**Информационная система «Контроль доступа к персональным данным»**

**Содержание**

[1. Сервисы Информационной системы «Контроля доступа к персональным данным» 2](#_Toc108006786)

[2. Сервис 1. Запрос доступа к персональным данным 3](#_Toc108006787)

[2.1. Схема функционирования сервиса запрос доступа к персональным данным 3](#_Toc108006788)

[2.2. Описание форматов взаимодействия с сервисом запроса персональных данных 4](#_Toc108006789)

[2.3. Пример запроса и ответа сервиса запроса доступа персональных данных 12](#_Toc108006790)

[3. Сервис 2. Получение истории согласий на доступ к персональным данным 15](#_Toc108006791)

[3.1. Схема функционирования сервиса получения истории согласий на доступ к персональным данным 15](#_Toc108006792)

[3.2. Описание форматов взаимодействия с сервисом получения истории согласий на доступ к персональным данным 15](#_Toc108006793)

[3.3. Пример запроса и ответа сервиса получения истории согласий на доступ к персональным данным 17](#_Toc108006794)

[4. Сервис 3. Отзыв согласия на доступ к персональным данным 21](#_Toc108006795)

[4.1. Схема функционирования сервиса отзыва согласия на доступ к персональным данным 21](#_Toc108006796)

[4.2. Описание форматов взаимодействия с сервисом отзыва согласия на доступ к персональным данным 22](#_Toc108006797)

[4.3. Пример запроса и ответа сервиса отзыва согласия на доступ к персональным данным 23](#_Toc108006798)

[5. Сервис 4. Проверка отзыва согласия на доступ к персональным данным 24](#_Toc108006799)

[5.1. Схема функционирования сервиса проверки отзыва согласия на доступ к персональным данным 24](#_Toc108006800)

[5.2. Описание форматов взаимодействия с сервисом проверки отзыва согласия на доступ к персональным данным 25](#_Toc108006801)

[5.3. Пример запроса и ответа сервиса проверки отзыва согласия на доступ к персональным данным 26](#_Toc108006802)

[6. Сервис 5. Сервис получения истории согласий, отзыва согласия, проверки согласия 27](#_Toc108006803)

# **Сервисы Информационной системы «Контроля доступа к персональным данным»**

Таблица 1. Сервисы Информационной системы «Контроля доступа к персональным данным» (далее – КДП).

|  |  |  |
| --- | --- | --- |
| **№ п.п.** | **Сервисы** | |
| **1** | Наименование | Запрос доступа к персональным данным |
| Ключ сервиса в Smart Bridge | KDP\_SERVICE |
| Режим взаимодействия | Синхронный |
| **2** | Наименование | Получение истории согласий на доступ к персональным данным |
| Ключ сервиса в Smart Bridge | KDP\_PERSONALDATA |
| Режим взаимодействия | Синхронный |
| **3** | Наименование | Отзыв согласия на доступ к персональным данным |
| Ключ сервиса в Smart Bridge | KDP\_REVOKE |
| Режим взаимодействия | Синхронный |
| **4** | Наименование | Проверка согласия на доступ к персональным данным |
| Ключ сервиса в Smart Bridge | KDP\_CHECKREVOKE |
| Режим взаимодействия | Синхронный |
| **5** | Наименование | Универсальный сервис получения истории согласий, отзыва согласия, проверки согласия |
| Ключ сервиса в Smart Bridge | KDP\_UNIVERSAL |
| Режим взаимодействия | Синхронный |

# **Сервис 1. Запрос доступа к персональным данным**

## **Схема функционирования сервиса запрос доступа к персональным данным**

**Основной сценарий сервиса:**

1. Информационная система/Организация, запрашивающая доступ к персональным данным (далее - Инициатор) направляет в КДП запрос на доступ к персональным данным;
2. КДП проверяет значение поля запроса omit-sms (запрос на доступ к персональным данным был заранее получен у субъекта персональных данных);
3. Если значение поля запроса omit-sms соответствует false, тогда:
   1. КДП сразу отправляет Инициатору ответ с status = PENDING;
   2. КДП отправляет запрос и получает ответ от Базы мобильных граждан (далее – БМГ);
   3. КДП получив номер из БМГ отправляет SMS субъекту персональных данных;
   4. КДП получив ответ от субъекта персональных данных, сохраняет ответ в blockchain;
   5. Инициатор при отправке повторно запроса на доступ к персональным данным получает ответ:

В случае, положительного ответа субъекта персональных данных:

status = VALID

code = <СГЕНЕРИРОВАННЫЙ ТОКЕН БЕЗОПАСНОСТИ>

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

В случае, отрицательного ответа субъекта персональных данных:

status = INVALID

code = <ПУСТО>

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

status = PENDING

code = <ПУСТО>

1. Если значение поля omit-sms соответствует true, тогда:
   1. КДП проверяет наличие токена верификации организации;
   2. КДП проверяет подпись токена верификации организации;
   3. КДП проверяет соответствие БИН в токене верификации организации и БИН указанный в запросе (Request);
   4. КДП проверяет способ получения доступа к персональным данным;
   5. КДП проверяет дату формирования токена верификации организации;
   6. В случае, прохождения всех проверок, Инициатору отправляется ответ:

status = VALID

code = <СГЕНЕРИРОВАННЫЙ ТОКЕН БЕЗОПАСНОСТИ>

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

**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:**

В случаях, когда разрешение на доступ к персональным данным было раннее получено у субъекта персональных данных (omit-sms=true), альтернативный сценарий может принимать следующие значения:

1. Токен верификации организации не найдет:

status = ERROR\_TV\_NOTFOUND

code = <ПУСТО>

1. В токене верификации подпись Invalid или данные из токена верификации не извлекаются:

status = ERROR\_TV\_NOTRETRIEVED

code = <ПУСТО>

1. БИН в токене верификации организации не соответствует БИН в запросе:

status = ERROR\_TV\_BIN\_NOTMATCH

code = <ПУСТО>

1. Способ получения доступа к персональным данным не соответствует значению из списка (Bio/Ds/Otp/DID/PC):

status = ERROR\_TV\_NOTFOUND

code = <ПУСТО>

1. Дата формирования токена верификации организации больше текущей даты:

status = ERROR\_TV\_MORECDATE

code = <ПУСТО>

В случаях, когда разрешение на доступ к персональным данным осуществляется средствами КДП, путем отправки и получения SMS сообщения (omit-sms=false), альтернативный сценарий может 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>

1. Ошибка, доступа к сервису База мобильных граждан:

status = ERROR\_MCDB\_SERVICE

code = <ПУСТО>

1. Ошибка, доступа к сервису SMS-шлюз электронного правительства 1414:

status = ERROR\_MGOV\_SMS\_GW

code = <ПУСТО>

1. Ошибка, не БИН и наименование организации не соответствуют предоставленным:

status = ERROR\_MISMATCH\_BINORNAME

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) проверить подпись токена безопасности на валидность;
   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).

## **Описание форматов взаимодействия с сервисом запроса персональных данных**

**Структура сервиса запроса персональных данных представляет (xsd-схема):**

<?xml version="1.0" encoding="UTF-8"?>

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"

xmlns="http://service.2fa-chain.kz/ns/kdp"

targetNamespace="http://service.2fa-chain.kz/ns/kdp" elementFormDefault="qualified">

<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:long" 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:element name="ovt" type="xs:string">

<xs:annotation>

<xs:documentation>Jwt токен, заполняется если omit-sms=true

</xs:documentation>

</xs:annotation>

</xs:element>

<xs:element name="operator\_bin" type="xs:string">

<xs:annotation>

<xs:documentation>БИН оператора данных

</xs:documentation>

</xs:annotation>

</xs:element>

<xs:element name="t\_operation" type="operation">

<xs:annotation>

<xs:documentation>Тип операции

</xs:documentation>

</xs:annotation>

</xs:element>

<xs:element name="d\_operation" type="xs:string">

<xs:annotation>

<xs:documentation>Измененные данные

</xs:documentation>

</xs:annotation>

</xs:element>

</xs:sequence>

</xs:complexType>

<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>

<xs:simpleType name="user-data-status">

<xs:restriction base="xs:string">

<xs:enumeration value="VALID">

<xs:annotation>

<xs:documentation>

Доступ предоставлен

</xs:documentation>

</xs:annotation>

</xs:enumeration>

<xs:enumeration value="INVALID">

<xs:annotation>

<xs:documentation>

В доступе отказано

</xs:documentation>

</xs:annotation>

</xs:enumeration>

<xs:enumeration value="PENDING">

<xs:annotation>

<xs:documentation>

Ожидание ответа субъекта персональных данных

</xs:documentation>

</xs:annotation>

</xs:enumeration>

<xs:enumeration value="TIMEOUT">

<xs:annotation>

<xs:documentation>

Время ожидания ответа субъекта персональных данных истекло

</xs:documentation>

</xs:annotation>

</xs:enumeration>

<xs:enumeration value="NOT\_FOUND">

<xs:annotation>

<xs:documentation>

По указанному в запросе ИИН отсутствует номер телефона в БМГ

</xs:documentation>

</xs:annotation>

</xs:enumeration>

<xs:enumeration value="ERROR">

<xs:annotation>

<xs:documentation>

Ошибка, полученная при отправке SMS

</xs:documentation>

</xs:annotation>

</xs:enumeration>

<xs:enumeration value="ERROR\_MCDB\_SERVICE">

<xs:annotation>

<xs:documentation>

Ошибка, полученная при обращении к БМГ

</xs:documentation>

</xs:annotation>

</xs:enumeration>

<xs:enumeration value="ERROR\_MGOV\_SMS\_GW">

<xs:annotation>

<xs:documentation>

Ошибка, полученная при обращении к СМС-шлюзу

</xs:documentation>

</xs:annotation>

</xs:enumeration>

<xs:enumeration value="ERROR\_TV\_NOT\_FOUND">

<xs:annotation>

<xs:documentation>

Ошибка ERROR\_TV\_NOT\_FOUND

</xs:documentation>

</xs:annotation>

</xs:enumeration>

<xs:enumeration value="ERROR\_TV\_NOT\_FOUND">

<xs:annotation>

<xs:documentation>

Ошибка ERROR\_TV\_NOTRETRIEVED

</xs:documentation>

</xs:annotation>

</xs:enumeration>

<xs:enumeration value="ERROR\_TV\_BIN\_NOTMATCH">

<xs:annotation>

<xs:documentation>

Ошибка ERROR\_TV\_BIN\_NOTMATCH

</xs:documentation>

</xs:annotation>

</xs:enumeration>

<xs:enumeration value="ERROR\_TV\_MORECDATE">

<xs:annotation>

<xs:documentation>

Ошибка ERROR\_TV\_MORECDATE

</xs:documentation>

</xs:annotation>

</xs:enumeration>

</xs:restriction>

</xs:simpleType>

<xs:simpleType name="operation">

<xs:restriction base="xs:string">

<xs:enumeration value="UPDATE">

<xs:annotation>

<xs:documentation>

Обновление

</xs:documentation>

</xs:annotation>

</xs:enumeration>

<xs:enumeration value="INSERT">

<xs:annotation>

<xs:documentation>

Добавление

</xs:documentation>

</xs:annotation>

</xs:enumeration>

<xs:enumeration value="DELETE">

<xs:annotation>

<xs:documentation>

Удаление

</xs:documentation>

</xs:annotation>

</xs:enumeration>

</xs:restriction>

</xs:simpleType>

</xs:schema>

**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\* - Перечень сервисов (ServiceID - ШЭП), у которых будут запрашиваться персональные данные (для государственных ИС) или наименование персональных данных (например, ФИО запросить ИИН) (для частных ИС);
7. personal\_data\_name\* – Наименование персональных запрашиваемых по субъекту персональных данных;
8. expiresIn\* - Время действия токена безопасности, указывается в миллисекундах (зависит от регламентного времени оказания услуг);
9. omit-sms\* – Запрос персональных данных получен иным путем (значение true возможно только для организаций получивших от уполномоченного органа в сфере контроля персональных данных, разрешения на самостоятельное получение разрешения от субъекта персональных данных).
10. ovt\*\* – Токен верификации организации получившего доступ разрешение на получение разрешения от субъекта персональных данных (данное поле является не обязательным и включается в запрос только теми организациями которые получили от уполномоченного органа в сфере контроля персональных данных, разрешения на самостоятельное получение разрешения от субъекта персональных данных).
11. respon-uin – ИИН опекуна, родителя ответственного за недееспособного ребенка и т.д.
12. operator\_bin - БИН/ИИН организации оператора данных.
13. t\_operation - Тип операции, возможные значения UPDATE (обновление персональных данных), INSERT (добавление персональных данных), DELETE (удаление персональных данных), null/пусто (просмотр персональных данных).
14. d\_operation - Данные которые должны быть изменены и/или добавлены и/или удалены, при значениях поля t\_operation= UPDATE/ INSERT/ DELETE.

\* - поля являющиеся обязательными для заполнения;

\*\* - поле обязательно в случае если значение поля omit-sms равняется true, в иных случаях значение поля не указывается.

Токен верификации организации должен представлять собой данные в формате json в виде jwt-токена подписанного ЭЦП организации отправляющей запрос и включать следующие параметры:

**Общий вид:**

Блок header (algorithm & token type):

{

"alg": "ES256",

"typ": "JWT"

}

Блок payload (data):

{

"cbin": <БИН\_организации>,

"mcheck": <способ\_получения\_подтверждения\_Bio/Ds/Otp/DID/PC>,

"iat": <дата\_время\_создания\_токена>,

"exp":<дата\_время\_окончания\_действия\_токена>

}

где:

1. cbin – БИН организации запросившая доступ к персональных данным (должен соответствовать полю company\_bin запроса (Request));
2. mcheck – способ которым организация получила подтверждение на доступ к персональным данным у субъекта персональных данных.

Возможные значения:

* 1. Bio (Система биометрии организации);
  2. Ds (Электронно-цифровая подпись);
  3. Otp (Одноразовый пароль OTP);
  4. DID (Система Digital ID);
  5. PC (Бумажный носитель информации).

1. iat – дата время создания токена верификации организации в формате Unix Time Stamp (обязательное поле JWT стандарта);
2. exp – дата время окончания действия токена верификации организации в формате Unix Time Stamp (обязательное поле JWT стандарта) (значение должно быть больше iat на один час).

**Пример:**

{

"alg": "ES256",

"typ": "JWT"

}

{

"cbin": 012345678909,

"mcheck": Bio,

"iat": 1631925900,

"exp": 1631929500

}

**ВАЖНО:** Публичный ключ ЭЦП, организации, которая получила от уполномоченного органа в сфере контроля персональных данных, разрешения на самостоятельное получение разрешения от субъекта персональных данных, должен быть передан в КДП для проверки достоверности подписи. В КДП ведется реестр организаций и публичных ключей для проверки ЭЦП.

**ВАЖНО:** Для проверки формирования токена верификации организации можно использовать ресурс https://jwt.io.

**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 Базе мобильных граждан;
   6. ERROR – Ошибка, полученная при отправке SMS;
   7. ERROR\_TV\_NOTRETRIEVED - Ошибка, невозможно извлечь данные из токена верификации (jwt)
   8. ERROR\_TV\_BIN\_NOTMATCH - Ошибка, значение параметра cbin в токене верификации не соответствует значением поля company\_bin запроса
   9. ERROR\_TV\_NOTFOUND - Ошибка, значение параметра mcheck в токене верификации не равно одному из следующих значений: Bio, Ds, Otp, DID, PC
   10. ERROR\_TV\_MORECDATE - Ошибка, значение параметра iat в токене верификации больше текущей даты
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.

**ВАЖНО**: Все даты и время в токене безопасности, указанные по Гринвичу.

## **Пример запроса и ответа сервиса запроса доступа персональных данных**

**Запрос:**

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><SOAP-ENV:Header xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"/><soap:Body>

<SendMessage xmlns="http://bip.bee.kz/SyncChannel/v10/Types">

<request xmlns="">

<requestInfo>

<messageId>dfcf789636a9477ebcc7573c001ced44</messageId>

<serviceId>KDP\_SERVICE</serviceId>

<messageDate>2021-07-29T17:18:38.7371976+06:00</messageDate>

<sender>

<senderId>login</senderId>

<password>password</password>

</sender>

<sessionId>{dff078b0-2ab7-44ae-aa50-1b7fc72ba941}</sessionId>

</requestInfo>

<requestData>

<data xsi:type="getUserDataRequest">

<uin>000000000000</uin>

<company>Наименование организации</company>

<company\_bin>012345678909</company\_bin>

<company\_responsible>Наименование организации</company\_responsible>

<employee\_name>Фамилия Имя Отчество</employee\_name>

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

<personal\_data\_name>Фамилия Имя Отчество</personal\_data\_name>

<expiresIn>600000</expiresIn>

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

</data>

</requestData>

</request>

</SendMessage></soap:Body></soap:Envelope>

**Ответ:**

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

<soap:Body><ns2:SendMessageResponse xmlns:ns2="http://bip.bee.kz/SyncChannel/v10/Types" xmlns:ns3="http://service.2fa-chain.kz/ns/kdp" xmlns:ns4="http://sms.egov.inessoft.kz/common/v10/Types" xmlns:ns5="http://smartbridge.b10.kz">

<response>

<responseInfo>

<messageId>fe60a2a7-7014-44f3-8d33-5eebe045f83b</messageId>

<responseDate>2021-08-04T06:25:07.413</responseDate>

<status>

<code>1</code>

<message>SUCCESS</message>

</status>

</responseInfo>

<responseData>

<data xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="ns3:getUserDataResponse">

<ns3:status>VALID</ns3:status>

<ns3:code>eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1aW4iOiAiODEwOTE4MzUwMTM1IiwgInNpZCI6ICJNQ0RCX1NFUlZJQ0UiLCAiZHRzIjogIjIwMjEtMDgtMDRUMDY6MjQ6NTkuMjA3IiwgImR0ZSI6ICIyMDIxLTA4LTA0VDA2OjM0OjU5LjIwNyIsICJiaW5jIjogIjEyMzQ1Njc4IiwgImlhdCI6IDE2MjgwNTgyOTkyMDcsICJleHAiOiAxNjI4MDU4ODk5MjA3fQ.kHsURkJdTzERKamS9BlUf9t3TTrflkMbKXZCjAFUALt-dh70B-rDYfgwf5\_3EY2ozqqhNP6qLNebsC-G-gIruGAfWK6y8fGHMDD4LxEAelu27oOmUQDlV5ruYpAeGUDCa0mNshlJmkJ7zlkqAp32B7GRePodf7zUh6wfr2WceCjW8SycRyY\_EtJpCwx-0RIJZleA69AR8tcxZvKaWlFdY\_o\_b4-9IokWnTG4h6v8GQqgJV\_HBJAHUR7hjEpSxdmac\_Jz5sotd30F6RNIg7qBkg3ShAOQv6ce4\_0n3QuUGxHTgOkUAhzxgtEsNpe4vxqAjfyhqW6YY3zGUXWBqT3apw</ns3:code>

<ns3:public-key>-----BEGIN CERTIFICATE-----

MIIG6zCCBNOgAwIBAgIUb6w9cFeIv32H/2Yr+zwRsL7sescwDQYJKoZIhvcNAQEL

BQAwUjELMAkGA1UEBhMCS1oxQzBBBgNVBAMMOtKw0JvQotCi0KvSmiDQmtCj05jQ

m9CQ0J3QlNCr0KDQo9Co0Ksg0J7QoNCi0JDQm9Cr0pogKFJTQSkwHhcNMjEwMzEw

MTExNDU3WhcNMjIwMzEwMTExNDU3WjCCASExJjAkBgNVBAMMHdCW0JXQotCf0JjQ

odCe0JIg0J3Qo9Cg0JHQldCaMRkwFwYDVQQEDBDQltCV0KLQn9CY0KHQntCSMRgw

FgYDVQQFEw9JSU45MTA4MTAzNTAwODMxCzAJBgNVBAYTAktaMXgwdgYDVQQKDG/Q

otCe0JLQkNCg0JjQqdCV0KHQotCS0J4g0KEg0J7Qk9Cg0JDQndCY0KfQldCd0J3Q

ntCZINCe0KLQktCV0KLQodCi0JLQldCd0J3QntCh0KLQrNCuICJBUkNUSUMgVEVD

SE5PTE9HWSBHUk9VUCIxGDAWBgNVBAsMD0JJTjE4MDM0MDAyNjI2NzEhMB8GA1UE

KgwY0KHQkNCT0JDQndCU0KvQmtCe0JLQmNCnMIIBIjANBgkqhkiG9w0BAQEFAAOC

AQ8AMIIBCgKCAQEApNJqtRfz/Ze4wLMi2VjrTBJD0y/XTZoWJBWLjoUtjFULEKdr

cEhklEMYbaUYC7g/0rJHEA1LjsXcdxsbCer45UFO5WRVtNGEWW8lZ9IMdE8iKjaM

NtcCiUdNv8yKAT7F5VKUzOHwfGevFP8gi4GQjDZnK5XWV/hMrSVBPRXYvseIKqQ+

fC4WidB6nYljEdxtmxnCr6cZx/BYdO3dl4rFfSJICA3sgdbwcUtAMCID4doNesMq

0SVDQcyJMrAHpK8ooDrLTGWFydpXvQu8PFPdBiG12PVZJvFhecB1iSYSRUvsm34B

W+iGIm3/eXf1JsRGr0iC5FmFRQ8Like74gIIzQIDAQABo4IB5jCCAeIwDgYDVR0P

AQH/BAQDAgWgMCgGA1UdJQQhMB8GCCsGAQUFBwMCBggqgw4DAwQBAgYJKoMOAwME

AQIBMA8GA1UdIwQIMAaABFtqdBEwHQYDVR0OBBYEFCtRSLLHB52ihQmztz8hCrvn

devKMF4GA1UdIARXMFUwUwYHKoMOAwMCAjBIMCEGCCsGAQUFBwIBFhVodHRwOi8v

cGtpLmdvdi5rei9jcHMwIwYIKwYBBQUHAgIwFwwVaHR0cDovL3BraS5nb3Yua3ov

Y3BzMFYGA1UdHwRPME0wS6BJoEeGIWh0dHA6Ly9jcmwucGtpLmdvdi5rei9uY2Ff

cnNhLmNybIYiaHR0cDovL2NybDEucGtpLmdvdi5rei9uY2FfcnNhLmNybDBaBgNV

HS4EUzBRME+gTaBLhiNodHRwOi8vY3JsLnBraS5nb3Yua3ovbmNhX2RfcnNhLmNy

bIYkaHR0cDovL2NybDEucGtpLmdvdi5rei9uY2FfZF9yc2EuY3JsMGIGCCsGAQUF

BwEBBFYwVDAuBggrBgEFBQcwAoYiaHR0cDovL3BraS5nb3Yua3ovY2VydC9uY2Ff

cnNhLmNlcjAiBggrBgEFBQcwAYYWaHR0cDovL29jc3AucGtpLmdvdi5rejANBgkq

hkiG9w0BAQsFAAOCAgEAZeK6Tty6eDUXDSx1HfohQAQlCIpfuOv0ZgntbbReLMEw

T0lqzSwlegZgzwLQ98YErC3fcrImf8g1ewowrPzVmNY569ZmofJ/+lD0+s7Pg33E

+9qVERlNAuVhUxquqBHBO2nezFOAJmr6To2zNuRILAJoZjJXTPMJiVXH49k8ZQP/

qZd2bzJKVFS97DB69p6znSUhx92fSz2HjGDjqBoIUzdz1YpuLoCgsOhXxImkqVx+

iQPo8uV7PgEP0yWuAs7lEdnXduIdTnvRskWvpESLoOAp0OW93Jk8R9hb4PmWCScw

x4wF5plvMaEnDDzNnizU3hfRMt/SmIqzSwPZvPDibjNBYktni7LPTrr/4U82ViTH

SUgrbXzSKpa8gZKmR/aaaD7koouelfNy3ESti9+FGujYKl3ZO18ezTnlfqeO4TSO

GXoJrEVs7MAOS3C6Uh5ptz9ZUlBZNj+br0WiDA4E/dD+7QtMMg0Zz27F1mNSurX3

Ihxms0AcCWG1/L6x0CU0OB847bx0+NyxGplQncnE2ZD5fokV70IgldSGEGBMlvSH

D5Zvtbzl1XJM4RdKvTDeVdeltltCcZSiy6Oa15MIfss5WYTvj+URjGeQJ4rLy16v

lohNxImGSXp3UVp+jukilHJWKq4kRRTZTBF7F+ZvHhAVUTaH4v4udtTnlHKr/PM=

-----END CERTIFICATE-----

</ns3:public-key>

</data>

</responseData>

</response>

</ns2:SendMessageResponse>

</soap:Body></soap:Envelope>

# **Сервис 2. Получение истории согласий на доступ к персональным данным**

## **Схема функционирования сервиса получения истории согласий на доступ к персональным данным**

**Основной сценарий сервиса:**

1. Информационная система/Организация (далее - Инициатор) направляет в КДП запрос на получение согласий на доступ к персональным данным;
2. КДП извлекает данные из запроса и проверяет значения полей uin, start\_date, end\_date.
3. КДП формирует выборку данных согласно значениям (start\_date, end\_date) запроса, при условии:
   1. Если start\_date и end\_date запроса являются пустыми, КДП формирует набор данных за весь период по uin;
   2. Если start\_date запроса являются пустым, КДП формирует набор данных за весь период по uin;
   3. Если end\_date запроса являются пустым, КДП формирует набор данных в период c start\_date по текущую дату по uin.
4. КДП формирует json и закодирует при помощи ЭЦП в jwt-формат;
5. КДП формирует xml и отправляется [ответ](https://docs.google.com/document/d/1nE1RyuAXXtNWcYKoEFOfZy5WTD-9ZqkHNgH-3DkuJEU/edit#heading=h.c7mup0bw1xwz).

## **Описание форматов взаимодействия с сервисом получения истории согласий на доступ к персональным данным**

**Структура сервиса получения истории согласий на доступ к персональным данным (xsd-схема):**

<xs:complexType name="personalDataRequest">

<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="start\_date" minOccurs="0" type="xs:dateTime">

<xs:annotation>

<xs:documentation>Дата начала</xs:documentation>

</xs:annotation>

</xs:element>

<xs:element name="end\_date" minOccurs="0" type="xs:dateTime">

<xs:annotation>

<xs:documentation>Дата окончания</xs:documentation>

</xs:annotation>

</xs:element>

</xs:sequence>

</xs:complexType>

<xs:complexType name="personalDataResponse">

<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="r\_pdata" type="xs:string" minOccurs="0">

<xs:annotation>

<xs:documentation>Данные, представленный в JWT-формате

</xs:documentation>

</xs:annotation>

</xs:element>

</xs:sequence>

</xs:complexType>

**Описание полей запроса (Request):**

1. uin\* - ИИН (субъекта персональных данных);
2. start\_date – Дата начала периода выгрузки истории согласий на доступ к персональным данным;
3. end\_date - Дата окончания периода выгрузки истории согласий на доступ к персональным данным.

**Описание полей ответа (Response):**

1. uin\* - ИИН (субъекта персональных данных);
2. r\_pdata - набор запросов (json) персональных данных в jwt-формате и подписанны ЭЦП, в блоке payload включены следующие параметры:

**Общий вид:**

Блок header (algorithm & token type):

{

"alg": "ES256",

"typ": "JWT"

}

Блок payload (data):

{

“uin”: <ИИН>,

“company”: <Наименование\_организации>,

“company\_bin”: <БИН/ИИН\_организации>,

“company\_responsible”: <Наименование\_организации\_у\_которой\_запрашиваются\_ПД>,

“employee\_name”: <ФИО\_сотрудника\_из\_организации>,

“access\_name”: <Перечень\_сервисов>,

“personal\_data\_name”: <Перечень\_ПД>,

“expiresIn”: <Время\_действия\_токена\_безопасности>,

“omit-sms”: <Запрос\_ПД\_получен\_иным\_путем>,

“ovt”: <Токен\_верификации>,

“status”: <Статус>,

“code”: <Токен\_безопасности>,

“operator\_bin”: <БИН/ИИН\_оператора>,

“t\_operation”: <Тип\_операции>,

“d\_operation”: <Измененные\_данные>

},

{

“uin”: <ИИН2>,

…

}

]

где:

1. uin - ИИН субъекта персональных данных;
2. company\_responsible - Наименование организации, у которой запрашиваются данные;
3. code - Код верификации, представленный в JWT-формате (передается в случае если доступ был предоставлен, содержит группу данных);
4. employee\_name - ФИО сотрудника из организации, запрашивающей персональные данные (третьей стороны);
5. ovt - Токен верификации организации получившего доступ разрешение на получение разрешения от субъекта персональных данных (данное поле является не обязательным и включается в запрос только теми организациями которые получили от уполномоченного органа в сфере контроля персональных данных, разрешения на самостоятельное получение разрешения от субъекта персональных данных);
6. expiresIn - Время действия токена безопасности, указывается в миллисекундах (зависит от регламентного времени оказания услуг);
7. company\_bin - БИН/ИИН организации, запрашивающей доступ к персональным данным (третьей стороны);
8. access\_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);
9. personal\_data\_name - Наименование персональных запрашиваемых по субъекту персональных данных;
10. company - Наименование организации, запрашивающей доступ к персональным данным (третьей стороны)
11. omit-sms - Запрос персональных данных получен иным путем (значение true возможно только для организаций получивших от уполномоченного органа в сфере контроля персональных данных, разрешения на самостоятельное получение разрешения от субъекта персональных данных).
12. operator\_bin - БИН/ИИН оператора данных (Это Кредитные бюро (ГКБ, ПКБ) через которых другие организации получают перс.данные),
13. t\_operation – Тип операции (возможные значения UPDATE, INSERT, DELETE, если null значит просмотр);
14. d\_operation – Измененные данные (возможные значения ТАБЛИЦА/ОБЪЕКТ].[ПОЛЕ/АТРИБУТ]=[ЗНАЧЕНИЕ]);
15. status – Статус согласия (INACTIVE - Согласие отозвано, VALID - Согласие активно).

## **Пример запроса и ответа сервиса получения истории согласий на доступ к персональным данным**

**Запрос:**

<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">

<S:Header/>

<S:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="id-d3e760ab-e2a8-4eb2-9a39-6f76cf959799">

<ns2:SendMessage xmlns:ns2="http://bip.bee.kz/SyncChannel/v10/Types" xmlns:ns3="http://service.2fa-chain.kz/ns/kdp/personalData" xmlns:ns4="http://service.2fa-chain.kz/ns/kdp/personalData">

<request>

<requestInfo>

<messageId>d47f0c73-0d7e-4196-935c-a30bb3cbcacd</messageId>

<serviceId>serviceId</serviceId>

<messageDate>2021-05-05T15:24:08.662+06:00</messageDate>

<sender>

<senderId>sendeId</senderId>

<password>password</password>

</sender>

</requestInfo>

<requestData>

<data xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="ns4:personalDataRequest">

<ns4:uin>000000000000</ns4:uin>

<ns4:start\_date>2021-01-01T15:24:08.662+06:00</ns4:start\_date>

<ns4:end\_date>2021-05-05T15:24:08.662+06:00</ns4:end\_date>

</data>

</requestData>

</request>

</ns2:SendMessage>

</S:Body>

</S:Envelope>

**Ответ:**

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

<soap:Body>

<ns2:SendMessageResponse xmlns:ns2="http://bip.bee.kz/SyncChannel/v10/Types" xmlns:ns3="http://service.2fa-chain.kz/ns/kdp" xmlns:ns4="http://service.2fa-chain.kz/ns/kdp/personalData" xmlns:ns5="http://smartbridge.b10.kz" xmlns:ns6="http://sms.egov.inessoft.kz/common/v10/Types">

<response>

<responseInfo>

<messageId>3a7c0351-f901-4aa9-b77e-91d30d75c7e9</messageId>

<responseDate>2022-05-12T19:14:07.060059300</responseDate>

<status>

<code>1</code>

<message>SUCCESS</message>

</status>

</responseInfo>

<responseData>

<data xsi:type="ns4:personalDataResponse" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<ns4:uin>000000000000</ns4:uin>

<ns4:r\_pdata>eyJ0eXAiOiJKV1QiLCJhbGciOiJFUzI1NiJ9..UyR\_h5dG20NuQk9EDfQYZKDd5N\_ZB5Und\_FBB\_YrBLnHulZNKBnm8dS6fyeU-Xv7EKfQ3YfkgryhsjXxOadchQ</ns4:r\_pdata>

</data>

</responseData>

</response>

</ns2:SendMessageResponse>

</soap:Body>

</soap:Envelope>

# **Сервис 3. Отзыв согласия на доступ к персональным данным**

## **Схема функционирования сервиса отзыва согласия на доступ к персональным данным**

**Основной сценарий сервиса:**

1. Информационная система/Организация (далее - Инициатор) направляет в КДП запрос на получение согласий на доступ к персональным данным;
2. КДП извлекает данные из запроса и проверяет значения полей uin, code на наличие данных.
3. Если данные uin и code запроса не являются пустыми, КДП выполняется поиск данных в блокчейне согласно значениям (uin, code).
4. Если в блокчейне данные найдены по значениям полей uin и code, записи присвоить статус INACTIVE.

**Альтернативные сценарии:**

1. Если uin и code запроса являются пустыми, КДП формирует ответ со статусом ERROR\_NO\_DATA;
2. Если uin запроса являются пустым, КДП формирует ответ со статусом ERROR\_NO\_IIN;
3. Если code запроса являются пустым, КДП формирует ответ со статусом ERROR\_NO\_CODE;
4. Если данные в блокчейне по значениям uin и code не были найдены, КДП формирует ответ со статусом NOT\_FOUND;
5. Если в блокчейне данные найдены по значениям полей uin и code, но записи по каким либо причинам не был присвоен статус INACTIVE, КДП формирует ответ со статусом ERROR\_NOTSET.

## **Описание форматов взаимодействия с сервисом отзыва согласия на доступ к персональным данным**

**Структура сервиса отзыва согласия на доступ к персональным данным (xsd-схема):**

<xs:complexType name="revokeRequest">

<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="code" minOccurs="1" type="xs:string">

<xs:annotation>

<xs:documentation>Токен безопасности (JWT)</xs:documentation>

</xs:annotation>

</xs:element>

</xs:sequence>

</xs:complexType>

<xs:complexType name="revokeResponse">

<xs:sequence>

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

<xs:annotation>

<xs:documentation>Токен безопасности (JWT)</xs:documentation>

</xs:annotation>

</xs:element>

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

<xs:annotation>

<xs:documentation>Статус: SUCCESS - Отзыв согласия успешно произведено;

ERROR\_NO\_DATA - Ошибка, значения uin и code запроса являются пустыми;

ERROR\_NO\_IIN - Ошибка, значение uin запроса являются пустым;

ERROR\_NO\_CODE - Ошибка, значение code запроса являются пустым;

NOT\_FOUND - Согласно значения uin и code данные не найдены;

ERROR\_NOTSET - Ошибка, согласие не было отозвано</xs:documentation>

</xs:annotation>

</xs:element>

</xs:sequence>

</xs:complexType>

**Описание полей запроса (Request):**

1. uin\* - ИИН (субъекта персональных данных);
2. code\* – Токен безопасности (JWT) полученный ранее.

**Описание полей ответа (Response):**

1. code\* -Токен безопасности (JWT);
2. status\* - Статус, который может принимать одно из следующих значений:

SUCCESS - Отзыв согласия успешно произведено;

ERROR\_NO\_DATA - Ошибка, значения uin и code запроса являются пустыми;

ERROR\_NO\_IIN - Ошибка, значение uin запроса являются пустым;

ERROR\_NO\_CODE - Ошибка, значение code запроса являются пустым;

NOT\_FOUND - Согласно значения uin и code данные не найдены;

ERROR\_NOTSET - Ошибка, согласие не было отозвано.

\* - поля являющиеся обязательными для заполнения.

## **Пример запроса и ответа сервиса отзыва согласия на доступ к персональным данным**

**Запрос:**

<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">

<S:Header/>

<S:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="id-d3e760ab-e2a8-4eb2-9a39-6f76cf959799">

<ns2:SendMessage xmlns:ns2="http://bip.bee.kz/SyncChannel/v10/Types" xmlns:ns3="http://service.2fa-chain.kz/ns/kdp/personalData" xmlns:ns4="http://service.2fa-chain.kz/ns/kdp/personalData">

<request>

<requestInfo>

<messageId>d47f0c73-0d7e-4196-935c-a30bb3cbcacd</messageId>

<serviceId>serviceId</serviceId>

<messageDate>2021-05-05T15:24:08.662+06:00</messageDate>

<sender>

<senderId>sendeId</senderId>

<password>password</password>

</sender>

</requestInfo>

<requestData>

<data xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="ns4:revokeRequest">

<ns4:uin>000000000000</ns4:uin>

<ns4:code>eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1aW4iOiAiODgwOTA3MzUwNjgzIiwgInNpZCI6ICJNQ0RCX1NFUlZJQ0UiLCAiZHRzIjogIjIwMjEtMDktMDFUMDA6MDQ6MzIuMjE4MDExMTAwIiwgImR0ZSI6ICIyMDIxLTA5LTAxVDAwOjE0OjMyLjIxODAxMTEwMCIsICJiaW5jIjogIjEyMzQ1Njc4IiwgImlhdCI6IDE2MzA0MzMwNzIyMTgsICJleHAiOiAxNjMwNDMzNjcyMjE4fQ.OgtdOqMFUMaf38WniLvpeUEqC8mPHZp8dWTFo0SuMDOgtDmFiaTplV-v2fhDXRKfg0GRxLyh9BYrhkKcU6bgMr\_3hha9qywtiTLUuYA3tvDObTnpaLycitVGcDNCyqonTug4-EPtlb4buDEpwHIJoeicRp0gJFUKkaSST9pjfyI9yWDJUTuPIK7ICMAkr6009xH8\_X0x7U-KixKAA6nF9Sc-4kKVz-Ba5MqO8w7EGWVL8nLEkx4diNAzX\_WR2uFkKN-kQWBnSBITWjbIQSTacwOW1D6B8GupjAIJjke4hp4gz8a6SfFAy\_tmgoVTFGmk2IWeahKzFyS7-0j66HG0zQ</ns4:code>

</data>

</requestData>

</request>

</ns2:SendMessage>

</S:Body>

</S:Envelope>

**Ответ:**

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

<soap:Body>

<ns2:SendMessageResponse xmlns:ns2="http://bip.bee.kz/SyncChannel/v10/Types" xmlns:ns3="http://service.2fa-chain.kz/ns/kdp" xmlns:ns4="http://service.2fa-chain.kz/ns/kdp/personalData" xmlns:ns5="http://smartbridge.b10.kz" xmlns:ns6="http://sms.egov.inessoft.kz/common/v10/Types">

<response>

<responseInfo>

<messageId>b71dae90-e817-4f60-bf3f-a990c79c6077</messageId>

<responseDate>2022-05-12T19:36:28.391423500</responseDate>

<status>

<code>1</code>

<message>SUCCESS</message>

</status>

</responseInfo>

<responseData>

<data xsi:type="ns4:revokeResponse" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<ns4:code>eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1aW4iOiAiODgwOTA3MzUwNjgzIiwgInNpZCI6ICJNQ0RCX1NFUlZJQ0UiLCAiZHRzIjogIjIwMjEtMDktMDFUMDA6MDQ6MzIuMjE4MDExMTAwIiwgImR0ZSI6ICIyMDIxLTA5LTAxVDAwOjE0OjMyLjIxODAxMTEwMCIsICJiaW5jIjogIjEyMzQ1Njc4IiwgImlhdCI6IDE2MzA0MzMwNzIyMTgsICJleHAiOiAxNjMwNDMzNjcyMjE4fQ.OgtdOqMFUMaf38WniLvpeUEqC8mPHZp8dWTFo0SuMDOgtDmFiaTplV-v2fhDXRKfg0GRxLyh9BYrhkKcU6bgMr\_3hha9qywtiTLUuYA3tvDObTnpaLycitVGcDNCyqonTug4-EPtlb4buDEpwHIJoeicRp0gJFUKkaSST9pjfyI9yWDJUTuPIK7ICMAkr6009xH8\_X0x7U-KixKAA6nF9Sc-4kKVz-Ba5MqO8w7EGWVL8nLEkx4diNAzX\_WR2uFkKN-kQWBnSBITWjbIQSTacwOW1D6B8GupjAIJjke4hp4gz8a6SfFAy\_tmgoVTFGmk2IWeahKzFyS7-0j66HG0zQ</ns4:code>

<ns4:status>SUCCESS</ns4:status>

</data>

</responseData>

</response>

</ns2:SendMessageResponse>

</soap:Body>

</soap:Envelope>

# **Сервис 4. Проверка отзыва согласия на доступ к персональным данным**

## **Схема функционирования сервиса проверки отзыва согласия на доступ к персональным данным**

**Основной сценарий сервиса:**

1. Информационная система/Организация (далее - Инициатор) направляет в КДП запрос на проверку отзыва согласия на доступ к персональным данным;
2. КДП извлекает данные из запроса и проверяет значения полей uin, code на наличие данных.
3. Если данные uin и code запроса не являются пустыми, КДП выполняется поиск данных в блокчейне согласно значениям (uin, code).
4. Если в блокчейне данные найдены по значениям полей uin и code, а также статус НЕ равен INACTIVE, КДП формирует ответ со статусом ACTIVE.

**Альтернативные сценарии:**

1. Если uin и code запроса являются пустыми, КДП формирует ответ со статусом ERROR\_NO\_DATA;
2. Если uin запроса являются пустым, КДП формирует ответ со статусом ERROR\_NO\_IIN;
3. Если code запроса являются пустым, КДП формирует ответ со статусом ERROR\_NO\_CODE;
4. Если данные в блокчейне по значениям uin и code не были найдены, КДП формирует ответ со статусом NOT\_FOUND;

## **Описание форматов взаимодействия с сервисом проверки отзыва согласия на доступ к персональным данным**

**Структура сервиса отзыва согласия на доступ к персональным данным (xsd-схема):**

<xs:complexType name="checkRevokeRequest">

<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="code" minOccurs="1" type="xs:string">

<xs:annotation>

<xs:documentation>Токен безопасности (JWT)</xs:documentation>

</xs:annotation>

</xs:element>

</xs:sequence>

</xs:complexType>

<xs:complexType name="checkRevokeResponse">

<xs:sequence>

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

<xs:annotation>

<xs:documentation>Токен безопасности (JWT)</xs:documentation>

</xs:annotation>

</xs:element>

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

<xs:annotation>

<xs:documentation>Статус: INACTIVE - Согласие отозвано;

ERROR\_NO\_DATA - Ошибка, значения uin и code запроса являются пустыми;

ERROR\_NO\_IIN - Ошибка, значение uin запроса являются пустым;

ERROR\_NO\_CODE - Ошибка, значение code запроса являются пустым;

NOT\_FOUND - Согласно значения uin и code данные не найдены;

ACTIVE - Согласие активно.</xs:documentation>

</xs:annotation>

</xs:element>

</xs:sequence>

</xs:complexType>

**Описание полей запроса (Request):**

1. uin\* - ИИН (субъекта персональных данных);
2. code\* – Токен безопасности (JWT) полученный ранее.

**Описание полей ответа (Response):**

1. code\* -Токен безопасности (JWT);
2. status - Статус, который может принимать одно из следующих значений:

INACTIVE - Согласие отозвано;

ERROR\_NO\_DATA - Ошибка, значения uin и code запроса являются пустыми;

ERROR\_NO\_IIN - Ошибка, значение uin запроса являются пустым;

ERROR\_NO\_CODE - Ошибка, значение code запроса являются пустым;

NOT\_FOUND - Согласно значения uin и code данные не найдены;

ACTIVE - Согласие активно.

## **Пример запроса и ответа сервиса проверки отзыва согласия на доступ к персональным данным**

**Запрос:**

<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">

<S:Header/>

<S:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="id-d3e760ab-e2a8-4eb2-9a39-6f76cf959799">

<ns2:SendMessage xmlns:ns2="http://bip.bee.kz/SyncChannel/v10/Types" xmlns:ns3="http://service.2fa-chain.kz/ns/kdp/personalData" xmlns:ns4="http://service.2fa-chain.kz/ns/kdp/personalData">

<request>

<requestInfo>

<messageId>d47f0c73-0d7e-4196-935c-a30bb3cbcacd</messageId>

<serviceId>serviceId</serviceId>

<messageDate>2021-05-05T15:24:08.662+06:00</messageDate>

<sender>

<senderId>sendeId</senderId>

<password>password</password>

</sender>

</requestInfo>

<requestData>

<data xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="ns4:checkRevokeRequest">

<ns4:uin>0000000000000</ns4:uin>

<ns4:code>eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1aW4iOiAiODgwOTA3MzUwNjgzIiwgInNpZCI6ICJNQ0RCX1NFUlZJQ0UiLCAiZHRzIjogIjIwMjEtMDktMDFUMDA6MDQ6MzIuMjE4MDExMTAwIiwgImR0ZSI6ICIyMDIxLTA5LTAxVDAwOjE0OjMyLjIxODAxMTEwMCIsICJiaW5jIjogIjEyMzQ1Njc4IiwgImlhdCI6IDE2MzA0MzMwNzIyMTgsICJleHAiOiAxNjMwNDMzNjcyMjE4fQ.OgtdOqMFUMaf38WniLvpeUEqC8mPHZp8dWTFo0SuMDOgtDmFiaTplV-v2fhDXRKfg0GRxLyh9BYrhkKcU6bgMr\_3hha9qywtiTLUuYA3tvDObTnpaLycitVGcDNCyqonTug4-EPtlb4buDEpwHIJoeicRp0gJFUKkaSST9pjfyI9yWDJUTuPIK7ICMAkr6009xH8\_X0x7U-KixKAA6nF9Sc-4kKVz-Ba5MqO8w7EGWVL8nLEkx4diNAzX\_WR2uFkKN-kQWBnSBITWjbIQSTacwOW1D6B8GupjAIJjke4hp4gz8a6SfFAy\_tmgoVTFGmk2IWeahKzFyS7-0j66HG0zQ</ns4:code>

</data>

</requestData>

</request>

</ns2:SendMessage>

</S:Body>

</S:Envelope>

**Ответ:**

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

<soap:Body>

<ns2:SendMessageResponse xmlns:ns2="http://bip.bee.kz/SyncChannel/v10/Types" xmlns:ns3="http://service.2fa-chain.kz/ns/kdp" xmlns:ns4="http://service.2fa-chain.kz/ns/kdp/personalData" xmlns:ns5="http://smartbridge.b10.kz" xmlns:ns6="http://sms.egov.inessoft.kz/common/v10/Types">

<response>

<responseInfo>

<messageId>9638a344-59af-443e-b864-e3bcac931916</messageId>

<responseDate>2022-05-12T20:10:33.791624700</responseDate>

<status>

<code>1</code>

<message>SUCCESS</message>

</status>

</responseInfo>

<responseData>

<data xsi:type="ns4:checkRevokeResponse" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<ns4:code>eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1aW4iOiAiODgwOTA3MzUwNjgzIiwgInNpZCI6ICJNQ0RCX1NFUlZJQ0UiLCAiZHRzIjogIjIwMjEtMDktMDFUMDA6MDQ6MzIuMjE4MDExMTAwIiwgImR0ZSI6ICIyMDIxLTA5LTAxVDAwOjE0OjMyLjIxODAxMTEwMCIsICJiaW5jIjogIjEyMzQ1Njc4IiwgImlhdCI6IDE2MzA0MzMwNzIyMTgsICJleHAiOiAxNjMwNDMzNjcyMjE4fQ.OgtdOqMFUMaf38WniLvpeUEqC8mPHZp8dWTFo0SuMDOgtDmFiaTplV-v2fhDXRKfg0GRxLyh9BYrhkKcU6bgMr\_3hha9qywtiTLUuYA3tvDObTnpaLycitVGcDNCyqonTug4-EPtlb4buDEpwHIJoeicRp0gJFUKkaSST9pjfyI9yWDJUTuPIK7ICMAkr6009xH8\_X0x7U-KixKAA6nF9Sc-4kKVz-Ba5MqO8w7EGWVL8nLEkx4diNAzX\_WR2uFkKN-kQWBnSBITWjbIQSTacwOW1D6B8GupjAIJjke4hp4gz8a6SfFAy\_tmgoVTFGmk2IWeahKzFyS7-0j66HG0zQ</ns4:code>

<ns4:status>INACTIVE</ns4:status>

</data>

</responseData>

</response>

</ns2:SendMessageResponse>

</soap:Body>

</soap:Envelope>

# **Сервис 5. Сервис получения истории согласий, отзыва согласия, проверки согласия**

Сервис получения истории согласий, отзыва согласия, проверки согласия объединяет функционал и структуру запросов/ответов Сервисов 2-4.