

Σύστημα Άυλων Υποβολών Παρόχων – Φάρμακο

**Τεχνική Προδιαγραφή API προς τρίτους φορείς για την
ανάκτηση και διαχείριση στοιχείων ταυτοποίησης συνταγών**

08/01/2026

Τεχνική Προδιαγραφή API Ταυτοποίησης Συνταγών

1. Εισαγωγή

Το παρόν έγγραφο περιγράφει το API που παρέχεται από την εφαρμογή προς τρίτους φορείς για την ανάκτηση και διαχείριση στοιχείων ταυτοποίησης συνταγών.

Το API υποστηρίζει δύο εναλλακτικούς τρόπους ολοκλήρωσης (integration patterns):

- **Long Polling**
- **Webhook (Callback mechanism)**

Και στις δύο περιπτώσεις εφαρμόζονται κοινές αρχές ασφάλειας, ταυτοποίησης και ακεραιότητας δεδομένων.

2. Κοινές Αρχές Ασφάλειας & Ταυτοποίησης

Όλες οι εισερχόμενες κλήσεις προς το API πρέπει να περιλαμβάνουν τα παρακάτω υποχρεωτικά πεδία:

```
{  
  
  "Usr": "username",  
  
  "Psw": "password",  
  
  "UniqueCode": "XXXXXX",  
  
  "Digest": "hash",  
  
  "RequestObject": { }  
  
}
```

2.1 Credentials

- **Usr / Psw:** Στοιχεία αυθεντικοποίησης που αποδίδονται στον καταναλωτή του API.
- Τα credentials είναι μοναδικά ανά φορέα.

2.2 UniqueCode

- Υποχρεωτικά μοναδικό ανά κλήση API.
- Συνιστώμενη μορφή: {PrescriptionNum}_{IncrementalNumber}
 - Παράδειγμα:123456789_01

2.3 Digest

Το Digest χρησιμοποιείται για την επαλήθευση της ακεραιότητας και της γνησιότητας του αιτήματος.

Παράγεται ως hash (π.χ. SHA-256) του παρακάτω concatenated string:

PrescriptionNum|CurrentYear|CurrentMonth|ClientSecret

- **ClientSecret** αποδίδεται στον φορέα κατά την ένταξή του στο σύστημα.
- Το Digest επαληθεύεται server-side πριν από οποιαδήποτε επεξεργασία.

3. Λειτουργία A: Ανάκτηση στοιχείων ταυτοποίησης μέσω Long Polling

3.1 Περιγραφή

Η λειτουργία αυτή επιτρέπει στον καταναλωτή να ανακτή την κατάσταση και τα στοιχεία ταυτοποίησης μίας συνταγής, μέσω επαναλαμβανόμενης κλήσης (long polling), έως ότου ολοκληρωθεί η διαδικασία ταυτοποίησης.

Η κλήση πραγματοποιείται βάσει του αριθμού συνταγής.

3.2.1 Request Path

/api/v1/VerificationStatus/retrieve

3.2.2 Request Method

Post

3.2.3 Payload Αιτήματος

```
{  
  "Usr": "username",  
  "Psw": "password",  
  "UniqueCode": "123456789_01",  
  "Digest": "654621b5b2e5e2d0510d4a636be5e6ce669b1f6018e637d14c36b9424f199478",  
  "RequestObject": {  
    "PrescriptionNum": "123456789"  
  }  
}
```

3.3 Payload Απόκρισης

```
{  
  "ResultID": true,  
  "ResultCode": "XXX-XXX",  
  "ResultReason": "",  
  "ResultData": {  
    "PersonVerified": true,  
    "PersonName": "ΙΩΑΝΝΗΣ",  
    "PersonSurname": "ΠΑΠΑΔΟΠΟΥΛΟΣ",  
    "VerificationCode": "ABC123",  
  }  
}
```

```
    "VerificationDateTime": "2025-01-12T14:35:22"
  }
}
```

Σημειώσεις:

- PersonVerified = false υποδηλώνει ότι η διαδικασία ταυτοποίησης δεν έχει ακόμη ολοκληρωθεί.
- Το endpoint δύναται να παραμένει σε αναμονή (blocking) για προκαθορισμένο χρονικό διάστημα (timeout).

4. Λειτουργία B: Ανάκτηση στοιχείων ταυτοποίησης μέσω Webhook

4.1 Περιγραφή

Η λειτουργία Webhook ακολουθεί ασύγχρονο μοντέλο επικοινωνίας.

Η διαδικασία περιλαμβάνει δύο στάδια:

1. **Ενεργοποίηση διαδικασίας ταυτοποίησης**
2. **Αποστολή αποτελέσματος μέσω callback (webhook)**

Μετά την επιτυχή ενεργοποίηση, η συνταγή:

- Κλειδώνει για **15 λεπτά**
- Μεταβαίνει σε κατάσταση «Προς Ταυτοποίηση»

4.2 Ενεργοποίηση Διαδικασίας Ταυτοποίησης

4.2.1 Request Path

/api/v1/VerificationStatus/Start

4.2.2 Request Method

Post

4.2.3 Payload Αιτήματος

```
{
  "Usr": "username",
  "Psw": "password",
  "UniqueCode": "123456789_01",
  "Digest":
    "654621b5b2e5e2d0510d4a636be5e6ce669b1f6018e637d14c36b9424f1994",
  "RequestObject": {
```

```
    "PrescriptionNum": "123456789"
  }
}
```

4.3 Payload Απόκρισης

```
{
  "ResultID": true,
  "ResultCode": "XXX-XXX",
  "ResultReason": "",
  "ResultData": {
    "VerificationCode": "ABC123"
  }
}
```

5. Webhook Endpoint (Callback)

5.1 Γενική Περιγραφή

Ο καταναλωτής του API οφείλει να παρέχει HTTP endpoint (Webhook URL), στο οποίο η εφαρμογή θα αποστέλλει το αποτέλεσμα της ταυτοποίησης.

Η κλήση του Webhook:

- Μπορεί να γίνεται **με ή χωρίς API Key**
- Η χρήση API Key ορίζεται κατά την ενεργοποίηση της ροής
- Το API Key αποστέλλεται μέσω HTTP Header
- Η Κλήση είναι HTTP Post.

5.2 Headers (προαιρετικά)

X-API-KEY: your-defined-api-key

Content-Type: application/json

5.3 Payload Webhook

```
{
  "PrescriptionCode": "123456789",
  "PersonVerified": true,
  "PersonName": "ΙΩΑΝΝΗΣ",
  "PersonSurname": "ΠΑΠΑΔΟΠΟΥΛΟΣ",
  "VerificationCode": "ABC123",
  "VerificationDateTime": "2025-01-12T14:35:22"
}
```

6. Διαχείριση Σφαλμάτων

Κοινή μορφή σφάλματος για όλα τα endpoints:

```
{  
  
  "ResultID": false,  
  "ResultCode": "XXX-XXX",  
  "ResultReason": "Περιγραφή σφάλματος",  
  "ResultData": null  
  
}
```

Ενδεικτικοί κωδικοί:

- "DG001" => Το Digest είναι λάθος
- "UC001" => Ο μοναδικός κωδικός είναι λάθος.
- "USRNF001" => Ο χρήστης δεν βρέθηκε.
- "PRESCNF001" => Η συνταγή δεν βρέθηκε.
- "E00001" => Σφάλμα εκτέλεσης στον κώδικα, επιστρέφεται και το exception message