NAV M2M

Általános

interfészleírás

0.4 verzió

TARTALOMJEGYZÉK

[1. Bevezetés 8](#_Toc188968840)

[2. Használati feltételek 8](#_Toc188968841)

[2.1. Kliensprogramra vonatkozó feltételek 8](#_Toc188968842)

[2.2. Kliensprogram fejlesztőkre vonatkozó feltételek 9](#_Toc188968843)

[2.3. Kliensprogram felhasználókra vonatkozó feltételek 9](#_Toc188968844)

[3. Technikai követelmények 9](#_Toc188968845)

[3.1. Alapvető technológiák 9](#_Toc188968846)

[3.2. Kódolási, titkosítási algoritmusok 9](#_Toc188968847)

[4. Folyamatok 11](#_Toc188968848)

[4.1. Regisztráció áttekintő folyamat 11](#_Toc188968849)

[4.2. Token igénylés és használat 12](#_Toc188968850)

[4.3. Nonce beváltás, felhasználó regisztráció aktiválás 13](#_Toc188968851)

[4.4. Fájlfeltöltés 14](#_Toc188968852)

[5. Általános interfész elemek 15](#_Toc188968853)

[5.1. Általános formátumok 15](#_Toc188968854)

[*5.1.1.* *Aláírás* 15](#_Toc188968855)

[*5.1.2.* *Minták* 15](#_Toc188968856)

[5.2. Általános technikai adatok 16](#_Toc188968857)

[*5.2.1.* *Feljéc* 16](#_Toc188968858)

[*5.2.2.* *Státuszkódok* 16](#_Toc188968859)

[*5.2.3.* *Méretkorlát* 16](#_Toc188968860)

[*5.2.4.* *Válaszidő* 16](#_Toc188968861)

[*5.2.5.* *Szerveróra* 16](#_Toc188968862)

[*5.2.6.* *Helyi idő konvertálása UTC időre* 17](#_Toc188968863)

[*5.2.7.* *Karakterkonverzió* 17](#_Toc188968864)

[*5.2.8.* *Forgalomkorlátozás* 17](#_Toc188968865)

[6. REST interfészek 18](#_Toc188968866)

[6.1. Üzenetek általános felépítése 18](#_Toc188968867)

[*6.1.1.* *Kérés (request)* 18](#_Toc188968868)

[*6.1.2.* *Válasz (response)* 18](#_Toc188968869)

[6.2. Felhasználó regisztráció kezelés interfésze 18](#_Toc188968870)

[*6.2.1.* *Nonce beváltás művelete* 18](#_Toc188968871)

[*6.2.2.* *Felhasználó regisztráció aktiválás művelete* 20](#_Toc188968872)

[6.3. Token kezelés interfésze 21](#_Toc188968873)

[*6.3.1.* *Token igénylés művelete* 21](#_Toc188968874)

[6.4. Fájltároló kezelés interfészei 23](#_Toc188968875)

[*6.4.1.* *Fájlfeltöltés művelete* 23](#_Toc188968876)

[*6.4.2.* *Fájlstátusz lekérdezés művelete* 25](#_Toc188968877)

[7. Környezetek elérhetősége 27](#_Toc188968878)

[7.1. Teszt környezet 27](#_Toc188968879)

[7.2. Éles környezet 27](#_Toc188968880)

[7.3. Definíciók elérhetősége: 27](#_Toc188968881)

**Dokumentum történet**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dátum | Szerző |  | Verzió | Változtatás |
| 2024.05.15. | Pillér Kft |  | 0.1 | Első verzió |
| 2024.05.22. | Pillér Kft |  | 0.2 | Paraméter minták és alapértékek, HTTP státuszkódok |
| 2024.06.26. | Pillér Kft |  | 0.3 | resultMessage megadása nem kötelező |
| 2024.10.30. | Pillér Kft |  | 0.4 | 1.1-es interfész változásainak átvezetése |

**Fogalomtár**

|  |  |
| --- | --- |
| Kifejezés (témakör) | Jelentés, magyarázat |
| Aláíró kulcs *(Security)* | Egyes API üzenetek hitelesítésére szolgáló aláíráshoz használt kulcs, amely teljes egészében csak magában a kliensprogramban áll össze. Titkosan kell kezelni úgy, hogy emberi megismerése reálisan lehetetlen legyen. Az láírókulcs a Felhasználóhoz kapcsolódik. |
| API *(API)* | Egy API alatt itt egy meghatározott üzleti célhoz kapcsolódó, egymással összefüggésben álló interfész-műveletek és az ezek által használt adatszerkezetek együttesét értjük. Egy API-ban ennek megfelelően több főnévre (tárgyra) vonatkozó műveletek is lehetnek, nem felétlenül csak egy adott tárgyra vonatkozó műveletek. Egy adott tárgyra vonatkozó CRUD műveletek fő szabály szerint egy API-ban vannak megfogalmazva. Egy SOAP API egy WSDL állományban, egy RESTful API egy OpenAPI dokumentumban kerül definiálásra. |
| API Key *(Security)* | A felhasználói regisztráció eredményeként a felhasználó számára kiadott, különböző biztonsági információkat tartalmazó titkos kód. |
| API Key alapú felhasználói regisztráció *(Általános)* | A kliensprogramnak az a működési módja, amikor a felhasználói regisztráció során kapott API Key-t a végfelhasználó a kliensprogramban rögzíti (a kliensprogramra rábízza) a célból, hogy a kliensprogram ennek a NAV M2M API műszaki dokumentációjában meghatározott módon való használatával igazolja a személyazonosságát a NAV M2M API felé létesített kapcsolat során, és így a kliensprogram a végfelhasználó nevében lép fel a NAV M2M API használata során.  Az API Key sorendben a következő adatokat tartalmazza:   1. felhasználó azonosító 2. felhasználó jelszó 3. aláírókulcs első fele 4. nonce (aláírókulcs második felének a beváltáshoz) |
| Authentication *(Security)* | ld. Azonosítás |
| Authorization *(Security)* | ld. Feljogosítás |
| Azonosítás *(Security)* | Azonosítás és beazonosítás, vagyis annak megállapítása, hogy *megy Felhasználó* használja az API-t, és az *mely valós személlyel* (természetes vagy nem természetes személlyel) feleltethető meg. |
| Azonosítási titok *(Security)* | Az Azonosítási titkok a regisztrációs és felhasználó-azonosítási eljárás során alkalmazott, a NAV M2M API műszaki dokumentációjában részletezett titkos információk. Az azonosítási titkok közé tartoznak például: client secret, felhasználói jelszó, felhasználói aláíró kulcs, nonce, stb.. |
| Client *(Security)* | ld. Kliens |
| Client ID *(Security)* | A regisztrált kliensprogram nyilvános (nem titkos) azonosítója |
| Client secret *(Security)* | A regisztrált kliensprogram titkos kódja, amivel a kliensprogram az API kommunikáció során azonosítja magát |
| Felhasználó *(Security)* | Egy természetes személy (végfelhasználó) számára regisztráció során létrehozott gépi személyiség, amely az adott természetes személy nevében adott kliensprogramon keresztül folytatott kommunikációt szolgálja. |
| Felhasználó jelszó *(Security)* | A felhasználói regisztráció során generált jelszó. |
| Felhasználó név *(Security)* | A felhasználói regisztráció generált egyedi azonosító. |
| Felhatalmazáson alapuló működés *(Általános)* | A kliensprogramnak az a működési módja, amikor a végfelhasználó a NAV M2M API műszaki dokumentációjában meghatározott módon történő, hiteltérdemlő azonosítását követően, a NAV M2M API felhatalmazási alrendszerén keresztül időben és terjedelemben korlátozott felhatalmazást ad a kliensprogramnak a NAV M2M API saját nevében való használatára. |
| Feljogosítás *(Security)* | Annak megállapítása, hogy az azonosított Felhasználó jogosult-e valamely szolgáltatást használni, illetve adathoz hozzáférni. |
| Kliens *(Security)* | Kliensnek, kliensprogramnak nevezzük azt a szoftveralkalmazást (vagy integráltan működő alkalmazás együttest), mely a NAV M2M API részét képező egyes szolgáltatásokhoz számítógép-hálózati kapcsolaton keresztül hozzáfér, függetlenül a szoftveralkalmazás műszaki, technológiai, architekturális kialakításától. (Például ERP rendszer, személyügyi rendszer, könyvelő program, bérszámfejtő program, stb.) |
| Kliensprogram *(Security)* | ld. Kliens |
| NAV M2M API *(Általános)* | A NAV M2M API a Nemzeti Adó- és Vámhivatal által kifejlesztett, Interneten keresztül webszolgáltatásként elérhető, gépi (nem közvetlen humán) hozzáférésre tervezett publikus és nem publikus szolgáltatások gyűjteménye. |
| Nonce *(Security)* | Egyszer használatos kódszó, amely az aláírókulcs második felének a kiváltására szolgál. A nonce-t csak egyszer lehet felhasználni az aláírókulcs megszerzésére, és a sikeres cserét csak egy megbízható fél hajthatja végre, ehhez általában egy további titkot (pl. User, client secret) is meg kell adni. A nonce használatának célja, hogy az aláírókulcs ne kelljen kiadni megbízhatatlan „közvetítők” számára (pl. felhasználó); a közvetítő az aláírókulcs helyett a nonce-ot kapja meg, melyet továbbíthat a megbízható fél felé. |
| REST *(API)* | A REST (representational state transfer) http alapú interneten zajló interakciókban résztvevő elemek együttműködésére kialakított tervezési megközelítés. Különböző megszorításokat és elvárásokat támaszt a résztvevőkkel és a kommunikációval kapcsolatban is. |
| RESTful *(API)* | (vagy RESTful API) Olyan interfész, amely megfelel a REST megszorításoknak. |
| SOAP *(API)* | A SOAP (Simple Object Access Protocol) egy protokoll, amelyet webszolgáltatások hálózaton keresztüli kommunikációjához terveztek. |
| Üzenet aláírás *(Security)* | Egyes API üzenetek esetében a releváns üzleti tartalom alapján az aláíró kulccsal képzett hitelesítő kód, amely az üzenet letagadhatatlanságát biztosítja. |
| Végfelhasználó *(Általános)* | A Végfelhasználó a kliensprogramot használó, vagy azon automatikus folyamatokat beállító, paraméterező természetes személy. |
| Zero Trust *(Security)* | A Zero Trust megközelítés alatt egy olyan megközelítést értünk, amikor az architektúra egyes elemei (pl. az egyes micro service-ek) nem bíznak meg senkiben. Amíg a kérés nem lett megfelelően hitelesítve, és a hívó nem igazolta a jogosultságát az adott művelet végrehajtására, addig nem kerül kiszolgálásra akkor sem, ha a hívás egy másik „belső” komponenstől, belső felhasználótól, vagy más, megbízhatónak „tűnő” féltől érkezett. Ezzel megnehezíthetjük az architektúrában való „oldalirányú” mozgással végzett támadásokat, amikor valamilyen, a belső hálózatunkban található elemtől indul támadás. Ezen támadások forrása lehet akár egy szolgáltatás hibájának kihasználása, vagy a határvédelem „feltörése”, de akár belső támadás is. Ezeket a támadásokat a klasszikus biztonsági megközelítés (amikor a biztonsági ellenőrzések a határvédelemhez kötődően történnek meg) nem tudja megakadályozni. |

# Bevezetés

A leírás a kliensek és NAV M2M közötti gép-gép kapcsolat azon interfészeit és műveleteit mutatja be, amelyek általánosan szükségesek a gépi kapcsolat használatához. Itt kerül bemutatásra a regisztráció és a fájlkezelés folyamata és műveletei.

# Használati feltételek

A gépi interfész megfelelő működéséhez az ebben a fejezetben felsorolt feltételeknek kell megfelelni.

## Kliensprogramra vonatkozó feltételek

* A kliensprogram az azonosítási titkok közül azokat, melyek tartós tárban való tárolása műszakilag nem feltétlenül szükséges, tartós tárban nem tárolhatja.
* A kliensprogram azokat az azonosítási titkokat, melyek tartós tárban való tárolása műszakilag szükséges, a tartós tárban mindig olyan módon titkosítva tárolja, hogy az azonosítási titkok reális erőfeszítés árán senki számára ne legyenek megismerhetők.
* A kliensprogram az azonosítási titkokat semmilyen módon nem teheti a NAV M2M API-n kívül (ember vagy gép számára) megismerhetővé, még műszaki indokokkal (például hibakeresés támogatása okán) sem, melynek értelmében a kliensprogram még a Végfelhasználónak sem teheti megismerhetővé a személyéhez kapcsolódó azonosítási titkokat.
* A kliensprogram az azonosítási titkokat a NAV M2M API számára kizárólag a NAV M2M API műszaki dokumentációjában részletezett esetekben és módon adhatja át.
* A kliensprogram a rá bízott végfelhasználói azonosító információkat vagy azonosító tokent csak olyan szolgáltatáshoz és adatokhoz való hozzáférés érdekében használhatja, amire a Végfelhasználótól engedéllyel rendelkezik. Ennek biztosítására a kliensprogramnak olyan kialakítással, illetve megoldásokkal kell rendelkeznie, amely biztosítja a kliensprogramot használó Végfelhasználó kliensprogram általi beazonosíthatóságát.
* A Kliensprogram a NAV M2M API által hozzá eljuttatott adatokat, információkat csak a Végfelhasználó szándékának megfelelő célra használhatja.
* A Kliensprogramban a Végfelhasználó számára olyan felhasználói felületet vagy eszközt kell biztosítani, mellyel az átlagos informatikai felkészültségű természetes személy végfelhasználó vagy gazdálkodó szervezet, együttműködő szerv végfelhasználó esetén a regisztrációt végző természetes személy törvényes képviselő a birtokában álló API Key-t a kliensprogramban más személy közreműködése nélkül rögzíteni képes (az API Key titka megőrzésének érdekében) .
* A kliensprogramban a Végfelhasználó számára olyan felhasználói felületet vagy eszközt kell biztosítani, mellyel az átlagos informatikai felkészültségű természetes személy végfelhasználó vagy gazdálkodó szervezet, együttműködő szerv végfelhasználó esetén a regisztrációt végző természetes személy törvényes képviselő az azonosítási titkokat más személy közreműködése nélkül a kliensprogram adattáraiból visszaállíthatatlanul törölni képes.
* A kliensprogramban olyan mechanizmust kell kialakítani, mely Végfelhasználó kliensprogramhoz való hozzáférésének megszűnése esetén az adott Végfelhasználóhoz kapcsolódó azonosítási titkokat a kliensprogram adattáraiból automatikusan és visszaállíthatatlanul törli.
* A kliensprogramban olyan mechanizmust kell kialakítani, amely a kliensprogram új regisztrációval nem járó verzióváltása, újratelepítése vagy más hasonló esemény esetén lehetővé teszi az elvégzett felhasználói regisztrációkból származó azonosítási titkok áthelyezését az új programpéldányba.
* A NAV M2M API dokumentációjában bemutatott, az API Key rögzítése után induló automata aktiválási folyamat a kliensprogram által teljesen automatizáltan, emberi közreműködés nélkül kell, hogy megvalósuljon.
* A kliensprogramban a Végfelhasználó számára olyan felhasználói felületet vagy eszközt kell biztosítani, mellyel az átlagos informatikai felkészültségű természetes személy végfelhasználó a személyéhez vagy gazdálkodó szervezet, együttműködő szerv végfelhasználó esetén az arra jogosult a Végfelhasználó személyéhez kapcsolódó NAV M2M API felhasználó nevet, valamint a kliensszoftver client ID-ját, megnevezését és pontos verziószámát megismerheti (például technikai bejelentés tétele céljából).
* A kliensprogramban a Végfelhasználó számára olyan felhasználói felületet vagy eszközt kell biztosítani, mellyel az átlagos informatikai felkészültségű természetes személy végfelhasználó a személyéhez vagy gazdálkodó szervezet, együttműködő szerv végfelhasználó esetén az arra jogosult a Végfelhasználó személyéhez kapcsolódó azonosítási titkok felhasználásával elvégzett NAV M2M API hívások főbb üzleti jellemzőit bemutató naplóhoz legalább 90 napra visszamenőleg hozzáférhet.

## Kliensprogram fejlesztőkre vonatkozó feltételek

* A kliensprogram fejlesztője elvégezte a kliensprogram regisztrációt az ÜPO felületén.
* A kliensprogram azonosítót elküldte a kliensprogramot használó ügyfeleinek.

## Kliensprogram felhasználókra vonatkozó feltételek

* Rendelkezik regisztrált kliensprogrammal.
* A kliensprogram fejlesztőjétől megkapta a kliensprogram azonosítót.
* Elvégezte a felhasználó regisztrációt a kliensprogram azonosítóval az ÜPO felületén.
* Az ÜPO-tól kapott API-key-t rögzítette a kliensprogramban.

Rendelkezik megfelelő képviseleti jogosultsággal az EKNYI-ben arra az adózóra vonatkozóan, akinek a nevében műveleteket szeretne elvégezni (pl. adott típusú bizonylatokat beküldeni).

# Technikai követelmények

A kliensprogramoknak a következő technikai feltételeknek kell megfelelniük a NAV M2M interfész használatához.

## Alapvető technológiák

A kliensprogramnak a következő alapvető technológiákat kell implementálnia:

* HTTPS
* REST API
* XML
* JSON

## Kódolási, titkosítási algoritmusok

A kliensprogramnak a következő titkosítási algoritmusokat kell implementálnia:

* SHA-256

# Folyamatok

## Regisztráció áttekintő folyamat

A következő szekvenciadiagram bemutatja a regisztrációs folyamatot.

A screenshot of a computer

Description automatically generated

## Token igénylés és használat

A képen szöveg, képernyőkép, diagram, sor látható

Automatikusan generált leírás

1. A kliens hozzáférési tokent igényel az NAV M2M-től a felhasználó számára, amelyhez megadja a kliens azonosítót és jelszót, valamint a felhasználó azonosítót és jelszót.
2. A NAV M2M ellenőrzi a bejövő adatok érvényességét, majd amennyiben mindent rendben talál, generál egy hozzáférési tokent. Biztonsági okból a token nem kerülhet olvasható formában a kliensprogramhoz, ezért a token kicserélésre kerül egy nem olvasható, úgynevezett phantom tokenre; a két token között kölcsönösen egyértelmű hozzárendelés van.
3. A NAV M2M a phantom tokent küldi vissza a kliensnek. A hozzáférés aktiválása előtt kiállított token kizárólag a nonce érvénytelenítési szolgáltatásra ad jogosultságot a kliensnek. A kiállított hozzáférési token biztonsági okból korlátozott ideig érvényes, és az érvényességi ideje nem meghosszabbítható.
4. A műveletek meghívásakor a kliens a phantom tokent küldi el a NAV M2M-nek.
5. Az NAV M2M a phantom tokent kicseréli az eredeti hozzáférési tokenre, és az alapján ellenőrzi a jogosultságot.

## Nonce beváltás, felhasználó regisztráció aktiválás

A képen szöveg, képernyőkép, diagram, Párhuzamos látható

Automatikusan generált leírás

1. A kliensprogram a nonce-ot elküldi a NAV M2M megfelelő API-jának, hogy azt beváltsa a titkos aláíró kulcs egy részére. A kérést a phantom token átadásával hitelesíti.
2. A NAV M2M a phantom tokent kicseréli az eredeti hozzáférési tokenre, ellenőrzi az adott felhasználó adott funkcióhoz való hozzáférését. Továbbá ellenőrzi a nonce érvényességét, és amennyiben érvényes, generál egy új kulcsrészletet.
3. A generált aláírókulcs részletet a NAV M2M visszaadja az őt meghívó kliensprogramnak.
4. A kliensprogram összeállítja a két részletből a végfelhasználói titkos aláírókulcsot, és eltárolja olyan módon (pl. megfelelő titkosítással), hogy ésszerű erőfeszítéssel azt ne lehessen kinyerni.
5. A kliensprogram meghívja a NAV M2M API-n a hozzáférés aktiválási funkciót. A hívást a phantom token átadásával hitelesíti. Emellett az üzenet aláírása is szükséges, amivel ellenőrzésre kerül, hogy a kiensprogram megfelelően állította össze az aláíró kulcsot.
6. A NAV M2M API sikeres biztonsági ellenőrzés esetén elvégzi a felhasználó aktiválását, és érvényteleníti a nonce-t (így ezután már nem ismételhetők meg az 1.9-1.12 lépések). Szintén érvényteleníti a kiadott OAuth 2.0 tokent, a további API használathoz tehát új token igénylése szükséges. Az aktiválást követően az adott felhasználó használatával a NAV M2M API üzleti célú felhasználása megkezdhető. (ld. Az üzleti célú API hívások részletes végrehajtása).
7. A NAV M2M API a sikeres aktiválásról visszajelzést ad a kliensprogramnak.

## Fájlfeltöltés

A képen szöveg, képernyőkép, diagram, sor látható

Automatikusan generált leírás

1. A kliens kezdeményezi a fájl feltöltését a NAV M2M fájltárolójába. Megadja a fájlt, a fájl SHA-256 hash-ét.
2. A NAV M2M ellenőrzi a hash-t, majd ha az helyes, akkor kér egy egyedi fájlazonosítót a fájltárolótól.
3. A NAV M2M visszaküldi a fájl egyedi azonosítóját a kliensnek, valamint ha a vírusellenőrzés 30mp alatt megtörténik, akkor azonnal visszaadja az eredményét. Ha több ideig tart az ellenőrzés, akkor a következő lépéssel lehet lekérdezni az eredményét. (A fájl további használatakor (pl bizonylat létrehozás) újból ellenőrzésre kerül a vírusellenőrző eredménye)
4. Opcionálisan a kliens lekérdezi a bizonylatfájl státuszát, benne a vírusellenőrzés eredményével.
5. A NAV M2M elküldi a vírusellenőrzés eredményét a kliensnek.

# Általános interfész elemek

## Általános formátumok

## *Aláírás*

A jogkövetkezménnyel járó, és/vagy érzékeny adatokat tartalmazó üzenetek küldésekor aláírást is meg kell adni. Az aláírás az aláírókulcs és egyéb adatok titkosított kombinációjaként áll elő. Az egyéb adatok részben egységesek, részben műveletspecifikusak. A műveletfüggő adatok az egyes műveletek leírásánál vannak megadva.

**Az aláírások egységes felépítése a következő:**

***base64(SHA-256(<üzenetazonosító> + <időbélyeg> + <műveletfüggő adat> + <aláírókulcs>))***

* ***üzenetazonosító*** : Az üzenetegyedi azonosítója, ami minden kérésben kötelezően küldendő.
* ***időbélyeg*** : Az üzenet elküldésének időpontja másodperc pontosan UTC időben,

YYYYMMDDHHmmss formátumban.

* ***műveletfüggő adat*** : Az egyes műveletek leírásánál megadott adat.
* ***aláírókulcs*** : A nonce beváltás során előállt kulcs.

A fenti adatokat kell összefűzni, majd SHA-256 szerint hash-elni, majd base64 kódolni, majd nagybetűsíteni.

**Példa:**

* ***üzenetazonosító*** = 7eae9ecf-f735-4a4f-aa49-e85ea411a313
* ***időbélyeg*** = 20240510123847
* ***műveletfüggő*** ***adat*** = 26549118-0ddc-4e30-81bc-eaddd6f54b21
* ***aláírókulcs*** = FA12BC4567CA12BC4588
* ***üzenetazonosító + időbélyeg + műveletfüggő adat + aláírókulcs*** =

7eae9ecf-f735-4a4f-aa49-e85ea411a3132024051012384726549118-0ddc-4e30-81bc-eaddd6f54b21FA12BC4567CA12BC4588

* ***aláírás = nagybetűsített base64(SHA-256(üzenetazonosító + időbélyeg + műveletfüggő adat + aláírókulcs))*** =

LOHXJMDUZR4ETMOA9Y6XMLGHWCRR3/OJQ6T6JBDKQOG=

Nem mindegyik, csak az érzékenyebb adatokat kezelő, vagy jogkövetkezménnyel járó műveletek üzeneteibe kerül aláírás.

## *Minták*

Az interfész olyan adatainál, ahol üzleti szempontból fontos jelentősége van a formátumnak (pl. email cím), bekerül az interfészbe az erre vonatkozó pattern információ. (Az első verzióban még nincs ilyen adat.)

A dokumentációban tájékoztatásul olyan, inkább technikai jellegű adatok esetén (pl. fájl id, aláírás) is megadjuk a használt mintát, ahol ez nem kerül az interfészbe. Ilyenkor adatátadásnál nem elvárás az adott formátum, az adat későbbi használata során viszont hibák keletkezhetnek. Ezen adatok formátumának megváltozása nem jár új interfészkiadással, ezért az arra épülő vizsgálatok beépítése nem javasolt.

## Általános technikai adatok

## *Feljéc*

A kérésben a következő HTTP fejléc mezőket kötelező megadni:

* content-type=application/json
* accept=application/json

## *Státuszkódok*

A szolgáltatás a hívónak helyes kérés esetén minden esetben HTTP 200-as választ ad. Ez nem feltétlenül jelzi, hogy a megfogalmazott kérés tartalmán az üzleti végrehajtás sikeresen lefutott, csak azt, hogy a kérés informatikai tekintetben jól formázott volt, a hívott erőforrás el tudta olvasni, be tudta fogadni. Mivel a szolgáltatás által kezelt hibakódok fel vannak mappelve, így a visszaadott hibakód is sikeres válasznak számít. Tehát egy HTTP 200-as válaszban is lehet hibakódokat tartalmazó üzenet.

Az általános HTTP státuszkódok a következők:

|  |  |
| --- | --- |
| **státuszkód** | **leírás** |
| 200 | Sikeres |
| 400 | Bad request - DTO validációs hiba |
| 401 | Unauthorized - Token ellenőrzés hiba |
| 403 | Forbidden - Role ellenőrzés hiba |
| 404 | Not found - GET esetén nem található a rekord |
| 413 | Entity too large – file feltöltéskor túl nagy méretű fájl |
| 429 | Too many requests - AGW Rate limiter |
| 500 | Internal server error - Exception következik be |
| 503 | Service unavailable - AGW Circuit breaker |
| 504 | Gateway timeout - AGW Timeout |

## *Méretkorlát*

Fájlfeltöltés esetén a méret nem haladhatja meg a 150MB-ot.

## *Válaszidő*

A szerver jellemzően 200 ms alatti válaszidőkkel szolgál ki. A szinkronhívások blokkoló timeout értéke 10000 ms. Kérjük, hogy kliens oldalon a fenti értéket meghaladó válaszidőt kezeljék csak időtúllépésként! Az abszolút timeout értéke 60 sec. Ha egy műveletre nem érkezik válasz a 60 másodperces timeout miatt, még nem jelenti a művelet sikertelenségét.

## *Szerveróra*

A szerver az időbeállításokat egy zárt, a külvilág számára nem hozzáférhető NTP szervertől kapja. Kliens oldalon a szerveridőhöz szinkronizálás nem követelmény, azonban opcionálisan a következő időszinkronizáció lehetséges: http://www.pool.ntp.org/zone/hu (a csatlakozáshoz NTP kliensre van szükség).

## *Helyi idő konvertálása UTC időre*

A helyes kliensoldali aláírás előállításához a helyi időt UTC időre kell konvertálni. Ez úgy tehető meg, hogy a kliensnél érvényes időzóna szerinti helyi idő értékéhez hozzá kell adni vagy ki kell vonni annyi egész órát, amennyivel az időzóna az UTC középidőtől eltér. Amelyik időzónában van téli/nyári időszámítás, ott a kivonásnál/összeadásnál erre is figyelni kell.

## *Karakterkonverzió*

A beküldött adatokon szerver oldali karakterkonverzió nem történik.

## *Forgalomkorlátozás*

A NAV - mivel az eÁFA M2M szolgáltatásként jelenik meg - az interfészspecifikációtól lényegesen eltérő és a rendszer működését zavaró vagy akadályozó kommunikáció megakadályozása érdekében a jövőben rate limiting megoldást vezethet be. A rate limiting azt jelenti, hogy a szerver oldali erőforrások védelmének érdekében az API Gateway képes lesz limitálni az adózónként adott idő alatt beküldhető kérések számát, és amennyiben egy adózó túllépi a limitben meghatározott kérések számát, akkor a HTTP szabványnak megfelelő HTTP 429 Too Many Request hibakóddal elutasításra kerülnek a kérései. A limit túllépése esetén a kérések forgalmazása az időablak leteltét követően folytatható.

# REST interfészek

## Üzenetek általános felépítése

## *Kérés (request)*

Az összes kérés üzenetben szerepelniük kell a következő paramétereknek:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **név** | **típus** | **hely** | **kötelező** | **leírás** |
| messageId | string | header | igen | Üzenet egyedi azonosítója. Egy GUID érték. |
| correlationId | string | header | nem | Kapcsolat azonosító. Egy GUID érték. |
| Authorization | string | header | igen\* | Authentikációs token.  \*Egyedül a tokenkérés műveletében nem kell szerepeljen. |

Tájékoztatásként a használt, de az interfészen nem előírt minták:

|  |  |  |  |
| --- | --- | --- | --- |
| **név** | **hossz** | **minta** | **alapérték** |
| messageId | 32 | [0-9a-fA-F]{8}-([0-9a-fA-F]{4}-){3}[0-9a-fA-F]{12} | - |
| correlationId | 32 | [0-9a-fA-F]{8}-([0-9a-fA-F]{4}-){3}[0-9a-fA-F]{12} | - |
| Authorization | 20 | .{2172} | - |

## *Válasz (response)*

Az összes válaszüzenet a BaseResponseType típusbból van leszármaztatva.

A BaseResponseType attribútumai a következők:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **név** | **típus** | **hely** | **kötelező** | **leírás** |
| resultMessage | string | body | nem | Válaszüzenet.  A válaszkódhoz kapcsolódó üzenet. A válaszkódok műveletenként, mint enum lettek definiálva. |

## Felhasználó regisztráció kezelés interfésze

|  |  |
| --- | --- |
| **interface** | UserregistrationService |
| **műveletek** | redeemNonce  activateUserRegistration |
| **OpenAPI** | <https://app.swaggerhub.com/apis/NAVGOVHU/m2m_common/1.0#UserregistrationService> |
| **leírás** | Felhasználó regisztráció kezelést támogató interfész |

## *Nonce beváltás művelete*

**Tulajdonságok:**

|  |  |
| --- | --- |
| **művelet** | redeemNonce |
| **művelettípus** | POST |
| **path** | /NavM2mCommon/userregistrationService/Nonce |
| **OpenAPI** | <https://app.swaggerhub.com/apis/NAVGOVHU/m2m_common/1.0#/UserregistrationService/redeemNonce> |
| **leírás** | Nonce beváltását biztosító művelet. A nonce-ért cserébe visszaadja az aláírókulcs második felét. |

**Bemenő paraméterek:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **név** | **típus** | **hely** | **kötelező** | **leírás** |
| requestData | RedeemNonceRequestType | body | igen | Bemenő paraméter struktúra |

A RedeemNonceRequestType attribútumai a következők:

|  |  |  |  |
| --- | --- | --- | --- |
| **név** | **típus** | **kötelező** | **leírás** |
| nonce | string | igen | Az aláírókulcs második felének elkérésére alkalmas ideiglenes jelszó. 10 karakteres alfanumerikus. |

Tájékoztatásként a használt, de az interfészen nem előírt minták:

|  |  |  |  |
| --- | --- | --- | --- |
| **név** | **hossz** | **minta** | **alapérték** |
| nonce | 10 | [0-9a-zA-Z]{10} | - |

**Válasz:**A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

A RedeemNonceResponseType attribútumai a következők:

|  |  |  |  |
| --- | --- | --- | --- |
| **név** | **típus** | **kötelező** | **leírás** |
| signatureKeySecondPart | string | nem | Az aláírókulcs második fele. |
| resultCode | RedeemNonceResult | igen | Válaszkód |
| resultMessage | string | nem | Válaszüzenet |

Tájékoztatásként a használt, de az interfészen nem előírt minták:

|  |  |  |  |
| --- | --- | --- | --- |
| **név** | **hossz** | **minta** | **alapérték** |
| signatureKeySecondPart | 10 | [0-9a-zA-Z]{10} | - |

**Válaszkódok:**

A RedeemNonceResult enum lehetséges értékei:

|  |  |
| --- | --- |
| **kód** | **jelentés** |
| REDEEM\_NONCE\_SUCCESSFUL | Sikeres nonce beváltás. |
| INAVLID\_NONCE | Érvénytelen nonce. |
| OTHER\_ERROR | Egyéb hiba. |

## *Felhasználó regisztráció aktiválás művelete*

**Tulajdonságok:**

|  |  |
| --- | --- |
| **művelet** | activateUserRegistration |
| **művelettípus** | POST |
| **path** | /NavM2mCommon/userregistrationService/Activation |
| **OpenAPI** | <https://app.swaggerhub.com/apis/NAVGOVHU/m2m_common/1.0#/UserregistrationService/activateUserRegistration> |
| **leírás** | A felhasználó regisztráció aktiválását biztosító művelet. Ezzel jelzi a kliensprogram, hogy sikeres volt a nonce beváltás, és eltárolta az aláírókulcsot. Az M2M aktiválja a felhasználó, aki ezután lesz jogosult üzleti műveletek elvégzésére. |

**Bemenő paraméterek:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **név** | **típus** | **hely** | **kötelező** | **leírás** |
| requestData | ActivateUserRegistrationRequestType | body | igen | Bemenő paraméter struktúra |

Az ActivateUserRegistrationRequestType attribútumai a következők:

|  |  |  |  |
| --- | --- | --- | --- |
| **név** | **típus** | **kötelező** | **leírás** |
| signature | string | igen | Felhasználó regisztráció aktiválás aláírása.  ***Az aláírásban szereplő műveletfüggő adat üres.*** |

Tájékoztatásként a használt, de az interfészen nem előírt minták:

|  |  |  |  |
| --- | --- | --- | --- |
| **név** | **hossz** | **minta** | **alapérték** |
| signature | 44-64 | .{44-64} | - |

**Válasz:**

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

Az ActivateUserRegistrationResponseType attribútumai a következők:

|  |  |  |  |
| --- | --- | --- | --- |
| **név** | **típus** | **kötelező** | **leírás** |
| resultCode | ActivateUserRegistrationResult | igen | Válaszkód |
| resultMessage | string | nem | Válaszüzenet |

**Válaszkódok:**

Az ActivateRegistrationResult enum lehetséges értékei:

|  |  |
| --- | --- |
| **kód** | **jelentés** |
| ACTIVATE\_USER\_REGISTRATION\_SUCCESSFUL | Sikeres felhasználói regisztráció aktiválás. |
| INVALID\_SIGNATURE | Érvénytelen aláírás. |
| USER\_REGISTRATION\_ALREADY\_ACTIVATED | A felhasználó regisztráció már aktiválva van. |
| OTHER\_ERROR | Egyéb hiba. |

## Token kezelés interfésze

Jelenleg csak A token igénylés támogatott, későbbi verzióban token frissítés is várható.

|  |  |
| --- | --- |
| **interface** | TokenService |
| **műveletek** | createToken |
| **OpenAPI** | <https://app.swaggerhub.com/apis/NAVGOVHU/m2m_common/1.0#/TokenService> |
| **leírás** | Tokenkezelést támogató interfész |

## *Token igénylés művelete*

**Tulajdonságok:**

|  |  |
| --- | --- |
| **művelet** | createToken |
| **művelettípus** | POST |
| **path** | /NavM2mCommon/tokenService/Token |
| **OpenAPI** | <https://app.swaggerhub.com/apis/NAVGOVHU/m2m_common/1.0#/TokenService/createToken> |
| **leírás** | Új hozzáférési token igénylését biztosító művelet. A kliens ezt kell küldje majd minden műveletben, hogy igazolja a felhasználó jogosultságát a művelet elvégzésére. A kiadott token 10 percig lesz használható. |

**Bemenő paraméterek:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **név** | **típus** | **hely** | **kötelező** | **leírás** |
| requestData | CreateTokenRequestType | body | igen | Bemenő paraméter struktúra |

A CreateTokenRequestType attribútumai a következők:

|  |  |  |  |
| --- | --- | --- | --- |
| **név** | **típus** | **kötelező** | **leírás** |
| clientId | string | igen | Kliens azonosító |
| clientSecret | string | igen | Kliens jelszó |
| password | string | igen | Felhasználó jelszó |
| username | string | igen | Felhasználónév |

Tájékoztatásként a használt, de az interfészen nem előírt minták:

|  |  |  |  |
| --- | --- | --- | --- |
| **név** | **hossz** | **minta** | **alapérték** |
| clientId | 10 | [0-9a-zA-Z]{10} | - |
| clientSecret | 32 | [0-9a-zA-Z]{32} | - |
| username | 10 | [0-9a-zA-Z]{10} |  |
| password | 10 | [0-9a-zA-Z]{10} | - |

**Válasz:**

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

A CreateTokenResponseType attribútumai a következők:

|  |  |  |  |
| --- | --- | --- | --- |
| **név** | **típus** | **kötelező** | **leírás** |
| expires | int | nem | A token ennyi másodperc után veszíti el érvényességét(jár le). Alapértelmezetten 10 perc. |
| accessToken | string | nem | A hozzáférést biztosító token |
| resultCode | CreateTokenResult | igen | Válaszkód |
| resultMessage | string | nem | Válaszüzenet |

Tájékoztatásként a használt, de az interfészen nem előírt minták:

|  |  |  |  |
| --- | --- | --- | --- |
| **név** | **hossz** | **minta** | **alapérték** |
| accessToken | 2056 | .{2172} | - |

**Válaszkódok:**

A CreateTokenResult enum lehetséges értékei:

|  |  |
| --- | --- |
| **kód** | **jelentés** |
| TOKEN\_CREATION\_SUCCESSFUL | Sikeres token generálás. |
| TOKEN\_CREATION\_FAILED | Sikertelen token generálás. |

## Fájltároló kezelés interfészei

|  |  |
| --- | --- |
| **interfész** | FilestoreUploadService |
| **műveletek** | addFile |
| **OpenAPI** | <https://app.swaggerhub.com/apis/NAVGOVHU/m2m_common/1.0#/FilestoreUploadService> |
| **leírás** | Fájlfeltöltést támogató interfész |

|  |  |
| --- | --- |
| **interfész** | FilestoreDownloadService |
| **műveletek** | getFileStatus |
| **OpenAPI** | <https://app.swaggerhub.com/apis/NAVGOVHU/m2m_common/1.0#/FilestoreDownloadService> |
| **leírás** | Fájlletöltést támogató interfész |

## *Fájlfeltöltés művelete*

**Tulajdonságok:**

|  |  |
| --- | --- |
| **művelet** | addFile |
| **interfész** | FilestoreUploadService |
| **művelettípus** | POST |
| **path** | /NavM2mCommon/filestoreUploadService/File |
| **OpenAPI** | <https://app.swaggerhub.com/apis/NAVGOVHU/m2m_common/1.0#/FilestoreUploadService/addFile> |
| **leírás** | A fájlok fájltárolóba való feltöltését biztosító művelet. A fájl mellett a fájlból képzett SHA-256 hash-t is át kell adni, amit az M2M ellenőriz. A válaszban a fájl egyedi azonosítóját adja meg a fájltárolóban, és elindítja a vírusellenőrzést. A vírusellenőrzés hosszabb ideig is eltarthat, ezért annak eredményét nem a válaszban adja vissza, hanem a getFileStatus művelettel kérdezhető le. A feltöltött fájlokat egy napig őrzi meg a rendszer, utána törlődnek. Ha 30mp-en belül befejeződik a víurellenőrzés, akkor azonnal visszakapja a választ. |

**Bemenő paraméterek:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **név** | **típus** | **hely** | **kötelező** | **leírás** |
| file | bináris | body | igen | A fájltárolóba betöltendő fájl. |
| sha256hash | string | query | igen | A fájltárolóba betöltendő fájlból képzett SHA-256 hash. |
| signature | string | query | igen | Aláírás.  ***Az aláírásban szereplő műveletfüggő adat az sha256hash kell legyen.*** |

Tájékoztatásként a használt, de az interfészen nem előírt minták:

|  |  |  |  |
| --- | --- | --- | --- |
| **név** | **hossz** | **minta** | **alapérték** |
| sha256hash | 64 | [0-9a-fA-F]{64} |  |
| signature | 44-64 | .{44-64} | - |

**Válasz:**

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

Az AddFileResponseType attribútumai a következők:

|  |  |  |  |
| --- | --- | --- | --- |
| **név** | **típus** | **kötelező** | **leírás** |
| fileId | string | nem | A fájl egyedi azonosítója, ami alapján a fájlra hivatkozni lehet. |
| result\_code | FileUploadResult | igen | Válaszkód |
| virusScanResultCode | VirusScanResult | igen | Válaszkód |
| resultMessage | string | nem | Válaszüzenet |

Tájékoztatásként a használt, de az interfészen nem előírt minták:

|  |  |  |  |
| --- | --- | --- | --- |
| **név** | **hossz** | **minta** | **alapérték** |
| fileId | 36 | [0-9a-fA-F]{8}-([0-9a-fA-F]{4}-){3}[0-9a-fA-F]{12} | - |

**Válaszkódok:**

A FileUploadResult enum lehetséges értékei:

|  |  |
| --- | --- |
| **kód** | **jelentés** |
| UPLOAD\_SUCCESS | Sikeres fájl feltöltés. Nem jelenti azt, hogy a fájl nem vírusos. A vírusellenőrzés eredményét a GetFileStatus művelettel kell lekérdezni. |
| HASH\_FAILURE | A fájl-ról képzett sha256 hash nem egyezik a paraméterben megadottal. |
| OTHER\_ERROR | Egyéb hiba következett be a feltöltés során. |

## *Fájlstátusz lekérdezés művelete*

**Tulajdonságok:**

|  |  |
| --- | --- |
| **művelet** | getFileStatus |
| **interfész** | FilestoreDownloadService |
| **művelettípus** | GET |
| **path** | /NavM2mCommon/filestoreDownloadService/File/{fileId} |
| **OpenAPI** | [https://app.swaggerhub.com/apis/NAVGOVHU/m2m\_common/1.0#/FilestoreDownloadService/getFileStatus](https://app.swaggerhub.com/apis/NANASSYLASZLO/nav-m2m_common/1.0#/FilestoreDownloadService/getFileStatus) |
| **leírás** | A fájlok státuszának lekérdezését biztosító művelet, amely visszaadja a vírusellenőrzés eredményét. |

**Bemenő paraméterek:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **név** | **típus** | **hely** | **kötelező** | **leírás** |
| fileId | string | path | igen | A fájl egyedi azonosítója. |

Tájékoztatásként a használt, de az interfészen nem előírt minták:

|  |  |  |  |
| --- | --- | --- | --- |
| **név** | **hossz** | **minta** | **alapérték** |
| fileId | 36 | [0-9a-fA-F]{8}-([0-9a-fA-F]{4}-){3}[0-9a-fA-F]{12} | - |

**Válasz:**

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

A GetFileStatusResponseType attribútumai a következők:

|  |  |  |  |
| --- | --- | --- | --- |
| **név** | **típus** | **kötelező** | **leírás** |
| retentionTime | datetime | igen | Az állomány garantált megőrzési ideje. |
| resultCode | VirusScanResult | igen | Válaszkód |
| resultMessage | string | nem | Válaszüzenet |

**Válaszkódok:**

A VirusScanResult enum lehetséges értékei:

|  |  |
| --- | --- |
| **kód** | **jelentés** |
| PASSED | A vírusellenőrző nem talált problémát. |
| FAILED | Vírusosnak jelölt és törölt állomány. |
| WAITING | A vírusellenőrzés még folyamatban van. |
| OTHER\_ERROR | Egyéb hiba következett be az ellenőrzés során. |

# Környezetek elérhetősége

## Teszt környezet

M2M fake service publikus végpont: **m2m-dev.nav.gov.hu**

## Éles környezet

M2M publikus végpont: **m2m.nav.gov.hu**

## Definíciók elérhetősége:

REST: **rest.api.nav.gov.hu**

[https://rest.api.nav.gov.hu/definitions/services/{verzió}/{api}](https://rest.api.nav.gov.hu/definitions/services/%7bverzió%7d/%7bapi%7d)

SOAP: **soap.api.nav.gov.hu**

A WSDL-ek és XSD-k névtere és a SoapAction jelenleg a következő tartományokban vannak definiálva:

* [https://soap.api.nav.gov.hu/definitions/services/{verzió}/{api}](https://soap.api.nav.gov.hu/definitions/services/%7bverzió%7d/%7bapi%7d)
* [https://soap.api.nav.gov.hu/definitions/messages/{verzió}/{api}](https://soap.api.nav.gov.hu/definitions/messages/%7bverzió%7d/%7bapi%7d)
* [https://soap.api.nav.gov.hu/definitions/model/{verzió}/\*](https://soap.api.nav.gov.hu/definitions/model/%7bverzió%7d/*)
* [https://soap.api.nav.gov.hu/definitions/services/{verzió}/{api}#operation](https://soap.api.nav.gov.hu/definitions/services/%7bverzió%7d/%7bapi%7d#operation)