Автоматизированная Информационная Система

<<Е-Заявление -> Е-Справка>>

Техническая инструкция сервиса, проверка апостиля по штрих-коду справки о несудимости (16 - значный код – идентификатор справки)

г. Бишкек 2023

Сервис работает посредством СМЭВ Түндүк, путем реализации веб-сервиса согласно протоколу СМЭВ.

Для получения WSDL файла необходимо обратиться по ссылке адреса в сервер безопасности СМЭВ Түндүк.

Терминология:

СМЭВ - система межведомственного электронного взаимодействия.

Сервер безопасности - Шлюз подключения к СМЭВ.

Веб-сервис разработан методом протокола SOAP.

Условные обозначения:

В этом разделе описываются заголовки SOAP, которые используются СМЭВ Түндүк.

В таблице ниже представлены заголовки СМЭВ Түндүк.

Когда клиент службы отправляет запрос на сервер безопасности, обязательно должна присутствовать одна из служб полей или centralService. Если используется поле centralService, сервер безопасности разрешает центральную службу и автоматически заполняется в поле службы идентификатором конкретной услуги, которая реализует центральную службу.

Поле	Тип	Обязательное или Опциональное	Описание
client	XRoadClientIdentifierType	Обязательное	Идентифицирует Клиента — сущность, которая инициирует вызов услуги.
service	XRoadServiceIdentifierType	Опциональное	Идентифицирует сервис, вызываемый запросом.
centralService	XRoadCentralServiceIdentifierType	Опциональное	Идентифицирует центральную службу, вызываемую запросом.
id	string	Обязательное	Уникальный идентификатор для сообщения. Рекомендуемый метод генерации сообщения ID - 30 байт случайных данных, в кодировке Base64.

userId	string	Обязательное	Пользователь, действие которого инициировало запрос. Идентификатор пользователя должен быть с двухбуквенным ISO код страны (например, KG20114199609123).
requestHash	string	Опциональное	Для ответов. Это поле содержит хэш запроса SOAP сообщения. Это поле автоматически заполняется поставщиком сервисов сервера безопасности.
requestHash/ @algorithmId	string	Обязательное	Идентифицирует хэшалгоритм, который был использован для вычисления значения запроса поля Hash. Алгоритмы обозначаются как URI перечисленные в XML-DSIG спецификации [DSI13].
issue	string	Опциональное	Идентифицирует заявление, основание или документ, который послужил основанием обращения к сервису. Это поле используется для подключения службы запросов (и ответов) к рабочим процедурам

authentication Method	string	Обязательное	Метод аутентификации
profileVersion	string	Обязательное	Версия протокола СМЭВ Түндүк. Для СМЭВ Түндүк 6 версия протокола 4.0

При ответе служба копирует все поля заголовка из запроса в ответ.

Поле requestHash используется для создания прочной связи между запросом и ответом.

Таким образом, можно подтвердить, что определенная запись реестра возвращается в ответ на определенный запрос. Используя журналы, можно восстановить и проверить пару запрос-ответ.

Поле requestHash автоматически создается сервером безопасности поставщика услуг и проверяется сервером безопасности клиента службы.

Поле authenticationMethod должно быть одним из следующих:

EID - с удостоверением личности (ID-CARD, DIGI-ID);
MID - с мобильным удостоверением личности (MOBILE-ID);
CERT - с другим сертификатом;
EXTERNAL - через стороннюю услугу (BANK-LINK);
PASSWORD - с идентификатором пользователя и паролем;
SYSTEM - когда запрос был отправлен заданием cron или другим автоматическим процессом.

Данные заголовки являются стандартными для использования СМЭВ Түндук и присутствуют во всех методах.

Описание сервиса:

VerifyApostilByCertificateBarcodeResponse ***VerifyApostilByCertificateBarcode (****VerifyApostilByCertificateBarcodeRequest* ***request)*** - Проверка апостиля по штрих-коду справки о несудимости (шестизначный бар-код).

Где:

request – параметры запроса с заголовком СМЭВ Түндук и дополнительные параметры;

documentCode - 16 значный код – идентификатор справки;

Сервиса возвращает:

Status – статус обработки данных:

a)

Code = 0;

Name = "Success";

Успешно, в этом случае возвращается объект ObjectResult где:

DocumentCode – 16 значный код – идентификатор справки;

ApostilStatus – статус апостиля;

DateOfApostil – дата апостилирования;

b)

Code = 1;

Name = " ServiceError";

Нет подключения или внутренняя ошибка!

ObjectResult = null

c)

Code = 2;

Name = " DocumentCodeMustContain16Characters";

Идентификатор справки должен содержать 16 цифр!

ObjectResult = null

d)

Code = 3;

Name = " ApostilNotFound";

Сведений не имеется!

ObjectResult = null

Пример запроса:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xro="http://x-road.eu/xsd/xroad.xsd" xmlns:iden="http://x-road.eu/xsd/identifiers"
xmlns:erec="http://erecord_tunduk.x-road.ee/erecordVerifyData">
   <soapenv:Header>
     <xro:protocolVersion>4.0</xro:protocolVersion>
     <xro:issue></xro:issue>
     <xro:id></xro:id>
     <xro:userId></xro:userId>
     <xro:service iden:objectType="SERVICE">
       <iden:xRoadInstance>central-server</iden:xRoadInstance>
       <iden:memberClass>GOV</iden:memberClass>
       <iden:memberCode>70000006</iden:memberCode>
       <iden:subsystemCode>record-service</iden:subsystemCode>
       <iden:serviceCode>VerifyApostilByCertificateBarcode</iden:serviceCode>
       <iden:serviceVersion>v1</iden:serviceVersion>
     </xro:service>
     <xro:client iden:objectType="SUBSYSTEM">
       <iden:xRoadInstance>central-server</iden:xRoadInstance>
       <iden:memberClass>YouMemberClass</iden:memberClass>
       <iden:memberCode>YouMemberCode</iden:memberCode>
       <iden:subsystemCode>YouSubsystemCode</iden:subsystemCode>
     </xro:client>
   </soapenv:Header>
   <soapenv:Body>
     <erec:VerifyApostilByCertificateBarcode>
       <erec:documentCode>00000000000000</erec:documentCode>
     </erec:VerifyApostilByCertificateBarcode>
   </soapenv:Body>
</soapenv:Envelope>
```