



ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΚΑΙ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

Κέντρο Διαλειτουργικότητας

Προδιαγραφές για το Web Service
Άντληση Δεδομένων για τη Δ.Π.Κ. του ΠΟΘΕΝ ΕΣΧΕΣ
από Χρηματοπιστωτικούς Οργανισμούς και
Πιστωτικά Ιδρύματα (ΧΟ-ΠΙ)
μέσω του Κέντρου Διαλειτουργικότητας
του Υπουργείου Ψηφιακής Διακυβέρνησης

Περιεχόμενα

Περιεχόμενα	2
1. Εισαγωγή	3
1.1 Όροι Χρήσης της υπηρεσίας Πόθεν Έσχες από τους ΧΟ-ΠΙ.....	4
1.2 Υλοποίηση API Πόθεν Έσχες από τους ΧΟ-ΠΙ για την λήψη αιτημάτων	4
2. Υπηρεσία άντλησης δεδομένων για τη Δ.Π.Κ. του ΠΟΘΕΝ ΕΣΧΕΣ	5
2.1 Διαβίβαση αιτήματος από το ΟΠΣ Πόθεν Έσχες στους ΧΟ-ΠΙ – API: sendPothenAithma	5
2.2 Αποστολή αποτελέσματος αιτήματος προς το ΟΠΣ Πόθεν – API: getPothenData.....	10
2.3 Λήψη πληροφοριών για το δημόσιο κλειδί (public key) της κρυπτογράφησης – API: getEncryptionInfo	13
3. Αυθεντικοποίηση (Authorization).....	15
4. Αντιμετώπιση Λαθών	17
Παράρτημα Α – Δείγματα κλήσεων των Web Services.....	18
Παράρτημα Β – Ημερολόγιο Καταγραφής Κλήσεων	25
Παράρτημα Γ – Περιγραφή τύπων δεδομένων	27
Παράρτημα Δ – Πίνακας ΧΟ-ΠΙ που υποστηρίζονται	30
Παράρτημα Ε – Προς υλοποίηση υπηρεσία από ΧΟ-ΠΙ.....	31
Παράρτημα ΣΤ – Περιορισμός πρόσβασης / Διαδικτυακή πρόσβαση προς τις υποδομές του ΚΕΔ (IP restriction).....	44

1. Εισαγωγή

Το παρόν κείμενο περιέχει τις προδιαγραφές για την άντληση δεδομένων με διαλειτουργικότητα για τη Δήλωση Περιουσιακής Κατάστασης Δ.Π.Κ. (ετήσιας και αρχικής) του ΠΟΘΕΝ ΕΣΧΕΣ από Χρηματοπιστωτικούς Οργανισμούς και Πιστωτικά Ιδρύματα (ΧΟ-ΠΙ), μέσω τεχνολογίας Web Service (WS) και του Κέντρου Διαλειτουργικότητας της ΓΓΠΣΨΔ (εναλλακτικός τρόπος αντί της χρήσης του FTPS).

Το WS περιλαμβάνει υπηρεσίες για αποκλειστική χρήση από το Ολοκληρωμένο Πληροφοριακό Σύστημα του ΠΟΘΕΝ ΕΣΧΕΣ (ΟΠΣ Πόθεν) αλλά και τα Πληροφοριακά Συστήματα των ΧΟ-ΠΙ.

Η συγκεκριμένη υπηρεσία WS παρέχεται μέσω της τεχνολογίας REST (Representational State Transfer) και χρησιμοποιεί Basic ή Bearer Authorization, παρέχεται δε από διακομιστές (server) που χρησιμοποιούν **το πρωτόκολλο TLS 1.2**.

Η πρόσβαση στο πιλοτικό περιβάλλον γίνεται με χρήση του κάτωθι base URL (endpoint):

<https://test.gsis.gr/esbpilot/pothenDataRestService>

Η πρόσβαση στο παραγωγικό περιβάλλον γίνεται με χρήση του κάτωθι base URL (endpoint):

<https://ked.gsis.gr/esb/pothenDataRestService>

1.1 Όροι Χρήσης της υπηρεσίας Πόθεν Έσχες από τους ΧΟ-ΠΙ

Οι ΧΟ-ΠΙ θα πρέπει να απαντούν στα αιτήματα που δέχονται από το ΟΠΣ Πόθεν εντός δύο εργάσιμων ημερών.

Για την ένταξη σε παραγωγική λειτουργία οι ΧΟ-ΠΙ θα πρέπει να δεσμεύονται και να αναφέρουν ρητά στο έγγραφο για ένταξη σε παραγωγική λειτουργία, ότι η απάντησή τους σε κάθε αίτημα που δέχονται από το API «getPothenAithma» θα δίνεται αυστηρά εντός δύο εργάσιμων ημερών, σύμφωνα με το ν. 5026/2023 άρθρο 21 παρ. 7*, όπως τροποποιήθηκε με το ν. 5130/2024 (Α'127) και ισχύει.

(*Για την υποστήριξη της συμπλήρωσης της δήλωσης από τα υπόχρεα πρόσωπα του προηγούμενου εδαφίου, κατόπιν ενημέρωσής τους, πραγματοποιείται άντληση των απαιτούμενων δεδομένων από τους φορείς που διαλειτουργούν εντός δύο (2) εργάσιμων ημερών από την έναρξη συμπλήρωσης της δήλωσης.)

1.2 Υλοποίηση API Πόθεν Έσχες από τους ΧΟ-ΠΙ για την λήψη αιτημάτων

Το παρόν έγγραφο περιέχει πληροφορίες για το API το οποίο πρέπει να υλοποιηθεί από τους ΧΟ-ΠΙ (Παράρτημα Ε). Περιγράφονται η κλήση με έμφαση στα πεδία/ορίσματα, η μορφή της αναμενόμενης απάντησης, η ασφάλεια καθώς και οι πιθανές αποκρίσεις.

Κάθε Χρηματοπιστωτικός Οργανισμός-Πιστωτικό Ίδρυμα θα χρειαστεί να κάνει τα εξής:

1. Να υλοποιήσει και να διαθέσει στο Κέντρο Διαλειτουργικότητας της ΓΠΣΨΔ (ΚΕΔ) ένα REST API (“getPothenAithma”) σύμφωνα με τις προδιαγραφές που περιγράφονται στο Παράρτημα Ε. Η υπηρεσία αυτή απαιτείται για την παραλαβή από τους ΧΟ-ΠΙ αιτημάτων τα οποία αποστέλλονται από το ΟΠΣ Πόθεν
2. Να δημιουργήσει λογισμικό-καταναλωτή (consumer) για το API getPothenData του ΚΕΔ (Ενότητα 2.2). Η υπηρεσία αυτή χρειάζεται για την αποστολή απάντησης από τους ΧΟ-ΠΙ (Pothen δεδομένα) στο ΟΠΣ Πόθεν σχετικά με αίτημα που έχει προηγουμένως παραληφθεί με κλήση προς την υπηρεσία getPothenAithma. Για την απόκτηση πρόσβασης στην υπηρεσία getPothenData του ΚΕΔ, θα χρειαστεί να υποβληθεί από εξουσιοδοτημένο υπάλληλο του ΧΟ-ΠΙ σχετικό αίτημα στην Εφαρμογή Διαχείρισης Αιτημάτων (ΕΔΑ – <https://www1.gsis.gr/eda>) του Κέντρου Διαλειτουργικότητας, σύμφωνα με τις ειδικές οδηγίες που έχουν αποσταλεί προς τους ΧΟ-ΠΙ.

2. Υπηρεσία άντλησης δεδομένων για τη Δ.Π.Κ. του ΠΟΘΕΝ ΕΣΧΕΣ

Η συγκεκριμένη υπηρεσία WS του ΚΕΔ περιλαμβάνει τα παρακάτω APIs:

- **sendPothenAithma** – Διαβιβάζει το αίτημα από το ΟΠΣ Πόθεν στους ΧΟ-ΠΙ
- **getPothenData** – Λαμβάνει το αποτέλεσμα του αιτήματος (pothen δεδομένα) και το στέλνει στο ΟΠΣ Πόθεν

Οι ΧΟ-ΠΙ θα χρειαστεί να καταναλώσουν μόνο το API getPothenData για την αποστολή των Pothen δεδομένων. Το API sendPothenAithma αφορά αποκλειστικά το ΟΠΣ Πόθεν.

2.1 Διαβίβαση αιτήματος από το ΟΠΣ Πόθεν Έσχες στους ΧΟ-ΠΙ – API: sendPothenAithma

***** ΠΡΟΣΟΧΗ: ΑΥΤΗ Η ΥΠΗΡΕΣΙΑ ΔΕΝ ΚΑΛΕΙΤΑΙ ΑΠΟ ΤΟΥΣ ΧΟ-ΠΙ *****

Περιγραφή

Η συγκεκριμένη υπηρεσία καλείται **αποκλειστικά** από το **ΟΠΣ Πόθεν** για να διαβιβάσει ένα αίτημα προς έναν συγκεκριμένο ΧΟ-ΠΙ. Για το σκοπό αυτό θα πρέπει να οριστεί στην είσοδο (πεδίο institutionId) ο μοναδικός αναγνωριστικός κωδικός του ΧΟ-ΠΙ προκειμένου να κατευθυνθεί το αίτημα προς το αντίστοιχο web service (getPothenAithma) του ΧΟ-ΠΙ με σκοπό την παραλαβή και καταγραφή του αιτήματος στο Πληροφοριακό Σύστημα του ΧΟ-ΠΙ.

Τα στοιχεία που θα περιλαμβάνονται στο αίτημα φαίνονται παρακάτω. Σε περίπτωση αποτυχίας λήψης του αιτήματος από τους ΧΟ-ΠΙ, θα επιχειρείται ξανά η αποστολή του αιτήματος **μετά από συγκεκριμένο χρονικό διάστημα**. Με την κλήση της υπηρεσίας getPothenAithma από έναν ΧΟ-ΠΙ αυτός λαμβάνει το αίτημα από το ΟΠΣ Πόθεν και θα πρέπει να απαντήσει με έναν κατάλληλο κωδικό ενημερώνοντας το ΟΠΣ Πόθεν για την επιτυχημένη καταγραφή του αιτήματος. Πιο συγκεκριμένα κατά την επιτυχημένη καταγραφή του αιτήματος, η υπηρεσία getPothenAithma θα επιστρέφει κατάλληλο μήνυμα και κωδικό ένδειξης επιτυχημένης κλήσης/καταγραφής του αιτήματος ενώ σε περίπτωση αποτυχίας θα επιστρέφει κωδικό σφάλματος και μήνυμα με την περιγραφή του σφάλματος που συνέβη.

HTTP μέθοδος	POST
URI	/sendPothenAithma
Headers	Authorization: Basic <διαπιστευτήρια> ή Bearer <token> Content-type: application/json; charset=utf-8
ENDPOINT (PILOT)	https://test.gsis.gr/esbpilot/pothenDataRestService/sendPothenAithma
ENDPOINT (PROD)	https://ked.gsis.gr/esb/pothenDataRestService/sendPothenAithma

Request: Οι παράμετροι εισόδου για την κλήση της υπηρεσίας μεταβιβάζονται σε JSON μορφή και περιλαμβάνουν τα παρακάτω πεδία:

Πεδίο	Περιγραφή
auditRecord	Audit Record (βλέπε Παράρτημα Β)
sendPothenAithmaInputRecord	Δομή επιχειρησιακών πεδίων εισόδου
institutionId*	Μοναδικός αναγνωριστικός κωδικός (ΑΦΜ) του ΧΟ-ΠΙ
requestId*	Μοναδικός αριθμός αιτήματος (γράμμα Α & 21 ψηφία)
requestType*	Τύπος αιτήματος. Δυνατές τιμές: 1 ή 2 1 => Με δάνεια 2 => Χωρίς δάνεια
referenceDate*	Ημερομηνία αναφοράς των δεδομένων (δεν μπορεί να είναι μεταγενέστερη της ημερομηνίας κλήσης). Μορφή: yyyy-mm-dd (π.χ. 2024-01-18)
afm*	Αριθμός Φορολογικού Μητρώου του υπόχρεου τον οποίον αφορά το αίτημα
name*	Όνομα υπόχρεου (συμπληρώνονται οι τρεις πρώτοι χαρακτήρες)
surname*	Επώνυμο υπόχρεου (συμπληρώνονται οι τρεις πρώτοι χαρακτήρες)
fatherName	Πατρώνυμο υπόχρεου (δεν χρησιμοποιείται, προς το παρόν)
motherName	Μητρώνυμο υπόχρεου (δεν χρησιμοποιείται, προς το παρόν)
birthDate*	Ημερομηνία γέννησης υπόχρεου. Μορφή yyyy-mm-dd (π.χ. 1986-06-25)
params	Παράμετροι κρυπτογράφησης. Συμπληρώνεται προαιρετικά και ορίζει τις παραμέτρους που απαιτούνται για την κρυπτογράφηση των δεδομένων της απάντησης του ΧΟ-ΠΙ, ανάλογα με τις προδιαγραφές που έχουν συμφωνηθεί. Το πλήθος και οι τιμές των παραμέτρων συμφωνούνται αποκλειστικά μεταξύ ΟΠΣ Πόθεν και ΧΟ-ΠΙ και δεν αφορούν το Κέντρο Διαλειτουργικότητας (ΚΕΔ)

* το πεδίο είναι υποχρεωτικό

Response: Η απάντηση επιστρέφεται σε JSON μορφή και περιλαμβάνει τα παρακάτω πεδία:

Πεδίο	Περιγραφή
sendPothenAithmaOutputRecord	Δομή επιχειρησιακών πεδίων εξόδου
code	Κωδικός απόκρισης από την πλευρά του ΧΟ-ΠΙ. Ακολουθεί ο πίνακας με όλους τους πιθανούς κωδικούς απόκρισης
message	Περιγραφή/μήνυμα απόκρισης από την πλευρά του ΧΟ-ΠΙ
replyDate	Ημερομηνία και ώρα στην οποία αναμένεται η ολοκλήρωση μεταφοράς/αποστολής πόθεν δεδομένων από τον ΧΟ-ΠΙ προς το ΟΠΣ Πόθεν (προτείνεται η επόμενη εργάσιμη ημέρα και ώρα 5μμ). Επιστρέφει τιμή μόνο όταν το code είναι 0 ή 1 Μορφή ημερομηνίας: yyyy-mm-ddThh24:mi:ssZ (π.χ. 2024-01-24T17:00:00Z)
callSequenceId	Μοναδικός αριθμός ο οποίος χαρακτηρίζει την κλήση του WS
callSequenceDate	Χρονοσήμανση κλήσης του WS
errorRecord	Δομή σφάλματος του ΚΕΔ (σε περίπτωση λάθους)
errorCode	Κωδικός λάθους (Παράγραφος 4, πίνακες 1 & 2)
errorDescr	Περιγραφή κωδικού λάθους (Παράγραφος 4, πίνακες 1 & 2)

Δυνατές τιμές των επιχειρησιακών πεδίων εξόδου code & message¹

code	message	Παρατηρήσεις
0	Το αίτημα με αριθμό <requestId> υποβλήθηκε επιτυχώς	Επιτυχημένη αποστολή αιτήματος (ο αίτημα έχει υποβληθεί και καταγραφεί επιτυχώς στο Π.Σ. του ΧΟ-ΠΙ). Επιστρέφεται η αναμενόμενη ημερομηνία & ώρα ολοκλήρωσης αποστολής των πόθεν δεδομένων στο πεδίο replyDate
1	Το αίτημα με αριθμό <requestId> έχει ήδη υποβληθεί	Το αίτημα έχει ήδη υποβληθεί και καταγραφεί επιτυχώς στο Π.Σ. του ΧΟ-ΠΙ από προηγούμενη κλήση η οποία έλαβε χώρα λίγη ώρα πριν (συνήθως μερικά δευτερόλεπτα). Το ΟΠΣ Πόθεν επανέλαβε την κλήση επειδή δεν κατάφερε να λάβει/διαβάσει το response της πρώτης/προηγούμενης κλήσης λόγω κάποιου τεχνικού προβλήματος. Και σε αυτή την περίπτωση επιστρέφεται η αναμενόμενη ημερομηνία & ώρα ολοκλήρωσης αποστολής των πόθεν δεδομένων στο πεδίο replyDate
3	Το αίτημα με αριθμό <requestId> έχει ήδη υποβληθεί και διεκπεραιωθεί	Το αίτημα έχει υποβληθεί και καταγραφεί επιτυχώς στο Π.Σ. του ΧΟ-ΠΙ ΚΑΙ, ο ΧΟ-ΠΙ έχει ήδη καλέσει την υπηρεσία getPothenData και έχει αποστείλει επιτυχώς στο ΟΠΣ Πόθεν τα κρυπτογραφημένα δεδομένα με την απάντηση στο αίτημα με αριθμό requestId που υποβλήθηκε από το ΟΠΣ Πόθεν
7	Ο ΑΦΜ αντιστοιχεί σε πελάτη αλλά δεν διαθέτει λογαριασμούς ή άλλα προϊόντα	Ο υπόχρεος για τον οποίον υποβλήθηκε το αίτημα δεν διαθέτει προϊόντα στον συγκεκριμένο ΧΟ-ΠΙ για τη συγκεκριμένη ημ/νία αναφοράς δεδομένων του αιτήματος (referenceDate).
8	Ο ΑΦΜ δεν μπορεί να ταυτοποιηθεί ²	Αδυναμία ταυτοποίησης του υπόχρεου λόγω μη πλήρους συμφωνίας των δεδομένων, πχ. βρέθηκε ο ΑΦΜ στο πελατολόγιο του ΧΟ-ΠΙ αλλά τα υπόλοιπα στοιχεία (όνομα, επώνυμο, ημ/νία γέννησης) δεν συμφωνούν ή βρέθηκε ο υπόχρεος με το συγκεκριμένο όνομα, επώνυμο ή ημ/νία γέννησης αλλά δεν συμφωνεί ο ΑΦΜ. Στην περίπτωση αυτή απαιτείται επικοινωνία μεταξύ του ΧΟ-ΠΙ και της ΓΓΠΣΨΔ για περαιτέρω διερεύνηση Η χρήση του συγκεκριμένου κωδικού απάντησης είναι μεν προαιρετική συστήνεται δε για την αποτελεσματικότερη επίλυση του προβλήματος. Εναλλακτικά, στη συγκεκριμένη περίπτωση ο ΧΟ-ΠΙ μπορεί να απαντήσει με τον κωδικό 9.
9	Ο ΑΦΜ δεν αντιστοιχεί σε πελάτη	Ο υπόχρεος για τον οποίον υποβλήθηκε το αίτημα δεν αντιστοιχεί σε πελάτη του ΧΟ-ΠΙ για τη συγκεκριμένη ημ/νία αναφοράς δεδομένων του αιτήματος (referenceDate).

¹ Με κόκκινο χρώμα οι κωδικοί και τα μηνύματα που αφορούν επιχειρησιακή αδυναμία αποστολής δεδομένων πόθεν για τον συγκεκριμένο υπόχρεο

² Η ταυτοποίηση του υπόχρεου πραγματοποιείται πάντα με τον ΑΦΜ. Εφόσον βρεθεί στο πελατολόγιο του ΧΟ-ΠΙ **συστήνεται** η επιβεβαίωση από τους ΧΟ-ΠΙ με χρήση των τριών (3) πρώτων χαρακτήρων του επωνύμου και του ονόματος καθώς και της ημ/νίας γέννησης (ιδιαίτερα του έτους και του μήνα). Σε περίπτωση μη επιβεβαίωσης μπορεί να χρησιμοποιηθεί ο κωδικός 8. Αν δεν βρεθεί ο συγκεκριμένος ΑΦΜ ο ΧΟ-ΠΙ **μπορεί να απαντήσει** ότι ο υπόχρεος δεν αντιστοιχεί σε πελάτη του (κωδικός 9) ή μπορεί (**δεν είναι υποχρεωτικό**) να ψάξει με βάση τα υπόλοιπα δεδομένα και εφόσον βρεθεί να απαντήσει με τον κωδικό λάθους 8.

<p>10</p>	<p>Μη έγκυρη είσοδος: <περιγραφή ελέγχου που απέτυχε>, π.χ. <i>Μη έγκυρη είσοδος: ο αριθμός αιτήματος είναι κενός</i> <i>Μη έγκυρη είσοδος: ο τύπος αιτήματος είναι κενός</i> <i>Μη έγκυρη είσοδος: ο τύπος αιτήματος δεν είναι έγκυρος</i> <i>Μη έγκυρη είσοδος: ο ΑΦΜ είναι κενός</i> <i>Μη έγκυρη είσοδος: ο ΑΦΜ δεν είναι αλγοριθμικά έγκυρος</i> <i>Μη έγκυρη είσοδος: το όνομα είναι κενό</i> <i>Μη έγκυρη είσοδος: το επώνυμο είναι κενό</i> <i>Μη έγκυρη είσοδος: η ημερομηνία γέννησης είναι κενή</i> <i>Μη έγκυρη είσοδος: η ημερομηνία γέννησης δεν είναι έγκυρη (μη έγκυρο format ή ημερομηνία που δεν υφίσταται)</i> <i>Μη έγκυρη είσοδος: η ημερομηνία αναφοράς δεδομένων είναι κενή</i> <i>Μη έγκυρη είσοδος: η ημερομηνία αναφοράς δεδομένων δεν είναι έγκυρη (μη έγκυρο format ή ημερομηνία που δεν υφίσταται)</i> <i>Μη έγκυρη είσοδος: η ημερομηνία αναφοράς δεδομένων είναι μεταγενέστερη της ημερομηνίας αποστολής του αιτήματος</i></p>	<p>Αυτός ο κωδικός σφάλματος υποδεικνύει ότι η μεταβιβαζόμενη τιμή σε ένα πεδίο απουσιάζει ή δεν είναι έγκυρη. Αυτή η περίπτωση είναι μάλλον απίθανο να συμβεί καθώς όλα τα αιτήματα που γίνονται από το ΟΠΣ Πόθεν έχουν έγκυρα δεδομένα εισόδου. Συνιστάται όμως η πραγματοποίηση ελέγχων και από την πλευρά του ΧΟ-ΠΙ</p>
<p>90</p>	<p>Το Π.Σ. του ΧΟ-ΠΙ είναι προσωρινά μη διαθέσιμο για λόγους προγραμματισμένης συντήρησης</p>	<p>Το αίτημα δεν μπόρεσε να αποθηκευτεί στο σύστημα του ΧΟ-ΠΙ λόγω (προγραμματισμένης) μη διαθεσιμότητας των υποδομών του</p>
<p>99</p>	<p>Σφάλμα κατά την καταγραφή του αιτήματος</p>	<p>Έκτακτο τεχνικό πρόβλημα στο Π.Σ. του ΧΟ-ΠΙ (π.χ. σφάλμα αποθήκευσης στη ΒΔ)</p>

Επεξηγήσεις

Για την καλύτερη κατανόηση των κωδικών απάντησης της συγκεκριμένης υπηρεσίας WS (πεδία code και message) δίνεται ο κάτωθι πίνακας αντιστοίχισης των περιπτώσεων κατά την υλοποίηση της διαλειτουργικότητας με χρήση του FTPS.

ΟΠΣ ΠΟΘΕΝ - ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ ΜΕΧΟ-ΠΙ					
ΤΡΟΠΟΣ ΥΛΟΠΟΙΗΣΗΣ	ΠΕΔΙΑ ΑΠΑΝΤΗΣΗΣ	ΠΕΛΑΤΗΣ ΜΕ ΠΡΟΪΟΝΤΑ	ΠΕΛΑΤΗΣ ΧΩΡΙΣ ΠΡΟΪΟΝΤΑ	ΔΕΝ ΕΝΑΙ ΠΕΛΑΤΗΣ	ΑΔΥΝΑΜΙΑ ΤΑΥΤΟΠΟΙΗΣΗΣ
FTPS	Εγγραφή υπόχρεου - Πλήθος εγγραφών προϊόντων υπόχρεου	>0	0	-1	-1
sendPothenAithmaOutputRecord					
	code	0/1	7	9	8/9
WS	message	Το αίτημα με αριθμό <requestId> υποβλήθηκε επιτυχώς/ Το αίτημα με αριθμό <requestId> έχει ήδη υποβληθεί	Ο ΑΦΜ αντιστοιχεί σε πελάτη αλλά δεν διαθέτει λογαριασμούς ή άλλα προϊόντα	Ο ΑΦΜ δεν αντιστοιχεί σε πελάτη	Ο ΑΦΜ δεν μπορεί να ταυτοποιηθεί / Ο ΑΦΜ δεν αντιστοιχεί σε πελάτη

Μόλις η υπηρεσία **sendPothenAithma** απαντήσει, θα πρέπει πρώτα απ' όλα να γίνει έλεγχος στη δομή **errorRecord** της απάντησης. Σε επιτυχή απάντηση η δομή **errorRecord** δεν πρέπει να περιέχει κάποιο μήνυμα λάθους (δηλαδή τα πεδία **errorCode** και **errorDescr** πρέπει να έχουν τιμή null). Αντιθέτως, η υπηρεσία θα πρέπει να επιστρέφει πάντα τιμές στα επιχειρησιακά πεδία εξόδου **code** & **message**. Επίσης θα πρέπει να επιστραφεί τιμή και στο πεδίο **replyDate**, εφόσον το πεδίο **code** έχει τιμή 0 ή 1 (ύπαρξη πόθεν δεδομένων για τον υπόχρεο προς αποστολή).

Στην περίπτωση όπου δεν επιστρέφονται καθόλου τιμές στα επιχειρησιακά πεδία εξόδου (**code**, **message**, **replyDate**), έχει συμβεί κάποιο σφάλμα και η δομή εξόδου **errorRecord** λαμβάνει από το ΚΕΔ τη σχετική πληροφορία σφάλματος. Σε αυτή την περίπτωση τα πεδία **errorCode** και **errorDescr** λαμβάνουν τιμές με βάση τους κωδικούς λαθών του ΚΕΔ όπως δίνονται στον Πίνακα 1 της Ενότητας 4.

Ιδιαίτερα, στην περίπτωση που το πεδίο **errorCode** επιστρέψει τον κωδικό λάθους «**GEN_DATABASE_CONNECTION_ERROR**» ή «**GEN_COMMUNICATION_ERROR**», αυτό σημαίνει ότι έχει συμβεί κάποιο προσωρινό σφάλμα και η κλήση πρέπει να επαναληφθεί.

2.2 Αποστολή αποτελέσματος αιτήματος προς το ΟΠΣ Πόθεν – API: getPothenData

Περιγραφή

Η συγκεκριμένη υπηρεσία καλείται **αποκλειστικά** από τα **Πληροφοριακά Συστήματα των ΧΟ-ΠΙ** με σκοπό να αποσταλεί το αποτέλεσμα (Pothen δεδομένα) για ένα αίτημα (requestId) που υποβλήθηκε προηγουμένως από το ΟΠΣ Πόθεν. Στην είσοδο του αιτήματος θα πρέπει να οριστεί ο μοναδικός αριθμός αιτήματος (requestId) που αντιστοιχεί στη συγκεκριμένη κλήση με την οποία ζητήθηκαν πόθεν δεδομένα για τον συγκεκριμένο υπόχρεο.

Τα δεδομένα πόθεν αποστέλλονται **ΠΑΝΤΑ** από τον ΧΟ-ΠΙ σε κρυπτογραφημένη μορφή (στο επιχειρησιακό πεδίο εισόδου data) σύμφωνα με τον αλγόριθμο κρυπτογράφησης που έχει συμφωνηθεί μεταξύ του ΟΠΣ Πόθεν και του ΧΟ-ΠΙ. Τα δεδομένα αποθηκεύονται επίσης κρυπτογραφημένα στη βάση δεδομένων του ΟΠΣ Πόθεν.

Το χρονικό διάστημα μεταξύ της υποβολής του αιτήματος από το ΟΠΣ Πόθεν και της απάντησης από τους ΧΟ-ΠΙ (Περίοδος Απάντησης) παρακολουθείται από την ΓΓΠΣΨΔ προκειμένου να διαπιστωθεί η τήρηση της συμφωνίας σχετικά με αυτό.

HTTP μέθοδος	POST
URI	/getPothenData
Headers	Authorization: Basic <διαπιστευτήρια> ή Bearer <token> Content-type: application/json; charset=utf-8
ENDPOINT (PILOT)	https://test.gsis.gr/esbpilot/pothenDataRestService/getPothenData
ENDPOINT (PROD)	https://ked.gsis.gr/esb/pothenDataRestService/getPothenData

Request: Οι παράμετροι εισόδου για την κλήση της υπηρεσίας μεταβιβάζονται σε JSON μορφή και περιλαμβάνουν τα παρακάτω πεδία:

Πεδίο WSDL	Περιγραφή
auditRecord	Audit Record (βλέπε Παράρτημα Β)
getPothenDataInputRecord	Δομή επιχειρησιακών πεδίων εισόδου
requestId*	Μοναδικός αριθμός αιτήματος (γράμμα Α & 21 ψηφία)
resultCode*	Κωδικός αποτελέσματος. Επιστρέφει 0 σε επιτυχία και 1 σε περίπτωση αδυναμίας αποστολής απάντησης
resultMessage*	Μήνυμα αποτελέσματος . Επιστρέφει το λεκτικό "OK" σε περίπτωση επιτυχίας, διαφορετικά επιστρέφει μια συνοπτική περιγραφή του προβλήματος σε ελεύθερο κείμενο (σε περίπτωση που ο ΑΦΜ του υπόχρεου δεν αντιστοιχεί σε πελάτη για τη συγκεκριμένη ημ/νία αναφοράς ή αντιστοιχεί αλλά δεν διαθέτει προϊόντα στον συγκεκριμένο ΧΟ-ΠΙ για τη συγκεκριμένη ημ/νία αναφοράς ή δεν μπορεί να ταυτοποιηθεί η πληροφορία αυτή δίνεται ως απάντηση της ws κλήσης sendPothenAithma (πεδία code και message) οπότε η συγκεκριμένη κλήση από τους ΧΟ-ΠΙ είναι περιττή και για λόγους αποδοτικότερης παραγωγικής λειτουργίας του συστήματος δεν πρέπει να πραγματοποιείται).
data	Το πεδίο data περιέχει τα δεδομένα πόθεν όταν το πεδίο resultCode έχει τιμή 0 (επιτυχία) όπως αναφέρεται παραπάνω. Τα δεδομένα πόθεν αποστέλλονται υποχρεωτικά σε κρυπτογραφημένη μορφή όταν προέρχονται από την παραγωγική βάση δεδομένων του ΧΟ-ΠΙ και σε κωδικοποίηση base64URL ή χωρίς κρυπτογράφηση/κωδικοποίηση όταν το πεδίο περιέχει τεστ δεδομένα.

	<p>Σε κάθε άλλη περίπτωση (resultCode=1) το πεδίο data περιέχει κενούς τους 5 πίνακες (arrays) δεδομένων διαλειτουργικότητας σύμφωνα με το υπόδειγμα</p> <pre>{ "rothenRequestId": "XXXXXXXXXXXXXXXXXXXXXXXXX", "investmentProducts": [], "depositPaymentsAccounts": [], "safeBoxes": [], "loans": [], "preciousMetals": [] }</pre> <p>Σε όλες τις περιπτώσεις το πεδίο data θα πρέπει να περιέχει και τους 5 πίνακες διαλειτουργικότητας. Όταν δεν υπάρχουν δεδομένα προς αποστολή για έναν ή περισσότερους πίνακες αυτοί θα αποστέλλονται κενοί.</p>
<p>params</p>	<p>Παράμετρος κρυπτογράφησης (enc)</p> <p>Συμπληρώνεται υποχρεωτικά εφόσον το πεδίο data δεν είναι κενό και ορίζει τον τρόπο με τον οποίο θα σταλούν τα δεδομένα πόθεν. Μπορεί να χρησιμοποιηθεί μία από τις εξής τιμές:</p> <ul style="list-style-type: none"> - enc=crypto (Υποδεικνύει ότι τα δεδομένα αποστέλλονται κρυπτογραφημένα με τον συμφωνημένο αλγόριθμο κρυπτογράφησης) - enc=base64URL (Υποδεικνύει ότι τα δεδομένα έχουν κωδικοποιηθεί κατά BASE64URL (δεν γίνεται κρυπτογράφηση)) - enc=none (Υποδεικνύει ότι τα δεδομένα αποστέλλονται χωρίς χρήση κρυπτογράφησης/κωδικοποίησης) <p>Οι δύο τελευταίες παράμετροι μπορούν να χρησιμοποιηθούν μόνο στο πλαίσιο των δοκιμαστικών κλήσεων και των ελέγχων λειτουργίας υλοποίησης και ΠΟΤΕ στο παραγωγικό περιβάλλον (επιτρέπεται μόνο enc=crypto).</p>

* το πεδίο είναι υποχρεωτικό

Response: Η απάντηση επιστρέφεται σε JSON μορφή και περιλαμβάνει τα παρακάτω πεδία:

Πεδίο WSDL	Περιγραφή
getPothenDataOutputRecord	Δομή επιχειρησιακών πεδίων εξόδου
code	Κωδικός απόκρισης από την πλευρά του ΟΠΣ Πόθεν. Ακολουθεί ο πίνακας με όλες τις δυνατές τιμές
message	Περιγραφή/μήνυμα απόκρισης από την πλευρά του ΟΠΣ Πόθεν
info	Πρόσθετες πληροφορίες για τυχόν σφάλμα εξαιτίας του οποίου δεν έγινε αποδεκτή η αποστολή των δεδομένων από το ΟΠΣ Πόθεν (το περιεχόμενο βοηθάει τον ΧΟ-ΠΙ στην αποσφαλμάτωση και τη διερεύνηση της αιτίας του σφάλματος)
callSequenceId	Μοναδικός αριθμός ο οποίος χαρακτηρίζει την κλήση του WS
callSequenceDate	Χρονοσήμανση κλήσης του WS
errorRecord	Δομή σφάλματος του ΚΕΔ (σε περίπτωση λάθους)
errorCode	Κωδικός λάθους (Πίνακα 1της Ενότητας 4)
errorDescr	Περιγραφή κωδικού λάθους (Πίνακας 1 της Ενότητας 4)

Δυνατές τιμές των επιχειρησιακών πεδίων εξόδου code & message³

code	message	Παρατηρήσεις
0	Το αποτέλεσμα στο αίτημα με αριθμό <requestId> λήφθηκε επιτυχώς.	Επιτυχημένη παραλαβή των δεδομένων πόθεν, δηλαδή τα δεδομένα έχουν παραληφθεί και αποθηκευτεί επιτυχώς στο ΟΠΣ Πόθεν για περαιτέρω επεξεργασία.
1	Το αποτέλεσμα στο αίτημα με αριθμό <requestId> έχει ήδη ληφθεί.	Το αίτημα έχει ήδη ληφθεί και καταγραφεί επιτυχώς στο ΟΠΣ Πόθεν, από προηγούμενη κλήση που έλαβε χώρα λίγη ώρα πριν (συνήθως μερικά δευτερόλεπτα πριν). Το Π.Σ. του ΧΟ-ΠΙ επανέλαβε την κλήση επειδή δεν κατάφερε να λάβει/διαβάσει το response της πρώτης/προηγούμενης κλήσης λόγω προσωρινού τεχνικού προβλήματος.
2	Μη έγκυρος αριθμός αιτήματος.	Δεν υπάρχει καταχωρημένο αίτημα στη Β.Δ. του ΟΠΣ Πόθεν για τον συγκεκριμένο αριθμό αιτήματος ή το αίτημα δεν αφορά τον συγκεκριμένο ΧΟ-ΠΙ.
3	Η επικύρωση των δεδομένων απέτυχε.	Το ΟΠΣ Πόθεν αποκρυπτογράφησε επιτυχώς το περιεχόμενο του πεδίου data ΑΛΛΑ αυτό δεν είναι έγκυρο με βάση τις προδιαγραφές. Για παράδειγμα, το περιεχόμενο δεν είναι σύμφωνο με τον μορφότυπο json ή δεν περιλαμβάνει τα υποχρεωτικά στοιχεία/δομές με βάση τις προδιαγραφές διαλειτουργικότητας Πόθεν Έσχος. Περισσότερες πληροφορίες επιστρέφονται στο πεδίο info.
4	Αποτυχία στην αποκρυπτογράφηση/αποκωδικοποίηση των δεδομένων. Τα δεδομένα έχουν κρυπτογραφηθεί/κωδικοποιηθεί με λάθος αλγόριθμο ή η δομή τους δεν είναι σωστή.	Το ΟΠΣ Πόθεν δεν κατάφερε να αποκρυπτογραφήσει το περιεχόμενο του πεδίου data με βάση τον συμφωνημένο αλγόριθμο κρυπτογράφησης.
90	Το ΟΠΣ Πόθεν είναι προσωρινά μη διαθέσιμο για λόγους προγραμματισμένης συντήρησης	Το αίτημα δεν μπόρεσε να αποθηκευτεί στο ΟΠΣ Πόθεν λόγω (προγραμματισμένης) μη διαθεσιμότητας των υποδομών του.
99	Σφάλμα κατά την παραλαβή και αποθήκευση του αποτελέσματος στο ΟΠΣ Πόθεν	Τυχόν προσωρινό τεχνικό πρόβλημα (π.χ. σφάλμα αποθήκευσης στη ΒΔ) κατά την καταγραφή/αποθήκευση του αποτελέσματος στο ΟΠΣ Πόθεν.

Επεξηγήσεις

Μόλις η υπηρεσία **getPothenData** απαντήσει, θα πρέπει πρώτα απ' όλα να γίνει έλεγχος στη δομή εξόδου **errorRecord**. Στην περίπτωση επιτυχούς απάντησης, η δομή εξόδου **errorRecord** δεν πρέπει να περιέχει κάποιο μήνυμα λάθους (δηλαδή τα πεδία **errorCode** και **errorDescr** περιέχουν τιμή null). Αντιθέτως, η υπηρεσία θα πρέπει να επιστρέφει πάντα τιμές στα επιχειρησιακά πεδία εξόδου **code** & **message**. Στην περίπτωση όπου δεν επιστρέφονται καθόλου τιμές στα επιχειρησιακά πεδία εξόδου (**code**, **message**), έχει συμβεί κάποιο σφάλμα και η δομή εξόδου **errorRecord** λαμβάνει από το ΚΕΔ τη σχετική πληροφορία σφάλματος. Τα πεδία **errorCode** και **errorDescr** επιστρέφουν τιμές με βάση τους κωδικούς λαθών του ΚΕΔ όπως δίνονται στον Πίνακα 1 της Ενότητας 4. Ιδιαίτερα, στην περίπτωση που το πεδίο **errorCode** επιστρέψει τον κωδικό λάθους «**GEN_DATABASE_CONNECTION_ERROR**» ή «**GEN_COMMUNICATION_ERROR**», αυτό σημαίνει ότι έχει συμβεί κάποιο προσωρινό σφάλμα και η κλήση πρέπει να επαναληφθεί.

³ Με κόκκινο χρώμα οι κωδικοί και τα μηνύματα που αφορούν επιχειρησιακή αδυναμία αποστολής δεδομένων πόθεν για τον συγκεκριμένο υπόχρεο.

2.3 Λήψη πληροφοριών για το δημόσιο κλειδί (public key) της κρυπτογράφησης – API: getEncryptionInfo

Η συγκεκριμένη υπηρεσία καλείται **αποκλειστικά** από τα **Πληροφοριακά Συστήματα των ΧΟ-ΠΙ** με σκοπό να παραληφθούν πληροφορίες για τη μέθοδο κρυπτογράφησης και το δημόσιο κλειδί που θα χρησιμοποιηθεί.

Πιο συγκεκριμένα, η υπηρεσία επιστρέφει στον ΧΟ-ΠΙ με μορφή JSON όλα τα απαραίτητα στοιχεία για το δημόσιο κλειδί, τα οποία καθορίζουν τις ιδιότητες του κλειδιού όπως ορίζονται από τις προδιαγραφές JWK (<https://datatracker.ietf.org/doc/html/rfc7517>).

HTTP μέθοδος	POST
URI	/getEncryptionInfo
Headers	Authorization: Basic <διαπιστευτήρια> ή Bearer <token> Content-type: application/json; charset=utf-8
ENDPOINT (PILOT)	https://test.gsis.gr/esbpilot/pothenDataRestService/getEncryptionInfo
ENDPOINT (PROD)	https://ked.gsis.gr/esb/pothenDataRestService/getEncryptionInfo

Request: Οι παράμετροι εισόδου για την κλήση της υπηρεσίας μεταβιβάζονται σε JSON μορφή και περιλαμβάνουν τα παρακάτω πεδία:

Πεδίο WSDL	Περιγραφή
auditRecord	Audit Record (βλέπε Παράρτημα Β)
getEncryptionInfoInputRecord	Δομή επιχειρησιακών πεδίων εισόδου (η υπηρεσία δεν δέχεται ορίσματα εισόδου)

Response: Η απάντηση επιστρέφεται σε JSON μορφή και περιλαμβάνει τα παρακάτω πεδία:

Πεδίο WSDL	Περιγραφή
getEncryptionInfoOutputRecord	Δομή επιχειρησιακών πεδίων εξόδου
keys	Λίστα αντικειμένων (κλειδιών) με τις ιδιότητες του κάθε κλειδιού. Κάθε κλειδί περιέχει τα εξής πεδία:
key	Καθορίζει την οικογένεια κρυπτογραφικών αλγορίθμων και στην εφαρμογή Πόθεν έχει πάντα την τιμή "RSA"
e	Ο εκθέτης (exponent) του δημόσιου κλειδιού RSA
use	Καθορίζει τον σκοπό χρήσης του κλειδιού. Στην εφαρμογή Πόθεν επιστρέφει πάντα την τιμή "enc" που σημαίνει χρήση για κρυπτογράφηση
kid	Το μοναδικό αναγνωριστικό για το κλειδί
alg	Καθορίζει τον συγκεκριμένο κρυπτογραφικό αλγόριθμο που χρησιμοποιείται με το συγκεκριμένο κλειδί
n	Ο συντελεστής-modulus του δημόσιου κλειδιού RSA
callSequenceId	Μοναδικός αριθμός ο οποίος χαρακτηρίζει την κλήση του WS
callSequenceDate	Χρονοσήμανση κλήσης του WS
errorRecord	Δομή σφάλματος του ΚΕΔ (σε περίπτωση λάθους)
errorCode	Κωδικός λάθους (Πίνακας 1 της Ενότητας 4)
errorDescr	Περιγραφή κωδικού λάθους (Πίνακας 1 της Ενότητας 4)

Εφαρμογή Πολιτικής Ορθής Χρήσης της Υπηρεσίας getEncryptionInfo

Για την αποφυγή υπερφόρτωσης της υπηρεσίας και τη διασφάλιση της απρόσκοπτης παροχής της θα πρέπει να ακολουθούνται οι παρακάτω οδηγίες σχετικά με τη λήψη πληροφοριών του δημόσιου κλειδιού του ΟΠΣ Πόθεν και τη διαχείρισή του:

1. Περιορισμός Κλήσεων στην Υπηρεσία

Η ws υπηρεσία λήψης πληροφοριών του δημόσιου κλειδιού (getEncryptionInfo) θα πρέπει να καλείται μόνο για έναν περιορισμένο αριθμό τηρώντας το ημερήσιο όριο κλήσεων όπως καθορίζεται από το ΚΕΔ για τη συγκεκριμένη υπηρεσία.

2. Αποθήκευση του Δημόσιου Κλειδιού

Μετά τη λήψη των στοιχείων του δημόσιου κλειδιού για την κρυπτογράφηση των δεδομένων πόθεν απαιτείται να αποθηκεύονται στο πληροφοριακό σύστημα του ΧΟ-ΠΙ. Για την κρυπτογράφηση των δεδομένων πόθεν θα πρέπει να χρησιμοποιείται όσο το δυνατόν περισσότερο το αποθηκευμένο κλειδί και να μην γίνονται άσκοπες κλήσεις στην υπηρεσία getEncryptionInfo.

3. Διαδικασία ενημέρωσης αλλαγής του Δημόσιου Κλειδιού

Σε περίπτωση που το δημόσιο κλειδί πρέπει να αλλάξει είτε λόγω παρέλευσης του χρόνου ζωής του (expiration date) είτε για λόγους ασφάλειας (π.χ. παραβίαση της εγκυρότητας του δημόσιου κλειδιού) οπότε το δημόσιο κλειδί καθίσταται άμεσα ανενεργό και η κλήση στην υπηρεσία getEncryptionInfo δεν επιστρέφει αποτέλεσμα, θα αποστέλλεται έγκαιρη ειδοποίηση προς όλους τους ΧΟ-ΠΙ μέσω email. Με τη λήψη του email ο ΧΟ-ΠΙ θα πρέπει να διαγράψει αμέσως το παλιό δημόσιο κλειδί και να μην το χρησιμοποιεί. Το email θα περιλαμβάνει την ακριβή ημερομηνία και ώρα ενεργοποίησης του νέου δημόσιου κλειδιού ώστε να γίνει λήψη του από τους ΧΟ-ΠΙ. Σε κάθε περίπτωση ο ΧΟ-ΠΙ θα πρέπει να ειδοποιεί **ΑΜΕΣΑ** την υπηρεσία Πόθεν αν υποπέσει στην αντίληψή του περίπτωση παραβίασης ή προσπάθειας αλλοίωσης του δημόσιου κλειδιού.

3. Αυθεντικοποίηση (Authorization)

Για την αυθεντικοποίηση (authorization) χρηστών μπορεί να χρησιμοποιηθεί είτε η Basic είτε η Bearer αυθεντικοποίηση. Στο παρόν εγχειρίδιο περιγράφεται η χρήση της Basic αυθεντικοποίησης.

Basic Αυθεντικοποίηση

Κάθε κλήση μιας υπηρεσίας (web service) περιλαμβάνει έναν Header ο οποίος περιέχει το όνομα του χρήστη (username) και τον κωδικό πρόσβασης (password), σε κωδικοποιημένη μορφή Base64. Ο Header αυτός πρέπει να είναι της μορφής:

Authorization: Basic <διαπιστευτήρια>

όπου τα διαπιστευτήρια είναι το αποτέλεσμα κωδικοποίησης σε Base64 του ονόματος χρήστη και του κωδικού πρόσβασης διαχωριζόμενα με το χαρακτήρα ":".

Για παράδειγμα, αν το όνομα χρήστη είναι "user" και ο κωδικός πρόσβασης είναι "password1", τότε για την αυθεντικοποίηση του συγκεκριμένου χρήστη θα αποσταλεί ο παρακάτω Header:

Authorization: Basic dXNlcjpwYXNzd29yZDE=

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

Σε περίπτωση που δοθούν λανθασμένα συνθηματικά (δηλαδή λάθος username ή password), τότε επιστρέφεται το μήνυμα λάθους: «**Η αυθεντικοποίηση χρήστη απέτυχε (λανθασμένα συνθηματικά)**». Συγκεκριμένα, επιστρέφεται το παρακάτω σφάλμα στη δομή errorRecord:

```
"errorRecord": {  
  "errorCode": "GEN_AUTHENTICATION_FAILED",  
  "errorDescr": "Η αυθεντικοποίηση χρήστη απέτυχε (λανθασμένα συνθηματικά)"  
}
```

Να επισημανθεί πως όταν η αυθεντικοποίηση αποτύχει, το HTTP STATUS που επιστρέφεται από την κλήση του REST (RESTful web) service είναι 200 και όχι 401, όπως συνηθίζεται στις περιπτώσεις αποτυχημένου authentication. Γενικότερα όλες οι κλήσεις προς τα REST services του Κέντρου Διαλειτουργικότητας επιστρέφουν το HTTP STATUS 200 και η διαχείριση λαθών γίνεται με βάση τον κωδικό και την περιγραφή σφάλματος της δομής errorRecord.

Αυθεντικοποίηση Θυγατρικών ΧΟ-ΠΙ

Η χρήση των ws υπηρεσιών Πόθεν μέσω του ΚΕΔ προϋποθέτει την υποβολή διαφορετικού/ξεχωριστού αιτήματος στην Εφαρμογή Διαχείρισης Αιτημάτων (ΕΔΑ), ανά ΑΦΜ ΧΟ-ΠΙ. Με άλλα λόγια, προϋποθέτει τη δημιουργία χωριστού λογαριασμού και τη λήψη χωριστού ονόματος χρήστη (username) και τη δημιουργία χωριστού κωδικού πρόσβασης (password) από όλους τους ΧΟ-ΠΙ, είτε αφορά την αυθεντικοποίηση της μητρικής εταιρείας είτε τις θυγατρικές της με βάση τον κανονισμό λειτουργίας του ΚΕΔ. Κάθε ΧΟ-ΠΙ (ανεξάρτητα αν είναι η μητρική εταιρεία ή θυγατρική της) από τα πληροφοριακά συστήματα του οποίου θα λαμβάνει δεδομένα το ΟΠΣ Πόθεν μέσω διαλειτουργικότητας θα πρέπει κατά την εγγραφή του στο ΚΕΔ για χρήση των ws υπηρεσιών Πόθεν να δηλώσει μοναδικό αναγνωριστικό του πληροφοριακού συστήματος από το οποίο θα αντλούνται τα δεδομένα, το οποίο θα είναι διαφορετικό για κάθε ΧΟ-ΠΙ.

Κάθε ΧΟ-ΠΙ για την παροχή των ws υπηρεσιών Πόθεν είναι ελεύθερος να υλοποιήσει είτε ένα κοινό endpoint (url) που θα χρησιμοποιηθεί και για τις θυγατρικές του είτε διακριτά endpoints για τη μητρική και τις θυγατρικές εφόσον ικανοποιούνται οι προϋποθέσεις της προηγούμενης παραγράφου.

4. Αντιμετώπιση Λαθών

Σε περίπτωση λάθους κατά την κλήση του Web Service, στην απάντηση επιστρέφεται ο κωδικός και το μήνυμα λάθους τα οποία περιγράφονται στον ακόλουθο πίνακα. Να τονιστεί πως γενικά το HTTP STATUS που επιστρέφεται είναι 200, εκτός κι αν έχει προκύψει κάποιο πολύ σοβαρό σφάλμα που δεν μπορούν να διαχειριστούν οι διακομιστές του Κέντρου Διαλειτουργικότητας.

Κωδικός λάθος (Error Code Name)	Περιγραφή μηνύματος λάθους (Error Description)
GEN_INVALID_STRUCTURE_FORMAT	Η δομή δεν είναι σύμφωνη με τις προδιαγραφές της υπηρεσίας. Τα πεδία εισόδου δεν μεταβιβάστηκαν στην κατάλληλη μορφή (σφάλμα στο JSON request ή μεταβίβαση μη αναμενόμενων πεδίων)
GEN_AUTHENTICATION_FAILED	Η αυθεντικοποίηση χρήστη απέτυχε, δηλαδή δόθηκαν λανθασμένα συνθηματικά (λάθος username ή/και password) ή χρησιμοποιήθηκαν τα συνθηματικά του πιλοτικού περιβάλλοντος στο παραγωγικό περιβάλλον (ή αντιστρόφως)
GEN_AUDIT_VALIDATION_INV_DATA_OR_UNAUTH_OPER	Τα διαπιστευτήρια (username & password) που χρησιμοποιήθηκαν για την αυθεντικοποίηση δεν έχουν εξουσιοδότηση για χρήση της συγκεκριμένης διαδικτυακής υπηρεσίας
GEN_AUDIT_VALIDATION_INVALID_AUDIT_DATA	Παρουσιάστηκε σφάλμα κατά τον έλεγχο των audit πεδίων της κλήσης. Κάποια από τα απαιτούμενα πεδία της εγγραφής ιχνηλασιμότητας λείπουν ή είναι κενά (τα συγκεκριμένα πεδία αναφέρονται ρητά) ή κάποιο πεδίο έχει λανθασμένη τιμή (π.χ. το πεδίο auditTransactionDate έχει εσφαλμένη μορφή ημ/νίας)
GEN_INVALID_DATA	Παρουσιάστηκε σφάλμα κατά τον έλεγχο εγκυρότητας των πεδίων εισόδου της υπηρεσίας. Κάποιο από τα υποχρεωτικά πεδία δεν δόθηκε ή δόθηκε με μη έγκυρη τιμή (αναφέρονται πιο συγκεκριμένες λεπτομέρειες για το σφάλμα)
GEN_COMMUNICATION_ERROR	Παρουσιάστηκε σφάλμα κατά την επικοινωνία με τη διαδικτυακή υπηρεσία του εξωτερικού φορέα (απαιτείται επικοινωνία με την Τεχνική Υποστήριξη του εξωτερικού φορέα)
GEN_DATABASE_CONNECTION_ERROR	Παρουσιάστηκε σφάλμα κατά τη σύνδεση με τη Βάση Δεδομένων (απαιτείται επικοινωνία με την Τεχνική Υποστήριξη)
GEN_GENERAL_ERROR	Παρουσιάστηκε απροσδιόριστο σφάλμα (απαιτείται επικοινωνία με την Τεχνική Υποστήριξη του ΚΕΔ)
GEN_AUTHORIZATION_MAX_OPEN_CALLS_EXCEEDED	Έχει γίνει υπέρβαση του ημερήσιου ορίου κλήσεων (Authorization Failed)

Πίνακας 1 – Πίνακας Γενικών Λαθών Κέντρου Διαλειτουργικότητας

Σημείωση: Στην περίπτωση που αποτύχει η σύνδεση κατά την επικοινωνία με το Web Service, επαναλαμβάνεται η κλήση από τη μεριά του client.

Παράρτημα Α – Δείγματα κλήσεων των Web Services

- **API: sendPothenAithma**

Κλήση 1. Παράδειγμα κλήσης με επιτυχημένη αποστολή και καταγραφή αιτήματος

Request:

```
{
  "auditRecord": {
    "auditTransactionId": "ab8b9618-c924-4edb-b214-4b029e2a3f71",
    "auditTransactionDate": "2024-01-18T17:51:30+02:00",
    "auditUnit": "POTHEN",
    "auditProtocol": "A123456789012345678901",
    "auditUserId": "user",
    "auditUserIp": "0.0.0.0"
  },
  "sendPothenAithmaInputRecord": {
    "institutionId": "TEST",
    "requestId": "A123456789012345678901",
    "requestType": 1,
    "referenceDate": "2023-12-31",
    "afm": "026310919",
    "name": "ΔΗΜ",
    "surname": "ΤΕΣ",
    "birthDate": "1962-05-08",
    "params": null
  }
}
```

Response:

```
{
  "sendPothenAithmaOutputRecord" : {
    "code" : 0,
    "message" : "Το αίτημα με αριθμό A123456789012345678901 υποβλήθηκε επιτυχώς",
    "replyDate" : "2024-01-19T17:00:00Z"
  },
  "callSequenceId": 73895838,
  "callSequenceDate": "2024-01-18T17:51:32.629+02:00",
  "errorRecord": {}
}
```

Κλήση 2. Παράδειγμα κλήσης με αποτυχημένη αποστολή αιτήματος

Request:

```
{
  "auditRecord": {
    "auditTransactionId": "518ae7b6-6e9c-4caf-a24e-eb3579185126",
    "auditTransactionDate": "2024-01-18T17:54:00+02:00",
    "auditUnit": "POTHEN",
    "auditProtocol": "A123456789112345678911",
    "auditUserId": "user",
    "auditUserIp": "0.0.0.0"
  },
  "sendPothenaithmaInputRecord": {
    "institutionId": "TEST",
    "requestId": "A123456789112345678911",
    "requestType": 2,
    "referenceDate": "2023-12-31",
    "afm": "000000000",
    "name": "ΟΝΟ",
    "surname": "ΕΠΩ",
    "birthDate": "1980-11-25",
    "params": null
  }
}
```

Response:

```
{
  "sendPothenaithmaOutputRecord": {
    "code": 99,
    "message": "Σφάλμα κατά την καταγραφή του αιτήματος"
  },
  "callSequenceId": 73895841,
  "callSequenceDate": "2024-01-18T17:54:01.286+02:00",
  "errorRecord": {}
}
```

- **API: getPothenData**

Κλήση 1. Παράδειγμα επιτυχημένης κλήσης (επιτυχημένη αποστολή & καταχώρηση αποτελέσματος)

Request:

```
{
  "auditRecord" : {
    "auditTransactionId" : "d9c2bb67-04d6-4ca2-a962-0db6ca17d357",
    "auditTransactionDate" : "2024-01-19T14:25:24+02:00",
    "auditUnit": "BANK",
    "auditProtocol": "A123456789012345678901",
    "auditUserId": "system",
    "auditUserIp": "0.0.0.0"
  },
  "getPothenDataInputRecord" : {
    "requestId" : "A123456789012345678901",
    "resultCode" : 0,
    "resultMessage" : "OK",
    "data" : "<encrypted_data>",
    "params" : "enc=crypto"
  }
}
```

Response:

```
{
  "getPothenDataOutputRecord" : {
    "code" : 0,
    "message" : "Το αποτέλεσμα στο αίτημα με αριθμό A123456789012345678901 λήφθηκε επιτυχώς."
  },
  "callSequenceId": 73895984,
  "callSequenceDate": "2024-01-19T14:25:26.814+02:00",
  "errorRecord": {}
}
```

Κλήση 2. Παράδειγμα κλήσης με **αποτυχία (επιχειρησιακή αδυναμία)** αποστολής απάντησης από την πλευρά του ΧΟ-ΠΙ

Request:

```
{
  "auditRecord" : {
    "auditTransactionId" : "28346662-ad71-47ce-a5fb-dfc01f70c25a",
    "auditTransactionDate" : "2024-02-13T14:05:00+02:00",
    "auditUnit": "BANK",
    "auditProtocol": "A123456789912345678990",
    "auditUserId": "system",
    "auditUserIp": "0.0.0.0"
  },
  "getPothenDataInputRecord" : {
    "requestId" : "A123456789912345678990",
    "resultCode" : 1,
    "resultMessage" : "Αδυναμία ταυτοποίησης του υπόχρεου"
  }
}
```

Response:

```
{
  "getPothenDataOutputRecord" : {
    "code" : 0,
    "message" : "Το αποτέλεσμα στο αίτημα με αριθμό A123456789912345678990 λήφθηκε επιτυχώς."
  },
  "callSequenceId": 73935841,
  "callSequenceDate": "2024-02-13T14:05:02.520+02:00",
  "errorRecord": {}
}
```

Κλήση 3. Παράδειγμα κλήσης με **αποτυχία στην αποκρυπτογράφηση** των δεδομένων από το ΟΠΣ ΠΟΘΕΝ

Request:

```
{
  "auditRecord" : {
    "auditTransactionId" : "bdc3f595-7926-4f64-a5ec-68ef99ad5e16",
    "auditTransactionDate" : "2024-01-19T14:28:15+02:00",
    "auditUnit" : "BANK",
    "auditProtocol" : "A100000000010000000000",
    "auditUserId" : "system",
    "auditUserIp" : "0.0.0.0"
  },
  "getPothenDataInputRecord" : {
    "requestId" : "A100000000010000000000",
    "resultCode" : 0,
    "resultMessage" : "OK",
    "data" : "<encrypted_data>",
    "params" : "enc=crypto"
  }
}
```

Response:

```
{
  "getPothenDataOutputRecord" : {
    "code" : 4,
    "message" : "Αποτυχία στην αποκρυπτογράφηση/αποκωδικοποίηση των δεδομένων. Τα δεδομένα έχουν κρυπτογραφηθεί/κωδικοποιηθεί με λάθος αλγόριθμο ή η δομή τους δεν είναι σωστή."
  },
  "callSequenceId" : 73895986,
  "callSequenceDate" : "2024-01-19T14:28:16.628+02:00",
  "errorRecord" : {}
}
```

Κλήση 4. Παράδειγμα αποτυχημένης κλήσης λόγω προσωρινού τεχνικού/διαδικτυακού προβλήματος που οφείλεται στον εξωτερικό φορέα (ΧΟ-ΠΙ)

Request:

```
{
  "auditRecord" : {
    "auditTransactionId" : "3eac7898-7e7f-4e7a-bf92-dbb8324a6837",
    "auditTransactionDate" : "2024-01-22T09:49:20+02:00",
    "auditUnit" : "BANK",
    "auditProtocol" : "A200000000020000000000",
    "auditUserId" : "system",
    "auditUserIp" : "0.0.0.0"
  },
  "getPothenDataInputRecord" : {
    "requestId" : "A200000000020000000000",
    "resultCode" : 0,
    "resultMessage" : "OK",
    "data" : "<encrypted_data>",
    "params" : "enc=crypto"
  }
}
```

Response:

```
{
  "callSequenceId": 101056003,
  "callSequenceDate": "2024-01-22T09:49:24.233+02:00",
  "errorRecord": {
    "errorCode": "GEN_COMMUNICATION_ERROR",
    "errorDescr": "Σφάλμα κατά την επικοινωνία με την εξωτερική διαδικτυακή υπηρεσία"
  }
}
```

- **API: getEncryptionInfo**

Παράδειγμα κλήσης της συγκεκριμένης υπηρεσίας

Request:

```
{
  "auditRecord": {
    "auditTransactionId": "4df6a8af-0605-420e-9e66-9ec65ec8fdd1",
    "auditTransactionDate": "2024-04-08T12:25:40+03:00",
    "auditUnit": "BANK",
    "auditProtocol": "NO_PROTOCOL",
    "auditUserId": "system",
    "auditUserIp": "0.0.0.0"
  },
  "getEncryptionInfoInputRecord": {
  }
}
```

Response:

```
{
  "getEncryptionInfoOutputRecord": {"keys": [ {
    "kty": "RSA",
    "e": "AQAB",
    "use": "enc",
    "kid": "gsis.gr",
    "alg": "RSA-OAEP-256",
    "n": "jR068 ... h63Vw"
  } ]},
  "callSequenceId": 107715637,
  "callSequenceDate": "2024-04-08T12:25:49.813+03:00",
  "errorRecord": {}
}
```

Παράρτημα Β – Ημερολόγιο Καταγραφής Κλήσεων

Η δομή της εγγραφής ιχνηλασιμότητας (σε WSDL περιγραφή) ορίζεται στον Κοινό Οδηγό Υλοποίησης Διαδικτυακών Υπηρεσιών

(<https://www.gsis.gr/dimosia-dioikisi/kentro-dialeitoyrgikotitas-ked-ypoyrgeiou-psifiakis-diakybernis/koinos-odigos>).

Πιο συγκεκριμένα, τα δύο πρώτα πεδία (auditTransactionId και auditTransactionDate) είναι υποχρεωτικά ενώ στη συγκεκριμένη διαδικτυακή υπηρεσία θεωρούνται υποχρεωτικά και τα πεδία auditUnit, auditProtocol.

Επιπλέον αποτελεί υποχρέωση του κάθε Φορέα να τηρεί το ημερολόγιο καταγραφής κλήσεων που πρέπει να περιλαμβάνει όλα τα παραπάνω στοιχεία για κάθε κλήση.

A/A	Περιγραφή	Τύπος Δεδομένων (Oracle / Java)	Σχόλια
1	auditTransactionId Μοναδικός Αριθμός Αίτησης WS Φορέα / Επιχειρησιακής Μονάδας	VARCHAR2(100) / String	Αλφαριθμητικό – μοναδικός αριθμός κλήσης της εφαρμογής πελάτη του Φορέα (π.χ. “1”, “2” κλπ) ο οποίος δίνεται από την client εφαρμογή του Φορέα για τη συγκεκριμένη κλήση της υπηρεσίας. Με τη χρήση αυτού του μοναδικού αριθμού, ο φορέας θα πρέπει να είναι σε θέση να απαντήσει ποιος ήταν ο πραγματικός (τελικός) χρήστης της υπηρεσίας από την πλευρά του, καθώς και ποιες ανάγκες εξυπηρετούσε
2	auditTransactionDate Ημ/νία και Ώρα Αίτησης WS Φορέα / Επιχειρησιακής Μονάδας YYYY-MM-DDThh:mm:ss+hh:mm (π.χ. 2025-02-15T16:20:14+02:00)	TIMESTAMP(6) / XMLGregorianCalendar	Χρονοσήμανση – ημερομηνία και ώρα σε μορφή ISO 8601 με timezone offset ως προς UTC, της μορφής: YYYY-MM-DDThh:mm:ss+hh:mm (π.χ. “2025-06-18T17:30:18+03:00”). Η χρονοσήμανση αντιστοιχεί στην ημερομηνία και ώρα της κλήσης από τον server του Φορέα που εκτελεί την client εφαρμογή και όχι στην ημερομηνία και ώρα του τοπικού υπολογιστή του χρήστη (end user).
3	auditUnit Περιγραφή Φορέα / Επιχειρησιακής Μονάδας	VARCHAR2(100) / String	Αλφαριθμητικό – όνομα φορέα που καλεί τη διαδικτυακή υπηρεσία (π.χ. “Eurobank” ή “Τράπεζα Ηπείρου”)

4	auditProtocol Αρ. Πρωτοκόλλου Αίτησης WS	VARCHAR2(100) / String	Αλφαριθμητικό – αριθμός πρωτοκόλλου (π.χ. “1123/10-10-2016”) προκειμένου να καλυφθούν συγκεκριμένες ανάγκες που σχετίζονται με μια Υπόθεση / Φάκελο που αναγνωρίζεται (από το Φορέα) με κάποιο μοναδικό τρόπο (π.χ. κάποιο αριθμό πρωτοκόλλου). Σ’ αυτές τις περιπτώσεις, ο web service client θα πρέπει να υποστηρίζει τη δυνατότητα ο τελικός χρήστης να μπορεί να συμπληρώσει τις πληροφορίες αυτές
5	auditUserId Αναγνωριστικό Χρήστη Φορέα / Επιχειρησιακής Μονάδας	VARCHAR2(100) / String	Αλφαριθμητικό – αναγνωριστικό τελικού χρήστη που καλεί τη διαδικτυακή υπηρεσία (π.χ. “user1”)
6	auditUserIp Διεύθυνση IP του Τελικού Χρήστη Φορέα / Επιχειρησιακής Μονάδας	VARCHAR2(20) / String	Αλφαριθμητικό – η διεύθυνση IP του τελικού χρήστη που καλεί τη διαδικτυακή υπηρεσία (π.χ. “10.18.24.13”)

Τα παραπάνω πεδία μεταβιβάζονται στο σώμα του JSON request κατά την κλήση της REST υπηρεσίας, μέσα στη δομή **auditRecord**, όπως παρακάτω:

```
"auditRecord": {
  "auditTransactionId": "Μοναδικός αριθμός κλήσης",
  "auditTransactionDate": "2025-06-27T12:40:25+03:00",
  "auditUnit": "Όνομα ΧΟΠΙ",
  "auditProtocol": "Αριθμός αιτήματος",
  "auditUserId": "Όνομα χρήστη",
  "auditUserIp": "Διεύθυνση IP (π.χ. 10.30.14.186)"
}
```

Ειδικά για την κλήση του API **getPothenData**, προτείνεται η συμπλήρωση των παρακάτω τιμών:

- * **auditTranscationId**: ένας μοναδικός αριθμός ανά κλήση (π.χ. ένα GUID ή αντίστοιχο μοναδικό αναγνωριστικό)
- * **auditTransactionDate**: η τρέχουσα ημερομηνία & ώρα κλήσης (μορφή YYYY-MM-DDThh:mm:ss+hh:mm)
- * **auditUnit**: η συνοπτική ονομασία της τράπεζας (π.χ. EUROBANK)
- * **auditProtocol**: ο αριθμός αιτήματος, δηλαδή το requestId (π.χ. A000000000000000000000)
- * **auditUserId**: εδώ θα συμπληρώνεται το κείμενο **"system"**
- * **auditUserIp**: εδώ θα συμπληρώνεται η IP του διακομιστή της Τράπεζας από τον οποίο πραγματοποιείται η κλήση ή η εικονική IP **"0.0.0.0"**

Παράρτημα Γ – Περιγραφή τύπων δεδομένων

1. API:sendPothenAithma

Πεδία εισόδου:

Περιγραφή	Τύπος Δεδομένων
auditRecord	-
sendPothenAithmaInputRecord	-
institutionId	String / VARCHAR2(30)
requestId	String / VARCHAR2(22)
requestType	Integer / NUMBER(1)
referenceDate	String / VARCHAR2(10)
afm	String / VARCHAR2(9)
name	String / VARCHAR2(40)
surname	String / VARCHAR2(80)
fatherName	String / VARCHAR2(40)
motherName	String / VARCHAR2(40)
birthDate	String / VARCHAR2(10)
params	String / CLOB

Πεδία εξόδου:

Περιγραφή	Τύπος Δεδομένων
sendPothenAithmaOutputRecord	-
code	Integer / NUMBER(2)
message	String / VARCHAR2(500)
replyDate	String / VARCHAR(20)
callSequenceId	BigDecimal / NUMBER(16)
callSequenceDate	String / TIMESTAMP(6)
errorRecord	-
errorCode	String / VARCHAR2(100)
errorDescr	String / VARCHAR2(500)

2. API:getPothenData

Πεδία εισόδου:

Όνομασίου πεδίου	Τύπος Δεδομένων
auditRecord	-
getPothenDataInputRecord	-
requestId	String / VARCHAR2(22)
resultCode	Integer / NUMBER(2)
resultMessage	String / VARCHAR2(1000)
data	String / CLOB
params	String / CLOB

Πεδία εξόδου:

Όνομασία πεδίου	Τύπος Δεδομένων
getPothenDataOutputRecord	-
code	Integer / NUMBER(2)
message	String / VARCHAR2(1000)
info	String / CLOB
callSequenceId	BigDecimal / NUMBER(16)
callSequenceDate	String / TIMESTAMP(6)
errorRecord	-
errorCode	String / VARCHAR2(100)
errorDescr	String / VARCHAR2(500)

3. API:getEncryptionInfo

Πεδία εισόδου:

Όνομασίου πεδίου	Τύπος Δεδομένων
auditRecord	-
getEncryptionInfoInputRecord	-
	-

Πεδία εξόδου:

Όνομασία πεδίου	Τύπος Δεδομένων
getEncryptionInfoOutputRecord	-
keys	List of objects
kty	String
e	String
use	String
kid	String
alg	String
n	String
callSequenceId	BigDecimal / NUMBER(16)
callSequenceDate	String / TIMESTAMP(6)
errorRecord	-
errorCode	String / VARCHAR2(100)
errorDescr	String / VARCHAR2(500)

Παράρτημα Δ – Πίνακας ΧΟ-ΠΙ που υποστηρίζονται

Παρακάτω αναφέρονται οι Χρηματοπιστωτικοί Οργανισμοί-Πιστωτικά Ιδρύματα (ΧΟ-ΠΙ) που υποστηρίζονται. Ο πίνακας ανανεώνεται συνεχώς.

Όνομασία ΧΟ-ΠΙ
ΕΘΝΙΚΗ ΤΡΑΠΕΖΑ ΕΛΛΑΔΑΣ
ΤΡΑΠΕΖΑ ALPHA BANK
ΤΡΑΠΕΖΑ ΠΕΙΡΑΙΩΣ
ΤΡΑΠΕΖΑ EUROBANK
ΑΤΤΙΚΑ BANK ΑΝΩΝΥΜΗ ΤΡΑΠΕΖΙΚΗ ΕΤΑΙΡΕΙΑ
ΟΡΤΙΜΑ BANK
ΣΥΝΕΤΑΙΡΙΣΤΙΚΗ ΤΡΑΠΕΖΑ ΧΑΝΙΩΝ
ΣΥΝΕΤΑΙΡΙΣΤΙΚΗ ΤΡΑΠΕΖΑ ΗΠΕΙΡΟΥ
ΠΑΓΚΡΗΤΙΑ ΤΡΑΠΕΖΑ
OLYMPUS BANK
ΣΥΝΕΤΑΙΡΙΣΤΙΚΗ ΤΡΑΠΕΖΑ ΚΑΡΔΙΤΣΑΣ
ΣΥΝΕΤΑΙΡΙΣΤΙΚΗ ΤΡΑΠΕΖΑ ΘΕΣΣΑΛΙΑΣ
ΤΑΜΕΙΟ ΠΑΡΑΚΑΤΑΘΗΚΩΝ ΚΑΙ ΔΑΝΕΙΩΝ (ΤΠΔ)
ΣΥΝΕΤΑΙΡΙΣΤΙΚΗ ΤΡΑΠΕΖΑ ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΤΡΑΠΕΖΑ ZIRAAT
PROCREDIT BANK
VIVA WALLET
ΔΟΚΙΜΑΣΤΙΚΟ ΤΡΑΠΕΖΙΚΟ ΙΔΡΥΜΑ

Παράρτημα Ε – Προς υλοποίηση υπηρεσία από ΧΟ-ΠΙ

Στο παράρτημα αυτό αποτυπώνονται οι προδιαγραφές που χρειάζεται να έχει το API που θα αναπτύξει/υλοποιήσει ο κάθε Χρηματοπιστωτικός Οργανισμός-Πιστωτικό Ίδρυμα (ΧΟ-ΠΙ) και θα διαθέσει στο Κέντρο Διαλειτουργικότητας.

Κάθε ΧΟ-ΠΙ θα χρειαστεί να υλοποιήσει μια διαδικτυακή υπηρεσία τεχνολογίας **REST** (API) για την υποδοχή των αιτημάτων από το ΟΠΣ Πόθεν. Το API θα έχει τα παρακάτω χαρακτηριστικά:

- Το API θα πρέπει να είναι τεχνολογίας **REST** και να δέχεται **POST** κλήσεις
- 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
- Το API θα μπορεί να υποδεχτεί σαν header παράμετρο (header "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. Καλό θα είναι το Πληροφοριακό Σύστημα του ΧΟ-ΠΙ να καταγράφει την μεταβιβαζόμενη τιμή για λόγους troubleshooting και ιχνηλασιμότητας.
- Ως μέθοδος αυθεντικοποίησης (για την πρόσβαση στο API από το ΚΕ.Δ.) θα χρησιμοποιείται η **Basic authentication**
- 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 ΣΤ)**
- 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**
- Σε περίπτωση επιτυχημένης απάντησης, το API θα επιστρέφει **HTTP STATUS 200** και η απάντηση θα έρχεται σε JSON format (με UTF-8 encoding)

Η υπηρεσία θα ονομάζεται "**getPothenAithma**" και 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 αντίστοιχα διαπιστευτήρια (credentials) για την αυθεντικοποίηση). Παράδειγμα URLs:

Δοκιμαστικό περιβάλλον (TEST): <https://bank.gr/gsis/test/getPothenAithma>

Παραγωγικό περιβάλλον (PROD): <https://bank.gr/gsis/getPothenAithma>

1. Ασφάλεια & Μέθοδος αυθεντικοποίησης

Η δικτυακή πρόσβαση στο web service των ΧΟ-ΠΙ θα γίνεται μέσω **HTTPS/TLS1.2** από τις υποδομές της ΓΓΠΣ&ΨΔ, με διαπιστευτήρια που θα δοθούν από τα ΧΟ-ΠΙ. Το ίδιο θα ισχύει και για τα web service του ΚΕ.Δ. για πρόσβαση από τα ΧΟ-ΠΙ.

Οι διαδικτυακές διευθύνσεις (IP addresses) του ΚΕ.Δ. της ΓΓΠΣ&ΨΔ θα δοθούν στα ΧΟ-ΠΙ, ώστε να διασφαλίσουν την πρόσβαση στην συγκεκριμένη υπηρεσία μόνο από τις συγκεκριμένες διευθύνσεις (**Παράρτημα ΣΤ**). Αντίστοιχα, οι διευθύνσεις (IP addresses) των web service των ΧΟ-ΠΙ θα δοθούν στη ΓΓΠΣ&ΨΔ, ώστε να διασφαλισθεί η άντληση πληροφοριών μόνο από τις συγκεκριμένες διευθύνσεις.

Κάθε ΧΟ-ΠΙ θα διαθέσει ως διαπιστευτήρια στο Κέντρο Διαλειτουργικότητας ζευγάρια συνθηματικών (username και password), ένα ζεύγος για το δοκιμαστικό και ένα για το παραγωγικό περιβάλλον, για την αυθεντικοποίηση των κλήσεων. Τα διαπιστευτήρια θα χρησιμοποιηθούν αποκλειστικά από το Κέντρο Διαλειτουργικότητας.

Ως μέθοδος αυθεντικοποίησης προτείνεται η Basic Authentication (εναλλακτικά μπορεί να χρησιμοποιηθεί η Bearer Authentication – υποενότητα 1.2).

1.1 Αυθεντικοποίηση μέσω Basic Authentication

Στην υποενότητα αυτή περιγράφεται η μέθοδος αυθεντικοποίησης μέσω **Basic Authentication**, την οποία και συνιστούμε στους ΧΟ-ΠΙ για λόγους ευρύτερης συμβατότητας, απλότητας στην υλοποίηση και ευκολίας στην χρήση.

Κάθε κλήση που θα πραγματοποιείται προς το service **getPothenAithma** του ΧΟ-ΠΙ, θα περιλαμβάνει έναν Header ο οποίος θα περιέχει το όνομα χρήστη και τον κωδικό πρόσβασης που έχουν δοθεί από το συγκεκριμένο ΧΟ-ΠΙ, 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, διαχωρισμένα με τον 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/και password) τότε το API **getPothenAithma** του ΧΟ-ΠΙ θα επιστρέφει http status **401/Unauthorized** χωρίς response.

Σε περίπτωση που πραγματοποιηθεί κλήση προς το API **getPothenAithma** από κάποια IP address που δεν ανήκει στη λίστα διαδικτυακών διευθύνσεων του Κέντρου

Διαλειτουργικότητας, τότε το API **getPothenAithma** του ΧΟ-ΠΙ θα επιστρέφει http status **403/Forbidden** χωρίς response. Για τη διαδικτυακή πρόσβαση και τις IP διευθύνσεις στις οποίες πρέπει να επιτρέπεται η πρόσβαση, παρακαλούμε δείτε το **Παράρτημα ΣΤ**.

Σε περίπτωση που στην είσοδο (body) δεν δοθεί ένα έγκυρο json request με τα προβλεπόμενα πεδία εισόδου (κακοσχηματισμένο request), το API **getPothenAithma** του ΧΟ-ΠΙ θα επιστρέφει http status **500/Internal Server Error**.

Εφόσον 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, το API **getPothenAithma** του ΧΟ-ΠΙ θα απαντάει με http status **200** και με κατάλληλο response, όπως περιγράφεται πιο κάτω.

1.2 Αυθεντικοποίηση μέσω Bearer Authentication

Στην περίπτωση που επιλεγεί αυτή η μέθοδος αυθεντικοποίησης, ο ΧΟ-ΠΙ θα πρέπει να διαθέσει ένα επιπλέον API για την αυθεντικοποίηση μέσω της παραγωγής ενός προσωρινού token. Το API αυτό θα ονομάζεται **authenticate** και θα χρησιμοποιείται για τη λήψη ενός κουπονιού πρόσβασης (access token) βραχείας διάρκειας:

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

Στην αρχή της επικοινωνίας μεταξύ του ΧΟ-ΠΙ και του Κέντρου Διαλειτουργικότητας (ΚΕΔ), το ΚΕΔ θα πρέπει να αποκτήσει ένα access token περιορισμένης διάρκειας. Γί αυτό το σκοπό, θα γίνεται μια προκαταρκτική κλήση απόκτησης του token, με μια POST κλήση προς το API **authenticate** και χρήση Basic Authentication (δηλαδή με username και password - <https://datatracker.ietf.org/doc/html/rfc7617>).

Ο ΧΟ-ΠΙ θα πρέπει να διαθέσει εκ των προτέρων στο ΚΕΔ ένα ζευγάρι συνθηματικών (username και password) για την αυθεντικοποίηση. Το ΚΕΔ θα δημιουργήσει ένα string της μορφής username:password, θα το κωδικοποιήσει σε **BASE64** και θα το προσθέσει στον Authorization header της κλήσης προς το API **authenticate**, όπως παρακάτω:

POST https://bank.gr/gsis/authenticate

Header => Authorization: Basic <base64-encoded username:password>

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

Authorization: **Basic dXNlcjpwYXNzd29yZDE=**

όπου “dXNlcjpwYXNzd29yZDE=” είναι η base64 κωδικοποίηση του αλφαριθμητικού “user:password1”.

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

```
curl -X POST https://bank.gr/gsis/authenticate -u 'user:password1'
```

Η απόκριση λάθους του API **authenticate** σε περίπτωση αποτυχίας 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 ΣΤ) θα είναι **403/Forbidden**.

Εφόσον το ζεύγος username και password είναι σωστό, το API **authenticate** θα απαντήσει με http status 200 και στο response θα επιστραφούν οι παρακάτω πληροφορίες σε json μορφή:

- * ο τύπος του token (*token_type: Bearer*)
- * το προσωρινό token (*access_token*)
- * η διάρκεια του token 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. Θα πρέπει να αρκεί ώστε να δώσει πρόσβαση στο κύριο API **getPothenAithma** και συνιστάται να έχει διάρκεια 600 δευτερόλεπτα/10 λεπτά (το expires_in συνιστάται να επιστρέφει την τιμή 600). Όλες οι κλήσεις προς το API **getPothenAithma** θα πρέπει να έχουν 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 έχει λήξει, το API **getPothenAithma** θα επιστρέφει http status **401/Unauthorized** χωρίς response

2. Είσοδος-Request

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

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

Οι παράμετροι εισόδου για την κλήση του API θα μεταβιβάζονται σε JSON μορφή και θα περιλαμβάνουν τα παρακάτω πεδία:

Πεδίο	Περιγραφή - Τύπος δεδομένων[Μέγιστο_Μήκος]
requestId*	Μοναδικός αριθμός αιτήματος – String[22] Αρχίζει με το ελληνικό κεφαλαίο γράμμα Α και ακολουθείται από 21 δεκαδικά ψηφία
requestType*	Τύπος αιτήματος – Integer[1] . Δυνατές τιμές: 1 ή 2: 1 => Με δάνεια 2 => Χωρίς δάνεια
referenceDate*	Ημερομηνία αναφοράς των δεδομένων – String[10] Η ημερομηνία δεν μπορεί να είναι μεταγενέστερη της ημερομηνίας κλήσης-τρέχουσας ημερομηνίας. Μορφή: yyyy-mm-dd (π.χ. 2024-01-18)
afm*	Αριθμός Φορολογικού Μητρώου υπόχρεου – String[9]
name*	Όνομα υπόχρεου – String[40]
surname*	Επώνυμο υπόχρεου – String[80]
fatherName	Πατρώνυμο υπόχρεου – String[40]
motherName	Μητρώνυμο υπόχρεου – String[40]
birthDate*	Ημερομηνία γέννησης υπόχρεου – String[10] Μορφή yyyy-mm-dd (π.χ. 1986-06-25)
params	Παράμετροι κρυπτογράφησης – String[65536] . Συμπληρώνεται προαιρετικά και ορίζει τις παραμέτρους που απαιτούνται για την κρυπτογράφηση των δεδομένων της απάντησης του ΧΟ-ΠΙ, ανάλογα με τις προδιαγραφές που έχουν συμφωνηθεί. Το πλήθος και οι τιμές των παραμέτρων συμφωνούνται αποκλειστικά μεταξύ ΟΠΣ Πόθεν και ΧΟ-ΠΙ και δεν αφορούν στο Κέντρο Διαλειτουργικότητας

** το πεδίο πρέπει να συμπληρώνεται υποχρεωτικά στην είσοδο*

Η κλήση θα μπορεί να δεχθεί στο σώμα της (body) όλα τα παραπάνω ορίσματα, ακόμα κι αν χρησιμοποιεί τελικά μόνο ένα μέρος αυτών. Όλα τα πεδία είναι μορφής String, εκτός από τον τύπο αιτήματος (requestType) που είναι ακέραιος αριθμός (Integer).

Επισήμανση σχετικά με τις συμπληρωμένες τιμές στα στοιχεία υπόχρεου:

Το ΟΠΣ Πόθεν θα αποστέλλει τον ΑΦΜ, την ημερομηνία γέννησης, τους τρεις πρώτους χαρακτήρες του ονόματος και τους τρεις πρώτους χαρακτήρες του επωνύμου του υπόχρεου. Δεν θα αποστέλλει το πατρώνυμο και το μητρώνυμο του υπόχρεου (τα πεδία `fatherName` & `motherName` υπάρχουν στις παραμέτρους κλήσης για πιθανή μελλοντική χρήση).

Παράδειγμα κλήσης (only request):

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 #1 (ΑΙΤΗΜΑ ΜΕ ΟΛΑ ΤΑ ΠΕΔΙΑ ΣΥΜΠΛΗΡΩΜΕΝΑ):

```
{
  "requestId": "A123456789112345678910",
  "requestType": 1,
  "referenceDate": "2023-12-31",
  "afm": "000000000",
  "name": "ΟΝΟΜΑ",
  "surname": "ΕΠΩΝΥΜΟ",
  "fatherName": "ΠΑΤΡΩΝΥΜΟ",
  "motherName": "ΜΗΤΡΩΝΥΜΟ",
  "birthDate": "1990-05-21"
}
```

Request #2 (ΑΙΤΗΜΑ ΑΠΟ ΟΠΣ ΠΟΘΕΝ):

```
{
  "requestId": "A123456789112345678910",
  "requestType": 1,
  "referenceDate": "2023-12-31",
  "afm": "000000000",
  "name": "ΟΝΟ",
  "surname": "ΕΠΩ",
  "birthDate": "1990-05-21"
}
```

3. Απάντηση-Response

Στις «επιτυχημένες» κλήσεις προς το API **getPothenAithma**, το http status της απάντησης θα είναι **200**, το δε περιεχόμενο θα επιστρέφεται σε JSON μορφή (με **UTF-8 encoding**) και θα περιλαμβάνει τα παρακάτω πεδία:

Πεδίο	Περιγραφή - Τύπος δεδομένων[Μέγιστο_Μήκος]
code*	Κωδικός απόκρισης – Integer[2] . Ακολουθεί το κωδικολόγιο με όλες τις δυνατές αποκρίσεις
message*	Περιγραφή/μήνυμα απόκρισης – String[1000] (ακολουθεί κωδικολόγιο)
replyDate	Ημερομηνία και ώρα αναμενόμενης ολοκλήρωσης μεταφοράς/αποστολής δεδομένων προς το ΟΠΣ Πόθεν Έσχες – String[20] Μορφή ημερομηνίας: yyyy-mm-ddThh24:mi:ssZ (π.χ. 2024-01-24T17:00:00Z) Το πεδίο επιστρέφει τιμή μόνο όταν το code είναι 0 ή 1. Ως ημερομηνία προτείνεται η επόμενη εργάσιμη ημέρα και ώρα 5μμ

* το πεδίο πρέπει να εμφανίζεται υποχρεωτικά στην απάντηση

Δυνατές τιμές των επιχειρησιακών πεδίων εξόδου code & message⁴

code	message	Παρατηρήσεις
0	Το αίτημα με αριθμό <requestId> υποβλήθηκε επιτυχώς	Επιτυχημένη αποστολή αιτήματος (ο αίτημα έχει υποβληθεί και καταγραφεί επιτυχώς στο Π.Σ. του ΧΟ-ΠΙ). Επιστρέφεται η αναμενόμενη ημερομηνία & ώρα ολοκλήρωσης αποστολής των πόθεν δεδομένων στο πεδίο replyDate
1	Το αίτημα με αριθμό <requestId> έχει ήδη υποβληθεί	Το αίτημα έχει ήδη υποβληθεί και καταγραφεί επιτυχώς στο Π.Σ. του ΧΟ-ΠΙ από προηγούμενη κλήση η οποία έλαβε χώρα λίγη ώρα πριν (συνήθως μερικά δευτερόλεπτα). Το ΟΠΣ Πόθεν επανέλαβε την κλήση επειδή δεν κατάφερε να λάβει/διαβάσει το response της πρώτης/προηγούμενης κλήσης λόγω κάποιου τεχνικού προβλήματος. Και σε αυτή την περίπτωση επιστρέφεται η αναμενόμενη ημερομηνία & ώρα ολοκλήρωσης αποστολής των πόθεν δεδομένων στο πεδίο replyDate
3	Το αίτημα με αριθμό <requestId> έχει ήδη υποβληθεί και διεκπεραιωθεί	Το αίτημα έχει υποβληθεί και καταγραφεί επιτυχώς στο Π.Σ. του ΧΟ-ΠΙ ΚΑΙ, ο ΧΟ-ΠΙ έχει ήδη καλέσει την υπηρεσία getPothenData και έχει αποστείλει επιτυχώς στο ΟΠΣ Πόθεν τα κρυπτογραφημένα δεδομένα με την απάντηση στο αίτημα με αριθμό requestId που υποβλήθηκε από το ΟΠΣ Πόθεν
7	Ο ΑΦΜ αντιστοιχεί σε πελάτη αλλά δεν διαθέτει λογαριασμούς ή άλλα προϊόντα	Ο υπόχρεος για τον οποίον υποβλήθηκε το αίτημα δεν διαθέτει προϊόντα στον συγκεκριμένο ΧΟ-ΠΙ για τη συγκεκριμένη ημ/νία αναφοράς δεδομένων του αιτήματος (referenceDate).

⁴ Με κόκκινο χρώμα οι κωδικοί και τα μηνύματα που αφορούν επιχειρησιακή αδυναμία αποστολής δεδομένων πόθεν για τον συγκεκριμένο υπόχρεο

8	Ο ΑΦΜ δεν μπορεί να ταυτοποιηθεί⁵	<p>Αδυναμία ταυτοποίησης του υπόχρεου λόγω μη πλήρους συμφωνίας των δεδομένων, πχ. βρέθηκε ο ΑΦΜ στο πελατολόγιο του ΧΟ-ΠΙ αλλά τα υπόλοιπα στοιχεία (όνομα, επώνυμο, ημ/νία γέννησης) δεν συμφωνούν ή βρέθηκε ο υπόχρεος με το συγκεκριμένο όνομα, επώνυμο ή ημ/νία γέννησης αλλά δεν συμφωνεί ο ΑΦΜ. Στην περίπτωση αυτή απαιτείται επικοινωνία μεταξύ του ΧΟ-ΠΙ και της ΓΓΠΣΨΔ για περαιτέρω διερεύνηση</p> <p>Η χρήση του συγκεκριμένου κωδικού απάντησης είναι μεν προαιρετική συστήνεται δε για την αποτελεσματικότερη επίλυση του προβλήματος. Εναλλακτικά, στη συγκεκριμένη περίπτωση ο ΧΟ-ΠΙ μπορεί να απαντήσει με τον κωδικό 9.</p>
9	Ο ΑΦΜ δεν αντιστοιχεί σε πελάτη	<p>Ο υπόχρεος για τον οποίον υποβλήθηκε το αίτημα δεν αντιστοιχεί σε πελάτη του ΧΟ-ΠΙ για τη συγκεκριμένη ημ/νία αναφοράς δεδομένων του αιτήματος (referenceDate).</p>
10	<p>Μη έγκυρη είσοδος: <περιγραφή ελέγχου που απέτυχε>, π.χ.</p> <p><i>Μη έγκυρη είσοδος: ο αριθμός αιτήματος είναι κενός</i></p> <p><i>Μη έγκυρη είσοδος: ο τύπος αιτήματος είναι κενός</i></p> <p><i>Μη έγκυρη είσοδος: ο τύπος αιτήματος δεν είναι έγκυρος</i></p> <p><i>Μη έγκυρη είσοδος: ο ΑΦΜ είναι κενός</i></p> <p><i>Μη έγκυρη είσοδος: ο ΑΦΜ δεν είναι αλγοριθμικά έγκυρος</i></p> <p><i>Μη έγκυρη είσοδος: το όνομα είναι κενό</i></p> <p><i>Μη έγκυρη είσοδος: το επώνυμο είναι κενό</i></p> <p><i>Μη έγκυρη είσοδος: η ημερομηνία γέννησης είναι κενή</i></p> <p><i>Μη έγκυρη είσοδος: η ημερομηνία γέννησης δεν είναι έγκυρη (μη έγκυρο format ή ημερομηνία που δεν υφίσταται)</i></p> <p><i>Μη έγκυρη είσοδος: η ημερομηνία αναφοράς δεδομένων είναι κενή</i></p> <p><i>Μη έγκυρη είσοδος: η ημερομηνία αναφοράς δεδομένων δεν είναι έγκυρη (μη έγκυρο format ή ημερομηνία που δεν υφίσταται)</i></p> <p><i>Μη έγκυρη είσοδος: η ημερομηνία αναφοράς δεδομένων είναι μεταγενέστερη της ημερομηνίας αποστολής του αιτήματος</i></p>	<p>Αυτός ο κωδικός σφάλματος υποδεικνύει ότι η μεταβιβαζόμενη τιμή σε ένα πεδίο απουσιάζει ή δεν είναι έγκυρη. Αυτή η περίπτωση είναι μάλλον απίθανο να συμβεί καθώς όλα τα αιτήματα που γίνονται από το ΟΠΣ Πόθεν έχουν έγκυρα δεδομένα εισόδου. Συνιστάται όμως η πραγματοποίηση ελέγχων και από την πλευρά του ΧΟ-ΠΙ</p>
90	Το Π.Σ. του ΧΟ-ΠΙ είναι προσωρινά μη διαθέσιμο για λόγους προγραμματισμένης συντήρησης	<p>Το αίτημα δεν μπόρεσε να αποθηκευτεί στο σύστημα του ΧΟ-ΠΙ λόγω (προγραμματισμένης) μη διαθεσιμότητας των υποδομών του</p>
99	Σφάλμα κατά την καταγραφή του αιτήματος	<p>Έκτακτο τεχνικό πρόβλημα στο Π.Σ. του ΧΟ-ΠΙ (π.χ. σφάλμα αποθήκευσης στη ΒΔ)</p>

⁵ Η ταυτοποίηση του υπόχρεου πραγματοποιείται πάντα με τον ΑΦΜ. Εφόσον βρεθεί στο πελατολόγιο του ΧΟ-ΠΙ **συστήνεται** η επιβεβαίωση από τους ΧΟ-ΠΙ με χρήση των τριών (3) πρώτων χαρακτήρων του επωνύμου και του ονόματος καθώς και της ημ/νίας γέννησης (ιδιαίτερα του έτους και του μήνα). Σε περίπτωση μη επιβεβαίωσης μπορεί να χρησιμοποιηθεί ο κωδικός 8. Αν δεν βρεθεί ο συγκεκριμένος ΑΦΜ ο ΧΟ-ΠΙ **μπορεί να απαντήσει** ότι ο υπόχρεος δεν αντιστοιχεί σε πελάτη του (κωδικός 9) ή μπορεί (**δεν είναι υποχρεωτικό**) να ψάξει με βάση τα υπόλοιπα δεδομένα και εφόσον βρεθεί να απαντήσει με τον κωδικό λάθους 8.

Για την καλύτερη κατανόηση των κωδικών απάντησης της συγκεκριμένης υπηρεσίας WS (πεδία code και message) δίνεται ο κάτωθι πίνακας αντιστοίχισης των περιπτώσεων κατά την υλοποίηση της διαλειτουργικότητας με χρήση του FTPS.

ΟΠΣ ΠΟΘΕΝ - ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ ΜΕΧΟ-ΠΙ					
ΤΡΟΠΟΣ ΥΛΟΠΟΙΗΣΗΣ	ΠΕΔΙΑ ΑΠΑΝΤΗΣΗΣ	ΠΕΛΑΤΗΣ ΜΕ ΠΡΟΪΟΝΤΑ	ΠΕΛΑΤΗΣ ΧΩΡΙΣ ΠΡΟΪΟΝΤΑ	ΔΕΝ ΕΝΑΙ ΠΕΛΑΤΗΣ	ΑΔΥΝΑΜΙΑ ΤΑΥΤΟΠΟΙΗΣΗΣ
FTPS	Εγγραφή υπόχρεου - Πλήθος εγγραφών προϊόντων υπόχρεου	> 0	0	-1	-1
	sendPothenAithmaOutputRecord				
	code	0/1	7	9	8/9
WS	message	Το αίτημα με αριθμό <requestId> υποβλήθηκε επιτυχώς/ Το αίτημα με αριθμό <requestId> έχει ήδη υποβληθεί	Ο ΑΦΜ αντιστοιχεί σε πελάτη αλλά δεν διαθέτει λογαριασμούς ή άλλα προϊόντα	Ο ΑΦΜ δεν αντιστοιχεί σε πελάτη	Ο ΑΦΜ δεν μπορεί να ταυτοποιηθεί / Ο ΑΦΜ δεν αντιστοιχεί σε πελάτη

4. Παραδείγματα κλήσης (πλήρη requests & responses)

1. Παράδειγμα κλήσης με επιστροφή κωδικού 0 (επιτυχημένη υποβολή αιτήματος)

Request:

```
curl -X POST https://bank.gr/gsis/getPothenAithma \  
-H 'CALL_ID: 1234567890123456' \  
-H 'Content-Type: application/json' \  
-H 'Authorization: Basic dXNlcjpwYXNzd29yZDE=' \  
--data '{"requestId": "A412663551041266355100", "requestType": 1, "referenceDate": "2023-12-31", "afm":  
"000000000", "name": "ONOMA", "surname": "ΕΠΩΝΥΜΟ", "fatherName": "ΠΑΤΡΩΝΥΜΟ", "motherName":  
"ΜΗΤΡΩΝΥΜΟ", "birthDate": "1990-05-21"}
```

Response:

```
-- HTTP STATUS 200 --  
  
{  
  "code": 0,  
  "message": "Το αίτημα με αριθμό A412663551041266355100 υποβλήθηκε επιτυχώς",  
  "replyDate": "2024-01-19T17:00:00Z",  
}
```

2. Παράδειγμα κλήσης με επιστροφή κωδικού 1 (το αίτημα έχει ήδη υποβληθεί)

Request:

```
curl -X POST https://bank.gr/gsis/getPothenAithma \  
-H 'CALL_ID: 1234567890123456' \  
-H 'Content-Type: application/json' \  
-H 'Authorization: Basic dXNlcjpwYXNzd29yZDE=' \  
--data '{"requestId": "A412663551041266355100", "requestType": 1, "referenceDate": "2023-12-31", "afm":  
"000000000", "name": "ONOMA", "surname": "ΕΠΩΝΥΜΟ", "fatherName": "ΠΑΤΡΩΝΥΜΟ", "motherName":  
"ΜΗΤΡΩΝΥΜΟ", "birthDate": "1990-05-21"}
```

Response:

```
-- HTTP STATUS 200 --  
  
{  
  "code": 1,  
  "message": "Το αίτημα με αριθμό A412663551041266355100 έχει ήδη υποβληθεί",  
  "replyDate": "2024-01-19T17:00:00Z",  
}
```

3. Παράδειγμα κλήσης με επιστροφή κωδικού 9 (όχι πελάτης του ΧΟ-ΠΙ/αδυναμία ταυτοποίησης προσώπου)

Request:

```
curl -X POST https://bank.gr/gsis/getPothenAithma \
-H 'CALL_ID: 1234567890123456' \
-H 'Content-Type: application/json' \
-H 'Authorization: Basic dXNlcjpwYXNzd29yZDE=' \
--data '{"requestId": "A412673958641267395860", "requestType": 1, "referenceDate": "2023-12-31", "afm": "660074123", "name": "ΑΓΝΩΣΤΟΣ", "surname": "ΑΓΝΩΣΤΟΣ", "fatherName": "ΑΓΝΩΣΤΟΣ", "motherName": "ΑΓΝΩΣΤΟΣ", "birthDate": "1987-12-18"}
```

Response:

-- HTTP STATUS 200 --

```
{
  "code": 9,
  "message": "Ο ΑΦΜ δεν αντιστοιχεί σε πελάτη"
}
```

4. Παράδειγμα κλήσης με επιστροφή κωδικού 10 (μη έγκυρη είσοδος)

Request:

```
curl -X POST https://bank.gr/gsis/getPothenAithma \
-H 'CALL_ID: 1234567890123456' \
-H 'Content-Type: application/json' \
-H 'Authorization: Basic dXNlcjpwYXNzd29yZDE=' \
--data '{"requestId": "A342834752534283475250", "requestType": 3, "referenceDate": "2023-12-31", "afm": "000000000", "name": "ΟΝΟΜΑ", "surname": "ΕΠΩΝΥΜΟ", "fatherName": "ΠΑΤΡΩΝΥΜΟ", "motherName": "ΜΗΤΡΩΝΥΜΟ", "birthDate": "1990-05-21"}
```

Response:

-- HTTP STATUS 200 --

```
{
  "code": 10,
  "message": "Μη έγκυρη είσοδος: Ο τύπος αιτήματος δεν είναι έγκυρος"
}
```

5. Δεύτερο παράδειγμα κλήσης με επιστροφή κωδικού 10 (μη έγκυρη είσοδος)

Request:

```
curl -X POST https://bank.gr/gsis/getPothenAithma \  
-H 'CALL_ID: 1234567890123456' \  
-H 'Content-Type: application/json' \  
-H 'Authorization: Basic dXNlcjpwYXNzd29yZDE=' \  
--data '{"requestId": "A152973148615297314860", "requestType": 1, "referenceDate": "2023-12-31", "afm":  
"999999999", "name": "ONOMA", "surname": "ΕΠΩΝΥΜΟ", "fatherName": "ΠΑΤΡΩΝΥΜΟ", "motherName":  
"ΜΗΤΡΩΝΥΜΟ", "birthDate": "1982-05-21"}
```

Response:

-- HTTP STATUS 200 --

```
{  
  "code": 10,  
  "message": "Μη έγκυρη είσοδος: Ο ΑΦΜ δεν είναι αλγοριθμικά έγκυρος"  
}
```

6. Παράδειγμα κλήσης με επιστροφή κωδικού 99 (σφάλμα στην καταγραφή αιτήματος)

Request:

```
curl -X POST https://bank.gr/gsis/getPothenAithma \  
-H 'CALL_ID: 1234567890123456' \  
-H 'Content-Type: application/json' \  
-H 'Authorization: Basic dXNlcjpwYXNzd29yZDE=' \  
--data '{"requestId": "A112233445511223344550", "requestType": 1, "referenceDate": "2023-12-31", "afm":  
"000000000", "name": "ONOMA", "surname": "ΕΠΩΝΥΜΟ", "fatherName": "ΠΑΤΡΩΝΥΜΟ", "motherName":  
"ΜΗΤΡΩΝΥΜΟ", "birthDate": "1982-05-21"}
```

Response:

-- HTTP STATUS 200 --

```
{  
  "code": 99,  
  "message": "Σφάλμα κατά την καταγραφή του αιτήματος"  
}
```

7. Παράδειγμα κλήσης με αποτυχημένη αυθεντικοποίηση (λανθασμένα credentials – μέθοδος Basic Authentication)

Request:

```
curl -X POST https://bank.gr/gsis/getPothenAithma \  
-H 'CALL_ID: 1234567890123456' \  
-H 'Content-Type: application/json' \  
-H 'Authorization: Basic dXNlcjB3cm9uZ3Bhc3N3b3Jk' \  
--data '{"requestId": "A123451234512345123450", "requestType": 1, "referenceDate": "2023-12-31", "afm":  
"000000000", "name": "ONOMA", "surname": "ΕΠΩΝΥΜΟ", "fatherName": "ΠΑΤΡΩΝΥΜΟ", "motherName":  
"ΜΗΤΡΩΝΥΜΟ", "birthDate": "1990-05-21"}
```

Response:

-- HTTP STATUS 401 --

8. Παράδειγμα κλήσης με αποτυχημένη αυθεντικοποίηση (ληγμένο access token – μέθοδος Bearer Authentication)

Request:

```
curl -X POST https://bank.gr/gsis/getPothenAithma \  
-H 'CALL_ID: 1234567890123456' \  
-H 'Content-Type: application/json' \  
-H 'Authorization: Bearer 6B29FC40-CA47-1067-B31D-00DD010662DA' \  
--data '{"requestId": "A123451234512345123450", "requestType": 1, "referenceDate": "2023-12-31", "afm":  
"000000000", "name": "ONOMA", "surname": "ΕΠΩΝΥΜΟ", "fatherName": "ΠΑΤΡΩΝΥΜΟ", "motherName":  
"ΜΗΤΡΩΝΥΜΟ", "birthDate": "1990-05-21"}
```

Response:

-- HTTP STATUS 401 --

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

Για περαιτέρω ασφάλεια, οι υπηρεσίες που θα αναπτυχθούν από τους Χρηματοπιστωτικούς Οργανισμούς και τα Πιστωτικά Ιδρύματα 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** ενώ θα απαγορεύεται (access forbidden) σε όλες τις υπόλοιπες.

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

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, είναι νόμιμες επιπλέον οι ακόλουθες εσωτερικές IP:

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)**

Απαιτείται 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 ΧΟ-ΠΙ (ανάλογα και με τις διαδικτυακές ρυθμίσεις που εφαρμόζονται) με IP (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 IP (ακόμα και οι εσωτερικές).

Όταν προς το API των ΧΟ-ΠΙ πραγματοποιείται μια κλήση από “άγνωστη” IP, το API θα πρέπει να μην αποδέχεται την κλήση και να απαντάει με http status **403/Forbidden**.