Республиканское государственное предприятие «Казахстанский центр межбанковских расчетов Национального Банка Республики Казахстан»

Регистрации и обращение к API на портале КЦМР

Методическая рекомендация

Алматы 2021 г.

Оглавление

Разработал:			
Должность	**Ф.И.О.**	**Подпись**	**Дата**
Главный системный аналитик Отдел технологии и архитектуры информационных систем УРИП	Усманов А.А.		

Введение

Символы и аббревиатуры

API – Application Programming Interface (программный интерфейс приложения)

HTTP – HyperText Transfer Protocol (протокол передачи гипертекста)

REST – Representational State Transfer (передача состояния представления)

TLS – Transport Layer Security (протокол защиты транспортного уровня)

MTLS – Mutual TLS (взаимные подключения по протоколу TLS)

Нормативные ссылки

Рекомендуется использовать следующие ссылочные документы.

OpenID Connect Core 1.0 incorporating errata set 1 (http://openid.net/specs/openid-connect-core-1_0.html)

OAuth 2.0 – (https://tools.ietf.org/html/rfc6749)

MTLS – Mutual TLS Profile for OAuth 2.0 (https://tools.ietf.org/html/draft-ietf-oauth-mtls-03)

Глава 1. Описание системы управления API КЦМР

Система предназначена для предоставления доступа к API (сервисам) КЦМР посредством архитектурного стиля REST. Аутентификация, реализуемая с помощью модели OAuth 2.0 и расширения OpenID Connect, основана на использовании токена идентификации (ID token). Система состоит из Front end и Back end. Front end представляет собой портал и служебные веб- сервисы для работы с системой.

Портал и служебные веб-сервисы предоставляют пользователям следующие основные функции:

- Создание/регистрация пользователя;
- Создание приложений;
- Подписка на API.

В данном документе описывается порядок работы с Порталом системы управления API КЦМР (далее - Портал).

Глава 2. Регистрация/создание пользователя в Портале

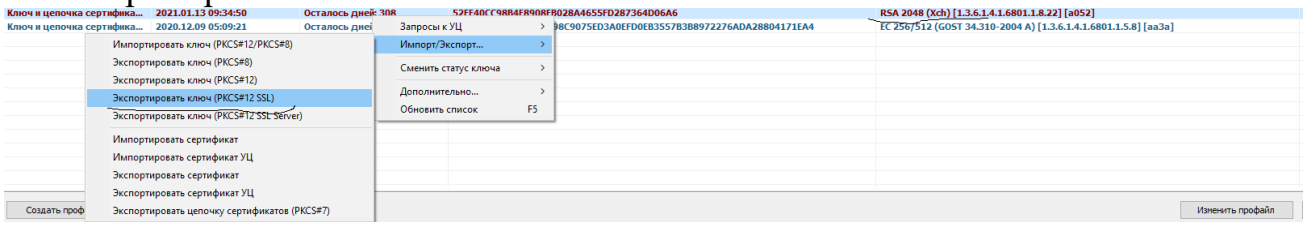
На Портале включен механизм MTLS, в связи с чем в Удостоверяющем Центре КЦМР необходимо получить комплект регистрационных свидетельств для одной из систем КЦМР (Платежная система, система массовых электронных платежей, Центр обмена идентификационными данными) включая сертификаты для авторизации. Контакты Удостоверяющего Центра размещены на корпоративном сайте КЦМР (http://www.kisc.kz/sections/kontakty. По всем вопросам, касающимся ключей, их продления, а также установки и настройки ПО «Tumar CSP» обращаться на e-mail: **supportca@kisc.kz** или по телефону: **2506675**). Сертификат для авторизации должен быть типа RSA, 2048bit, «client authentication» с указанием в CN - системного имени (идентификатор пользователя в системе для одной из систем КЦМР) который должен быть указан, как «имя пользователя» при регистрации (глава 3 пункт 1).

Удостоверяющий Центр КЦМР предоставляет временный комплект регистрационных свидетельств (срок действия 14 дней) который необходимо использовать для выпуска регистрационных свидетельств боле продолжительного действия (срок действия 1 год). После выпуска регистрационных свидетельств необходимо экспортировать комплект регистрационных свидетельств на файловую систему компьютера. В ПО «Tumar CSP» в профиле «FSystem» выделяете строку с сертификатом и нажимаете правой клавишей мыши, в появившемся контекстном меню найти пункт «Импорт/Эскпорт» и в раскрывшемся меню выбрать для каждого типа сертификата нужную опцию:

- RSA – Экспортировать ключ (PKCS#12 SSL), экспортируется файл с расширением *.p12;

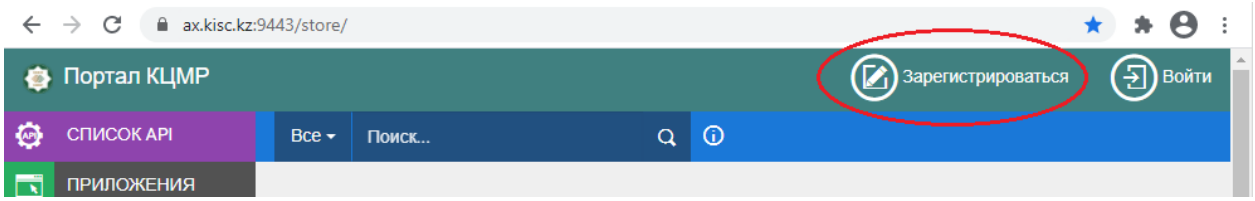
- ГОСТ, Шифрование – Экспортировать ключ (PKCS#12), экспортируется файл с расширением *.pfx;

Пример:



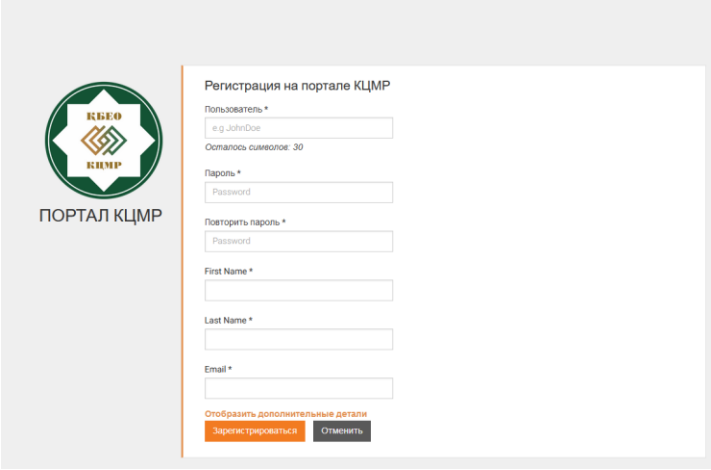
Для доступа на портал необходимо установить RSA сертификат (расширение *.p12) в локальное хранилище Windows если используется браузер Google Chrome или в хранилище браузера если используется Firefox. Прописать 91.195.226.56 в файле hosts под именем ax.kisc.kz, если по DNS не доступен., а затем перейти по ссылке тестового портала https://ax.kisc.kz:9443/store.

URL боевого портала: https://online.kisc.kz:9443/store - доступен только через выделенный канал.



Для регистрации нового пользователя на Портале следует пройти по ссылке необходимо нажать на кнопку «Зарегистрироваться»/«Sign-up» на открывшейся странице заполнить все обязательные поля и принять политику конфиденциальности.

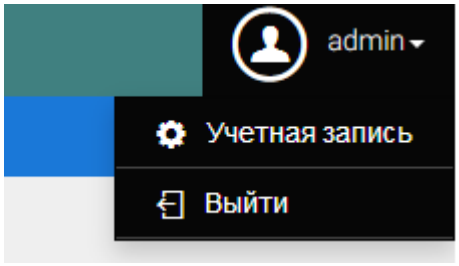
В поле «Пользователь» указывается системное имя (идентификатор пользователя) который должен быть тем же самым, что и CN в сертификате (полученном в УЦ КЦМР, без префикса Системы).

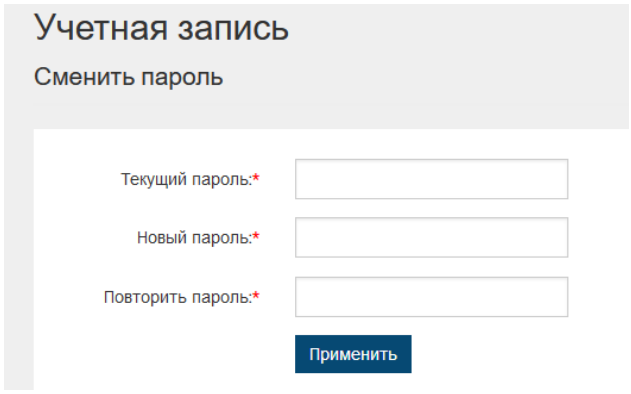


После регистрации, учетную запись пользователя необходимо подтвердить. Для этого необходимо обратиться к ответственному менеджеру КЦМР (тел.: 2506626).

Для изменения пароля необходимо авторизоваться на портале, затем в правом верхнем углу на иконке пользователя выбрать из выпадающего

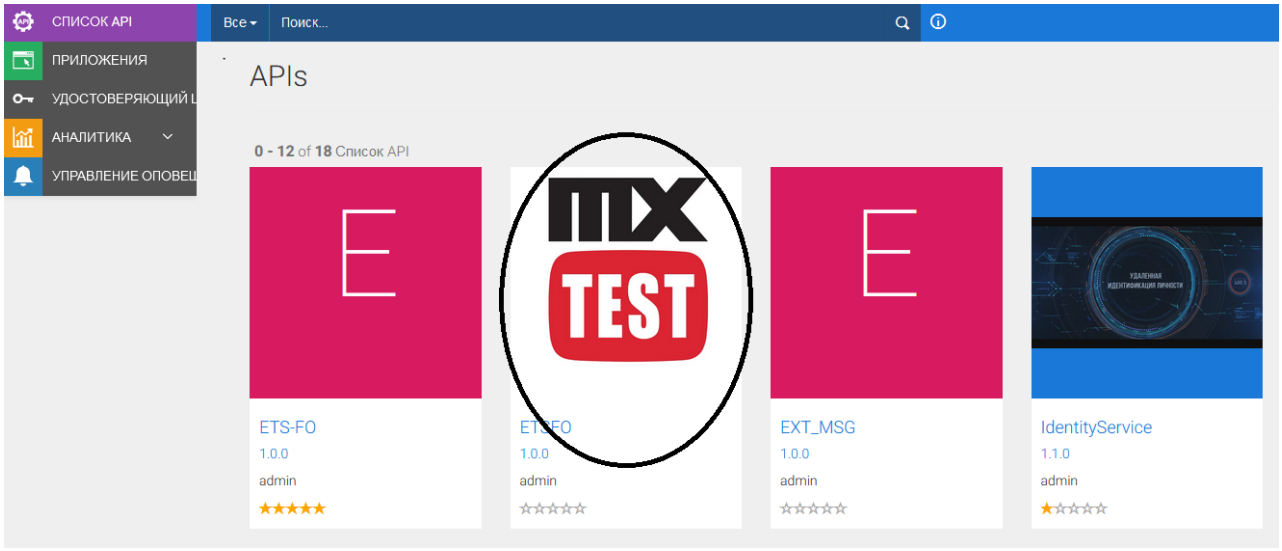
списка «Учетная запись». В открывшемся окне ввести текущий пароль и дважды новый.



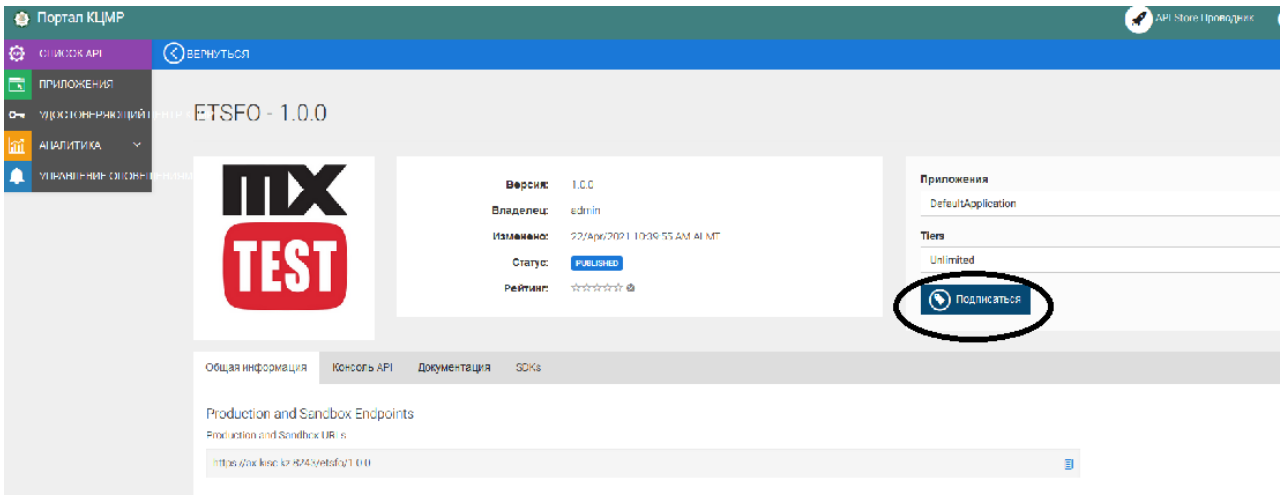


Глава 3. Процесс подписки на API

Для того, чтобы произвести подписку на API «необходимо авторизоваться на портале КЦМР и выбрать необходимый API.



После чего в открывшемся окне выбрать приложение (по умолчанию это DefaultApplication) и нажать на кнопку «Подписаться». Для завершения подписки на API необходимо дождаться подтверждения от администратора портала (тел.: 2506626).



Глава 4. Работа с API

Для получения доступа к API должны быть выполнены следующие требования:

– получение регистрационных свидетельств и ключей в Удостоверяющем Центре КЦМР (для тестового стенда – тестовые ключи RSA-клиент УЦ КЦМР betaca.kisc.kz);

– авторизация, запрос токена доступа, использование токена доступа для вызова API;

– обновление токена доступа по истечению срока действия.

Для подписи запросов API необходимо использовать сертификат и ключ.

Для этого необходимо использовать openssl.

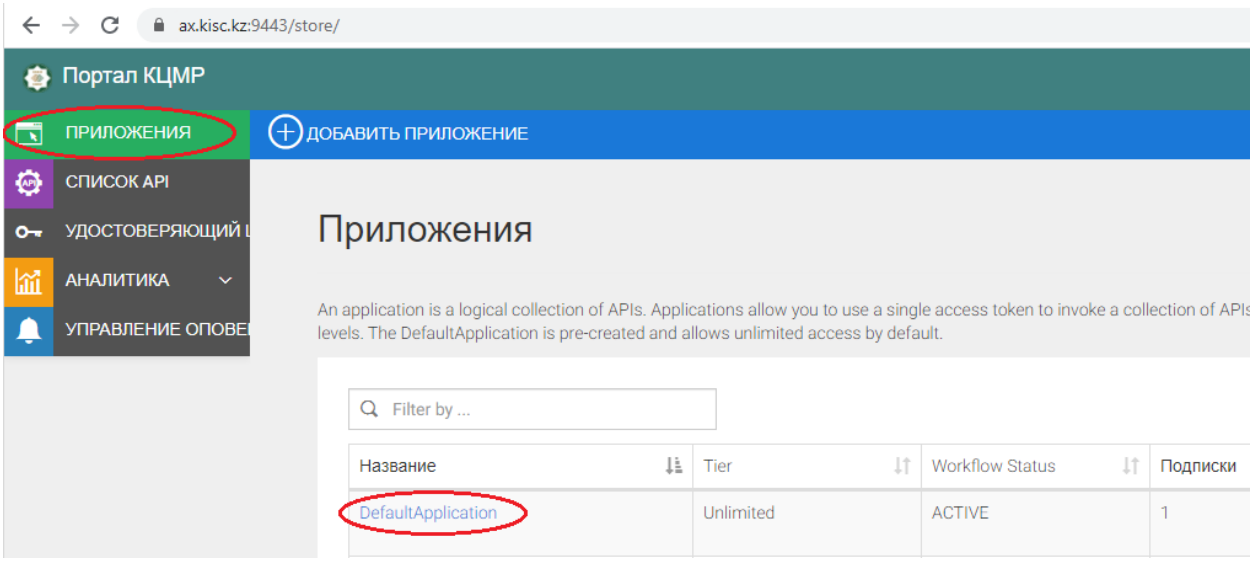
Пример:

openssl pkcs12 -in pkcs12_sign.p12 -nocerts -nodes -out K0531900.key

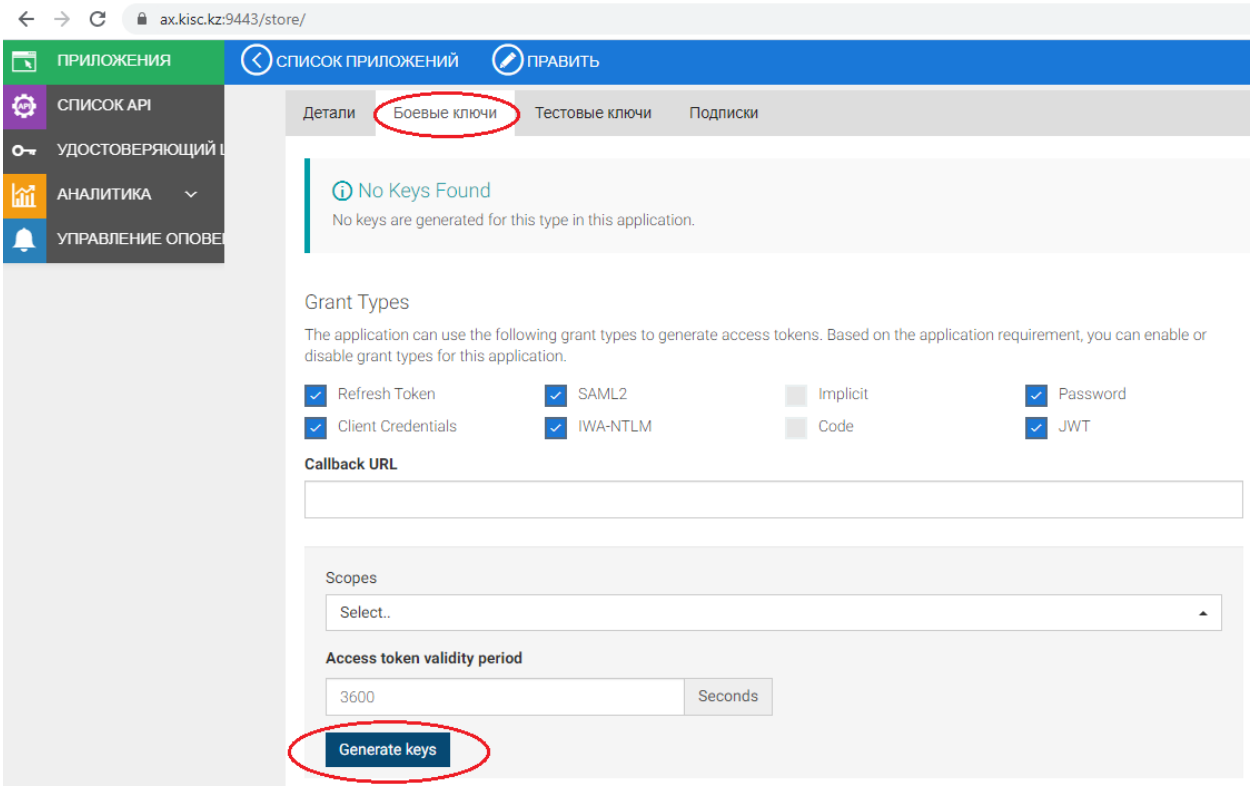
openssl pkcs12 -in pkcs12_sign.p12 -clcerts -nokeys -out K0531900.cer

4.1. Генерация «Consumer Key» и «Consumer Secret»

Для генерации токена доступа (access token) необходимо получить «Consumer Key» и «Consumer Secret» для этого необходимо перейти в раздел «Приложения» и выбрать приложение которым вы подписались на необходимый API.



Далее выбрать вкладку «Боевые ключи» и нажать на кнопку «Generate keys», после чего будут сгенерированы «Consumer Key» и «Consumer Secret», для отображения параметра «Consumer Key» необходимо нажать на кнопку «Show Keys». Параметр «Consumer Secret» после генерации посмотреть нельзя, для того, чтобы узнать значение его нужно пере генерировать, нажав на кнопку «Regenerate», после чего он отобразится в отдельном окне. На вкладке «Подписки» можно проверить статус приложения, он должен быть «UNBLOCKED». Вкладка «Тестовые ключи» не используется.



4.2. Авторизация

Пример запроса:

```
curl -X POST -H "Authorization: Basic {Consumer Key:Consumer Secret в
base64}" -d "grant_type=password&username={логин от
портала}&password={пароль от портала}&scope=default"
https://ax.kisc.kz:8243/token --cert {имя файла сертификата}.cer --key
{имя файла ключа}.key -i -k -v
```

Пример ответа:

```
{"access_token":"1df635d7-5efd-34fc-9ea7-
9b3c1483c202","refresh_token":"197a4a8d-4f3f-3341-b0e4-
f7bd4dbfd37b","scope":"default","token_type":"Bearer","expires_in":3600}
```

Время жизни токена доступа можно указать на выбор (указывается в секундах, 3600 – 1 час). После того, как токен доступа устарел вернется ошибка. Для того, чтобы продолжить работу необходимо обновить токен доступа с помощью «refresh_token».

4.3. Обновление токена доступа

Пример запроса:

```
curl -k -X POST -d "grant_type=refresh_token&refresh_token=a7820819-788d-
33ee- 941f-daa42ec6e1cd" -H "Authorization: Basic
R3d0RWZERWZiZUVwSGR2NV9jNDdkRWNkX3pVYTpPaGh4S3pSRjAwQmRaN2JNN3ZPVk43enA0cD
hh" https://ax.kisc.kz:8243/token --cert {имя файла сертификата}.cer --key {имя
файла ключа}.key –i
```

Пример ответа:

```
{
      "access_token":"1bd295a9-edab-3798-afe0-d29da22f6e82",
      "refresh_token":"d6a9264e-0283-377f-91a9-0c73123c5b92",
      "scope":"default",
      "token_type":"Bearer",
      "expires_in":3600
}
```

4.4. Вызов API

Банк использует токен доступа для создания/запроса (POST/GET) ресурса /messages/ серверу ресурсов КЦМР.

4.4.1. Отправка сообщений в транспортную систему КЦМР

Для отправки сообщений в транспортную систему КЦМР используется запрос методом POST на ресурс /messages/. Транспортная среда КЦМР в зависимости от типа сообщения маршрутизирует его получателям.

Пример запроса:

```
curl -k -X POST " https://ax.kisc.kz:8243/etsfo/1.0.0/messages/" -
H"accept: application/xml" -H "Content-Type: application\xml"
-d @filename.xml -H"Authorization: Bearer 2223a49a-399a-3a28-959d-
ab8e9ce0c482" -H "x-idempotency-key: 1000000000000402" --cert {имя файла
сертификата}.cer --key {имя файла ключа}.key –i
```

Статус обработки сообщения:

```
HTTP/1.1 202 Accepted
```

4.4.2. Получения сообщения из транспортной системы КЦМР

Для получения сообщений из транспортной системы КЦМР используется запрос методом GET на ресурс /messages/. Транспортная среда КЦМР отправляет получателям соответствующее сообщения если таковые имеются в системе.

4.4.2.1. Получение списка не прочитанных сообщений

Для получения списка не прочтенных сообщений используется ресурс /messages/ методом GET.

Пример запроса:

```
curl -k -X GET " https://ax.kisc.kz:8243/etsfo/1.0.0/messages/" -H"accept:
application/xml" -H"Authorization: Bearer 2223a49a-399a-3a28-959d-
ab8e9ce0c482" -H "Content-Type: application\xml" --cert {имя файла
сертификата}.cer --key {имя файла ключа}.key –i
```

Пример ответного сообщения:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <Data>
      <MESSAGES xmlns="http://ws.wso2.org/dataservice">
        <IDEMPOTENCY_KEY>GRO2021051114103</IDEMPOTENCY_KEY>
        <INTERACTION_ID />
        <CONTENTTYPE>application/xml</CONTENTTYPE>
        <MESSAGE_TYPE>camt.054.001.07</MESSAGE_TYPE>
        <RSTATUS>0</RSTATUS>
        <RLASTERR>0</RLASTERR>
        <RSENDER>KZGRO.SGROSS00</RSENDER>
      </MESSAGES>
      <MESSAGES xmlns="http://ws.wso2.org/dataservice">
        <IDEMPOTENCY_KEY>GRO2021051114105</IDEMPOTENCY_KEY>
        <INTERACTION_ID />
        <CONTENTTYPE>application/xml</CONTENTTYPE>
        <MESSAGE_TYPE>pacs.008.001.08</MESSAGE_TYPE>
        <RSTATUS>0</RSTATUS>
        <RLASTERR>0</RLASTERR>
        <RSENDER>KZGRO.SGROSS00</RSENDER>
      </MESSAGES>
      <MESSAGES xmlns="http://ws.wso2.org/dataservice">
```

```
        <IDEMPOTENCY_KEY>GRO2021060123853</IDEMPOTENCY_KEY>
        <INTERACTION_ID />
        <CONTENTTYPE>application/xml</CONTENTTYPE>
        <MESSAGE_TYPE>pacs.002.001.11</MESSAGE_TYPE>
        <RSTATUS>0</RSTATUS>
        <RLASTERR>0</RLASTERR>
        <RSENDER>KZGRO.SGROSS00</RSENDER>
      </MESSAGES>
    </Data>
  </soapenv:Body>
</soapenv:Envelope>
```

4.4.2.2. Получение сообщения

Для получения сообщения из списка не прочтенных сообщений используется ресурс /messages/{id}, где {id} – «x-idempotency-key» сообщения

Пример запроса:

```
curl -k -X GET " https://ax.kisc.kz:8243/etsfo/1.0.0/messages/ {id}" -
H"accept: application/xml" -H"Authorization: Bearer 2223a49a-399a-3a28-
959d- ab8e9ce0c482" -H "Content-Type: application\xml" --cert {имя файла
сертификата}.cer --key {имя файла ключа}.key –i
```

Пример ответного сообщения:

```
<?xml version="1.0" encoding="UTF-8"?>
<Data>
  <Envelope>
    <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
        <FIId>
          <FinInstnId>
            <Othr>
              <Id>SGROSS00</Id>
              <SchmeNm>
                <Prtry>KZGRO</Prtry>
              </SchmeNm>
            </Othr>
          </FinInstnId>
        </FIId>
      </Fr>
      <To>
        <FIId>
          <FinInstnId>
            <Othr>
              <Id>K9000666</Id>
              <SchmeNm>
                <Prtry>KZGRO</Prtry>
              </SchmeNm>
            </Othr>
          </FinInstnId>
        </FIId>
      </To>
      <BizMsgIdr>GRO2021051114103</BizMsgIdr>
      <MsgDefIdr>camt.054.001.07</MsgDefIdr>
      <CreDt>2021-05-11T18:18:29+06:00</CreDt>
      <Prty>NORM</Prty>
```

```
      <Sgntr />
    </AppHdr>
    <Document xmlns="urn:iso:std:iso:20022:tech:xsd:camt.054.001.07">
      <BkToCstmrDbtCdtNtfctn>
        <GrpHdr>
          <MsgId>GRO2021051114103</MsgId>
          <CreDtTm>2021-05-11T18:18:29+06:00</CreDtTm>
        </GrpHdr>
        <Ntfctn>
          <Id>GRO2021051114103</Id>
          <Acct>
            <Id>
              <IBAN>KZ86319KZT1001300234</IBAN>
            </Id>
            <Svcr>
              <FinInstnId>
                <BICFI>NBRKKZKX</BICFI>
              </FinInstnId>
            </Svcr>
          </Acct>
          <Ntry>
            <Amt Ccy="KZT">2450</Amt>
            <CdtDbtInd>CRDT</CdtDbtInd>
            <Sts>
              <Cd>BOOK</Cd>
            </Sts>
            <BkTxCd>
              <Prtry>
                <Cd>01</Cd>
              </Prtry>
            </BkTxCd>
            <NtryDtls>
              <Btch>
                <MsgId>MsgId_4d5e65d-77eb_1</MsgId>
                <NbOfTxs>2</NbOfTxs>
                <TtlAmt Ccy="KZT">2450</TtlAmt>
              </Btch>
            </NtryDtls>
          </Ntry>
        </Ntfctn>
      </BkToCstmrDbtCdtNtfctn>
    </Document>
  </Envelope>
</Data>
```

4.4.3. Пример отправки сообщений

Форматы сообщений утвержденных сообщений, а также описание структуры транспортных сообщений, подписи и шифрования в платежных системах Казахстана хранятся на интернет-ресурсе КЦМР в разделе Технологии - Стандарт ISO 20022 (https://www.kisc.kz/uploaded/files/Examples.rar, https://www.kisc.kz/uploaded/files/Opis_struck_transports_soobsh_podpisy_shifrovanie.pdf).

Для примера рассмотрим отправку сообщения «Клиентский кредитовый перевод»

Кредитовый перевод банком:

- метод POST;
- сообщение - pacs.008.001.08;
- получатель платежная система.

Пример запроса:

```
POST https://ax.kisc.kz:8243/etsfo/1.0.0/messeges HTTP/1.1
x-fapi-auth-date: 2021-06-02T16:46:31+06:00
x-fapi-interaction-id: ID-INT-007
Authorization: Bearer e5519f53-2b0b-3182-afec-fcc7b37c6b2d
x-idempotency-key: ID-KEY-007
x-fapi-interaction-id: KISC_KK01DXVO6J
Content-Type: application/xml
```

```
<Envelope>
  <EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#"
Type="http://www.w3.org/2001/04/xmlenc#Element">
    <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#gost34310-gost34311 " />
    <CipherData>

<CipherValue>5sAuDgWH+OxxxolHu1rE2TDf6+KzQGgd9gO1WmXVh7+g74Hs8db</CipherValue>
    </CipherData>
  </EncryptedData>
</Envelope>
```

Статус обработки сообщения:

```
HTTP/1.1 202 Accepted
```

Отчет о статусе кредитового перевода банком:

- метод GET;
- сообщение - pacs.002.001.11;
- получатель банк отправителя денег;

Пример запроса:

```
GET https://ax.kisc.kz:8243/etsfo/1.0.0/messeges/GRO2021051114105 HTTP/1.1
x-fapi-auth-date: 2021-06-02T16:46:31+06:00
x-fapi-interaction-id: ID-INT-007
Authorization: Bearer e5519f53-2b0b-3182-afec-fcc7b37c6b2d
x-idempotency-key: ID-KEY-007
x-fapi-interaction-id: KISC_KK01DXVO6J
Content-Type: application/xml
```

Пример ответного сообщения:

```
<Envelope>
  <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
    <Fr>
      <FIId>
        <FinInstnId>
          <Othr>
```

```
                <Id>SGROSS00</Id>
                <SchmeNm>
                  <Prtry>KZGRO</Prtry>
                </SchmeNm>
              </Othr>
            </FinInstnId>
          </FIId>
        </Fr>
        <To>
          <FIId>
            <FinInstnId>
              <Othr>
                <Id>K0000014</Id>
                <SchmeNm>
                  <Prtry>KZGRO</Prtry>
                </SchmeNm>
              </Othr>
            </FinInstnId>
          </FIId>
        </To>
        <BizMsgIdr>GRO2021051114106</BizMsgIdr>
        <MsgDefIdr>pacs.002.001.11</MsgDefIdr>
        <CreDt>2021-05-11T18:18:28+06:00</CreDt>
        <Prty>NORM</Prty>
        <Sgntr/>
      </AppHdr>
      <Document xmlns="urn:iso:std:iso:20022:tech:xsd:pacs.002.001.11">
        <FIToFIPmtStsRpt>
          <GrpHdr>
            <MsgId>GRO2021051114106</MsgId>
            <CreDtTm>2021-05-11T18:18:28+06:00</CreDtTm>
          </GrpHdr>
          <OrgnlGrpInfAndSts>
            <OrgnlMsgId>MsgId_4d5e65d-77eb_1</OrgnlMsgId>
            <OrgnlMsgNmId>pacs.008.001.08</OrgnlMsgNmId>
            <OrgnlCreDtTm>2021-04-22T14:01:44+06:00</OrgnlCreDtTm>
            <GrpSts>ACSP</GrpSts>
          </OrgnlGrpInfAndSts>
          <TxInfAndSts>
            <OrgnlEndToEndId>EToEId_4d5e65d-77eb_1</OrgnlEndToEndId>
            <OrgnlTxId>MsgId_4d5e65d-77eb_1</OrgnlTxId>
          </TxInfAndSts>
        </FIToFIPmtStsRpt>
      </Document>
    </Envelope>
```


Сообщение о дебетовании счета:
- метод GET;
- сообщение - camt.054.001.07;
- получатель банк отправителя денег;

Пример запроса:

```
GET https://ax.kisc.kz:8243/etsfo/1.0.0/messeges/GRO2021051914129 HTTP/1.1
x-fapi-auth-date: 2021-06-02T16:46:31+06:00
x-fapi-interaction-id: ID-INT-007
Authorization: Bearer e5519f53-2b0b-3182-afec-fcc7b37c6b2d
x-idempotency-key: ID-KEY-007
x-fapi-interaction-id: KISC_KK01DXVO6J
Content-Type: application/xml
```

Пример ответного сообщения:

```
<Envelope>
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <Othr>
                  <Id>SGROSS00</Id>
                  <SchmeNm>
                     <Prtry>KZGRO</Prtry>
                  </SchmeNm>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <Othr>
                  <Id>K0000014</Id>
                  <SchmeNm>
                     <Prtry>KZGRO</Prtry>
                  </SchmeNm>
               </Othr>
            </FinInstnId>
         </FIId>
      </To>
      <BizMsgIdr>GRO2021051114097</BizMsgIdr>
      <MsgDefIdr>camt.054.001.07</MsgDefIdr>
      <CreDt>2021-05-11T18:14:45+06:00</CreDt>
      <Prty>NORM</Prty>
      <Sgntr/>
   </AppHdr>
   <Document xmlns="urn:iso:std:iso:20022:tech:xsd:camt.054.001.07">
      <BkToCstmrDbtCdtNtfctn>
         <GrpHdr>
            <MsgId>GRO2021051114097</MsgId>
            <CreDtTm>2021-05-11T18:14:45+06:00</CreDtTm>
         </GrpHdr>
         <Ntfctn>
            <Id>GRO2021051114097</Id>
            <Acct>
               <Id>
                  <IBAN>KZ98125KZT1001300600</IBAN>
               </Id>
               <Svcr>
                  <FinInstnId>
```

```
                <BICFI>NBRKKZKX</BICFI>
              </FinInstnId>
            </Svcr>
          </Acct>
          <Ntry>
            <Amt Ccy="KZT">2450</Amt>
            <CdtDbtInd>DBIT</CdtDbtInd>
            <Sts>
              <Cd>BOOK</Cd>
            </Sts>
            <BkTxCd>
              <Prtry>
                <Cd>01</Cd>
              </Prtry>
            </BkTxCd>
            <NtryDtls>
              <Btch>
                <MsgId>MsgId_3bdba70-b369_1</MsgId>
                <NbOfTxs>2</NbOfTxs>
                <TtlAmt Ccy="KZT">2450</TtlAmt>
              </Btch>
            </NtryDtls>
          </Ntry>
        </Ntfctn>
      </BkToCstmrDbtCdtNtfctn>
    </Document>
</Envelope>
```