fintechiO
creative software solutions

A1155 – ERP to EFTPOS protocol proposal – v3 (Μαρτιος 2024)

1.1. Εισαγωγή

Το κείμενο περιγράφει τις ελάχιστες απαιτήσεις υλοποίησης για την επικοινωνία των συστημάτων έκδοσης στοιχείων λιανικής πώλησης ERP με τα τερματικά αποδοχής καρτών (EFTPOS) που βρίσκονται στο πεδίο. Σημαντικό ζητούμενο είναι να μπορέσουμε χρησιμοποιώντας την τεχνογνωσία της αγοράς να δημιουργήσουμε το Εθνικό Πρωτόκολλο επικοινωνίας που θα καλύπτει το μεγαλύτερο δυνατό αριθμό αναγκών.

η εξασφάλιση παρουσίας στα φορολογικά συστήματα κάθε συναλλαγής που έχει εκτελεστεί στα EFTPOS.

1. Το γενικό σχήμα

Η διασύνδεση αφορά τρία συστήματα: ERP, EFTPOS και ΠΑΡΟΧΟΥΣ ΥΠΗΡΕΣΙΩΝ ΠΛΗΡΩΜΩΝ (BANK):

Η συνήθης ροή επικοινωνίας ακολουθεί 5 βήματα:

- Το ERP ξεκινάει την συναλλαγή και επικοινωνεί είτε με τον ΥΠΑΗΕΣ είτε με τον ΦΗΜ, ΑΔΔΣΣ,κλπ και λαμβάνει είτε το Provider Signature είτε το ECR token με την μορφή της συναλλαγής Amount που προβλέπει η A1098.

Στην συνέχεια επικοινωνεί με το EFTPOS και ακολουθουν τα εξης βήματα :

- Η συναλλαγή ξεκινά από την ERP. Ο χειριστής επιλέγει πληρωμή με κάρτα και η ERP στέλνει σχετικό αίτημα στο EFTPOS.
- Το EFTPOS επιβεβαιώνει αμέσως στην ERP τη λήψη του αιτήματος θέτοντάς της σε αναμονή του τελικού αποτελέσματος.
- Το EFTPOS συνδέεται στον πάροχο υπηρεσιών πληρωμών για online έγκριση ή εγκρίνει offline ή απορρίπτει offline ή διακόπτει τη συναλλαγή.
- Το EFTPOS αποκρίνεται στην ERP με το τελικό αποτέλεσμα: απόρριψη ή έγκριση. Στην έγκριση αποστέλλει στοιχεία της συναλλαγής (όπως αριθμό συναλλαγής, κωδικό έγκρισης κλπ). Το τελικό αποτέλεσμα στέλνεται άμεσα στο ERP, πριν την έναρξη εκτύπωσης από το EFTPOS. Εφόσον το ERP το υποστηρίζει, στα στοιχεία της συναλλαγής περιλαμβάνονται και δεδομένα για εκτύπωση της απόδειξης του EFTPOS από την ERP
- Το ERP επιβεβαιώνει τη λήψη του τελικού αποτελέσματος. Αν αυτή η επιβεβαίωση δε φτάσει στο EFTPOS για οποιοδήποτε λόγο, το EFTPOS θέτει σήμανση στη συναλλαγή αυτή ότι δεν έχει πλήρως διεκπεραιωθεί ως προς την ERP.

1.2. Βασικές παραδοχές και περιορισμοί

1. Μόνο από την ERP μπορεί να ξεκινήσει νέα χρεωστική συναλλαγή (αγορά, αγορά με δόσεις, καταχώρηση προέγκρισης, mailorder). Το EFTPOS έχει κλειδωμένο πληκτρολόγιο και μενού για πραγματοποίηση χρεωστικών συναλλαγών.

2. Σε περίπτωση βλάβης θα πρέπει να προβλεφθεί διαδικασία διαχείρισης για την “autonomous operation”

3. Το EFTPOS εξυπηρετεί μόνο ένα ERP αίτημα κάθε φορά, δεν τηρεί ουρά αναμονής αιτημάτων και ούτε μπορεί καν να αποκριθεί σε νέο αίτημα όσο διαρκεί η επεξεργασία του τρέχοντος.

4. Η επικοινωνία δεν περιέχει σε καμία περίπτωση ευαίσθητα δεδομένα συναλλαγής, όπως ακάλυπτο αριθμό κάρτας, cvv2, track2 ή όνομα κατόχου της κάρτας.

1.3. Η φυσική σύνδεση

Στη σύνδεση μεταξύ των μερών το EFTPOS ενεργεί ως "server" σε σχέση με την ERP και ως "client" σε σχέση με τον πάροχο υπηρεσιών πληρωμών.

- Σύνδεση μέσω TCP/IP

Η σύνδεση μεταξύ EFTPOS και ERP μέσω TCP/IP γίνεται:

- Με απευθείας σύνδεση ERP-EFTPOS. Παραδείγματα: σύνδεση σε δίκτυο LAN με καλώδια Ethernet, σύνδεση WIFI κλπ.
- Μέσω συστήματος middleware για EFTPOS που δεν μπορούν να συνδεθούν με άλλο τρόπο.

Το LAN switch μπορεί να είναι εξωτερική συσκευή ή ενσωματωμένο.

Στην περίπτωση σύνδεσης μέσω middleware, επειδή η local IP του EFTPOS κατά κανόνα είναι άγνωστη ή μη προσβάσιμη από την ERP, απαιτείται κάποια επιπλέον υλοποίηση, όπου τη σύνδεση στο middleware θα την ανοίγει το EFTPOS με ένα "logon" και θα την κρατά ανοικτή όσο χρειάζεται, μπαίνοντας το ίδιο σε βρόχο αναμονής αιτημάτων ERP. Το middleware λειτουργεί ως απλός διαβιβαστής των μηνυμάτων.

- Σύνδεση μέσω USB, Bluetooth και RS232

Υποστηρίζεται η σύνδεση μέσω USB, Bluetooth χωρίς να αλλάζει καθόλου το πρωτόκολλο επικοινωνίας.

Υποστηρίζεται επίσης η σύνδεση μέσω RS232, με μοναδική αλλαγή στο πρωτόκολλο την προσθήκη μιας μικρής συμβολοσειράς ως προθέματος σε κάθε ανταλλασσόμενο μήνυμα.

1.4. Ροή και μηνύματα συνοπτικά

Χρησιμοποιώντας συμβολικά ονόματα, τα μηνύματα που ανταλλάσσονται μεταξύ ERP και EFTPOS είναι:

[AMOUNT]: Αίτημα έναρξης αγοράς (ERP->EFTPOS)

- [CONFIRMED]: Επιβεβαίωση λήψης αιτήματος (EFTPOS->ERP)
- [ERROR]: Αδυναμία εξυπηρέτησης αιτήματος (EFTPOS->ERP)
- [RESULT]: Αποτέλεσμα της συναλλαγής (EFTPOS->ERP)
- [ACK-RESULT]: Επιβεβαίωση λήψης του [RESULT] (ERP->EFTPOS)
- [RESEND-ONE]: Αίτημα εκ νέου αποστολής [RESULT] μίας συναλλαγής (ERP->EFTPOS)

[REGRECEIPT]: Αίτημα φόρτωσης απόδειξης ή τιμολογίου για μεταγενέστερη χρεωστική συναλλαγή (ERP->EFTPOS)

[RESEND-ALL]: Αίτημα αποστολής [RESULT] των εκκρεμών πιστωτικών συναλλαγών που εκτελέστηκαν αυτόνομα από EFTPOS χωρίς χρήση ERP, των εκτελεσμένων συναλλαγών που αφορούν σε προφορτωμένες αποδείξεις και τιμολόγια που έχουν ήδη εκδοθεί από την ERP, καθώς και των χρεωστικών συναλλαγών που εκτελέστηκαν από το EFTPOS μη συνδεδεμένο με την ERP, εξαιτίας της βλάβης της ERP ή εξαιτίας βλάβης της διασύνδεσης EFTPOS-ERP. (ERP ->EFTPOS)

Αλλες συναλλαγές:

[AMOUNT-INSTALM]: Αίτημα έναρξης αγοράς με χρήση δόσεων (ERP->EFTPOS)

[AMOUND-REFUND]: Αίτημα έναρξης επιστροφής (ERP->EFTPOS)

[AMOUNT-VOID]: Αίτημα έναρξης ακύρωσης (ERP->EFTPOS)

[AMOUNT-COMPLETION]: Αίτημα έναρξης καταχώρησης προέγκρισης(ERP->EFTPOS)

[AMOUNT-MAIL]: Αίτημα έναρξης συναλλαγής MAIL ORDER (ERP->EFTPOS)

Control Messages:

[ECHO]: Δοκιμή επικοινωνίας (ERP->EFTPOS->ERP)

[CONTROL]: Εντολή για διάφορες ρυθμίσεις (ERP->EFTPOS)

[SUCCESS]: Γενικό μήνυμα επιτυχίας (EFTPOS->ERP)

1.5. Συνήθης ροή αγοράς (ή λοιπών συναλλαγών)

[t0]	EFTPOS → [AMOUNT] → ERP Εκτός του ποσού αγοράς η ERP στέλνει και άλλες πληροφορίες, όπως αριθμό απόδειξης, αριθμό ταμειακής, κωδικό ταμία κλπ	
[t1]	EFTPOS → [CONFIRMED] → ERP	

	Το EFTPOS επιβεβαιώνει αμέσως τη λήψη, και η ERP μπαίνει σε αναμονή αποτελέσματος.	t1-t0 < 2 sec
	Το EFTPOS επεξεργάζεται το αίτημα, ζητά εισαγωγή κάρτας, συνδέεται για online έγκριση κλπ.	
[t2]	EFTPOS → [RESULT] → ERP Το EFTPOS απαντά με το αποτέλεσμα, που μπορεί να είναι απόρριψη ή έγκριση. Αν είναι έγκριση, αποστέλλει επιπλέον στοιχεία της συναλλαγής (π.χ. κωδικό έγκρισης, αρ. συναλλαγής κλπ)	Συνήθως t2-t1 < 60 sec
[t3]	EFTPOS → [ACK-RESULT] → ERP Η ERP επιβεβαιώνει τη λήψη του τελικού αποτελέσματος και το EFTPOS καταχωρεί (εφόσον βέβαια αφορούσε έγκριση) ότι η συναλλαγή έχει διεκπεραιωθεί πλήρως ως προς την ERP.	t3-t2 < 2 sec

Τα ανωτέρω τέσσερα μηνύματα ([AMOUNT], [CONFIRMED], [RESULT], [ACK- RESULT]) φέρουν έναν κοινό 6-ψήφιο κωδικό (session number), διαφορετικό για κάθε νέα συναλλαγή, τον οποίο δημιουργεί η ERP και χρησιμεύει ως στοιχείο ελέγχου της συνάφειας των μηνυμάτων και αποφυγής κρίσιμων λαθών.

Left Blank on purpose

1.6. Ροή προσωρινής καταχώρησης εκδοθείσας απόδειξης ή τιμολογίου από την ERP στο EFTPOS

[t0]	EFTPOS → [REGRECEIPT] → ERP Η ERP παρέχει πληροφορία για ΑΛΠ ή για τιμολόγιο που μόλις εξέδωσε, έτσι ώστε το EFTPOS να τη χρησιμοποιήσει σε ετεροχρονισμένη συναλλαγή (π.χ. σε παράδοση κατ' οίκον)	
[t1]	EFTPOS → [SUCCESS] → ERP Η ενέργεια αναμένεται πάντα επιτυχής (εκτός περιπτώσεων τεχνικού προβλήματος)	t1-t0 < 2 sec

1.7. Ροή σε περίπτωση αδυναμίας επεξεργασίας συναλλαγής

[t0]	EFTPOS → [AMOUNT] → ERP	
[t1]	EFTPOS → [ERROR] → ERP Το EFTPOS επιβεβαιώνει αμέσως τη λήψη, όμως με κωδικό λάθους, δηλώνοντας στην ERP ότι η επεξεργασία δεν είναι δυνατή.	t1-t0 < 2 sec

1.8. Στοιχειώδης ροή ηχούς

[t0]	EFTPOS → [ECHO] → ERP	
[t1]	EFTPOS → [ECHO] → ERP	t1-t0 < 2 sec

1.9. Ροή εκτέλεσης εντολής ρυθμίσεων

[t0]	EFTPOS → [CONTROL] → ERP Δίνεται η δυνατότητα ρύθμισης από την ERP ορισμένων παραμέτρων του EFTPOS που αφορούν τη διασύνδεση με την ERP.	
[t1]	EFTPOS →[SUCCESS ή ERROR]→ ERP	t1-t0 < 2 sec

1.10. Ροή επανάληψης [RESULT] τελευταίας συναλλαγής

[t0]	EFTPOS → [RESEND-ONE] → ERP Αν η συναλλαγή εγκρίθηκε στο EFTPOS αλλά λόγω προβλήματος σύνδεσης η ERP δε λαμβάνει την απάντηση [RESULT] ή το EFTPOS δε λαμβάνει την απάντηση [ACK-RESULT] ο χειριστής της ERP μπορεί να επιλέξει αυτή την ενέργεια ώστε να ολοκληρωθεί η συνήθης ροή.	
[t1]	EFTPOS → [RESULT] → ERP Το EFTPOS αναζητά στο πακέτο συναλλαγών την τελευταία συναλλαγή και εφόσον ταιριάζει με τα δεδομένα του αιτήματος αποστέλλει άμεσα τα στοιχεία της. Διαφορετικά επιστρέφει απόρριψη.	t1-t0 < 5 sec
[t2]	EFTPOS → [ACK-RESULT] → ERP Η ERP επιβεβαιώνει τη λήψη του τελικού αποτελέσματος και το EFTPOS καταχωρεί (εφόσον βέβαια αφορούσε έγκριση) ότι η συναλλαγή έχει διεκπεραιωθεί πλήρως ως προς την ERP.	t2-t1 < 2 sec

---

1.11. Ροή επανάληψης [RESULT] για όλες τις εκκρεμείς συναλλαγές

[t0]	EFTPOS [RESEND-ALL] ERP Αν το EFTPOS έχει αποθηκευμένες πιστωτικές συναλλαγές που εκτελέστηκαν αυτόνομα ή χρεωστικές συναλλαγές που ξεκίνησαν από το EFTPOS ως προφορτωμένες αποδείξεις (μέσω ροών REGRECEIPT) ή προφορτωμένα τιμολόγια της ERP , τότε το EFTPOS δεν επιτρέπει την επιλογή «ΑΠΟΣΤΟΛΗ ΠΑΚΕΤΟΥ», δηλαδή την εκκαθάριση των συναλλαγών από τον πάροχο υπηρεσιών πληρωμών και την πίστωση του εμπόρου. Σε αυτήν την περίπτωση ο χειριστής της ERP θα πρέπει να ζητήσει από το EFTPOS μέσω ειδικής εντολής τη λήψη των εκκρεμών αυτών συναλλαγών.	
[t1]	Το EFTPOS ξεκινά και στέλνει όσες συναλλαγές	t1-t0 < 5 sec

	• ήταν πιστωτικές κι εκτελέστηκαν αυτόνομα Στην περίπτωση αυτή επειδή δεν είχαν ERP *session-number*, αυτό στέλνεται ως POSTXN. • ήταν χρεωστικές κι εκτελέστηκαν με βάση προφορτωμένες αποδείξεις ή προφορτωμένα τιμολόγια. • EFTPOS [RESULT] ERP EFTPOS [ACK-RESULT] EFFTPOS [RESULT] ERP EFTPOS [ACK-RESULT] E . . . . EFTPOS [RESULT] ERP EFTPOS [ACK-RESULT] R Κατά το [RESEND-ALL] δε στέλνονται δεδομένα εκτύπωσης ακόμη κι αν αυτή υποστηρίζεται από την ERP. Το τελευταίο [RESULT] έχει μηδενικό ποσό, μηδενικό *session number* και είναι απόρριψη, σημαίνοντας τη λήξη της αποστολής.	
	•	

Left Blank on purpose

1.12. Ροή και μηνύματα αναλυτικά

Σύνταξη των μηνυμάτων

Κάθε μήνυμα αποτελείται από μια κεφαλίδα κι ένα κυρίως μέρος ως ακολούθως:

BYTES	ΠΕΡΙΓΡΑΦΗ	
0-1	MSG SIZE (2 bytes, binary)	Το μέγεθος του μηνύματος σε bytes που ακολουθεί: MSG SIZE: b0*256 + b1
2-4	DIRECTION INDICATOR (3 bytes, ascii)	Χαρακτηρίζει την πηγή του μηνύματος: ERP (από ERP προς EFTPOS) EFTPOS (από EFTPOS προς ERP)
5-6	PROTOCOL VARIANT (2 bytes, ascii)	Καθορίζει τη ροή και τη λειτουργία: 01: default λειτουργία ("variant 1") 02: η ERP αναλαμβάνει την εκτύπωση της απόδειξης του EFTPOS ("variant 2") 03 : Provider Signature 04 : ECRtoken
7-8	PROTOCOL VERSION (2 bytes, ASCII)	Καθορίζει τη σύνταξη στο σώμα του μηνύματος. Για το προτεινόμενο πρωτόκολλο η τιμή του είναι 10.
9-.	Κυρίως μέρος μηνύματος (MSG SIZE-7)	Όπως προδιαγράφεται στη συνέχεια.

ΕΙΔΙΚΕΣ ΠΕΡΙΠΤΩΣΕΙΣ

Στη σύνδεση μέσω RS232 θα χρησιμοποιείται ως πρόθεμα ολόκληρου του μηνύματος (δηλαδή πριν και από το πρόθεμα μήκους) η συμβολοσειρά "ERP" ή "POS" αντιστοίχως και ως κατάληξη (δηλαδή ως τελευταίο byte του κυρίως μέρους) ένα ψηφίο LRC για συμπληρωματικό έλεγχο ακεραιότητας του μηνύματος (βλ. 4.14).

Στη σύνδεση μέσω middleware θα χρησιμοποιείται ως πρόθεμα ολόκληρου του μηνύματος η συμβολοσειρά "ACQ<3-digits-acqId>TID<B-digits-POS-tid>", όπου ACQ θα είναι κάποιος καθορισμένος τριψήφιος κωδικός του φορέα εκκαθάρισης.

Το κυρίως μέρος του μηνύματος αποτελείται από ένα πρόθεμα κεφαλαίου λατινικού γράμματος που χαρακτηρίζει τον τύπο του, ακολουθούμενο από πεδία (fields) που κι αυτά κατά κανόνα έχουν ως πρόθεμα ένα κεφαλαίο γράμμα. Κάθε πεδίο μπορεί να υποδιαιρείται σε επιμέρους πεδία (subfields), που η σημασία τους καθορίζεται από τη θέση τους και μόνο.

Ως field separator χρησιμοποιείται το '/' και ως subfield separator το ':'. Ως escape χαρακτήρας ορίζεται ο '\', ωστόσο στην πράξη δεν προκύπτει ανάγκη για χρήση escape χαρακτήρα. Έτσι το κυρίως μέρος κάθε μηνύματος ακολουθεί την εξής σύνταξη:

MSG BODY **:= <*msg type*>/<*field*>{/<*field*>{/<*field*>}.}**

msg type **:= <*letter*>**

field **:= {<*letter*>}<*subfield*>{:<*subfield*>{:<*subfield*>}.}**

letter **:= A ❙ B ❙ C ❙ _ ❙ Z**

subfield **:= όπως προδιαγράφεται σε κάθε περίπτωση (τύπος δεδομένων, πλήθος bytes, σημασία)**

Για τους ορισμούς τύπων δεδομένων χρησιμοποιούνται οι ακόλουθες συντομογραφίες:

num - numeric, δεξιά στοίχιση και πλήρωση με 0

an - alphanumeric, δεν επιτρέποντα διαστήματα ούτε ειδικοί χαρακτήρες

anp - alphanumeric, επιτρέπονται διαστήματα

ans - alphanumeric, επιτρέπονται διαστήματα και ειδικοί χαρακτήρες

1.13. Μήνυμα [ECHO]

Στέλνεται από την ERP με επιλογή του χειριστή (συνήθως κατά την εγκατάσταση) για έλεγχο της σύνδεσης με το EFTPOS. Στην ηχώ response προστίθενται το terminal ID και το EFTPOS application version.

Σύνταξη:

ERP REQUEST:

X/<*text*>

EFTPOS RESPONSE:

X/<*text*>/Π<*tid*>:<*app-version*>

Στοιχείο	Τύπος	Μέγεθος	Περιγραφή
text	anp	1..200	Ελεύθερο κείμενο, το οποίο αναμένεται το ίδιο στην απάντηση
tid	an	1..8	Terminal ID
app-version	ans	1..10	EFTPOS application version

Ειδικότερα, επιτρέπεται να χρησιμοποιηθεί η ακόλουθη μορφή της εντολής ECHO, προκειμένου να ενημερωθεί το EFTPOS από το ERP (ΦΗΜΑΣ) για τον αριθμό μητρώου του ΦΗΜΑΣ, ώστε να μπορέσει το EFTPOS να υποβάλλει αίτηση στο ΠΣΦΗΜ Esend, για την λήψη του Master Key, όπως περιγράφεται στην παράγραφο 1.18 :

X/INIT:ECRNumber

1.14. Συναλλαγές και Πεδία

(ERP > EFTPOS) REQUEST

Στέλνεται από την ERP κατά την έναρξη μιας νέας αγοράς.

Σύνταξη:

ERP REQUEST:

<msg type>/S<session number>/F<amount>:<cur-code>:<cur-exp>

/D<datetime>/**R<ERP-id>/**H<operator-number>/T<receipt number>

/M<custom-data>{/Q<mac>}{<custom-data>}

Πεδίο <custom-data> συντίθεται από τα ακόλουθα πεδία :

{/V<Uid>:<Mark>:<NetAmount>:<VatAmount>:<TotalAmount>:}

{/W<isTaxfree>:<OnBehalfCollection>:<InitialTransaction>:<TipAmount>:<CashbackAmount>}

{/X<Signature-timestamp>:<ProviderSignature>:<providerid>}

{/Y<ECRtoken>}}

Notes :

(a) Εάν το πεδίο X είναι συμπληρωμένο έχουμε εγκατάσταση με Πάροχο ΥΠΑΗΕΣ και τότε στο πεδίο ERPid θα πρέπει να εχει "ERPE0000999».

(b) Στο πεδίο <providerid> θα πρέπει να έχει τον τριψηφιο κωδικό ΥΠΑΗΕΣ της ΑΑΔΕ για να μπορεί να χρησιμοποιηθεί για τον εντοπισμό του κλειδιού για το provider signature decode.

(c) /Q<mac> field, θα πρέπει να είναι άδειο σε περίπτωση που το protocol var 03 = providerSignature και στις περιπτώσεις var 04 = ECRtoken

(d) Στην περίπτωση που το πεδίο <ECRToken> είναι συμπληρωμένο τότε το, ERPid θα πρέπει να περιλαμβάνει το ECRid του ΦΗΜΑΣ αποτυπωμένο με την αντίστοιχη λογική της Α1098.

---------- (immediately)

(EFTPOS>ERP) RESPONSE (CONFIRMED)

Στέλνεται άμεσα από το EFTPOS ως απάντηση στο αρχικό αίτημα αγοράς της ERP, επιβεβαιώνοντας ότι η επεξεργασία του βρίσκεται σε εξέλιξη.

Σύνταξη:

EFTPOS RESPONSE:

<*msg type*>/S<session number>/F<amount>/R<ERP-id>/T<receipt-number>

--------- Response (II) After AUTH received from POS

(EFTPOS>ERP) RESPONSE (RESULT)

Στέλνεται από το EFTPOS ως τελική απάντηση στο αρχικό αίτημα αγοράς (ή άλλης συναλλαγής) της ERP σχετικά με την έκβαση της συναλλαγής.

Η απάντηση μπορεί να έρθει άμεσα (αν αφορά offline απόρριψη ή έγκριση), σε λίγα δευτερόλεπτα (τυπική περίπτωση online έγκρισης) ή ακόμη και περισσότερο από λεπτό αν καθυστερεί η online επικοινωνία ή η εισαγωγή PIN. Συνίσταται ρύθμιση timeout <150 sec στο ERP.

R/S<session number>/R<ERP-id>/T<receipt-number>{:<receipt-number>}

/M<custom-data>/C<rsp-code>{/D<trans-data>/S<acquirerSignature>

/X<ProviderSignature> or <ECRtoken>{/P<prndata>}

Το πεδίο **<trans-data>** επιστρέφεται μόνο εφόσον η συναλλαγή εγκρίθηκε, δηλ το <rsp-code> είναι 00.

Το πεδίο <trans-data> συντίθεται από τα ακόλουθα στοιχεία:

<trans-data> = <card-type>:<txn-type>:<cardpan-masked>:

<amount>:<amount-final>:<amount-tip>:

<amount-loy>:<amount-cb>:<bankId (Acqid)>:<terminalId>:

<batch-num>:<rrn>:<stan>:<authcode>:

<trans-datetime>:<txn-ERP-status>

<acquirerSignature> =<AcquirerID>:<RRN>:<approvalcode> **or**

=<acquirerID>:<batchNumber>:<sequenceNumber>:<approvalCode>

Το πεδίο <prn-data> επιστρέφεται εφόσον :

α) η συναλλαγή εγκρίθηκε

β) το protocol variant στην κεφαλίδα του μηνύματος [AMOUNT] ήταν 02

γ) το protocol variant στην κεφαλίδα του μηνύματος [RESULT] είναι επίσης 021. Έχει συνήθως μέγεθος 1-4 Kb και συντίθεται από τις σειρές προς εκτύπωση μαζί με καθορισμένους χαρακτήρες μορφοποίησης, όπως προδιαγράφεται στη συνέχεια.

--------- After RESPONSE (II)

(ERP>ERTPOS) (ACK-RESULT)

Στέλνεται από την ERP ως επιβεβαίωση λήψης του [RESULT]. Σύνταξη:

ERP RESPONSE:

R/S<session number>/R<ERP-id>/F<amount>/T<receipt-number>{:<receipt-number>}

1.15. Special Messages

--------- SUCCESS

Αποτελεί ειδική περίπτωση μηνύματος [ERROR] με κωδικό 000.

Σύνταξη:

EFTPOS RESPONSE:

E/000

1.16. Μηνύματα Control

Resend ONE

Στέλνεται από την ECR μετά από επιλογή του χειριστή, στην περίπτωση που το EFTPOS ενέκρινε τη συναλλαγή αλλά απέτυχε η αποστολή του [RESULT].

Σύνταξη:

ECR REQUEST:

O/S<*session number*>/F<*amount*>:<*cur-code*>:<*cur-exp*>
/R<*ecr-id*>/T<*receipt-number*>{/Q<*mac*>}

Στοιχείο	Τύπος	Μέγεθος	Περιγραφή
session number	an	6	Πρέπει να ταιριάζουν με αυτά της συναλλαγής που εγκρίθηκε στο EFTPOS.
amount	num	1..12	
cur-code	num	3	
cur-expo	num	1	
ecr-id	an	11	
receipt-number	an	1..8	
mac	an	8	**Σε όλες τις περιπτώσεις μένει κενό, εφόσον το protocol var=03 or var=04**

Resend ALL

Στέλνεται από το ERP μετά από επιλογή του χειριστή, στην περίπτωση που το EFTPOS **μπορεί να κλείσει πακέτο** αρκεί να κρατήσει σε εκκρεμότητά τις εν λόγω συναλλαγές για αποστολή προς το ERP.

Σύνταξη:

ECR REQUEST:

L/*R<erp-id>*/D<*datetime*>{/*Q<mac>*}

Σημείωση :

(a) Κατά το [RESEND-ALL] δε στέλνονται δεδομένα εκτύπωσης ακόμη κι αν αυτή υποστηρίζεται από το ERP.
(b) Το τελευταίο [RESULT] έχει μηδενικό ποσό, μηδενικό session number και είναι απόρριψη, σημαίνοντας τη λήξη της αποστολής.
(c) Εάν έχουμε εγκατάσταση με Πάροχο ΥΠΑΗΕΣ και τότε στο πεδίο <erp-id> θα πρέπει να εχει "ERP00000999».
(d) /Q<mac> field, θα πρέπει να είναι άδειο σε περίπτωση που το protocol var 03 = providerSignature
(e) Στην περίπτωση που στην αρχική συναλλαγή το πεδίο <ECRToken> είναι συμπληρωμένο τότε το, ERPid θα πρέπει να περιλαμβάνει το ECRid του ΦΗΜΑΣ αποτυπωμένο με την αντίστοιχη λογική της A1098.

Element name	Type	Size	Description
ecr-id	an	11	Το EFTPOS πρέπει να παρακάμπτει συναλλαγές που έχουν ληφθεί από διαφορετική ECR.
datetime	num	14	(Βλ. [AMOUNT])
mac	an	8	**Σε όλες τις περιπτώσεις μένει κενό, εφόσον το protocol var=03 or var=04**

1.17. Format Πεδίων

REQUEST FIELDS

<msg type>

A: Amount - SALE I : Amount – InstalM. Z: Amount REFUND W:REGRECEIPT

M: Amount – MOTO

V: Amount – VOID P: Amount – Completion (Pre-Auth Completion)

Στοιχείο	Τύπος	Μέγεθος	Περιγραφή
session number	an	6	Διαφορετικός για κάθε νέα αγορά 6- ψήφιος αριθμός. Μπορεί να είναι ακολουθιακός, ψευδοτυχαίος ή βάσει άλλης σύμβασης. Το EFTPOS πρέπει να ελέγχει πως κάθε νέο αίτημα έρχεται με διαφορετικό session number από το προηγούμενο.
amount	num	1..12	Το ποσό της συναλλαγής
cur-code	num	3	Ο ISO 4217 κωδικός νομίσματος (978 για €)
cur-exp	num	1	Τα δεκαδικά του νομίσματος (2 για €)
datetime	num	14	Τρέχουσα ημ/νία και ώρα σε μορφή YYYYMMDDhhmmss
ERP-id	an	11	Αριθμός μητρώου ERP
operator-number	an	1..8	Κωδικός ταμία
receipt-number	an	1..8	Προοδευτικός αριθμός απόδειξης ERP
custom-data	ans	1..100	Δεδομένα που καθορίζονται ανά περίπτωση και τύπο ταμειακής. Αν δε χρησιμοποιείται αρκεί να στέλνεται ένας χαρακτήρας του
			μηδενός ("M0"). Σε συναλλαγές πληρωμής λογαριασμού τα custom-data περιλαμβάνουν ειδικό 12-ψήφιο κωδικό πληρωμής.
mac	an	8	Κενό, στην περίπτωση protocol var 03 = Provider Signature var 04 = ERPtoken

Στοιχείο	Τύπος	Μέγεθος	Περιγραφή
Uid	an	40	Uid αναγνωριστικο παραστατικού (UID of invoice) όπως ορίζεται από την παρ 6 του αρθρου 5 της Α1138/2020. (*) Να επιβεβαιωθουν τα στοιχεία τύπος και μηκος πεδίου από τα ERP
MAPK	num	1..15	Μοναδικος αριθμος παραστατικου σε περίπτωση ετεροχρονισμένης συναλλαγης (*) Να επιβεβαιωθουν τα στοιχεία τύπος και μηκος πεδίου από τα ERP
NetAmount	num	1….12	Καθαρο ποσό (Σημειωση = α) δεν είναι το πληρωτέο ποσό) b) είναι στο ίδοο currency με του πεδίου /F<amount> c) έχει τα ίδια δεκαδικά με το πεδίο /F<amount>
VatAmount	num	1….12	Απόλυτο Ποσό ΦΠΑ, όχι ποσοστό (Σημειωση = α) δεν είναι το πληρωτέο ποσό) b) είναι στο ίδοο currency με του πεδίου /F<amount> c) έχει τα ίδια δεκαδικά με το πεδίο /F<amount>
TotalAmount	num	1….12	Συνολικό Ποσό Παραστατικου (Σημειωση = α) δεν είναι το πληρωτέο ποσό) b) είναι στο ίδοο currency με του πεδίου /F<amount> c) έχει τα ίδια δεκαδικά με το πεδίο /F<amount>

/W			
isTAXfree	num	1	0 = default, δεν είναι Taxfree συναλλαγή, πρέπει να υπάρχει ERPToken ή Providr Signature 1= Taxfree συναλλαγή μπορεί και να μην υπάρχει provider signature ή ERPToken
OnBehlafCollection	num	14	VAT number , αφορα συναλλαγες για είσπραξη τρίτων (π.χ Bill payment…klp)
InitialTransactrion	num	0…12	AcquirerSignature, με βαση τα όσα περιγράφονται στην απόφαση Α1155
TipAmount	num	1…12	Ποσό TIP (Σημειωση = α) δεν είναι το πληρωτέο ποσό) b) είναι στο ίδιο currency με του πεδίου /F<amount> c) έχει τα ίδια δεκαδικά με το πεδίο /F<amount>
CashbackAmount	num	1…12	Ποσό Cashback (Σημειωση = α) δεν είναι το πληρωτέο ποσό) b) είναι στο ίδοο currency με του πεδίου /F<amount> c) έχει τα ίδια δεκαδικά με το πεδίο /F<amount>

/X			

SignatureTmestamp	num	14	Τρέχουσα ημ/νία και ώρα σε μορφή YYYYMMDDhhmmss
Providerid	num	3	ProviderID

/Y			
ECRToken	Alphanumeric	TB	Ολόκληρο το μηνυμα της συναλλαγης Amount με βαση τον ορισμό της A1098/2023

Message – CONFIRM / FIELDS

Στοιχείο	Τύπος	Μέγεθος	Περιγραφή
session number	an	6	Πρέπει να είναι τα ίδια με αυτό του [AMOUNT] και αυτό να ελέγχεται από την ERP.
amount	num	1..12	
ERP-id	an	11	
receipt-number	an	1..8	

Message – RESULTS / FIELDS

Στοιχείο	Τύπος	Μέγεθος	Περιγραφή
session number	an	6	Πρέπει να είναι τα ίδια με αυτά του [CONFIRMED] και αυτό να ελέγχεται από την ERP εκτός κι αν πρόκειται για την ακόλουθη εξαίρεση όπου τέτοιος έλεγχος δεν μπορεί να γίνει ή δεν είναι βέβαιο ότι θα πετύχει. Εξαίρεση: σε περίπτωση που το μήνυμα [RESULT] έρχεται ως απάντηση σε μήνυμα [RESEND-ALL], το *session number* μπορεί να έχει την ειδική τιμή "POSTXN", που σημαίνει ότι η συναλλαγή ξεκίνησε από το EFTPOS. Σε αυτή την περίπτωση τα στοιχεία: • *ERP-id* και *receipt-number* θα έχουν μηδενική τιμή αν η συναλλαγή πραγματοποιήθηκε μόνο στο EFTPOS. • *ERP-id* και *receipt-number* θα έχουν μη μηδενική τιμή αν η συναλλαγή αντιστοιχεί σε προφορτωμένη απόδειξη ή τιμολόγιο που έχουν εκδοθεί από τον ΦΗΜ.
ERP-id	an	11	
receipt-number *(προοδευτικός αριθμός σήμανσης στις ΦΤΜ,ΑΔΗΜΕ,ΕΑ ΦΔΣΣ/ΦΗΜΑΣ)*	an	1..8	
rsp-code	num	2	EFTPOS κωδικός έκβασης της συναλλαγής:

			00: επιτυχία, συναλλαγή εγκρίθηκε 33: γενικός κωδικός απόρριψης Σε ορισμένες υλοποιήσεις ο κωδικός έκβασης προσδιορίζει καλύτερα το λόγο της απόρριψης ως εξής: 03: user cancellation or timeout 04: declined by the terminal 05: declined by the host 06: communication problem 09: bank's host unreachable 66: system error in EFTPOS
card-type	an	1..20	Ο τύπος της κάρτας (Visa, Mastercard κλπ)
txn-type	num	2	Τύπος συναλλαγής: 00: αγορά 01: ακύρωση 02: επιστροφή 03: καταχώρηση προέγκρισης 04: mail order 05: αγορά με δόσεις
card-pan-masked	ans	14..19	Ο αριθμός της κάρτας με καλυμμένα τα ενδιάμεσα ψηφία.
amount	num	1..12	Το ποσό της συναλλαγής. Πρέπει να είναι το ίδιο με αυτό του [CONFIRMED] και αυτό να ελέγχεται από την ERP. Το πεδίο έχει πρόσημο συν αν πρόκειται για πληρωμή με κάρτα, ενώ έχει το πρόσημο μείον αν πρόκειται για επιστροφή σε κάρτα.

amount-final	num	1..12	Μπορεί να διαφέρει από το *amount* σε περίπτωση loyalty με εξαργύρωση ή προσθήκης φιλοδωρήματος. Το πεδίο έχει πρόσημο συν αν πρόκειται για πληρωμή με κάρτα, ενώ έχει το πρόσημο μείον αν πρόκειται για επιστροφή σε κάρτα.
amount-tip	num	1..12	Ποσό φιλοδωρήματος
amount-loy	num	1..12	Ποσό εξαργύρωσης loyalty

amount-cb	num	1..12	Ποσό cashback
*bankId (*Acqid)	num	1..3	Κωδικός του παρόχου υπηρεσιών πληρωμών ή της τελικής τράπεζας εκκαθάρισης. Χρήσιμο σε διαμορφώσεις με περισσότερες τράπεζες εγκρίσεων (multiacquiring)
terminalId	an	1..8	Το terminal Id.
batch-num	num	1..6	Ο αριθμός πακέτου στο EFTPOS
rrn	num	0..12	Το rrn της συναλλαγής Σε κάποιες υλοποιήσεις μπορεί να είναι κενό στην περίπτωση offline σ/γών.
stan	num	1..6	Ο αριθμός συναλλαγής στο EFTPOS
authcode	an	6..8	Ο κωδικός έγκρισης
trans-datetime	num		Ημ/νία και ώρα έγκρισης σε μορφή YYYYMMDDhhmmss

txn-ERP-status	num	1	Χαρακτηρίζει τη συναλλαγή ως προς την επικοινωνία με την ERP • 0 - έναρξη από ERP - επιτυχία • 1 - έναρξη από ERP - αποτυχία στην ολοκλήρωση (αρχικό RESULT) • 2 – έναρξη στο EFTPOS με χρήση στοιχείων προφορτωμένης ΑΛΠ/ΑΠΥ/ τιμολογίου • 3 - έναρξη στο EFTPOS με στοιχεία ΑΛΠ/ΑΠΥ/τιμολογίου τα οποία έχουν εντοπιστεί σε προγενέστερη εγγραφή του EFTPOS. • 4 – έναρξη από EFTPOS χωρίς εισαγωγή στοιχείων ΑΛΠ/ΑΠΥ/τιμολογίου (αντιστοιχεί σε βλάβη της ERP). • 5 – Αδυναμία επικοινωνίας ECR-EFTPOS λόγω βλάβης των επιμέρους συστημάτων διασύνδεσης (βλάβη υποδομής).
prn-data	ans	0..4Kb	Συντίθεται από σειρές προς εκτύπωση και χαρακτήρες ελέγχου για ειδική μορφοποίηση ως ακολούθως: • 0x0A - αλλαγή γραμμής • 0x1B 0x01 - εκτύπωση βασικού

			λογότυπου • 0x1B 0x02 - εκτύπωση 2ου λογότυπου (π.χ. loyalty) • 0x1B 0x03 - εκτύπωση εικονιδίου c- less • 0x1B 0x04 ως 0x1B 0x06 δεσμευμένα για χρήση εικονιδίων • 0x1B 0x07 ως 0x1B 0x09 δεσμευμένα για χρήση BAR/QR codes • 0x1B 0x0C - παύση για εκτύπωση αντιγράφου πελάτη • 0x1B 0x43 - στοίχιση κέντρο • 0x1B 0x52 - στοίχιση δεξιά • 0x1B 0x4C ('L') - στοίχιση αριστερά (default μετά από νέα γραμμή) • 0x1B 0x4E ('N') - χρήση χαρακτήρων κανονικού μεγέθους (default) • 0x1B 0x42 ('B')- χρήση bold χαρακτήρων • 0x1B 0x53 ('S') - χρήση χαρακτήρων μικρού μεγέθους. Ελληνικοί χαρακτήρες στέλνονται σε ISO- 8859-7. Κυριλλικοί σε ISO-8859-5.

AcquirerSignature	num	14	

Message – ACK-RESULT / FIELDS

Στοιχείο	Τύπος	Μέγεθος	Περιγραφή
session number	an	6	Πρέπει να είναι τα ίδια με αυτά του [RESULT] και αυτό να ελέγχεται από το EFTPOS. Εξαίρεση: (βλ. μήνυμα [RESULT])
ERP-id	an	11	
amount	num	1..12	
receipt-number	an	1..8	

Message – ERROR/ FIELDS

Στοιχείο	Τύπος	Μέγεθος	Περιγραφή
error code	num	3	001: "protocol not supported" 002: "duplicate request received" 003: "Syntax error in request" 004: "Invalid currency" 100: "Internal EFTPOS error" 500: "Invalid command" 501: "Wrong parameter" 502: "Missing MAC"
			503: "MAC error" 504: "MAC not supported" 505: "Provider id error" 506: "Provider not Supported" 777: "EFTPOS not connected" 999: "BUSY"

Επεξηγήσεις ανά κωδικό:

---

1. Κωδικός 001: μη υποστηριζόμενο πρωτόκολλο. Ωστόσο η απάντηση του EFTPOS χρησιμοποιεί στην κεφαλίδα τα ίδια version και variant του αιτήματος της ERP.

2. Κωδικός 002: το session number είναι το ίδιο με αυτό της προηγούμενης σ/γής.

3. Κωδικός 003: συντακτικό λάθος στο σώμα του μηνύματος.

4. Κωδικός 004: η ταμειακή στέλνει ποσό σε διαφορετικό νόμισμα από αυτό του EFTPOS.

5. Κωδικός 100: εσωτερικό πρόβλημα του EFTPOS.

6. Κωδικός 500/501: στέλνεται στην περίπτωση μη έγκυρου [CONTROL] μηνύματος.

7. Κωδικός 502: στο αίτημα ERP λείπει MAC πεδίο ενώ είναι υποχρεωτικό

8. Κωδικός 503: το αίτημα ERP έχει λάθος MAC

9. Κωδικός 504: το EFTPOS δεν μπορεί να υποστηρίξει MAC (π.χ. λείπουν κλειδιά)

10. Κωδικός 503: το αίτημα ERP έχει λάθος providerID

11. Κωδικός 504: το EFTPOS δεν μπορεί να υποστήριξη το Provider Signature (π.χ. λείπουν κλειδιά)

12. Κωδικός 777: μη συνδεδεμένο EFTPOS (δεσμευμένος κωδικός για middleware)

13. Κωδικός 999: το EFTPOS είναι κατειλημμένο (π.χ. εκτελούνται χειρισμοί από το μενού, επικοινωνεί για παραμέτρους κλπ).

1.18. ΈΚΔΟΣΗ ΚΑΙ ΔΙΑΘΕΣΗ ΑΡΧΙΚΟΥ ΚΛΕΙΔΙΟΥ (MASTER KEY-MK) (reference A1098) (ECRtoken)

Για την αποφυγή της δημοσιοποίησης των κλειδιών κατά την σύζευξη της ECR και του EFTPOS και με σκοπό την αποτροπή οποιασδήποτε ενέργειας παράκαμψης της αρχικής σύνδεσης, η έκδοση και η εγκατάσταση του αρχικού κλειδιού (master key-MK) γίνεται μέσω ανεξάρτητων κλήσεων των ECR και EFTPOS στο ΠΣΦΗΜ Esend, που λειτουργεί και συντηρείται στις υποδομές της ΑΑΔΕ.

Οι κλήσεις εκτελούνται με πεδία αρχικοποίησης για την ECR: τον αριθμό μητρώου ECR και το ΑΦΜ της επιχείρησης, ενώ για το EFTPOS: το TID του EFTPOS, το

ΑΦΜ της επιχείρησης, το διακριτικό όνομα του κατασκευαστή EFTPOS και το αντίστοιχο APIKEY.

Η διαδικασία δημιουργίας του αρχικού κλειδιού(master key-MK) εκκινεί από την ECR έτσι ώστε μετά τη δημιουργία και επιστροφή στην ECR του αρχικού κλειδιού από το ΠΣΦΗΜ Esend, αυτό να είναι διαθέσιμο για την λήψη του και από το EFTPOS.

Security

- Το url επικοινωνίας των EFTPOS με το ΠΣΦΗΜ Esend για την λήψη του MK είναι το : https://www1.aade.gr/tameiakes/mysec/eftposmk.php

- Για την επικοινωνία των ΦΗΜ με το ΠΣΦΗΜ Esend χρησιμοποιείται η διαδικασία κρυπτογράφησης μέσω AES-256 που καθορίζεται στην Απόφαση Διοικητή ΑΑΔΕ ΠΟΛ 1166/2018. Το url επικοινωνίας των ΦΗΜ με το ΠΣΦΗΜ Esend για την λήψη του MK είναι το : http://tam.gsis.gr/eafdss/ myweb/fhmmk.php

Standard API Description (EFTPOS <--> Esend)

Production endpoint: https://www1.aade.gr/tameiakes/mysec/eftposmk.php

Μορφή ανταλλαγής δεδομένων: JSON HTTP method: POST

Πεδία πακέτου αποστολής

Field	Size	Description
TID	≤10 chars	Terminal Identification Number (EFTPOS)
ECRID	11 chars	Fiscal device number from ECR ECHO call
TAX ID	9 chars	ΑΦΜ επιχείρησης
MAN	<=20 chars	Διακριτικό όνομα κατασκευαστή EFTPOS
APIKEY	<= 64 chars	APIKEY

Μορφοποίηση πεδίων:

{"TID": "99009999", "ECRID": "XXX99000000", "TAXID": "01345678",

"MAN": "eftpos-hellas", "APIKEY":
"012345678901234567890123456789QWERTYUIOPASDFGHJKLZ12345678 901234" }

Το πεδίο MAN, καθορίζεται από τον ενδιαφερόμενο κατασκευαστή EFTPOS που το κοινοποιεί στην αρμόδια υπηρεσία του ΠΣΦΗΜ Esend με αίτηση μέσω email, ενώ το πεδίο APIKEY καθορίζεται από την αρμόδια υπηρεσία του ΠΣΦΗΜ Esend που το κοινοποιεί στον ενδιαφερόμενο κατασκευαστή EFTPOS μέσω email.

Πεδία απάντησης

Field	Size	Description
Status	3 chars	Replied status code
Description	<= 25 chars	Status description
TID	≤10 chars	Terminal Identification Number (EFTPOS)
MACKEY	32 chars	master key-MK

Μορφοποίηση πεδίων:

{

"Status": "000", "Description": "SUCCESS", "TID": "990099",

"MACKEY": "30001234C330001234C330001234C322"

}

Standard API Description (ΦΗΜ <--> Esend)

Production endpoint: http://tam.gsis.gr/eafdss/myweb/fhmmk.php

---

Μορφή ανταλλαγής δεδομένων: ENCRYPTED RAW (AES KEY encryption method). HTTP method: POST

Πεδία πακέτου αποστολής

Field	Size	Description
ECRID	11 chars	Αριθμός Μητρώου ΦΗΜ
TID	≤10 chars	Terminal Identification Number (EFTPOS)
TAX ID	9 chars	ΑΦΜ επιχείρησης

Μορφοποίηση πεδίων (αν δεν ήταν κρυπτογραφημένα) : "XXX99000000;990099;01345678"

Πεδία απάντησης

Field	Size	Description
Status	3 chars	Replied status code
Description	<= 25 chars	Status description
TID	≤10 chars	Terminal Identification Number (EFTPOS)
MACKEY	32 chars	master key-MK

Μορφοποίηση πεδίων (αν δεν ήταν κρυπτογραφημένα):
"000;SUCCESS;XXX99000000;30001234C330001234C330001234C322"

Response Status codes

Status	Description
000	SUCCESS
101	Check the contents of the fields
102	Format error
103	Unregistered Fiscal Device
104	Busy-Retry
105	Unspecified error

Ειδικότερα, για την λήψη του Master Key (MK , MACKEY) ισχύουν οι ακόλουθοι κανόνες κρυπτογράφησης:

Ερώτημα από ΦΗΜ:

1) ECRID

2) TID-encrypted-HEX_representation

3) TAXID ΑΦΜ-encrypted-HEX_representation(με το ίδιο IV)

4) IV (Initialization vector του ΦΗΜ)-HEX_representation Το encryption γίνεται με το AESKEY του κατασκευαστή.

Όλα τα πεδία είναι συνεχόμενα, με διαχωριστή delimiter (;), plain/text POST.

Απάντηση από Esend:

1) Status

2) Description

3) TID-encrypted-HEX_representation

4) MACKEY-encrypted-HEX_representation(με το ίδιο IV)

5) IV (Initialization vector του server)-HEX_representation Το decryption γίνεται με το AESKEY του κατασκευαστή.

Όλα τα πεδία είναι συνεχόμενα, με διαχωριστή delimiter (;).

1.19. ΛΗΨΗ ΤΟΥ AESKEY ΑΠΟ ΤΟ ΠΣΦΗΜ ΓΙΑ ΤΟΥΣ ΦΗΜ.(reference A1098) (ECRtoken)

Ταυτόχρονα με την απόφαση έγκρισης ΦΗΜ, κοινοποιείται στην κατασκευάστρια επιχείρηση ΦΗΜ, το «βασικό AESKEY» της κατασκευάστριας επιχείρησης για τους ΦΗΜ της συγκεκριμένης έγκρισης. Μετά την υποβολή της δήλωσης έναρξης Δ13, ο ΦΗΜ μπορεί να επικοινωνήσει με ειδικό url του ΠΣΦΗΜ Esend, χρησιμοποιώντας ως AESKEY το βασικό AESKEY του κατασκευαστή. Το ΠΣΦΗΜ

Esend, επιστρέφει στον ΦΗΜ κρυπτογραφημένο, το AESKEY του ΦΗΜ που θα χρησιμοποιείται για τις κρυπτογραφήσεις των διαβιβάσεων δεδομένων συναλλαγών.

Standard API Description (ΦΗΜ <--> Esend)

Production endpoint: http://tam.gsis.gr/eafdss/myweb/aeskey.php

Μορφή ανταλλαγής δεδομένων: ENCRYPTED RAW (AES KEY encryption method). HTTP method: POST

Πεδία πακέτου αποστολής

Field	Size	Description
ECRID	11 chars	Αριθμός Μητρώου ΦΗΜ
TAX ID	9 chars	ΑΦΜ επιχείρησης - κατόχου

Μορφοποίηση πεδίων (αν δεν ήταν κρυπτογραφημένα): "XXX99000000;01345678"

Πεδία απάντησης

Field	Size	Description
Status	3 chars	Replied status code
Description	25 chars	Status description
ECRID	11 chars	Αριθμός Μητρώου ΦΗΜ
AESKEY	40 chars	AESKEY

Μορφοποίηση πεδίων (αν δεν ήταν κρυπτογραφημένα):

"000;SUCCESS;XXX99000000;30001234C330001234C330001234C3223456 789F"

Response Status codes

Status	Description
000	SUCCESS
101	Check the contents of the fields
102	Format error
103	Unregistered Fiscal Device
104	Busy-Retry
105	Unspecified error

Ειδικότερα, κατά την λήψη του AESKEY για τους ΦΗΜ από το Esend, ισχύουν οι ακόλουθοι κανόνες κρυπτογράφησης:

Ερώτημα από ΦΗΜ:

1) ECRID

2) TAXID ΑΦΜ-encrypted-HEX_representation

3) IV (Initialization vector του ΦΗΜ)-HEX_representation Το encryption γίνεται με το AESKEY του κατασκευαστή.

Όλα τα πεδία είναι συνεχόμενα, με διαχωριστή delimiter (;), plain/text POST.

Απάντηση από ESEND:

1) Status

2) Description

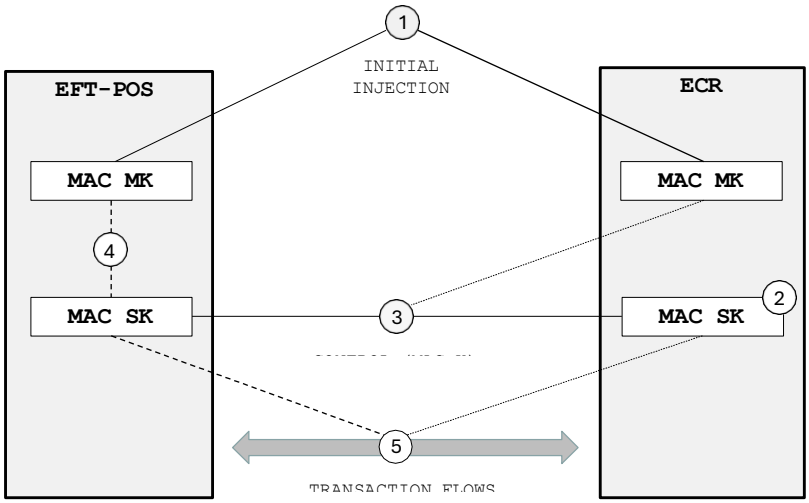
3) ECRID-encrypted-HEX_representation

4) AESKEY-encrypted-HEX_representation(με το ίδιο IV)

5) IV (Initialization vector του server)-HEX_representation Το decryption γίνεται με το AESKEY του κατασκευαστή. Όλα τα πεδία είναι συνεχόμενα, με διαχωριστή delimiter (;).

1.20. ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΜΗΧΑΝΙΣΜΟΥ MAC (Reference A1098) (ECRtoken)

Ο σχετικός μηχανισμός του MAC (message authentication checksum) από πλευράς υλοποίησης για την επικοινωνία των δύο μερών συνοψίζεται στην Εικόνα 8.



Εικόνα 8

1) Στο αρχικό στάδιο προετοιμασίας συμφωνείται μεταξύ των παρόχων EFTPOS και ECR η εμφύτευση σε αμφότερες τις συσκευές ενός κοινού αρχικού κλειδιού (master key - MK), με διαδικασίες και πρακτικές που θα το προστατεύουν από το να διαρρεύσει.

Η διαδικασία περιγράφεται στο κεφάλαιο «Έκδοση και διάθεση αρχικού κλειδιού (master key-MK)»

2) Η ECR παράγει ένα ψευδοτυχαίο session κλειδί (SK) για χρήση.

3) Μέσω ροής ελέγχου ([CONTROL] μήνυμα), η ECR στέλνει στο EFTPOS το SK κρυπτογραφημένο υπό το MK με T-DES

4) Το EFTPOS αποκρυπτογραφεί το SK υπό το MK και το αποθηκεύει για χρήση.

5) Κατά τις ροές των συναλλαγών είναι το SK που χρησιμοποιείται για έλεγχο εγκυρότητας του αποστολέα των αιτημάτων.

Το SK μπορεί να ανανεώνεται τακτικά με χρήση [CONTROL] μηνύματος από την ECR.

Το MK μπορεί να ανανεώνεται σε πιο αραιά χρονικά διαστήματα, με διαδικασίες και μηχανισμούς που θα συμφωνούν από κοινού οι πάροχοι των EFTPOS και των ECR.

Προτείνεται η χρήση T-DES MAC αλγορίθμου (του συνήθους mode CBC 1) με double length κλειδί (16 bytes).

Παράδειγμα κρυπτογράφησης session κλειδιού και υπολογισμού MAC

Test MK (plain): ABCDEF0123456789987654321OABCDEF
(KCV: 48934A) Test SK (plain):
12340000ABCD111122223333FFFFDDDD (KCV: CC5FFF) Test
SK (encr): 1ED9F7AE0B2509281BBC2DE38EF2A12B

Message:

A/S000922/F2000:978:2/D20220513150958/RABC00111222/H121/T000922/M00000000

Στοιχείο mac: /Q4540A254

Ο υπολογισμός του MAC του παραπάνω παραδείγματος γίνεται ως εξής:

INPUT AFTER PADDING (length=80):
41 2F 53 30 30 30 39 32 32 2F 46 32 30 30 30 3A |A/S000922/F2000:
39 37 38 3A 32 2F 44 32 30 32 32 30 35 31 33 31 |978:2/D202205131
35 30 39 35 38 2F 52 41 42 43 30 30 31 31 31 32 |50958/RABC001112
32 32 2F 48 31 32 31 2F 54 30 30 30 39 32 32 2F |22/H121/T000922/
4D 30 30 30 30 30 30 30 30 00 00 00 00 00 00 00 |M00000000.....
Number of blocks: 10

Block 0:		Block 5:	
P:		P:	
41 2F 53 30 30 30 39 32	|A/S00092	42 43 30 30 31 31 31 32	|BC001112
H:		H:	
00 00 00 00 00 00 00 00	|.....	E2 D8 E8 13 0F 40 1A F0	|.....@..
P(xor)H:		P(xor)H:	
41 2F 53 30 30 30 39 32	|A/S00092	A0 9B D8 23 3E 71 2B C2	|...#>q+.
TDES of P(xor)H:		TDES of P(xor)H:	
00 41 06 32 34 81 FB 65	|.A.24..e	1C 84 7B 3C E8 0D 33 41	|..{<..3A
Block 1:		Block 6:	
P:		P:	
32 2F 46 32 30 30 30 3A	|2/F2000:	32 32 2F 48 31 32 31 2F	|22/H121/
H:		H:	
00 41 06 32 34 81 FB 65	|.A.24..e	1C 84 7B 3C E8 0D 33 41	|..{<..3A
P(xor)H:		P(xor)H:	
32 6E 40 00 04 B1 CB 5F	|2n@...._	2E B6 54 74 D9 3F 02 6E	|..Tt.?.n
TDES of P(xor)H:		TDES of P(xor)H:	
EB 92 A8 CD 45 24 2A 10	| ... E$*.	15 9E 89 04 3F B1 CA 40	| ... ?..@
Block 2:		Block 7:	
P:		P:	

39 37 38 3A 32 2F 44 32	|978:2/D2	54 30 30 30 39 32 32 2F	|T000922/
H:		H:	
EB 92 A8 CD 45 24 2A 10	| ...E$*.	15 9E 89 04 3F B1 CA 40	| ...?..@
P(xor)H:		P(xor)H:	
D2 A5 90 F7 77 0B 6E 22	|....w.n"	41 AE B9 34 06 83 F8 6F	|A..4...o
TDES of P(xor)H:		TDES of P(xor)H:	
CE 85 08 94 25 AE 32 5E	|....%.2^	19 48 5D 23 E9 36 DD 38	|.H]#.6.8
Block 3:		Block 8:	
P:		P:	
30 32 32 30 35 31 33 31	|02205131	4D 30 30 30 30 30 30 30	|M0000000
H:		H:	
CE 85 08 94 25 AE 32 5E	|....%.2^	19 48 5D 23 E9 36 DD 38	|.H]#.6.8
P(xor)H:		P(xor)H:	
FE B7 3A A4 10 9F 01 6F	|.......o	54 78 6D 13 D9 06 ED 08	|Txm.....
TDES of P(xor)H:		TDES of P(xor)H:	
D5 E9 95 DF DA 5F DF 69	|....._.i	93 56 0E CE A7 E2 CA 8A	|.V.....
Block 4:		Block 9:	
P:		P:	
35 30 39 35 38 2F 52 41	|50958/RA	30 00 00 00 00 00 00 00	|0.....
H:		H:	
D5 E9 95 DF DA 5F DF 69	|....._.i	93 56 0E CE A7 E2 CA 8A	|.V.....
P(xor)H:		P(xor)H:	
E0 D9 AC EA E2 70 8D 28	|.....p.(	A3 56 0E CE A7 E2 CA 8A	|.V.....
TDES of P(xor)H:		TDES of P(xor)H:	
E2 D8 E8 13 0F 40 1A F0	| ....@..	45 40 A2 54 7C FB A2 3A	|E@.T|..:
		Result: [4540A2547CFBA23A]	

1.21. ΜΗΝΥΜΑ [CONTROL] (U) (Reference A1098) (ECRtoken)

Γενικό μήνυμα για έλεγχο συμπεριφοράς του EFTPOS από την ECR, σύνταξη:

ECR REQUEST:

U/*R<ecr-id>/C<command-name>:<parameter-value>{:paramater-value}*

Στοιχείο	Τύπος	Μέγεθος	Περιγραφή
ecr-id	an	11	
command-name	an	1..20	Συμβολική ονομασία της παραμέτρου προς ρύθμιση
parameter-value	an	1..50	Τιμή της παραμέτρου

Το σύνολο των παραμέτρων και των δυνατών τιμών τους είναι επεκτάσιμο, ανάλογα με τις ανάγκες που θα προκύπτουν.

ΠΑΡΑΜΕΤΡΟΣ	ΤΙΜΕΣ
UNBIND_POS	• *0 - το EFTPOS έχει κλειδωμένο πληκτρολόγιο και δεν μπορεί να ξεκινήσει συναλλαγές αυτόνομα.* • *1 - το EFTPOS μπορεί να εκτελέσει πιστωτικές συναλλαγές αυτόνομα, χωρίς εντολή ECR* **Η λειτουργία αυτή δεν θα χρησιμοποιηθεί στην A1155 καθώς υπάρχει το "Autonomous Mode"**
MAC_K	1η τιμή: MAC session κλειδί (32 hex digits), κρυπτογραφημένο υπό ορισμένο master key εμφυτευμένο σε αμφότερα ECR και EFTPOS. 2η τιμή: το CV του κλειδιού (6 hex digits). Αν αποτύχει ο έλεγχος του KCV, το EFTPOS επιστρέφει E/503 Για του παράδειγμα του κεφαλαίου Error: Reference source not found θα ήταν: MAC_K:1ED9F7AE0B2509281BBC2DE38EF2A12B:CC5FFF