# ТЕХНИЧЕСКОЕ ЗАДАНИЕ

**Наименование Системы:** **Веб-приложение для работы с сервисами Цифровых документов**

**Назначение:** Веб-приложение предназначено для работы с Цифровыми документами и идентификации клиентов.

**Цель:** Обеспечить безопасный и эффективный способ проверки персональных данных, а также выполнения процедур идентификации.

1. **Требования к платформе:**

 1. Разработать и установить на сервера банка платформу позволяющую производить интеграцию с государственными органами через шлюз SmartBridge:

 1) Платформа должна содержать интеграционный модуль и/или набор микросервисов с поддержкой форматов обмена SOAP, RPC-JSON, RPC-XML в виде сервисов, разработанных для возможности интеграции с информационными системами банка и SmartBridge;

 2) Логирование событий интеграционной платформы в соответствии с Едиными требованиями в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденными постановлением Правительства Республики Казахстан от 20 декабря 2016 года №832 (далее - ЕТ);

 3) Мониторинг работы платформы в соответствии сЕТ;

 4) Функционал интеграции со SmartBridge в части сервисов Цифровых документов, ГБД ФЛ\ЮЛ в том числе КДП;

 5) Необходимо, чтобы все конфиденциальные и персональные данные, получаемые в результате работы сервисов не сохранялись в хранилище, в том числе Базе данных, кэш, файлы и другие виды хранения данных **Требования к веб-приложению:**

Система будет являться частью интеграционной платформы для взаимодействия с сервисами Государственных органов (далее ГО), предназначена для отправки и получения запросов на электронный шлюз SmartBridge в части сервисов Цифровых документов физических лиц. Необходима интеграция со следующими сервисами SmartBridge:

- Сервис "Цифровые документы" по поиску сгенерированного документа - DL\_DocSearch;

- Сервис "Цифровые документы" DigitalDocuments;

- Сервис для предоставления удаленного доступа к цифровым документам через ОТП - DL\_Online\_Access;

- Сервис контроля доступа к персональным данным - KDP\_SERVICE;

- Прочие сервисы необходимые для работы «Цифровых документов».

Рисунок 2. Концептуальная схема веб-приложения и интеграция с сервисами ГО.

**СТРУКТУРА СИСТЕМЫ**

1. **ADMIN** – Административный модуль**;**
2. **ARM** – Рабочее место Менеджера Банка;
3. **Dictionaries** - Справочники;
4. **Logs**  - Сбор логов;
5. **Monitoring** – Мониторинг состояния системы;
6. **Integrations** - Интеграционный модуль;
7. **ECP** – Модуль работы с ЭЦП.

**ADMIN – АДМИНИСТРАТИВНЫЙ МОДУЛЬ**

Административный модуль предназначен для пользовательского администрирования системы. Доступ только у пользователей с ролью – Администратор, у остальных ролей – этот модуль не отображается.

Данные пользователей «Администрирование> Пользователи» отображать в табличном виде (колонки ID, Login, Name, Department, Roles, Status), в таблице активные пользователей подсвечивать зеленым, заблокированных – красным, как в примере ниже. Добавить сортировку по active и blocked пользователям. По умолчанию отображать active пользователей.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Login | Name | Department | Roles | Status |
| 1 | ……. | ……. | IT | Admin | Active |
| 2 | ……. | ……. | IT | Admin | Blocked |

 Функционал, доступный Администратору:

* Добавление пользователя;
* Редактирование существующего пользователя;
* Блокирование пользователя;

Необходима интеграция с Active Directory. Каждая таблица должна иметь таблицу аудита, для отслеживания изменений в системе, кем изменение было внесено, когда и что было заменено. Технический аудит по таблицам. Отображать создание записи. Таблицы аудита должна вестись в базе данных.

Роли:

1. **Admin.** Имеет полный доступ к модулю ADMIN;
2. **Manager.** Имеет доступ на модули: Dictionaries - Справочники; ARM – Рабочее место менеджера;
3. **Operator.** Имеет доступ на модули: ARM – Рабочее место менеджера;
4. **IB -** специалист, обеспечивающий информационную безопасность в Банке.

**ARM – Рабочее место Менеджера Банка**

Рабочее место Менеджера Банка предназначено для работы менеджера Банка и позволяет просматривать модуль Справочники и работать с сервисами Цифровых документов. Процесс получения Цифровых документов можно разделить на несколько методов:

1. Получение «Цифрового документа» через сервис 1414 в виде СМС на мобильный телефон, привязанный через БМГ (База мобильных граждан).
2. Получение «Цифрового документа» через сервис KDP и код документа из мобильного приложения egov mobile.

**Процесс получения «Цифрового документа» по методу 1:**

1. Сотрудник Банка заведенный в Active Directory и в системе с ролью «Менеджер» проходит аутентификацию по логину и паролю в модуль «ARM».



1. После успешного входа в ARM, пользователь в левой боковой меню выбирает пункт «Цифровые документы», после чего выбирает «Получение ЦД через 1414».
2. Открывается окно.



Рисунок 3. Окно «АРМ Менеджер».

1. Менеджер запрашивает у Клиента ИИН для подтверждения, после чего вводит ИИН.

Для поля ИИН должна быть настроена валидация:

* Длина значения ИИН 12 символов;
* Типа данных – Числовой;
* Проверять значение ИИН на алгоритм ИИН/БИН.
1. После чего, в модуле ARM формируется запрос на получение документа «Удостоверение личности» (из справочника **DocType) через интеграционный модуль в сервис** предоставления удаленного доступа к цифровым документам через ОТП - DL\_Online\_Access.
2. После чего на мобильный телефон Клиента, должен прийти код подтверждения, Менеджер вводит код в поле «Код SMS».
3. В случае если код корректный, в окне ARM открывается цифровой документ в виде изображения и реквизиты документа.
4. Менеджер производит визуальное сравнение и закрывает окно через кнопку «Закрыть».

**Процесс получения «Цифрового документа» по методу 2:**

1. Сотрудник Банка заведенный в Active Directory и в системе с ролью «Менеджер» проходит аутентификацию по логину и паролю в модуль «ARM».



1. После успешного входа в ARM, пользователь в левой боковой меню выбирает пункт «Цифровые документы», после чего выбирает «Получение ЦД через egov».
2. Открывается окно.



Рисунок 4. Окно «АРМ Менеджер».

1. Менеджер запрашивает у Клиента ИИН для подтверждения, после чего вводит ИИН.

На поле ИИН должна быть валидация:

* Длина значения ИИН 12 символов;
* Типа данных – Числовой;
* Проверять значение ИИН на алгоритм ИИН/БИН.
1. После чего, в модуле ARM формируется запрос на получение согласия «Удостоверение личности» (из справочника **DocType) через интеграционный модуль** Сервис контроля доступа к персональным данным - KDP\_SERVICE**.**
2. **После успешного получения токена от сервиса KDP, интеграционный модуль взывает сервис** предоставления удаленного доступа к цифровым документам через - DigitalDocuments.
3. После чего Клиент вызывает в мобильном приложении egov mobile в разделе Цифровые документ – Удостоверение личности кнопку «Предъявить документ» и диктует менеджеру 6-значный код. Менеджер вводит код в поле «Код».
4. В случае если код корректный, в окне ARM открывается цифровой документ в виде изображения и реквизиты документа.
5. Менеджер производит визуальное сравнение и закрывает окно через кнопку «Закрыть».

**Logs** - **Сбор логов**

Модуль сбора логов позволяет хранить централизованно логи работы приложения и сервисов, а также осуществлять просмотр логов и поиск по контексту. Формат сбора и отображения логов должен соответствовать требования информационной безопасности перечисленных в приложенном файле – check-list-fib-rus.pdf.

**Monitoring –** **Мониторинг состояния системы**

Модуль мониторинг состояния системы позволяет получить состояние системы и отдельных модулей в виде удобных графиков и дашбордов.

**Integrations - Интеграционный модуль**

Интеграционный модуль представляется собой прослойку для работы с внешними сервисами и сервисами ГО. В том числе позволяет использовать сервис в виде удобного API на базе SOAP/RPC JSON протоколов, при этом скрывая реализацию работы с транспортной и другими электронными подписями. Модуль поддерживает методы проверки работы для мониторинга системы и централизованного логирования процессов интеграции.

**ECP – Модуль работы с ЭЦП.**

Модуль позволяет использовать с ЭЦП НУЦ РК.

**DICTIONARIES – Справочники**

Модуль справочники предназначен для хранения актуальной информации. Любой набор справочников представлен в табличном виде. В верхней панели необходимы кнопки добавления, редактирования, удаления, поиск и обновления датасета

**DocType – типы цифровых документов:**

**Данные будут интегрироваться со внешней системы.** Параметры в справочнике:

|  |  |  |
| --- | --- | --- |
| Name | Type | Description |
| ID | Number(10) | уникальный номер контракта |
| Code | VARCHAR2(20) | код документа |
| Name | VARCHAR2(200) | Наименование документа (Рус.) |
| Name\_Kz | VARCHAR2(200) | Наименование документа (Каз.) |



Рисунок 5. Схема сети передачи данных.

**Основным сетевым узлом** является сервер PfSense (виртуальная машина), который выполняет функцию маршрутизатора, межсетевого экрана и основного шлюза, а также разделяет сеть на следующие VLAN’ны:

1. Интернет (включающая в себя VPN каналы до ВШЭП и до резервного ЦОДа)
2. DMZ – зона, содержащая сервер приложений.
3. Защищенная внутренняя сеть – содержит сервер базы данных, сервер логирования и сервер мониторинга, доступы в данную сеть организованы только для сервера приложений на вход, и на выход для серверов логирования и мониторинга.

Подключение основного узла системы к ВШЭП осуществляется через SSL VPN канал, организованный посредством SmartBridge.

**Резервный узел** защищается межсетевым экраном PfSense. Серверы находятся в двух раздельных подсетях, взаимодействие между которыми осуществляется через межсетевой экран. Связь резервного и основного узла осуществляется по оVPN.

Взаимодействие основного и резервного серверов баз данных осуществляется через VPN канал, так же организован доступ по заданным портам для сервера мониторинга.

**Не функциональные требования:**

 1) Приложение должно быть разработано на современном фреймворке (React, Angular, Vue и др.);

 2) Приложение поддерживает аутентификацию и авторизацию на базе интеграции с Active Directory;

 3) Необходимо, чтобы все конфиденциальные и персональные данные получаемые в результате работы веб-приложения не сохранялись в хранилище, в том числе Базе данных, кэш, файлы и другие виды хранения данных;

 4) Исполнитель обязуется передать исходные коде и скрипты сборки проекта.

 5) Исполнитель должен обеспечить настройки всех процессов обеспечения информационной безопасности перед прохождением испытаний на соответствие требованиям информационной безопасности в аккредитованной испытательной лаборатории в соответствии с Законом Республики Казахстан от 24 ноября 2015 года «Об информатизации», Методикой и правилами проведения испытаний объектов информатизации «электронного правительства» и информационных систем, отнесенных к критически важным объектам информационно-коммуникационной инфраструктуры, утвержденной приказом Министра цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан от 3 июня 2019 года №111/НҚ и ЕТ. В случае выявления несоответствий Исполнитель должен в течении 20 рабочих дней внести исправления и обеспечить повторное успешное прохождение испытания.

6) Возможность в приложении организовать группы доступов с возможностью предоставлять пользователям ограниченный или полный функционал системы.

**Требования к коммерческому предложению:**

1. Стоимость разработки, развертывания, инсталляции и настройки интеграционной платформы в тенге включая налоговые и прочие отчисления в бюджет РК.

2. Стоимость лицензий в тенге включая налоговые и прочие отчисления.

3. График внедрения(этапы) как сквозной процесс: внедрение ПО, аттестация, документирование с зонами ответственности между банком и компанией.

**Требования к документированию**

1. Перечень и описание интеграции с другими системами.
2. Описание инфраструктуры (тестовой, предпрод, прод)
3. Техническая инструкция с перечнем информации, хранящейся в БД (описание таблиц, связей, настроек, процессов интеграции в части описания сервисов с параметрами, процессов логирования и др.).
4. Архитектурная схема/Схема сервиса (для продуктивных стендов и для тестовых стендов с полным перечнем: серверы, порты, протоколы, потоки данных).
5. Список ПО используемого в сервисе (именование, версии)
6. Инструкция для администраторов приложений (администрирования модуля, заведения пользователей, определения прав, изменения настроек и т.д.).
7. Список компонентов, подлежащих мониторингу
8. Инструкция пользователя (которая будет содержать описание всей функциональности системы с приведенными скринами). Обязательный документ к заявке
9. Процедура (инструкция) аварийного восстановления сервиса и его компонент
10. Отчет о проведенном нагрузочном тестировании
11. список разработанных интеграционных сервисов и примеры как их можно вызвать из других систем.

**Гарантийная поддержка**

1. Наличие гарантийной поддержки от поставщика 90 дней после подписания акта выполненных работ и ввода системы в эксплуатацию.

**Требования к инфраструктуре**

1. В качестве платформы сервиса должна использоваться ОС Centos версии не ниже 7.9
2. Если в решении предполагается наличие БД — это должен быть PostgreSQL не ниже версии 14
3. Решение должно быть отказоустойчивым в части платформы (предусмотрено дублирование серверов)