Αριθμ. ΠΟΛ. 1166 (7)

Τεχνικές προδιαγραφές πρωτοκόλλου επικοινωνίας και κρυπτογράφησης για την διαβίβαση δεδομένων στο πληροφοριακό σύστημα των ΦΗΜ.

Ο ΔΙΟΙΚΗΤΗΣ ΤΗΣ ΑΝΕΞΑΡΤΗΤΗΣ ΑΡΧΗΣ ΔΗΜΟΣΙΩΝ ΕΣΟΔΩΝ

Έχοντας υπόψη:

1. Τις διατάξεις:

α) Των άρθρων 12 παρ. 9 και 40 του ν. 4308/2014 (Α’ 251) «Ελληνικά Λογιστικά Πρότυπα, συναφείς ρυθμίσεις και άλλες διατάξεις».

β) Του άρθρου 20 του ν. 3842/2010 (Α΄ 58) «Αποκατάσταση φορολογικής δικαιοσύνης, αντιμετώπιση της φοροδιαφυγής και άλλες διατάξεις.» και ειδικότερα του εδαφίου β της παραγράφου 6 αυτού.

γ) Της Α.Υ.Ο. ΠΟΛ. 1220/2012 (Β’3517) «Κωδικοποίηση - Συμπλήρωση τεχνικών προδιαγραφών Φορολογικών ηλεκτρονικών μηχανισμών και συστημάτων. Διαδικασίες χρήσης και λειτουργίας τους. Προδιαγραφές αποστελλομένων αρχείων στην ΓΓΠΣ».

δ) Της Α.Υ.Ο. ΠΟΛ 1221/2012 (Β’ 3513) «Αναβάθμιση λογισμικών υποστήριξης των Ε.Α.Φ.Δ.Σ.Σ. - Καθορισμός αποστελλομένων αρχείων δεδομένων των φορολογικών στοιχείων στην Γ.Γ.Π.Σ. κατ’ εφαρμογή των διατάξεων του άρθρου 20 του ν. 3842/2010 (ΦΕΚ 58/Α/23.4.2010)».

ε) της απόφασης Γ.Γ.Δ.Ε ΠΟΛ 1068/1-4-2015 (Β’497) «Διαδικασίες έγκρισης και ανάκλησης Φ.Η.Μ.. Υποχρεώσεις κατόχων άδειας καταλληλότητας Φορολογικών Ηλεκτρονικών Μηχανισμών (Φ.Η.Μ.), πωλητών Φ.Η.Μ., πιστοποιημένων τεχνικών Φ.Η.Μ., κατόχων - χρηστών Φ.Η.Μ..».

στ) του κεφαλαίου Α’ «Σύσταση Ανεξάρτητης Αρχής Δημοσίων Εσόδων» του Μέρους Πρώτου του ν. 4389/2016 (Α’ 94), και ειδικότερα των παραγράφων 1 και 5 του άρθρου 14, της παρ. 1 του άρθρου 2, του άρθρου 7 και των υποπαραγράφων 2 και 3 του άρθρου 41 αυτού.

ζ) της Δ.ΟΡΓ.Α 1036960 ΕΞ2017/10-3-2017 (Β’ 968 και 1238) απόφασης του Διοικητή της Ανεξάρτητης Αρχής Δημοσίων Εσόδων «Οργανισμός της Ανεξάρτητης Αρχής Δημοσίων Εσόδων (Α.Α.Δ.Ε.)».

2. Την αριθμ. 1 της 20-1-2016 πράξη του Υπουργικού Συμβουλίου (ΥΟΔΔ 18) «Επιλογή και διορισμός Γενικού Γραμματέα της Γενικής Γραμματείας Δημοσίων Εσόδων του Υπουργείου Οικονομικών», σε συνδυασμό με τις διατάξεις του πρώτου εδαφίου της παρ. 10 του άρθρου 41 του ν. 4389/2016.

3. Την Δ6Α 1015213 ΕΞ 2013/28-1-2013 (Β’ 130 και Β’ 372) απόφαση του Υπουργού Οικονομικών και του Υφυπουργού Οικονομικών «Μεταβίβαση αρμοδιοτήτων στον Γενικό Γραμματέα της Γενικής Γραμματείας Δημοσίων Εσόδων του Υπουργείου Οικονομικών», όπως τροποποιήθηκε, συμπληρώθηκε και ισχύει, σε συνδυασμό με την υποπαράγραφο α’ της παρ. 3 του άρθρου 41 του ν. 4389/2016.

4. Το Δ30Β4008733/1-3-2013 έγγραφο με θέμα «Ορισμός πρωτοκόλλου επικοινωνίας του Λογισμικού Υποστήριξης των ΕΑΦΔΣΣ και των ΦΗΜ νέων προδιαγραφών με την ΓΓΠΣ. Διευκρινίσεις για τα αποστελλόμενα αρχεία».

5. Τη διασφάλιση του απορρήτου των επικοινωνιών (ΦΕΚ Β’ 2715/17-11 -2011).

6. Το γεγονός ότι, από τις διατάξεις της παρούσας απόφασης, δεν προκαλείται δαπάνη σε βάρος του Προϋπολογισμού της Ανεξάρτητης Αρχής Δημοσίων Εσόδων (Α.Α.Δ.Ε.), αποφασίζουμε:

Τον ορισμό προδιαγραφών πρωτοκόλλου επικοινωνίας και κρυπτογράφησης, που εφαρμόζουν αφενός το πληροφοριακό σύστημα των ΦΗΜ και αφετέρου οι ΦΗΜ που έλαβαν έγκριση με τις διατάξεις των τεχνικών προδιαγραφών της ΠΟΛ 1220/2012, όλες οι ΕΑΦΔΣΣ και τα λογισμικά διαβίβασης δεδομένων των Παροχών Υπηρεσιών Ηλεκτρονικής Έκδοσης Παραστατικών Πωλήσεων.

Άρθρο 1
Ορισμοί - Διευκρινίσεις

Το λογισμικό διαβίβασης δεδομένων που λειτουργεί σε Πάροχο υπηρεσιών ηλεκτρονικής έκδοσης παραστατικών πωλήσεων του ν. 4308/2014 (Α’251) διαβιβάζει συγκεκριμένα δεδομένα των παραστατικών στο πληροφοριακό σύστημα των ΦΗΜ.

Για λόγους συντομογραφίας, στο κείμενο της απόφασης αυτής με τον όρο «Διαβιβαστής Δεδομένων (Δ.Δ.)» νοούνται οι Φορολογικοί Ηλεκτρονικοί Μηχανισμοί που έλαβαν έγκριση με την ΠΟΛ 1220/2012, όλες οι ΕΑΦΔΣΣ και τα λογισμικά διαβίβασης δεδομένων που λειτουργούν σε παρόχους υπηρεσιών ηλεκτρονικής έκδοσης παραστατικών πωλήσεων.

Η πρόσβαση στο Πληροφοριακό σύστημα των ΦΗΜ γίνεται μέσω της ιστοσελίδας της Α.Α.Δ.Ε. (www.aade.gr), επιλέγοντας από τις φορολογικές υπηρεσίες: «Επιχειρήσεις - Φορολογικές υπηρεσίες - Βιβλία - Στοιχεία -Ταμειακές μηχανές - Πληροφοριακό Σύστημα των ΦΗΜ».

Άρθρο 2
Αλγόριθμος κρυπτογράφησης
και πρωτόκολλο επικοινωνίας

Οι Δ.Δ. κρυπτογραφούν τα προς αποστολή δεδομένα με τον συμμετρικό αλγόριθμο κρυπτογράφησης AES-256.

Το κλειδί κρυπτογράφησης AES key παρέχεται από την ιστοσελίδα του Πληροφοριακού Συστήματος των ΦΗΜ στην επιλογή «Επιχειρήσεις». Το κλειδί κρυπτογράφησης AES key, είναι μοναδικό ανά Δ.Δ.

Η κρυπτογράφηση γίνεται εντός του Δ.Δ., έτσι ώστε να μην αποκαλύπτονται τα δεδομένα εκτός αυτού.

Τα προς αποστολή δεδομένα των Δ.Δ. είναι τα αρχεία s.txt. Το url αποστολής τους αναγράφεται στο πληροφοριακό σύστημα των ΦΗΜ. Οι προδιαγραφές που πρέπει να τηρούνται κατά την αποστολή των δεδομένων, παρέχονται στο παράρτημα Α της παρούσας απόφασης.

Άρθρο 3
Διευκρινίσεις για τα δεδομένα
των μεταδιδόμενων αρχείων.

Τα δεδομένα που μεταδίδονται καθορίζονται από τον πίνακα Γ της ΑΥΟ ΠΟΛ 1220/2012.

3.1 Ειδικότερα, σε ότι αφορά το πεδίο είδος παραστατικού:

Στην περίπτωση που υπάρχει παρακράτηση φόρου, θα περιλαμβάνεται το ποσό παρακράτησης ως επιπλέον πληροφορία μέσα στο πεδίο είδος παραστατικού του

αρχείου e.txt (πίνακας Γ της ΑΥΟ ΠΟΛ 1220/2012) ως εξής: <είδος παραστατικού> $ <ποσό> (π.χ. 161$100.00, 161#22$100.10).

Οι ανακτήσεις των ανωτέρω εξειδικευμένων πληροφοριών γίνονται από το λογισμικό των ΕΑΦΔΣΣ, με κάθε πρόσφορο τρόπο. Ενδεικτικά δύναται να γίνονται, α) μέσω της γραμμής δεδομένων που εκτυπώνεται στο παραστατικό από το εμπορικό λογισμικό της επιχείρησης β) από την ανίχνευση του ποσού παρακρατούμενου φόρου σε συγκεκριμένα σημεία του παραστατικού. Το πρόσημο του ποσού τυχούσας παρακράτησης φόρου καθορίζεται με βάση τον πίνακα Δ της ΑΥΟ ΠΟΛ 1220/2012.

3.2 Στο πεδίο κωδικός νομίσματος, χρησιμοποιείται κωδικός 3 γραμμάτων σύμφωνα με το διεθνές πρότυπο ISO 4217. Όταν χρησιμοποιείται το ευρώ, στο αντίστοιχο πεδίο του πίνακα Γ της ΑΥΟ ΠΟΛ 1220/2012 αντί του «EUR», εναλλακτικά μπορεί να χρησιμοποιείται ο αριθμός 0.

Άρθρο 4
Αυτόματος συγχρονισμός ώρας

Οι ΦΗΜ έχουν την δυνατότητα αυτόματου συγχρονισμού της ώρας με την ώρα του πληροφοριακού συστήματος των ΦΗΜ. Οι σχετικές προδιαγραφές για τον συγχρονισμό της ώρας, παρέχονται στο παράρτημα Β της παρούσας απόφασης.

Άρθρο 5
Έναρξη ισχύος

Η παρούσα απόφαση ισχύει από την δημοσίευσή της στην Εφημερίδα της Κυβερνήσεως.

Η απόφαση αυτή να δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως.

Παράρτημα Α: Προδιαγραφές αλγορίθμου κρυπτογράφησης και του πρωτοκόλλου επικοινωνίας

Α1. Η μετάδοση των δεδομένων γίνεται με τη χρήση τηλεπικοινωνιακών δικτύων που λειτουργούν βάσει του κανονισμού για τη διασφάλιση του απορρήτου των ηλεκτρονικών επικοινωνιών της Αρχής Διασφάλισης Απορρήτου των Επικοινωνιών (ΑΔΑΕ) (ΦΕΚ Β’ 2715/17-11-2011).

Α2. Η μετάδοση γίνεται αφού το αρχείο δεδομένων κρυπτογραφηθεί με χρήση αλγορίθμου κρυπτογράφησης AES-256. Ως κλειδί κρυπτογράφησης χρησιμοποιείται κλειδάριθμος ελάχιστου μήκους 256 bits που εκδίδεται από το Πληροφοριακό Σύστημα των ΦΗΜ για τον συγκεκριμένο Δ.Δ. και φυλάσσεται στο πληροφοριακό σύστημα των ΦΗΜ της Α.Α.Δ.Ε..

Το πληροφοριακό σύστημα των ΦΗΜ αποκρυπτογραφεί τα δεδομένα με τον ίδιο τρόπο. Το κλειδί ανακτάται από το μητρώο των ΦΗΜ του πληροφοριακού συστήματος των ΦΗΜ. Η αναφορά στο μητρώο γίνεται βάσει του ονόματος του κρυπτογραφημένου αρχείου, σύμφωνα με την ΑΥΟ ΠΟΛ 1220/2012.

Α3. Το πρωτόκολλο επικοινωνίας των Δ.Δ. με το πληροφοριακό σύστημα των ΦΗΜ είναι το ακόλουθο:

Το αρχείο S.TXT κρυπτογραφείται με AES256 σε mode CBC (Cipher Block Chaining) και τυχαίο initialization vector μήκους 16 bytes που παράγεται αυτόματα από το λογισμικό του Δ.Δ. και με κλειδί (AES Key) που έχει παραλάβει ο κάτοχος του Δ.Δ.

Το κρυπτογραφημένο περιεχόμενο διαβιβάζεται με HTTP POST multipart form ως αρχείο με όνομα αυτό του S.TXT, σε κωδικοποίηση GR-ELOT928, από το οποίο προκύπτει ο σειριακός αριθμός του Δ.Δ. που αφορά και ο αριθμός Z που υποβάλλεται. Ειδικά για τα λογισμικά διαβίβασης των παροχών υπηρεσιών ηλεκτρονικής έκδοσης παραστατικών πωλήσεων, ως αριθμός Z εννοείται ο αριθμός πακέτου αποστολής.

Η διαβίβαση περιέχει ένα πεδίο τύπου TEXT με όνομα IV και περιεχόμενο την Hexadecimal αναπαράσταση του initialization vector (32 χαρακτήρες HEX έναντι των 16 byte που αποτελούν το initialization vector) και ένα μοναδικό πεδίο τύπου FILE με ονομασία πεδίου "S_TXT_FILE". Στο πεδίο τύπου FILE "S_TXT_FILE" η τιμή για το όνομα του αρχείου είναι το όνομα του διαβιβαζόμενου S.TXT ενώ η τιμή του περιεχομένου του αρχείου είναι το κρυπτογραφημένο περιεχόμενο του αρχείου S.TXT.

Ο Δ.Δ. αποστέλλει τα δεδομένα, υλοποιεί το πρωτόκολλο HTTP 1.1 και ειδικότερα την εντολή redirect που ενδέχεται να αποστέλλεται από το πληροφοριακό σύστημα των ΦΗΜ προκειμένου να μεταφέρεται η επικοινωνία στον server κάποιου provider.

Το πληροφοριακό σύστημα των ΦΗΜ αποκρυπτογραφεί τα περιεχόμενα των αρχείων S.TXT που υποβάλλονται με βάση το κλειδί που γνωρίζει και αντιστοιχεί στο συγκεκριμένο Δ.Δ., και απαντάει με κωδικοποίηση text/plain GR-ELOT928 ως εξής:

• Σε περίπτωση που όλα είναι εντάξει, το πληροφοριακό σύστημα των ΦΗΜ απαντάει με την ένδειξη OK (λατινικοί χαρακτήρες) και επιβεβαιώνει έτσι την επιτυχή ολοκλήρωση της διαβίβασης του S.TXT αρχείου.

• Σε περίπτωση που υπάρχει κάποιο λάθος, το πληροφοριακό σύστημα των ΦΗΜ απαντάει με 3 πεδία, χωρισμένα με delimiter (;), από τα οποία το πρώτο είναι πάντα η ένδειξη ERR, το δεύτερο ο κωδικός λάθους σύμφωνα με τον Πίνακα λαθών, και το τρίτο μια παράμετρος για επεξήγηση του λάθους.

Πίνακας λαθών 1

Πεδίο 1	Πεδίο 2	Πεδίο 3
ERR	1 = Λάθος ονομασία αρχείου S.TXT (π.χ. όχι 31 χαρακτήρες, λάθος σε τμήματα του ονόματος, κ.λπ.).	
ERR	2 = Λάθος S/N Δ.Δ. (π.χ. δεν είναι καταχωρημένος στην βάση της ΑΑΔΕ, οι χαρακτήρες δεν είναι λατινικοί, κ.λπ.).	
ERR	3 = Το Z έχει ήδη υποβληθεί	N = Τελ. αριθμός υποβληθέντος Z
ERR	4=ΛείπειτοπροηγούμενοZ	N = Τελ. αριθμός υποβληθέντος Z

Η επιστροφή λαθών (ERR 1 - 4) από το πληροφοριακό σύστημα των ΦΗΜ ολοκληρώνει ανεπιτυχώς την επικοινωνία, καθιστώντας μη αποδέκτη την διαβίβαση του αρχείου S.TXT.

Επίσης κάθε άλλη απάντηση από το πληροφοριακό σύστημα των ΦΗΜ θεωρείται επίσης λάθος για άγνωστο λόγο (π.χ. δυσλειτουργία κάποιου υποσυστήματος του πληροφοριακού συστήματος των ΦΗΜ ή του provider).

Δεν γίνεται έλεγχος ημερομηνίας του S.TXT ούτε των γραμμών του (e.txt), καθώς σε πραγματικές συνθήκες είναι δυνατόν να προκύψει σχετικό λάθος μετά από (λάθος) επέμβαση τεχνικού στον ΦΗΜ.

Παράρτημα Β: Προδιαγραφές συγχρονισμού της ώρας των ΦΗΜ με την ώρα του πληροφοριακού συστήματος των ΦΗΜ.

Καθώς το πρωτόκολλο επικοινωνίας ανάμεσα στο πληροφοριακό σύστημα των ΦΗΜ και τους ΦΗΜ είναι το HyperText Transfer Protocol (HTTP), οι ΦΗΜ πρέπει να διαβάζουν την ημερομηνία και ώρα από το header της απάντησης του πληροφοριακού συστήματος των ΦΗΜ, όπως προβλέπεται από το RFC7231. Παράδειγμα: Date: Sun, 06 Nov 1994 08:49:37 GMT. Σημειωτέο ότι η ώρα που παρέχει το πληροφοριακό σύστημα των ΦΗΜ είναι GMT και γι’ αυτό οι ΦΗΜ πρέπει να κάνουν την κατάλληλη προσαρμογή σε ώρα Ελλάδος.

Ο ΦΗΜ, μετά την λήψη της σωστής ημέρας, ώρας, λεπτών και δευτερολέπτων από το πληροφοριακό σύστημα των ΦΗΜ κατά την επικοινωνία με αυτό όταν εκδίδεται Ζ, αναπροσαρμόζει τις αντίστοιχες ρυθμίσεις του, εφόσον:

α) Ο ημερήσιος μετρητής αποδείξεων-σημάνσεων είναι 0 (άρα δεν έχει ανοίξει νέα ημέρα) και

β) Η ληφθείσα σειρά ημερομηνίας-ώρας-λεπτών-δευτερολέπτων έχει απόκλιση μέχρι 30 λεπτά από την ημερομηνία-ώρα του τελευταίου Ζ του ΦΗΜ και

γ) Η επιλογή «Αυτόματη προσαρμογή ώρας από τον SERVER» στον ΦΗΜ είναι ενεργή.

Ειδικά για την περίπτωση όπου η ώρα του ΦΗΜ είναι πιο μπροστά από την ώρα του πληροφοριακού συστήματος των ΦΗΜ, αμέσως μετά τον συγχρονισμό της ώρας του ΦΗΜ κατά την έκδοση αναφοράς Ζ, θα πρέπει ο ΦΗΜ να απενεργοποιείται για όσο χρόνο χρειαστεί, προκειμένου να μην εκδοθεί απόδειξη εσόδου με ημερομηνία - ώρα προγενέστερη της τελευταίας φορολογικής απόδειξης (της αναφοράς Ζ συμπεριλαμβανομένης).

Η απόφαση αυτή να δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως.

Μοσχάτο, 10 Αυγούστου 2018

Ο Διοικητής

ΓΕΩΡΓΙΟΣ ΠΙΤΣΙΛΗΣ

ΕΘΝΙΚΟ ΤΥΠΟΓΡΑΦΕΙΟ
Καποδιστρίου 34, Τ.Κ. 104 32, Αθήνα
Τηλ. Κέντρο 210 5279000
Κείμενα προς δημοσίευση: webmaster.et@et.gr
02036032408180008