**Описание функциональных характеристик программного обеспечения и руководство по его установке и эксплуатации cистемы Corp.bank**

Москва

2022

**Оглавление**

[1. Введение 4](#_Toc68787561)

[1.1. Термины и сокращения 4](#_Toc68787562)

[2. Общие сведения 5](#_Toc68787563)

[3. Требования к оборудованию и среде 6](#_Toc68787564)

[3.1. Требования к оборудованию 6](#_Toc68787565)

[3.2. Требования к среде 6](#_Toc68787566)

[4. Архитектура системы 7](#_Toc68787567)

[4.1. On-Premise размещение 8](#_Toc68787568)

[4.2. Cloud размещение 9](#_Toc68787569)

[4.3. Комбинированное размещение 10](#_Toc68787570)

[5. Описание компонентов и принципа работы системы 11](#_Toc68787571)

[5.1. Общее описание системы 11](#_Toc68787572)

[5.2. Компонент Сервис-провайдер 12](#_Toc68787573)

[5.3. Компонент Банк адаптер 12](#_Toc68787574)

[5.4. Компонент подписи 13](#_Toc68787575)

[5.5. Компонент Конвертер 13](#_Toc68787576)

[6. Сетевое взаимодействие компонентов системы 14](#_Toc68787577)

[7. Описание механизма подтверждения отправителя и ПК (внутренний анти-фрод) 16](#_Toc68787578)

[7.1. Настройка механизма внутреннего анти-фрода 17](#_Toc68787579)

[7.2. Формирование блока данных 18](#_Toc68787580)

[8. Установка и настройка компонентов системы 20](#_Toc68787581)

[8.1. Установка и настройка RabbitMQ 20](#_Toc68787582)

[8.1.1. Установка 20](#_Toc68787583)

[8.1.2. Настройка 21](#_Toc68787584)

[8.1.3. Настройка SSL 22](#_Toc68787585)

[8.2. Установка и настройка КриптоПро CSP 23](#_Toc68787586)

[8.2.1. Установка 23](#_Toc68787587)

[8.2.2. Настройка 23](#_Toc68787588)

[8.3. Установка и настройка компонента ServiceProvider 24](#_Toc68787589)

[8.3.1. Установка 24](#_Toc68787590)

[8.3.2. Обновление компонента 26](#_Toc68787591)

[8.3.3. Описание конфигурационного файла 27](#_Toc68787592)

[8.4. Установка и настройка компонента BankAdapter 28](#_Toc68787593)

[8.4.1. Установка 28](#_Toc68787594)

[8.4.2. Обновление компонента 29](#_Toc68787595)

[8.4.3. Описание утилиты AAStatement.exe 29](#_Toc68787596)

[8.4.4. Просмотр веб-журнала обмена 30](#_Toc68787597)

[8.4.5. Описание конфигурационного файла 32](#_Toc68787598)

[8.5. Установка и настройка компонента DocSigner 33](#_Toc68787599)

[8.5.1. Установка 33](#_Toc68787600)

[8.5.2. Обновление компонента 34](#_Toc68787601)

[8.5.3. Описание конфигурационного файла 35](#_Toc68787602)

[8.6. Установка и настройка компонента DocConverter 36](#_Toc68787603)

[8.6.1. Установка 36](#_Toc68787604)

[8.6.2. Обновление компонента 37](#_Toc68787605)

[8.6.3. Описание конфигурационного файла 38](#_Toc68787606)

[8.7. Проверка работоспособности компонентов УПСК 39](#_Toc68787607)

[8.8. Настройки подключения к банкам 40](#_Toc68787608)

[8.8.1. Настройки для банка ВТБ 40](#_Toc68787609)

[8.8.2. Настройки для банка Сбербанк 42](#_Toc68787610)

[8.8.3. Настройки для банка Газпромбанк 44](#_Toc68787611)

[8.8.4. Настройки для банка Банк Россия 45](#_Toc68787612)

[8.8.5. Настройки для банка Промсвязьбанк 46](#_Toc68787613)

[8.8.6. Настройки для банка Альфабанк 48](#_Toc68787614)

[8.8.7. Настройки для банка Росбанк (H2H - собственное API банка) 51](#_Toc68787615)

[8.8.8. Настройки для банка Росбанк (1C.ДиректБанк) 52](#_Toc68787616)

[8.8.9. Настройки для банка Юникредит 53](#_Toc68787617)

## 

# **Введение**

## Термины и сокращения

**Таблица 1 Перечень терминов и сокращений**

| **Термин / Сокращение** | **Определение** |
| --- | --- |
| **УПСК** | Программный продукт Универсальная Платежная Система Корпораций (Corp.bank) |
| **КС** | Казначейские Системы. Компания-разработчик системы. |
| **On-Premise** | вариант размещения всех компонентов на стороне Клиента и прямое взаимодействие с Банками. |
| **Cloud** | вариант частичного размещения компонентов у Клиента и частичного в облаке, взаимодействие через третью доверенную сторону – дата-центр Казначейских Систем. |
| **RMQ** | компонент системы программный брокер сообщений, отвечающий за межкомпонентное взаимодействие на основе стандарта AMPQ. |
| **SP, ServiceProvider** | компонент УПСК Сервис-провайдер. |
| **BA, BankAdapter** | компонент УПСК Банк адаптер. |
| **DS, DocSigner** | компонент УПСК Компонент подписи. |
| **DC, DocConverter** | компонент УПСК Конвертер. |
| **ЭЦП** | электронно-цифровая подпись. |
| **ДЦ** | дата-центр. |
| **УС** | учетная система, ERP система. |
| **vCPU** | виртуальный процессор. |
| **RAM** | оперативная память. |
| **HDD** | жесткий диск. |
| **ОС** | операционная система. |
| **ПП** | платежное поручение. |

# **Общие сведения**

УПСК предназначена для обмена электронными документами, информационными или системными запросами между УС Клиента и Банками. УПСК использует технологию прямой интеграции с Банками. В ее основе может лежать любой сетевой протокол, выбранный конкретным Банком – HTTP, SFTP, AMPQ, практически любой формат документа и протокол взаимодействия.

УПСК реализует требования по безопасности, протокол взаимодействия и форматы документов конкретного Банка и предоставляет возможность Клиенту производить обмен с любым Банком, подключенным к системе, по единому внутреннему АПИ УПСК на основе JSON и единому формату документа ISO 20022. В результате, УПСК является агрегатором сервисов прямой интеграции с Банками и предоставляет клиентам универсальный (единый) протокол обмена и формат документа.

УПСК разработан на языках программирования C++ и Golang. Компоненты системы взаимодействуют между собой с помощью программного брокера сообщений RabbitMQ на основе стандарта AMPQ.

В состав УПСК может быть включено следующее аппаратное обеспечение в зависимости от требований конкретной инсталляции:

* ПАК ФПСУ IP – аппаратное канальное оборудование для организации защищенного соединения с Банком. Устанавливается в ДЦ Клиента.
* ПАК «Соболь» – программно-аппаратный модуль доверенной загрузки для автоматизации криптографических операций. Устанавливается на сервер(а) компонентов Клиента.
* Токены типа Рутокен, JaCarta – устройства для хранения закрытых частей сертификатов и аппаратного выполнения криптографических операций.

Для осуществления криптографических операций УПСК использует криптопровайдер, который требуется для работы с конкретным Банком. В настоящий момент поддерживаются криптопровайдеры КриптоПро CSP и Бикрипт.

# **Требования к оборудованию и среде**

## Требования к оборудованию

Конфигурация сервера или ПК для компонента системы – от **2x vCPU 2GHz**, от **4Gb RAM**, от **200Gb HDD**.

В зависимости от количества документов, передающихся через систему в течение дня и пиковых нагрузок конфигурация системы может измениться, потребовав более производительного оборудования. В первую очередь может потребоваться увеличение размера HDD – в среднем, на один отправленный или принятый системой документ создается 250 Kb логов на всех компонентах системы.

## Требования к среде

Компоненты системы могут быть установлены как на физические, так и на виртуальные сервера. Поддерживаемые среды виртуализации – ESXi 5.1 и старше. В среде виртуализации Hyper-V возможна корректная работа компонентов системы, но полностью в этой среде сервис не тестировался.

**ОС Windows 64 битная**. Поддерживаются ОС начиная с Windows 7:

* Windows 7 x64
* Windows 8 x64
* Windows 10 x64
* Windows Server 2008R2
* Windows Server 2012
* Windows Server 2016

Компоненты системы могут быть установлены как на десктопной, так и на серверной версии ОС Windows, но мы рекомендуем, чтобы как минимум компоненты RMQ, ServiceProvider и BankAdapter были установлены на серверной версии ОС Windows. В случае децентрализованной конфигурации сервиса подписи, компоненты DocSigner могут быть свободно установлены на десктопной версии ОС Windows.

Обязательное ПО:

* **КриптоПро CSP** версии 4.0 или 5.0. КриптоПро CSP должно быть установлено на серверах компонентов DocSigner и BankAdapter.
* **RabbitMQ** версии 3.7.15. Может быть установлено как на сервере с каким-либо из компонентов системы, так и на отдельном сервере. Мы рекомендуем устанавливать это ПО на одном сервере совместно с компонентом ServiceProvider.
* **Erlang/OTP** версии 22.0. Должно быть установлено на одном сервере совместно с RabbitMQ.

Опциональное ПО:

* **Notepad++** версии 7.7 и старше с установленным плагином XML Tools. Используется администратором системы для работы с журналами УПСК и JSON/XML-структурами.
* **curl** версии 7.65.0 и старше. Используется администратором системы для ручной отправки API-запросов компоненту ServiceProvider.

# **Архитектура системы**

УПСК состоит из нескольких компонентов, каждый из которых выполняет определенную роль.

Компоненты могут быть установлены как на отдельные сервера, так и совместно на один сервер или комбинированно. В случае использования нескольких экземпляров одного и того же компонента системы, каждый из них должен быть установлен на отдельном сервере или в рамках тестовой среды при необходимости на одном сервере под разными учетными записями ОС.

Компоненты УПСК:

* Брокер (RMQ) – компонент системы, отвечающий за межкомпонентное взаимодействие на основе стандарта AMPQ. Является точкой входа и связующим звеном для компонентов SP, BA, DS и DC.
* Сервис-провайдер (SP) – точка входа для потребителей сервиса со стороны Клиента. Содержит встроенный веб-сервер. В настоящий момент поддерживается только синхронное клиент-серверное взаимодействие.
* Банк адаптер (BA) – компонент системы, отвечающий за сетевой обмен с серверами Банков.
* Компонент подписи (DS) – компонент системы, отвечающий за криптографические операции с документами в УПСК, который в том числе подписывает документы, передаваемые в Банк. Хранит ЭЦП, используя выбранный криптопровайдер и криптоносители. Компонент может быть установлен на выделенный сервер и использоваться централизованно или же устанавливаться на каждый ПК подписанта и использоваться децентрализованно.
* Конвертер (DC) – компонент системы, осуществляющий конвертацию документа из единого формата, принятого для конкретной инсталляции, в формат целевого Банка.
* Компонент управления и мониторинга (Cloud-часть) – с помощью этого компонента осуществляется управление и мониторинг Cloud-компонентами УПСК.
* Компонент биллинга (Cloud-часть) – компонент, осуществляющий биллинг компаний, подключенных по Cloud или комбинированной схеме.

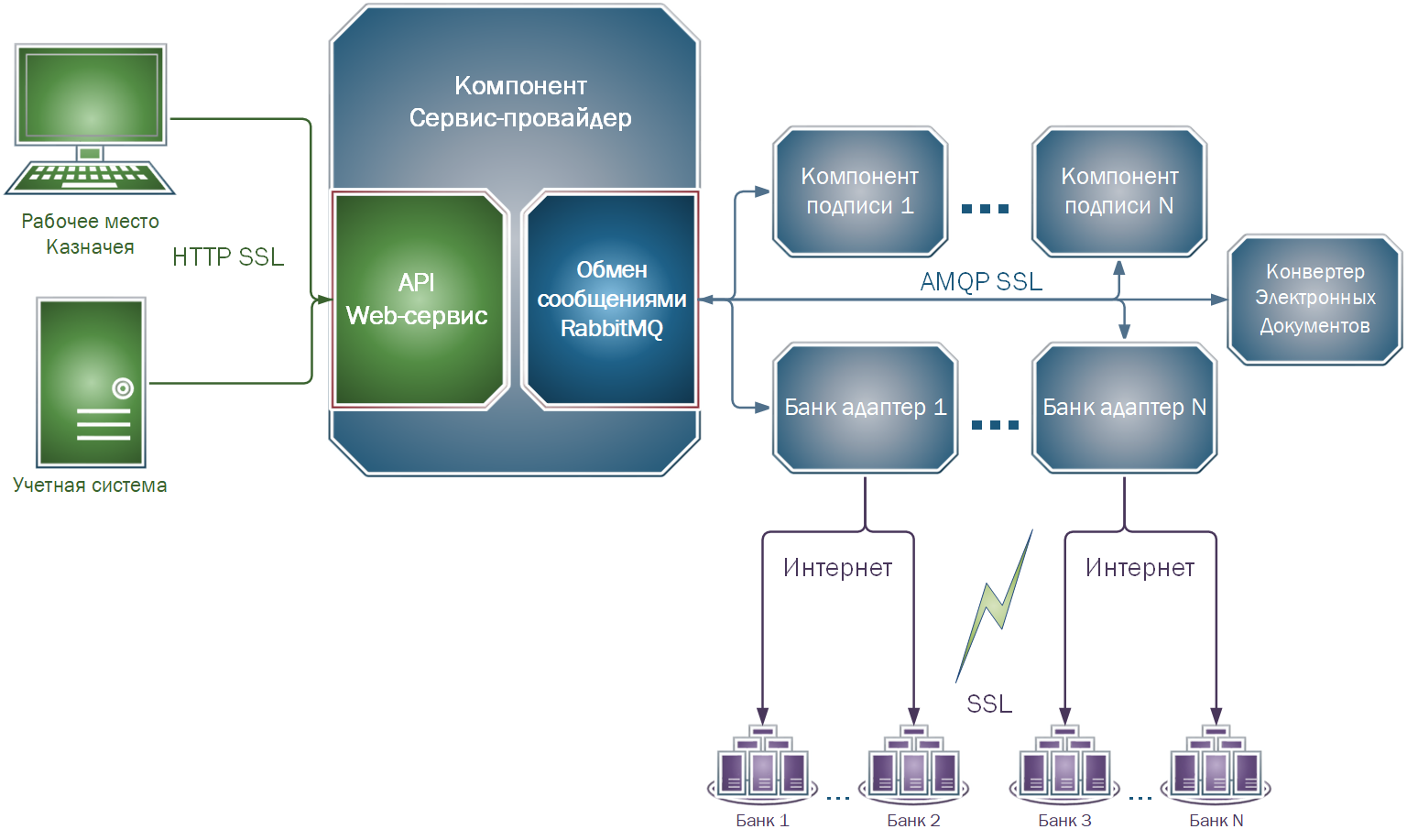
Определенные компоненты могут использоваться в нескольких экземплярах в рамках одной инсталляции, а именно:

* DS – в зависимости от выбранной модели хранения ЭЦП в инсталляции системы может присутствовать как один централизованный компонент подписи, так и несколько компонентов подписи, установленных на каждом из ПК подписантов.
* BA – в рамках одной инсталляции могут быть развернуты один или несколько компонентов банк-адаптер.

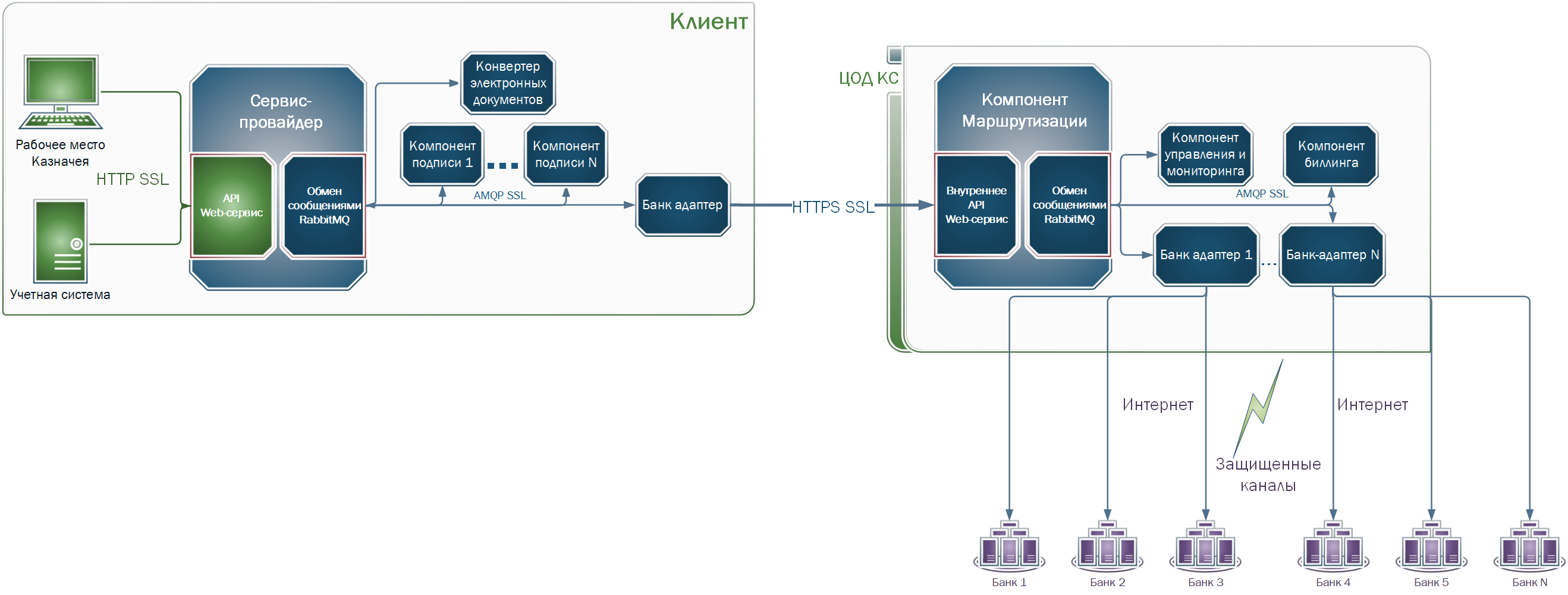
Существует три варианта размещения ПАК УПСК – On-Premise, Cloud и комбинированное.

* В случае On-Premise размещения все компоненты системы размещаются на серверах Клиента и осуществляется прямой обмен между Клиентом и Банками.
* В случае Cloud размещения часть компонентов системы размещается у Клиента, а часть в ДЦ КС. Обмен осуществляется через третью доверенную сторону – ДЦ КС.
* В случае комбинированного размещения все компоненты системы размещаются на серверах Клиента. Обмен с частью Банков происходит напрямую, а с частью через третью доверенную строну – ДЦ КС.

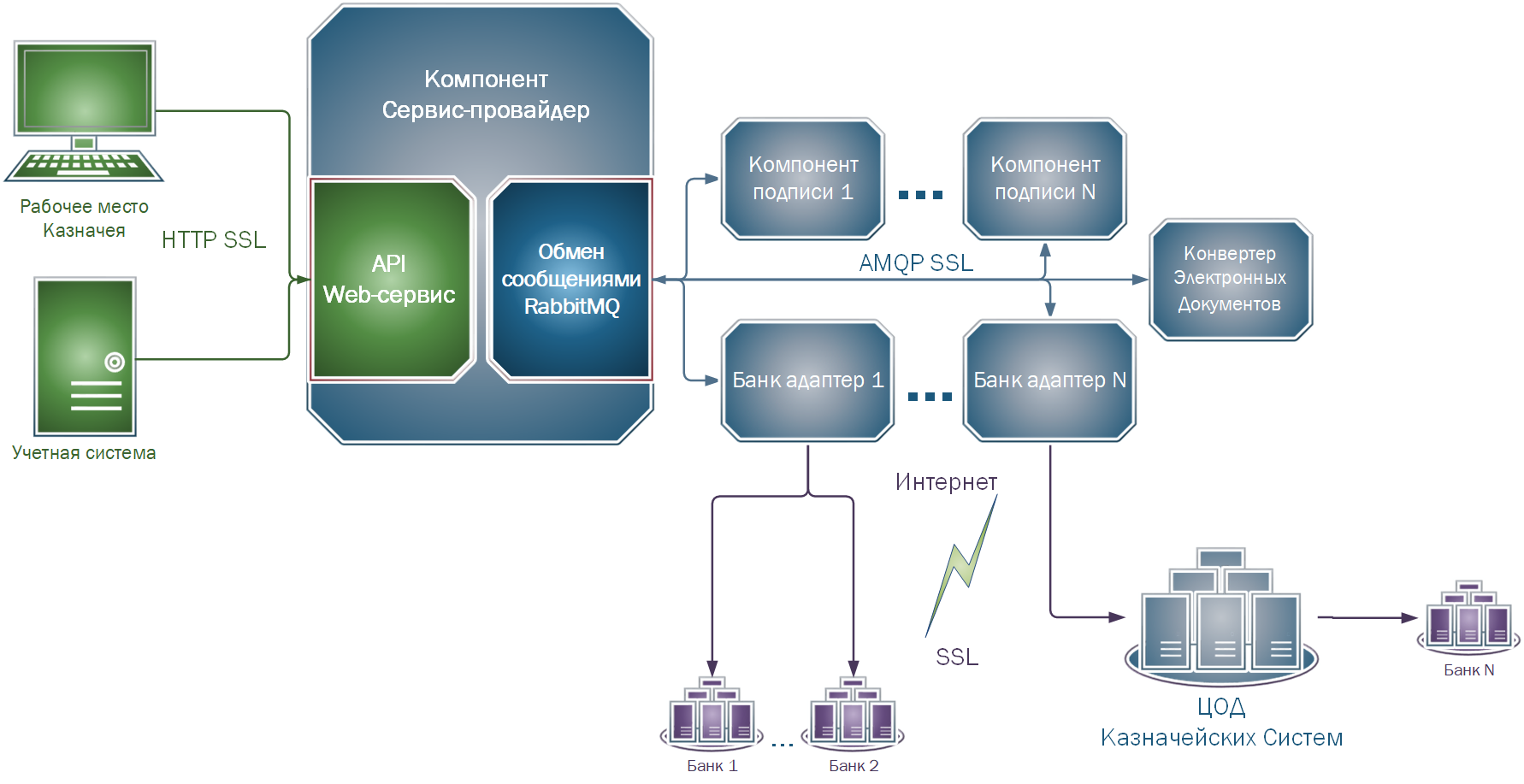
## On-Premise размещение



## Cloud размещение



## Комбинированное размещение



# **Описание компонентов и принципа работы системы**

## Общее описание системы

Компоненты системы взаимодействуют между собой с помощью очередей RabbitMQ. У каждого компонента системы есть очередь на брокере сообщений RMQ, которую они постоянно проверяют на наличие в ней входящих сообщений.

Каждый поддерживаемый документ, может иметь собственный уникальный путь, который он проходит по компонентам системы в процессе своего приема или отправки. Карта этих путей находится в конфигурационном файле компонента ServiceProvider.

**Пример взаимодействия компонентов при входящем (выписка, статус и т.д.) документе:**

Пример демонстрирует процесс получения выписки и ее конвертацию после получения в единый формат ISO 20022.

Шаги:

1. Веб-сервер компонента SP получает АПИ-запрос на получение выписки.
2. SP ставит задачу в очередь компонента BA.
3. BA считывает задачу из очереди и производит запрос выписки.
4. BA ставит задачу в очередь компонента DC.
5. DC получает задачу из очереди, конвертирует полученный документ из формата Банка в формат ISO 20022.
6. DC ставит задачу в очередь компонента SP.
7. SP получает задачу из очереди и отдает полученный из Банка и сконвертированный документ в ответ на АПИ-запрос.

**Пример взаимодействия компонентов при исходящем (рублевое ПП, СВО и т.д.) документе:**

Пример демонстрирует процесс отправки рублевого платежного поручения, полученного от клиента в едином формате ISO 20022, и сконвертированного в формат целевого Банка. Конвертация в формат целевого Банка и проставление ЭЦП подписанта(ов) происходит в одном клиентском АПИ запросе.

Шаги:

1. Веб-сервер компонента SP получает АПИ-запрос на отправку рублевого ПП.
2. SP ставит задачу в очередь компонента DC.
3. DC получает задачу из очереди и производит конвертацию документа из формата ISO 20022 в формат целевого Банка.
4. DC ставит задачу в очередь компоненту DS.
5. DS получает задачу из очереди и подписывает документ требуемым количеством ЭЦП.
6. DS ставит задачу в очередь компоненту BA.
7. BA получает задачу из очереди, производит отправку документа в Банк и получает из Банка обратное сообщение.
8. BA ставит задачу в очередь компонента SP.
9. SP получает задачу из очереди и отвечает сообщением из Банка на АПИ-запрос.

## Компонент Сервис-провайдер

SP предоставляет синхронный веб-интерфейс (веб-сервис) для потребителей/клиентов системы на основе встроенного веб-сервера и АПИ УПСК. При получении запроса со стороны клиента, SP анализирует запрос и если запрос не содержит ошибок, то SP ставит задачу в соответствующую очередь соответствующего компонента. После обработки задачи всеми компонентами сервиса, SP отдает полученный результат клиенту в той же сессии.

Компонент представляет из себя Windows-сервис. Для установки и запуска компонента необходима учетная запись, права которой позволяют запускать сервисы и производить установку инсталляционного пакета. Рабочий каталог компонента будет находиться в \Users\%username%\AppData\Local\UPGServiceProvider, где %username% - имя учетной записи, под которой установлен компонент.

Компонент сохраняет подробный журнал своей работы. Файл(ы) журнала находятся в \Users\%username%\AppData\Local\UPGServiceProvider\logs.

Конфигурационный файл upg\_service\_provider.json компонента находится в корне рабочего каталога.

Файл commands\_decomposer.json, находящийся в корне рабочего каталога компонента, содержит в себе карту команд, в соответствии с которой тот или иной документ проходит по компонентам системы.

Файл components\_registry.json, находящийся в корне рабочего каталога компонента, содержит в себе список всех зарегистрированных в данной инсталляции компонентов сервиса и сертификатов подписантов.

## Компонент Банк адаптер

BA взаимодействует с сервисами Банков по требуемым Банками протоколам. Обычно у каждого Банка собственный протокола обмена, и BA содержит все поддерживаемые системой протоколы обмена. На сервере BA обязательно должно быть установлено ПО КриптоПро CSP, так как для взаимодействия с некоторыми Банками необходимо хранить и генерировать сертификаты защищенного соединения. В рамках одной инсталляции системы может быть развернуто несколько компонентов BA, например, для разграничения подключений к разным Банкам или же для балансировки нагрузки.

Компонент представляет из себя Windows-сервис. Для установки и запуска компонента необходима учетная запись, права которой позволяют запускать сервисы, осуществлять интерактивный вход в систему и производить установку инсталляционного пакета. Рабочий каталог компонента будет находиться в \Users\%username%\AppData\Local\UPGBankAdapter, где %username% - имя учетной записи, под которой установлен компонент.

Компонент сохраняет подробный журнал своей работы. Файл(ы) журнала находятся в \Users\%username%\AppData\Local\UPGBankAdapter\logs. Дополнительный журнал для веб-просмотра находится в файле eventlog.db в корне рабочего каталога. Файл представляет собой БД в формате SQLite.

Конфигурационный файл bankadapterconfig.json компонента находится в корне рабочего каталога.

Так же в каталоге \Users\%username%\AppData\Local\UPGBankAdapter\AAStatement находится утилита AAStatement.exe, с помощью которой можно произвести настройки компонента в оконном режиме и запуск которой позволяет просматривать веб-журнал. Утилита AAStatement.exe должна быть запущена в сессии, авторизованной под учетной записью %username%.

## Компонент подписи

DS осуществляет криптографические операции с документами в системе. В основном, это подпись исходящих документов. Каждый Банк имеет собственный формат документов и соответственно собственные правила составления дайджестов для каждого документа. DS содержит в себе все правила составления дайджестов для поддерживаемых системой документов. На сервере компонента DS обязательно должно быть установлено ПО КриптоПро CSP, с помощью которого на основе дайджеста генерируется ЭЦП документа. Так же КриптоПро CSP используется как хранилище контейнеров закрытых частей ключа. Компонент может быть установлен на выделенный сервер и использоваться централизованно или же устанавливаться на каждый ПК подписанта и использоваться децентрализованно.

Компонент представляет из себя Windows-сервис. Для установки и запуска компонента необходима учетная запись, права которой позволяют запускать сервисы, осуществлять интерактивный вход в систему и производить установку инсталляционного пакета. Рабочий каталог компонента будет находиться в \Users\%username%\AppData\Local\UPGDocSigner, где %username% - имя учетной записи, под которой установлен компонент.

Компонент сохраняет подробный журнал своей работы. Файл(ы) журнала находятся в \Users\%username%\AppData\Local\UPGDocSigner\logs. Дополнительно компонент сохраняет составленный дайджест документа в каталоге \Users\%username%\AppData\Local\UPGDocSigner\artifacts.

Конфигурационный файл upg\_doc\_signer.jsonкомпонента находится в корне рабочего каталога.

## Компонент Конвертер

DC осуществляет конвертирование входящего или исходящего документа из целевого формата УС в формат требуемого Банка или наоборот. По умолчанию для документов УС поддерживается формат ISO 20022, но с помощью механизма правил конвертации могут быть добавлены любые другие наборы правил для других форматов документов.

Компонент представляет из себя Windows-сервис. Для установки и запуска компонента необходима учетная запись, права которой позволяют запускать сервисы и производить установку инсталляционного пакета. Рабочий каталог компонента будет находиться в \Users\%username%\AppData\Local\UPGDocConverter, где %username% - имя учетной записи, под которой установлен компонент.

Компонент сохраняет подробный журнал своей работы. Файл(ы) журнала находятся в \Users\%username%\AppData\Local\UPGDocConverter\logs. Конвертер также сохраняет оригинал поступившего документа и документ, получившийся после конвертации в каталоге \Users\%username%\AppData\Local\UPGDocConverter\artifacts в случае успешной операции конвертации.

Конфигурационный файл upg\_doc\_converter.jsonкомпонента находится в корне рабочего каталога. Также в корне рабочего каталога находятся правила конвертации в формате JSON – converter\_spec.json, converter\_status.json, converter\_currency\_op\_info.json и т.д.

# **Сетевое взаимодействие компонентов системы**

Компоненты системы взаимодействуют между собой с помощью брокера сообщений RMQ. Каждый компонент подключается к серверу RMQ, используя порт 5672 по умолчанию или 5671 в режиме шифрования трафика TLS. Потребители сервиса, используя встроенный веб-сервер компонента SP, подключаются на порт, определенный в настройках SP. По умолчанию 80 для открытого взаимодействия и 443 в режиме шифрования трафика.

**Примеры размещения серверов сервиса у Заказчика.**

**Вариант 1:**

Изображение выглядит как снимок экрана

Автоматически созданное описаниеУстановка на отдельный сервер компонента BA и размещение его в DMZ зоне. Остальные компоненты RMQ, SP, DS и DC устанавливаются на один сервер. Вариант подходит в случае, если необходимо вынести компонент системы, требующий интернет-соединения, в DMZ зону дата-центра компании.

**Вариант 2:**

Изображение выглядит как снимок экрана

Автоматически созданное описаниеУстановка всех компонентов УПСК на один сервер. Вариант подходит в случае, когда нет необходимости разнесения компонентов системы на разные сервера, например, для тестового стенда УПСК.

**Вариант 3:**

Изображение выглядит как снимок экрана

Автоматически созданное описаниеУстановка компонента BA на выделенный сервер и SP совместно с RMQ также на выделенный сервер. Вариант подходит в случае, если необходимо вынести компонент системы, требующий интернет-соединения, в DMZ зону дата-центра компании и одновременно вынести на отдельный сервер компонент системы, являющийся точкой входа для потребителей сервиса.

**Вариант 4:**

Установка всех компонентов УПСК на выделенные сервера. Вариант подходит в случае, когда необходима максимальная гибкость в настройках параметров информационной безопасности. Вынесение компонента, требующего интернет-соединение, в DMZ-зону, установка на отдельный сервер компонента, являющегося точкой входа для потребителей сервиса и установка компонента, обеспечивающего межкомпонентный обмен сообщениями, также на выделенный сервер.

Изображение выглядит как снимок экрана

Автоматически созданное описание

# **Описание механизма подтверждения отправителя и ПК (внутренний анти-фрод)**

В УПСК реализован механизм, который существенно увеличивает безопасность отправки финансовых сообщений в Банк за счет небольшого снижения производительности системы (увеличение общего времени на отправку документа). Механизм внутреннего анти-фрода может проверять документ, полученный из УС и опционально рабочее место, т.е. ПК, с которого был отправлен документ.

Механизм может работать в двух режимах:

* Только документ.
* Документ плюс ПК.

Для того, чтобы механизм внутреннего анти-фрода был задействован, необходимо выпустить внутренний сертификат(ы), с помощью которого будут подписываться сообщения, отправляемые из УС в УПСК. Также, если УПСК интегрируется с УС, которая полностью поддерживается Заказчиком самостоятельно, то специалисты Заказчика должны доработать механизм отправки документов в УПСК, включив в него все необходимые действия для поддержки внутреннего анти-фрода – составление внутреннего дайджеста документа, запрос системной информации о компонентах ПК и ее структурированное сохранение в отправляемом сообщении, подпись отправляемого запроса в УПСК внутренней ЭЦП, выпущенной для механизма анти-фрода.

Пример работы механизма подтверждения отправителя и документа в режиме «Документ плюс ПК»:

1. Сотрудник, работающий в УС, подготовил исходящий документ к отправке и нажал на кнопку «Отправить в Банк».
2. УС составляет внутренний дайджест документа.
3. УС запрашивает системную информацию о компонентах ПК.
4. УС объединяет внутренний дайджест документа и данные о ПК в единый дайджест внутреннего механизма анти-фрода.
5. УС подписывает единый дайджест механизма антифрода внутренней ЭЦП.
6. УС отправляет документ, содержащий в себе дополнительный блок данных внутреннего механизма анти-фрода в УПСК.
7. При поступлении документа на компонент DS начинается процесс проверки блока данных внутреннего механизма анти-фрода.
8. Составляется внутренний дайджест документа.
9. В случае децентрализованной конфигурации запрашиваются данные ПК, на котором установлен компонент подписи. В случае централизованной конфигурации данные о ПК запрашиваются из заранее составленного внутреннего реестра разрешенных к отправке рабочих мест.
10. Внутренний дайджест документа и данные о ПК объединяются в единый дайджест внутреннего механизма анти-фрода.

Происходит верификация полученного дайджеста, подписанного в УС и собранного на компоненте DS, и открытой части сертификата.

## Настройка механизма внутреннего анти-фрода

**Настройка DS**Для регулировки режимов работы механизма, в конфигурационном файле компонента DS upg\_doc\_signer.json предусмотрена секция:

"anti\_fraud" : {

"security\_level" : "disabled",

"supported\_certificates" : [

{

"name" : "Молоко Анна Андреевна, \"ООО Компания\", Бухгалтер, maa@company.ru, RU, 10026, Москва",

"serial" : "77779ea3f2644b120cfa"

}

]

}

security\_level может принимать значения:

* documents\_and\_pc\_props – документ плюс ПК
* documents\_only – только документ
* disabled – отключено, опция установлена по умолчанию

supported\_certificates содержит в себе данные сертификата, используемого для верификации подписи.

**Структура секции antiFraud в АПИ-запросе**

"antiFraud": {

"documents" : [

{

"content" : "dGVzdF90ZXh0", // документ

"crypto" :

{

"signatures" : [

{

"content" : "MIIHbQYJKoZIhvcNAQcCoIIHXjCCB1...", // подпись

}

]

}

}

]

}

В поле content передается значение document.content (отправляемый документ в конкретном АПИ-запросе) до конвертации в DC.

В поле signatures.content передается значение подписи, полученной по блоку данных.

## Формирование блока данных

**Общее правило формирования**

Блок данных формируется из поля command.document.content АПИ-запроса, приходящего на SP и строки str\_bank\_parameters, а также, в зависимости от необходимости, строки str\_pcProp.  
Знак + означает конкатенацию строк c вставкой символа ASCII #10 (LF).  
Кодировка строки – UTF-8.

* Без str\_pcProp (только документ):  
  **command.document.content+str\_bank\_parameters**
* С str\_pcProp (документ плюс ПК):  
  **command.document.content+str\_bank\_parameters+str\_pcProp**

command.document.content – строка контента документа, закодированная в base64.  
str\_bank\_parameters – передаваемые в АПИ-запросе параметры банка, набор данных из секции bank.parameters. Правило формирования описано ниже.  
str\_pcProp – набор идентификаторов оборудования. Правило формирования описано ниже.

**Правило формирования str\_bank\_parameters**

str\_bank\_parameters формируется из блока bank АПИ-запроса, приходящего на SP. Например:

"bank": {

"name": "vtb",

"parameters" : {

"clientId" : "7000002",

"currCode" : "840",

"kbopid" : "1",

"sets" : [

{

"clientId" : "1",

"currCode" : "2",

"kbopid" : "3"

},

{

"clientId" : "4",

"currCode" : "5",

"kbopid" : "6"

}

]

}

}

Все имена параметров необходимо привести к нижнему регистру и в лексикографическом порядке расположить их поэлементно «имя»=«значение». Если «значение» в элементе отсутствует, строку следует исключить из формируемого блока. Элементы разделяем ASCII #10 (LF).

Для приведенного выше блока bank должен получиться следующий str\_bank\_parameters:

bank.name=vtb

bank.parameters.clientid=700002

bank.parameters.currcode=840

bank.parameters.kbopid=1

bank.parameters.sets.clientid=1

bank.parameters.sets.clientid=4

bank.parameters.sets.currcode=2

bank.parameters.sets.currcode=5

bank.parameters.sets.kbopid=3

bank.parameters.sets.kbopid=6

**Правило формирования str\_pcProp**

str\_pcProp формируется из идентификаторов оборудования следующим образом:

**str\_cpuID+str\_serialBIOS+str\_serialHDD**

* str\_cpuID – строка значение cpuID. Например: BFEBFBFF000806E9.
* str\_serialBIOS – строка значение serialBIOS. Например: PF0UXFUM.
* str\_serialHDD – строка значение serialHDD. Например: 5CD2\_E415\_71A2\_26EF.

В строку **не должны попасть** идентификаторы извлекаемых носителей. При наличии нескольких жестких дисков необходимо вывести их идентификаторы друг за другом в лексикографическом порядке по возрастанию.

В результате должен получиться следующий str\_pcProp:

BFEBFBFF000806E9

PF0UXFUM

5CD2\_E415\_71A2\_26EF

**Пример итогового блока данных**

Пример состоит из строки контента документа «test\_text» (dGVzdF90ZXh0 в base64), параметров банка str\_bank\_parameters и идентификаторов оборудования str\_pcProp из примеров, указанных выше.

Без str\_pcProp (только документ):  
**command.document.content+str\_bank\_parameters**

dGVzdF90ZXh0

bank.name=vtb

bank.parameters.clientid=700002

bank.parameters.currcode=840

bank.parameters.kbopid=1

bank.parameters.sets.clientid=1

bank.parameters.sets.clientid=4

bank.parameters.sets.currcode=2

bank.parameters.sets.currcode=5

bank.parameters.sets.kbopid=3

bank.parameters.sets.kbopid=6

С str\_pcProp (документ плюс ПК)  
**command.document.content+str\_bank\_parameters+str\_pcProp**

dGVzdF90ZXh0

bank.name=vtb

bank.parameters.clientid=700002

bank.parameters.currcode=840

bank.parameters.kbopid=1

bank.parameters.sets.clientid=1

bank.parameters.sets.clientid=4

bank.parameters.sets.currcode=2

bank.parameters.sets.currcode=5

bank.parameters.sets.kbopid=3

bank.parameters.sets.kbopid=6

BFEBFBFF000806E9

PF0UXFUM

5CD2\_E415\_71A2\_26EF

# **Установка и настройка компонентов системы**

Перед началом работы:

* Дистрибутивы компонентов системы получены Клиентом;
* Дистрибутивы обязательного и опционального ПО загружены Клиентом;
* Выбрана модель установки компонентов системы;
* Выбрана модель работы компонента DS – централизованная или децентрализованная;
* Выбран режим работы веб-сервера компонента SP – HTTP или HTTPS;
* Выбран режим работы RabbitMQ – AMPQ без шифрования или AMPQ TLS;
* Выделены и подготовлены в соответствии с п.3 виртуальные или физические сервера для установки компонентов системы;
* Если требуется, установлено необходимое аппаратное обеспечение;
* Сервер компонента BA имеет сетевой доступ до серверов требуемых Банков;
* Настроено сетевое взаимодействие между серверами компонентов системы, согласно схеме сетевого взаимодействия конкретной инсталляции;
* Выделены доменные или локальные аккаунты ОС для установки и запуска компонентов системы согласно п.5.

## Установка и настройка RabbitMQ

### Установка

Рекомендуется устанавливать RabbitMQ на тот же сервер, на котором будет установлен компонент SP. RabbitMQ должен устанавливаться в первую очередь, до всех остальных компонентов системы.

Для этого необходимо выполнить следующие шаги:

1. Запускаем инсталляционный пакет Erlang/OTP и устанавливаем его. Установка производится с параметрами по умолчанию;
2. Запускаем инсталляционный пакет RabbitMQ. Установка также производится с параметрами по умолчанию.

После установки компонентов необходимо убедиться, что служба RabbitMQ запущена

### Настройка

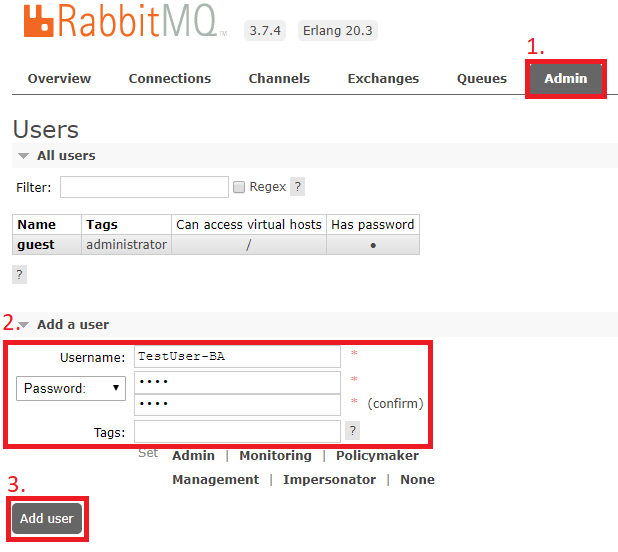
Для настройки необходимо включить панель управления RabbitMQ. Для этого нужно:

1. Открыть командную строку
2. Перейти в командной строке в директорию, куда была произведена установка RabbitMQ, и перейти в папку rabbitmq\_server-3.7.x\sbin. Обычно этот путь имеет следующий вид: \Program Files\RabbitMQ Server\rabbitmq\_server-3.7.x\sbin
3. Выполнить команду: rabbitmq-plugins enable rabbitmq\_management
4. Перезапустить службу RabbitMQ

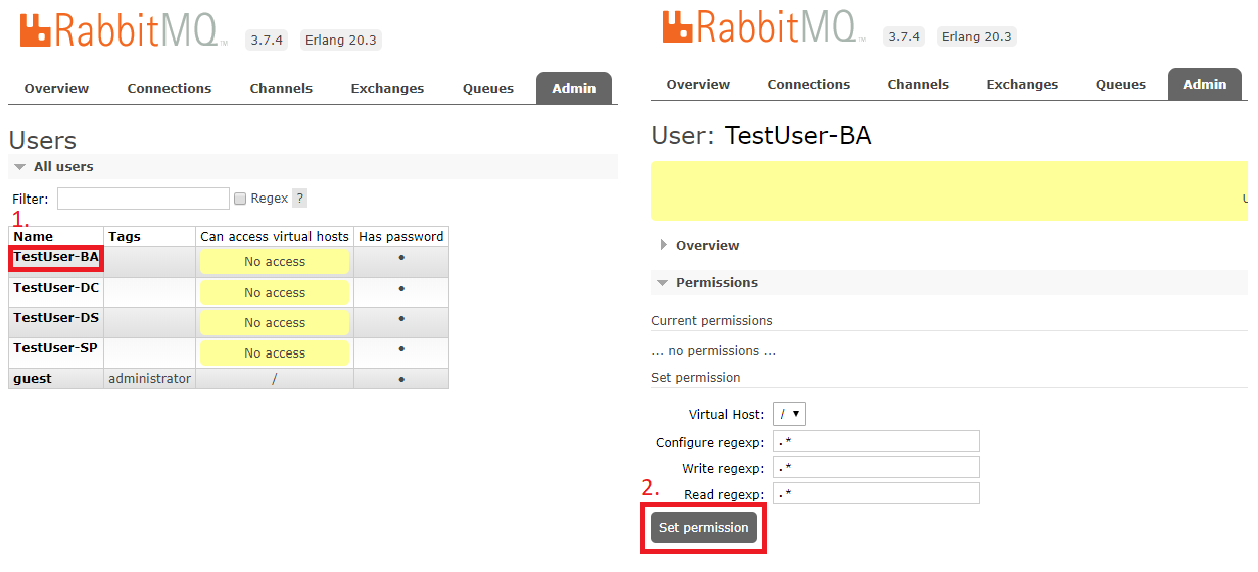
Панель управления становится доступна по адресу http://localhost:15672/. По умолчанию в RabbitMQ создается пользователь guest с паролем guest, которого можно использовать для входа в панель управления. Доступ к панели управления под данным пользователем возможен только локально.

Если все компоненты системы расположены на одном сервере, то для взаимодействия компонентов с RMQ можно использовать учетную запись по умолчанию (guest).

Если же компоненты расположены на разных серверах, то для каждого компонента системы УПСК необходимо создать пользователя, через которого будет осуществляться взаимодействие с RabbitMQ. Для создания пользователя в панели управления RabbitMQ нужно перейти на вкладку «Admin», ввести желаемое имя пользователя, пароль и нажать кнопку «Add user».



После добавления всех пользователей, каждому необходимо выдать права доступа к виртуальному хосту. Для этого нужно нажать на пользователя и в секции «Permissions» нажать на кнопку «Set Permission».



### Настройка SSL

Для того чтобы настроить SSL, необходимо выполнить следующие шаги:

1. Перейти в директорию с конфигурационным файлом RabbitMQ. По умолчанию путь до директории: \Users\%username%\AppData\Roaming\RabbitMQ
2. Создать или открыть конфигурационный файл advanced.config
3. Содержимое конфигурационного файла должно быть следующим:

[

{ tcp\_listeners, []}, // указываются порты для TCP-соединений. В данном примере

// отключен прием сообщений без SSL

{ rabbit, [

{ ssl\_listeners, [5671] }, //указываются порты для SSL-соединений

{ ssl\_options, [

{ cacertfile, "path/testca/cacert.pem"}, // путь до корневого сертификата

{ certfile, "path/server/cert.pem"}, // путь до сертификата

{ keyfile, "path/server/key.pem"}, // путь до закрытого ключа

{ verify, verify\_peer},

{ fail\_if\_no\_peer\_cert, false}]}

]

}

]

1. Перезапустить службу RabbitMQ
2. В случае успешной настройки, в журналах RabbitMQ будет содержаться строка «started SSL Listener on 0.0.0.0:5671».   
   Журналы можно найти в директории Users\%username%\AppData\Roaming\RabbitMQ\log

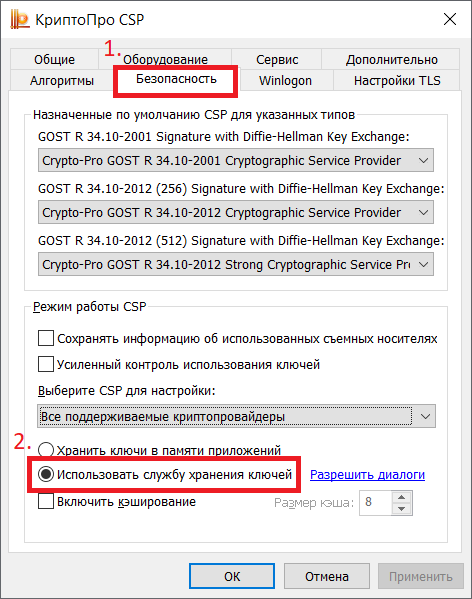
## Установка и настройка КриптоПро CSP

### Установка

Установка КриптоПро CSP выполняется с параметрами по умолчанию.

### Настройка

Для работы с сертификатами может потребоваться включить службу хранения ключей. Для этого необходимо запустить КриптоПро CSP от имени администратора, перейти на вкладку «Безопасность» и выбрать режим работы с использованием службы хранения ключей.

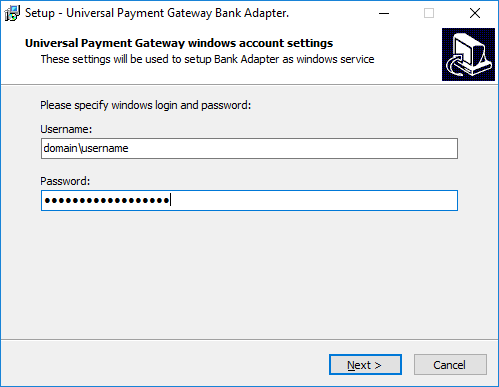


## Установка и настройка компонента ServiceProvider

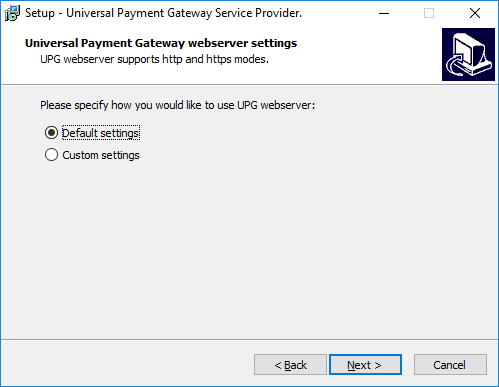
### Установка

Для того чтобы установить компонент ServiceProvider, необходимо выполнить следующие шаги:

1. Запустить инсталляционный пакет SP. Первое окно установки является одинаковым для всех компонентов УПСК. Оно содержит поля ввода логина и пароля учетной записи Windows. Если учетная запись является доменной, то к имени пользователя необходимо добавить домен.

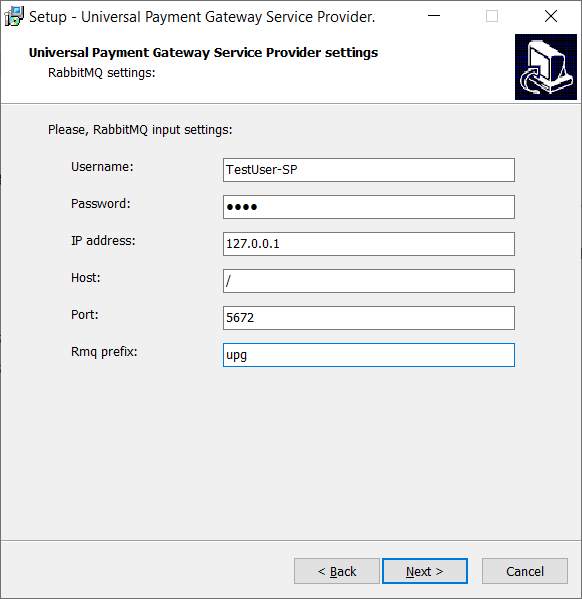


1. В следующем окне выбрать установку с настраиваемыми параметрами (Custom settings)



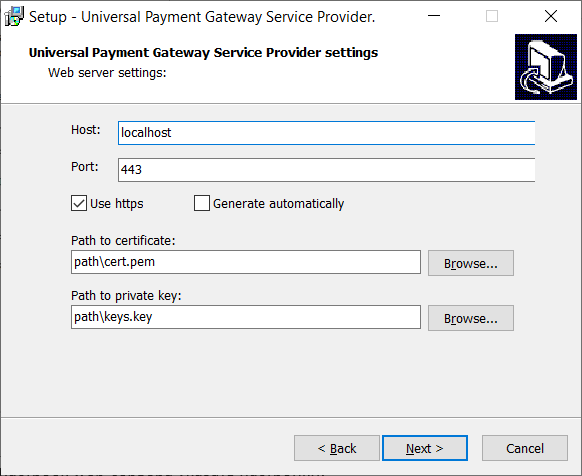
1. В окне настроек RabbitMQ указать следующие настройки:

* Username и password – имя и пароль пользователя RabbitMQ, который был создан для компонента SP;
* IP address – IP-адрес машины, на которой установлен RabbitMQ. Если RMQ установлен на локальной машине, то оставить без изменений;
* Host – указывается имя виртуального хоста;
* Port – порт, на котором работает веб-сервер RabbitMQ;
* Rmq prefix – указывается префикс наименования очередей для компонентов. Значение поля можно оставить по умолчанию.



1. В окне настроек веб-сервера указать настройки:

* Host – указывается значение localhost;
* Port – порт, на котором будет работать компонент;
* Use https – при активации настройки компонент будет работать в режиме https. При этом необходимо указать пути до сертификата и закрытого ключа;
* Generate automatically – при активации настройки будет сгенерирован самоподписанный сертификат и ключ.



1. !Окно настроек подключения к конвертеру в будущем будет убрано. Настройки из этого окна более не используются. Указать любые значения! Окно настроек подключения к компоненту DC:

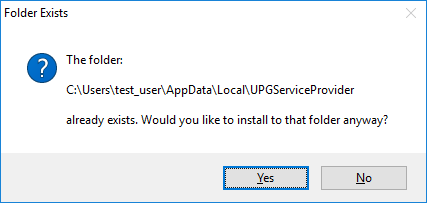
* Use Converter – указывается, если необходимо использовать компонент DC;
* Host – IP-адрес машины, на которой установлен компонент DC;
* Port – порт на котором работает компонент DC.

1. В последующих окнах настройки остаются без изменения.

После установки компонента проверить, что служба UPGServiceProvider\_username запущена.

### Обновление компонента

1. Запустить инсталляционный пакет SP. Ввести логин и пароль пользователя Windows;
2. Выбрать тип установки с настройками по умолчанию;
3. В окне настроек веб-сервера необходимо ввести любые символы в поля host и port (данные параметры применяться не будут), деактивировать настройку Use https. В последующих окнах оставить значения по умолчанию;
4. В окне выбора места установки компонента согласиться на установку в существующую директорию:



После обновления компонента проверить, что служба UPGServiceProvider\_username запущена.

### Описание конфигурационного файла

Конфигурационный файл находится в директории установленного компонента и называется upg\_service\_provider.json

{

  "log\_files\_rotation\_max\_size\_mb" : 200,  // размер файла с логами, после которого

// происходит его ротация, в мегабайтах

  "should\_archive\_old\_log\_files" : "true",  // следует ли проводить ротацию логов

  "rmq\_host" : "127.0.0.1",  // адрес машины с брокером RabbitMQ (RMQ)

  "rmq\_port" : "5672",  // порт, на котором работает брокер RMQ

  "rmq\_username" : "guest",  // имя пользователя SP в RMQ

  "rmq\_password" : "guest",  // пароль пользователя SP в RMQ

  "rmq\_vhost" : "/",   // виртуальный хост на брокере RMQ

  "rmq\_delete\_entities\_on\_start": "false",  // пересоздать очереди RMQ при запуске

  "rmq\_message\_expiration\_msec": 180000,  // время жизни задачи (применяется только при

// создании очередей)

  "rmq\_ssl\_enabled" : "false",  // использовать SSL подключение

  "rmq\_ssl\_CACertPath" : "path\\testca\\cacert.pem", // путь до сертификата CA для RMQ

  "rmq\_ssl\_keyPemPath" : "path\\client\\key.pem",  // путь до ключей сертификата клиента для RMQ

  "rmq\_ssl\_certPemPath" : "path\\client\\req.pem",  // путь до сертификата клиента для RMQ

  "rmq\_ssl\_verifyHostname" : "false",  // проверка сертификата сервера RMQ

  "sp\_host" : "127.0.0.1", // локальный адрес компьютера, на котором установлен SP

  "sp\_port" : "9090",  // порт, на котором работает SP

  "sp\_https\_on" : "false", // использовать SSL соединение для веб-сервера SP

  "sp\_cert\_path" : "C:\\Users\\${username}\\AppData\\Local\\UPGServiceProvider\\sp\_server.pem",

// путь к .pem файлу для веб-сервера (нужен, если https включен)

    "sp\_key\_path" : "C:\\Users\\${username}\\AppData\\Local\\UPGServiceProvider\\sp\_server.key",

// путь к .key файлу для веб-сервера (нужен, если https включен)

"sp\_web\_server\_read\_timeout\_sec" : 120,  // таймаут веб-сервера на чтение

  "sp\_web\_server\_write\_timeout\_sec" : 120, // таймаут веб-сервера на запись

  "sp\_max\_sync\_commands": 2000, // максимальное количество синхронных подключений к компоненту

  "sp" : {

   "timeout\_sec" : 121, // таймаут обращения к компоненту Банк адаптер

    "rmq" : {

     "input\_exchange\_name" : "upg-sp-input-exch", // имя точки обмена для входной очереди RMQ

      "input\_queue\_name" : "upg-sp-input-queue",   // имя входной очереди RMQ

      "output\_exchange\_name" : "upg-sp-output-exch", // имя точки обмена для выходной очереди RMQ

      "output\_queue\_name" : "upg-sp-output-queue",  // имя выходной очереди RMQ

      "routing\_key" : "upg-key"  // имя ключа маршрутизации для очереди/точки обмена RMQ

    }

  }

}

## Установка и настройка компонента BankAdapter

### Установка

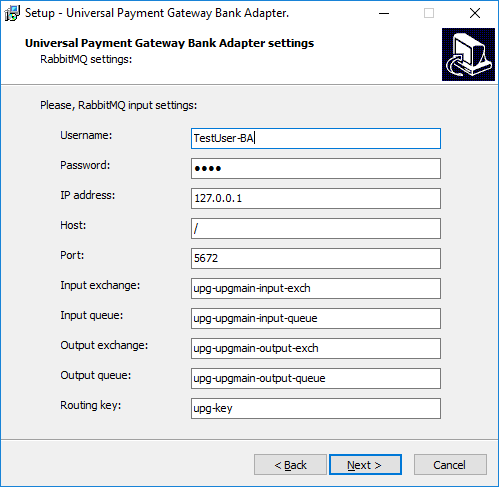
Для того чтобы установить компонент BankAdapter, необходимо выполнить следующие шаги:

1. Запускаем инсталляционный пакет BA. Вводим логин и пароль учетной записи Windows;
2. В следующем окне выбрать установку с custom параметрами;
3. В окне настроек RabbitMQ указываем настройки:

* Username и password – имя и пароль пользователя RabbitMQ, который был создан для компонента SP;
* IP address – IP-адрес машины, на которой установлен RabbitMQ. Если RMQ установлен на локальной машине, оставить без изменений;
* Port – порт, на котором работает веб-сервер RabbitMQ.

Следующие параметры можно оставить с настройками по умолчанию:

* Host – указывается имя виртуального хоста;
* Input exchange – имя обменника для маршрутизации входящих сообщений;
* Input queue – имя очереди для входящих команд;
* Output exchange – имя обменника для маршрутизации исходящих сообщений;
* Output queue – имя очереди для исходящих команд;
* Routing Key – ключ маршрутизации.



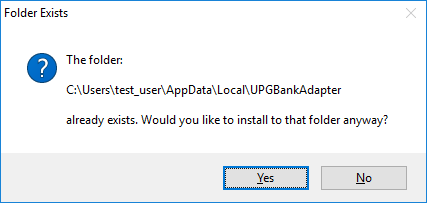
1. В последующих окнах настройки остаются без изменения.

После установки компонента необходимо проверить, что служба UPGBankAdapter\_username запущена.

### Обновление компонента

Для того чтобы обновить компонент BankAdapter, необходимо выполнить следующие шаги:

1. Перед обновлением компонента BA необходимо убедиться, что утилита AAStatement.exe закрыта;
2. Запустить инсталляционный пакет BA. Ввести логин и пароль учетной записи Windows;
3. Выбрать тип установки с настройками по умолчанию;
4. В последующих окнах оставить значения по умолчанию;
5. В окне выбора места установки компонента согласиться на установку в существующую директорию:



После обновления компонента проверить, что служба UPGBankAdapter\_username запущена.

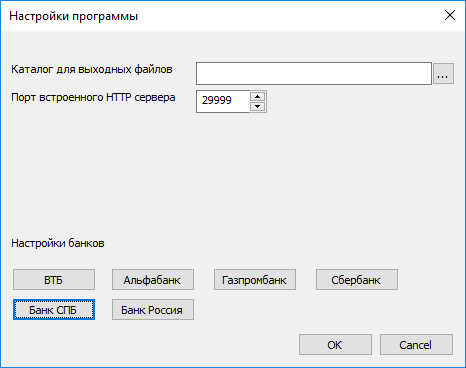
### Описание утилиты AAStatement.exe

Утилита AAStatement.exe находится в директории, куда был установлен компонент BA, в папке AAStatement.

Путь по умолчанию, следующий:

\Users\USERNAME\AppData\Local\UPGBankAdapter\AAStatement\AAStatement.exe

После открытия программы и нажатия кнопки Настройки будут доступны настройки для просмотра веб-логов и настройки подключения к банкам.

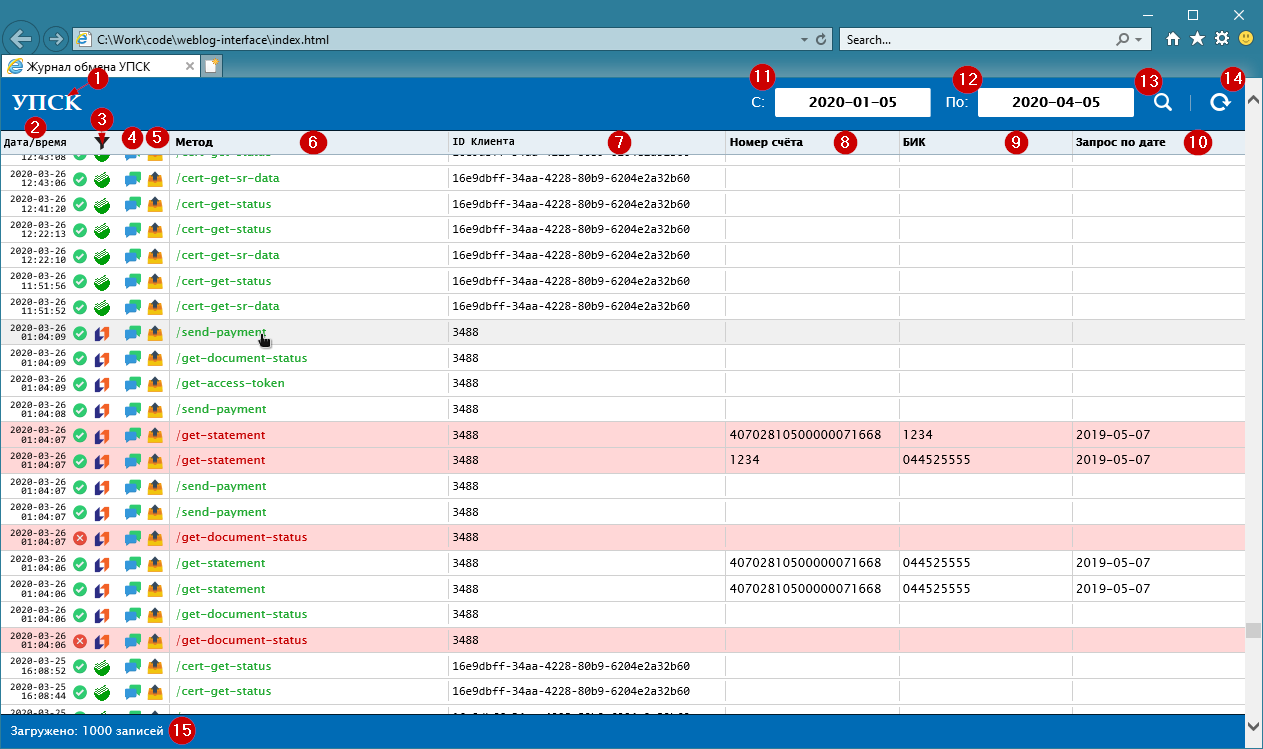


### Просмотр веб-журнала обмена

**Для коректной работы веб-журнала обмена требуется браузер Internet Explorer 11 или старше, Microsoft Edge или Google Chrome.** В браузере Internet Explorer необходимо разрешить исполнение активного содержимого.

Для просмотра веб-журнала обмена необходимо открыть файл index.html, который находится в директории, куда был установлен компонент BA, в папке AAStatement. Для удобства доступа рекомендуется создать на рабочем столе администратора УПСК ярлык для этого файла.

Путь по умолчанию, следующий: \Users\USERNAME\AppData\Local\UPGBankAdapter\AAStatement\index.html



Интерфейс веб-журнала обмена.

1. Логотип. При нажатии на него страница обновляется и подгружаются свежие данные.
2. Дата и время запроса полученного компонентом BA.
3. Банк назначения запроса с возможностью фильтрации по нему.
4. Журнал обмена данными с банком. При нажатии подробные данные по обмену откроются в отдельном поле. Данные можно использовать для анализа инцидентов и обращения в службу технической поддержки Банка.
5. Результат запроса, полученный компонентом BA от банка. При нажатии полный текст ответа на запрос откроется в отдельном поле.
6. Тип запроса, полученный компонентом SP. При нажатии на заголовок появится возможность отфильтровать данные по этому полю. Для очистки фильтра необходимо нажать в свободную часть заголовка.
7. Идентификатор клиента в банке. Может быть пустым, в случае если в банке собственная идентификации клиента или поле clientId в запросе не заполнено. При нажатии на заголовок появится возможность отфильтровать данные по этому полю. Для очистки фильтра необходимо нажать в свободную часть заголовка.
8. Номер счёта, по которому совершался запрос. Может быть пустым, в случае если в запросе отсутствует поле «номер счёта». При нажатии на заголовок появится возможность отфильтровать данные по этому полю. Для очистки фильтра необходимо нажать в свободную часть заголовка.
9. БИК банка назначения запроса. При нажатии на заголовок появится возможность отфильтровать данные по этому полю. Для очистки фильтра необхадимо нажать в свободную часть заголовка.
10. Дата за которую запрашивались данные из банка. Может быть пустой, в случае если в запросе отсутствует поле «дата». При нажатии на заголовок появится возможность отфильтровать данные по этому полю. Для очистки фильтра необходимо нажать в свободную часть заголовка.
11. Дата с которой запрашиваются данные веб-журнала обмена.
12. Дата по которую запрашиваются данные веб-журнала обмена.
13. Кнопка поиска.
14. Переключатель автообновления. Если активен – запрашивает данные о последних 500 операциях каждые 30 секунд. Предназначен для оперативного мониторинга запросов обрабатываемых компонентом BA.
15. Количество записей веб-журнала загруженных на страницу в текущий момент, с учётом фильтрации.

Записи веб-журнала отсортированы в порядке убывания – самый последний запрос, обработанный компонентом BA расположен сверху списка. Записи загружаются в интерфейс блоками по 500 запросов.

### Описание конфигурационного файла

Конфигурационный файл находится в директории установленного компонента и имеет название bankadapterconfig.json

{

"outdir" : "",

// настройки ротации логов

  "logtotalsize" : 1073741824, // УТОЧНИТЬ

  "logrotationsize" : 104857600, // УТОЧНИТЬ

"httpPort" : 80, // порт, на котором запускается веб-сервер AAStatement

"webServerHttpsEnabled" : false, // использовать ли https в веб-сервере

"webServerKeyFilePath" : "path\\cert.key", // путь к .key файлу для веб-сервера

// (нужен, если https включен)

"webServerCertFilePath" : "path\\cert.pem",// путь к .pem файлу для веб-сервера

// (нужен, если https включен)

"rmq\_host" : "127.0.0.1", // адрес машины с RMQ

"rmq\_port" : "5672", // порт, на котором работает RMQ

"rmq\_username" : "guest", // имя пользователя для компонента BA

"rmq\_password" : "guest", // пароль пользователя

"rmq\_vhost" : "/", // виртуальный хост на RMQ

"rmq\_inputExchangeName" : "upg-upgmain-input-exch", // имя точки обмена для входной очереди RMQ

"rmq\_inputQueueName" : "upg-upgmain-input-queue", // имя входной очереди RMQ

"rmq\_outputExchangeName" : "upg-upgmain-output-exch",// имя точки обмена для выходной очереди RMQ

"rmq\_outputQueueName" : "upg-upgmain-output-queue", // имя выходной очереди RMQ

"rmq\_routingKey" : "upg-key", // имя ключа маршрутизации для RMQ

"rmq\_ssl\_enabled" : "false", // использовать SSL подключение

"rmq\_ssl\_CACertPath" : "path\\testca\\cacert.pem", // путь до сертификата CA

"rmq\_ssl\_keyPemPath" : "path\\client2\\key.pem", // путь до ключей сертификата клиента

"rmq\_ssl\_certPemPath" : "path\\client2\\req.pem", // путь до сертификата клиента

"rmq\_ssl\_verifyPeer" : "false", // отправить сертификат серверу

"rmq\_ssl\_verifyHostname" : "false", // проверять сертификата сервера

//Массив с настройками для банков

"banks" : [

{

"bankdir" : "", // УТОЧНИТЬ (ГПБ)

"outbox" : "", // УТОЧНИТЬ (ГПБ)

"maxSimultaneousConnections" : 5, // максимальное количество одновременных запросов к банку

"certsubject" : "RU, MSK, JSC Vneshtorgbank, vtbClient, 0550439093\_KondrashovRA",

// указывается сертификат (информация берется из поля

// Subject в информации о сертификате)

"name" : "vtb", // строковый идентификатор банка

"url" : "https://”, // URL для обращений к банку

"url2" : "https://”, // URL загрузки больших файлов (Сбербанк)

"orgData" : "", // зашифрованные данные организации. (Сбербанк)

"sender" : "", // идентификатор отправителя. (ГПБ)

"repeatingRequestsTimeout" : 1000

}

]

}

## Установка и настройка компонента DocSigner

### Установка

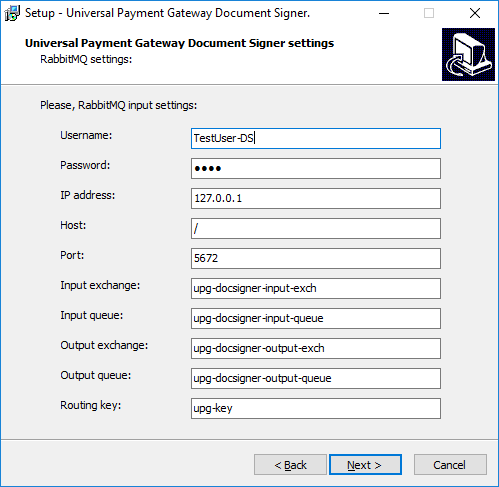
Для того чтобы установить компонент DocSigner, необходимо выполнить следующие шаги:

1. Запускаем инсталляционный пакет BA. Вводим логин и пароль учетной записи Windows;
2. В следующем окне выбираем установку с настраиваемыми параметрами (Custom settings);
3. В окне настроек RabbitMQ указываем настройки:

* Username и password – имя и пароль пользователя RabbitMQ, который был создан для компонента SP;
* IP address – IP-адрес машины, на которой установлен RabbitMQ. Если RMQ установлен на локальной машине, то оставить без изменений;
* Port – порт, на котором работает веб-сервер RabbitMQ.

Следующие параметры можно оставить с настройками по умолчанию:

* Host – указывается имя виртуального хоста;
* Input exchange – имя обменника для маршрутизации входящих сообщений;
* Input queue – имя очереди для входящих команд;
* Output exchange – имя обменника для маршрутизации исходящих сообщений;
* Output queue – имя очереди для исходящих команд;
* Routing Key – ключ маршрутизации.



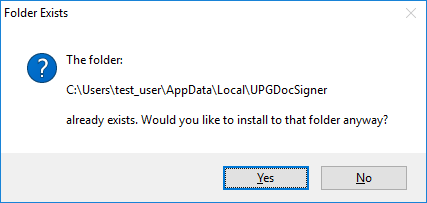
1. В последующих окнах настройки остаются без изменения.

После установки компонента необходимо проверить, что служба UPGDocSigner\_username запущена.

### Обновление компонента

Для того, чтобы обновить компонент DocSigner необходимо выполнить следующие шаги:

1. Запустить инсталляционный пакет DS. Ввести логин и пароль учетной записи Windows;
2. Выбрать тип установки с настройками по умолчанию;
3. В последующих окнах оставить значения по умолчанию;
4. В окне выбора места установки компонента согласиться на установку в существующую директорию:



После обновления компонента проверить, что служба UPGDocSigner\_username запущена.

### Описание конфигурационного файла

Конфигурационный файл находится в директории установленного компонента и имеет название upg\_doc\_signer.json

{

// секция настройки антифрода

  "anti\_fraud": {

    "security\_level": "disabled", // режим работы. Доступны "disabled", "documents\_only",

// "documents\_and\_pc\_props"

    "supported\_certificates": [

{

   "name" : "Молоко Анна Андреевна, \"ООО Компания\", Бухгалтер, maa@company.ru, RU, 10026, Москва",

        "serial" : "77779ea3f2644b120cfa"

      }

    ]

  },

// секция настройки RabbitMQ

 "rmq\_ip" : "127.0.0.1", // адрес машины с RMQ

  "rmq\_port" : "5672", // порт, на котором работает RMQ

  "rmq\_username" : "guest", // имя пользователя DS в RabbitMQ

  "rmq\_password" : "guest", // пароль пользователя

  "rmq\_vhost" : "/", // виртуальный хост на RabbitMQ

  "rmq\_inputExchangeName" : "upg-docsigner-input-exch", // имя точки обмена для входной очереди RMQ

  "rmq\_inputQueueName" : "upg-docsigner-input-queue", // имя входной очереди RMQ

  "rmq\_outputExchangeName" : "upg-docsigner-output-exch",// имя точки обмена для выходной очереди

  "rmq\_outputQueueName" : "upg-docsigner-output-queue", // имя выходной очереди RMQ

  "rmq\_routingKey" : "upg-key", // имя ключа маршрутизации для RMQ

  "rmq\_ssl\_enabled" : "false", // использовать SSL подключение

  "rmq\_ssl\_CACertPath" : "path\\testca\\cacert.pem", // путь до сертификата CA

  "rmq\_ssl\_keyPemPath" : "path\\client2\\key.pem", // путь до ключей сертификата клиента

  "rmq\_ssl\_certPemPath" :"path\\client2\\req.pem", // путь до сертификата клиента

  "rmq\_ssl\_verifyPeer" : "false", // отправить сертификат серверу для проверки

  "rmq\_ssl\_verifyHostname" : "false", // проверка сертификата сервера

//секция настроек банка

  "banks" : [

   {

      "name" : "vtb", //имя банка, для которого будут использоваться сертификаты

      "crypto" : {

//секция настроек сертификатов

        "certificates" : [

          {

// уникальный ID (GUID) сертификата (используется в запросе к UPG)

            "id" : "5B6F72CD-1C16-4DF2-A374-BA5C4DA58DD7",

// subject сертификата

            "name" : "RU, MSK, JSC Vneshtorgbank, vtbClient, 0550400138\_SidorovSS",

// серийный номер сертификата (serial)

            "serial" : "405017306a88126586bce35d5c24be3c"

          }

        ]

     }

    }

  ]

}

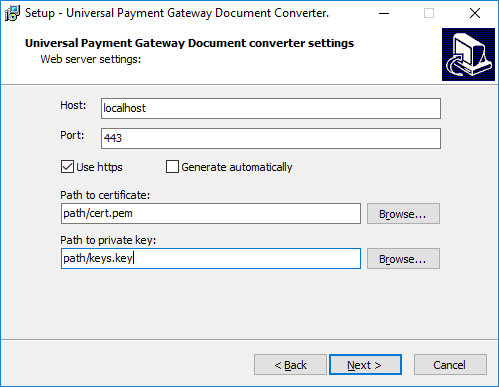
## Установка и настройка компонента DocConverter

### Установка

Для того чтобы установить компонент DocConverter, необходимо выполнить следующие шаги:

1. Запускаем инсталляционный пакет DC. Вводим логин и пароль учетной записи Windows.
2. !Окно настроек веб-сервера в будущем будет убрано. Настройки из этого окна более не используются. Указать любые значения! В окне настроек веб-сервера указать настройки:

* Host – указывается значение localhost;
* Port – порт, на котором будет работать компонент;
* Use https – при активации настройки компонент будет работать в режиме https. При этом потребуется указать пути до сертификата и его закрытого ключа;
* Generate automatically – при активации настройки будет сгенерирован самоподписанный сертификат и ключ.



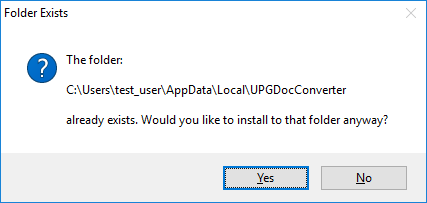
1. В последующих окнах настройки остаются без изменения.

После установки компонента необходимо проверить, что служба UPGDocConverter\_username запущена.

### Обновление компонента

Для того чтобы обновить компонент DocConverter, необходимо выполнить следующие шаги:

1. Запустить инсталляционный пакет DC. Ввести логин и пароль пользователя Windows;
2. Выбрать тип установки с настройками по умолчанию;
3. В окне настроек веб-сервера необходимо ввести любые символы в поля host и port (данные параметры применяться не будут), деактивировать настройку Use https. В последующих окнах оставить значения по умолчанию;
4. В окне выбора места установки компонента согласиться на установку в существующую директорию:



После обновления компонента проверить, что служба UPGDocConverter\_username запущена.

### Описание конфигурационного файла

Конфигурационный файл находится в директории установленного компонента и имеет название upg\_doc\_converter.json

{

"log\_files\_rotation\_max\_size\_mb" : 200, // размер файла с логами, после которого происходит

// ротация

  "should\_archive\_old\_log\_files" : true,  // следует ли проводить архивацию логов

  // секция настройки RabbitMQ

 "rmq\_ip" : "127.0.0.1", // адрес машины с RMQ

  "rmq\_port" : "5672", // порт, на котором работает RMQ

  "rmq\_username" : "guest", // имя пользователя DS в RabbitMQ

  "rmq\_password" : "guest", // пароль пользователя

  "rmq\_vhost" : "/", // виртуальный хост на RabbitMQ

"rmq\_ssl\_enabled" : "false", //использовать SSL подключение

  "rmq\_ssl\_CACertPath" : "path\\testca\\cacert.pem", //путь до сертификата CA

  "rmq\_ssl\_keyPemPath" : "path\\client2\\key.pem", //путь до ключей сертификата клиента

  "rmq\_ssl\_certPemPath" :"path\\client2\\req.pem", //путь до сертификата клиента

  "rmq\_ssl\_verifyPeer" : "false", //отправить сертификат серверу для проверки

  "rmq\_ssl\_verifyHostname" : "false", //проверка сертификата сервера

  "rmq": {

    "input\_exchange\_name": "upg-converter-input-exch", // имя точки обмена для входной очереди RMQ

    "input\_queue\_name": "upg-converter-input-queue", // имя входной очереди RMQ

    "output\_exchange\_name": "upg-converter-output-exch",// имя точки обмена для выходной очереди

    "output\_queue\_name": "upg-converter-output-queue", // имя выходной очереди RMQ

    "routing\_key": "upg-key” // имя ключа маршрутизации для RMQ

  },

  "dc\_strict\_conversions" : true, // настройка проверки ошибок при конвертации

  "dc\_artifacts\_dir": "C:\\Users\\%username%\\AppData\\Local\\UPGDocConverter\\artifacts",

  // массив документов с правилами конвертации

"dc\_documents\_supported" : [

    {

     "name" : "commercial\_payment", // имя документа для запроса

      "conversion\_specs" : [ // массив документов, которые будут использоваться

        {"filename" : "converter\_spec.json"}

      ]

    },

    {

      "name" : "tax\_payment",

      "conversion\_specs" : [

        {"filename" : "converter\_spec.json"},

        {"filename" : "converter\_tax\_pain.json"}

      ]

    }

  ]

}

## Проверка работоспособности компонентов УПСК

Проверку работоспособности компонентов УПСК можно провести с помощью тестового банка treasure. Для этого в конфигурационном файле BA в настройках банка нужно добавить следующую секцию:

{

"bankdir" : "",

"outbox" : "",

"maxSimultaneousConnections" : 2,

"version" : 0,

"cert" : {

"id" : "e9351841-85b3-4891-97a9-0ba8232769ee"

},

"name" : "treasure",

"url" : "",

"orgData" : "",

"sender" : "",

"repeatingRequestsTimeout" : 1000,

"fintechClientId" : "",

"fintechClientSecret" : "",

"secure" : "false",

"management\_mode" : ""

},

После необходимо отправить запрос send-payment (см. Документацию по протоколу AA-API v1) на компонент ServiceProvider. С помощью данного запроса осуществляется взаимодействие всех компонентов системы УПСК.

При успешном выполнении запроса ответ будет следующим:

{

"upg\_response": {

"code": 0,

"comment": "client--sp--signer--adapter",

"operationResult": {

"bank": {

"name": "treasure"

},

"document": {

"id": "1\_414213562\_373\_0951488"

}

}

}

}

## Настройки подключения к банкам

### Настройки для банка ВТБ

Для настройки подключения к банку ВТБ необходимо:

1. Открыть конфигурационный файл компонента BankAdapter
2. В массив banks добавить секцию настроек банка ВТБ:

"banks" : [

{

"bankdir" : "",

"outbox" : "",

"maxSimultaneousConnections" : 0,

"version" : 0,

"cert" : {

"id" : "3e88140b-50e0-4288-869b-47406178b4ef",

"name" : "RU, MSK, JSC Vneshtorgbank, vtbClient, 0559180\_IvanovVS",

"serial" : "405017306a88126586bce35d5c24be3c"

},

"name" : "vtb",

"url" : "https://dbotest.vtb.ru",

"orgData" : "",

"sender" : "",

"repeatingRequestsTimeout" : 0,

"fintechClientId" : "",

"fintechClientSecret" : "",

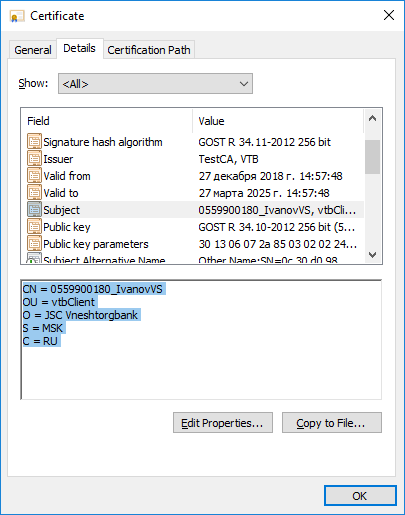
"secure" : "false",

"management\_mode" : ""

}

]

* Поле cert.id должно содержать уникальный идентификатор сертификата (GUID). Его можно получить в PowerShell, выполнив команду New-Guid;
* Поле cert.name должно содержать значения параметров Subject из сертификата.



Значение параметров необходимо указывать в поле name в порядке снизу вверх.

* Поле cert.serial должно содержать серийный номер сертификата;
* Перезапустить службу UPGBankAdapter\_username.

Для настройки подписи документов необходимо:

1. Открыть конфигурационный файл компонента DocSigner;
2. В массив banks добавить секцию для настройки банка ВТБ:

"banks" : [

{

“name" : "vtb",

"crypto" : {

"certificates" : [

]

}

}

]

1. В массив certificates добавляются установленные ранее сертификаты, предназначенные для подписи документов:

"certificates" : [

{

"id" : "5B6F72CD-1C16-4DF2-A374-BA5C4DA58DD7",

"name" : "RU, MSK, JSC Vneshtorgbank, vtbClient, 0559900180\_IvanovVS",

"serial" : "405017306a88126586bce35d5c24be3c"

}

]

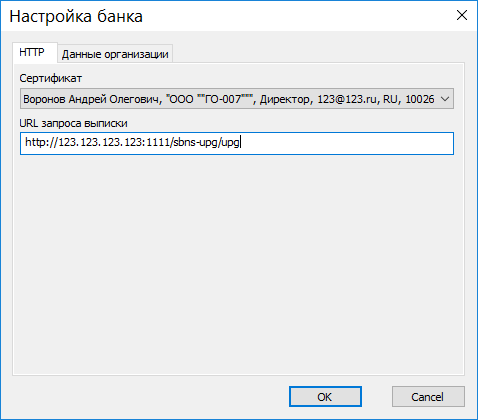
* Поле id должно содержать уникальный идентификатор сертификата (GUID). GUID можно получить в PowerShell, выполнив команду: New-Guid
* Поле name должно содержать значения параметров Subject из сертификата
* Поле cert.serial должно содержать серийный номер сертификата

1. После указания настроек служба компонента UPGDocSigner\_username должна быть перезапущена.

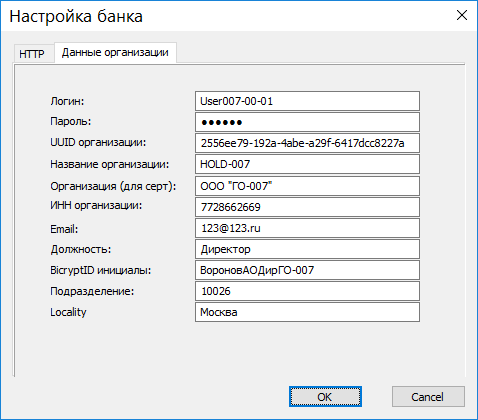
### Настройки для банка Сбербанк

Для настройки подключения к банку Сбербанк необходимо:

1. Открыть утилиту AAStatement;
2. Нажать на кнопку «Настройки» и выбрать банк «Сбербанк»;
3. Во вкладке «HTTP» выбрать установленный ранее транспортный сертификат и ввести URL-адрес для обращения к банку;



1. Во вкладке «Данные организации» указываются параметры, которые используются для генерации транспортного сертификата и авторизации у банка;



1. После указания настроек необходимо нажать на кнопку «OK» в окне «Настройка банка» и затем в окне «Настройка программы»;
2. Для работы функционала загрузки больших файлов (атачментов) для команды send-currency-op-info в конфигурационном файле компонента BankAdapter в секции настроек банка sberbank необходимо добавить URL-адрес сервера загрузки файлов (выделен желтым на примере)

"banks" : [

{

"bankdir" : "",

"outbox" : "",

"maxSimultaneousConnections" : 2,

"cert" : {

"id" : "3d542e2d-5757-4f69-8d55-06084a060b15",

"name" : "Молоко Анна Андреевна, \"ООО Компания\", Бухгалтер, maa@company.ru, RU, 10026, Москва",

"serial" : "77779ea3f2644b120cfa"

"name" : "sberbank",

"url" : "http://123.123.123.123:1111/sbns-upg/upg",

"url2" : "http://123.123.123.123:2222/sbns-app/",

"orgData" : "AQAAANCMnd8BFdERjHoAwE...",

"sender" : "",

"repeatingRequestsTimeout" : 1000

}

]

1. Перезапустить сервис компонента UPGBankAdapter\_username.

Настройка компонента DocSigner для подписи документов проходит аналогично настройке подписи для банка ВТБ, в массив banks добавляется секция для настройки банка Sberbank, затем в массив certificates добавляются необходимы сертификаты и уникальные идентификаторы:

"banks" : [

{

"name" : "sberbank",

"crypto" : {

"certificates" : [

{

"id" : "98833AB2-8BAF-4A9A-A121-52A238C92075",

"name" : "Воронов Андрей Олегович, \"ООО Компания\", Директор, vao@company.ru, RU, 10026, Москва",

"serial" : "1234567"

},

{

"id" : "C256F5F8-50EA-4A1A-9D30-8697A8EB9348",

"name" : "Молоко Анна Андреевна, \"ООО Компания\", Бухгалтер, maa@company.ru, RU, 26, Москва",

"serial" : "1234567"

}

]

}

}

]

После окончания настройки служба компонента UPGDocSigner\_username должна быть перезапущена.

### Настройки для банка Газпромбанк

Настройка банка Газпромбанк подразумевает под собой уже установленное и настроенное в соответствии с документацией клиентское программное обеспечение ICLTransportSystem (ITS), предоставляемое Газпромбанком.

Для настройки подключения к банку Газпромбанк необходимо:

1. Открыть конфигурационный файл компонента BankAdapter;
2. В параметре outdir указать желаемый путь до папки, в которой будут храниться документы, полученные из банка;
3. В массив banks добавить блок настроек банка Газпромбанк:

"outdir" : "C:\\gpb\_documents\\outdir",

"banks" : [

{

"bankdir" : "C:\\GPB\_CLNT\\SUBSYS\\ICL\\INBOX",

"outbox" : "C:\\GPB\_CLNT\\SUBSYS\\ICL\\OUTBOX",

"maxSimultaneousConnections" : 1000,

"certsubject" : "",

"name" : "gazprombank",

"url" : "",

"orgData" : "",

"sender" : "OrganisationID",

"repeatingRequestsTimeout" : 1000

}

]

* В поле bankdir указывается путь до каталога для приема данных от программы ITS;
* В поле outbox указывается путь до каталога для отсылки данных программе ITS;
* В поле name указывается имя банка (gazprombank);
* В поле sender указывается идентификатор отправителя.

1. После указания настроек перезапустить службу UPGBankAdapter\_username

Настройка компонента DocSigner для подписи документов проходит аналогично настройке подписи для банка ВТБ, в массив banks добавляется секция для настройки банка Gazprombank, затем в поле certificates добавляются необходимые сертификаты и уникальные идентификаторы:

"banks" : [

{

"name" : "gazprombank",

"crypto" : {

"certificates" : [

{

"id" : "70d2c65b-a4b4-4fab-8f5e-67496f2a50f1",

"name" : "1234567899999, 1234567899999, RU, Город Москва, Москва, \"ООО Компания\", Иванов Иван Иванович"

}

]

}

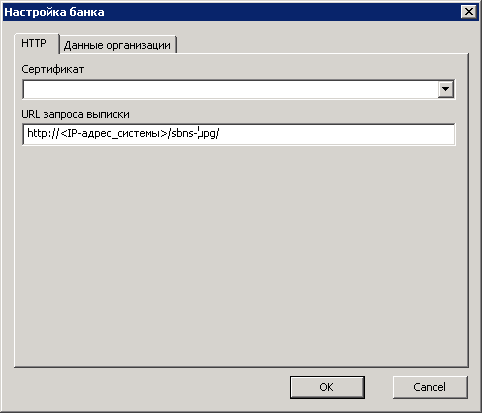
}

]

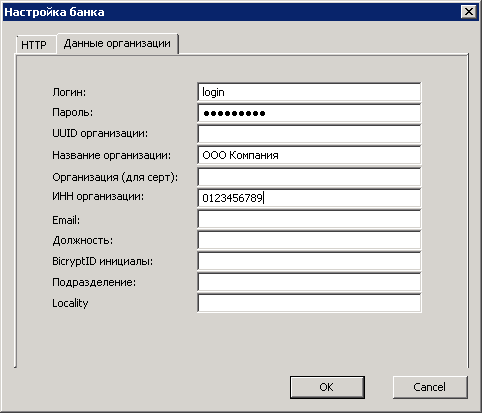
После окончания настройки служба компонента UPGDocSigner\_username должна быть перезапущена.

### Настройки для банка Банк Россия

1. Открыть утилиту AAStatement;
2. Нажать на кнопку Настройки и выбрать банк «Банк Россия»;
3. Во вкладке «HTTP» ввести URL-адрес для обращения к банку:



1. Во вкладке «Данные организации» указываются параметры, которые используются для авторизации у банка:



1. После указания настроек необходимо нажать на кнопку OK в окне «Настройка банка» и затем в окне «Настройка программы».

После окончания настройки служба компонента UPGBankAdapter\_username должна быть перезапущена.

### Настройки для банка Промсвязьбанк

Для настройки подключения к банку Промсвязьбанк необходимо:

1. Экспортировать открытую часть транспортного сертификата с токена в директорию, доступную компоненту BankAdapter.
2. Открыть конфигурационный файл компонента BankAdapter
3. В массив banks добавить секцию настроек банка Промсвязьбанк:

"banks" : [

{

"bankdir" : "",

"outbox" : "",

"maxSimultaneousConnections" : 0,

"version" : 0,

"cert" : {

"id" : "4e5e555a-54e7-4777-b896-e079c2cb2dbb",

"name" : "RU, Moscow, Promsvyazbank PJSC, PSB Corporate, Нейгебауэр Александр Юрьевич",

"serial" : "017203554303f4ff93ea11913e22b7d160"

},

"name" : "psb",

"url" : "https://corporate.psbank.ru",

"orgData" : "",

"sender" : "",

"repeatingRequestsTimeout" : 1000,

"waitingBankTimemout" : 30000,

"management\_mode" : "0",

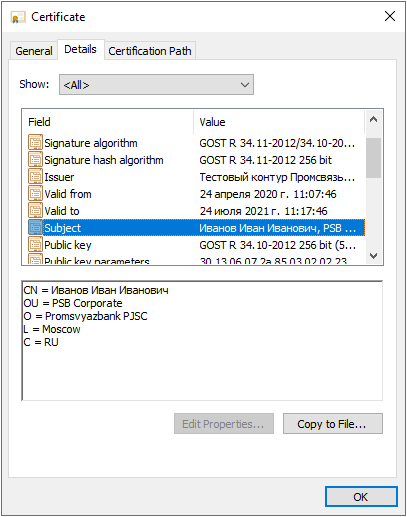
"certPath" : "C:\\cert\_path\\psb.cer"

}

]

* Поле cert.id должно содержать уникальный идентификатор сертификата (GUID). Его можно получить в PowerShell, выполнив команду New-Guid;
* Поле cert.name должно содержать значения параметров Subject из сертификата.

Значение параметров необходимо указывать в поле name в порядке снизу вверх.



* Поле cert.serial должно содержать серийный номер сертификата;
* Поле certPath должно содержать путь к открытой части сертификата, экспортированной на первом шаге.

Перезапустить службу UPGBankAdapter\_username.

### Настройки для банка Альфабанк

Для настройки подключения к банку Альфабанк необходимо:

1. Экспортировать открытую часть транспортного сертификата в формате Base64 в директорию, доступную компоненту BankAdapter;
2. Открыть конфигурационный файл компонента BankAdapter;
3. В массив banks добавить секцию настроек банка Альфабанк:

"banks": [

{

"bankdir": "",

"outbox": "",

"maxSimultaneousConnections": 1,

"version": 0,

"cert": {

"id": "4b8fb305-e39c-49a9-8394-fb5e1c4c9735",

"name": "IIvanov@org.ru, 65687654, 17394568, 1231399, Директор, Иванов Иван Иванович",

"serial": "017203554303f4ff93ea11913e22b7d160",

"path": "C:\\Users\\UPG\_SA\\AppData\\Local\\UPGBankAdapter\\certs\\alfabank.cer"

},

"name": "alfabank",

"url": "https://scf.alfabank.ru",

"orgData": "",

"sender": "",

"repeatingRequestsTimeout": 1000,

"waitingBankTimemout": 60000,

"connectionsTimeout": 60000,

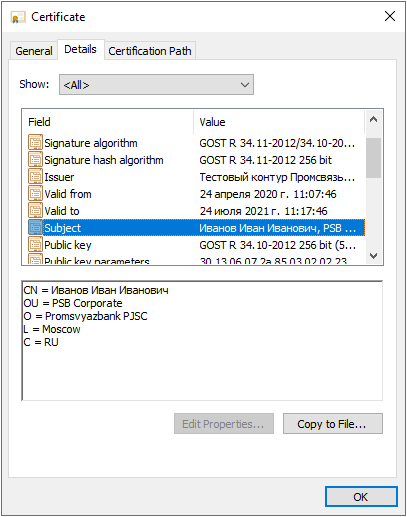
"management\_mode": "0"

}

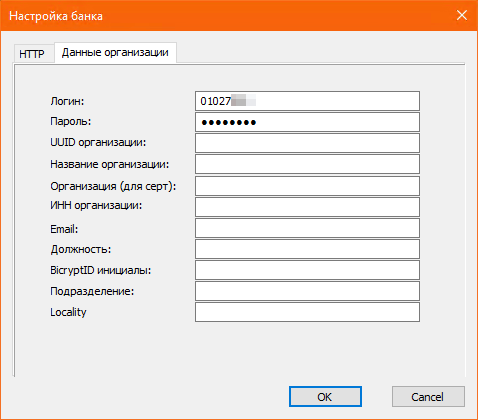
]

* Поле cert.id должно содержать уникальный идентификатор сертификата (GUID). Его можно получить в PowerShell, выполнив команду New-Guid;
* Поле cert.name должно содержать значения параметров Subject из сертификата.

Значение параметров необходимо указывать в поле name в порядке снизу вверх.



* Поле cert.serial должно содержать серийный номер сертификата;
* Поле cert.path должно содержать путь к открытой части сертификата, экспортированной на первом шаге.

1. Открыть утилиту AAStatement под пользователем, под которым исполняется служба компонента BankAdapter;
2. Нажать на кнопку Настройки и выбрать банк «Альфабанк»;
3. Во вкладке «Данные организации» указать параметры, которые используются для авторизации в банке – логин и пароль:  
   
4. После указания настроек необходимо нажать на кнопку OK в окне «Настройка банка» и затем в окне «Настройка программы» и кнопку «Закрыть» в основном окне утилиты.
5. После окончания настройки необходимо перезапустить службу UPGBankAdapter\_username

Для настройки подписи документов необходимо:

1. Открыть конфигурационный файл компонента DocSigner;
2. В поле banks добавить секцию для настройки банка Альфабанк:

"banks": [

{

“name": "alfabank",

"crypto": {

"certificates": [

]

}

}

]

1. В массив certificates добавляются установленные ранее сертификаты, предназначенные для подписи документов:

"certificates": [

{

"id": " 6635c1af-223e-4095-8945-9e75e859ecec",

"name": "PPetrov@org.ru, 65687654, 17394568, 1231399, Бухгалтер, Петров Пётр Петрович",

"serial" : "83f7eee9ad1fe4a044fb3593fe4505c5"

}

]

* Поле id должно содержать уникальный идентификатор сертификата (GUID). GUID можно получить в PowerShell, выполнив команду: New-Guid
* Поле name должно содержать значения параметров Subject из сертификата
* Поле cert.serial должно содержать серийный номер сертификата

1. После окончания настройки необходимо перезапустить службу UPGDocSigner\_username

### Настройки для банка Росбанк (H2H - собственное API банка)

Для настройки подключения к банку Росбанк с использованием канала H2H необходимо:

1. Открыть конфигурационный файл компонента BankAdapter;
2. В массив banks добавить секцию настроек банка Росбанк:

"banks": [

{

"version": 0,

"cert": {

"id": "4b8fb305-e39c-49a9-8394-fb5e1c4c9735",

"name": "Кефир Юлия Николаевна, ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ КАЗНАЧЕЙСКИЕ СИСТЕМЫ, 97834Y1211KYN",

"serial": "017203554303f4ff93ea11913e22b7d160",

"signType": "0"

},

"name": "rosbank",

"url": "https://www.bankline.ru/h2h/iso/H2HService",

"repeatingRequestsTimeout": 0,

"waitingBankTimemout": 60000,

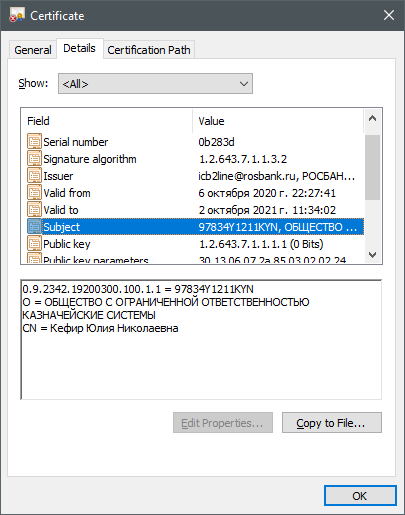
"connectionsTimeout": 30000

}

]

* Поле cert.id должно содержать уникальный идентификатор сертификата (GUID). Его можно получить в PowerShell, выполнив команду New-Guid;
* Поле cert.name должно содержать значения параметров Subject из сертификата.

Значение параметров необходимо указывать в поле name в порядке снизу вверх.



* Поле cert.serial должно содержать серийный номер сертификата;
* Поле cert.signType указывается в соответствии с типом сертификата, указанный в договоре. Возможные значения: 0 - подпись банка. 1 - подпись руководителя. 2 - подпись бухгалтера. 3 - подпись ст. сотрудника. 4 - подпись мл. сотрудника;

1. После окончания настройки необходимо перезапустить службу UPGBankAdapter\_username

### Настройки для банка Росбанк (1C.ДиректБанк)

Для настройки подключения к банку Росбанк с использованием канала 1С.ДиректБанк необходимо:

1. Открыть конфигурационный файл компонента BankAdapter;
2. В массив banks добавить секцию настроек банка Росбанк:

"banks": [

{

"apiVersion": "2.2.1",

"version": 0,

"maxSimultaneousConnections": 5,

"crypto": {

"certificates": [  
 {

"id": "4b8fb305-e39c-49a9-8394-fb5e1c4c9735",

"name": "Кефир Юлия Николаевна, ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ КАЗНАЧЕЙСКИЕ СИСТЕМЫ, 97834Y1211KYN",

"serial": "017203554303f4ff93ea11913e22b7d160"

}  
 ]  
 },

"name": "rosbank\_direct",

"url": "https://www.bankline.ru/1ctest/directbanktest",

"repeatingRequestsTimeout": 0,

"waitingBankTimemout": 60000,

"connectionsTimeout": 30000,

"secure": "true",

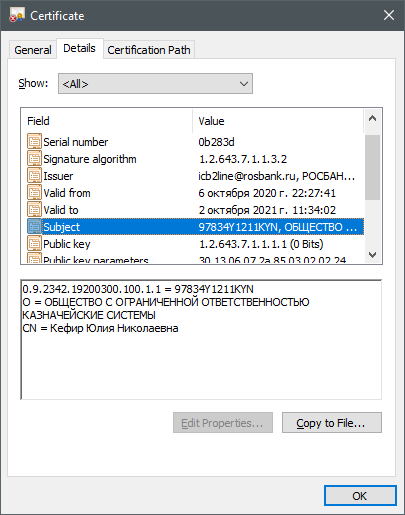
"serverUtcOffset": "+3:0"

}

]

* Поле cert.id должно содержать уникальный идентификатор сертификата (GUID). Его можно получить в PowerShell, выполнив команду New-Guid;
* Поле cert.name должно содержать значения параметров Subject из сертификата.

Значение параметров необходимо указывать в поле name в порядке снизу вверх.



* Поле cert.serial должно содержать серийный номер сертификата;

1. После окончания настройки необходимо перезапустить службу UPGBankAdapter\_username

### Настройки для банка Юникредит

Для настройки подключения к банку Юникредит с использованием канала SFTP необходимо:

1. Открыть конфигурационный файл компонента BankAdapter;
2. В массив banks добавить секцию настроек банка Юникредит:

"banks": [

{

"version": 0,

"name": "unicreditbank",

"url": "h2h.unicredit.ru",

"port": "22",

"bankdir": "/treasysrumm/imbkrumm",  
 "outbox": "/treasysrumm/treasysrumm",

"orgData": "AQAAANCMnd8...",

"maxSimultaneousConnections": 9,

"repeatingRequestsTimeout": 5000,

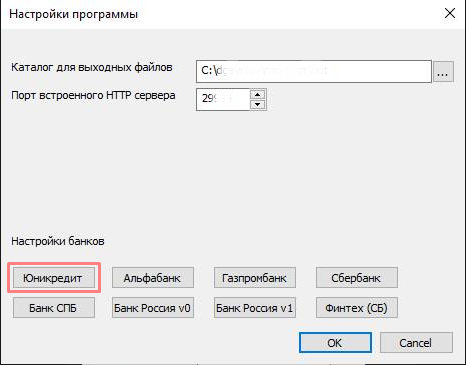
"waitingBankTimemout": 60000,

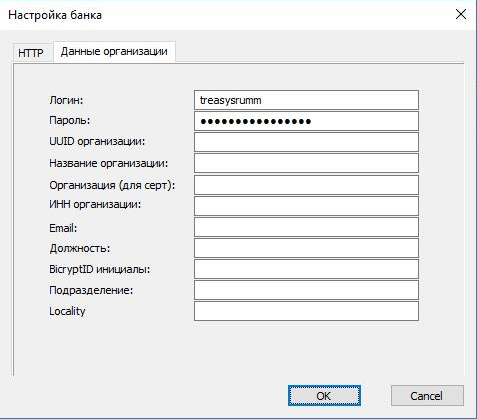
"connectionsTimeout": 30000,

}

]

* Поле url должно содержать адрес сервера банка;
* Поле port должно содержать порт сервера банка;
* Поле bankdir должно содержать путь к папке входящих документов банка;
* Поле outbox должно содержать путь к папке исходящих документов клиента;
* Поле maxSimultaneousConnections задаёт максимальное количество одновременных подключений к серверу банка.

1. Запустить AAStatement.exe под тем же пользователем, под которым исполняется сервис компонента BankAdapter и ввести логин и пароль пользователя зарегистрированного в банке в поля «логин» и «пароль» в окне настроек банка Юникредит:  
   



1. После окончания настройки необходимо перезапустить службу UPGBankAdapter\_username

Для настройки подписи документов необходимо:

1. Открыть конфигурационный файл компонента DocSigner;
2. В поле banks добавить секцию для настройки банка Юникредит:

"banks": [

{

“name": "unicreditbank",

"crypto": {

"certificates": [

]

}

}

]

1. В массив certificates добавляются установленные ранее сертификаты, предназначенные для подписи документов:

"certificates": [

{

"id": "98c9a169-3b87-498d-b458-907790df0c1b",

"name": "PPetrov@org.ru, 65687654, 17394568, 1231399, Бухгалтер, Петров Пётр Петрович",

"serial" : "83f7eee9ad1fe4a044fb3593fe4505c5"

}

]

* Поле id должно содержать уникальный идентификатор сертификата (GUID). GUID можно получить в PowerShell, выполнив команду: New-Guid
* Поле name должно содержать значения параметров Subject из сертификата
* Поле cert.serial должно содержать серийный номер сертификата

1. После окончания настройки необходимо перезапустить службу UPGDocSigner\_username