ИНФОРМАЦИОННО ОБСЛУЖВАНЕ

1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340, факс: 02/ 943 66 07
office@is-bg.net www.is-bg.net
ЕИК: 831641791

Приложение № 11

Техническа спецификация за реализация на автентикацията за достъп до бизнес API на НЗИС

Съдържание

История на документа

Дата	Версия	Автор
26.10.2020	1.0	ИО АД
04.11.2020	1.0.1	ИО АД
18.11.2020	1.0.2	ИО АД

Използвани термини и съкращения

Термин/Съкращение	Описание
НЗИС	Национална здравно информационна система
API	Application Programming Interface
REST	Representational State Transfer
VPN	Virtual Private Network

1. Общо описание

Целта на този документ е да предостави информация за метода на достъп до публичното REST-ful API на системата НЗИС по отношение на сигурността.

Забележка: Под „публично“ API се разбира програмен интерфейс, предоставящ бизнес услуги, който е достъпен за външни системи на предварително известен уеб-адрес в Интернет без нуждата от VPN (Virtual Private Network). Това не означава, че самото API предоставя свободен достъп. НЗИС изисква от външните системи предварителна автентикация, преди да позволи достъп до набора от бизнес услуги.

Бизнес услугите, предоставяни от НЗИС, могат да бъдат достъпени чрез стандартна HTTPS комуникация на адрес https://api.his.bg/{service-path} за продукционна среда и https://ptest-api.his.bg/{service-path} за публичната тестова среда.

2. Метод за автентикация за достъп до НЗИС API

Адресът https://api.his.bg (https://ptest-api.his.bg за тест) очаква автентикация чрез Authorization header от тип Bearer Token. За да получите такъв токен е необходимо да достъпите отделен адрес за аутентикация на https://auth.his.bg за продукционна среда и https://ptest-auth.his.bg за публичната тестова среда. Обръщението е към адрес https://auth.his.bg/token (https://ptest-auth.his.bg/token за тест) и трябва да го извършите с валидно удостоверение за квалифициран електронен подпис (КЕП).

След успешна автентикация, услугата ще върне следния резултат:

```
<?xml version="1.1" encoding="UTF-8"?>
<nhis:message xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:nhis="https://www.his.bg" xsi:schemaLocation="https://www.his.bg
https://www.his.bg/api/v1/NHIS-S001.xsd">
  <nhis:contents>
    <nhis:accessToken value="imSXTs2OqSrGWzsF3rF..." dataType="[string]"/>
    <nhis:tokenType value="bearer" dataType="[string]"/>
    <nhis:expiresIn value="7200" dataType="[positiveInt]"/>
    <nhis:issuedOn value="2020-10-21T18:11:23" dataType="[dateTime]"/>
    <nhis:expiresOn value="2020-10-21T18:13:23" dataType="[dateTime]"/>
  </nhis:contents>
</nhis:message>
```

В примерът стойността на **accessToken** е съкратена за по-добра четимост, но реалният стринг е по-дълъг. Останалите елементи в резултата целят да ви помогнат с информация относно типът токен и неговата валидност.

С така полученият токен, достъп до бизнес услугите на НЗИС на адрес https://api.his.bg (https://ptest-api.his.bg за тест) се извършва чрез добавяне на следния хедър към заявките:

```
header 'Authorization: Bearer imSXTs2OqSrGWzsF3rF...'
```

Моля забележете, че токенът има максимален срок на валидност, посочен в резултата от заявката в поле **expiresIn** (стойност в секунди). В случай, че валидността на токена е изтекла или поради друга причина е бил инвалидиран, при обръщение към https://api.his.bg (https://ptest-api.his.bg за тест) ще получите грешка от тип **401** (Unauthorized). В такъв случай е необходимо да извършите нова заявка за автентикация, за да получите нов валиден токен.

3. Алтернативен метод за автентикация за достъп до НЗИС API

Достъпът до https://auth.his.bg (респективно https://ptest-auth.his.bg) е с включено опционално предоставяне на клиентски сертификат. В случай, че такъв не е част от заявката, ще Ви бъде върнат отговор със статус код **401** (Unauthorized) и съдържание - допълнително XML съобщение (challenge) със следния вид:

```
<?xml version="1.1" encoding="UTF-8"?>
<nhis:message xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:nhis="https://www.his.bg" xsi:schemaLocation="https://www.his.bg
https://www.his.bg/api/v1/NHIS-S001.xsd">
  <nhis:contents>
    <nhis: challenge value="imSXTs2OqSrGWzsF3rF..." dataType="[string]"/>
  </nhis:contents>
</nhis:message>
```

За да се оторизирате и да получите token е необходимо да подпишете това съобщение с валидно удостоверение за квалифициран електронен подпис (КЕП) и да изпратите POST заявка към същата входна точка (https://auth.his.bg/token за продукционна среда и https://ptest-auth.his.bg/token за тестова) в тялото на която да подадете полученото и подписано от Вас идентификационно съобщение. Подписът следва да бъде в същия формат (XMLDSig), който се използва и при подписването на XML съобщенията, които се изпращат към API слоя на НЗИС.

След успешна автентикация, услугата ще върне съобщение с токен за достъп. С така полученият токен, достъп до бизнес услугите на НЗИС на адрес https://api.his.bg (https://ptest-api.his.bg за тест) се извършва чрез добавяне на **Authorization** хедър към заявките. Примерен отговор и хедър може да видите в т. 2 Метод за автентикация за достъп до НЗИС API.