**Методы КДП**

Тип методов КДП: Синхронный.

getUserData - Запрос доступа к персональным данным.

**Запрос доступа к персональным данным (getUserData)**

**Запрос (Request) включает:**

<xs:complexType name="getUserDataRequest">

<xs:sequence>

<xs:element name="uin" minOccurs="1" type="xs:string">

<xs:annotation>

<xs:documentation>ИИН</xs:documentation>

</xs:annotation>

</xs:element>

<xs:element name="company" minOccurs="1" type="xs:string">

<xs:annotation>

<xs:documentation>Наименование организации</xs:documentation>

</xs:annotation>

</xs:element>

<xs:element name="company\_bin" minOccurs="1" type="xs:string">

<xs:annotation>

<xs:documentation>БИН/ИИН организации</xs:documentation>

</xs:annotation>

</xs:element>

<xs:element name="company\_responsible" type="xs:string">

<xs:annotation>

<xs:documentation>Наименование организации, у которой запрашиваются данные</xs:documentation>

</xs:annotation>

</xs:element>

<xs:element name="employee\_name" type="xs:string">

<xs:annotation>

<xs:documentation>ФИО сотрудника из организации, запрашивающей персональные данные (третьей

стороны)

</xs:documentation>

</xs:annotation>

</xs:element>

<xs:element name="access\_name" type="xs:string">

<xs:annotation>

<xs:documentation>Наименование госуслуги</xs:documentation>

</xs:annotation>

</xs:element>

<xs:element name="personal\_data\_name" type="xs:string">

<xs:annotation>

<xs:documentation>Наименование персональных данных (например, ФИО запросить ИИН)</xs:documentation>

</xs:annotation>

</xs:element>

<xs:element name="expiresIn" type="xs:int" minOccurs="0" default="600000">

<xs:annotation>

<xs:documentation xml:lang="ru">Срок действия кода в миллисекундах</xs:documentation>

</xs:annotation>

</xs:element>

<xs:element name="omit-sms" minOccurs="0" type="xs:boolean" default="false">

<xs:annotation>

<xs:documentation>Запрос персональных данных получен иным путем, значение по умолчанию False

</xs:documentation>

</xs:annotation>

</xs:element>

</xs:sequence>

</xs:complexType>

**Описание полей запроса (Request):**

1. uin\* - ИИН (субъекта персональных данных);
2. company\* - Наименование организации, запрашивающей доступ к персональным данным (третьей стороны);
3. company\_bin\* - БИН/ИИН организации, запрашивающей доступ к персональным данным (третьей стороны);
4. company\_responsible - Наименование организации, у которой запрашиваются данные;
5. employee\_name - ФИО сотрудника из организации, запрашивающей персональные данные (третьей стороны);
6. access\_name - Наименование госуслуги;
7. personal\_data\_name – Перечень сервисов (ServiceID - ШЭП), у которых будут запрашиваться персональные данные (для государственных ИС) или наименование персональных данных (например, ФИО запросить ИИН) (для частных ИС);
8. expiresIn\* - Время действия токена безопасности, указывается в миллисекундах (зависит от регламентного времени оказания услуг);
9. omit-sms – Запрос персональных данных получен иным путем.

**Ответ (Response) включает:**

<xs:complexType name="getUserDataResponse">

<xs:sequence>

<xs:element name="status" type="user-data-status" minOccurs="1">

<xs:annotation>

<xs:documentation>Статус запроса</xs:documentation>

</xs:annotation>

</xs:element>

<xs:element name="code" type="xs:string" minOccurs="0">

<xs:annotation>

<xs:documentation>Код верификации, представленный в JWT-формате (если статус VALID)

</xs:documentation>

</xs:annotation>

</xs:element>

<xs:element name="public-key" type="xs:string" minOccurs="0">

<xs:annotation>

<xs:documentation>Публичный ключ, необходимый для проверки валидности кода</xs:documentation>

</xs:annotation>

</xs:element>

</xs:sequence>

</xs:complexType>

**Описание полей ответа (Response):**

1. status – Статус запроса, может принимать одно из следующих значений:
   1. VALID – Доступ предоставлен;
   2. INVALID – В доступе отказано;
   3. PENDING – Ожидание ответа субъекта персональных данных;
   4. TIMEOUT – Время ожидания ответа субъекта персональных данных истекло;
   5. NOT\_FOUND – По указанному в запросе ИИН отсутствует номер телефона в БМГ;
   6. ERROR – Ошибка, полученная при отправке SMS.
2. public-key - Публичный ключ, необходимый для проверки валидности токена безопасности.
3. code – Токен безопасности представляет собой JWT и включает в payload следующую информацию:
   1. ИИН (данные поля uin);
   2. Перечень сервисов (ServiceID - ШЭП), у которых будут запрашиваться персональные данные, через точку с запятой (данные поля personal\_data\_name);
   3. **Дата и время получения положительного ответа от владельца персональных данных через SMS** в формате ISO 8601;
   4. Дата и время окончания действия токена безопасности, рассчитывается от **Даты и время получения** **положительного ответа от владельца персональных данных через SMS** + данные из поля expiresIn в формате ISO 8601;
   5. БИН/ИИН организации, запрашивающей доступ к персональным данным (третьей стороны) (данные поля company\_bin);
   6. Дата и время создания токена безопасности в формате Unix Time Stamp (обязательное поле JWT стандарта), совпадает с подпунктом c (обязательное поле JWT стандарта).;
   7. Дата и время окончания действия токена безопасности в формате Unix Time Stamp, совпадает с подпунктом d (обязательное поле JWT стандарта).

Токен безопасности подписывается ЭЦП владельца ИС КДП.

**Общий вид:**

{

"uin": ИИН, //описание в подпункте a.

"sid": ПЕРЕЧЕНЬ\_SERVICEID, //описание в подпункте b.

"dts": ДАТА\_ВРЕМЯ\_ПОЛУЧЕНИЯ\_ОТВЕТА\_ЧЕРЕЗ\_SMS, //описание в подпункте с.

"dte": ДАТА\_ВРЕМЯ\_ОКОНЧАНИЯ\_ДЕЙСТВИЯ\_ТОКЕНА\_БЕЗОПАСНОСТИ, //описание в подпункте d.

"binc": БИН/ИИН, //описание в подпункте e.

"iat": ДАТА\_ВРЕМЯ\_СОЗДАНИЯ\_ТОКЕНА\_БЕЗОПАСНОСТИ, //описание в подпункте f.

"exp": ДАТА\_ВРЕМЯ\_ОКОНЧАНИЯ\_ДЕЙСТВИЯ\_ТОКЕНА\_БЕЗОПАСНОСТИ //описание в подпункте g.

}

**Пример:**

**{**

"uin": "123456789132",

"sid": "MCDB\_SERVICE;MGOV\_SMS\_GW",

"dts": "2021-04-13T07:36:40",

"dte": "2021-04-13T07:46:40",

"binc": "0123456789123",

"iat": 1516239022,

"exp": 1516239022

}

В КДП должен вестись справочник сервисов у которых запрашиваются данные. При формировании Токена безопасности должен сверять ServiceID из personal\_data\_name со справочником сервисов у которых запрашиваются данные. Справочник должен содержать следующую информацию:

1. ServiceID – Идентификатор сервиса;
2. Наименование информационной системы;
3. Наименование услуги.

**Алгоритм функционирования КДП**

**Основной сценарий запроса персональных данных (getUserData):**

1. Информационная система (Организация), запрашивающая доступ к персональным данным (далее - Инициатор) направляет в КДП запрос на доступ к персональным данным (getUserDataRequest);
2. КДП сразу отправляет Инициатору ответ с status = PENDING (getUserDataResponse);
3. КДП отправляет запрос и получает ответ от БМГ;
4. КДП получив номер от БМГ отправляет SMS субъекту персональных данных;
5. КДП получив ответ от субъекта персональных данных, сохраняет ответ в blockchain;
6. Инициатор при отправке повторно запроса на доступ к персональным данным (getUserDataRequest) получает ответ (getUserDataResponse):
   1. В случае, положительного ответа субъекта персональных данных:

status = VALID

code = <СГЕНЕРИРОВАННЫЙ ТОКЕН БЕЗОПАСНОСТИ>

publicKey=<ПУБЛИЧНЫЙ КЛЮЧ ДЛЯ ДОСТУПА К ДАННЫМ В ТОКЕНЕ БЕЗОПАСНОСТИ >

* 1. В случае, отрицательного ответа субъекта персональных данных:

status = INVALID

code = <ПУСТО>

При условии, что повторный запрос на доступ к персональным данным (getUserDataRequest) от Инициатора будет получен до ответа, полученного от субъекта персональных данных будет сформирован следующий ответ (getUserDataResponse):

status = PENDING

code = <ПУСТО>

**ВАЖНО**: Инициатор, при отправке запроса персональных данных, должен в обязательном порядке включить ИИН (владельца данных), токен безопасности, публичный ключ (для получения доступа к информации токена безопасности и его верификации).

**Альтернативные сценарии запроса персональных данных (getUserData):**

В иных случаях ответ на запрос на доступ к персональным данным будет принимать следующие значения:

1. Время ожидания ответа субъекта персональных данных истекло:

status = TIMEOUT

code = <ПУСТО>

1. По указанному в запросе ИИН отсутствует номер телефона в БМГ:

status = NOT\_FOUND

code = <ПУСТО>

1. Ошибка, полученная при отправке SMS:

status = ERROR

code = <ПУСТО>

**Основной сценарий проверки токена безопасности:**

1. Информационная система (Организация), у которой запрашиваются данные (Источник данных) получив токен безопасности:
   1. Используя публичный ключ (publicKey) получить доступ к информации из токена безопасности;
   2. Сравнить ИИН в токене безопасности (uin) и ИИН в запросе персональных данных;
   3. Проверить наименование сервиса (ServiceID ШЭП) в перечне сервисов (sid);
   4. Проверить время действия токена безопасности (dte или exp).

**Пример запроса и ответа**

**Запрос getUserDataRequest:**

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns="http://service.2fa-chain.kz/ns/kdp">

<soapenv:Header/>

<soapenv:Body>

<sendMessageRequest>

<request>

<requestInfo>

<messageId>0f3d8368-215a-4a20-a306-5222548f5e87</messageId>

<serviceId>ServiceID</serviceId>

<sessionId>4958523f-423a-45bb-1aa1-5222548f5e87</sessionId>

<messageDate>2018-12-11T11:45:12.574+06:00</messageDate>

<sender>

<senderId>login</senderId>

<password>password</password>

</sender>

</requestInfo>

<requestData>

<data>

<uin>810918350135</uin>

<company>ЗАО Складские решения</company>

<company\_bin>12345678</company\_bin>

<company\_responsible>База мобильных граждан</company\_responsible>

<employee\_name>Иванов Иван Иванович</employee\_name>

<access\_name>MCDB\_SERVICE</access\_name>

<personal\_data\_name>Номер телефона</personal\_data\_name>

<expiresIn>600000</expiresIn>

<omit-sms>false</omit-sms>

</data>

</requestData>

</request>

</sendMessageRequest>

</soapenv:Body>

</soapenv:Envelope>

**Ответ getUserDataResponse:**

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">

<SOAP-ENV:Header/>

<SOAP-ENV:Body>

<sendMessageResponse xmlns:ns2="http://service.2fa-chain.kz/ns/kdp">

<ns2:response>

<ns2:responseInfo>

<ns2:messageId>a17d3e6d-614b-4e80-88ab-b920be91db07</ns2:messageId>

<ns2:responseDate>2021-04-15T01:44:16</ns2:responseDate>

<ns2:status/>

<ns2:sessionId>4958523f-423a-45bb-1aa1-5222548f5e87</ns2:sessionId>

</ns2:responseInfo>

<ns2:responseData>

<ns2:data>

<ns2:status>VALID</ns2:status>

<ns2:code>eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1aW4iOiIxMjM0NTY3ODkxMzIiLCJzaWQiOiJNQ0RCX1NFUlZJQ0U7TUdPVl9TTVNfR1ciLCJkdHMiOiIyMDIxLTA0LTEzVDA3OjM2OjQwIiwiZHRlIjoiMjAyMS0wNC0xM1QwNzo0Njo0MCIsImJpbmMiOiIwMTIzNDU2Nzg5MTIzIiwiaWF0IjoxNTE2MjM5MDIyLCJleHAiOiIxNTE2MjM5NjIyIn0.LCbPwu4dQ7e2r5-bFfKVYR7eIUL-4uFetsQ-CHEFs-BptBsCYnnGYe30Wg1ch2Hv-TwTJD3U4s1V3kBRH8JI6joX82EVXn00Pjz80VxjxVEZt-k9bB6f29XY\_Uq5nB3qFTxG1ofGOC8LHjLQeoAWyZALvTmVfYZpH6G2teK8mjkETVO8yktx9M921RoVe\_EdL6qxt46Xx6cJnzWJuCVbEFsOHPfE71Ea16JqjrhK7uKhNS4YXs6t832vTjzhfFydeqYjgljNj2rfZrQMK4KXPEBPKt1zJ5ScQe24AZWGbcD\_P1vvgnURkazTbGdkzJ68HaCm\_7ysAxWfOPqrNOHrOw</ns2:code>

<ns2:public-key>-----BEGIN PUBLIC KEY-----

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAhjwEDOZQ5BhLt0HKkJfQ

uLGfw1BR5HQ3Yx26/Aryf2kZAQ5/O0EKPJKdb8lC6Z/Y/yH39dEzuluQk0ACW88b

N1F5XVH4sc+08cS1miHwjz5ct6W6A5Mww/lLNeJGqpJWaueq409mO/FU3RIzrEeH

3qFYFi4UPgBzCjt70iDUWtFo2jfsm696oUz1eIbo191mIfSl3GCgK644mxGAOLXn

tRkUX4RKYST0noiiZ4021rtG6oahSPVvdLKNX27fjSyLg1Nj24ybEZkkAalLnGfH

0fdo8ddSzmPEtK6rvYKd3WWsoZu7vxULLs4qWunFCyW4PmMcjxkO6tGNLKpeGBpc

uQIDAQAB

-----END PUBLIC KEY-----</ns2:public-key>

</ns2:data>

</ns2:responseData>

</ns2:response>

</sendMessageResponse>

</SOAP-ENV:Body>

</SOAP-ENV:Envelope>