Краткое техническое описание системы «Corp.Bank»

(программный продукт «Универсальная платежная система корпораций»)

Москва

Оглавление

1. Термины и сокращения

Термин / Сокращение	Определение
Corp.Bank УПСК	Программно-Аппаратный Комплекс Универсальная Платежная Система Корпораций (ПАК УПСК), торговая марка Corp.Bank
КС	Казначейские Системы. Компания разработчик системы.
On-Premise	вариант размещения всех компонентов на стороне Клиента и прямое взаимодействие с Банками.
RMQ	компонент системы программный брокер сообщений, отвечающий за межкомпонентное взаимодействие на основе стандарта AMPQ
SP	компонент УПСК Сервис-провайдер.
BA	компонент УПСК Банк адаптер.
DS	компонент УПСК Компонент подписи.
DC	компонент УПСК Конвертер.
ЭЦП	электронно-цифровая подпись.
УС	учетная система, ERP система.
vCPU	виртуальный процессор.
RAM	оперативная память.
HDD	жесткий диск.
ОС	операционная система.
ПП	платежное поручение.

2. Общие сведения

УПСК (а также здесь и в дальнейшем Corp.Bank) 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, выбранная 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.

Для осуществления криптографических операций УПСК использует криптопровайдер, который требуется для работы с конкретным Банком. В настоящий момент полностью поддерживается криптопровайдер КриптоПро CSP. В тестовом режиме поддерживается криптопровайдер Бикрипт.

Компоненты системы взаимодействуют между собой с помощью программного брокера сообщений RabbitMQ на основе стандарта AMPQ.

Компоненты системы представляют из себя Windows-сервисы. Рабочие каталоги компонентов находятся в \Users\%username%\AppData\Local\ComponentName, где %username% имя учетной записи, под которой установлен и запущен компонент, а ComponentName наименование конкретного компонента.

Все компоненты сохраняют подробные журналы своей работы. Файлы журналов в формате .txt находятся в рабочих каталогах компонентов.

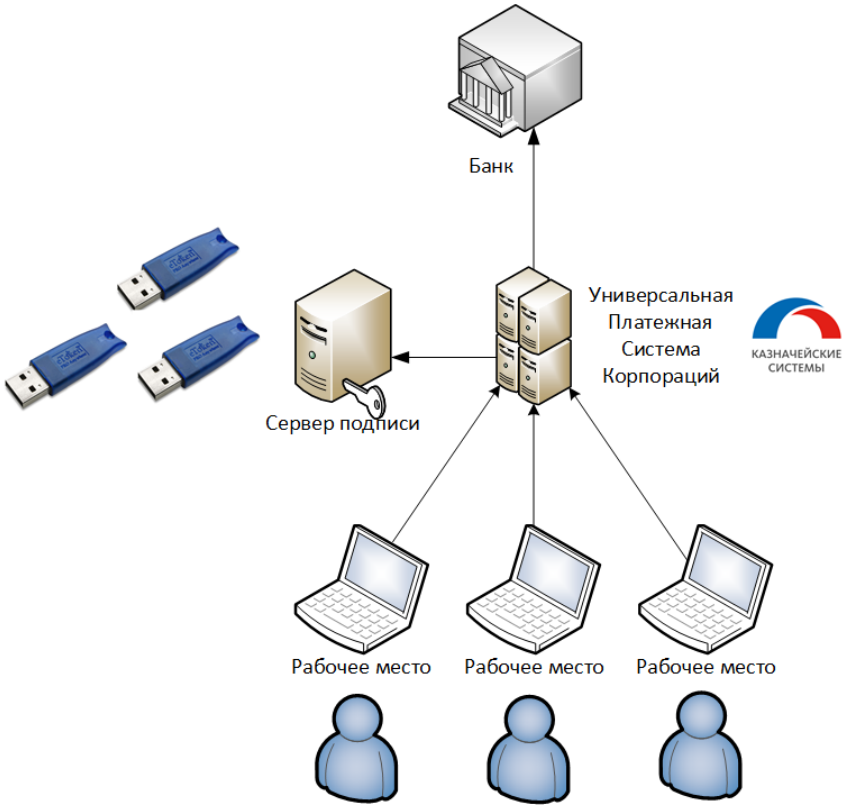
Встроенный веб-сервер компонента SP может работать как в режиме открытого (не шифрованного) трафика, так и в режиме HTTPS. Так же и межкомпонентное взаимодействие может быть открытым или использовать шифрование трафика AMPQ TLS.

Компоненты УПСК:

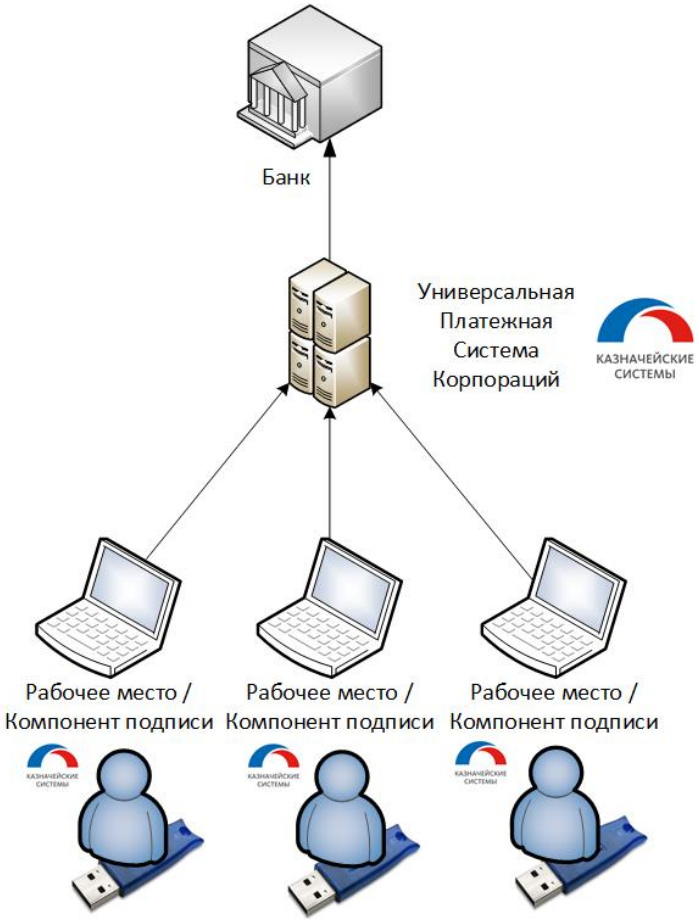
- Брокер (RMQ) – компонент системы, отвечающий за межкомпонентное взаимодействие на основе стандарта AMPQ. Является точкой входа и связующим звеном для компонентов SP, BA, DS и DC.
- Сервис-провайдер (SP) – точка входа для потребителей сервиса со стороны Клиента. Содержит встроенный веб-сервер. В настоящий 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 децентрализовано.

- Конвертер (DC) – компонент системы, осуществляющий конвертацию документа из единого формата, принятого для конкретной инсталляции, в формат целевого Банка.

2.1. Пример централизованного использования компонента подписи



2.2. Пример децентрализованного использования компонента подписи



3. Требования к оборудованию и среде

3.1. Требования к оборудованию

Конфигурация сервера или ПК для компонента системы – от **2x vCPU 2GHz**, от **2Gb 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 документ системой создается 250 Kb логов на всех компонентах системы.

3.2. 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 на 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, SP и BA были установлены на серверной версии ОС Windows. В случае децентрализованной конфигурации сервиса подписи, компоненты DS свободно могут быть установлены на десктопной версии ОС Windows.

Обязательное ПО:

- **КриптоПро CSP** версии 4.0 или 5.0. КриптоПро CSP должно быть установлено на серверах компонентов DS и BA.
- **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 SP
- **Erlang/OTP** версии 22.0. Должно быть установлено но одном сервере совместно с RabbitMQ.

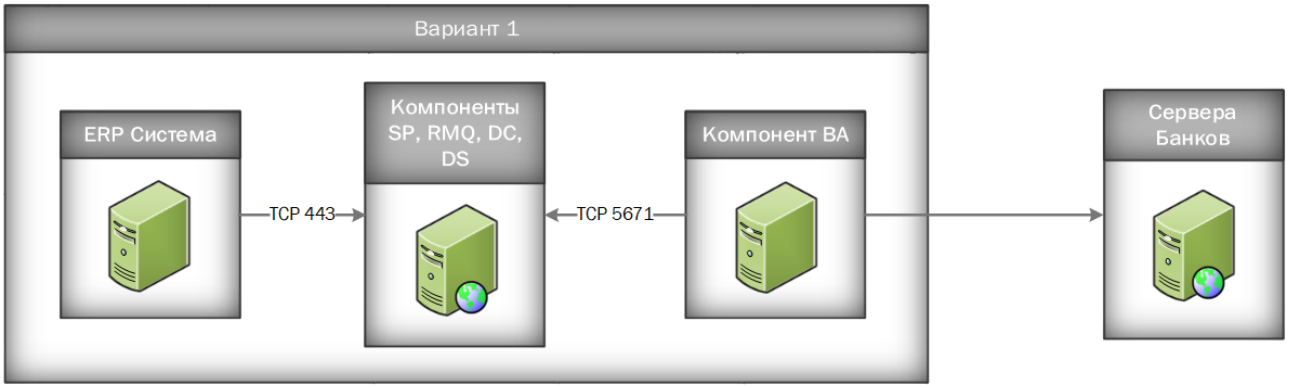
Опциональное ПО:

- **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 на SP.

4. Варианты размещения компонентов УПСК

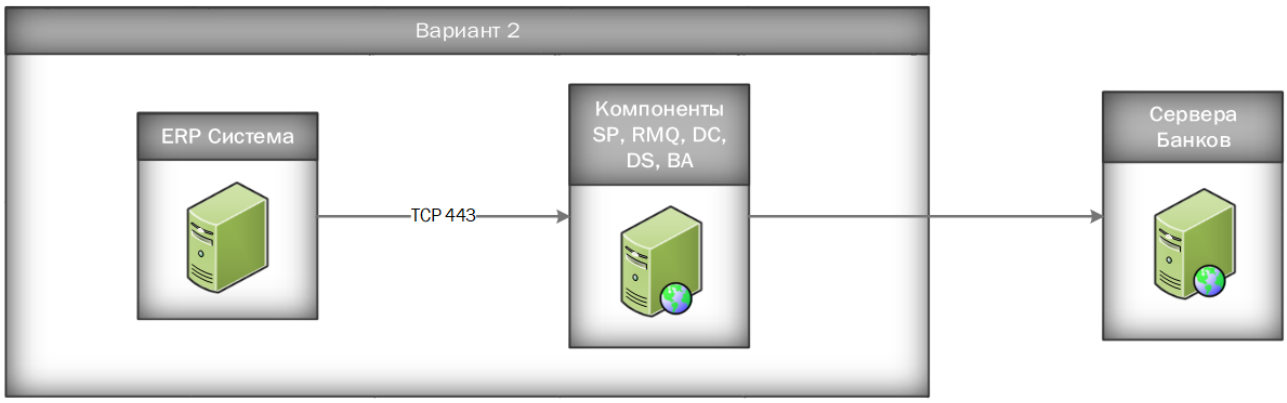
4.1. Вариант 1

Установка на отдельный сервер компонента BA и размещение его в DMZ зоне. Остальные компоненты SP, RMQ, 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.



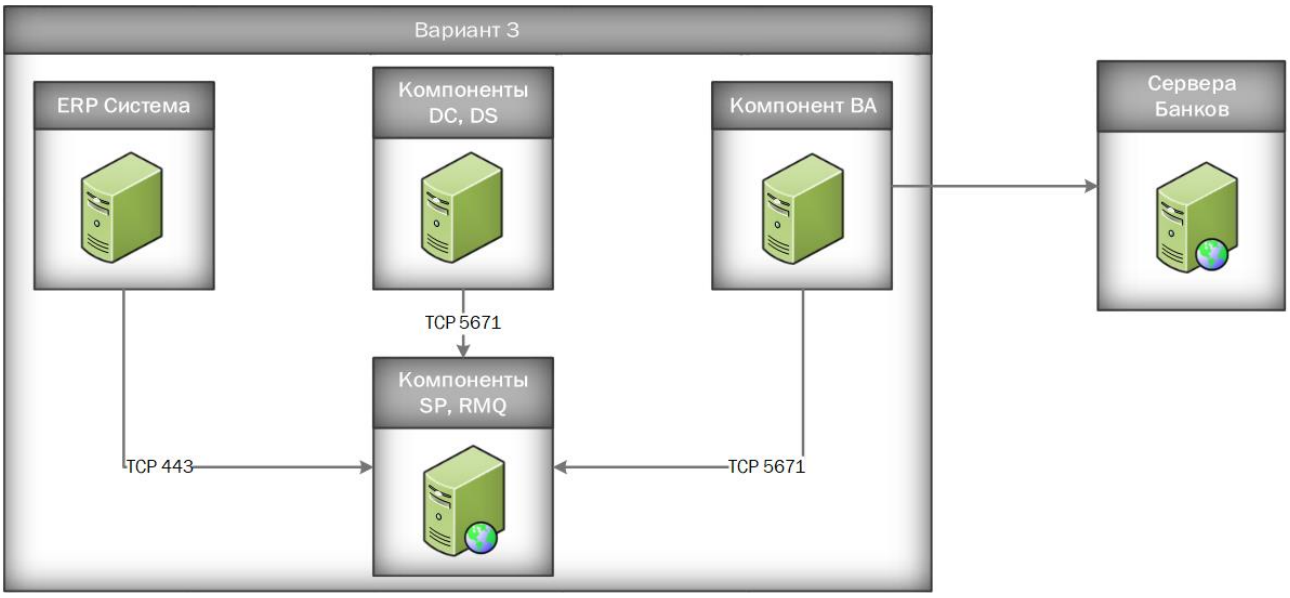
4.2. Вариант 2

Установка всех компонентов УПСК на один сервер. Вариант подходит в случае, когда нет необходимости разнесения компонентов системы на разные сервера. Такой вариант подходит, например, для тестового стенда УПСК.



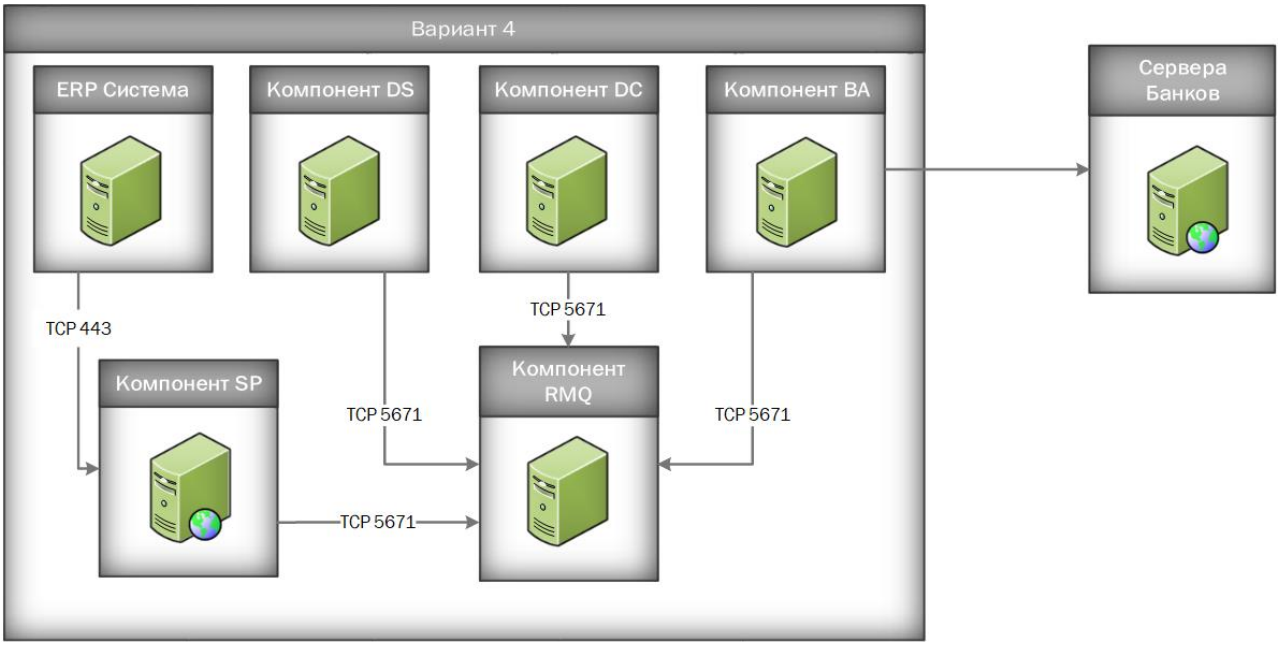
4.3. Вариант 3

Установка компонента BA на выделенный сервер и SP вместе с RMQ так же 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.



4.4. 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 компонента, являющегося точкой входа для потребителей сервиса, на отдельный сервер и установка компонента, обеспечивающего межкомпонентный обмен сообщениями, так же на выделенный сервер.



5. Описание процесса приема и отправки документов

У каждого компонента системы есть очередь на брокере сообщений RMQ, которую они постоянно мониторят на наличие в ней входящих сообщений.

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

5.1. Пример входящего документа

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

Шаги:

1. На веб-сервер компонента SP поступил 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.

5.2. Пример исходящего документа

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. На веб-сервер компонента SP поступил 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.
8. SP получает задачу из очереди и отдает обратное сообщение из Банка в ответ на АПИ-запрос.

6. Описание механизма подтверждения отправителя и ПК (внутренний антифрод)

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 антифрода может проверять документ, отправленный 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 антифрода был задействован, необходимо выпустить внутренний сертификат(ы), с помощью которого будут подписываться сообщения, отправляемые из УС в УПСК. Так же, если УПСК интегрируется с УС, которая полностью поддерживается Заказчиком самостоятельно, что специалисты Заказчика должны доработать механизм отправки документов в УПСК, включив в него все необходимые действия для поддержки внутреннего антифрода – составление внутреннего дайджеста документа, запрос системной информации о компонентах ПК и ее структурированное сохранение в отправляемом сообщение, подпись отправляемого запроса в УПСК внутренней ЭЦП, выпущенной для механизма антифрода.

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 антифрода.
5. УС подписывает блок единый дайджест механизма антифрода внутренней ЭЦП.
6. УС отправляет документ, содержащий в себе дополнительный блок данных внутреннего механизма антифрода в УПСК.
7. При поступление документа на компонент DS начинается процесс проверки блока данных внутреннего механизма антифрода.
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 антифрода.
11. Происходит верификация полученного подписанного от УС дайджеста и собранного на компоненте DS и открытой части сертификата.