ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ
ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ

ΚΟΙΝΟΣ ΟΔΗΓΟΣ ΥΛΟΠΟΙΗΣΗΣ

ΔΙΑΔΙΚΤΥΑΚΩΝ ΥΠΗΡΕΣΙΩΝ

για client applications

Εκδοση

(client v1.)

Οδηγίες χρήσης

Πίνακας Περιεχομένων

Περιεχόμενα

1. Γενικά Στοιχεία

Οι διαδικτυακές υπηρεσίες (web services) είναι μία τεχνολογία που επιτρέπει στα πληροφοριακά συστήματα - εφαρμογές να επικοινωνούν μεταξύ τους ανεξαρτήτως γλώσσας προγραμματισμού και πλατφόρμας. Μία διαδικτυακή υπηρεσία είναι μία διεπαφή λογισμικού (software interface) που περιλαμβάνει: α) μία συλλογή από λειτουργίες, οι οποίες περιγράφουν τον τρόπο ανταλλαγής μηνυμάτων, που βασίζονται στο μορφότυπο XML (Extensible Markup Language) και β) τα δεδομένα προς ανταλλαγή με άλλη εφαρμογή.

Οι διαδικτυακές υπηρεσίες παρέχουν λειτουργικότητα σε χρήστες του διαδικτύου μέσα από ένα δικτυακό πρωτόκολλο το οποίο στις περισσότερες περιπτώσεις είναι το SOAP (Simple Object Access Protocol). Οι SOAP διαδικτυακές υπηρεσίες προσφέρουν έναν λεπτομερή τρόπο περιγραφής των διεπαφών τους και επιτρέπουν στον τελικό χρήστη-καταναλωτή (consumer) να αναπτύξει μια εφαρμογή-πελάτη (client application) για να επικοινωνήσει μαζί τους. Η περιγραφή παρέχεται σε ένα έγγραφο XML το οποίο ονομάζεται έγγραφο WSDL (Web Services Description Language).

Το έγγραφο WSDL μιας διαδικτυακής υπηρεσίας στο Κέντρο Διαλειτουργικότητας του Υπουργείου Οικονομικών παρέχεται μέσω ενός URL, όπως παρακάτω:

https://www1.gsis.gr/esb/testService?wsdl

2. Αρχές Υλοποίησης των Web Services στο Κέντρο Διαλειτουργικότητας

2.1. Κοινές Υπηρεσίες

Στο Κέντρο Διαλειτουργικότητας έχει υλοποιηθεί ένα σύνολο κοινών υπηρεσιών. Οι κοινές υπηρεσίες περιλαμβάνουν τις παρακάτω λειτουργίες:

- ✓ Αυθεντικοποίηση Χρηστών (User Authentication)
- ✓ Έλεγχο Δικαιωμάτων Πρόσβασης Χρηστών (User Authorization)
- ✓ Υπηρεσία Ιχνηλασιμότητας (Auditing)
- ✓ Επαλήθευση Ψηφιακής Υπογραφής (Digital Signature Verification)
- ✓ Διαχείριση Εξαιρέσεων (Exception Handling)

Οι κοινές υπηρεσίες (Common Services) έχουν υλοποιηθεί στο Enterprise Service Bus (ESB) και χρησιμοποιούνται από όλες τις διαδικτυακές υπηρεσίες του Κέντρου Διαλειτουργικότητας. Η υλοποίηση των παραπάνω υπηρεσιών συμβάλλει στην υιοθέτηση αρθρωτής αρχιτεκτονικής και προτυποποιεί την ανάπτυξη των διαδικτυακών υπηρεσιών, διαθέτοντας τις παραπάνω λειτουργίες για χρήση από όλες τις διαδικτυακές υπηρεσίες.

2.1.1 Αυθεντικοποίηση χρηστών

Η υπηρεσία αυτή περιλαμβάνει πιστοποίηση του ονόματος χρήστη (username) και κωδικού πρόσβασης (password) που χρησιμοποιεί η διαδικτυακή υπηρεσία. Τα παραπάνω διαπιστευτήρια εκδίδονται μέσω της Εφαρμογής Διαχείρισης Αιτημάτων Διαλειτουργικότητας (ΕΔΑ).

2.1.2 Έλεγχος Δικαιωμάτων Πρόσβασης Χρηστών

Η υπηρεσία αυτή ελέγχει αν ο (αυθεντικοποιημένος) χρήστης έχει δικαίωμα χρήσης της συγκεκριμένης διαδικτυακής υπηρεσίας που καλεί.

2.1.3 Ιχνηλασιμότητα (Auditing)

Η υπηρεσία ιχνηλασιμότητας αποτελεί έναν μηχανισμό καταγραφής πληροφοριών για όλες τις διαδικτυακές υπηρεσίες του Κέντρου Διαλειτουργικότητας. Λαμβάνει χώρα σε κάθε κλήση διαδικτυακής υπηρεσίας, μετά από την επιτυχημένη αυθεντικοποίηση χρήστη. Η υπηρεσία ιχνηλασιμότητας περιλαμβάνει:

- Έλεγχο για την ύπαρξη των απαραίτητων πεδίων audit σε κάθε κλήση.
- Δημιουργία ενός μοναδικού αριθμού εξυπηρέτησης κλήσης καθώς και της ημερομηνίας κλήσης (callSequenceId και callSequenceDate).
- Λήψη των δεδομένα εισόδου (Request XML) του αιτήματος κλήσης και καταγραφή των απαραίτητων στοιχείων της.

2.1.3.1 Στοιχεία - Εγγραφή Ιχνηλασιμότητας

Όλες οι διαδικτυακές υπηρεσίες απαιτούν κατά την κλήση τους την προσθήκη των **στοιχείων** (**εγγραφής) ιχνηλασιμότητας** (**auditRecord**). Τα στοιχεία αυτά χρησιμοποιούνται προκειμένου να γίνεται καταγραφή της κάθε κλήσης (request call) αλλά και για να είναι εφικτή η ιχνηλασιμότητα των κλήσεων που έχουν εξυπηρετηθεί. Τα στοιχεία ιχνηλασιμότητας (auditRecord) περιέχουν τα παρακάτω 6 πεδία:

1. **auditTransactionId**: αλφαριθμητικό – α/α κλήσης της εφαρμογής πελάτη του Φορέα (π.χ. “1”, “2” κλπ)
2. **auditTransactionDate**: ημερομηνία & ώρα, της μορφής yyyy-mm-ddThh:mm:ssZ – η ημερομηνία & ώρα κλήσης (π.χ. “2016-09-21T10:08:24Z”)
3. **auditUnit**: αλφαριθμητικό – όνομα φορέα που καλεί τη διαδικτυακή υπηρεσία (π.χ. “ΙΚΑ” ή “Δήμος Αθηναίων”)
4. **auditProtocol**: αλφαριθμητικό – αριθμός πρωτοκόλλου (π.χ. “1123/10-10-2016”)
5. **auditUserId**: αλφαριθμητικό – αναγνωριστικό τελικού χρήστη που καλεί τη διαδικτυακή υπηρεσία (π.χ. “user1”)
6. **auditUserIp**: αλφαριθμητικό – η διεύθυνση IP του τελικού χρήστη που καλεί τη διαδικτυακή υπηρεσία (π.χ. “10.18.24.13”)

2.1.3.2 Περιγραφή της Εγγραφής Ιχνηλασιμότητας (WSDL)

Η δομή της εγγραφής ιχνηλασιμότητας (σε WSDL περιγραφή) ορίζεται ως εξής:

```
<xs:complexType name="auditRecord">
    <xs:sequence>
        <xs:element name="auditTransactionId" type="xs:string"/>
        <xs:element name="auditTransactionDate" type="xs:dateTime"/>
        <xs:element minOccurs="0" name="auditUnit" type="xs:string"/>
        <xs:element minOccurs="0" name="auditProtocol" type="xs:string"/>
        <xs:element minOccurs="0" name="auditUserId" type="xs:string"/>
        <xs:element minOccurs="0" name="auditUserIp" type="xs:string"/>
    </xs:sequence>
</xs:complexType>
```

Τα δύο πρώτα πεδία (auditTransactionId και auditTransactionDate) είναι υποχρεωτικά, ενώ από τα υπόλοιπα τέσσερα πεδία είναι υποχρεωτικό τουλάχιστον ένα (ορίζονται από το Διαχειριστή της Διαδικτυακής υπηρεσίας μέσα από την Εφαρμογή Διαχείρισης Αιτημάτων Διαλειτουργικότητας (ΕΔΑ)). Συνίσταται κατά την κλήση των λειτουργιών των διαδικτυακών υπηρεσιών να συμπληρώνονται **όλα** τα παραπάνω πεδία.

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

Περισσότερες πληροφορίες παρέχονται στο Παράρτημα Α.

2.1.4 Επαλήθευση Ψηφιακής Υπογραφής

Η υπηρεσία επαλήθευσης ψηφιακής υπογραφής μηνύματος διενεργεί την επαλήθευση της ορθότητας του υπογεγραμμένου μηνύματος που λαμβάνεται από τη διαδικτυακή υπηρεσία. Το κύκλωμα της ψηφιακής υπογραφής/επαλήθευσης είναι προαιρετικό και ενεργοποιείται κατά περίπτωση.

2.1.5 Διαχείριση Εξαιρέσεων

Η υπηρεσία διαχείρισης εξαιρέσεων έχει υλοποιηθεί μέσω ενός μηχανισμού χειρισμού και καταγραφής αναπάντεχων συμβάντων (εξαιρέσεων) ο οποίος έχει τη δυνατότητα να εντοπίζει και να καταγράφει οποιοδήποτε «έκτακτο» πρόβλημα (exception) δημιουργηθεί κατά τη διάρκεια της εξυπηρέτησης της κλήσης μιας διαδικτυακής υπηρεσίας στο Κέντρο Διαλειτουργικότητας.

3. Ασφάλεια

Οι διαδικτυακές υπηρεσίες του Κέντρου Διαλειτουργικότητας χρησιμοποιούν WS-Security πρωτόκολλο[1] και η εξουσιοδότηση στις υπηρεσίες τους γίνεται με χρήση διαπιστευτηρίων-συνθηματικών (username και password). Τα συνθηματικά δημιουργούνται στην Εφαρμογή Διαχείρισης Αιτημάτων Διαλειτουργικότητας (ΕΔΑ).

Κάθε κλήση (call request) μιας λειτουργίας διαδικτυακών υπηρεσιών που πραγματοποιείται στο Κέντρο Διαλειτουργικότητας θα πρέπει να περιλαμβάνει το SOAP Header στο οποίο δηλώνονται τα παραπάνω διαπιστευτήρια (username και password), και επιπρόσθετα στοιχεία που αφορούν στη συγκεκριμένη κλήση.

Ένα παράδειγμα SOAP Header μιας κλήσης (call request) είναι το παρακάτω:

```
<soapenv:Header>
  <wsse:Security soapenv:mustUnderstand="1" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
    <wsse:UsernameToken wsu:Id="UsernameToken-134F28397E84840D3F14484484569051">
      <wsse:Username>myUsername</wsse:Username>
      <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-
token-profile-1.0#PasswordText">myPassword</wsse:Password>
    </wsse:UsernameToken>
  </wsse:Security>
</soapenv:Header>
```

Σε περίπτωση που παραλειφθεί το SOAP Header ή που δεν δοθούν σωστά συνθηματικά τότε η διαδικτυακή υπηρεσία επιστρέφει κατάλληλο μήνυμα λάθους, όπως για παράδειγμα:

“A security error was encountered when verifying the message”

[1] Το πρωτόκολλο **WS-security** καθορίζει τον τρόπο με τον οποίο μπορεί να επιβληθεί η ακεραιότητα και η εμπιστευτικότητα σε μηνύματα και επιτρέπει την επικοινωνία διαφόρων μορφών token ασφαλείας, όπως το Security Assertion Markup Language (SAML), Kerberos, και X.509. Κύριος στόχος του είναι η χρήση της XML υπογραφής και κρυπτογράφησης (XML Signature και XML Encryption) για την παροχή ασφάλειας από σημείο σε σημείο (end-to-end security).

4. Πεδία εισόδου διαδικτυακών υπηρεσιών

Κάθε λειτουργία των διαδικτυακών υπηρεσιών (web service operation) που περιγράφεται στο WSDL αποτελείται από τα παρακάτω πεδία εισόδου:

- SoapHeader: είναι η SOAP κεφαλίδα του μηνύματος στην οποία παρέχονται τα διαπιστευτήρια κλήσης της διαδικτυακής υπηρεσίας,
- auditRecord: η εγγραφή ιχνηλασιμότητας,
- requestRecord: αποτελεί το ουσιαστικό κομμάτι της κλήσης διαδικτυακής υπηρεσίας. Περιλαμβάνει τα κατά περίπτωση πεδία εισόδου επιχειρησιακών δεδομένων της λειτουργίας

5. Πεδία εξόδου διαδικτυακών υπηρεσιών

Κάθε λειτουργία των διαδικτυακών υπηρεσιών (web service operation) που περιγράφεται στο WSDL επιστρέφει πάντοτε τα παρακάτω πεδία εξόδου:

• **callSequenceId**: αποτελεί το μοναδικό αριθμό αναγνώρισης της εξυπηρέτησης κλήσης της διαδικτυακής υπηρεσίας (web service request). Ο αριθμός αυτός παράγεται αυτόματα κατά την έναρξη της κλήσης και είναι μοναδικός για όλες τις κλήσεις στο Κέντρο Διαλειτουργικότητας,

• **callSequenceDate**: καταγράφει την ημερομηνία και την ώρα κλήσης. Ουσιαστικά αποτελεί τη χρονοσήμανση (timestamp) του εξυπηρετητή του Κέντρου Διαλειτουργικότητας κατά την οποία αποδόθηκε το callsequenceId κλήσης και αποτελεί ζευγάρι με αυτό,

• **errorRecord**: αποτελεί μια δομή στην οποία καταγράφονται τα σφάλματα που προκύπτουν κατά την εξυπηρέτηση της κλήσης και περιέχει τα πεδία **errorCode** (κωδικός σφάλματος) και **errorDescr** (περιγραφή μηνύματος σφάλματος). Σε περίπτωση που δεν συμβεί κάποιο σφάλμα (τεχνικό/λογικό) τότε τα πεδία της δομής επιστρέφουν με τιμή NULL

Η δομή των παραπάνω πεδίων (σε WSDL περιγραφή) είναι η εξής:

```
<xs:element name="callSequenceId" type="xs:decimal"/>
<xs:element name="callSequenceDate" type="xs:dateTime"/>
<xs:element name="errorRecord" type="tns:errorRecord"/>

<xs:complexType name="errorRecord">
    <xs:sequence>
        <xs:element minOccurs="0" name="errorCode" type="xs:string"/>
        <xs:element minOccurs="0" name="errorDescr" type="xs:string"/>
    </xs:sequence>
</xs:complexType>
```

Εκτός από τα παραπάνω πεδία, κάθε λειτουργία διαδικτυακής υπηρεσίας επιστρέφει και τα πεδία των εκάστοτε επιχειρησιακών δεδομένων της λειτουργίας (τα παραπάνω πεδία εξαρτώνται από τη συγκεκριμένη λειτουργία).

5.1 Πεδία εξόδου με τιμές NULL

Γενικά υπάρχουν δύο τρόποι για την αναπαράσταση των πεδίων που έχουν τιμή NULL στο Response XML. Ο πρώτος τρόπος είναι να μην εμφανίζονται καθόλου τα πεδία με τιμή NULL στο Response XML ενώ ο δεύτερος τρόπος είναι να εμφανίζονται έχοντας στο αντίστοιχο XML tag τους την ιδιότητα (attribute) nil=”true”, για παράδειγμα:

```
<surname xsi:nil=”true” />
```

Στις διαδικτυακές υπηρεσίες του Κέντρου Διαλειτουργικότητας έχει υιοθετηθεί ο πρώτος τρόπος. Επομένως, η απουσία των πεδίων εξόδου από το Response XML σημαίνει αυτομάτως ότι έχουν τιμή NULL.

6. Αντιμετώπιση Λαθών

Σε περίπτωση λάθους κατά την κλήση μιας διαδικτυακής υπηρεσίας του Κέντρου Διαλειτουργικότητας, στην απάντηση (Response XML) επιστρέφεται ο κωδικός και το μήνυμα λάθους που αποτυπώνονται από τα πεδία **errorCode** και **errorDescr**.

Στον παρακάτω πίνακα καταγράφονται οι πιο συνηθισμένες περιπτώσεις λαθών.

Κωδικός λάθος (Error Code Name)	Περιγραφή μηνύματος λάθους
GEN_AUDIT_VALIDATION_INV_DATA_OR_UNAUTH_OPER	Τα διαπιστευτήρια (username & password) που χρησιμοποιήθηκαν στον SoapHeader κατά την κλήση δεν έχουν εξουσιόδοτηση χρήσης της συγκεκριμένης διαδικτυακής λειτουργίας
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 περιγράφονται στο μήνυμα λάθους errorDescr)
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 (στο μήνυμα λάθους errorDescr αναφέρονται πιο συγκεκριμένες λεπτομέρειες για το σφάλμα)
GEN_COMMUNICATION_ERROR	Παρουσιάστηκε σφάλμα κατά την επικοινωνία με τη διαδικτυακή υπηρεσία του εξωτερικού φορέα (επικοινωνήστε με την Τεχνική Υποστήριξη του εξωτερικού φορέα)
GEN_DATABASE_CONNECTION_ERROR	Παρουσιάστηκε σφάλμα κατά τη σύνδεση με τη Βάση Δεδομένων (επικοινωνήστε με την Τεχνική Υποστήριξη του ΚΕΔ)
GEN_GENERAL_ERROR	Παρουσιάστηκε απροσδιόριστο σφάλμα (επικοινωνήστε με την Τεχνική Υποστήριξη του ΚΕΔ)

7. Γενική δομή αιτήματος κλήσης (Request XML) των διαδικτυακών υπηρεσιών

Κάθε λειτουργία των διαδικτυακών υπηρεσιών του Κέντρου Διαλειτουργικότητας απαιτεί ως είσοδο (input) τα παρακάτω πεδία:

* **εγγραφή ιχνηλασιμότητας** (βλέπε παράγραφο 2.1.3)

* **εγγραφή πεδίων εισόδου της λειτουργίας**. Το όνομα της εγγραφής περιλαμβάνει ένα κομμάτι της ονομασίας της λειτουργίας και έχει ως κατάληξη τη λέξη “Record” (για παράδειγμα "oaedHistoryRecord", "getIdentityRecord" κλπ). Περιλαμβάνει επίσης και τα κατά περίπτωση πεδία των επιχειρησιακών δεδομένων.

Οι παραπάνω δύο εγγραφές "εσωκλείονται" από μια γενική δομή, το όνομα της οποίας ορίζεται από το όνομα της λειτουργίας και έχει ως κατάληξη τη λέξη “Request” (για παράδειγμα “oaedHistoryRequest”, “getIdentityRequest” κλπ).

Ακολουθεί ένα παράδειγμα κλήσης (XML Request) για τη λειτουργία *retrieveVerificationProgress* της διαδικτυακής υπηρεσίας *verificationProgressService*:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ind="http://gsis.ggps.interoperability/verificationProgressService">
   <soapenv:Header>
    …
   </soapenv:Header>
   <soapenv:Body>
         <retrieveVerificationProgressRequest>
               <auditRecord>  <!-- η εγγραφή του auditRecord -->
                     <auditTransactionId> ... </auditTransactionId>
                     <auditTransactionDate> ... </auditTransactionDate>
                     <auditUnit> ... </auditUnit>
                     <auditProtocol> ... </auditProtocol>
                     <auditUserId> ... </auditUserId>
                     <auditUserIp> ... </auditUserIp>
               </auditRecord>
               <VerificationProgressRecord>  <!-- η εγγραφή με τα πεδία εισόδου της υπηρεσίας -->
                     <dateFrom> ... </dateFrom>
                     <dateTo> ... </dateTo>
                     <extOrg> ... </extOrg>
```

```
                </VerificationProgressRecord>
        <retrieveVerificationProgressRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

8. Γενική δομή απόκρισης (Response XML) των διαδικτυακών υπηρεσιών

Τα πεδία που λαμβάνονται ως απόκριση της κλήσης (Response XML) κάθε λειτουργίας των διαδικτυακών υπηρεσιών είναι τα ακόλουθα:

* **εγγραφή πεδίων εξόδου της λειτουργίας**. Το όνομα της εγγραφής περιλαμβάνει ένα κομμάτι της ονομασίας της λειτουργίας και έχει ως κατάληξη τη λέξη “Record” (για παράδειγμα "oaedHistoryRecord", "getIdentityRecord" κλπ). Η εγγραφή αυτή περιλαμβάνει τα κατά περίπτωση πεδία των επιχειρησιακών δεδομένων που επιστρέφονται.

* **πεδίο callSequenceId** , **πεδίο callSequenceDate** , **εγγραφή σφάλματος** (βλέπε παράγραφο 5).

Όλα τα παραπάνω πεδία "εσωκλείονται" από μια γενική δομή, το όνομα της οποίας ορίζεται από την ονομασία της λειτουργίας και έχει ως κατάληξη τη λέξη “Response” (για παράδειγμα “oaedHistoryResponse”, “getIdentityResponse” κλπ).

Ακολουθεί ένα παράδειγμα απόκρισης (XML Response) για τη λειτουργία *retrievePayProgress* της διαδικτυακής υπηρεσίας *payProgressService*:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Body>
        <ns2:retrievePayProgressResponse xmlns:ns2=" http://gsis.ggps.interoperability
/payProgressService">
                <retrievePayProgressRecord>  <!-- η εγγραφή με τα πεδία εξόδου της υπηρεσίας -->
                        <deletedAmount> ... </deletedAmount>
                        <firstEstablishedAmount> ... </firstEstablishedAmount>
                        <overdueAmount> ... </overdueAmount>
                        <paidAmount> ... </paidAmount>
                        <reducedAmount> ... </reducedAmount>
                        <restAmount> ... </restAmount>
                        <totalAmount> ... </totalAmount>
                </retrievePayProgressRecord>
                <callSequenceId> ... </callSequenceId>
```

```
                <callSequenceDate> ... </callSequenceDate>
                <errorRecord/>  <!-- η εγγραφή του errorRecord, εδώ τα πεδία του errorDescr &
errorCode είναι null επειδή δεν συνέβη κάποιο σφάλμα -->
        </ns2:retrievePayProgressResponse>
    </soap:Body>
</soap:Envelope>
```

9. Προαπαιτούμενα για κατανάλωση διαδικτυακών υπηρεσιών του ΚΕΔ

Η κατανάλωση διαδικτυακών υπηρεσιών του Κέντρου Διαλειτουργικότητας μπορεί να γίνει από οποιοδήποτε σύγχρονο περιβάλλον που υποστηρίζει δημιουργία συνδέσεων διαδικτύου (internet connections) μέσω πρωτοκόλλου TLSv1.2, αποστολή XML εγγράφων (XML requests) και λήψη XML εγγράφων (XML responses), ανεξάρτητα από το λειτουργικό σύστημα (Windows, Linux, MacOS κλπ) που χρησιμοποιείται.

Στα περισσότερα περιβάλλοντα θα χρειαστεί επιπλέον η λήψη και η εγκατάσταση του πιστοποιητικού σελίδας της ΓΓΠΣ (αρχείο gsis.gr.cer).

Ακολουθούν ενδεικτικά τα προπαιτούμενα σε γλώσσα προγραμματισμού Java και σε περιβάλλον ανάπτυξης ORACLE (PL/SQL) όπου έχουν γίνει δοκιμές στις διαδικτυακές υπηρεσίες του ΚΕΔ:

Java

- Java 1.8.x
- Λήψη πιστοποιητικού σελίδας gsis.gr (αρχείο gsis.gr.cer)
- Προσθήκη του πιστοποιητικού στην αποθήκη πιστοποιητικών της Java (java_home\jre\lib\security\cacerts)

Oracle (PL/SQL)

- Oracle 11g R2 ή ανώτερη
- Δυνατότητα χρήσης του πακέτου UTL_HTTP και ενεργοποίηση HTTPS πρόσβασης
- Λήψη πιστοποιητικού σελίδας gsis.gr (αρχείο gsis.gr.cer)
- Δημιουργία oracle wallet και προσθήκη του πιστοποιητικού

ΠΑΡΑΡΤΗΜΑ Α : Αναλυτική περιγραφή πεδίων Εγγραφής Ιχνηλασιμότητας

Α/Α	Περιγραφή	Τύπος Δεδομένων	Σχόλια
1	**AUDIT_TRANSACTION_ID** Μοναδικός Α/Α Αίτησης WS Φορέα / Επιχειρηματικής Μονάδας	VARCHAR2(100)	Μοναδικός κωδικός αίτησης ο οποίος δίνεται από την client εφαρμογή του Φορέα για τη συγκεκριμένη κλήση της υπηρεσίας. Με τη χρήση του κωδικού αυτού και μόνο 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	**AUDIT_TRANSACTION_DATE** Ημ/νία και Ώρα Αίτησης WS Φορέα / Επιχειρηματικής Μονάδας yyyy-mm-ddThh:mm:ssZ πχ 2016-10-10T10:08:24Z	DATE	Χρονοσήμανση Φορέα - Ημερομηνία και ώρα της κλήσης - από τον server του Φορέα που τρέχει την Client εφαρμογή και όχι το end user client pc.
3	**AUDIT_UNIT** Περιγραφή Φορέα / Επιχειρηματικής Μονάδας	VARCHAR2(100)	Το όνομα του Φορέα που καλεί τη διαδικτυακή υπηρεσία.
4	**AUDIT_ PROTOCOL** Αρ. Πρωτοκόλλου Αίτησης WS	VARCHAR2(100)	Ενδέχεται η κλήση ενός web service να γίνεται από ένα Φορέα για 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	**AUDIT_USER_ID** Αναγνωριστικό Χρήστη Φορέα / Επιχειρηματικής Μονάδας	VARCHAR2(100)	Το όνομα που χρησιμοποιεί ο τελικός χρήστης ώστε να συνδεθεί στην εφαρμογή πελάτη μέσω της οποίας γίνεται η συγκεκριμένη κλήση της διαδικτυακής υπηρεσίας. Το AUDIT_USER_ID μπορεί να είναι είτε κάποιο κωδικοποιημένο αναγνωριστικό είτε το πλήρες όνομα του τελικού χρήστη.

A/A	Περιγραφή	Τύπος Δεδομένων	Σχόλια
6	**AUDIT_USER_IP** Διεύθυνση IP του Τελικού Χρήστη Φορέα / Επιχειρηματικής Μονάδας	VARCHAR2(20)	Η διεύθυνση IP του τελικού χρήστη (end user pc) που κάνει χρήση της διαδικτυακής υπηρεσίας.

ΠΑΡΑΡΤΗΜΑ Β : Παραδείγματα κλήσης & απάντησης διαδικτυακών υπηρεσιών

1. XML Request διαδικτυακής λειτουργίας "getAFMIdentification" (Επιβεβαίωση Στοιχείων Φυσικού Προσώπου με βάση τον ΑΦΜ):

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ind="http://gsis.ggps.interoperability/IndividualConfirmationInterface">
  <soapenv:Header>
    <wsse:Security soapenv:mustUnderstand="1" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
      <wsse:UsernameToken wsu:Id="UsernameToken-134F28397E84840D3F14484484569051">
        <wsse:Username>T12345678T92345BY6KK4Y9E9MESVLRYY2W</wsse:Username>
        <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-
token-profile-1.0#PasswordText">*********</wsse:Password>
      </wsse:UsernameToken>
    </wsse:Security>
  </soapenv:Header>
  <soapenv:Body>
    <ind:getAFMIdentificationRequest>
        <auditRecord>
          <auditTransactionId>1</auditTransactionId>
          <auditTransactionDate>2016-10-21T12:15:21Z</auditTransactionDate>
          <auditUnit>ΓΓΠΣ</auditUnit>
          <auditProtocol>114</auditProtocol>
          <auditUserId>user1</auditUserId>
          <auditUserIp>10.6.32.28</auditUserIp>
      </auditRecord>
      <getAFMIdentificationRecord>
        <afm>123456783</afm>
        <surname>ΠΕΤΡΟΠΟΥΛΟΣ</surname>
        <name>ΠΕΤ</name>
        <birthYear>1983</birthYear>
      </getAFMIdentificationRecord>
    </ind:getAFMIdentificationRequest>
```

```
  </soapenv:Body>
</soapenv:Envelope>
```

2. XML Response διαδικτυακής λειτουργίας "getAFMIdentification" (Επιβεβαίωση Στοιχείων Φυσικού Προσώπου με βάση τον ΑΦΜ):

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ns2:getAFMIdentificationResponse
xmlns:ns2="http://gsis.ggps.interoperability/IndividualConfirmationInterface">
      <getAFMIdentificationRecord>
        <afm>123456783</afm>
        <id>AB123456</id>
        <name>ΠΕΤΡΟΣ</name>
        <surname>ΠΕΤΡΟΠΟΥΛΟΣ</surname>
        <fname>ΠΕΤΡΟΣ</fname>
        <mname>ΠΕΤΡΟΥΛΑ</mname>
        <birthYear>1983</birthYear>
        <msg>Ταυτοποιείται ορθώς</msg>
      </getAFMIdentificationRecord>
      <callSequenceId>387866172</callSequenceId>
      <callSequenceDate>2016-10-21T12:15:24.329+03:00</callSequenceDate>
      <errorRecord/>
    </ns2:getAFMIdentificationResponse>
  </soap:Body>
</soap:Envelope>
```