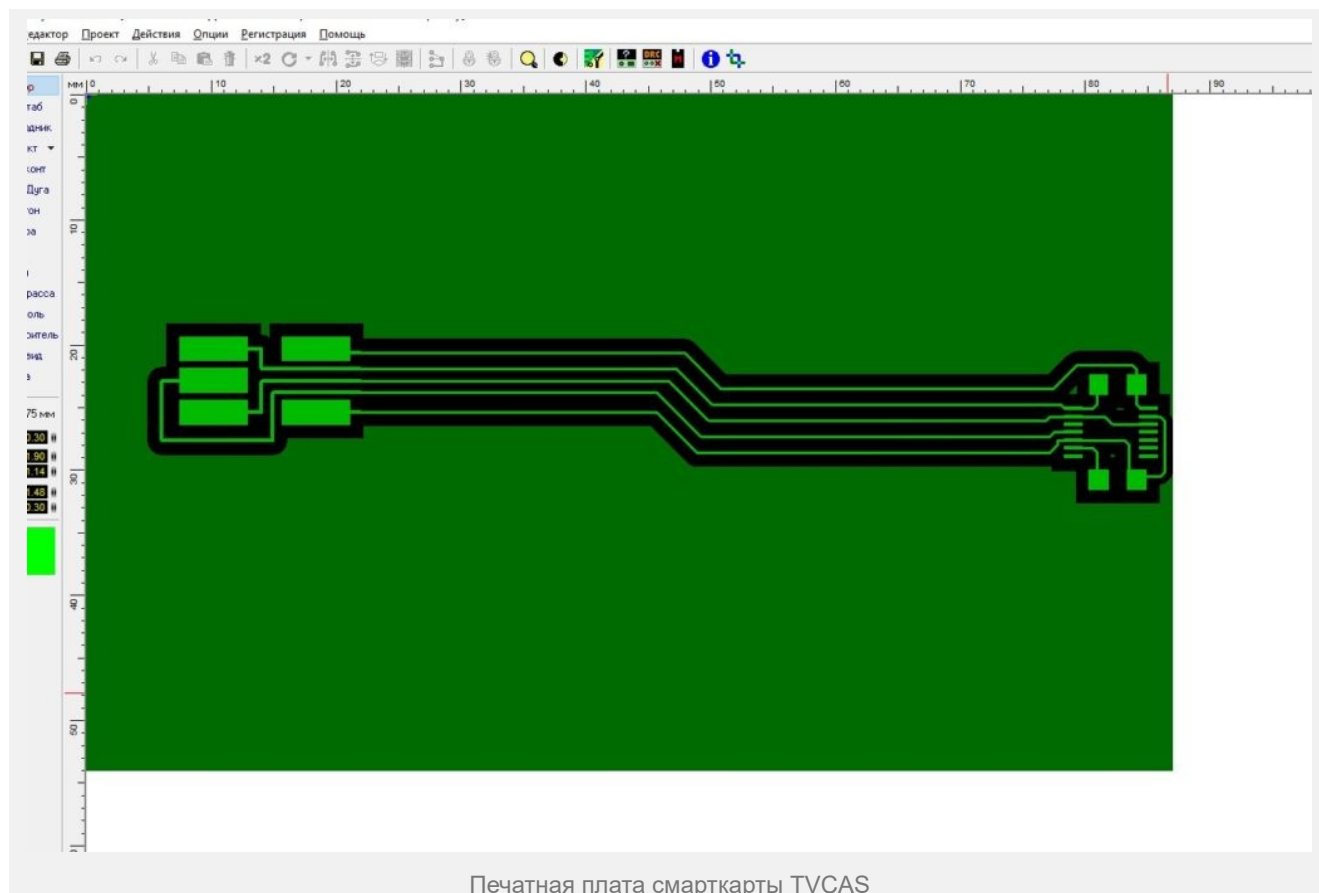
Если у вас всё получилось и работает как на картинках, то переходим к самому интересному, на мой взгляд.

СМАРТКАРТЫ системы TVCAS

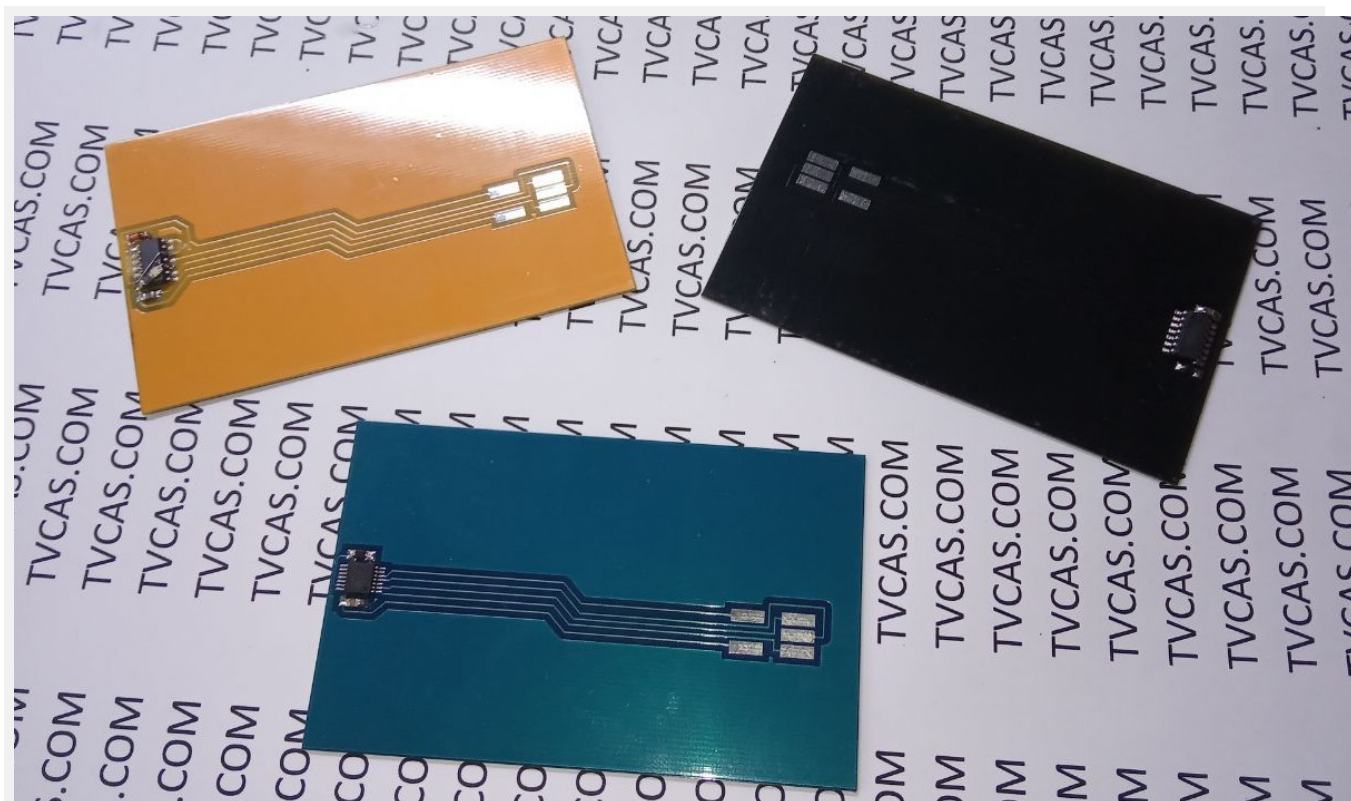
Самой затратной частью в разработке этого проекта пришлось именно смарткарты. Хотя, затраты были связаны как раз с поиском подходящей «белки-болванки», которую можно было запрограммировать под свои нужды. Я даже сделал несколько закупок Java-карт в Канаде и Америке, ведь продавцы утверждали, что кастомный ATR они умеют. Но как оказалось выброшенные деньги. На ebay есть некоторые интересные варианты, но ценник в 10\$ за штуку считаю не демократичным. Поэтому решил разработать свои. Себестоимость без учёта работы получилась около 1.5\$/шт. Вероятно, что при БОЛЬШИХ объёмах закупки в Китае можно договориться о скидке.



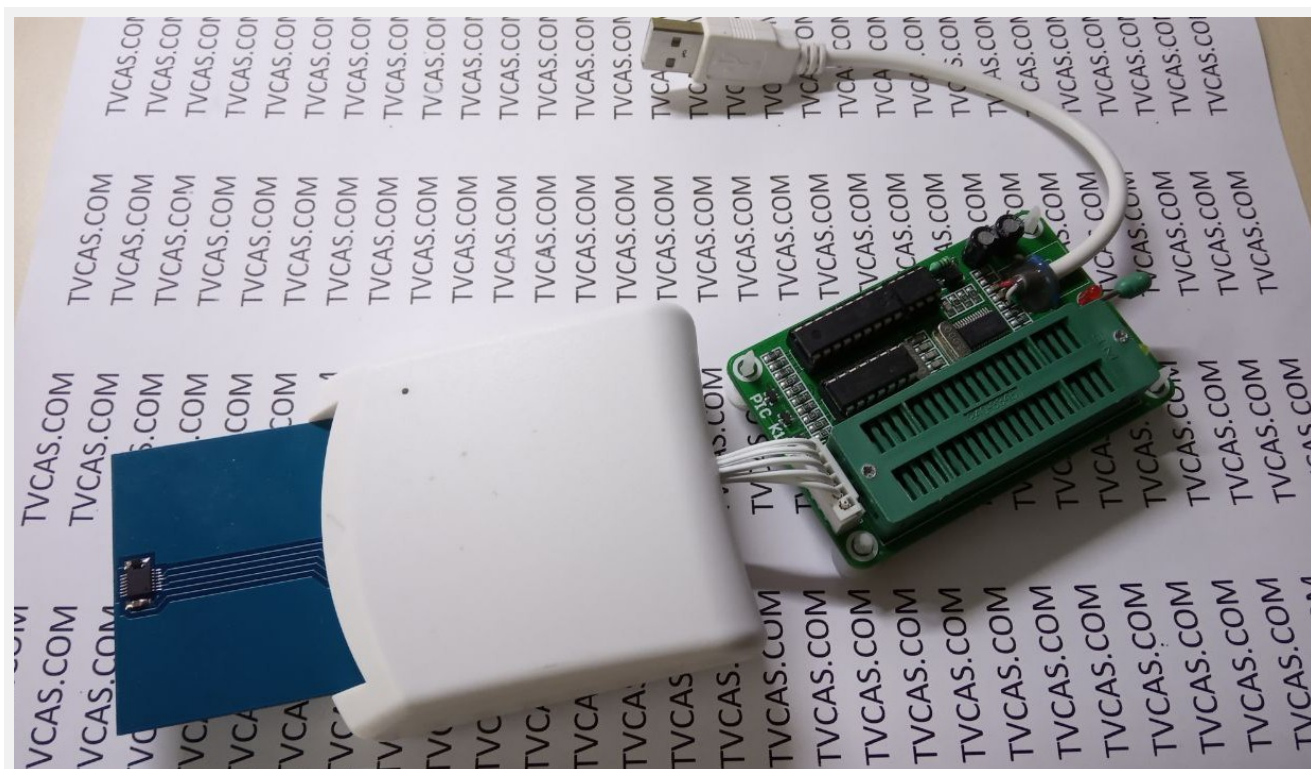
Смарткарта выполнена на одностороннем текстолите, толщиной около 0.8 мм. Заготовки можно заказать на pcbway.com([download](#) LAY и Gerber). [Здесь](#) можно залить проект в гербере и повертеть печатную плату в 3D.



На плате размещены три детали: PIC-контроллер, конденсатор по питанию 0.1 мкФ (типоразмер 0805) и диод с барьером Шоттки. Пунктиром показана необязательная часть, служащая для отладки прошивки: в нормальном режиме работы при скорости 9600 бод (в оскаме или приставке) диод мигает короткой вспышкой при ЕСМ-пакете и длинной при ЕММ. При скорости 55800 бод (работа в САМ-модуле) диод напротив, — горит постоянно, а тухнет кратковременно при ЕСМ и продолжительно при ЕММ-пакетах.



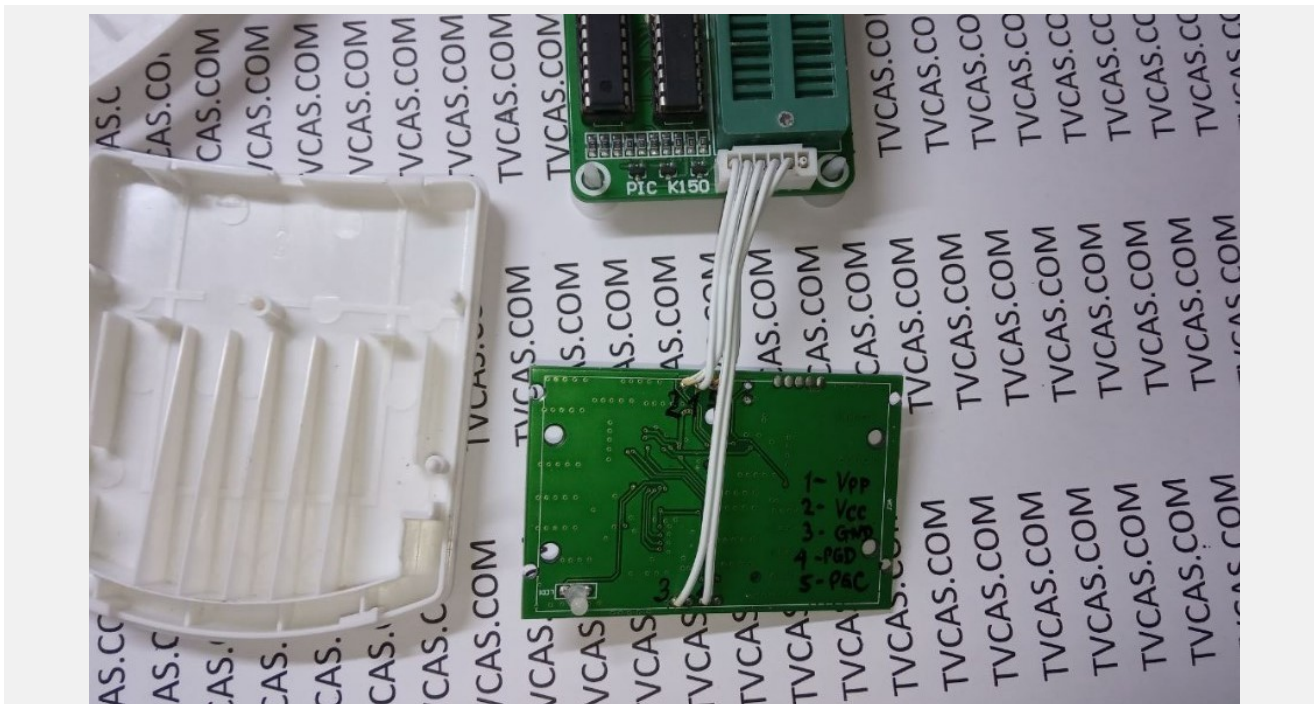
Для прошивки карт подойдёт любой программатор PIC-контроллеров. Пользовался я [PIC-K150](#) , но учитывая, что в современных Windows всё больше и больше проблем с СОМ-портами, буду рекомендовать [PICKIT2](#) как стабильный.

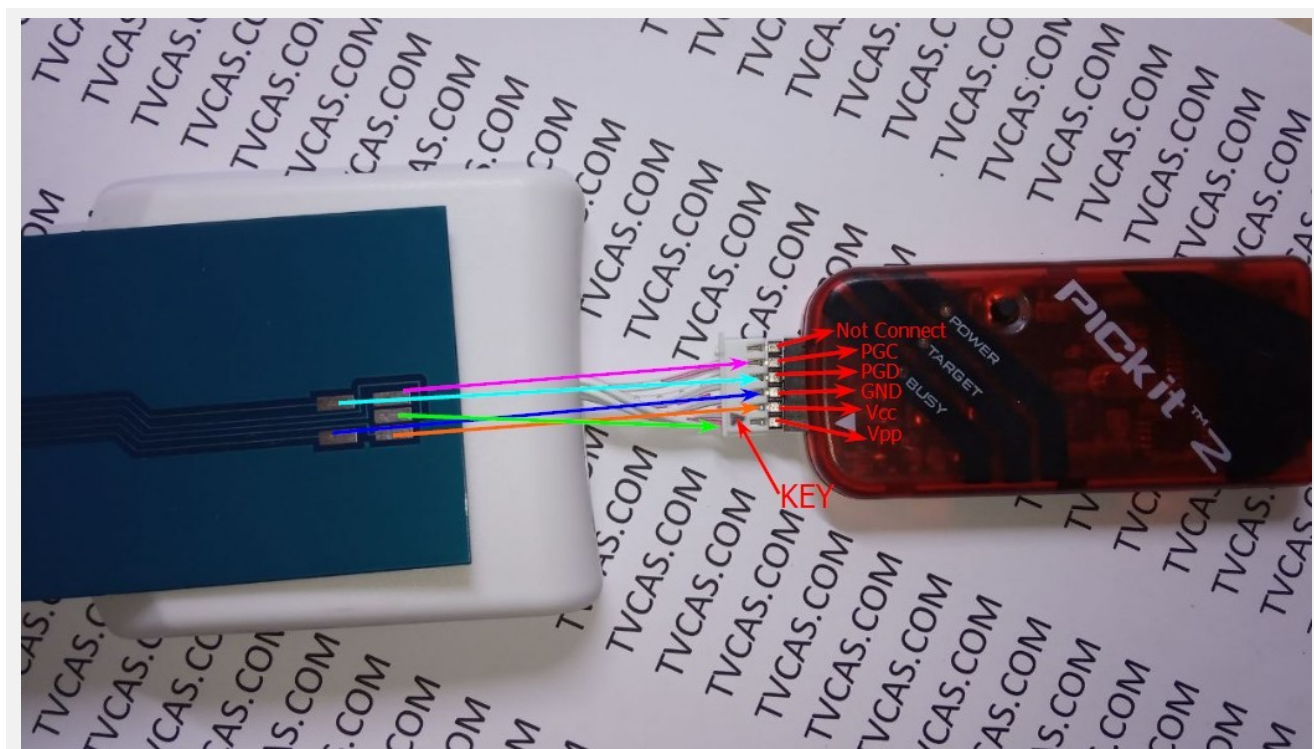




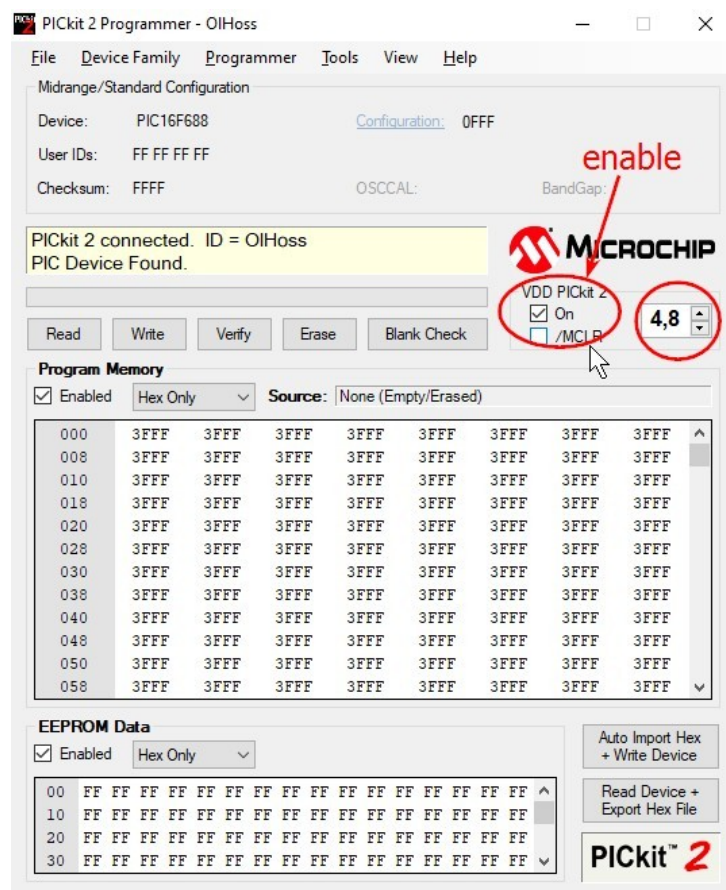
Обратите внимание, что на обоих программаторах я припаял шнуры USB. Советую и вам делать то же самое. Укорачивать не обязательно, если только у вас не ноутбук, а вот пайка не повредит, а только избавит от головной боли с китайскими разъёмами.

При программировании большого количества смарткарт, необходимо сделать слот из какого-нибудь картридера. Я использовал [MicroUSB EMV](#). Более менее жёлтые, похожие на позолоту коннекторы, внулили, что прослужит этот слот долго))). Все радиоэлементы с платы я удалил, а к сокету припаял разъём ICSP.



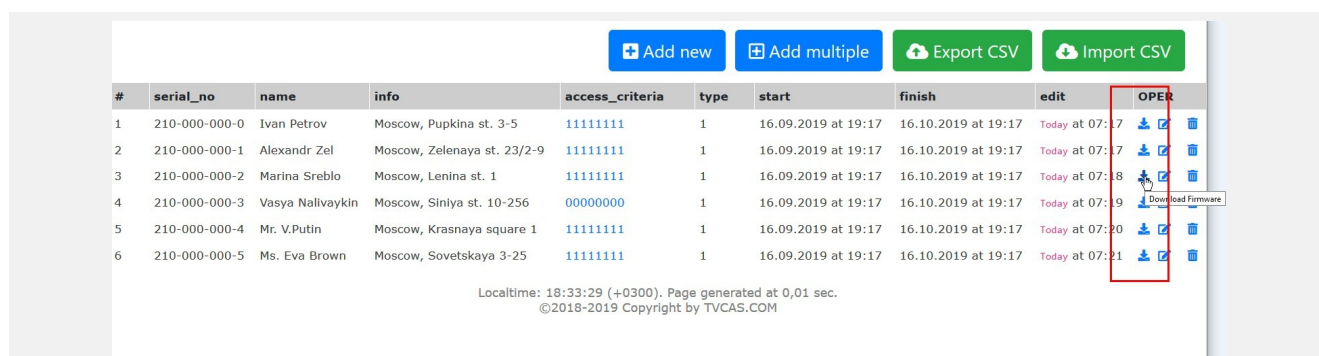


[Программу для программаторов PICKIT2](#) на сайте Microchip-а вы не найдёте, потому что компания прекратила поддержку данного девайса из-за китайских клонов. Работают они, к слову, ничуть не хуже оригинальных, а стоят в разы дешевле. После установки драйверов и запуска программы PicKit2 видим такой интерфейс...



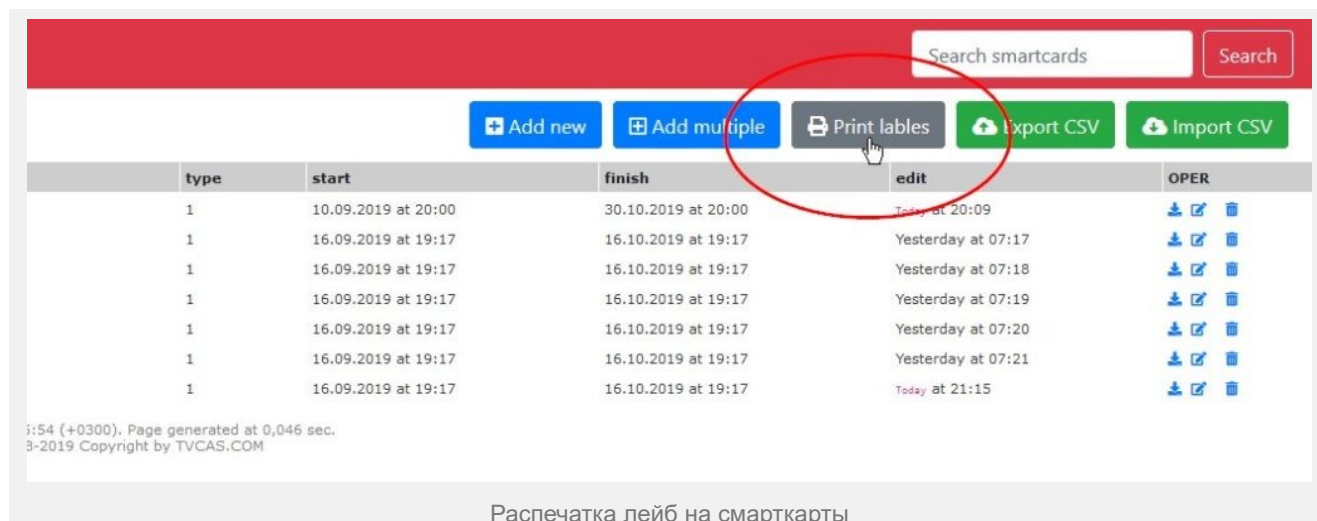
Если смарткарта подключена, то программмер определит автоматом тип микросхемы. Единственное, что дополнительно надо сделать — это включить VDD и выставить питание 4.8 В. Это необходимо для прошивки китайских вариантов PIC-ов. И не судите строго — они не подделки. Просто оригинальные с магазина идут «чистые», а китайские — с какой-то записанной прошивкой. Вероятно, что «боевой» запас какого-то завода))). Перепрошиваются они легко. Работоспособность проверена, нюансов не обнаружено.

Если вы были внимательными, то в панели администратора напротив каждой смарткарты имеется значок «Download Firmware»..



Скачиваем прошивку (для каждой карты своя) и заливаем её через программмер в смарткарту: **File -> Import HEX**, затем клавиша **Write**.

Если Вы создали смарткарты в течение 3 последних часов, то появится кнопка «Print labels» по нажатию на которую можно распечатать номера карт (например на самоклейке) и таким образом пометить прошитые карточки.



Теперь карту можно использовать совместно с САМ-модулем или в приставке.

Больше информации в группе в телеграмме <https://t.me/tvcas>
Там много чего интересного!