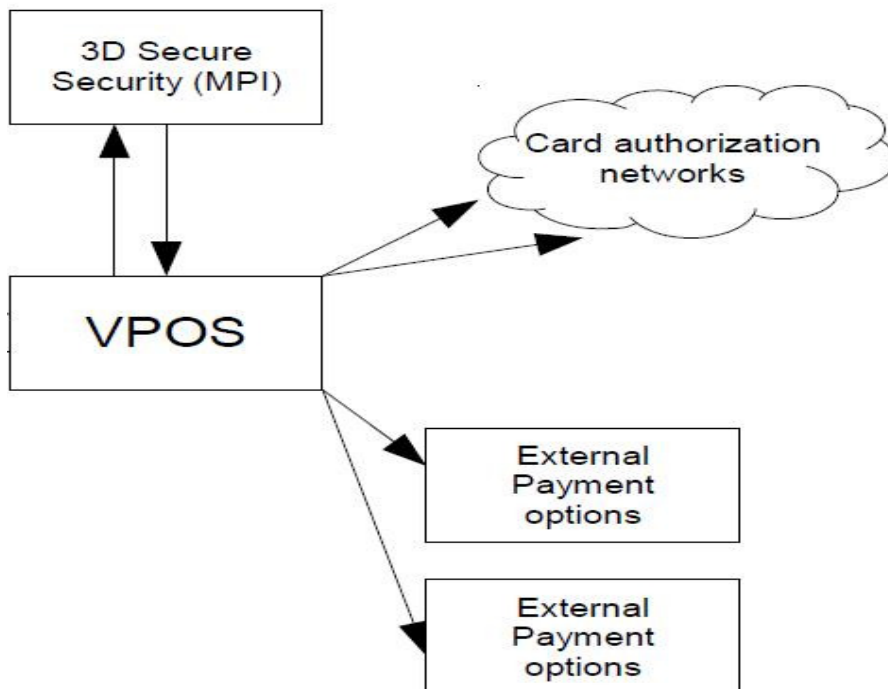


# Alpha e-Commerce

## Τεχνικές οδηγίες για την διασύνδεση επιχείρησης με την Υπηρεσία Alpha e-Commerce μέσω XML Direct



**Ιστορικό ενημερώσεων**

Έκδοση	Ημερομηνία	Περιγραφή / Αλλαγές
1.0	15.01.2015	Αρχική έκδοση
1.1	16.10.2015	Παροχή δυνατότητας αναζήτησης με xml queries

Οι πληροφορίες που περιέχονται στο παρόν έγγραφο υπόκεινται σε αλλαγές χωρίς προηγούμενη ειδοποίηση.

**ΤΟ ΠΑΡΟΝ ΕΓΓΡΑΦΟ ΑΠΟΤΕΛΕΙ ΕΜΠΙΣΤΕΥΤΙΚΟ ΚΑΙ ΙΔΙΟΚΤΗΣΙΑΚΟ ΠΡΟΪΟΝ ΤΗΣ ALPHA BANK.**

ΑΠΑΓΟΡΕΥΕΤΑΙ ΑΥΣΤΗΡΑ Η ΜΗ ΕΓΚΕΚΡΙΜΕΝΗ ΧΡΗΣΗ, ΑΝΑΠΑΡΑΓΩΓΗ, ΤΡΟΠΟΠΟΙΗΣΗ, ΔΙΑΝΟΜΗ ΚΑΙ ΜΕΤΑΒΙΒΑΣΗ ΤΟΥ ΠΑΡΟΝΤΟΣ ΕΓΓΡΑΦΟΥ.

**COPYRIGHT © ALPHA BANK (2013)**

**ΔΙΑΤΗΡΗΣΗ ΠΑΝΤΟΣ ΝΟΜΙΜΟΥ ΔΙΚΑΙΩΜΑΤΟΣ.**

Κανένα τμήμα της παρούσας εκδόσεως δεν επιτρέπεται να αναπαραχθεί, αποθηκευτεί ή να μεταδοθεί σε οποιαδήποτε μορφή και με οποιοδήποτε τρόπο, ηλεκτρονικό, μηχανικό, φωτοαντίγραφο, εγγραφή ή άλλο, χωρίς την προηγούμενη έγγραφη άδεια της ALPHA BANK.

Όλα τα προϊόντα που αναφέρονται στο παρόν χρησιμοποιούνται αποκλειστικά για σκοπούς αναγνώρισης και μπορεί να αποτελούν εμπορικά σήματα των αντίστοιχων εταιριών και / ή οργανισμών που τα διαθέτουν.

## Περιεχόμενα

1.	Διαδικασία μετάβασης επιχείρησης στο παραγωγικό περιβάλλον .....	4
2.	Τεχνική Διασύνδεση Επιχείρησης .....	5
2.1.	Κατηγορίες διασύνδεσης.....	5
2.2.	Διαθέσιμοι τύποι συναλλαγών μέσω XML Direct.....	5
3.	Συναλλαγές XML Direct με χρήση 3D Secure .....	7
3.1.	Προδιαγραφές μηνυμάτων XML Direct με χρήση 3D Secure.....	7
4.	Υπολογισμός Digest.....	22
4.1.	Υπολογισμός Digest για το MPI Request .....	22
4.2.	Υπολογισμός Digest XML μηνύματος .....	24
5.	Έλεγχος του digest στις απαντήσεις του MPI Response και του XML Response.....	28
5.1.	Έλεγχος του digest στις απαντήσεις του MPI Response.....	28
5.2.	Έλεγχος του digest στις απαντήσεις του XML Response.....	29
6.	Παροχή δυνατότητας αναζήτησης με xml queries .....	31

# 1. Διαδικασία μετάβασης επιχείρησης στο παραγωγικό περιβάλλον

Για να μπορέσει η επιχείρηση να ενταχθεί στο παραγωγικό περιβάλλον της υπηρεσίας Alpha e-Commerce θα πρέπει να ολοκληρωθούν τα παρακάτω βήματα:

1. Να πραγματοποιηθεί η τεχνική υλοποίηση της διασύνδεσης της επιχείρησης με την υπηρεσία Alpha e-Commerce, ακολουθώντας τις οδηγίες του παρόντος εγχειριδίου.
2. Τα στοιχεία που θα χρειαστούν για την έναρξη των δοκιμαστικών συναλλαγών είναι:
  - a. FORM Action POST URL: <https://alpha.test.modirum.com/vpos/xmlpayvpos>  
mid: (περιέχεται στο αρχικό mail που λαμβάνει ο τεχνικός της επιχείρησης)  
Shared secret key: (περιέχεται στο αρχικό mail που λαμβάνει ο τεχνικός της επιχείρησης)

b. Δοκιμαστικοί Αριθμοί Καρτών

Τύπος Κάρτας	Αριθμός	Ημερομηνία Λήξης	CVV2	Όνομα Κατόχου	3D Secure κωδικός
Visa	4509036603437007	12/19	464	test	Visanew4
MasterCard	5100990637713009	01/20	200	test	Mastercard2
American Express	375537684045006	01/18	4664/663	test	-

Για την καλύτερη διαχείριση των τεστ καρτών, παρακαλούμε να πραγματοποιείτε δοκιμαστικές συναλλαγές με μικρά ποσά (κάτω από 0.20 ευρώ)

- c. Πρόσβαση σε Test Περιβάλλον Διαχειριστικού Εργαλείου BackOffice  
Merchant BackOffice url: <https://alpha-admin.test.modirum.com/mpivposmgr>  
Username: (περιέχεται στο αρχικό mail που λαμβάνει ο τεχνικός της επιχείρησης)  
Password: (περιέχεται στο αρχικό mail που λαμβάνει ο τεχνικός της επιχείρησης)
3. Να ολοκληρωθούν επιτυχώς οι δοκιμές της τεχνικής διασύνδεσης της επιχείρησης με την υπηρεσία **Alpha e-Commerce** (απαιτείται τουλάχιστον μια επιτυχημένη δοκιμαστική συναλλαγή)
  4. Η επιχείρηση να ενημερώσει την Τράπεζα για την επιτυχή ολοκλήρωση των δοκιμών στέλνοντας e-mail στο [ecommerce@alpha.gr](mailto:ecommerce@alpha.gr) και δηλώνοντας παράλληλα την επιθυμητή ημερομηνία μετάβασης στη νέα πλατφόρμα, προκειμένου η Τράπεζα να προβεί στις απαραίτητες ενέργειες.
  5. Η Τράπεζα θα προχωρήσει στον έλεγχο της τελικής ιστοσελίδας (το URL της οποίας έχει κοινοποιηθεί στην Τράπεζα με τη συμπλήρωση του ερωτηματολογίου «Ρυθμίσεις Υπηρεσίας Alpha e-Commerce») μέσω της παρακάτω λίστας ελέγχου:
    1. ΠΛΗΡΗΣ ΠΕΡΙΓΡΑΦΗ ΠΡΟΪΟΝΤΩΝ – ΥΠΗΡΕΣΙΩΝ
    2. ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ – ΑΡΙΘΜΟΣ ΤΗΛΕΦΩΝΟΥ (σταθερό) / FAX
    3. ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ – E-MAIL
    4. ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ – ΔΙΕΥΘΥΝΣΗ
    5. ΠΟΛΙΤΙΚΗ ΕΠΙΣΤΡΟΦΩΝ / ΑΚΥΡΩΣΕΩΝ ΠΡΟΪΟΝΤΩΝ
    6. ΠΟΛΙΤΙΚΗ ΠΑΡΑΔΟΣΗΣ ΠΡΟΪΟΝΤΩΝ
    7. ΟΡΟΙ – ΠΡΟΫΠΟΘΕΣΕΙΣ ΧΡΗΣΗΣ ΤΟΥ SITE
    8. ΑΠΟΔΟΧΗ ΟΡΩΝ ΧΡΗΣΗΣ ΚΑΤΑ ΤΗ ΣΥΝΑΛΛΑΓΗ
    9. ΑΣΦΑΛΕΙΑ ΣΥΝΑΛΛΑΓΩΝ
    10. ΤΡΟΠΟΙ ΠΛΗΡΩΜΗΣ
    11. ΕΜΦΑΝΙΣΗ LOGO ΑΠΟΔΕΚΤΩΝ ΚΑΡΤΩΝ\*  
\*Οι διεθνείς οργανισμοί καρτών επιβάλλουν την προβολή του σήματος των αποδεκτών καρτών στην ιστοσελίδα της επιχείρησης. Για τη διευκόλυνσή σας, στο φάκελο «Logos» του αρχείου «Technical Integration.zip»
    12. ΕΜΦΑΝΙΣΗ ΑΠΟΔΕΙΞΗΣ & ΔΥΝΑΤΟΤΗΤΑ ΕΚΤΥΠΩΣΗΣ ΤΗΣ ΑΠΟ ΤΟΝ ΠΕΛΑΤΗ
    13. ΕΠΙΤΥΧΗΜΕΝΗ ΠΡΑΓΜΑΤΟΠΟΙΗΣΗ ΔΟΚΙΜΑΣΤΙΚΗΣ ΣΥΝΑΛΛΑΓΗΣ

## 2. Τεχνική Διασύνδεση Επιχείρησης

### 2.1. Κατηγορίες διασύνδεσης

Η Alpha Bank προσφέρει τη δυνατότητα σε όλες τις συνεργαζόμενες επιχειρήσεις και εμπόρους να παρέχουν υπηρεσίες ηλεκτρονικών πληρωμών από την ιστοσελίδα τους, 24 ώρες το 24ωρο, 365 ημέρες το χρόνο, με τη χρήση χρεωστικών, πιστωτικών ή προπληρωμένων καρτών. Για το σκοπό αυτό είναι αναγκαία η διασύνδεση του συστήματος της επιχείρησης με την υπηρεσία Alpha e-Commerce.

Οι επιλογές για την online διασύνδεση της επιχείρησης με την υπηρεσία Alpha e-Commerce είναι:

#### 1. Διασύνδεση Re-direct

Ο πελάτης, επιλέγοντας σαν τρόπο πληρωμής την κάρτα, μεταβαίνει αυτόματα στη σελίδα πληρωμής της υπηρεσίας, όπου και πληκτρολογεί τα στοιχεία της κάρτας του (HTTP Post Method).

#### 2. Διασύνδεση XML Direct

Η επικοινωνία μεταξύ της επιχείρησης και της υπηρεσίας Alpha e-Commerce γίνεται μέσω XML μηνυμάτων.

##### 2.1. Συναλλαγές XML Direct με χρήση 3D Secure

Ο πελάτης, επιλέγοντας σαν τρόπο πληρωμής την κάρτα, παραμένει στην ιστοσελίδα της επιχείρησης, και ολοκληρώνει την πληρωμή του σε αυτή. Υποχρεωτικά παρέχεται SSL encryption 256 bit ενώ πρέπει να πληρούνται και οι προδιαγραφές ασφαλείας των Διεθνών Οργανισμών Visa, MasterCard και American Express.

##### 2.2. Συναλλαγές XML Direct για Call Center (Virtual Terminal XML)

Ο πελάτης παρέχει τα στοιχεία της κάρτας του στην επιχείρηση η οποία και αποστέλλει στην υπηρεσία Alpha e-Commerce τη συναλλαγή, μέσω του συστήματός της, με μήνυμα XML

Στο παρόν εγχειρίδιο, αναλύεται η διασύνδεση μέσω **XML Direct με χρήση 3D Secure**.

### 2.2. Διαθέσιμοι τύποι συναλλαγών μέσω XML Direct

Οι διαθέσιμοι τύποι συναλλαγών μέσω XML Direct (είτε με χρήση 3D Secure είτε μέσω Virtual Terminal XML) που υποστηρίζονται από την υπηρεσία Alpha e-Commerce είναι οι παρακάτω και για κάθε μια πρέπει να αποστέλλεται το αντίστοιχο XML μήνυμα.

SaleRequest – πληρωμή (Sale)

AuthorisationRequest – προέγκριση (Pre-Auth)

CaptureRequest – ολοκλήρωση προέγκρισης

RefundRequest – επιστροφή συναλλαγής έπειτα από την εκκαθάριση (settlement)

CancelRequest – ακύρωση (reversal) συναλλαγής πριν από την εκκαθάριση (settlement)

RecurringOperationRequest – ακύρωση επαναλαμβανόμενης πληρωμής με τη χρήση της λειτουργίας Cancel

RecurringNotification – ενημερωτικό μήνυμα για την εκτέλεση επαναλαμβανόμενης πληρωμής το οποίο αποστέλλεται σε URL το οποίο έχει καταχωρηθεί στο προφίλ της επιχείρησης

Για ορισμένα από τα παραπάνω μηνύματα και ανάλογα με τον τύπο της συναλλαγής που η επιχείρηση εκτελεί (Sale ή Pre-Auth), ισχύουν τα εξής:

Τύπος Συναλλαγής	CaptureRequest	CancelRequest (Reversal)	RefundRequest
Sale	Δεν ισχύει για τις Sale συναλλαγές	Μπορεί να αποσταλεί μόνο την ημέρα που έχει πραγματοποιηθεί η συναλλαγή (πριν κλείσει το πακέτο συναλλαγών <sup>1</sup> )	Για να αποσταλεί πρέπει να έχει προηγηθεί το κλείσιμο πακέτου (settlement)
Pre-Auth	Μπορεί να αποσταλεί μέσα σε 7 ημερολογιακές ημέρες από την ημερομηνία της αρχικής συναλλαγής	Μπορεί να αποσταλεί μέσα σε 7 ημερολογιακές ημέρες από την ημερομηνία της αρχικής συναλλαγής και εφόσον δεν έχει σταλεί το CaptureRequest	Για να αποσταλεί πρέπει να έχουν προηγηθεί: α) το CaptureRequest β) το κλείσιμο πακέτου (settlement)

Για κάθε τύπο συναλλαγής που αποστέλλεται στην υπηρεσία Alpha e-Commerce επιστρέφεται το αντίστοιχο απαντητικό μήνυμα από την Τράπεζα το οποίο και περιέχει τα διάφορα στοιχεία έγκρισης ή απόρριψης. Έτσι, ανάλογα με τον τύπο της συναλλαγής υπάρχουν τα εξής απαντητικά μηνύματα:

SaleResponse  
 AuthorisationResponse  
 CaptureResponse  
 RefundResponse  
 CancelResponse  
 RecurringOperationResponse

<sup>1</sup> Το κλείσιμο του πακέτου πραγματοποιείται αυτόματα στο τέλος κάθε ημέρας (στις 23:59:59)

### 3. Συναλλαγές XML Direct με χρήση 3D Secure

Η ροή μιας τυπικής 3D Secure συναλλαγής με χρήση του XML περιλαμβάνει τα παρακάτω βήματα:

1. Ο πελάτης της επιχείρησης επιλέγει τα προϊόντα ή τις υπηρεσίες που θα αγοράσει, αποδέχεται υποχρεωτικά τους Όρους Χρήσης του ηλεκτρονικού καταστήματος και καταλήγει στη σελίδα επιλογής τρόπου πληρωμής της επιχείρησης (checkout page)
2. Εφόσον επιλέξει σαν τρόπο πληρωμής την κάρτα, θα μεταβεί αυτόματα στη σελίδα πληρωμής, η οποία φιλοξενείται στο site της επιχείρησης.
3. Ο κάτοχος της κάρτας συμπληρώνει στη σελίδα πληρωμής τα στοιχεία της κάρτας του και η επιχείρηση αποστέλλει το σχετικό request στο MPI. Στα στοιχεία της συναλλαγής περιλαμβάνεται και το πεδίο Digest που περιέχει κρυπτογραφημένα τα στοιχεία της συναλλαγής και το οποίο υπολογίζεται με βάση ένα **shared secret key** (η διαδικασία περιγράφεται αναλυτικά στο κεφάλαιο 4).
4. Αν η κάρτα είναι εγγεγραμμένη στην υπηρεσία 3D Secure (για κάρτες Visa / MasterCard / American Express), ο browser του κατόχου της κάρτας δρομολογείται στην αντίστοιχη υπηρεσία της εκδότριας τράπεζας, για την εισαγωγή από τον κάτοχο του μοναδικού κωδικού που διαθέτει για τη χρήση της υπηρεσίας.
5. Εφόσον το αποτέλεσμα της πιστοποίησης (authentication) είναι θετικό, η συναλλαγή αποστέλλεται από την Τράπεζα για έγκριση (authorization) αφού πρώτα το σύστημα της υπηρεσίας Alpha e-Commerce αποκωδικοποιήσει το Digest που περιέχει τις πληροφορίες της συναλλαγής και ελέγξει την εγκυρότητά της καθώς και εάν οι παράμετροι της συναλλαγής είναι σωστές.
6. Το σύστημα της υπηρεσίας Alpha e-Commerce στέλνει απαντητικό μήνυμα XML προς την επιχείρηση, ενημερώνοντας για το τελικό status της συναλλαγής. Από την πλευρά της η επιχείρηση, εμφανίζει την ανάλογη με το τελικό status σελίδα, στον κάτοχο της κάρτας.

Τονίζεται ότι σε περίπτωση επιτυχημένης συναλλαγής, είναι **υποχρεωτική** η εμφάνιση της «Απόδειξης Συναλλαγής» καθώς και η δυνατότητα εκτύπωσής της από τον πελάτη (βλ. Παράρτημα Β)

#### 3.1. Προδιαγραφές μηνυμάτων XML Direct με χρήση 3D Secure

Η πραγματοποίηση μιας συναλλαγής με χρήση της υπηρεσίας 3D Secure περιλαμβάνει τα εξής στάδια:

- 1) Δημιουργία MPI Request μέσω http post (με βάση τον παρακάτω πίνακα μεταβλητών) και αποστολή του στο <https://alpha.test.modirum.com/mdpaympi/MerchantServer>

Μεταβλητή	Υποχρεωτικό (Υ) Προαιρετικό (Π)	Μήκος Πεδίου	Περιγραφή
version	Υ	AN3	Η τιμή της τρέχουσας έκδοσης είναι 2.0
pan	Υ	N13...19	Ο αριθμός της κάρτας
expiry	Υ	N4	Ημερομηνία λήξης της κάρτας (με τη μορφή YYMM)
deviceCategory	Π	N1	Προσωρινά μη διαθέσιμη μεταβλητή

purchAmount	Y	N3...12	Ποσό συναλλαγής Ακέραιος αριθμός όπου τα δύο τελευταία ψηφία αποτελούν τα δεκαδικά ψηφία  (π.χ. για ποσό 67,56 η τιμή πρέπει να είναι 6756)
exponent	Y	N1	Παίρνει την τιμή 2
description	Π	AN...125	Περιγραφή συναλλαγής
currency	Y	N3	Κωδικός νομίσματος σύμφωνα με το πρότυπο ISO 4217.  Για το Ευρώ η τιμή είναι 978
merchantID	Y	N10	Κωδικός Εμπόρου (όπως έχει δοθεί από την τράπεζα)
xid	Y	AN28	Μοναδικός κωδικός συναλλαγής καθοριζόμενος από την επιχείρηση.  Τιμή με αρχικό μήκος 20 byte το οποίο κωδικοποιείται κατά Base64 και η τελική τιμή που προκύπτει είναι 28 χαρακτήρες  <b>Παράδειγμα:</b> 00000000000000689392 (20 bytes)  Μετά την κωδικοποίηση κατά Base64 το αποτέλεσμα είναι:  MDAwMDAwMDAwMDAwMDA2ODkzOTI=
okUrl	Y	A...250	Το url της επιχείρησης στο οποίο στέλνονται οι απαντητικές μεταβλητές του MPI Repsonse σε περίπτωση επιτυχημένης πιστοποίησης
failUrl	Y	A...250	Το url της επιχείρησης στο οποίο στέλνονται οι απαντητικές μεταβλητές του MPI Repsonse σε περίπτωση αποτυχημένης πιστοποίησης
MD	Π	AN...254	Ελεύθερο πεδίο για την επιχείρηση. Το πεδίο πρέπει να περιλαμβάνει μόνο ASCII χαρακτήρες με εύρος από 0x20 έως 0x7E.  Το πεδίο κωδικοποιείται κατά Base64 και η τελική τιμή που προκύπτει πρέπει να είναι μέχρι 254 χαρακτήρες.



recurFreq	Π	N1...2	<p>Η συχνότητα σε ημέρες για την εκτέλεση επαναλαμβανόμενης πληρωμής (recurring payment)</p> <p><b>(ως μήνας θεωρείται η τιμή 28)</b></p>
recurEnd	Π/Υ	N8	<p>Η ημερομηνία πέραν της οποίας ΔΕΝ θα πραγματοποιείται η επαναλαμβανόμενη πληρωμή</p> <p><b>ΠΡΟΣΟΧΗ!!</b>  <b>Η αποστολή της μεταβλητής είναι υποχρεωτική αν έχει αποσταλεί η μεταβλητή recurFreq</b></p> <p><b>Η ημερομηνία πρέπει να είναι σε μορφή YYYYMMDD</b></p> <p><b>Επαναλαμβανόμενη πληρωμή ΔΕΝ μπορεί να αποσταλεί ταυτόχρονα με δόσεις (installments)</b></p>
installments	Π	N1...2	<p>Ο αριθμός των μηνιαίων δόσεων (εφόσον υφίσταται εμπορική συμφωνία με την Τράπεζα)</p> <p><b>ΠΡΟΣΟΧΗ!!</b></p> <p><b>Οι δόσεις ΔΕΝ μπορούν να αποσταλούν ταυτόχρονα με επαναλαμβανόμενες πληρωμές (recurring payments)</b></p>
digest	Υ	Δεν υπάρχει συγκεκριμένο μήκος πεδίου	<p>Ο υπολογισμός του αναφέρεται αναλυτικά στο κεφάλαιο 4</p>

**Παράδειγμα MPI Request:**

```

<html>
<head>
<title>Test Page</title>
</head>
<body>
<form name="myform" action="https://alpha.test.modirum.com/mdpaympi/MerchantServer"
method="POST">
<div align="center">
<br><br>

<input type="text" name="version" value="2.0">
<input type="text" name="pan" value="4509036603504004">
<input type="text" name="expiry" value="1601">
<input type="text" name="purchAmount" value="10">
<input type="text" name="exponent" value="2">
<input type="text" name="currency" value="978">
<input type="text" name="merchantID" value="9508532">
<input type="text" name="xid" value="MDAwMDAwMDAwMDAwMDAyNzk2MTk=">
<input type="text" name="okUrl" value="https://merchanturl.com/PaymentId_Ok">

```

```
<input type="text" name="failUrl" value="https://merchanturl.com/PaymentId_Fail">
<input type="text" name="MD" value="This is a test order">
<input type="text" name="digest" value="lux0deFayK34IX5K2slh58g2EA4=">
```

```
<br><input type="submit" value="Send"><br>
</div>
</form>
</body>
</html>
```

2) Τα πεδία που επιστρέφονται από το MPI response αναλύονται στον παρακάτω πίνακα:

Μεταβλητή	Υποχρεωτικό (Υ) Προαιρετικό (Π)	Μήκος Πεδίου	Περιγραφή
version	Υ	AN3	Επιστρέφεται η τιμή που είχε σταλεί στο MPI Request
merchantID	Υ	N10	Επιστρέφεται η τιμή που είχε σταλεί στο MPI Request
xid	Υ	AN28	Επιστρέφεται η τιμή που είχε σταλεί στο MPI Request
mdStatus	Υ	N1	<p>Το τελικό αποτέλεσμα της συναλλαγής. Οι πιθανές τιμές είναι:</p> <ul style="list-style-type: none"> <li>0 = Η συναλλαγή δεν πιστοποιήθηκε ως προς την υπηρεσία 3D Secure</li> <li>1 = Η συναλλαγή πιστοποιήθηκε επιτυχώς ως προς την υπηρεσία 3D Secure</li> <li>2 = Η κάρτα του πελάτη δεν είναι εγγεγραμμένη στην υπηρεσία 3D Secure ή η εκδότρια τράπεζα δεν συμμετέχει στην υπηρεσία</li> <li>3 = Η κάρτα του πελάτη δεν είναι εγγεγραμμένη στην υπηρεσία 3D Secure ή η εκδότρια τράπεζα δεν συμμετέχει στην υπηρεσία</li> <li>4 = Έγινε προσπάθεια για πιστοποίηση της κάρτας χωρίς όμως να ολοκληρωθεί επιτυχώς</li> <li>5, 6, 7 = Παρουσιάστηκε πρόβλημα κατά τη διάρκεια πιστοποίησης της συναλλαγής</li> <li>8 = Η συναλλαγή διακόπηκε από τον Fraud Score Server<sup>2</sup></li> <li>9 = Το MPI Request δεν έχει ολοκληρωθεί</li> </ul>
mdErrorMsg	Υ	AN...128	Αποστέλλεται σε περίπτωση που προκύψει κάποιο πρόβλημα κατά τη διάρκεια της πιστοποίησης
txstatus	Υ	A1	Επιστρέφεται από τον ACS Server
iReqCode	Π	N2	Επιστρέφεται από τον ACS Server

<sup>2</sup> Η υπηρεσία του Fraud Score Server δεν είναι διαθέσιμη προς το παρόν

iReqDetail	Π	Δεν υπάρχει συγκεκριμένο μήκος πεδίου	Επιστρέφεται από τον ACS Server
vendorCode	Π	Δεν υπάρχει συγκεκριμένο μήκος πεδίου	Επιστρέφεται από τον ACS Server
eci	Π	N2	Επιστρέφεται από τον ACS Server
cavv	Π	AN28	Επιστρέφεται από τον ACS Server
cavvAlgorithm	Π	Δεν υπάρχει συγκεκριμένο μήκος πεδίου	Επιστρέφεται από τον ACS Server
MD	Π	AN...254	Επιστρέφεται η τιμή που είχε σταλεί στο MPI Request
digest	Π	Δεν υπάρχει συγκεκριμένο μήκος πεδίου	Τιμή που υπολογίζεται με βάση το σύνολο των μεταβλητών που αποστέλλεται στο MPI Response
PAResVerified	Π	Δεν υπάρχει συγκεκριμένο μήκος πεδίου	Επιστρέφεται από τον ACS Server Πιθανές Τιμές: "true", "false"
PAResSyntaxOK	Π	Δεν υπάρχει συγκεκριμένο μήκος πεδίου	Επιστρέφεται από τον ACS Server Πιθανές Τιμές: "true", "false"
veresEnrolledStatus	Π	Δεν υπάρχει συγκεκριμένο μήκος πεδίου	Επιστρέφεται από τον ACS Server
mparesTxStatus	Π	Δεν υπάρχει συγκεκριμένο μήκος πεδίου	Επιστρέφεται από τον ACS Server

3) Από τις μεταβλητές που επιστρέφονται από το MPI response, οι παρακάτω:

CAVV  
XID  
ECI  
EnrollmentStatus  
AuthenticationStatus

θα πρέπει να ενσωματωθούν στο μήνυμα XML μέσω του οποίου η επιχείρηση θα αποστείλει τη συναλλαγή στην υπηρεσία Alpha e-Commerce για έγκριση.

Για την ενσωμάτωση των μεταβλητών EnrollmentStatus και AuthenticationStatus στο XML μήνυμα που θα αποσταλλεί στην υπηρεσία Alpha e-Commerce χρησιμοποιείται ο παρακάτω πίνακας:

Μεταβλητή mdStatus	Τιμή που συμπληρώνεται στο πεδίο EnrollmentStatus του XML μηνύματος	Τιμή που συμπληρώνεται στο πεδίο AuthenticationStatus του XML μηνύματος	Ενέργεια
Av mdStatus=0	Y	N	Η συναλλαγή δεν πρέπει να αποσταλεί στην Τράπεζα προς έγκριση <b>No Liability Shift *</b>
Av mdStatus=1	Y	Y	Η συναλλαγή να αποσταλεί στην Τράπεζα προς έγκριση <b>Liability Shift</b>
Av mdStatus=2	N	κενό	Η συναλλαγή να αποσταλεί στην Τράπεζα προς έγκριση <b>Liability Shift</b>
Av mdStatus=4	Y	A	Η συναλλαγή να αποσταλεί στην Τράπεζα προς έγκριση <b>Liability Shift</b>
Av mdStatus=5	U	κενό	Η συναλλαγή δεν πρέπει να αποσταλεί στην Τράπεζα προς έγκριση <b>No Liability Shift</b>
Av mdStatus=5	Y	U	Η συναλλαγή δεν πρέπει να αποσταλεί στην Τράπεζα προς έγκριση <b>No Liability Shift</b>
Av mdStatus=6	Y	κενό	Η συναλλαγή δεν πρέπει να αποσταλεί στην Τράπεζα προς έγκριση <b>No Liability Shift</b>
Av mdStatus=6	κενό	κενό	Η συναλλαγή δεν πρέπει να αποσταλεί στην Τράπεζα προς έγκριση <b>No Liability Shift</b>
Av mdStatus=7	N/A	N/A	Η συναλλαγή δεν πρέπει να αποσταλεί στην Τράπεζα προς έγκριση <b>No Liability Shift</b>

\* *Liability Shift*: Μετακύλιση ευθύνης στην εκδότρια τράπεζα του κατόχου κάρτας.

- 4) Το τελευταίο στάδιο περιλαμβάνει τη δημιουργία του xml μηνύματος με τα στοιχεία της συναλλαγής και την αποστολή του στην υπηρεσία Alpha e-Commerce για έγκριση (Post URL: <https://alpha.test.modirum.com/vpos/xmlpayvpos>).

Η γενική δομή του XML μηνύματος είναι η παρακάτω:

Το Root element όλων των μηνυμάτων είναι το **VPOS**

Το xsd schema καθορίζεται από το <https://vposadmin.modirum.com/vpos/xsd/VPOS.xsd>

Το xsd για τα xml μηνύματα βρίσκεται στην διεύθυνση:

<https://alpha.test.modirum.com/vpos/xsd/VPOS.xsd>

Το σύνολο των elements που περιλαμβάνονται σε ένα XML μήνυμα είναι τα παρακάτω (ανάλογα με τον τύπο της συναλλαγής ορισμένα elements είναι υποχρεωτικά και άλλα προαιρετικά, περιγράφεται παρακάτω):

Element	Τύπος πεδίου	Περιγραφή
<b>VPOS</b>	element	<b>Στοιχείο XML Root</b>
<b>Message</b>	element type Message	<b>Στοιχείο Message</b>
lang	attribute, xsi:string (A2)	Κωδικός γλώσσας Για ελληνικά: el Για αγγλικά: en  Για τις υπόλοιπες γλώσσες, ο κωδικός της γλώσσας με βάση το πρότυπο ISO 639-1
messageld	attribute, xsi:string	Μοναδικός κωδικός μηνύματος (καθορίζεται από την επιχείρηση)
version	attribute, xsi:string	Η τιμή της τρέχουσας έκδοσης είναι 1.0
<b>Authentication</b>	element	<b>Στοιχείο Authentication</b>
Mid	xsi:string (N10)	Κωδικός Εμπόρου (όπως έχει δοθεί από την τράπεζα)
Digest	xsi:string	Το πεδίο Digest υπολογίζεται μέσω Base64(SHA1((utf8bytes(canonicalize(Message))+utf8bytes(sharedSecret))).  Αναλυτικά ο τρόπος υπολογισμού του στο κεφάλαιο 4
Password	xsi:string (AN7..16)	Χρησιμοποιείται μόνο σε περίπτωση που δεν στέλνεται το digest
<b>OrderInfo</b>	element	<b>Στοιχείο Orderinfo</b>
DeviceCategory	xsi:string (N1)	Προσωρινά μη διαθέσιμη μεταβλητή
OrderId	xsi:string (AN1..50)	Μοναδικός κωδικός συναλλαγής που καθορίζει η επιχείρηση.  Επιτρέπονται μόνο αλφαριθμητικοί χαρακτήρες χωρίς κενά μεταξύ τους
OrderDesc	xsi:string (AN1..128)	Περιγραφή συναλλαγής
OrderAmount	xsi:decimal (max 9+2)	Ποσό συναλλαγής  Δεκαδικός αριθμός με δύο δεκαδικά ψηφία χωρισμένα είτε με τελεία είτε με κόμμα (π.χ. 0,10 - 10,00 – 10.45 - 1345,56 – 1234.45)

Currency	xsi:string (A3)	Κωδικός νομίσματος (EUR)
PayerEmail	xsi:string (AN1..64)	e-mail πελάτη
PayerPhone	xsi:string (N1..30)	Τηλέφωνο Πελάτη
AddFraudScore	xsi:string (N1..10)	Δείκτης ρίσκου της συναλλαγής (στέλνεται σε περίπτωση που είναι ενεργοποιημένος ο Fraud Score Server – μελλοντικά διαθέσιμη υπηρεσία)
BlockScore	xsi:string (N1..10)	Τιμή κατά την οποία η συναλλαγή μπλοκάρεται από τον Fraud Score Server – μελλοντικά διαθέσιμη υπηρεσία)
Var1	xsi:string (AN1..255)	Δεσμευμένο πεδίο για την αποστολή του αριθμού της Κάρτας Αποδείξεων του Υπουργείου Οικονομικών (ΦΟΡΟΚΑΡΤΑ) (μελλοντικά διαθέσιμη υπηρεσία)
Var2	xsi:string (AN1..255)	Ελεύθερο πεδίο (στις μεταβλητές var2 – var5 μπορούν να σταλούν ελεύθερα επιπλέον μεταβλητές που επιθυμεί η επιχείρηση)
Var3	xsi:string (AN1..255)	Ελεύθερο πεδίο (στις μεταβλητές var2 – var5 μπορούν να σταλούν ελεύθερα επιπλέον μεταβλητές που επιθυμεί η επιχείρηση)
Var4	xsi:string (AN1..255)	Ελεύθερο πεδίο (στις μεταβλητές var2 – var5 μπορούν να σταλούν ελεύθερα επιπλέον μεταβλητές που επιθυμεί η επιχείρηση)
Var5	xsi:string (AN1..255)	<p>Δεσμευμένο πεδίο για το χαρακτηρισμό του καναλιού από το οποίο στέλνεται μια συναλλαγή. Οι τιμές που μπορούν να αποσταλούν είναι:</p> <ul style="list-style-type: none"> <li>• Web browser</li> <li>• mobile</li> <li>• IP TV</li> </ul> <p><b>Οι μεταβλητές των πεδίων Var2 έως Var5 δεν επιστρέφονται στο απαντητικό μήνυμα που στέλνει η Τράπεζα κατά την ολοκλήρωση της συναλλαγής</b></p>
MOTO	xsi:integer (N1)	Χαρακτηρισμός συναλλαγής ως ΜΟ/ΤΟ (η τιμή 1 υποδεικνύει ότι η συναλλαγή είναι ΜΟ/ΤΟ)
<b>Billing Address</b>	element	<b>Στοιχείο Billing Adress</b>
Country	xsi:string (A2)	Κωδικός χώρας (π.χ. GR, US, IT) με βάση το πρότυπο ISO 3166-1
State	xsi:string (AN1..50)	Περιοχή χρέωσης του πελάτη
Zip	xsi:string (AN1..16)	Τ.Κ. χρέωσης του πελάτη
City	xsi:string (AN1..64)	Πόλη χρέωσης του πελάτη
Address	xsi:string (AN1..100)	Διεύθυνση χρέωσης του πελάτη

<b>ShippingAddress</b>	<b>element</b>	<b>Στοιχείο shipping address</b>
Country	xsi:string (A2)	Κωδικός χώρας αποστολής του προϊόν (π.χ. GR, US, IT). με βάση το πρότυπο ISO 3166-1
State	xsi:string (AN1..50)	Περιοχή αποστολής προϊόντος
Zip	xsi:string (AN1..16)	T.K. περιοχής που θα αποσταλεί το προϊόν
City	xsi:string (AN1..64)	Πόλη αποστολής προϊόντος
Address	xsi:string (AN1..100)	Διεύθυνση αποστολής προϊόντος
<b>PaymentInfo</b>	<b>element</b>	<b>Στοιχείο Payment info</b>
PayMethod	xsi:string (AN1..20)	Μέθοδος πληρωμής Διαθέσιμες τιμές: visa, mastercard, visaElectron, maestro, amex, diners
CardPan	xsi:string (N13..19)	Αριθμός κάρτας πελάτη
CardExpDate	xsi:string (N4)	Ημερομηνία λήξης της κάρτας (με τη μορφή YYMM)
CardHolderName	xsi:string (AN1..24)	Όνοματεπώνυμο κατόχου κάρτας
CardCvv2	xsi:string (N3..4)	Ο κωδικός CVV2 ή CVC2 ή CID
RecurringIndicator	xsi:string (A1)	Η τιμή R υποδεικνύει ότι πρόκειται για επαναλαμβανόμενη πληρωμή
<b>RecurringParameters</b>	<b>element</b>	<b>Στοιχείο RecurringParameters</b>
ExtRecurringfrequency	xsi:string (N1..3)	Η συχνότητα σε ημέρες για την εκτέλεση επαναλαμβανόμενης πληρωμής (recurring payment) (ως μήνας θεωρείται η τιμή 28)
ExtRecurringenddate	xsi:string (N8)	Η ημερομηνία πέραν της οποίας ΔΕΝ θα πραγματοποιείται η επαναλαμβανόμενη πληρωμή  <b>ΠΡΟΣΟΧΗ!!</b> <b>Η ημερομηνία πρέπει να είναι σε μορφή YYYYMMDD</b>  <b>Επαναλαμβανόμενη πληρωμή ΔΕΝ μπορεί να αποσταλεί ταυτόχρονα με δόσεις (installments)</b>
<b>InstallmentParameters</b>	<b>element</b>	<b>Στοιχείο Installments parameters</b>
ExtInstallmentoffset	xsi:integer (N1..2)	Ο αριθμός των μηνών χάριτος (μεταχρονολόγησης), πριν ξεκινήσουν να χρεώνονται δόσεις (εφόσον υφίσταται εμπορική συμφωνία με την Τράπεζα)
ExtInstallmentperiod	xsi:integer (N1..2)	Ο αριθμός των μηνιαίων δόσεων (εφόσον υφίσταται εμπορική συμφωνία με την Τράπεζα)  <b>ΠΡΟΣΟΧΗ!!</b> <b>Η αποστολή της μεταβλητής είναι υποχρεωτική αν έχει αποσταλεί το extInstallmentoffset</b>

		<b>Οι δόσεις ΔΕΝ μπορούν να αποσταλούν ταυτόχρονα με επαναλαμβανόμενες πληρωμές (recurring payments)</b>
<b>ThreeDSecure</b>	<b>element</b>	<b>Στοιχείο 3DSecure</b>
EnrollmentStatus	xsi:string (AN1)	Η τιμή υπολογίζεται με βάση τον προηγούμενο πίνακα
AuthenticationStatus	xsi:string (AN1)	Η τιμή υπολογίζεται με βάση τον προηγούμενο πίνακα
CAVV	xsi:string (AN28)	Η τιμή που στάλθηκε από το MPI Response (Av MD status = 2,3,5, 6 η τιμή του CAVV μένει κενή)
XID	xsi:string (AN28)	Η τιμή που στάλθηκε από το MPI Response
ECI	xsi:string (N2)	Η τιμή που στάλθηκε από το MPI Response (Av MD status = 2,3,5, 6 η τιμή του ECI μένει κενή)
<b>TransactionInfo</b>	<b>element</b>	<b>Στοιχείο TransactionInfo (χρησιμοποιείται μόνο σε περίπτωση που στέλνεται ακύρωση επαναλαμβανόμενης πληρωμής με τη χρήση του RecurringOperationRequest)</b>
OrderId	xsi:string (AN1..50)	Μοναδικός κωδικός συναλλαγής που καθορίζει η επιχείρηση. Επιτρέπονται μόνο αλφαριθμητικοί χαρακτήρες με μέγιστο μήκος 50 χαρακτήρες και χωρίς κενά μεταξύ τους
Operation	xsi:string (AN1..25)	Χρησιμοποιείται η τιμή Cancel για την ακύρωση επαναλαμβανόμενης πληρωμής

- 5) Μετά την επεξεργασία της συναλλαγής από την υπηρεσία Alpha e-Commerce, τα πεδία που επιστρέφονται φαίνονται στον παρακάτω πίνακα:

<b>Elements απαντητικού μηνύματος από Τράπεζα (Response)</b>		
<b>VPOS</b>	<b>element</b>	<b>Στοιχείο XML Root</b>
<b>Message</b>	<b>element type message</b>	<b>Στοιχείο Message</b>
lang	attribute, xsi:string	Επιστρέφεται η τιμή που είχε σταλεί στο XML Request μήνυμα
messageId	attribute, xsi:string	Επιστρέφεται η τιμή που είχε σταλεί στο XML Request μήνυμα
version	attribute, xsi:string	Επιστρέφεται η τιμή που είχε σταλεί στο XML Request μήνυμα
Digest	xsi:string	Υπολογίζεται με βάση τις μεταβλητές του απαντητικού μηνύματος
<b>Response</b>	<b>element</b>	<b>Στοιχείο Response</b>



OrderId	xsi:string	Επιστρέφεται η τιμή που είχε σταλεί στο XML Request μήνυμα
OrderAmount	xsi:decimal	Επιστρέφεται η τιμή που είχε σταλεί στο XML Request μήνυμα
Currency	xsi:string	Επιστρέφεται η τιμή που είχε σταλεί στο XML Request μήνυμα
PaymentTotal	xsi:decimal	Επιστρέφεται η τιμή που είχε σταλεί στο XML Request μήνυμα
Status	xsi:long	Το αποτέλεσμα της συναλλαγής: <b>AUTHORIZED</b> εάν η επιχείρηση έχει στείλει PRE-AUTH συναλλαγή και αυτή ολοκληρώθηκε επιτυχώς <b>CAPTURED</b> αν η επιχείρηση έχει στείλει SALE συναλλαγή και αυτή ολοκληρώθηκε επιτυχώς <b>REFUSED</b> εάν η συναλλαγή δεν πήρε έγκριση <b>CANCELED</b> (επιστρέφεται μόνο σε περίπτωση ακύρωσης επαναλαμβανόμενης συναλλαγής) <b>ERROR</b> εάν παρουσιάστηκε πρόβλημα κατά τη διάρκεια της συναλλαγής
TxId	xsi:string	Κωδικός συναλλαγής που παράγεται αυτόματα από την υπηρεσία Alpha e-Commerce
Sequence	xsi:integer	Σε περίπτωση επαναλαμβανόμενης πληρωμής, ο αύξων αριθμός της επαναλαμβανόμενης πληρωμής
SeqTxId	xsi:long	Σε περίπτωση επαναλαμβανόμενης πληρωμής, το TxId της επαναλαμβανόμενης συναλλαγής
PaymentRef	xsi:string	Κωδικός έγκρισης συναλλαγής
RiskScore	xsi:integer	Δείκτης ρίσκου της συναλλαγής (επιστρέφεται σε περίπτωση που έχει χρησιμοποιηθεί ο Fraud Score Server – μελλοντικά διαθέσιμη υπηρεσία)
ErrorCode	xsi:string	Σε περίπτωση που η συναλλαγή έχει status ERROR, ο κωδικός του error
Description	xsi:string	Σε περίπτωση που η συναλλαγή έχει status ERROR περιγράφεται λεκτικά το πρόβλημα (όλα τα λεκτικά περιέχονται στην ενότητα Δ του Παραρτήματος)
OriginalXML	xsi:string	Το αρχικό XML Μήνυμα κωδικοποιημένο

Τα διάφορα elements (είτε του request είτε του response) ενδέχεται να είναι υποχρεωτικά ή προαιρετικά ανάλογα με τον τύπο του μηνύματος.

Ο παρακάτω πίνακας περιέχει την υποχρεωτικότητα του κάθε element (R - required, O-optional, C-conditional) ανάλογα με τον τύπο του μηνύματος.

Field element/ Request	SaleRequest	Authorisation Request	CaptureRequest	RefundRequest	CancelRequest	RecurringOperationRequest	SaleResponse	AuthorisationResponse	CaptureResponse	RefundResponse	CancelResponse	RecurringOperationResponse	RecurringNotification	Παρατηρήσεις
<b>VPOS</b>														
<b>Message</b>														
lang	O	O	O	O	O	O								
messageld	R	R	R	R	R	R								
version	R	R	R	R	R	R								
<b>Authentication</b>														
Mid	R	R	R	R	R	R							R	
Digest	R	R	R	R	R	R								
Password	C	C	C	C	C	C							C	Χρησιμοποιείται μόνο σε περίπτωση που δεν στέλνεται το digest
<b>OrderInfo</b>														
DeviceCategory														
OrderId	R	R	R	R	R									
OrderDesc	O	O												
OrderAmount	R	R	R	R	R									
Currency	R	R	R	R	R									
PayerEmail	O	O												
PayerPhone	O	O												
AddFraudScore	C	C												
BlockScore	C	C												Χρησιμοποιούνται μόνο σε περίπτωση που έχει ενεργοποιηθεί ο Fraud Score Server (Μελλοντικά διαθέσιμη υπηρεσία)
Var1	O	O												
Var2	O	O												
Var3	O	O												
Var4	O	O												
Var5	O	O												
MOTO	O	O												
<b>BillingAddress</b>														
Country	O	O												
State	O	O												
Zip	O	O												

City	O	O																	
Address	O	O																	
<b>ShippingAddress</b>	O	O																	
Country	O	O																	
State	O	O																	
Zip	O	O																	
City	O	O																	
Address	O	O																	
<b>PaymentInfo</b>																			
PayMethod	O	O	O	O	O														
CardPan	R	R	O	O	O														
CardHolderName	O	O																	
CardExpDate	R	R																	
CardCvv2	R	R																	
RecurringIndicator	C																		Η τιμή R υποδηλώνει ότι πρόκειται για επαναλαμβανόμενη πληρωμή
<b>RecurringParameters</b>	C																		
ExtRecurringfrequency	C																		Απαραίτητη εφόσον έχει αποσταλεί η τιμή R στη μεταβλητή RecurringIndicator
ExtRecurringenddate	C																		
<b>InstallmentParameters</b>	C	C																	Απαραίτητο εφόσον η συναλλαγή είναι με δόσεις
ExtInstallmentoffset	C	C																	Απαραίτητο εφόσον η συναλλαγή είναι με δόσεις
ExtInstallmentperiod	C	C																	Απαραίτητο εφόσον η συναλλαγή είναι με δόσεις
<b>ThreeDSecure</b>																			
EnrollmentStatus	C	C																	
AuthenticationStatus	C	C																	
CAVV	C	C																	
XID	C	C																	
ECI	C	C																	
<b>TransactionInfo</b>																			
OrderId										R									
Operation										R									

Response message														
Field element/ Response	SaleRequest	Authorisation Request	CaptureRequest	RefundRequest	CancelRequest	RecurringOperationRequest	SaleResponse	AuthorisationResponse	CaptureResponse	RefundResponse	CancelResponse	RecurringOperationResponse	RecurringNotification	Παρατηρήσεις
<b>VPOS</b>														
<b>Message</b>														
lang							O	O	O	O	O	O	O	
messageld							R	R	R	R	R	R	R	
version							R	R	R	R	R	R	R	
Digest							R	R	R	R	R	R	R	
<b>Response</b>														
OrderId							R	R	R	R	R	R	R	
OrderAmount							R	R	R	R	R		R	
Currency							R	R	R	R	R		R	
PaymentTotal							R	R	R	R	R		R	
Status							R	R	R	R	R	R	R	
TxId							C	C	C	C	C		R	
Sequence													R	
SeqTxId													R	
PaymentRef							C	C	C	C	C		C	Στέλνεται εφόσον είναι διαθέσιμο
RiskScore							O	O						
ErrorCode							C	C	C	C	C	C	C	Στέλνεται σε περίπτωση που η μεταβλητή Status έχει την τιμή "ERROR"
Description							O	O	O	O	O	O	O	
OriginalXML														

Ακολουθούν παραδείγματα μηνυμάτων XML request και XML response για συναλλαγές 3D Secure.

### Παράδειγμα Request με 3D Secure

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><VPOS
xmlns="http://www.modirum.com/schemas"><Message messageld="1384766095985"
version="1.0"><SaleRequest><Authentication><Mid>9496025</Mid></Authentication><OrderInfo><O
rderId>1384766088960</OrderId><OrderDesc></OrderDesc><OrderAmount>1.25</OrderAmount><
Currency>EUR</Currency><PayerEmail></PayerEmail></OrderInfo><PaymentInfo><PayMethod>vis
a</PayMethod><CardPan>4509036603504004</CardPan><CardExpDate>1601</CardExpDate><Ca
rdCvv2>345</CardCvv2><CardHolderName>John
Smith</CardHolderName><ThreeDSecure><EnrollmentStatus>Y</EnrollmentStatus><Authentication
Status>Y</AuthenticationStatus><CAVV>AAABBgJ3lgABOEdmCHciEH8AAAE=</CAVV><XID>MDA
wMDAwMDEzODQ3NjU0ODY2ODk=</XID><ECI>05</ECI></ThreeDSecure></PaymentInfo></Sale
Request></Message><Digest>XaPzslxleWPdpX7RrMR6yJo/H8OY=</Digest></VPOS>
```

**Παράδειγμα Response με 3D Secure**

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><VPOS
xmlns="http://www.modirum.com/schemas"><Message messageId="1384766095985"
version="1.0"><SaleResponse><OrderId>1384766088960</OrderId><OrderAmount>1.25</OrderAm
ount><Currency>EUR</Currency><PaymentTotal>1.25</PaymentTotal><Status>CAPTURED</Statu
s><TxId>312341</TxId><PaymentRef>022018</PaymentRef><RiskScore>0</RiskScore><Descriptio
n>OK, CAPTURED response code
00</Description></SaleResponse></Message><Digest>UhMjwPmzE8SCBqgEfgaGITmihGw=</Diges
t></VPOS>
```

## 4. Υπολογισμός Digest

Ο έλεγχος εγκυρότητας είναι ένας επιπλέον όρος ασφάλειας που αποτρέπει την επεξεργασία των εσφαλμένων συναλλαγών. Κάποιος που προσπαθεί να πραγματοποιήσει μια απάτη θα προσπαθήσει να αλλοιώσει τα στοιχεία της συναλλαγής και να αποστείλει πλαστές αξίες (π.χ. μικρότερος λογαριασμός, άλλο νόμισμα κ.λπ.). Το σύστημα της υπηρεσίας Alpha e-Commerce, κάνοντας έλεγχο στις παραμέτρους που λαμβάνει, μπορεί να αποτρέψει αυτές τις προσπάθειες.

Η δικλείδα ασφαλείας για τις συναλλαγές μεταξύ του συστήματος της υπηρεσίας Alpha e-Commerce και της επιχείρησης κατά τη διάρκεια της συναλλαγής είναι το πεδίο DIGEST.

Τα βήματα της διαδικασίας είναι:

- 1) Η τράπεζα για κάθε συνεργαζόμενη επιχείρηση εκδίδει ένα μοναδικό κωδικό, το SHARED SECRET KEY, το οποίο και κοινοποιεί στην επιχείρηση
- 2) Το σύστημα της τράπεζας ελέγχει σε κάθε συναλλαγή την τιμή των πεδίων που αποστέλλει η checkout σελίδα σε συνδυασμό με το πεδίο digest
- 3) Εάν ο έλεγχος των πεδίων και του digest είναι επιτυχής ο πελάτης δρομολογείται στην σελίδα εισαγωγής των στοιχείων της κάρτας για την ολοκλήρωση της συναλλαγής (σε περίπτωση παραποιημένων πεδίων η συναλλαγή διακόπτεται)

Σημειώνεται ότι η διαδικασία επιβεβαίωσης δεν γίνεται αντιληπτή στον κάτοχο της κάρτας.

### 4.1. Υπολογισμός Digest για το MPI Request

Ο υπολογισμός του Digest για το MPI Request απαιτεί τα εξής:

#### 1) Τις τιμές των πεδίων που αποστέλλονται στην φόρμα (post\_fields\_values)

Με βάση όλες τις τιμές των πεδίων που αποστέλλονται στο MPI Request θα πρέπει να δημιουργηθεί ένα string (αναλύεται παρακάτω)

#### 2) Το SHARED SECRET KEY

Το SHARED SECRET KEY είναι το κλειδί μεταξύ επιχείρησης και τράπεζας, για την ασφαλή μεταφορά των στοιχείων της συναλλαγής. Επίσης χρησιμοποιείται και για το κλείδωμα των δεδομένων που αποστέλλονται στο σύστημα της τράπεζας. Το SHARED SECRET KEY το παρέχει η τράπεζα και πρέπει να συμπεριληφθεί στο τέλος του προηγούμενου string που δημιουργήθηκε

#### 3) Τις συναρτήσεις base64 και sha-1

- a. base64: Μέθοδος κωδικοποίησης που μετατρέπει δυαδικά δεδομένα σε κείμενο ASCII και αντίστροφα
- b. sha-1: hash αλγόριθμος μιας κατεύθυνσης, που χρησιμοποιείται για τη δημιουργία ψηφιακών υπογραφών

### Προσοχή:

Τεχνολογίες JavaScript (ή παρόμοιες), είναι πιθανόν να εμφανίσουν το shared secret key σε τρίτους, και για το λόγο αυτό ΔΕΝ συνιστάται η δημιουργία του Digest μόνο με αυτές. Αντίθετα server side scripting τεχνολογίες (π.χ. PHP, ASP) παρέχουν μεγαλύτερη ασφάλεια και συνιστώνται για τη δημιουργία e-shops.

Τα βήματα υπολογισμού του digest είναι:

1. Ταξινόμηση μεταβλητών ακριβώς ίδια με τον πίνακα μεταβλητών του MPI Request
2. Δημιουργία ενός ενιαίου String με τις τιμές των μεταβλητών του MPI Request
3. Προσθήκη shared secret key
4. Κρυπτογράφηση του string και παραγωγή της τιμής στη μεταβλητή digest

### 1. Ταξινόμηση μεταβλητών ακριβώς ίδια με τον πίνακα μεταβλητών του MPI Request

Στο MPI Request πρέπει να σταλούν όλα τα υποχρεωτικά πεδία και κάποια από τα προαιρετικά. Η επιχείρηση έχει τη δυνατότητα να επιλέξει ποια από τα προαιρετικά πεδία θα αποστείλει. Σε κάθε περίπτωση, τα πεδία θα πρέπει να ταξινομηθούν με βάση τον πίνακα μεταβλητών του MPI Request.

### 2. Δημιουργία ενός ενιαίου String με τις τιμές του πίνακα μεταβλητών του MPI Request

Θα πρέπει να δημιουργηθεί ένα string με όλες τις τιμές των πεδίων που αποστέλλονται στο MPI Request:

- Οι τιμές στο string δεν θα έχουν κάποιο διαχωριστικό, αλλά θα προστίθενται η μία ακριβώς μετά την άλλη
- Στο string θα πρέπει να συμπεριληφθούν όλες οι τιμές των πεδίων που αποστέλλονται
- Η σειρά των μεταβλητών θα πρέπει να είναι ίδια με αυτή στον πίνακα μεταβλητών του MPI Request
- Η κωδικοποίηση των τιμών στο string πρέπει να είναι UTF-8. Αυτό μπορεί να επιτευχθεί με την χρήση συναρτήσεων που παρέχει η γλώσσα που υλοποιεί την λύση κάθε φορά (πχ utf8\_encode για php ή Encoding.Convert για .NET )

### 3. Προσθήκη shared secret key

Το shared secret key είναι το κλειδί μεταξύ επιχείρησης και τράπεζας, για την ασφαλή μεταφορά των στοιχείων της συναλλαγής και πρέπει να συμπεριληφθεί στο τέλος του προηγούμενου string που δημιουργήθηκε.

**Προσοχή :** Το shared secret key δεν αποστέλλεται στο σύστημα της τράπεζας, αλλά χρησιμοποιείται μόνο στο παραπάνω string.

### 4. Κρυπτογράφηση του string και παραγωγή της τιμής της μεταβλητής digest

Το τελικό βήμα για την δημιουργία του digest είναι η χρήση των συναρτήσεων base64 και sha-1. Ο τρόπος υπολογισμού είναι:

```
base64 (sha-1 (utf8bytes( string* ) ) )  
* string = "τιμές post πεδίων + shared secret key"
```

#### Παράδειγμα κώδικα για χρήση Java:

```
MessageDigest mdigest = MessageDigest.getInstance("SHA-1");  
byte[] digestResult =digest.digest(concatString.getBytes("UTF-8"));  
String calculatedDigest = Base64.encode(digestResult);
```

#### Παράδειγμα κώδικα για χρήση .NET:

```
System.Security.Cryptography.SHA1 sha = new  
System.Security.Cryptography.SHA1 CryptoServiceProvider();  
byte[] hashValue = sha.ComputeHash(System.Text.Encoding.UTF8.GetBytes(valueToDigest) );  
string digest = System.Convert.ToBase64String(hashValue);
```

## 4.2. Υπολογισμός Digest XML μηνύματος

Για τη δημιουργία του digest XML μηνύματος απαιτούνται τα εξής:

### 1) Το XML element <Message>

- Το περιεχόμενο του <Message> θα πρέπει να μετατραπεί σε κανονική μορφή. Η μέθοδος που θα πρέπει να χρησιμοποιηθεί είναι η <http://www.w3.org/TR/2001/REC-xml-c14n-20010315>).
- Η κωδικοποίηση πρέπει να είναι UTF-8.

### 2) Το SHARED SECRET KEY

Το SHARED SECRET KEY είναι το κλειδί μεταξύ επιχείρησης και τράπεζας, για την ασφαλή μεταφορά των στοιχείων της συναλλαγής. Επίσης χρησιμοποιείται και για το κλείδωμα των δεδομένων που αποστέλλονται στο σύστημα της τράπεζας. Το SHARED SECRET KEY το παρέχει η τράπεζα και πρέπει να συμπεριληφθεί στο τέλος του προηγούμενου string που δημιουργήθηκε

### 3) Οι συναρτήσεις base64 και sha-1

- base64: Μέθοδος κωδικοποίησης που μετατρέπει δυαδικά δεδομένα σε κείμενο ASCII και αντίστροφα
- sha-1: hash αλγόριθμος μιας κατεύθυνσης, που χρησιμοποιείται για τη δημιουργία ψηφιακών υπογραφών

Τα βήματα υπολογισμού digest XML μηνύματος είναι:

1. Δημιουργία αρχικού XML
2. Επιλογή του περιεχομένου στο element <Message>
3. Κανονικοποίηση του element <Message>
4. Προσθήκη του shared secret key στο τέλος του element <Message> και δημιουργία ενός ενιαίου String
5. Μετατροπή σε UTF8
6. Κρυπτογράφηση του string και παραγωγή της τιμής στη μεταβλητή digest
7. Εισαγωγή της τιμής digest στο element <Digest> του αρχικού XML

### Αναλυτικότερα:

1. Δημιουργία αρχικού XML.

Όλα τα υποχρεωτικά πεδία και κάποια από τα προαιρετικά. Η επιχείρηση έχει την δυνατότητα να επιλέξει ποια από τα προαιρετικά πεδία θα αποστείλει.

Παράδειγμα:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<VPOS xmlns="http://www.modirum.com/schemas">
```



```
<Message lang="en" messageId="1370004820649" version="1.0">
<SaleRequest>
<Authentication>
<Mid>0000001</Mid>
</Authentication>
<OrderInfo>
<OrderId>1369981694782</OrderId>
<OrderDesc>
</OrderDesc>
<OrderAmount>1.25</OrderAmount>
<Currency>EUR</Currency>
<PayerEmail>andri.kruus@modirum.com</PayerEmail>
</OrderInfo>
<PaymentInfo>
<PayMethod>visa</PayMethod>
<CardPan>
</CardPan>
<CardExpDate>1406</CardExpDate>
<CardCvv2>756</CardCvv2>
</PaymentInfo>
</SaleRequest>
</Message>
</VPOS>
```

2. Επιλογή του περιεχομένου στο element <Message>.

Πρέπει να επιλεγεί το element <Message>.

**ΠΡΟΣΟΧΗ:** Θα πρέπει να προστεθεί το namespace στο element

Παράδειγμα:

```
<Message xmlns="http://www.modirum.com/schemas"
lang="en" messageId="1370004820649" version="1.0">
  <SaleRequest>
    <Authentication>
      <Mid>0000001</Mid>
    </Authentication>
    <OrderInfo>
      <OrderId>1369981694782</OrderId>
      <OrderDesc>
      </OrderDesc>
      <OrderAmount>1.25</OrderAmount>
      <Currency>EUR</Currency>
      <PayerEmail>andri.kruus@modirum.com</PayerEmail>
    </OrderInfo>
    <PaymentInfo>
      <PayMethod>visa</PayMethod>
      <CardPan>
      </CardPan>
      <CardExpDate>1406</CardExpDate>
      <CardCvv2>756</CardCvv2>
    </PaymentInfo>
  </SaleRequest>
</Message>
```

### 3. Κανονικοποίηση του element <Message>

Παράδειγμα:

```
<Message xmlns="http://www.modirum.com/schemas" lang="en"
messageId="1370004820649"version="1.0"><SaleRequest><Authentication><Mid>0000001</Mid></
Authentication><OrderInfo><OrderId>1369981694782</OrderId><OrderDesc></OrderDesc><OrderA
mount>1.25</OrderAmount><Currency>EUR</Currency><PayerEmail>andri.kruus@modirum.com</
PayerEmail></OrderInfo><PaymentInfo><PayMethod>visa</PayMethod><CardPan></CardPan><Ca
rdExpDate>1406</CardExpDate><CardCvv2>756</CardCvv2></PaymentInfo></SaleRequest></Mes
sage>
```

### 4. Προσθήκη του shared secret key στο τέλος του element <Message> και δημιουργία ενός ενιαίου String

Παράδειγμα:

```
<Message xmlns="http://www.modirum.com/schemas" lang="en"
messageId="1370004820649"version="1.0"><SaleRequest><Authentication><Mid>0000001</Mid></
Authentication><OrderInfo><OrderId>1369981694782</OrderId><OrderDesc></OrderDesc><OrderA
mount>1.25</OrderAmount><Currency>EUR</Currency><PayerEmail>andri.kruus@modirum.com</
PayerEmail></OrderInfo><PaymentInfo><PayMethod>visa</PayMethod><CardPan></CardPan><Ca
rdExpDate>1406</CardExpDate><CardCvv2>756</CardCvv2></PaymentInfo></SaleRequest></Mes
sage>SecRetDigest
```

### 5. Μετατροπή σε UTF8

Η κωδικοποίηση των τιμών στο string πρέπει να είναι UTF-8. Αυτό μπορεί να επιτευχθεί με την χρήση συναρτήσεων που παρέχει η γλώσσα που υλοποιεί την λύση κάθε φορά (πχ utf8\_encode για php ή Encoding.Convert για .NET).

### 6. Κρυπτογράφηση του string και παραγωγή της τιμής της μεταβλητής digest

Το τελικό βήμα για την δημιουργία του digest είναι η χρήση των συναρτήσεων base64 και sha-1. Η σειρά που χρησιμοποιούνται οι συναρτήσεις είναι :

- a. base64 (sha-1 (utf8bytes (string\*)))  
\* string = XML message + sharedsecret

**Digest = Base64(SHA1((utf8bytes(canonicalize(Message))+utf8bytes(sharedSecret)))**

Παράδειγμα:

```
<Message xmlns="http://www.modirum.com/schemas" lang="en" messageId="1370004820649"
version="1.0"><SaleRequest><Authentication><Mid>0000001</Mid></Authentication><OrderInfo><O
rderId>1369981694782</OrderId><OrderDesc></OrderDesc><OrderAmount>1.25</OrderAmount><
Currency>EUR</Currency><PayerEmail>andri.kruus@modirum.com</PayerEmail></OrderInfo><Pay
mentInfo><PayMethod>visa</PayMethod><CardPan></CardPan><CardExpDate>1406</CardExpDat
e><CardCvv2>756</CardCvv2></PaymentInfo></SaleRequest></Message>SecRetDigest
```

Digest= RzlvrA646BKH0MWCIA00s00hRWQ=

7. Εισαγωγή της τιμής digest στο element <Digest> του αρχικού XML και αποστολή

Παράδειγμα:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><VPOS
xmlns="http://www.modirum.com/schemas"><Message xmlns="http://www.modirum.com/schemas"
lang="en" messageId="1370004820649"
version="1.0"><SaleRequest><Authentication><Mid>0000001</Mid></Authentication><OrderInfo><O
rderId>1369981694782</OrderId><OrderDesc></OrderDesc><OrderAmount>1.25</OrderAmount><
Currency>EUR</Currency><PayerEmail>andri.kruus@modirum.com</PayerEmail></OrderInfo><Pay
mentInfo><PayMethod>visa</PayMethod><CardPan></CardPan><CardExpDate>1406</CardExpDat
e><CardCvv2>756</CardCvv2></PaymentInfo></SaleRequest></Message>SecRetDigest
<Digest>RzlvA646BKHoMWCIA0OsO0hRWQ=</Digest></VPOS>
```

## 5. Έλεγχος του digest στις απαντήσεις του MPI Response και του XML Response

Η επιχείρηση, για λόγους ασφαλείας, πρέπει να ελέγχει τις απαντήσεις που λαμβάνει τόσο από το MPI Response όσο και από το XML Response. Ο έλεγχος γίνεται με τη μεταβλητή Digest.

Στα responses, μαζί με τις υπόλοιπες μεταβλητές υπάρχει και η μεταβλητή digest, η οποία περιέχει κλειδωμένες τις απαντητικές μεταβλητές προς την επιχείρηση. Για να ελέγξει η επιχείρηση την απάντηση που θα δεχθεί, θα πρέπει να δημιουργήσει το digest με τις μεταβλητές που λαμβάνει και να το συγκρίνει με το digest που της έχει στείλει η Τράπεζα.

**Προσοχή:** η τιμή της μεταβλητής digest που στέλνει η επιχείρηση στην τράπεζα, θα είναι διαφορετική από την τιμή της μεταβλητής digest που θα λάβει η επιχείρηση ως απάντηση (είτε στο MPI Response είτε στο XML Response), μιας και αφορά κλειδωμά διαφορετικών μεταβλητών. Επομένως, δεν θα πρέπει να γίνεται σύγκριση της τιμής της μεταβλητής του digest που στάλθηκε αρχικά από την επιχείρηση στην τράπεζα με την τιμή της μεταβλητής του digest που επέστρεψε η τράπεζα στην απάντησή της.

### 5.1. Έλεγχος του digest στις απαντήσεις του MPI Response

Η επιχείρηση θα πρέπει να έχει ετοιμάσει το σύστημά της έτσι ώστε να λάβει όλες τις μεταβλητές που αναφέρονται στον παρακάτω πίνακα.

#### Παράδειγμα

Απάντηση στην Confirmation σελίδα.

A/A	Post field	Post field value
1	version	2.0
2	merchantID	0000001
3	xid	K+3FGOC9xU28b4tC22XbCfAAAAA=
4	mdStatus	2
5	mdErrorMsg	N-status/Not enrolled from Directory Server: <a href="https://dsw.visa3dsecure.com/DSMsgServlet">https://dsw.visa3dsecure.com/DSMsgServlet</a>
6	txstatus	N
7	iReqCode	
8	iReqDetail	
9	vendorCode	
10	eci	
11	cavv	
12	cavvAlgorithm	
13	MD	1c1acf6f-0846-4160-8d2a-facc20898c88
14	digest	fM7Fww3ZfbEzNDNDPxo97s7zLnU=
15	PAResVerified	false
16	PAResSyntaxOK	false
17	veresEnrolledStatus	N
18	paresTxStatus	-

Έστω ότι το Shared Secret Key είναι: SecRetDigest

Για να ελέγξει η επιχείρηση την εγκυρότητα των μεταβλητών από το MPI Response σε αυτή, πρέπει να υπολογίσει εκ νέου το πεδίο της μεταβλητής του digest και να το συγκρίνει με αυτό που της έχει στείλει η Τράπεζα.

**ΠΡΟΣΟΧΗ:** Στον υπολογισμό του digest δεν πρέπει να ληφθούν υπόψη οι παρακάτω μεταβλητές:

15	PResVerified
16	PResSyntaxOK
17	veresEnrolledStatus
18	piresTxStatus

Εφαρμόζοντας τις συναρτήσεις έχουμε:

```
Digest = base64 (sha-1 (utf8bytes("2.00000001K+3FGOC9xU28b4tC22XbCfAAAAA=2N-status/Not enrolled from Directory Server: https://dsw.visa3dsecure.com/DSMsgServletN1c1acf6f-0846-4160-8d2a-facc20898c88SecRetDigest"))) )
```

Παρατηρούμε ότι η τιμή που προκύπτει είναι fM7Fww3ZfbEzNDNDPx097s7zLnU= η οποία και συμφωνεί με αυτή που έστειλε η τράπεζα στη μεταβλητή 14 του παραπάνω πίνακα.

## 5.2. Έλεγχος του digest στις απαντήσεις του XML Response

Η επιχείρηση θα πρέπει να έχει ετοιμάσει το σύστημά της έτσι ώστε να λάβει όλες τις μεταβλητές που αναφέρονται στον παρακάτω πίνακα.

### Παράδειγμα

Απάντηση μέσω XML

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><VPOS xmlns="http://www.modirum.com/schemas"><Message messageId="1370331022042" version="1.0"><SaleResponse><OrderId>1370330662800</OrderId><OrderAmount>1.25</OrderAmount><Currency>EUR</Currency><PaymentTotal>1.25</PaymentTotal><Status>REFUSED</Status><TxId>465101</TxId><PaymentRef></PaymentRef><RiskScore>12</RiskScore><Description>Refused, REFUSED response code 03</Description></SaleResponse></Message><Digest>li1d/h+pb7/TVICh9v39HxX7uqE=</Digest></VPOS>
```

Έστω ότι το Shared Secret Key είναι: SecRetDigest

Για να ελέγξει η επιχείρηση την εγκυρότητα των μεταβλητών από το XML Response σε αυτή, πρέπει να υπολογίσει εκ νέου το πεδίο της μεταβλητής του digest και να το συγκρίνει με αυτό που της έχει στείλει η Τράπεζα.

Απομονώνουμε το message element από το response, προσθέτοντας το attribute xmlns=<http://www.modirum.com/schemas> και στο τέλος το Shared Secret Key:

Εφαρμόζουμε τις συναρτήσεις:

Digest = base64 (sha-1 (utf8bytes(<Message xmlns="http://www.modirum.com/schemas" messageId="1370331022042" version="1.0"><SaleResponse><OrderId>1370330662800</OrderId><OrderAmount>1.25</OrderAmount><Currency>EUR</Currency><PaymentTotal>1.25</PaymentTotal><Status>REFUSED</Status><TxId>465101</TxId><PaymentRef></PaymentRef><RiskScore>12</RiskScore><Description>Refused, REFUSED response code 03</Description></SaleResponse></Message>SecRetDigest) ) )

παρατηρούμε ότι η τιμή που προκύπτει είναι:  
li1d/h+pB7/TVICH9v39HxX7uqE=

η οποία και συμφωνεί με αυτή που έστειλε η τράπεζα στο παραπάνω XML μήνυμα.

## 6. Παροχή δυνατότητας αναζήτησης με xml queries

Επιπλέον υπάρχει η δυνατότητα, σε όσες επιχειρήσεις το επιθυμούν, να μπορούν να ενημερώνονται άμεσα χωρίς την είσοδο τους στο Διαχειριστικό Εργαλείο BackOffice, μέσω ενός xml request που θα πραγματοποιούν, για τις συνολικές πληροφορίες κάποιας συναλλαγής.

Παράδειγμα xml request:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<VPOS xmlns="http://www.modirum.com/schemas">
<Message version="1.0" messageId="1430385661520">
<StatusRequest>
<Authentication>
<Mid>0000001</Mid>
</Authentication>
<TransactionInfo>
<TxId>1356471</TxId>
</TransactionInfo>
</StatusRequest>
</Message>
<Digest>xODeZzNn7mVev2nNe4hMFKeCz4=</Digest>
</VPOS>
```

Η επιχείρηση στέλνει το StatusRequest element καθώς και το TransactionInfo μαζί με το Txid της συναλλαγής που αναζητά.

Το XML Response που λαμβάνει είναι το ακόλουθο και αποτυπώνει το σύνολο των αποτελεσμάτων που απεικονίζονται και στο Διαχειριστικό Εργαλείο BackOffice:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<VPOS xmlns="http://www.modirum.com/schemas">
<Message version="1.0" messageId="1430385661520" timeStamp="2015-04-30T12:21:02.402+03:00">
<StatusResponse>
<TransactionDetails>
<OrderAmount>0.12</OrderAmount>
<Currency>EUR</Currency>
<PaymentTotal>0.12</PaymentTotal>
<Status>REFUSED</Status>
<TxId>1356471</TxId>
<PaymentRef>
</PaymentRef>
<Description>Refused, REFUSED response code 15</Description>
<TxType>PAYMENT</TxType>
<TxDate>2015-04-28T11:50:45.151+03:00</TxDate>
<TxStarted>2015-04-28T11:50:10.446+03:00</TxStarted>
<TxCompleted>2015-04-28T11:50:46.749+03:00</TxCompleted>
<Attribute name="MERCHANT NO">0000001</Attribute>
<Attribute name="USER IP">195.222.10.3</Attribute>
<Attribute name="CHANNEL">Redirection</Attribute>
<Attribute name="3D STATUS">1 - Fully authenticated</Attribute>
<Attribute name="SETTLEMENT STATUS">NA</Attribute>
<Attribute name="BATCH NO">28</Attribute>
<Attribute name="ISO response code">15</Attribute>
<Attribute name="ORDER DESCRIPTION" />
```

```
<Attribute name="CARD MASK PAN">4016#####0002</Attribute>
<Attribute name="ECOM-FLG">5</Attribute>
<Attribute name="ECI">05</Attribute>
<Attribute name="PAYEREMAIL">demo@modirum.com</Attribute>
<Attribute name="PAYERPHONE">+372 123 1234</Attribute>
<Attribute name="BILLCOUNTRY">FI</Attribute>
<Attribute name="BILLSTATE">Harjumaa</Attribute>
<Attribute name="BILLZIP">76543</Attribute>
<Attribute name="BILLADDRESS">Billto tn 6-9</Attribute>
<Attribute name="SHIPCOUNTRY">FI</Attribute>
<Attribute name="SHIPSTATE">Harjumaa</Attribute>
<Attribute name="SHIPZIP">12345</Attribute>
<Attribute name="SHIPADDRESS">Viru tn 6-9</Attribute>
<Attribute name="BONUS PARTICIPATION">No</Attribute>
</TransactionDetails>
</StatusResponse>
</Message>
<Digest>9owiYEcxlQs9nVPH9K8UsJfSKzA=</Digest>
</VPOS>
```



## ΠΑΡΑΡΤΗΜΑ

### A. ΥΠΟΔΕΙΓΜΑΤΑ E-MAIL (ΕΠΙΧΕΙΡΗΣΗΣ ΚΑΙ ΠΕΛΑΤΗ)

#### A.1 E-MAIL ΕΠΙΧΕΙΡΗΣΗΣ (MERCHANT E-MAIL)

Όταν η πληρωμή είναι επιτυχής, είναι προαιρετικά εφικτή η αποστολή e-mail στην επιχείρηση, έτσι ώστε να ενημερωθεί για τη νέα συναλλαγή. Το περιεχόμενο του e-mail περιέχει έναν συνδυασμό κειμένου και μεταβλητών (οι μεταβλητές φαίνονται με κόκκινα γράμματα) και είναι το παρακάτω:

**Θέμα:** Υπηρεσία Alpha e-Commerce – Ειδοποίηση για νέα ηλεκτρονική συναλλαγή

Έχετε μια νέα ηλεκτρονική συναλλαγή.

#### Στοιχεία Εμπόρου

Όνομα Εμπόρου: *Merchant Name*  
Κωδικός Εμπόρου: *Merchant No*  
Ιστοσελίδα Εμπόρου: *Merchant URL*

#### Στοιχεία Συναλλαγής

Ημερομηνία Συναλλαγής: *Date started*  
Κωδικός Συναλλαγής: *TX ID*  
Κωδικός Παραγγελίας: *Order ID*  
Κωδικός Έγκρισης: *Payment Reference*  
Ποσό Παραγγελίας: *Order Amount*  
Τύπος: *Type*  
Τρόπος Πληρωμής: *Payment Method*  
Αριθμός Δόσεων: *Number of Installments*  
Συχνότητα Επαναλαμβανόμενων Πληρωμών: *Number of Recurring Frequency*  
Αριθμός Επαναλαμβανόμενων Πληρωμών: *Number of Recurring Sequence*

Σας υπενθυμίζουμε πως, εφόσον ο τύπος της συναλλαγής είναι PRE-AUTHORISATION, θα πρέπει να προχωρήσετε στη χρέωση (CAPTURE) της μέσα σε 7 ημερολογιακές ημέρες.

#### Στοιχεία Παραγγελίας

Περιγραφή παραγγελίας: *Order Description*  
Φοροκάρτα: *Tax Id*  
Var2: *Var2*  
Var3: *Var3*  
Var4: *Var4*  
Var5: *Var5*

#### Στοιχεία Πελάτη

Όνομ/πώνυμο: *Cardholder Name*  
Αριθμός Κάρτας: *Card Number (Masked)*  
E-mail: *Payer e-mail*  
Τηλέφωνο: *Payer Phone*  
IP: *User IP*

Φιλικά,  
Alpha e-Commerce  
[ecommerce@alpha.gr](mailto:ecommerce@alpha.gr)

## A.2 E-MAIL ΠΕΛΑΤΗ (CUSTOMER E-MAIL)

Όταν η πληρωμή είναι επιτυχημένη, είναι προαιρετικά εφικτή η αποστολή e-mail στον πελάτη για την επιβεβαίωση της πληρωμής του. Το περιεχόμενο του e-mail περιέχει έναν συνδυασμό κειμένου και μεταβλητών (οι μεταβλητές φαίνονται με κόκκινα γράμματα) και είναι το παρακάτω:

**Θέμα:** Επιβεβαίωση συναλλαγής από το ηλεκτρονικό κατάστημα *Merchant Name* με κωδικό *TX ID*

Αγαπητέ/ή *Name on Card*

Το παρόν e-mail επιβεβαιώνει ότι η συναλλαγή που πραγματοποιήσατε στο ηλεκτρονικό κατάστημα *Merchant Name* διεκπεραιώθηκε με επιτυχία από την πλατφόρμα ηλεκτρονικών πληρωμών Alpha e-Commerce της Alpha Bank. Τα στοιχεία της συναλλαγής σας είναι:

Ηλεκτρονικό Κατάστημα:	<i>Merchant Name</i>
Ιστοσελίδα Επιχείρησης:	<i>Merchant URL</i>
Κωδικός Συναλλαγής:	<i>TX ID</i>
Ποσό Παραγγελίας:	<i>Order Amount</i>
Ημερομηνία Συναλλαγής:	<i>Date started</i>
Τύπος Κάρτας:	<i>Payment Method</i>
Κωδικός Παραγγελίας:	<i>Order ID</i>
Κωδικός Έγκρισης:	<i>Payment Reference</i>
Αριθμός Δόσεων:	<i>Number of Installments</i>
Συχνότητα Επαναλαμβανόμενων Πληρωμών:	<i>Number of Recurring Frequency</i>
Αριθμός Επαναλαμβανόμενων Πληρωμών:	<i>Number of Recurring Sequence</i>

Το παρόν e-mail επιβεβαιώνει μόνο την επιτυχή επεξεργασία της συναλλαγής σας μέσω του συστήματος της υπηρεσίας Alpha e-Commerce της Alpha Bank. Σε καμία περίπτωση δεν επιβεβαιώνει ότι η παραγγελία σας έχει γίνει αποδεκτή από το ηλεκτρονικό κατάστημα *Merchant Name*. Είναι αποκλειστική ευθύνη του ηλεκτρονικού καταστήματος να σας ενημερώσει για την αποδοχή της παραγγελίας σας και να σας παραδώσει τα προϊόντα / υπηρεσίες που έχετε παραγγείλει.

Παρακαλούμε, κρατήστε αυτό το e-mail για τυχόν μελλοντική αναφορά.

Με εκτίμηση,

Υπηρεσία Alpha e-Commerce  
Alpha Bank

**B. ΥΠΟΔΕΙΓΜΑ ΑΠΟΔΕΙΞΗΣ ΣΥΝΑΛΛΑΓΗΣ ΑΓΟΡΑΣ (PURCHASE TRANSACTION RECEIPT)**

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΑΓΟΡΑΣΤΗ / PURCHASER NAME	
ΑΡΙΘΜΟΣ ΣΥΝΑΛΛΑΓΗΣ / ORDER I.D.	
ΕΠΩΝΥΜΙΑ ΕΠΙΧΕΙΡΗΣΗΣ / MERCHANT NAME	
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΕΠΙΧΕΙΡΗΣΗΣ / MERCHANT ON-LINE ADDRESS	
ΠΕΡΙΓΡΑΦΗ ΕΜΠΟΡΕΥΜΑΤΩΝ – ΥΠΗΡΕΣΙΩΝ / DESCRIPTION OF MERCHANTISE - SERVICES	
ΠΟΣΟ ΑΓΟΡΑΣ / TRANSACTION AMOUNT	
ΗΜΕΡΟΜΗΝΙΑ ΣΥΝΑΛΛΑΓΗΣ / TRANSACTION DATE	
ΝΟΜΙΣΜΑ / CURRENCY	
ΑΡΙΘΜΟΣ ΕΓΚΡΙΣΗΣ / AUTHORIZATION CODE	
E.C. (Electronic Commerce)*	Η ένδειξη αυτή τίθεται στη θέση υπογραφής του κατόχου.
ΠΟΛΙΤΙΚΗ ΑΚΥΡΩΣΗΣ / CANCELLATION POLICY	Αναφέρεται αναλυτικά η πολιτική της Επιχείρησης όσον αφορά τις ακυρώσεις, επιστροφές υπηρεσιών, επιστροφές χρημάτων.

**Γ. ΜΗΝΥΜΑΤΑ ΛΑΘΟΥΣ**

Κατά την εκτέλεση συναλλαγών (δοκιμαστικών ή παραγωγής) ενδέχεται να εμφανιστούν κωδικοί και μηνύματα λάθους. Η παρακάτω λίστα περιλαμβάνει τα πιο συχνά μηνύματα λάθους.

M1 – Invalid merchant id

M2 – Authentication failed (wrong password or digest)

SE – System Error (message contains error id, system or configuration error to be investigated)

XE – Invalid XML request not parseable or does not validate

I0 – Invalid or unsupported request

I1 – Message contains invalid data item

I2 – Message contains invalid installment parameters

I3 – Message contains invalid recurring parameters

I4 (Ο κωδικός λάθους I4 έχει τις παρακάτω υποπεριπτώσεις)

- Μη έγκυρη κάρτα / Card PAN invalid
- Η κάρτα σας δεν αναγνωρίζεται από το σύστημα / Your card is not recognized by system
- Η κάρτα δεν αντιστοιχεί στον τύπο πληρωμής που επιλέχθηκε / Card does not match payment type selected
- Η κάρτα σας δεν έγινε δεκτή, παρακαλώ χρησιμοποιήστε άλλη κάρτα / Sorry, this card cannot be accepted, please use another card
- Η κάρτα σας δεν συμμετέχει σε προγράμματα άτοκων δόσεων / Sorry, this card cannot be accepted for installment payments, use another card

- Η κάρτα σας δεν συμμετέχει σε προγράμματα παγίων εντολών / Sorry, this card can not accpeted for recurring payments, use another card
- Μη έγκυρο CVV / Invalid CVV
- Απαιτείται η εισαγωγή του κωδικού επιβεβαίωσης (CVV) / Security Code (CVV) Required
- Μη έγκυρη ημερομηνία λήξης / Invalid expiration date

I5 - Message contains invalid expiration date card data

I6 – Selected payment method does is not supported or not matching the payment card

O1 – Operation is not allowed because logic is violated or wrong amounts

O2 – Original transaction is not found to perform operation.

#### Δ. ΚΩΔΙΚΟΙ ΚΑΙ ΛΕΚΤΙΚΑ ΑΠΟΡΡΙΨΗΣ ΣΥΝΑΛΛΑΓΩΝ

Κατά την εκτέλεση συναλλαγών (δοκιμαστικών ή παραγωγής) σε περίπτωση απόρριψης εμφανίζονται κωδικοί και λεκτικά απόρριψης στη σελίδα του Διαχειριστικού Εργαλείου BackOffice της υπηρεσίας Alpha e-Commerce της Τράπεζας, καθώς και στη μεταβλητή “description” του response μηνύματος που στέλνει η Τράπεζα στην επιχείρηση. Η παρακάτω λίστα περιλαμβάνει τα κυριότερα λεκτικά απόρριψης και τους κωδικούς.

Κωδικός	Λεκτικό
00	APPROVED OR COMPLETED SUCCESSFULLY
01	REFER TO CARD ISSUER
02	REFER TO SPECIAL CONDITIONS FOR CARD ISSUER
03	INVALID MERCHANT
04	PICK-UP
05	DO NOT HONOR
06	ERROR
08	HONOR WITH IDENTIFICATION
11	APPROVED (VIP)
12	INVALID TRANSACTION
13	INVALID AMOUNT
14	INVALID CARD NUMBER (NO SUCH NUMBER)
15	NO SUCH ISSUER
30	FORMAT ERROR
31	BANK NOT SUPPORTED BY SWITCH
33	EXPIRED CARD
36	RESTRICTED CARD
38	ALLOWABLE PIN TRIES EXCEEDED
41	LOST CARD
43	STOLEN CARD, PICK UP
51	NOT SUFFICIENT FUND
54	EXPIRED CARD
55	INCORRECT PERSONAL IDENTIFICATION NUMBER
56	NO RECORD FOUND
57	TRANSACTION NOT PERMITTED TO CARDHOLDER
61	EXCEEDS WITHDRAWAL AMOUNT LIMIT



62	RESTRICTED CARD
65	EXCEEDS WITHDRAWAL FREQUENCY LIMIT
68	RESPONSE RECEIVED TOO LATE
75	ALLOWABLE NUMBER OF PIN TRIES EXCEEDED
76	APPROVED COUNTRY CLUB
77	APPROVED PENDING IDENTIFICATION (SIGN PAPER DRAFT)
78	APPROVED BLIND
79	APPROVED ADMINISTRATIVE TRANSACTION
80	APPROVED NATIONAL NEG HIT OK
81	APPROVED COMMERCIAL
82	RESERVED FOR PRIVATE USE
83	NO ACCOUNTS
84	NO PBF
85	PBF UPDATE ERROR
86	INVALID AUTHORIZATION TYPE
87	BAD TRACK DATA
88	PTLF ERROR
89	INVALID ROUTE SERVICE
94	DUPLICATE TRANSACTION
N0	UNABLE TO AUTHORIZE
N1	INVALID PAN LENGTH
N2	PREAUTHORIZATION FULL
N3	MAXIMUM ONLINE REFUND REACHED
N4	MAXIMUM OFFLINE REFUND REACHED
N5	MAXIMUM CREDIT PER REFUND REACHED
N6	MAXIMUM REFUND CREDIT REACHED
N7	CUSTOMER SELECTED NEGATIVE FILE REASON
N8	OVER FLOOR LIMIT
N9	MAXIMUM NUMBER OF REFUND CREDIT
O1	FILE PROBLEM
O2	ADVANCE LESS THAN MINIMUM
O3	DELINQUENT
O4	OVER LIMIT TABLE
O5	PIN REQUIRED
O6	MOD 10 CHECK
O7	FORCE POST
O8	BAD PBF
O9	NEG FILE PROBLEM
P0	CAF PROBLEM
P1	OVER DAILY LIMIT
P2	CAPF NOT FOUND
P3	ADVANCE LESS THAN MINIMUM
P4	NUMBER TIMES USED
P5	DELINQUENT
P6	OVER LIMIT TABLE
P7	ADVANCE LESS THAN MINIMUM
P8	ADMINISTRATIVE CARD NEEDED
P9	ENTER LESSER AMOUNT
Q0	INVALID TRANSACTION DATE
Q1	INVALID EXPIRATION DATE
Q2	INVALID TRANSACTION CODE



Q3	ADVANCE LESS THAN MINIMUM
Q4	NUMBER TIMES USED
Q5	DELINQUENT
Q6	OVER LIMIT TABLE
Q7	AMOUNT OVER MAXIMUM
Q8	ADMINISTRATIVE CARD NOT
Q9	ADMINISTRATIVE CARD NOT
R0	APPROVED ADMINISTRATIVE
R1	APPROVED ADMINISTRATIVE
R2	APPROVED ADMINISTRATIVE
R3	CHARGEBACK, CUSTOMER FILE
R4	CHARGEBACK, CUSTOMER FILE
R5	CHARGEBACK, INCORRECT
R6	CHARGEBACK, INCORRECT
R7	ADMINISTRATIVE TRANSACTIONS
R8	CARD ON NATIONAL NEGATIVE FILE
S4	PTLF FULL
S5	CHARGEBACK APPROVED
S6	CHARGEBACK APPROVED
S7	CHARGEBACK ACCEPTED
S8	ADMN FILE PROBLEM
S9	UNABLE TO VALIDATE PIN; SECURITY MODULE IS DOWN
T1	INVALID CREDIT CARD ADVANCE INCREMENT
T2	INVALID TRANSACTION DATE
T3	CARD NOT SUPPORTED
T4	AMOUNT OVER MAXIMUM
T5	CAF STATUS = 0 OR 9
T6	BAD UAF
T7	CASH BACK EXCEEDS DAILY
T8	INVALID ACCOUNT