Техническа спецификация за идентификация и достъп до НЗОК API

**Съдържание**

[История на документа 3](#_Toc70021730)

[Използвани термини и съкращения 3](#_Toc70021731)

[1. Общо описание 4](#_Toc70021732)

[2. Метод за идентификация и достъп до НЗOK API 4](#_Toc70021733)

[3. Алтернативен метод за идентификация и достъп до НЗOK API 5](#_Toc70021734)

# История на документа

|  |  |  |
| --- | --- | --- |
| Дата | Версия | Автор |
| 01.04.2021 | 1.0.0 | ИО АД |
| 05.04.2021 | 1.0.1 | ИО АД |
| 20.04.2021 | 1.0.2 | ИО АД |

# Използвани термини и съкращения

|  |  |
| --- | --- |
| Термин/Съкращение | Описание |
| НЗOK | Национална здравно осигурителна каса |
| 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 API на системите на НЗОК 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. НЗОК изисква от външните системи предварителна идентификация, преди да позволи достъп до набора от бизнес услуги.*

Бизнес услугите, предоставяни от НЗОК, чрез API, могат да бъдат достъпни, чрез стандартна HTTPS комуникация на адрес [https://api.nhif.bg/{service-path}](https://api.nhif.bg/%7bservice-path%7d) за продукционна среда и [https://ptest-api.nhif.bg/{service-path}](https://ptest-api.nhif.bg/%7bservice-path%7d) за публичната тестова среда.

# Метод за идентификация и достъп до НЗOK API

Адресът <https://api.nhif.bg> (<https://ptest-api.nhif.bg> за тест) очаква идентификация, чрез Authorization header от тип Bearer Token. За да се получи такъв ***Token*** е необходимо да се достъпи отделен адрес за идентификация на <https://auth.nhif.bg> за продукционна среда и <https://ptest-auth.nhif.bg> за публичната тестова среда. Обръщението е към адрес <https://auth.nhif.bg/token> (<https://ptest-auth.nhif.bg/token> за тест) и трябва да се извърши с валидно удостоверение за квалифициран електронен подпис (КЕП).

След успешна идентификация, услугата връща следния резултат:



В примерът стойността на **accessToken** е съкратена за по-добра четимост, но реалната стойност е по-дълга. Останалите елементи в резултата дават допълнителна информация относно типът ***Token*** и неговата валидност.

С така полученият ***Token***, се достъпва до бизнес услугите на НЗОК на адрес <https://api.nhif.bg> (<https://ptest-api.nhif.bg> за тест), чрез добавяне на следния хедър към заявките:



Да се обърне внимание, че ***Token-ът*** има максимален срок на валидност, посочен в резултата от заявката в поле **expiresIn** (стойност в секунди). В случай, че валидността на ***Token-ът*** е изтекла или поради друга причина е станал невалиден, при обръщение към <https://api.nhif.bg> (<https://ptest-api.nhif.bg> за тест) ще се получи грешка от тип **401** (Unauthorized). В такъв случай е необходимо да се направи нова заявка за идентификация, за да се получи нов валиден ***Token***.

# Алтернативен метод за идентификация и достъп до НЗOK API

Достъпът до <https://auth.nhif.bg> (респективно <https://ptest-auth.nhif.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:



За да се направи оторизация и да се получи ***Token*** е необходимо да се подпише това съобщение с валидно удостоверение за квалифициран електронен подпис (КЕП) и да се изпрати POST заявка към същата входна точка (<https://auth.nhif.bg/token> за продукционна среда и <https://ptest-auth.nhif.bg/token> за тестова) в тялото на която да се подаде полученото и подписано 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 НЗОК.

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