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

**Съдържание**

[История на документа 3](#_Toc54613321)

[Използвани термини и съкращения 3](#_Toc54613322)

[1. Общо описание 4](#_Toc54613323)

[2. Метод за автентикация за достъп до НЗИС API 4](#_Toc54613324)

# История на документа

|  |  |  |
| --- | --- | --- |
| Дата | Версия | Автор |
| 26.10.2020 | 1.0 | ИО АД |
| 04.11.2020 | 1.0.1 | 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 |

# 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}](https://api.his.bg/%7bservice-path%7d) за продукционна среда и [https://ptest-api.his.bg/{service-path}](https://ptest-api.his.bg/%7bservice-path%7d) за публичната тестова среда.

# Метод за автентикация за достъп до НЗИС API

Адресът [https://api.his.bg](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:



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://api.his.bg/) (<https://ptest-api.his.bg> за тест) се извършва чрез добавяне на следния хедър към заявките:



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.