

Протокол JSON для настольного считывателя PW Desktop

Ревизия 1.01

Оглавление

Описание устройства	3
Драйвер USB ↔ COM.....	3
Сервис для конвертации JSON запросов	3
Параметры подключения	3
Мобильные приложения Proxway	3
Общие информационные команды	4
Информация об устройстве.....	4
Режим работы считывателя (разрешенные типы идентификаторов)	4
Получение текущего режима работы считывателя.....	4
Установка нового режима работы считывателя	4
Получение информации об оставшемся количестве мобильных идентификаторов	5
Чтение кодов идентификаторов	5
Описание форматов вывода	5
Процедура чтения существующего мобильного идентификатора с помощью PW Desktop	8
Выпуск мобильных идентификаторов.....	9
Локальная выдача идентификаторов.....	9
Выдача идентификаторов по e-mail	9
Описание форматов вывода	12
Отправка по e-mail	12
Дополнительная защита систем доступа (персонификация идентификаторов).....	13
Определение, включен ли режим шифрования идентификаторов	13
Установка режима шифрования мобильных идентификаторов.....	13
Включение режима шифрования и установка пароля шифрования	13
Выключение режима шифрования и очистка пароля.....	13
Установка режима шифрования Mifare®	14
Установка режима шифрования	14
Установка режима шифрования с персонифицированным номером идентификатора	14
Отключение режима шифрования	15
Выпуск зашифрованной карты.....	15
Настройка отправки электронной почты сервисом JSON при выдаче мобильных идентификаторов по e-mail ..	16

Описание устройства

Настольный считыватель ASK / FSK / Mifare и поддержкой BLE с USB интерфейсом и открытым текстовым протоколом предназначен для максимально простой интеграции в любую систему СКУД.

Может использоваться для выдачи мобильных идентификаторов из выделенного списка мобильных идентификаторов.

Характеристики

RF ID ASK, FSK, ASK+FSK (125 кГц)
Mifare (ISO 14443A - 13,56 МГц)
Чтение мобильных идентификаторов PW ID.
Выдача мобильных идентификаторов PW ID из выделенного списка мобильных идентификаторов. Переход в режим выдачи PW ID по мастер-карте.
Обмен данными со смартфонами по Bluetooth Low Energy (Bluetooth Smart, BLE)
Используется зашифрованный 256-битным ключом и стойкий к саботажу протокол для обмена данными со смартфонами
Программирование PW Desktop по BLE со смартфона с Android с помощью ПО PW Config по BLE - устанавливается размерность (битность) идентификаторов, загружаются лицензии на мобильные идентификаторы.

Драйвер USB ↔ COM

Для эмуляции COM порта в системе используется SyLabs CP210x USB to UART мост.

Драйвера можно скачать по следующей ссылке:

<http://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers>

Сервис для конвертации JSON запросов

Для работы с настольным считывателем в протоколе JSON предназначено программное обеспечение Acs.DesktopService.exe. Текущая поддерживаемая платформа – Windows, необходимо наличие .NET4.5

Исполняемые файлы и bat файл для установки программы как системного сервиса размещены в каталоге Software.

Запуск исполняемого файла или bat файла для установки следует выполнять от имени администратора.

Параметры подключения

POST запросы на <http://127.0.0.1:40011>

Мобильные приложения Proxway



Конфигуратор PW Config
для Android



Мобильный идентификатор PW ID
для Android



Мобильный идентификатор PW ID
для iOS

Общие информационные команды

Информация об устройстве

С помощью данной команды можно **получить** информацию об устройстве - его серийном номере и версии микропрограммы

Запрос:

```
http://localhost:40011/GetVersion
```

Тело запроса:

```
{  
}
```

Ответ:

```
{  
  "Model": "DESKTOP READER",  
  "Serial": "00:32:00:17:00:20",  
  "Version": "09.35"  
}
```

Режим работы считывателя (разрешенные типы идентификаторов)

С помощью данной команды можно включить или отключить работу (чтение и запись) с определенными типами идентификаторов.

Получение текущего режима работы считывателя

Запрос:

```
http://localhost:40011/GetReaderType
```

Тело запроса:

```
{  
}
```

Ответ:

```
{  
  "BLEEnabled": true  
  "MifareEnabled": true  
  "FSKEnabled": true  
  "ASKEEnabled": true  
}
```

Установка нового режима работы считывателя

Запрос:

```
http://localhost:40011/SetReaderType
```

Тело запроса:

```
{  
  "BLEEnabled": true  
  "MifareEnabled": true  
  "FSKEnabled": true  
  "ASKEEnabled": true  
}
```

Ответ:

```
{  
  "BLEEnabled": true  
  "MifareEnabled": true  
  "FSKEnabled": true  
  "ASKEEnabled": true  
}
```

Получение информации об оставшемся количестве мобильных идентификаторов

Устройство используется для выдачи мобильных идентификаторов из выделенного списка. Базовая поставка включает 5 бесплатных идентификаторов.

С помощью данной команды можно посмотреть количество неиспользованных лицензий в списке мобильных идентификаторов.

Запрос:

```
http://localhost:40011/GetQuantity
```

Тело запроса:

```
{
}
```

Ответ:

```
{
  "Quantity": 58
}
```

Чтение кодов идентификаторов

С помощью данной команды можно получить код идентификатора в заданных форматах.

Запрос:

```
http://127.0.0.1:40011/GetIdentifiers
```

Тело запроса по умолчанию, выводимый формат кода hex5:

```
{
}
```

Ответ:

```
{
  "Identifiers": [ "String content", "String content", "String content" ]
}
```

Описание форматов вывода

"Raw" – без преобразований, как получено от считывателя

Запрос:

```
http://127.0.0.1:40011/GetIdentifiers
```

Тело запроса:

```
{
  "OutputAs": "Raw"
}
```

Получение данных:

```
{
  "Identifiers": ["Em-Marine[565A] 123,16044"]
}
```

Например:

```
{
  "Identifiers": [
    "Mifare[E4009A14] 000,39444 1K (0004,08)",
    "Mifare[04B62AE1BB0280] 182,10977 UL (0044,00)",
    "Mifare[C2ECA99C] 236,43420 4K (0002,18)",
    "Mifare[04210D21B21C80] 033,03361 DF (0344,20)",
    "CryptedMifare[01EB931000] 147,04096 1K (0004,08)",
    "Em-Marine[565A] 123,16044",
    "FSK[00120040] 08111",
    "FSK[0010029A] 38193",
    "MobileID[1122334455667788]"
  ]
}
```

Где:

- Mifare – карточки Mifare® стандарта ISO14443a,
- CryptedMifare – персонализированная карта (дополнительно защищенная) с индивидуальным кодом.
- Em-Marine – карточки с амплитудной модуляцией (ASK),
- FSK – карточки с частотной модуляцией
- MobileID – мобильный идентификатор, полученный от смартфона.

"FacilityCode" – отображение в формате facility.code. Код усекается до 3-х байт, старшая часть отбрасывается.

Запрос:

<http://127.0.0.1:40011/GetIdentifiers>

Тело запроса:

```
{
  "OutputAs": "FacilityCode"
}
```

Получение данных:

```
{
  "Identifiers": ["123,16044"]
}
```

"Dec3" – отображение кода в десятичном формате. Код усекается до 3-х байт, старшая часть отбрасывается.

Запрос:

<http://127.0.0.1:40011/GetIdentifiers>

Тело запроса:

```
{
  "OutputAs": "Dec3"
}
```

Получение данных:

```
{
  "Identifiers": ["08076972"]
}
```

"Hex3" – отображение кода в шестнадцатеричном формате. Код усекается до 3-х байт, старшая часть отбрасывается.

Запрос:

<http://127.0.0.1:40011/GetIdentifiers>

Тело запроса:

```
{
  "OutputAs": "Hex3"
}
```

Получение данных:

```
{
  "Identifiers": ["7B3EAC"]
}
```

"Hex4" – отображение кода в шестнадцатеричном формате. Если код длиннее - усекается до 4-х байт (старшая часть отбрасывается) если короче – дополняется нулями (старшая часть)

Запрос:

<http://127.0.0.1:40011/GetIdentifiers>

Тело запроса:

```
{
  "OutputAs": "Hex4"
}
```

Получение данных:

```
{
  "Identifiers": ["5A7B3EAC"]
}
```

"Hex5" — отображение кода в шестнадцатеричном формате. Если код длиннее - усекается до 5-х байт, если короче – дополняется нулями (старшая часть)

Запрос:

<http://127.0.0.1:40011/GetIdentifiers>

Тело запроса:

```
{
  "OutputAs": "Hex5"
}
```

Получение данных (карточка Em-Marine):

```
{
  "Identifiers": ["565A7B3EAC"]
}
```

Получение данных (карточка FSK):

```
{
  "Identifiers": ["000010029A"]
}
```

"Hex5f3" — отображение кода в шестнадцатеричном формате. Код усекается до 3-х байт (старшая часть отбрасывается) и далее дополняется нулями до 5-ти байт (старшая часть)

Запрос:

<http://127.0.0.1:40011/GetIdentifiers>

Тело запроса:

```
{
  "OutputAs": "Hex5f3"
}
```

Получение данных (карточка Em-Marine):

```
{
  "Identifiers": ["00007B3EAC"]
}
```

"Hex6" – отображение кода в шестнадцатеричном формате. Если код длиннее - усекается до 6-ти байт (старшая часть отбрасывается) если короче – дополняется нулями (старшая часть)

Запрос:

<http://127.0.0.1:40011/GetIdentifiers>

Тело запроса:

```
{
  "OutputAs": "Hex6"
}
```

Получение данных (карточка Em-Marine):

```
{
  "Identifiers": ["00565A7B3EAC"]
}
```

Получение данных (мобильный идентификатор):

```
{
  "Identifiers": ["334455667788"]
}
```

"Hex7" – отображение кода в шестнадцатеричном формате. Если код длиннее - усекается до 7-ми байт (старшая часть отбрасывается) если короче – дополняется нулями (старшая часть)

Запрос:

<http://127.0.0.1:40011/GetIdentifiers>

Тело запроса:

```
{
  "OutputAs": "Hex7"
}
```

Получение данных (карточка Em-Marine):

```
{
  "Identifiers": ["0000565A7B3EAC"]
}
```

Получение данных (мобильный идентификатор):

```
{
  "Identifiers": ["22334455667788"]
}
```

"Hex8" – отображение кода в шестнадцатеричном формате. Если код длиннее - усекается до 8-ми байт (старшая часть отбрасывается) если короче – дополняется нулями (старшая часть)

Запрос:

<http://127.0.0.1:40011/GetIdentifiers>

Тело запроса:

```
{
  "OutputAs": "Hex8"
}
```

Получение данных (карточка Em-Marine):

```
{
  "Identifiers": ["000000565A7B3EAC"]
}
```

Получение данных (мобильный идентификатор):

```
{
  "Identifiers": ["1122334455667788"]
}
```

Процедура чтения существующего мобильного идентификатора с помощью PW Desktop

1. Пользователь подносит смартфон к PW Desktop , и запускает или активирует мобильное приложение PW ID
2. Настольный считыватель получает код от смартфона
3. Код полученного мобильного идентификатора выводится в COM порт
4. Сервис JSON сохраняет полученный код в памяти и далее по http POST-запросу <http://127.0.0.1:40011/GetIdentifiers> передает в приложение.

Выпуск мобильных идентификаторов

Устройство используется для выдачи мобильных идентификаторов из выделенного списка. Базовая поставка включает 5 бесплатных идентификаторов.

Код идентификатора будет получен также, как и при обычном чтении кодов, с помощью запроса <http://127.0.0.1:40011/GetIdentifiers>.

Локальная выдача идентификаторов

Процедура локальной выдачи нового идентификатора с помощью PW Desktop

1. Администратор системы переводит настольный считыватель в режим выдачи идентификаторов – размещает на считывателе мастер-карту.
2. Пользователь подносит смартфон к PW Desktop, и в настройках приложения PW ID нажимает кнопку "Получить от Desktop"- приложение соединяется и получает мобильный идентификатор из выделенного списка мобильных идентификаторов.
3. Код полученного мобильного идентификатора выводится в COM порт
4. Сервис JSON сохраняет полученный код в памяти и далее по http POST-запросу <http://127.0.0.1:40011/GetIdentifiers> передает в приложение.

Запрос:

```
http://127.0.0.1:40011/GetIdentifiers
```

Тело запроса:

```
{
  "OutputAs": "Raw"
}
```

Получение данных:

```
{
  "Identifiers": ["NewMobileID[1122334455667788]"]
}
```

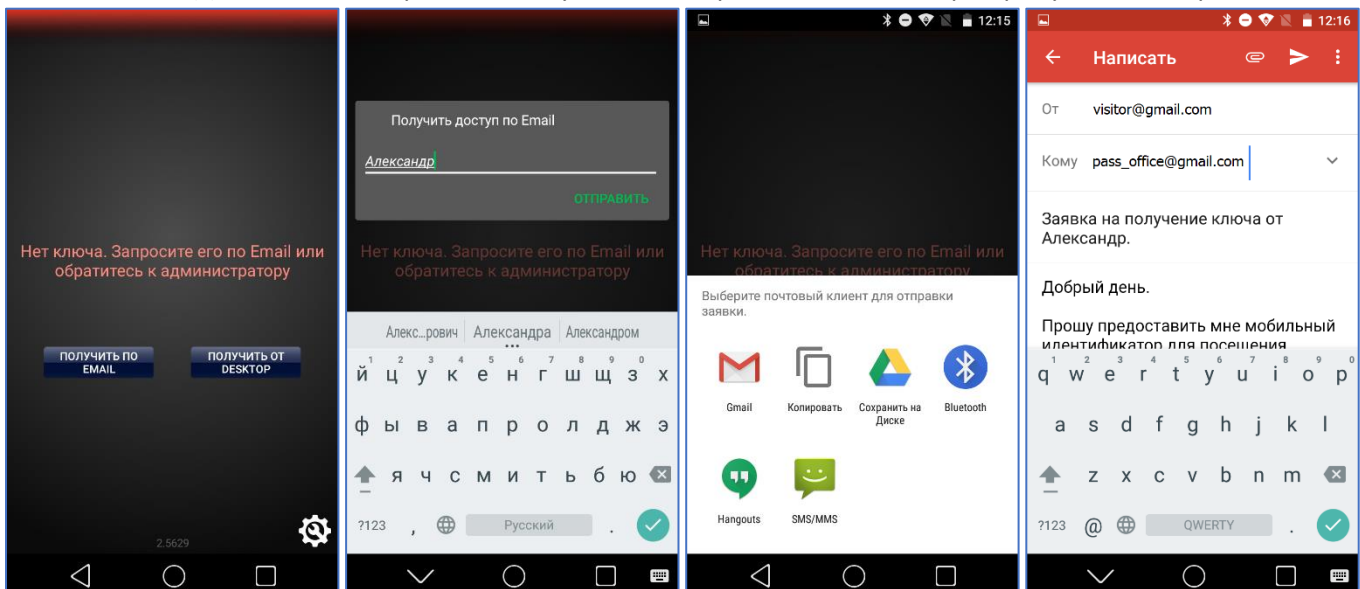
Выдача идентификаторов по e-mail

С помощью сервиса JSON и PW Desktop возможна выдача мобильных идентификаторов по e-mail

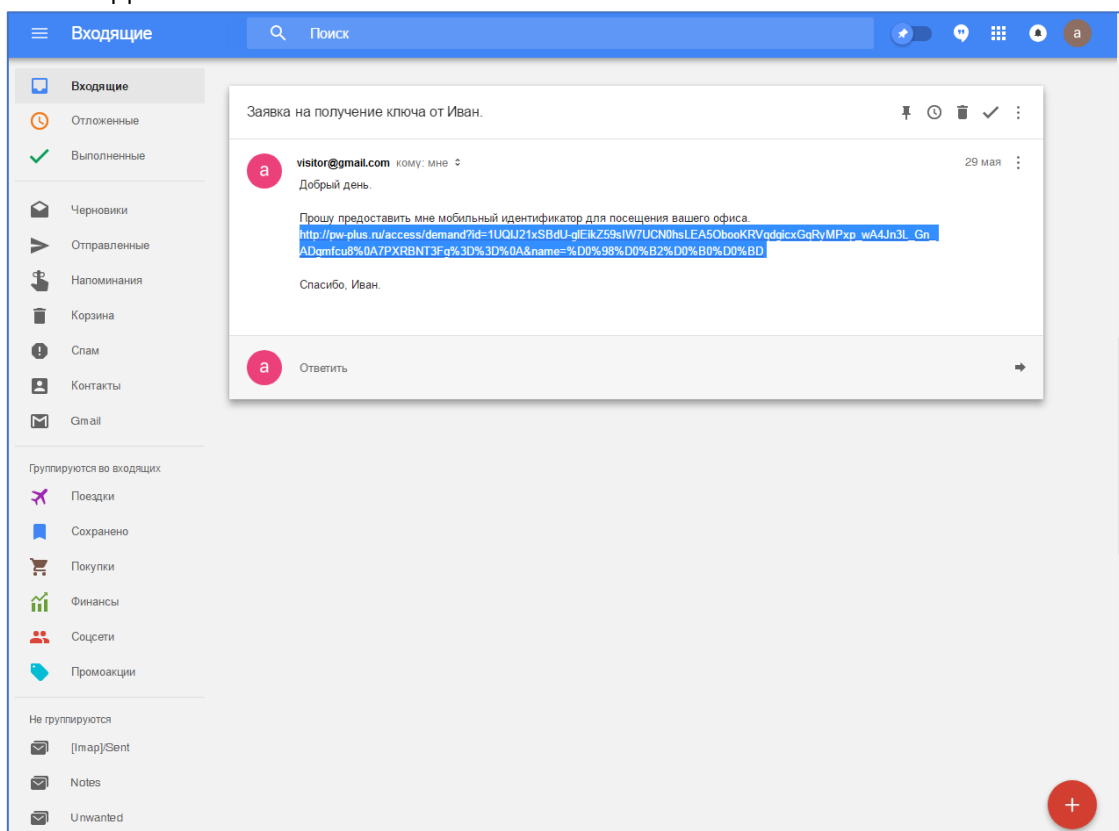
Процедура нового идентификатора по e-mail с помощью PW Desktop и PW Config

1. Если у посетителя еще нет приложения Proxway ID, он его устанавливает на своем смартфоне
2. В приложении Proxway ID пользователь нажимает кнопку "Получить по e-mail"(или в настройках приложения использует форму "Запрос сетевого ключа"), вводит свое имя и выбирает программу почты для отправки заявки.

Далее вводит адрес, используемый для приема заявок в бюро пропусков, и отправляет письмо



- Получив почту с заявкой, сотрудник бюро пропусков переводит настольный считыватель в режим выдачи идентификаторов – размещает на считывателе мастер-карту.
- Затем сотрудник бюро пропусков открывает письмо и копирует параметр "ID пользователя" в СКУД.



Для удобства операторов рекомендуем копировать полную ссылку и уже средствами ПО СКУД извлекать параметр "ID пользователя"

Выпуск мобильных идентификаторов для удаленных пользователей

Передача - POST запрос:

`http://localhost:4001/issueRemoteIdentifier`

Тело запроса:

```
{
  "UserCode": "VnztWvpazJfIKIMKQb2KCKJEmWg_cN48UnRczPmjcyK5rLOA-sZLE_xp_wA4Jn3L_Gn_ADgmfcu8%0A7PXRBNT3Fq%3D%3D%0A",
  "SendEmail": true,
  "Email": "visitor@gmail.com",
  "OutputAs": "Raw"
}
```

Url:	<code>http://pw-plus.ru/access/de</code>
Код пользователя:	<code>VnztWvpazJfIKIMKQb2KC</code>
Email:	<input checked="" type="checkbox"/> <code>visitor@gmail.com</code>
Формат идентификатора:	<input checked="" type="checkbox"/> Raw
<input type="button" value="Отправить"/>	

Ответ:

```
{
  "Identifier": "MobileID[5CF0CF54BE81EAFB] E237D9E381C792C2DC",
  "ActivationLink": "http://pw-plus.ru/access/accept?id=rembPN_tr-xluUprslXQAw%3D%3D%0A"
}
```

- СКУД у JSON сервиса запрашивает лицензию для выдачи мобильного идентификатора
- JSON сервис получает мобильный идентификатор из выделенного списка PW Desktop, код полученного мобильного идентификатора выводится в COM порт. Сервис JSON сохраняет полученный код в памяти и далее передает в приложение СКУД вместе с сформированной ссылкой подтверждения.

Запрос:

<http://localhost:40011/IssueRemoteIdentifier>

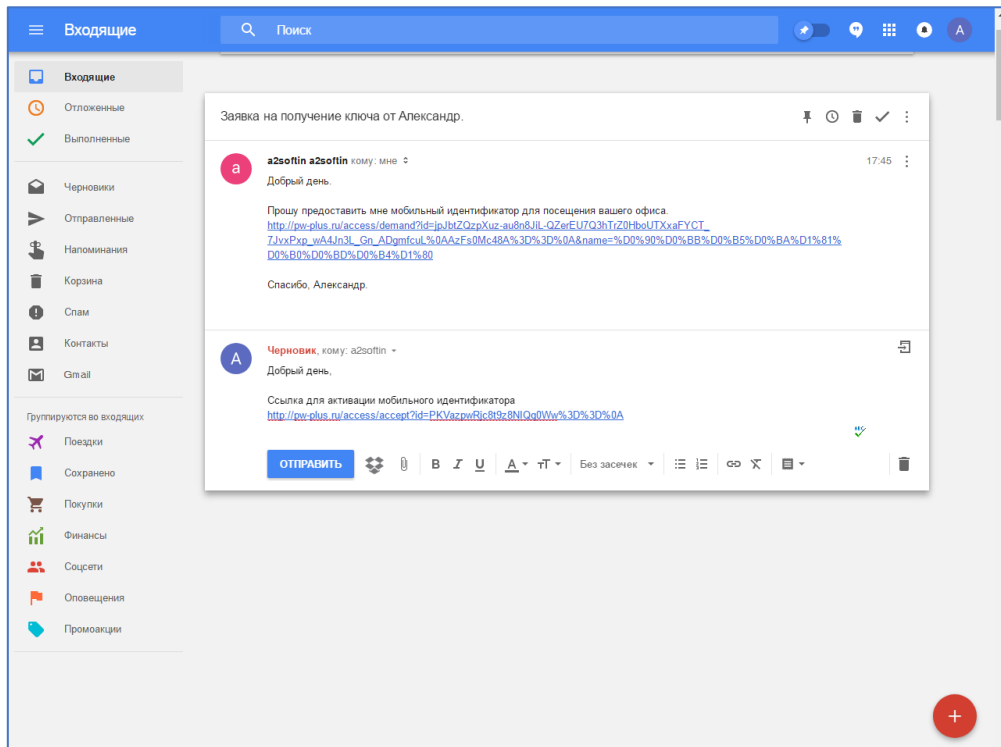
Тело запроса:

```
{
  "UserCode": "rPMU130_rsi_Rjr5zjKt4nT-z0-l_fhxdR0plbGcImURrdGWW6qEPxp_wA4Jn3L_Gn_ADgmfcwtw%0ALGkKpUmcLg%3D%3D%0A"
}
```

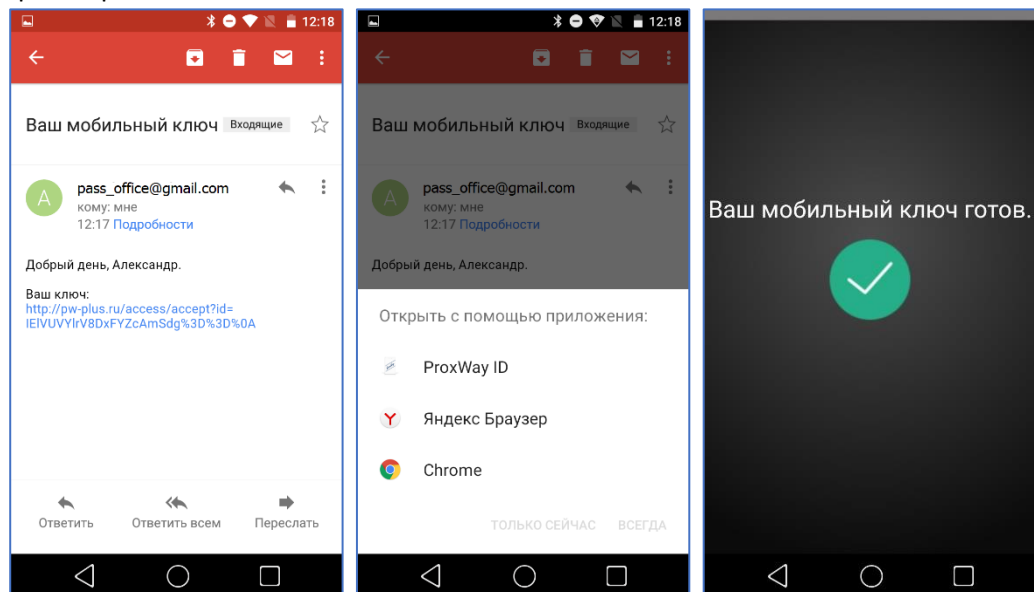
Получение данных:

```
{
  "Identifier": "54BE81EAF4",
  "ActivationLink": "http://pw-plus.ru/access/accept?id=uPZnzueJCPuhpxHAKl8kIQ%3D%3D%0A"
}
```

7. Сотрудник бюро пропусков копирует полученную ссылку в e-mail и отправляет письмо на адрес посетителя.



8. Получив почту с заявкой, посетитель открывает её на смартфоне с помощью приложения Proxway ID. После нажатия на ссылку в письме будет запущено приложение и сохранен код идентификатора.



Описание форматов вывода

Форматы вывода кода идентификатора те же, что для процедуры чтения кодов идентификаторов

Запрос:

<http://localhost:40011/IssueRemoteIdentifier>

Тело запроса:

```
{
  "UserCode": "rPMU130_rsi_Rjr5zjKt4nT-z0-l_fhxdR0plbGcImURrdGWWW6qEPxp_wA4Jn3L_Gn_ADgmfctw%0ALGkKpUmcLg%3D%3D%0A",
  "OutputAs": "Raw"
}
```

Получение данных:

```
{
  "Identifier": "NewMobileID[5CF0CF54BE81EAF4] ",
  "ActivationLink": "http://pw-plus.ru/access/accept?id=uPZnzueJCPuhpxHAKl8kIQ%3D%3D%0A"
}
```

Отправка по e-mail

Если настроена отправка электронной почты сервисом JSON, то при удаленной выдаче мобильных идентификаторов ссылка для их активации будет отправлена на указанный в запросе e-mail адрес.

Запрос:

<http://localhost:40011/IssueRemoteIdentifier>

Тело запроса:

```
{
  "UserCode": "VnztWVpazJFikIMQb2KCKjEmWg_cN48UnRczPmjcyK5rLOA-sZLE_xp_wA4Jn3L_Gn_ADgmfctl E8eldICONw== ",
  "SendEmail": true,
  "Email": "visitor@gmail.com",
  "OutputAs": "Raw"
}
```

Получение данных:

```
{
  "Identifier": "MobileID[5CF0CF54BE81EAFB] E237D9E381C792C2DC",
  "ActivationLink": "http://pw-plus.ru/access/accept?id=rembPN_rr-xluUprslXQAw%3D%3D%0A"
}
```

Дополнительная защита систем доступа (персонификация идентификаторов)

Считыватели PW поддерживают режим, в котором они принимают код только тех мобильных идентификаторов, которые зашифрованы известными им ключом шифрования (паролем).

Чтобы создать закрытую систему достаточно выполнить программирование считывателей задав им секретный пароль, и PW Desktop будет выдавать уже закрытые уникальным ключом шифрования идентификаторы.

Персонификация поддерживается для идентификаторов Mobile ID и Mifare®. Также для Mifare® есть возможность хранить свой номер идентификатора в зашифрованных секторах данных.

Внимание!!! При работе с идентификатором Mifare® шифруются все свободные сектора данных, чтобы исключить возможность взлома с помощью подбора. Если до этого на карточке были сектора с данными другой программы, то они пропускаются.

Определение, включен ли режим шифрования идентификаторов

С помощью данной команды можно информацию об режиме шифрования включенном в устройстве.

Таблица значений возможных режимов приведена ниже, по умолчанию – все значения "false".

Запрос:

```
http://localhost:40011/isEncrypted
```

Тело запроса:

```
{  
}
```

Ответ:

```
{  
  "EncryptedMobile": false,  
  "EncryptedMifare": false  
}
```

Установка режима шифрования мобильных идентификаторов

Включение режима шифрования и установка пароля шифрования

Запрос:

```
http://localhost:40011/SecureMobileIDs
```

Тело запроса:

```
{  
  "MobilePassword": "123456AA"  
}
```

Ответ:

```
{  
  "EncryptedMobile": true  
}
```

Внимание!!! Шифрованные и нешифрованные идентификаторы хранятся в различных областях памяти программы PW ID.

Выключение режима шифрования и очистка пароля

Запрос:

```
http://localhost:40011/SecureMobileIDs
```

Тело запроса:

```
{
```

```
"MobilePassword": ""
}
```

Ответ:

```
{
  "EncryptedMobile": false
}
```

Выдача зашифрованных мобильных идентификаторов происходит таким же образом, как и незашифрованных. Возможен локальный или удаленный (по e-mail) выпуск Mobile ID.

Установка режима шифрования Mifare®

Установка режима шифрования

С помощью данной команды можно включить только шифрование карт Mifare®.

Запрос:

```
http://localhost:40011/SecureMifareIDs
```

Тело запроса:

```
{
  "MifarePassword": "1122334455FF"
}
```

Ответ:

```
{
  "EncryptedMifare": true
}
```

Установка режима шифрования с персонифицированным номером идентификатора

С помощью данной команды можно только включить шифрование для Mifare® и задать стартовый номер для записи индивидуальных идентификаторов. После каждого выпуска карты номер будет увеличиваться на единицу.

Запрос:

```
http://localhost:40011/SecureMifareIDs
```

Тело запроса:

```
{
  "MifarePassword": "1122334455FF",
  "StartingCode": "1000EA1000"
}
```

Ответ:

```
{
  "EncryptedMifare": true
}
```

где 1122334455FF пароль - 6 байт (12 символов hex), а 1000EA1000 (5 байт, 10 символов hex) - стартовый номер для записи индивидуальных идентификаторов

Отключение режима шифрования

Будет отключен режим шифрования, очищен пароль и текущее значение индивидуального идентификатора

Запрос:

```
http://localhost:40011/SecureMifareIDs
```

Тело запроса:

```
{
  "MifarePassword": ""
}
```

Ответ:

```
{
  "EncryptedMifare": false
}
```

Выпуск зашифрованной карты

Будет выпущен новый идентификатор с заданными параметрами

Запрос:

```
http://localhost:40011/GetEncryptedMifareID
```

Тело запроса (можно установить формат вывода):

```
{
  "OutputAs": "Raw"
}
```

Ответ:

```
{
  "CryptedMifare[1000EA1000] 234,04096 1K (0004,08) "
}
```

Процедура выдачи нового идентификатора

1. Администратор размещает на считывателе новую (чистую) карту Mifare®.
2. Администратор дает команду на выпуск новой карты – выполняется шифрование.
3. По завершению шифрования код полученного идентификатора считывается и выводится в COM порт (передается в СКУД и т.д.)

Возможные ошибки при выпуске карты:

Выпуск не удался, все 16 секторов недоступны для шифрования

```
{
  "code": 5,
  "message": "All mifare card blocks are inaccessible"
}
```

Карта была убрана со считывателя, несколько секторов не зашифрованы (потенциальная брешь для атаки, следует перевыпустить этот идентификатор)

```
{
  "code": 6,
  "message": "Mifare card blocks protection error"
}
```

Настройка отправки электронной почты сервисом JSON при выдаче мобильных идентификаторов по e-mail

Можно настроить работу сервиса JSON с почтовым SMTP сервером. Тогда при удаленной выдаче мобильных идентификаторов ссылка для их активации будет отправлена на указанный в запросе e-mail адрес.

Параметры почтового сервера сохраняются в реестре:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ELICS\ProxWayIP\2.00]
    "SmtpServerEnabled"
    "SMTPEncrypted"
    "SMTPServer"
    "SMTPPort"
    "SMTPUser"
    "SMTPPassword"
    "SMTPSendFrom"
```

Запрос:

```
http://localhost:40011/SecureMifareIDs
```

Тело запроса:

```
{
  "SmtpServerEnabled": false,
  "SMTPEncrypted": false,
  "SMTPServer": "192.168.1.1",
  "SMTPPort": 25,
  "SMTPUser": "user",
  "SMTPPassword": "password",
  "SMTPSendFrom": "user@domail.com"
}
```

Ответ:

```
{
  "SmtpServerEnabled": true
}
```