ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
& ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

Κέντρο Διαλειτουργικότητας

Οδηγός Υλοποίησης -Τεχνικές Προδιαγραφές για Φορείς Παρόχους Διαδικτυακών Υπηρεσιών στο Κέντρο Διαλειτουργικότητας του Υπουργείου Ψηφιακής Διακυβέρνησης

Version 0.80 - 16/10/2024

Περιεχόμενα

1. Εισαγωγή

Το παρόν έγγραφο περιγράφει τις τεχνικές προδιαγραφές των διαδικτυακών υπηρεσιών των Φορέων με σκοπό τη διάθεση (των υπηρεσιών) στο Κέντρο Διαλειτουργικότητας της ΓΓΠΣΨΔ.

Περιέχει χρήσιμες πληροφορίες για τον τρόπο με τον οποίο θα πρέπει να αναπτυχθούν από τους Φορείς τα APIs, ώστε να είναι δυνατή η ενσωμάτωσή τους στο Κέντρο Διαλειτουργικότητας. Περιγράφονται οι μορφές της εισόδου και της αναμενόμενης απάντησης, η διαχείριση λαθών καθώς και η ασφάλεια.

2. Επισκόπηση

Ακολουθούν συνοπτικά οι προδιαγραφές που χρειάζεται να έχει κάθε καινούργια υπηρεσία που πρόκειται να διατεθεί για υλοποίηση και ενσωμάτωση στο Κέντρο Διαλειτουργικότητας.

1. Η υπηρεσία θα είναι τεχνολογίας REST και θα δέχεται κλήσεις με τη μέθοδο POST (σε συγκεκριμένες περιπτώσεις, που αφορούν κυρίως ανάκτηση στοιχείων με βάση απλά κριτήρια αναζήτησης, μπορεί να χρησιμοποιηθεί και η μέθοδος GET)

2. Όλα τα επιχειρησιακά δεδομένα θα μεταβιβάζονται ως json request, σε UTF-8 encoding, μέσα στο σώμα (body) της POST κλήσης που θα γίνεται προς την υπηρεσία

3. Ως μέθοδος αυθεντικοποίησης (για την πρόσβαση στην υπηρεσία από το ΚΕΔ) θα χρησιμοποιείται Basic Authorization ή Bearer Authorization (προτείνεται η μέθοδος Basic Authorization)

4. Σε περίπτωση ανεπιτυχούς αυθεντικοποίησης, η υπηρεσία θα επιστρέφει http status 401

5. Σε περίπτωση επιτυχημένης απάντησης, η υπηρεσία θα επιστρέφει http status 200 και η απάντηση θα έρχεται σε json format (UTF-8 encoding). Αν έχει συμβεί κάποιο επιχειρησιακό λάθος, θα επιστρέφεται μια συνοπτική περιγραφή του λάθους σε ειδικό πεδίο εξόδου (π.χ. {"errorMessage": "Δεν βρέθηκαν αποτελέσματα"})

6. Σε περίπτωση σοβαρού σφάλματος (π.χ αδυναμία ανάγνωσης του body request λόγω μη έγκυρου format ή μη διαχειρήσιμη εξαίρεση), η υπηρεσία θα επιστρέφει http status 500 ή 400 (όποιο βολεύει, αρκεί να είναι διαφορετικό από το status 200)

7. Αν χρειάζεται να διακινηθούν binary δεδομένα, αυτά θα μεταβιβάζονται στην κλήση σε ένα πεδίο τύπου String με **κωδικοποίηση base64**

8. Η υπηρεσία θα διαθέτει δύο ξεχωριστά περιβάλλοντα: το δοκιμαστικό και το παραγωγικό

9. Κάθε καινούργια υπηρεσία θα πρέπει να συνοδεύεται από ένα αναλυτικό εγχειρίδιο τεχνικών προδιαγραφών το οποίο θα αναλύει τη λειτουργικότητα της υπηρεσίας που διατίθεται και θα περιέχει μια συνοπτική περιγραφή για όλα τα επιχειρησιακά πεδία εισόδου & εξόδου της υπηρεσίας. Επίσης, το εγχειρίδιο πρέπει να περιλαμβάνει αρκετά παραδείγματα κλήσης (full json requests & json responses) ώστε να καλύπτει (όλες, αν είναι εφικτό) τις δυνατές περιπτώσεις που μπορούν να παρουσιαστούν

10. Για τις δοκιμές και του ελέγχους της νέας υπηρεσίας από το Κέντρο Διαλειτουργικότητας, χρειάζεται να διατεθούν μερικά δοκιμαστικά δεδομένα εισόδου (test input data). Τα δοκιμαστικά δεδομένα θα μπορούσαν (ιδανικά) να περιλαμβάνονται μέσα στο εγχειρίδιο τεχνικών προδιαγραφών, σε ειδική/ξεχωριστή ενότητα

3. Προδιαγραφές των υπηρεσιών προς υλοποίηση

Στην ενότητα αυτή αποτυπώνονται οι προδιαγραφές που χρειάζεται να έχει η διαδικτυακή υπηρεσία που θα αναπτύξει/υλοποιήσει ένας Φορέας και θα διαθέσει στο Κέντρο Διαλειτουργικότητας.

Ο Φορέας θα χρειαστεί να υλοποιήσει μια διαδικτυακή υπηρεσία τεχνολογίας **REST** (API) με τα παρακάτω τεχνικά χαρακτηριστικά:

- Το API θα πρέπει γενικά να είναι τεχνολογίας **REST** και να δέχεται **POST** κλήσεις. Σε συγκεκριμένες περιπτώσεις, που αφορούν κυρίως ανάκτηση στοιχείων με βάση κάποια απλά κριτήρια αναζήτησης (π.χ. αριθμός μητρώου), μπορεί να χρησιμοποιηθεί και η μέθοδος **GET**
- Όλα τα επιχειρησιακά δεδομένα θα μεταβιβάζονται ως json request, σε UTF-8 encoding, μέσα στο σώμα (body) της **POST** κλήσης που θα γίνεται προς το API
- Αν η κλήση υποστηρίζει τη μέθοδο GET, θα δέχεται τα ορίσματα κλήσης ως παραμέτρους στο HTTP GET REQUEST (π.χ. /service?afm=000000000&amka=01010100007)
- Το API του Φορέα θα μπορεί να υποδεχτεί σαν header παράμετρο (header parameter: "CALL_ID") το μοναδικό αριθμό κλήσης του ΚΕ.Δ. (callSequenceId). Το ΚΕ.Δ. θα μεταβιβάζει τον μοναδικό/αναγνωριστικό αριθμό κλήσης (callSequenceId, που είναι ένας μεγάλος αριθμός μέχρι 16 ψηφία) σαν header παράμετρο (CALL_ID) στην κλήση που θα κάνει προς το API του Φορέα. Καλό θα είναι το Πληροφοριακό Σύστημα του Φορέα να καταγράφει την μεταβιβαζόμενη τιμή για λόγους troubleshooting
- Ως μέθοδος αυθεντικοποίησης (για την πρόσβαση στο API από το ΚΕ.Δ.) θα χρησιμοποιείται **Basic ή Bearer Authorization**
- Σε περίπτωση ανεπιτυχούς αυθεντικοποίησης, το API θα επιστρέφει **http status 401**
- Σε περίπτωση απαγόρευσης πρόσβασης (IP restriction) λόγω άγνωστης IP address, το API θα επιστρέφει **http status 403 (Παράρτημα Β)**
- Σε περίπτωση σοβαρού σφάλματος (π.χ αδυναμία ανάγνωσης του body request λόγω μη έγκυρου format ή μη διαχειρίσιμη εξαίρεση) το API θα επιστρέφει **http status 500 ή 400**
- Σε περίπτωση επιτυχημένης απάντησης, το API θα επιστρέφει **http status 200** και η απάντηση θα έρχεται σε json format (UTF-8 encoding)
- Αν χρειάζεται να διακινηθούν binary data (π.χ. δεδομένων αρχείων φωτογραφίας ή PDF κλπ), αυτά θα μεταβιβάζονται στην κλήση σε ένα πεδίο τύπου String με **κωδικοποίηση base64**

Η υπηρεσία που θα υλοποιήσει ο Φορέας θα έχει δύο περιβάλλοντα: το δοκιμαστικό (TEST) και το παραγωγικό (PROD). Επομένως θα διαθέτει δύο σημεία κλήσης (endpoints) τα οποία και θα γνωστοποιηθούν στο Κέντρο Διαλειτουργικότητας (μαζί με τα credentials για την αυθεντικοποίηση). Παράδειγμα URLs:

Δοκιμαστικό περιβάλλον (TEST): ***https://foreas.gr/ked/test/service***
Παραγωγικό περιβάλλον (PROD): ***https://foreas.gr/ked/service***

Όταν η υπηρεσία του Φορέα είναι έτοιμη στο δοκιμαστικό περιβάλλον, θα πρέπει να γνωστοποιούνται στο ΚΕΔ τα σημεία κλήσης της (endpoints) καθώς και τα διαπιστευτήρια (username & password) για την αυθεντικοποίηση.

1. Είσοδος-Request

Η υπηρεσία θα υποστηρίζει κλήσεις με τη μέθοδο **POST** και θα δέχεται αιτήματα σε **JSON format** (**UTF-8 encoding**).

HTTP μέθοδος	**POST**
URI	**/serviceName**
Headers	**Authorization: Basic <encoded_credentials> OR Bearer <access_token>** **Content-type: application/json; charset=utf-8** **CALL_ID: <callSequenceId>**
Παράδειγμα ENDPOINT	**https://foreas.gr/ked/serviceName**

Οι παράμετροι εισόδου για την κλήση του API θα μεταβιβάζονται σε JSON μορφή και θα περιλαμβάνουν διακριτά πεδία («επιχειρησιακά πεδία εισόδου»). Οι τεχνικές ονομασίες των πεδίων θα πρέπει να αποτελούνται μόνο από λατινικά γράμματα και αριθμούς (απαγορεύεται η χρήση ελληνικών, σημείων στίξης, ειδικών χαρακτήρων κλπ) και συνίσταται να δίνονται σε **camelCase μορφή** (π.χ. firstName, birthDate, requestType, personalPhoneNumber κλπ).

Στο εγχειρίδιο τεχνικών προδιαγραφών της υπηρεσίας, θα πρέπει να υπάρχει ειδικός πίνακας στον οποίο θα αποτυπώνονται όλα τα πεδία εισόδου της κλήσης, μαζί με μια σύντομη τεχνική περιγραφή αλλά και τον τύπο (και μήκος) δεδομένων κάθε πεδίου. Όταν ένα πεδίο εισόδου είναι υποχρεωτικό να δίνεται στην είσοδο, αυτό θα πρέπει να επισημαίνεται (π.χ. με ένα αστεράκι ή με ειδική αναφορά στην περιγραφή του πεδίου).

Ακολουθεί ένα παράδειγμα πίνακα πεδίων εισόδου:

Πεδίο	**Περιγραφή**	**Τύπος δεδομένων (Μήκος)**
requestType*	Τύπος αιτήματος. Δυνατές τιμές: 1 => Αίτηση χωρίς δικαιολογητικά 2 => Αίτηση με δικαιολογητικά	**Integer (1)**
afm*	Αριθμός Φορολογικού Μητρώου του πολίτη	**String (9)**
name*	Όνομα πολίτη	**String (40)**
surname*	Επώνυμο πολίτη	**String (80)**
fatherName	Πατρώνυμο πολίτη	**String (40)**
motherName	Μητρώνυμο πολίτη	**String (40)**
birthDate*	Ημερομηνία γέννησης πολίτη. Μορφή: dd/mm/yyyy (π.χ. 18/04/1986)	**String (10)**

**** το πεδίο συμπληρώνεται υποχρεωτικά στην είσοδο***

2. Απάντηση-Response

Στις «επιτυχημένες» κλήσεις προς την υπηρεσία, το http status της απόκρισης θα είναι **200** και το περιεχόμενο θα επιστρέφεται σε JSON μορφή (**UTF-8 encoding**). Δηλαδή τα πεδία εξόδου («επιχειρησιακά πεδία εξόδου») θα επιστρέφονται σε JSON format.

Για τις τεχνικές ονομασίες των πεδίων εξόδου ισχύει ό,τι ακριβώς και για τα πεδία εισόδου: τα πεδία εξόδου θα πρέπει να αποτελούνται μόνο από λατινικά γράμματα και αριθμούς και συνίσταται να δίνονται σε **camelCase μορφή** (π.χ. successCode, requestId, fileBase64Data, κλπ).

Στο εγχειρίδιο τεχνικών προδιαγραφών της υπηρεσίας, θα υπάρχει ειδικός πίνακας στον οποίο θα αποτυπώνονται όλα τα πεδία εξόδου της κλήσης, μαζί με μια σύντομη τεχνική περιγραφή αλλά και τον τύπο (και μήκος) δεδομένων κάθε πεδίου.

Ακολουθεί ένα παράδειγμα πίνακα πεδίων εξόδου:

Πεδίο	Περιγραφή	Τύπος δεδομένων (Μήκος)
successCode	Κωδικός επιτυχημένης υποβολής αιτήματος. Επιστρέφει 1 σε περίπτωση επιτυχίας	**Integer (1)**
requestId	Μοναδικός κωδικός αιτήματος	**Integer (6)**
requestDate	Ημερομηνία υποβολής αιτήματος (dd/mm/yyyyy)	**String (10)**
info	Ενημερωτικό μήνυμα	**String (100)**
errorMessage	Μήνυμα λάθους. Επιστρέφει περιεχόμενο αν παρουσιαστεί κάποιο σφάλμα κατά την κλήση, διαφορετικά επιστρέφει null	**String (100)**

Επισήμανση: Τα πεδία εξόδου που επιστρέφουν τιμή (null) στην απάντηση, μπορούν είτε να αποτυπώνονται στο response ρητά με την ένδειξη null (π.χ. “mobileNumber”: null) είτε να μην αποτυπώνονται καθόλου (αυτό αυτομάτως θα σημαίνει ότι το πεδίο είναι null).

Παράδειγμα κλήσης (request & response):

Method: **POST**

HTTP Headers:

Authorization: **Basic** dXNlcjpwYXNzd29yZDE=

Content-Type: application/json; charset=utf-8

CALL_ID: 1234567890123456 <--- μοναδικός αριθμός κλήσης του ΚΕ.Δ. (callSequenceId)

Request:

```
{
  "requestType": 1,
  "afm": "000000000",
  "name": "ONOMA",
  "surname": "ΕΠΩΝΥΜΟ",
  "fatherName": "ΠΑΤΡΩΝΥΜΟ",
  "motherName": "ΜΗΤΡΩΝΥΜΟ",
  "birthDate": "21/05/1990"
}
```

Response (HTTP STATUS 200):

```
{
  "successCode": 1,
  "requestId": 12345,
  "requestDate": "11/10/2024",
  "errorMessage": null
}
```

4. Ασφάλεια (Security)

1. Ασφάλεια & Μέθοδος αυθεντικοποίησης

Για την αυθεντικοποίηση των υπηρεσιών μπορεί να χρησιμοποιηθεί είτε **Basic Authorization** είτε **Bearer Authorization**, αλλά ως μέθοδος αυθεντικοποίησης προτείνεται η **Basic Authorization.**

Ο Φορέας που έχει υλοποιήσει την υπηρεσία, θα διαθέτει στο Κέντρο Διαλειτουργικότητας ζευγάρια συνθηματικών (username και password), ένα για το δοκιμαστικό και ένα για το παραγωγικό περιβάλλον, για την αυθεντικοποίηση των κλήσεων. Τα διαπιστευτήρια θα χρησιμοποιηθούνται αποκλειστικά από το Κέντρο Διαλειτοργικότητας.

1.1 Αυθεντικοποίηση μέσω Basic Authorization

Στην υποενότητα αυτή περιγράφεται η μέθοδος αυθεντικοποίησης μέσω **Basic Authorization,** η οποία και συνίσταται στους Φορείς.

Κάθε κλήση που θα πραγματοποιείται προς την υπηρεσία του Φορέα, θα περιλαμβάνει έναν Header ο οποίος θα περιέχει το όνομα χρήστη και τον κωδικό πρόσβασης, σε κωδικοποιημένη μορφή **Base64**. Ο header θα είναι της μορφής:

*Authorization: **Basic** <**διαπιστευτήρια**>*

όπου τα διαπιστευτήρια είναι η κωδικοποίηση σε Base64 του ονόματος χρήστη και του κωδικού πρόσβασης, συνενωμένα με το χαρακτήρα ":".

Για παράδειγμα, αν το όνομα χρήστη είναι "user" και ο κωδικός πρόσβασης είναι "password1", τότε θα πρέπει να συμπεριληφθεί ο παρακάτω Header για την αυθεντικοποίηση:

*Authorization: **Basic** **dXNlcjpwYXNzd29yZDE=***

όπου "**dXNlcjpwYXNzd29yZDE=**" είναι η Base64 κωδικοποίηση του αλφαριθμητικού "**user:password1**".

Σε περίπτωση που δοθούν λανθασμένα διαπιστευτήρια (δηλαδή λάθος username ή password) τότε η υπηρεσία του Φορέα θα επιστρέφει status **401/Unauthorized** χωρίς response.
Στην περίπτωση που το ζεύγος των διαπιστευτηρίων (username και password) που χρησιμοποιούνται στο authorization header είναι σωστά ΚΑΙ η κλήση πραγματοποιείται από αναμενόμενη IP address ΚΑΙ στο σώμα εισόδου περιλαμβάνεται ένα έγκυρο json

request, η υπηρεσία του Φορέα θα απαντάει με http status **200** και με κατάλληλο response, που θα περιλαμβάνει τα επιχειρησιακά πεδία εξόδου της υπηρεσίας.

Σε περίπτωση που στην είσοδο (body) δεν δοθεί ένα έγκυρο json request με τα προβλεπόμενα πεδία εισόδου (κακοσχηματισμένο request), η υπηρεσία του Φορέα θα επιστρέφει http status **500/Internal Server Error**.

1.2 Αυθεντικοποίηση μέσω Bearer Authentication

Στην περίπτωση που επιλεγεί αυτή η μέθοδος αυθεντικοποίησης, ο Φορέας θα πρέπει να διαθέσει ένα επιπλέον API για την αυθεντικοποίηση και την παραγωγή ενός προσωρινού token. Το API αυτό, το οποίο προτείνεται να ονομάζεται **authenticate ή authToken**, θα χρησιμοποιείται για την εξουσιοδότηση και τη λήψη ενός κουπονιού πρόσβασης (access token) βραχείας διάρκειας:

HTTP μέθοδος	**POST**
URI	**/authenticate**
Headers	**Authorization: Basic <κωδικοποιημένα διαπιστευτήρια>**
Παράδειγμα ENDPOINT (TEST)	**https://foreas.gr/ked/test/authenticate**
Παράδειγμα ENDPOINT (PROD)	**https://foreas.gr/ked/authenticate**

Στην αρχή της επικοινωνίας μεταξύ του Φορέα και του Κέντρου Διαλειτουργικότητας, το Κέντρο Διαλειτουργικότητας θα χρειαστεί να αποκτήσει ένα access token περιορισμένης διάρκειας. Γι' αυτό το σκοπό, θα πρέπει να παρέχεται μια προκαταρκτική κλήση απόκτησης του token, με μια POST κλήση προς το API **authenticate** και χρήση Basic Authorization (δηλαδή με username και password - https://datatracker.ietf.org/doc/html/rfc7617).

Ο Φορέας θα διαθέσει εκ των προτέρων στο Κέντρο Διαλειτουργικότητας ένα ζευγάρι συνθηματικών (username & password) για την αυθεντικοποίηση. Το ΚΕΔ θα δημιουργήσει ένα string της μορφής username:password, θα το κωδικοποιεί σε base64 και θα το προσθέτει στους headers της POST κλήσης προς το API **authenticate**, ως εξής:

POST https://foreas.gr/ked/authenticate
Header => Authorization: Basic <base64 encoded username:password>

Για παράδειγμα, αν το όνομα χρήστη είναι "user" και ο κωδικός πρόσβασης είναι "password1", τότε πρέπει στην κλήση να προστεθεί ο παρακάτω Authorization Header για την αυθεντικοποίηση:

Authorization: **Basic dXNlcjpwYXNzd29yZDE=**

όπου "dXNlcjpwYXNzd29yZDE=" είναι η Base64 κωδικοποίηση του αλφαριθμητικού "user:password1".

Διαφορετικά, π.χ. με χρήση της εντολής curl που κάνει αυτόματα τη μετατροπή σε base64:

curl -X POST https://foreas.gr/ked/service/authenticate -u 'user:password1'

Οι αποκρίσεις λάθους του API **authenticate** σε περίπτωση αποτυχημένης εξουσιοδότησης λόγω χρήσης λανθασμένων συνθηματικών θα είναι **401/Unauthorized**, ενώ σε περίπτωση κλήσης από «άγνωστη» IP (δηλαδή από IP που δεν ανήκει στις υποδομές του ΚΕΔ – Παράρτημα Β) θα είναι **403/Forbidden**.

Εφόσον το ζεύγος username και password είναι σωστά, το API **authenticate** θα απαντάει με http status 200 και στο response θα επιστρέφει τις παρακάτω πληροφορίες σε json μορφή:

** τον τύπο του token (token_type: Bearer)*
** το προσωρινό token (access_token)*
** τη διάρκειά του σε δευτερόλεπτα (expires_in)*

Παράδειγμα επιτυχημένης απόκρισης (HTTP STATUS 200) του API **authenticate**:

```
{
  "token_type": "Bearer",
  "access_token": "6B29FC40-CA47-1067-B31D-00DD010662DA",
  "expires_in": "600"
}
```

Το access_token που επιστρέφεται μπορεί να είναι μορφής JWT ή απλώς ένα GUID. Το access token θα πρέπει να αρκεί ώστε να δώσει πρόσβαση στο κυρίως API του Φορέα και συνίσταται να έχει διάρκεια 600 δευτερόλεπτα/10 λεπτά (δηλαδή, το expires_in συνίσταται να επιστρέφει την τιμή 600). Όλες οι κλήσεις προς το κυρίως API θα περιέχουν το access token (που λήφθηκε από το API **authenticate**) στο header της κλήσης με την παρακάτω μορφή:

Authorization: Bearer <access_token>

Σε περίπτωση που το access token είναι λανθασμένο (μη έγκυρο) ή ληγμένο, τότε το κυρίως API θα επιστρέφει http status **401/Unauthorized** χωρίς response

2. Διαδικτυακή Πρόσβαση

Η δικτυακή πρόσβαση στις υπηρεσίες των Φορέων θα γίνεται με **HTTPS/TLS1.2** μέσα από τις υποδομές της ΓΓΠΣ&ΨΔ, με κωδικούς χρήσης που θα δίνονται από τους Φορείς. Οι διαδικτυακές διευθύνσεις (IP addresses) του ΚΕ.Δ. της ΓΓΠΣ&ΨΔ θα δοθούν στο Φορέα ώστε να διασφαλίσει την πρόσβαση στην συγκεκριμένη υπηρεσία μόνο από τις συγκεκριμένες διευθύνσεις (**Παράρτημα Β**). Αντίστοιχα, οι διευθύνσεις (IP addresses) των υπηρεσιών των Φορέων θα δοθούν στη ΓΓΠΣ&ΨΔ, ώστε να διασφαλισθεί η άντληση πληροφοριών μόνο από τις συγκεκριμένες διευθύνσεις.

Σε περίπτωση που πραγματοποιηθεί κλήση προς την υπηρεσία από κάποια IP address που δεν ανήκει στη λίστα διαδικτυακών διευθύνσεων του Κέντρου Διαλειτουργικότητας, τότε η υπηρεσία του Φορέα θα επιστρέφει http status **403/Forbidden** χωρίς response.
Για τη διαδικτυακή πρόσβαση και τις IPs στις οποίες πρέπει να επιτρέπεται η πρόσβαση, παρακαλούμε δείτε το **Παράρτημα Β**.

5. Αντιμετώπιση/Διαχείριση Λαθών

Αναφορικά με τη διαχείριση λαθών, όπως αναφέρθηκε και παραπάνω, στην υπηρεσία του Φορέα θα πρέπει να υπάρχει ένα διακριτό πεδίο εξόδου (π.χ. errorMessage) το οποίο θα επιστρέφει τιμή όταν συμβεί κάποιο λογικό/επιχειρησιακό σφάλμα.

Ακόμη και στην περίπτωση σφάλματος, το επιστρεφόμενο **HTTP STATUS** πρέπει να είναι **200**, εκτός και αν προκύψει κάποιο πολύ σοβαρό σφάλμα (μη διαχειρίσιμη εξαίρεση) που δεν μπορεί να διαχειριστεί η υπηρεσία του Φορέα – οπότε το HTTP STATUS μπορεί να είναι διαφορετικό (συνήθως **500/Internal Server Error** ή **400/Bad Request**).

Αν οι περιπτώσεις λαθών είναι αρκετές και διαφορετικές, ο Φορέας δύναται να κάνει κάποια ομαδοποίηση και να διαθέσει δύο διακριτά πεδία: ένα για τον κωδικό λάθους (π.χ. errorCode) και ένα για την περιγραφή λάθους (π.χ. errorDescription)

Παραδείγματα response σε περίπτωση λάθους:

-- http status: 200
-- response:

```
{
  "errorMessage": "Δεν βρέθηκαν αποτελέσματα, αλλάξτε τα κριτήρια αναζήτησης"
}
```

ή

-- http status: 200
-- response:

```
{
  "errorCode": "WS_INVALID_INPUT",
  "errorDescription": "Το πεδίου εισόδου afm δεν είναι έγκυρος Αριθμός Φορολογικού Μητρώου"
}
```

Στο εγχειρίδιο τεχνικών προδιαγραφών που θα διαθέσει ο Φορέας, θα πρέπει να υπάρχει ειδική ενότητα για τη διαχείριση λαθών που θα αναφέρει όλες τις δυνατές περιπτώσεις σφαλμάτων και θα περιλαμβάνει ειδικό κωδικολογίο λαθών, δηλαδή πίνακα με όλα τα μηνύματα λαθών που μπορούν να προκύψουν κατά τις κλήσεις της υπηρεσίας.

Παράρτημα Α – Δείγματα κλήσεων των Υπηρεσιών

Για κάθε διαθέσιμο API της υπηρεσίας, θα πρέπει να δίνονται αρκετά παραδείγματα κλήσης (full json requests & json responses). Οπωσδήποτε ένα παράδειγμα επιτυχημένης κλήσης (επιτυχημένη απόκριση) και ένα παράδειγμα με επιστροφή σφάλματος.

- **API /submitRequest**

Κλήση 1. Παράδειγμα κλήσης με **επιτυχημένη υποβολή αιτήματος**

Request:

```
{
 "requestType": 1,
 "afm": "026310919",
 "name": "ΔΗΜΗΤΡΙΟΣ",
 "surname": "ΤΕΣΤΟΠΟΥΛΟΣ",
 "fatherName": "ΝΙΚΟΛΑΟΣ",
 "motherName": "ΜΑΡΙΑ",
 "birthDate": "08/05/1986"
}
```

Αποτέλεσμα απόκρισης της παραπάνω κλήσης:

```
{
  "successCode": 1,
  "requestId": 123456,
  "requestDate" : "15/10/2024"
  "info" : "Το αίτημα με αριθμό 123456 υποβλήθηκε επιτυχώς",
  "errorMessage": null
}
```

Κλήση 2. Παράδειγμα κλήσης με **αποτυχημένη υποβολή αιτήματος** (**επιχειρησιακό σφάλμα**)

Request:

```
{
  "requestType": 1,
  "afm": "000000000",
  "name": "ΟΝΟΜΑ",
  "surname": "ΕΠΩΝΥΜΟ",
  "fatherName": "ΠΑΤΡΩΝΥΜΟ",
  "motherName": "ΜΗΤΡΩΝΥΜΟ",
  "birthDate": "01/01/1980"
}
```

Αποτέλεσμα απόκρισης της παραπάνω κλήσης:

```
{
  "successCode": 0,
  "errorMessage": "Δεν επιτρέπεται το αίτημα για αυτόν τον πολίτη, ο πολίτης δεν υπάρχει στο Φορολογικό Μητρώο"
}
```

Παράρτημα Β – Περιορισμός πρόσβασης / Διαδικτυακή πρόσβαση προς τις υποδομές του ΚΕΔ (IP restriction)

Για περαιτέρω ασφάλεια, οι υπηρεσίες που θα αναπτυχθούν από τους Φορείς θα πρέπει γενικά να είναι προσβάσιμες μόνο μέσα από τις υποδομές του Κέντρου Διαλειτουργικότητας και να είναι «αποκομμένες» από το υπόλοιπο δίκτυο. Όλες οι κλήσεις θα πραγματοποιούνται μέσα από τους ESB Servers του Κέντρου Διαλειτουργικότητας της ΓΓΠΣ και θα χρειαστεί να δοθεί πρόσβαση προς συγκεκριμένες IP διευθύνσεις. Δηλαδή η **διαδικτυακή πρόσβαση** θα επιτρέπεται μόνο σε **επιλεγμένες IP addresses** και θα απαγορεύεται (access forbidden) προς όλες τις υπόλοιπες.

Η **Public IP address** των υποδομών του Κέντρου Διαλειτουργικότητας είναι η **84.205.223.156**. Η εξερχόμενη http/https κίνηση (destination port) διέρχεται μέσω proxy και ισχύουν και οι παρακάτω IPs:

84.205.231.33 έως **46**
84.205.244.129 έως **142**

Επειδή οι κλήσεις πραγματοποιούνται μέσω proxy server από τους ESB Servers του ΚΕΔ, ισχύουν επιπλέον οι ακόλουθες IPs:

10.16.172.131
10.16.172.132
10.16.172.162
10.16.171.44
10.16.171.45
10.16.171.46
10.16.171.124
10.16.171.125
10.16.171.49
10.30.11.176
10.30.239.242 (Old Proxy Server)
10.30.239.204 (New Proxy Server)
10.30.239.200 έως **207 (interface of new Load Balancer)**
Θα χρειαστεί να δοθεί πρόσβαση προς όλες τις ανωτέρω IPs.

Να επισημανθεί πως επειδή η πρόσβαση θα γίνεται από τους ESB Servers του ΚΕΔ μέσω proxy server, οι κλήσεις ενδέχεται να φθάνουν στις υποδομές των Φορέων (ανάλογα και με τις διαδικτυακές ρυθμίσεις που εφαρμόζονται) με IP addresses (τριπλέτες) της μορφής: (**ESB_Server_IP**, **Proxy_Server_IP**, **Public_IP**), π.χ.
(**10.16.172.132**, **10.30.239.204**, **84.205.223.156**)

Επομένως καλό θα είναι να προστεθούν στο access list όλες οι παραπάνω IPs (ακόμα και οι διευθύνσεις των δικτύων της μορφής 10.X.X.X).

Όταν προς το API του Φορέα πραγματοποιείται μια κλήση από "άγνωστη" IP, το API θα πρέπει να μην αποδέχεται την κλήση και να απαντάει με http status 403/Forbidden.