Дополнительные вопросы к описанию реализации сервисов «обеспечение» и «кредитование»

1. Все взаимодействия с банками идут по SSL? Взаимная идентификация абонентов (ТП и Банка) производится (путем проверки сертификатов) до передачи данных? Какой алгоритм используется в SSL: зарубежный или ГОСТ (КриптоПро)?
2. Из описаний не ясно, какие операции выполняются автоматически (сугубо на программном уровне), а какие в ручном режиме (требуется действие оператора). В частности, это касается функций «Подтверждение зачисления денежных средств и изменение виртуального счета свободных средств участника», «Подтверждение заявки на возврат денежных средств и отправка в банк платежного поручения», «Отправка запроса на получение выписки по счету в банк», «Проверка квитования платежных поручений» (пп.5.5-5.8 раздела 1 «Постановка задачи»). Понятно, что сотрудник ТП (оператор-бухгалтер) вовлечен в технологический процесс, но вот границы - ?
   1. Операции, которые инициируются оператором:

* Подтверждение зачисления денежных средств (зачисление денежных средств на виртуальный счет)
* Обработка невыясненного платежа
* Отклонение платежа на возврат
* Отправка платежа на возврат средств участника (после подтверждения)
* Квитирование (нажатие кнопки «Получить выписку»)

b. Остальные операции идут в автоматическом режиме.

3. Раздел 2 (системная архитектура).

Так все-таки: добавлена одна БД «fabrikant\_payment» или несколько? Если одна, как она физически может находиться на двух серверах? Или «fabrikant\_payment» - это БД для организации процесса взаимодействия ТП и баз данных обеспечения и кредитования, которые (какие у них имена?) размещены на серверах tranchedb и loandb?

База одна, fabrikant\_payment, в которой хранится вся информация по обеспечению\кредитованию. Есть несколько полей, которые хранятся в основной базе fabrikant (таблицы auctions и tenders) и базах под новые процедуры (таблица lots), в которых хранится: сумма обеспечения, тип обеспечения и реквизиты организатора (если требуется).

Взаимодействие между OCSP и app именно такое, как показано на схеме: соединение может быть инициировано обеими сторонами? Или стрелками показан поток данных? Есть предложение придерживаться таких правил: если схема техническая (адреса, порты, протоколы), то стрелки показывают инициацию сетевых соединений, а если схема информационная (логическая), то стрелки показывают движение данных.

Не понимаю наличие связи по http (tcp-80) между внешним ресурсом (Солид-АСК) и внутренней базой данных (loandb). Если это поток данных, то см. выше, если прямое сетевое взаимодействие, то оно должно идти не напрямую, а через фронт-сервер (сервер-приложений). Также, вероятно, ошибка на схеме: связи между loandbr и loandb и tranchedb и tranchedbr не совпадают.

4. Программная архитектура

При постановке вопроса говорилось о необходимости таких сведений: «имена БД и таблиц, в которых хранится критичная для работы и безопасности сервиса информация, состав полей (с описанием), содержащих такую информацию». Это не сделано.

SHOW tables FROM fabrikant\_paymet;

SHOW columns FROM fabricant.auctions;

SHOW columns FROM fabricant.tenders;

Также не понимаю, почему на обоих серверах loandb и loandbr (tranchedb и tranchedbr) размещены БД и приложения. Если у “-r” серверов не просто роль хранения реплики БД, то получается, что у нас некий кластер. Тогда должно быть описано, как идет взаимодействие между ТП и внешней системой с точки зрения задействования “-r” серверов (они всегда участвуют в обмене, в случае отказа основного сервера, еще как-то? Как синхронизируются данные в БД? И т.д.).

5. В разделе «Схема информационных потоков» нет описания сервиса кредитования, а приведенная схема является частной (только для Альфа-Банка) для сервиса обеспечения.

6. В разделе 6 (Укрупненный алгоритм (блок-схема) работы сервисов) ожидалось увидеть блок-схему (или текстовое описание) алгоритма работы кода (собственно, «бизнес-логика», как она названа в п.6.2), а не схему связей компонентов (ей самое место в разделе 2). К тому же на схеме нет легенды, поэтому не ясно отличие черных стрелок от белых.

Не ясно, бизнес-логика какого сервиса описана в разделе 6.2. Если это схема «обеспечения», то где схема «кредитования»? На схеме нет легенды, поэтому не ясны отличия компонентов разного цвета. С точки зрения полноты также не все хорошо, так как хотелось видеть не только бизнес-логику, но и часть программной логики (как осуществляются проверки и контроли). Сейчас эти процедуры либо не указаны, либо являются «черными ящиками».

На совместных совещаниях рассматривали усложненные ситуации, когда деньги приходят с нескольких счетов, могут возвращаться по-разному, проблемные ситуации (невозможность возврата на начальный счет). Все это не описано.

7. Раздел 7 (применение ЭП и шифрования) тоже описан поверхностно. Как минимум, не ясно, где работа идет вручную, а где автоматически. Например, проверку ЭП наверняка можно делать автоматически и показывать оператору в интерфейсе уже результат. Термин «применяется» не дает понимания, как конкретно это происходит, т.к. какой набор данных (файлов, посылок и т.п.) подписывается и проверяется.

Говорится про шифрование (SSL) только с Альфа-Банком. Означает ли это, что взаимодействие с Солидом происходит без шифрования?

Про применение ЭП на стыке ТП-Банк не говорится.

Очень важно понимать, какие данные в БД хранятся с ЭП, а какие – без. Т.е. если перед обработкой у нас был подписанный ЭП пакет данных, то после его обработки данные, вероятно, кладутся в БД в «очищенном» виде (без подписи, хэша и т.п.)? Сохранятся ли при этом первоначальный пакет, который был с ЭП? Где он сохраняется?

Это все вопросы к уровню детализации описания.

8. В разделе 8 (Описание точек обеспечения конфиденциальности и целостности критичных данных) не ясно, что означает «Целостность виртуальных средств обеспечивается очередью».

Очередь обеспечивает последовательное выполнение всех операций. Целостность также обеспечивается созданием субсчетов для виртуальных счетов пользователей (контроль осуществляется сверками по различным разрезам счетов (Свободные средства\Организация\Площадка, Заблокированные средства\Организация, Заблокированные средства\Организация\Процедура и т.п.)

Не говорится о целостности информации о принимаемых ТП средствах.

И хоть где-то хочется увидеть короткое, но полное описание, где у нас **виртуальные деньги, а где реальные**. Например, в файле «Солид.pdf» есть блок «Оператор СОЛИД-АСК перечисляет денежные средства на счет клиента в системе ТП.» Что за счет клиента в системе ТП? На ТП же только виртуальные деньги? Или речь идет о том, что реальные деньги перемещаются со счета клиента в Банке1 на счет ТП в Банке2?

Реальные средства хранятся на счету ТП в банке. В рамках площадки оперируем мы исключительно виртуальными средствами. Информация о реальных средствах хранится в платежах.