**ТЕХНИКАЛЫҚ ТАПСЫРМА**

**Жүйе атауы:** **Цифрлық құжаттардың сервистерімен жұмыс істеуге арналған веб-қосымша**

**Нысаны:** Веб-қосымша цифрлық құжаттармен жұмыс істеуге және клиенттерді анықтауға арналған.

**Мақсаты:** Жеке деректерді тексерудің қауіпсіз және тиімді әдісін, сондай-ақ сәйкестендіру процедураларын орындауды қамтамасыз ету.

1. **Платформаға қойылатын талаптар:**

 1. SmartBridge шлюзі арқылы мемлекеттік органдармен интеграцияға мүмкіндік беретін платформаны банк серверлеріне әзірлеу және орнату:

 1) Платформада SOAP, RPC-JSON, RPC-XML алмасу пішімдерін қолдауы бар интеграциялық модуль және/немесе микросервистердің жиынтығы банктік ақпараттық жүйелермен және SmartBridge-мен интеграцияға арналған қызметтер түрінде болуы керек;

 2) Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысымен бекітілген Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарға сәйкес интеграциялық алаң оқиғаларын тіркеу (бұдан әрі - БТ);

 3) БТ сәйкес платформаның жұмысын бақылау;

 4) Цифрлық құжаттар қызметтері, ГБД ФЛ\ЮЛ, соның ішінде КДП тұрғысынан SmartBridge-пен интеграцияның функционалдығы;

 5) Қызметтер нәтижесінде алынған барлық құпия және жеке деректер деректер базасын, кэшті, файлдарды және деректерді сақтаудың басқа түрлерін қоса алғанда, сақтауда сақталмауы керек.

**Веб-қосымшаға қойылатын талаптар:**

Жүйе жеке тұлғалардың цифрлық құжаттарының қызметтеріне қатысты SmartBridge электрондық шлюзіне сұраныстарды жіберуге және қабылдауға арналған мемлекеттік органдардың (бұдан әрі - МO) қызметтерімен өзара әрекеттесуге арналған интеграциялық платформаның бөлігі болады. Келесі SmartBridge қызметтерімен біріктіруді қажет етеді:

- Жасалған құжатты іздеуге арналған «Цифрлық құжаттар» қызметі - DL\_DocSearch;

- "Цифрлық құжаттар" қызметі DigitalDocuments;

- OTП арқылы цифрлық құжаттарға қашықтан қол жеткізуді қамтамасыз ету қызметі - DL\_Online\_Access;

- Жеке деректерге қол жеткізуді бақылау қызметі - KDP\_SERVICE;

- «Цифрлық құжаттардың» жұмысына қажетті басқа қызметтер.

2 сурет. Веб-қосымшаның тұжырымдамалық сұлбасы және МО қызметтерімен интеграция

**ЖҮЙЕ ҚҰРЫЛЫМЫ**

1. **ADMIN** – Әкімшілік модуль**;**
2. **ARM** – Банк менеджерінің жұмыс орны;
3. **Dictionaries** - Анықтамалар;
4. **Logs**  - Логтарды жинау;
5. **Monitoring** – Жүйе денсаулығын бақылау;
6. **Integrations** - Интеграциялық модуль;
7. **ECP** – ЭЦҚ-мен жұмыс істеу модулі.

**ADMIN – ӘКІМШІЛІК МОДУЛЬ**

Әкімшілік модуль жүйені пайдаланушы әкімшілігіне арналған. Қатынас тек Әкімші рөлі бар пайдаланушылар үшін қолжетімді, басқа рөлдер үшін бұл модуль көрсетілмейді.

Қолданушы деректері «Басқару>Пайдаланушылар» кесте пішінінде (ID бағандар, Login, Name, Department, Roles, Status) көрсетіледі, кестеде белсенді пайдаланушылар жасыл түспен, блокталған пайдаланушылар төмендегі мысалдағыдай қызыл түспен белгіленген. Белсенді және блокталған пайдаланушылар бойынша сұрыптауды қосыңыз. Әдепкі бойынша белсенді пайдаланушыларды көрсету.

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

Әкімшіге қолжетімді функционал:

* • Пайдаланушыны қосу;
* • Бар пайдаланушыны өңдеу;
* • Пайдаланушыны блоктау;

Active Directory интеграциясы қажет. Әрбір кестеде жүйедегі өзгерістерді, өзгертуді кім енгізгенін, қашан және нені ауыстырғанын бақылау үшін аудит кестесі болуы керек. Кестелер бойынша техникалық аудит. Жазбаның жасалуын көрсету. Аудит кестелері дерекқорда сақталуы керек.

Рөлдері:

1. **Admin.** ADMIN модуліне толық рұқсаты бар;
2. **Manager.** Модульдерге рұқсаты бар: Dictionaries – Анықтамалар; ARM – менеджердің жұмыс орны;
3. **Operator.** Модульдерге рұқсаты бар: ARM – менеджердің жұмыс орны;
4. **IB -** Банкте ақпараттық қауіпсіздікті қамтамасыз ететін маман.

**ARM – Банк менеджердің жұмыс орны**

Банк менеджерінің жұмыс орны Банк менеджерінің жұмысына арналған және Анықтамалық модулін көруге және цифрлық құжат қызметтерімен жұмыс істеуге мүмкіндік береді. Цифрлық құжаттарды алу процесін бірнеше әдістерге бөлуге болады:

1. МАБ (Мобильді азаматтардың мәліметтер базасы) арқылы қосылған ұялы телефонға 1414 қызметі арқылы «Цифрлық құжатты» СМС түрінде алу.
2. КДП қызметі арқылы «Цифрлық құжатты» және egov мобильді қосымшасынан құжат кодын алу.

**1-әдіс бойынша «Цифрлық құжатты» алу процесі:**

1. Active Directory-де және жүйеде «Менеджер» рөлімен тіркелген Банк қызметкері «ARM» модулінде логин мен пароль арқылы аутентификацияланады.



1. ARM жүйесіне сәтті кіргеннен кейін, пайдаланушы сол жақ мәзірден «Цифрлық құжаттар» тармағын таңдап, одан кейін «1414 арқылы ЦҚ қабылдау» опциясын таңдайды.
2. Терезе ашылады.



3 сурет. «АРМ Менеджер» терезесі.

1. Менеджер растау үшін Клиенттің ЖСН-ін сұрайды, содан кейін ол ЖСН енгізеді.

ЖСН өрісі үшін валидация орнатылған болуы тиіс:

* - ЖСН мәнінің ұзындығы 12 таңбаны құрайды;
* - Деректер түрі – Сандық;
* - ЖСН мәнін ЖСН/БСН алгоритміне сәйкес тексеріңіз.
1. Осыдан кейін ARM модулінде OTP - DL\_Online\_Access арқылы цифрлық құжаттарға қашықтан қол жеткізуді қамтамасыз ету қызметіне біріктіру модулі арқылы «Жеке куәлік» құжатын (DocType анықтамасынан) алуға сұраныс қалыптастырылады.
2. Осыдан кейін клиенттің ұялы телефонына растау коды жіберіледі, Менеджер кодты «SMS коды» өрісіне енгізеді.
3. Егер код дұрыс болса, ARM терезесінде сурет пен құжат мәліметтері түріндегі цифрлық құжат ашылады.
4. Менеджер визуалды салыстыруды жүргізеді және «Жабу» батырмасы арқылы терезені жабады.

**2-әдіс бойынша «Цифрлық құжатты» алу процесі:**

1. Active Directory-де және жүйеде «Менеджер» рөлімен тіркелген Банк қызметкері «ARM» модулінде логин мен пароль арқылы аутентификацияланады.



1. ARM жүйесіне сәтті кіргеннен кейін пайдаланушы сол жақтағы мәзірден «Цифрлық құжаттар» тармағын таңдап, одан кейін «egov арқылы ЦҚ қабылдауды» таңдайды».
2. Терезе ашылады.



4 сурет. «АРМ Менеджер» терезесі.

1. Менеджер растау үшін Клиенттің ЖСН-ін сұрайды, содан кейін ол ЖСН-ді енгізеді.

ЖСН өрісі үшін валидация орнатылған болуы тиіс:

* ЖСН мәнінің ұзындығы 12 таңбаны құрайды;
* Деректер түрі – Сандық;
* ЖСН мәнін ЖСН/БСН алгоритміне сәйкес тексеріңіз
1. Осыдан кейін ARM модулінде жеке деректерге қол жеткізуді басқару қызметі - KDP\_SERVICE интеграциялық модулі арқылы «Жеке куәлік» (DocType анықтамасынан) келісім алуға сұраныс жасалады**.**
2. **KDP қызметінен белгіні сәтті алғаннан кейін интеграциялық модуль - DigitalDocuments арқылы цифрлық құжаттарға қашықтан қол жеткізуді қамтамасыз ету қызметін шақырады**.
3. Осыдан кейін Клиент «Цифрлық құжат – жеке куәлік» бөліміндегі egov мобильді қосымшасындағы «Құжатты көрсету» батырмасын басады және менеджерге 6 таңбалы кодты айтады. Менеджер кодты «Код» өрісіне енгізеді.
4. Егер код дұрыс болса, ARM терезесінде сурет пен құжат мәліметтері түріндегі цифрлық құжат ашылады.
5. Менеджер визуалды салыстыруды жүргізеді және «Жабу» батырмасы арқылы терезені жабады.

**Logs** – **Логтарды жинау**

Логтарды жинау модулі қолданба мен қызмет логтарын орталықтан сақтауға, сонымен қатар логтарды қарауға және мәтінмән бойынша іздеуге мүмкіндік береді. Логтарды жинау және көрсету пішімі қоса берілген файлда – check-list-fib-rus.pdf көрсетілген ақпараттық қауіпсіздік талаптарына сәйкес болуы керек.

**Monitoring – Жүйе күйін бақылау**

Жүйе күйін бақылау модулі жүйенің және жеке модульдердің күйін ыңғайлы графиктер мен бақылау тақталары түрінде алуға мүмкіндік береді

**Integrations - Интеграциялық модуль**

Интеграциялық модуль сыртқы қызметтермен және МО қызметтерімен жұмыс істеу қабаты болып табылады. Атап айтқанда, ол көлікпен және басқа электрондық қолтаңбалармен жұмысты жүзеге асыруды жасыра отырып, SOAP/RPC JSON хаттамаларына негізделген ыңғайлы API түрінде қызметті пайдалануға мүмкіндік береді. Модуль жүйені бақылау және интеграциялық процестерді орталықтандырылған тіркеу үшін жұмысты тексеру әдістерін қолдайды.

**ECP – ЭЦҚ-мен жұмыс істеу модулі.**

Модуль оны ҚР ҰКО ЭЦҚ-мен пайдалануға мүмкіндік береді.

**DICTIONARIES – Анықтамалар**

Анықтамалық модуль жаңартылған ақпаратты сақтауға арналған. Анықтамалық әдебиеттердің кез келген жинағы кесте түрінде берілген. Жоғарғы панель деректер жиынын қосу, өңдеу, жою, іздеу және жаңарту үшін батырмаларды қажет етеді.

**DocType – цифрлық құжаттардың түрлері:**

**Деректер сыртқы жүйеден біріктіріледі.** Анықтамадағы параметрлер:

|  |  |  |
| --- | --- | --- |
| Name | Type | Description |
| ID | Number(10) | бірегей келісімшарт нөмірі |
| Code | VARCHAR2(20) | Құжат коды |
| Name | VARCHAR2(200) | Құжат атауы (орысша) |
| Name\_Kz | VARCHAR2(200) | Құжат атауы (қазақша) |



5 сурет. Мәліметтерді беру жүйесінің сұлбасы.

**Негізгі желі түйіні** маршрутизатор, желіаралық экран және негізгі шлюз қызметін атқаратын, сонымен қатар желіні келесі VLAN желілеріне бөлетін PfSense сервері (виртуалды машина) болып табылады:

1. Интернет (соның ішінде VPN арналары, ВШЭП және ЦОД резервтік дейін)
2. DMZ – қосымша сервері бар аймақ.
3. Қауіпсіз ішкі желі – мәліметтер базасының сервері, тіркеу сервері және мониторинг сервері бар, бұл желіге кіру тек кіре берістегі қолданбалы сервер үшін, ал шығуда тіркеу және бақылау серверлері үшін ұйымдастырылады.

Жүйенің негізгі түйінін ВШЭП -ке қосу SmartBridge көмегімен ұйымдастырылған SSL VPN арнасы арқылы жүзеге асырылады.

**Сақтық көшірме түйіні** PfSense желіаралық экранмен қорғалған. Серверлер екі бөлек ішкі желіде орналасқан, олардың арасындағы өзара әрекеттесу желіаралық экран арқылы жүзеге асырылады. Сақтық көшірме және бастапқы түйіндер арасындағы байланыс oVPN арқылы жүзеге асырылады.

Негізгі және резервтік дерекқор серверлері арасындағы өзара әрекеттесу VPN арнасы арқылы жүзеге асырылады, сонымен қатар қол жеткізу мониторинг сервері үшін белгіленген порттар арқылы ұйымдастырылады.

**Функционалды емес талаптар:**

 1) Қолданба заманауи негізде әзірленуі керек (React, Angular, Vue және басқа);

 2) Қолданба Active Directory интеграциясына негізделген аутентификация мен авторизацияны қолдайды;

 3) Веб-қосымшаның жұмыс істеуі нәтижесінде алынған барлық құпия және жеке деректер деректер базасын, кэшті, файлдарды және деректерді сақтаудың басқа түрлерін қоса алғанда, сақтауда сақталмауы керек;

 4) Орындаушы бастапқы кодты және жоба құрастыру скриптарын беруге міндеттенеді.

 5) Орындаушы Қазақстан Республикасының «Ақпараттандыру туралы» 2015 жылғы 24 қарашадағы Заңына, Қазақстан Республикасы Цифрлық даму, қорғаныс және аэроғарыш өнеркәсібі министрінің 2019 жылғы 3 маусымдағы № 111/НК және ЕТ бұйрығымен бекітілген «Электрондық үкіметтің» ақпараттық объектілерін және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне жатқызылған ақпараттық жүйелерді тестілеу әдістемесі мен қағидаларына сәйкес аккредиттелген сынақ зертханасында ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтардан өту алдында ақпараттық қауіпсіздіктің барлық процестерінің конфигурациялануын қамтамасыз етуі тиіс. Егер сәйкессіздіктер анықталса, Орындаушы 20 жұмыс күні ішінде түзетулер енгізуі және сынақтың қайтадан сәтті өтуін қамтамасыз етуі керек.

6) Пайдаланушыларға жүйенің шектеулі немесе толық функционалдығын қамтамасыз ету мүмкіндігімен қолданбада кіру топтарын ұйымдастыру мүмкіндігі.

**Коммерциялық ұсынысқа қойылатын талаптар:**

1. Интеграциялық платформаны әзірлеуге, орналастыруға, орнатуға және конфигурациялауға ҚР салық және бюджетіне төленетін басқа да жарналарды қоса алғанда теңгедегі құны.

2. Салық және басқа шегерімдерді қоса алғанда, лицензиялардың құны теңгемен.

3. Іске асыру кестесі (кезеңдері) түпкілікті процесс ретінде: бағдарламалық қамтамасыз етуді енгізу, аттестациялау, банк пен компания арасындағы жауапкершілік салаларымен құжаттамалау.

**Құжаттамаға қойылатын талаптар**

1. Басқа жүйелермен интеграцияның тізбесі және сипаттамасы.
2. Инфрақұрылымның сипаттамасы (сынақ, өндіріске дейінгі, өнім)
3. Мәліметтер базасында сақталатын ақпарат тізімі бар техникалық нұсқаулар (кестелерді, қатынастарды, баптауларды, қызметтерді параметрлермен сипаттау тұрғысынан интеграциялық процестерді, журналдарды тіркеу процестерін және т.б. сипаттау).
4. Архитектуралық сұлба/Қызмет сұлбасы (өнімді стендтер үшін және толық тізімі бар сынақ стендтері үшін: серверлер, порттар, хаттамалар, деректер ағындары).
5. Сервисте қолданылатын бағдарламалық құралдар тізімі (атауы, нұсқалары)
6. Қолданба әкімшілеріне арналған нұсқаулар (модульді басқару, пайдаланушыларды құру, құқықтарды анықтау, параметрлерді өзгерту және т.б.)
7. Бақыланатын компоненттер тізімі.
8. Пайдаланушы нұсқаулары (бұл скриншоттармен бірге жүйенің барлық функцияларының сипаттамасын қамтиды). Өтінім үшін міндетті құжат.
9. Апаттық қызметті қалпына келтіру тәртібі (нұсқаулары) және оның құрамдас бөліктері.
10. Орындалған жүктеме сынағы туралы есеп
11. әзірленген интеграциялық қызметтердің тізімі және оларды басқа жүйелерден шақыруға болатын мысалдар.

**Кепілдік қолдау**

1. Орындалған жұмыстар актісіне қол қойылғаннан және жүйені іске қосқаннан кейін 90 күн ішінде жеткізушіден кепілдік қолдауының болуы.

**Инфрақұрылымға қойылатын талаптар**

1. Қызмет көрсету платформасы ретінде 7.9 төмен емес Centos OS нұсқасын пайдалануы керек
2. Егер шешім ДБ болуы көзделсе, ол 14 кем емес PostgreSQL нұсқасы болуы керек
3. Шешім платформа тұрғысынан ақауларға төзімді болуы керек (серверлердің қайталануы қамтамасыз етіледі).