Notification Update

Business Management Platform

April 2016

amadeus

Document control

Security level	ACO & Travel Agency			
Company	Product and Solution Centre, CESE			
	BMP development group			
Author	Yanina Lyapunova			
Reviewed by	Alexander Pavlov		**Date**	23 / 05 / 2016
Approved by			**Date**	23 / 05 / 2016
Version	**Date**	**Change**	**Comment**	**By**
1.0				

Index

РАБОТА С SFTP ***4***

Генерация серкетного и открытого ключа 4
Добавление открытого ключа в список разрешенных для доступа к сервису sFTP BMP 6
Интерфейс управления RSA ключами 7
Настройка sFTP клиента 8
Настройка FileZilla *8*
Настройка консольного клиента *11*
Использование менеджера ключей Pageant *11*
Сервис замены устаревшего ключа 12

Работа с sFTP

В связи с требованиями PCI DSS сертификации по сохранности и защите данных доступ к AIR файлам и сгенерированным XML будет предоставляться сервисом sFTP.

SFTP (англ. *SSH File Transfer Protocol*) — протокол прикладного уровня, предназначенный для копирования и выполнения других операций с файлами поверх надёжного и безопасного соединения. Протокол разработан группой IETF как расширение к SSH-2, однако SFTP допускает реализацию и с использованием иных протоколов сеансового уровня.

Протокол предполагает, что он работает поверх установленного безопасного канала, что сервер уже аутентифицировал клиента и что идентификатор клиента доступен протоколу.
Сервер SFTP обычно использует порт 22.

SSH File Transfer Protocol не является протоколом FTP работающим поверх SSH — это другой, новый протокол. Также SFTP иногда путают с Simple File Transfer Protocol из-за совпадающего сокращения «SFTP».

Итак, для работы с сервисом sFTP потребуется клиент с поддержкой sFTP и сгенерированный RSA ключ для авторизации клиента, заведенный в список доступных для использования сервиса.

Генерация секретного и открытого ключа

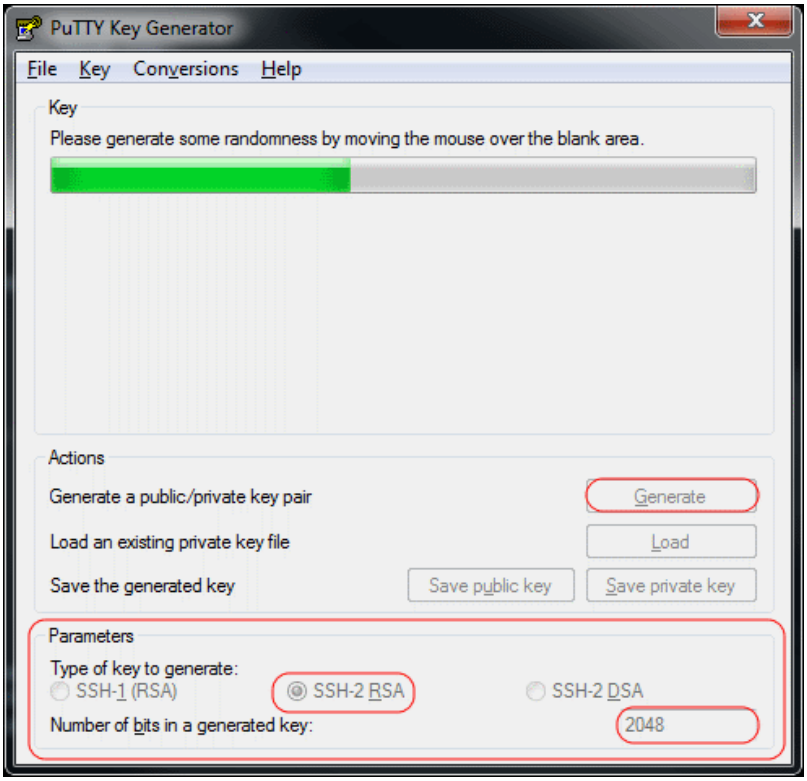
ВНИМАНИЕ: BMP не предоставляет услуги по генерации, не хранит и не распространяет секретные ключи клиента.

Для работы с сервисом под операционной системой windows рекомендуется использовать пакет утилит PuTTY (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html). Используйте MSI установщик для установки всего пакета или утилиты по отдельности.

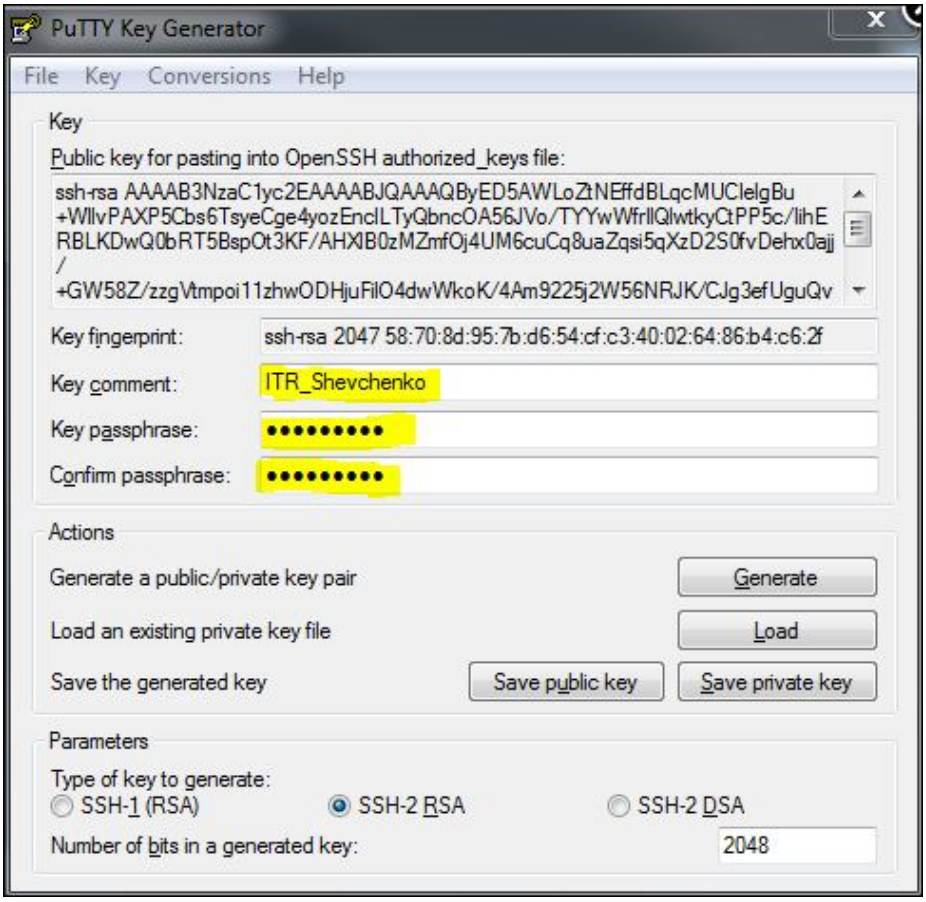
Генерацию ключей нужно производить на компьютере и аккаунте пользователя, который будет работать с сервисом sFTP.

Для этого используем утилиту *PuTTYgen*.

После того как запустится программа, находим набор полей 'Parameters'. Убедитесь что в параметрах выбрано SSH-2 RSA, a Number of bits in a generated key равен 2048. Затем нужно нажать кнопку "Generate" и после этого двигаем мышкой поверх этого окна в произвольном порядке и скорости (это нужно для генерации "случайностей" ключа).



Когда прогресс генерации достигнет 100 % вы увидите следующее окно:



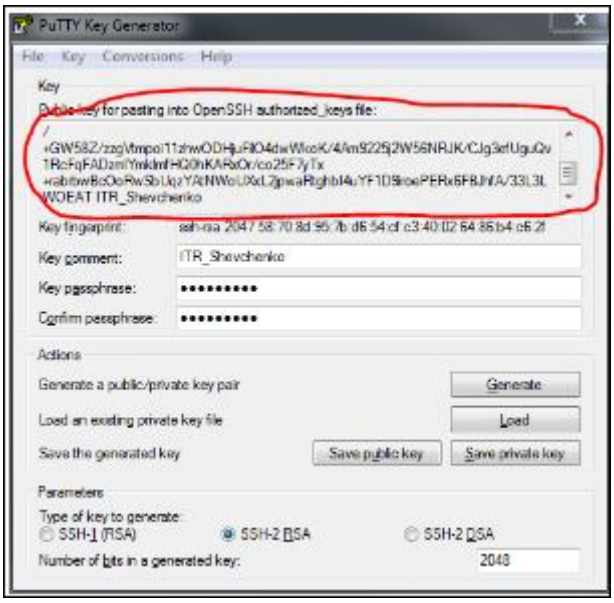
Введите фразу-пароль в поле 'Key passphrase' и подтвердите в поле 'Confirm passphrase'.

ВНИМАНИЕ: Пароль должен быть не менее 8 символов, содержать хотя бы одну строчную, заглавную букву, цифру, спецсимвол. Пример: ***0ewNºS6=W.*)**

Пароль обязательный для ввода при каждом подключении к сервису.

Для удобства администрирования ключа в дальнейшем можно указать "Key comment" (например, можно указать компьютер-и-пользователя владельца ключа).

Затем необходимо сохранить публичный ('Save public key') и приватный ключ ('Save private key'), нажав на соответствующие кнопки.



Далее следует скопировать содержимое текстового блока с публичным ключом, для добавления его в список разрешенных ключей, для доступа к сервису sFTP BMP

ВНИМАНИЕ: **ЗАПРЕЩЕНО** передавать секретные ключи (private key) сторонним пользователям.

Добавление открытого ключа в список разрешенных для доступа к сервису sFTP BMP

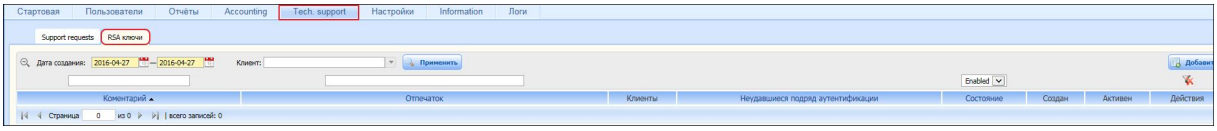
Добавление Открытого ключа в список разрешенных для доступа к сервису sFTP BMP предусмотрен для клиентов с типом доступа администратор (ACO, Консолидатор и Субагента).

Для добавления ключа необходимо воспользоваться интерфейсом добавления нового ключа. Введенный ранее ключ вводить повторно - запрещено.

После добавления статус ключа - "включен". Ключ автоматически добавится на sFtp сервер, и разрешит доступ к сервисам BMP.

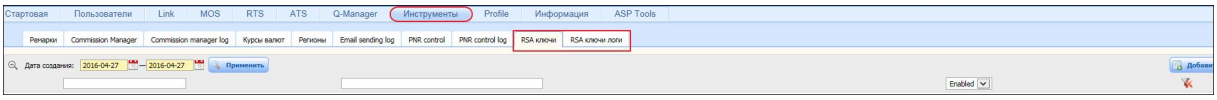
Интерфейс управления RSA ключами

Для администратора ACO в меню Tech.support добавлена закладка RSA ключи



Добавление нового ключа

Для Администратора Консолидатора и Субагента в меню **Инструменты** добавлены подпункт RSA ключи и RSA ключи логи.



На странице RSA ключи находится список ключей, доступных для управления sFTP доступом.

Возможные действия над ключом

- Создание нового
- Блокирование/Разблокирование
- Обновление всех ключей (обновляет ключи на sFTP сервере у клиента)
- Переход на страницу логов с фильтром по данному ключу

Статусы ключа

Включен

Ключ добавлен и готов к использованию.

Разрешает пользоваться сервисами BMP

Статус может быть изменен на "выключен"

Выключен

Использование ключа запрещает пользоваться сервисами BMP.

Статус может быть изменен на "*включен*"

Просроченный

По истечению 45 суток с момента создания, ключ перейдет в состояние "Просрочен", не смотря на предыдущий статус, о чем будет дополнительно отправлено уведомление на электронную почту администратора клиента.

"Просроченный" ключ не дает права входа на сервисы BMP.

У просроченного ключа нельзя изменить статус.

Настройка sFTP клиента

Для настройки sFTP клиента нужно использовать следующие параметры:

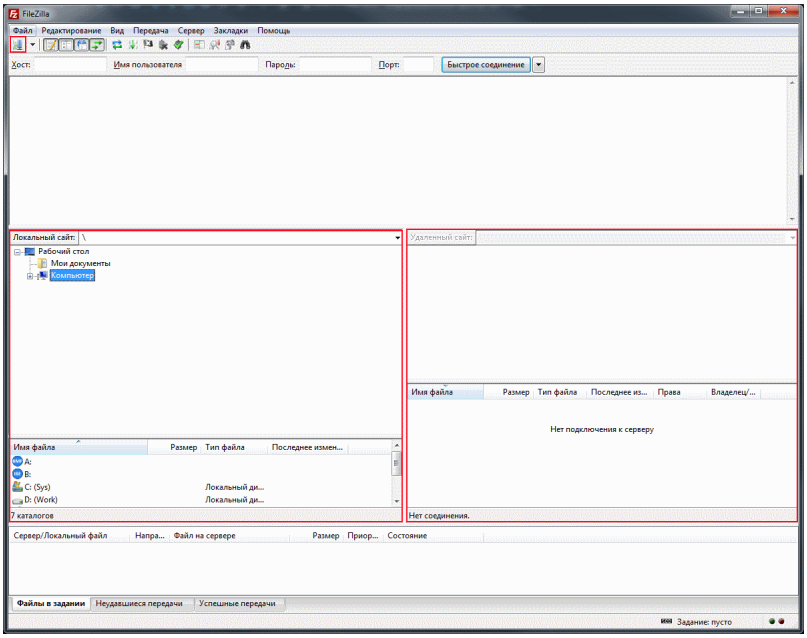
- Хост: ftp.bmp.viaamadeus.com
- Порт: 22
- Протокол: sftp
- Тип входа: файл с ключем
- Пользователь: пользователь ftp заведенный в системе BMP на странице профиля в закладке "Общие"
- Файл с ключем: сгенерированый секретный ключ, сохраненный в файл (private key)

Остальные настройки - по умолчанию

Настройка FileZilla

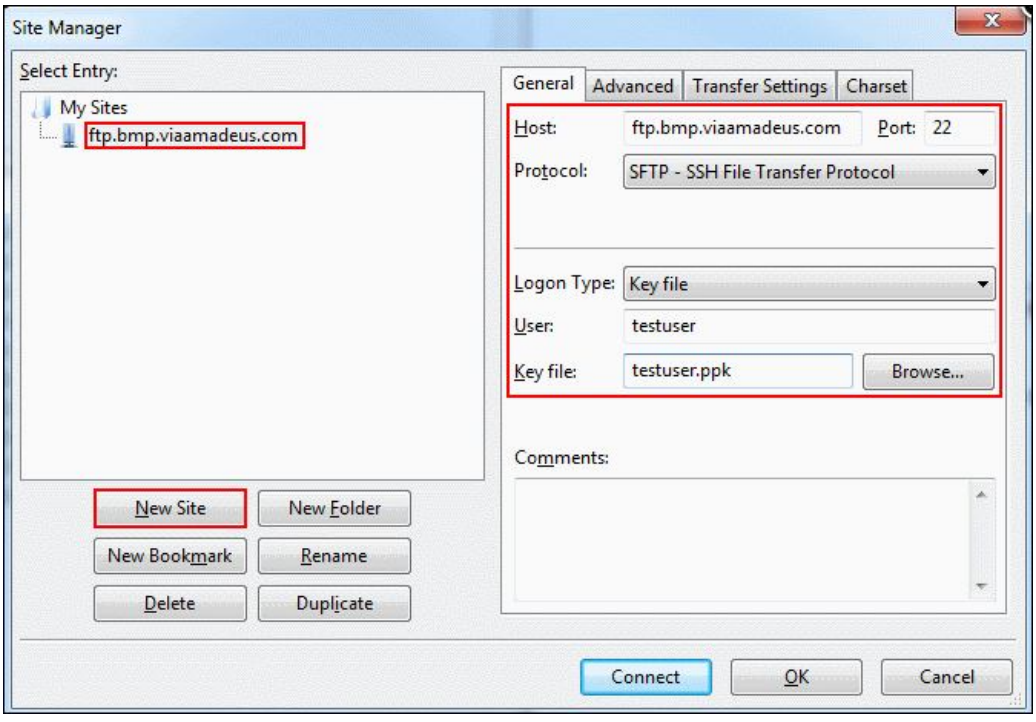
Для примера организации такого сервиса рассмотрим **FileZilla. FileZilla** — это свободно распространяемый многоязычный FTP-клиент с открытым исходным кодом для Microsoft Windows, Mac OS X и Linux. Он поддерживает FTP, SFTP, и FTPS (FTP через SSL/TLS) и имеет настраиваемый интерфейс с поддержкой смены тем оформления. Оснащен возможностью перетаскивания объектов, синхронизацией директории и поиском на удаленном сервере.[1] Поддерживает многопоточную загрузку файлов, а также докачку при обрыве (если поддерживается сервером[2]) интернет-соединения.[3][4]

Главное окно программы:



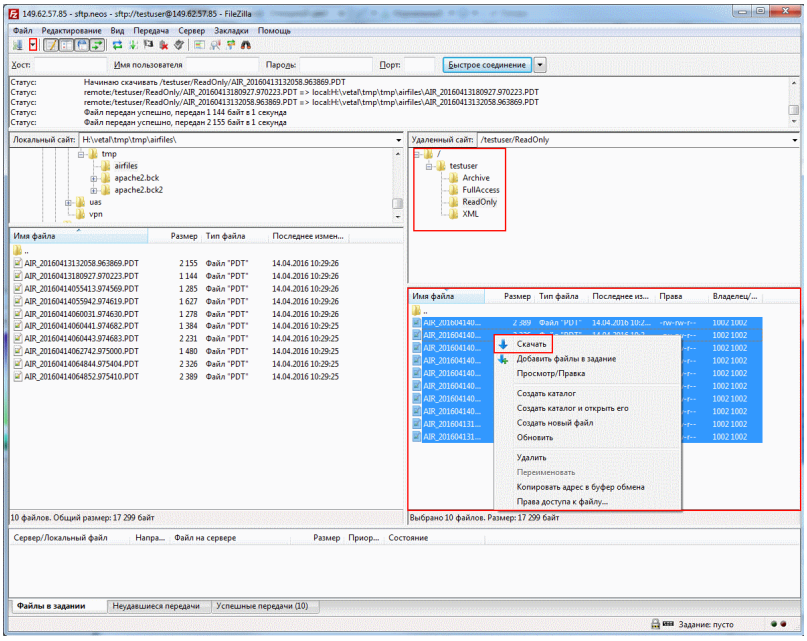
Для добавления учетной записи требуется нажать иконку **Менеджера сайтов** (или сочетание клавиш Ctrl+s).

В появившемся окне менеджера сайтов

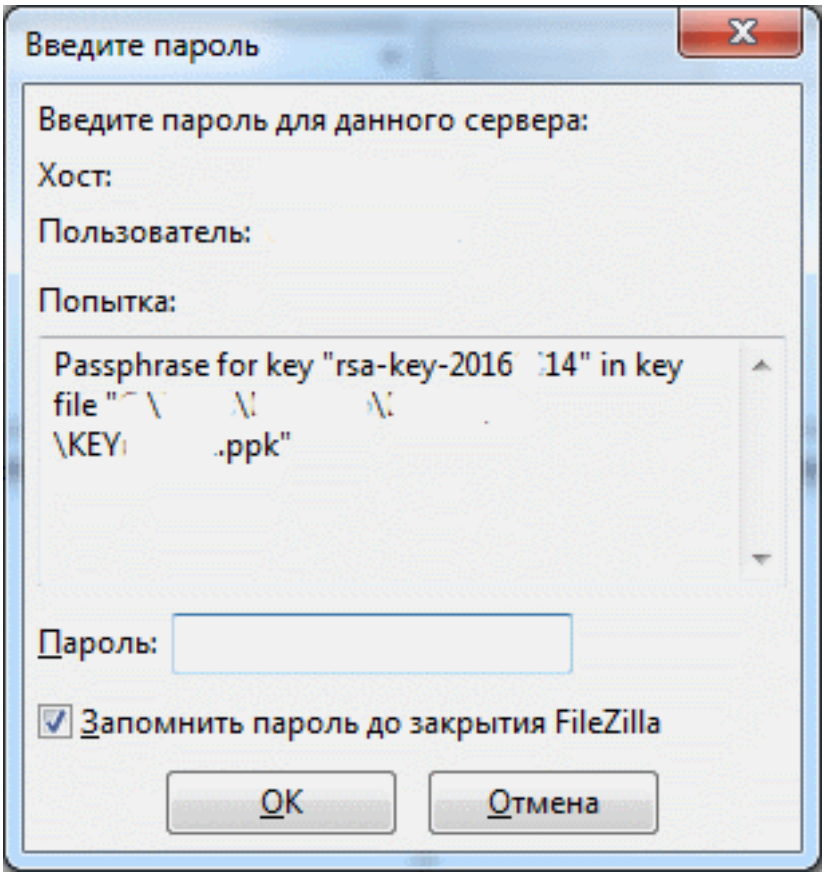


Необходимо нажать на **Новый сайт**, заполнить вышеописанные настройки, Сохранить изменения, нажав на OK.

FTP клиент готов для работы.



В процессе установки связи будет запрошен пароль секретного ключа



Настройка консольного клиента

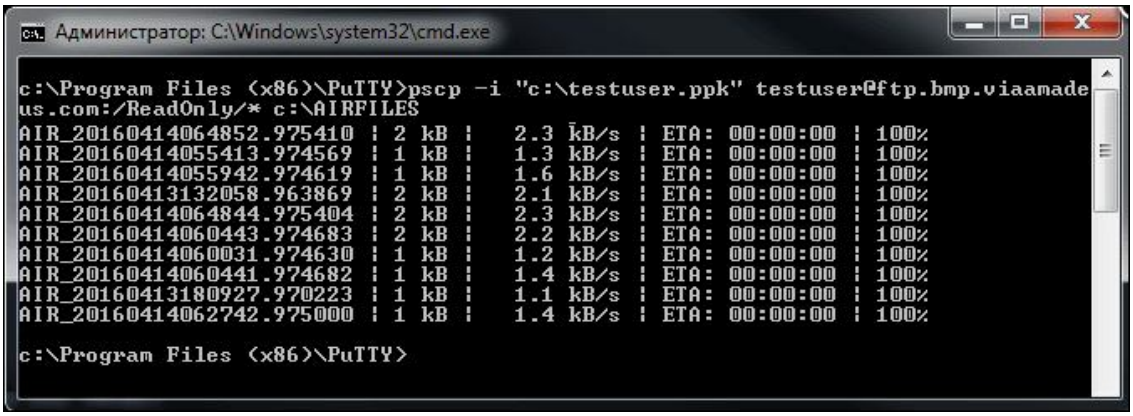
Для примера использования консольного клиента возьмем windows клиент pscp из пакета PuTTY

Использование PSCP:

pscp [options] [user@]host:source target

Пример копирования файлов с удаленного сервиса на локальное устройство

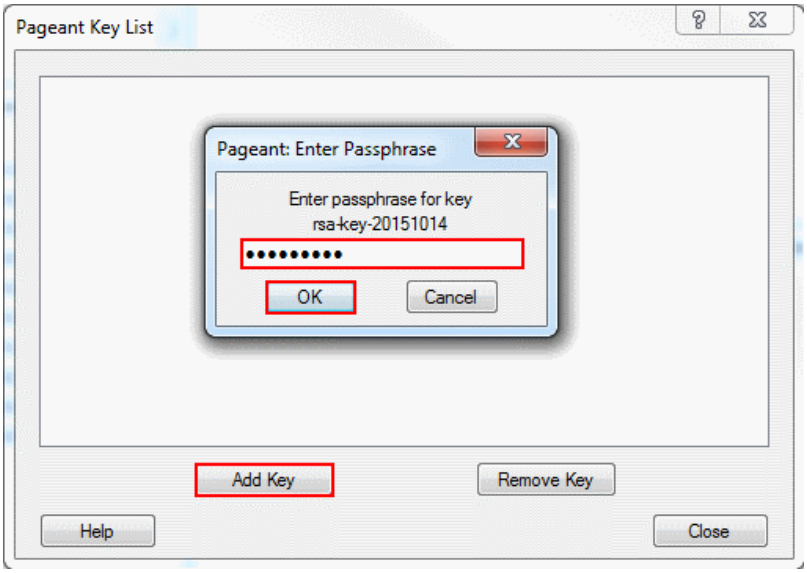
pscp -i "<путь к ключу>\testuser.ppk" testuser@149.62.57.85:/testuser/ReadOnly/* c:\AIR_FILES\



Проверьте, конечная папка должна быть создана заранее, до начала копирования файлов.

Использование менеджера ключей Pageant

Для возможности работать с sftp сервисом с использованием RSA ключей, не вводя пароль при каждой операции можно использовать утилиту Pageant (входит в состав утилиты PuTTY).
Для этого нужно запустить утилиту, и в открывшемся окне нажать кнопку "Add Key".



В появившемся окне нужно ввести пароль секретного ключа. Подтвердить нажатием кнопки "Ок".

Таким образом, в списке ключей Pageant появится добавленный ключ, которым можно будет пользоваться не вводя более пароля, пока он находится в списке.

Сервис замены устаревшего ключа

Так как, согласно директивам PCI DSS, ключи должны иметь конечный срок использования, через 45 дней после добавления в BMP, ключ будет автоматически заблокирован со статусом "просрочен". Такой ключ не дает право использовать сервисы BMP.

Для автоматизации процесса замены публичного ключа был создан сервис замены ключа.

Любой действующий ключ можно заменить в любое время.

Сервис реализован с помощью SOAP

Параметры:

Точка входа: http://webservices.bmp.viaamadeus.com/rsa_key.php

WSDL: http://webservices.bmp.viaamadeus.com/rsa_key.php?wsdl

Для xml запроса:

terminal - id терминала администратора в системе BMP

old_key - старый действительный публичный ключ (в состоянии "включен") который будет заменен

new_key - новый уникальный (не заведенный ранее в системе) публичный ключ который должен быть добавлен

Пример запроса

```
<soapenv:Envelope
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
   xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
   xmlns:urn="urn:rsa_key">
   <soapenv:Header/>
   <soapenv:Body>
      <urn:changeKey soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
         <terminal xsi:type="xsd:string">486</terminal>
         <old_key xsi:type="xsd:string">ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAxm0nECFH6laVQeALzbRirBEDkC6nV8CRXdVKOor1k/NGrT9VWOCWu
xTLmYBKx6g74sfOg3/MIO4Ctcz9Y0wiRuqoTNJCG2d5XdcCkEjrcC3qNggCmcwabqPVgHYOKqqgsWgu5Qp1tA
eIpw6KpGZ/FK50RCx43UDHHjdQq6GB2e3zmG25jXrCEgWO6/1IBR528XKNhqwvJbZ9f+6SOVf4cFWvjg1FWXa
KXNduzwmbW3hno30Bmqf73xM+1ntk6hWtder0WXDh2WbcGryWLCh0SfEbcPJXo+S63i+U1tqGX4CWAywCsJi
+/Q9vHDngoeumlO7jOIylxFPGRlJD/ZwSNQ== superkey</old_key>
         <new_key xsi:type="xsd:string">ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAop5ljhi5PVbBI3TrKh0jtjui4GshtAYMBMRxZisuk4ma4vDtUpUmRwrhDAE
Z6P6Q3KtxkjBvUn+SBcAebJ1xHwvNWFmLFrsWdFyynD8cLWURB4PDpdnr90VHWS89jdRDCfJ/lZFZvd98L4YI1
RWM/YvmB8ims6iR+PV+TOFMhmle2CBCSuzai4UCo7IkYBjvJf8vXH8quN1cOgrZEMAvIDw62yqYibTf90oK4FO8
ySA2t8uKqZGey3NDfhfI+igOuHyZxxgNqzIIvNJ9HbCeOQgMtLGcqTlMbbQ1S1iSM5ZXSu4osLe7JSN4nmnaYYn
Qh7pOgMCig7c9ZNHxwT62xw== sk21-32</new_key>
      </urn:changeKey>
   </soapenv:Body>
</soapenv:Envelope>
```

Пример ответа

```
<SOAP-ENV:Envelope SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
   xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/">
   <SOAP-ENV:Body>
      <ns1:changeKeyResponse
         xmlns:ns1="urn:rsa_key">
         <message xsi:type="xsd:string">Success</message>
      </ns1:changeKeyResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

После успешной операци замены ключа, прийдет положительный ответ и старый ключ будет заблокирован со статусом "отключен".