



Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής  
Πρόγραμμα Μεταπτυχιακών Σπουδών  
«Πληροφορική»

**Μεταπτυχιακή Διατριβή**

Τίτλος Διατριβής	<b>ΗΛΕΚΤΡΟΝΙΚΗ ΤΡΑΠΕΖΙΚΗ</b>
Όνοματεπώνυμο Φοιτητή	<b>Βασίλειος Φωτεινόπουλος</b>
Πατρώνυμο	<b>Δημήτριος</b>
Αριθμός Μητρώου	<b>ΜΠΠΛ/ 07013</b>
Επιβλέπων	<b>Σινανιώτη Αριστέα, Καθηγήτρια</b>

Μεταπτυχιακή Διατριβή

Βασίλειος Φωτεινόπουλος

**Τριμελής Εξεταστική Επιτροπή**

Σινανιώτη Αριστέα  
Καθηγήτρια

Φούντας Ευάγγελος  
Καθηγητής

Δουληγέρης Χρήστος  
Καθηγητής

**Θερμές Ευχαριστίες**

*Προς την επιβλέπουσα Καθηγήτρια κα Αριστέα Σινανιώτη-Μαυρουδή, για τον χρόνο που μου διέθεσε και για την βοήθεια της στην συλλογή των απαραίτητων για την ολοκλήρωση της εργασίας αυτής πληροφοριών τόσο βιβλιογραφικών όσο και κατευθυντήριων γραμμών.*

*Προς τον Πρόεδρο του Τμήματος Πληροφορικής, Καθηγητή και μέλος της επιτροπής κο Φούντα Ευάγγελο, όχι μόνο για το χρόνο που μου διέθεσε και τις παρατηρήσεις του, αλλά και για την ακαδημαϊκή βοήθεια που μου προσέφερε ως δάσκαλος μέχρι τώρα για να μπορέσω όχι να ολοκληρώσω απλώς αυτή την εργασία, αλλά για να είμαι σε θέση να την αρχίσω.*

*Προς τον Καθηγητή και μέλος της επιτροπής κο Δουληγέρη Χρήστο για το χρόνο που διέθεσε και τις παρατηρήσεις του πάνω στο κείμενο της εργασίας και την προτροπή του για διορθώσεις.*

*Θα ήθελα να ευχαριστήσω επίσης το κο Ιωάννη Φαρσαρώτα, για την βοήθεια και τις κατευθύνσεις που μου προσέφερε, ως άνθρωπος του τραπεζικού χώρου με μεγάλη εμπειρία τόσο στον τρόπο και τις διαδικασίες μέσα από τις οποίες διαμορφώνεται η σύγχρονη Τραπεζική στην εποχή μας, αλλά και στον τρόπο που θα έπρεπε να κινηθώ και να εργαστώ προσωπικά για την ολοκλήρωση αυτής της εργασίας με στόχο να μπορέσω να αντιληφθώ και να κατανοήσω όσο καλύτερα μπορούσα τις νέες προκλήσεις της εποχής.*

*Ευχαριστώ επίσης, τον φίλο και συμφοιτητή Γεώργιο Λίτινα, μεταπτυχιακό φοιτητή της κατεύθυνσης Δικτυοκεντρικά Συστήματα του Μεταπτυχιακού Προγράμματος του Τμήματος Ψηφιακών Συστημάτων για την βοήθεια του τόσο στην συγκέντρωση στοιχείων όσο και για τις ιδέες που ανταλλάξαμε πάνω σε αυτά, για την ολοκλήρωση της εργασίας αυτής και όχι μόνο.*

*Τέλος θα ήθελα να ευχαριστήσω το Πανεπιστήμιο Πειραιώς, για όλα τα μέχρι τώρα χρόνια της ακαδημαϊκής μου ζωής, από προπτυχιακός φοιτητής του Τμήματος Ψηφιακών Συστημάτων πριν μερικά χρόνια έως σήμερα που ολοκληρώνω αυτή την εργασία στα πλαίσια του Μεταπτυχιακού Προγράμματος Πληροφορικής του Τμήματος Πληροφορικής.*

*Με σεβασμό και εκτίμηση,*

*Βασίλειος Δ. Φωτεινόπουλος*

## ΠΕΡΙΛΗΨΗ

Στα ακόλουθα κεφάλαια της εργασίας, περιγράφεται τόσο ο τρόπος και το νομικό πλαίσιο λειτουργίας του τραπεζικού συστήματος στην Ελλάδα, και κατά συνέπεια οι αρχές και οι στόχοι λειτουργίας των ηλεκτρονικών υποκαταστημάτων των ελληνικών τραπεζών που δραστηριοποιούνται στον Ελληνικό χώρο, υπό το ελληνικό / ευρωπαϊκό δίκαιο, όσο και οι κίνδυνοι που αυτές διατρέχουν.

Επίσης θα αναφερθούμε στα διάφορα διατραπεζικά συστήματα που χρησιμοποιούνται στον ελληνικό και ευρωπαϊκό τραπεζικό χώρο και πως γίνεται η επόπτευση τους από την Τράπεζα της Ελλάδος και την Ευρωπαϊκή Κεντρική Τράπεζα αντίστοιχα.

Θα δούμε τόσο τις οργανωτικές ανακατατάξεις που έχουν γίνει, ή πρέπει να γίνουν, στο ελληνικό τραπεζικό σύστημα ώστε να αντιμετωπιστούν οι εσωτερικοί κίνδυνοι κατάρρευσης μιας τράπεζας στην νέα εποχή. Κίνδυνοι όπως, να μείνει πίσω τεχνολογικά και να ξεπεραστεί από την εποχή της, όσο και οργανωτικά/λειτουργικά προβλήματα που μπορούν να δημιουργηθούν εσωτερικά και να την βλάψουν ανεπανόρθωτα, αν δεν εντοπισθούν και αντιμετωπιστούν έγκαιρα.

Τέλος, παραθέτονται και αναλύονται, με όσο το δυνατό λιγότερους τεχνικούς όρους, οι κίνδυνοι που μπορούν να επηρεάσουν καταλυτικά, και κυριολεκτικά να καταστρέψουν ένα ηλεκτρονικό τραπεζικό κατάστημα και όχι μόνο, αν δεν εντοπισθούν και αντιμετωπιστούν εγκαίρως από το αρμόδιο τμήμα.

Επίσης παρατίθενται, σύγχρονες τεχνικές αντιμετώπισης και λύσεις, τέτοιων συμβατικών και ασύμβατων απειλών οι οποίες έχουν αναπτυχθεί και προσπορηθεί από πολλούς διεθνής οργανισμούς που ασχολούνται με την ασφάλεια των ηλεκτρονικών συναλλαγών, τόσο των τραπεζικών όσο και εν γένει των συναλλαγών ηλεκτρονικού εμπορίου παγκοσμίως.

## ABSTRACT

In the following chapters, the method and the legal framework of the banking system in Greece, and consequently the principles and objectives of the operation of electronic branches of Greek banks operating in the Greek market, under the Greek / European law, and also the risks they run, are both described.

Another issue mentioned will be the various interbank systems used in Greek and European banking sector and how supervision is made by the Bank of Greece and the European Central Bank respectively.

We will also see the organizational realignments that have been or should be done in the Greek banking system so as to face the internal collapse of a bank in the new era. Hazards such as falling behind technologically and organizational / operational problems that can be created internally and cause serious damage if not detected and treated early.

Finally, with as few as possible technical terms, the risks that may affect catalytic and literally destroy an electronic bank branch and not only, if not identified and dealt with properly by the department, are listed and analyzed.

In the last section, modern management techniques and solutions are listed, for conventional and incompatible threats which have been developed and pretend from many international organizations dealing with the security of electronic transactions, both bank and in general the e-commerce transactions worldwide.

## **ΕΙΣΑΓΩΓΗ**

Μέσω του υπολογιστή μπορούμε πλέον να κάνουμε σχεδόν όλες τις τραπεζικές μας συναλλαγές εκτός από την ανάληψη μετρητών. Μπορούμε εύκολα και γρήγορα να πληρώσουμε σχεδόν όλους τους λογαριασμούς μας όπως τηλέφωνο, ΔΕΗ, την πιστωτική μας κάρτα κτλ με μια απλή κίνηση οποιαδήποτε ώρα του 24ώρου οποιαδήποτε ημέρα γρήγορα και από το σπίτι μας. Το μόνο που χρειάζεται να έχουμε είναι πρόσβαση στο internet και κωδικούς πρόσβασης στο λογαριασμό IBAN μας τους οποίους μας τους προμηθεύει η τράπεζα στην οποία διατηρούμε τον λογαριασμό μας.

Η διαδικασία αυτή του web-banking / τραπεζική μέσω διαδικτύου ή όπως εμπορικά ονομάζεται e-banking, υπερέρχει σε σχέση με τις άλλες δύο, του ATM και του phone banking που μέχρι πρόσφατα ήταν και οι μόνες εναλλακτικές μέθοδοι απομακρυσμένων τραπεζικών συναλλαγών.

Οι συναλλαγές που μπορούμε να κάνουμε σε ένα ATM είναι σχετικά απλές και γρήγορες, και αυτό γιατί η βασική είναι η ανάληψη μετρητών κατά βάση και σε δεύτερο επίπεδο η πληρωμή ορισμένων λογαριασμών. Οι υπόλοιπες συναλλαγές όπου μπορούν να γίνουν από ένα ATM είναι συμπλήρωμα αυτών των δύο πχ οι τελευταίες κινήσεις του λογαριασμού ή ερώτηση υπολοίπου.

Μέσω του phone banking οι επιλογές μας είναι ακόμα πιο περιορισμένες. Είναι κατά βάση συναλλαγές που αφορούν πιστωτικές κάρτες και είναι αρκετά αυτοματοποιημένες και το μόνο που χρειάζεται από εμάς είναι να ακολουθήσουμε τις φωνητικές οδηγίες για να ολοκληρώσουμε την συναλλαγή μας.

Στο e-banking όπως είπαμε μπορούμε να κάνουμε σχεδόν τα πάντα εκτός από ανάληψη χρημάτων. Μπορούμε να μεταφέρουμε χρήματα να αποπληρώσουμε δόσεις καρτών ή δανείων, να πληρώσουμε λογαριασμούς ή και να διαχειριστούμε το χαρτοφυλάκιο μας.

Για να τα κάνουμε όλα αυτά πρέπει να είμαστε πρέπει να ήμαστε και σίγουροι ότι τα δεδομένα που δίνουμε στο internet είναι ασφαλή και κανείς άλλος δεν μπορεί να έχει πρόσβαση σε αυτά εκτός από εμάς και την τράπεζα, διότι σε αντίθετη περίπτωση υπάρχει πιθανότητα να χάσουμε αρκετά μεγάλο ποσό χρημάτων από κακόβουλες ενέργειες.

Οι τεχνολογίες που χρησιμοποιούνται εκτός από την γνωστή χρήση του προσωπικού κωδικού pin που χρησιμοποιείται και στα ATM και στο phone banking, ελέγχονται, εγκρίνονται και πιστοποιούνται από οργανισμούς οι οποίοι μας παρέχουν την ασφάλεια του ότι τα προσωπικά μας δεδομένα δεν θα υποκλαπούν και δεν θα χρησιμοποιηθούν από τρίτους με σκοπό να μας εκβιάσουν, εξαπατήσουν ή οποιαδήποτε άλλη ενέργεια θα μπορούσε να γίνει δίχως την άδεια μας και εναντίων μας.

### **Μερικά από τα ζητήματα που τίθενται είναι :**

- A) Υπάρχει το νομικό πλαίσιο το οποίο να μας διασφαλίσει ότι δεν θα «πέσουμε» θύματα ηλεκτρονικής εξαπάτησης. Πώς η Τράπεζα μπορεί να διασφαλίσει ότι τα δεδομένα των πελατών της δεν θα υποκλαπούν και πώς μπορούμε να υπερασπίσουμε νομικά τα δικαιώματά μας;
- B) Με ποιόν τρόπο μπορεί η τράπεζα να συλλέξει πληροφορίες για τους πελάτες τις δίχως να παραβιάσει το απόρρητο των συναλλαγών και των προσωπικών τους δεδομένων και,

υπάρχουν εποπτικές αρχές που να διασφαλίζουν ότι τα στοιχεία αυτά δεν θα γίνουν αντικείμενο εμπορικής εκμετάλλευσης από την τράπεζα προς τρίτους;

Γ) Πώς κάποιος μπορεί να διασφαλιστεί, ότι μέσω του ιστοχώρου του ηλεκτρονικού καταστήματος μιας τράπεζας, κάποιος άλλος δεν θα εισβάλει στον προσωπικό του υπολογιστή για να υποκλέψει δεδομένα, ή πώς θα διασφαλιστεί μέσα σε ένα παγκοσμιοποιημένο πλέον και πλήρως διασυνδεδεμένο δίκτυο τραπεζών, ότι δεν μπορεί να παραβιαστεί η ιδιωτικότητα των συναλλαγών του;

Δ) Πώς διασφαλίζει η τράπεζα το πως οι κωδικοί των πελατών είναι ασφαλείς και πως δεν μπορούν τρίτοι να έχουν πρόσβαση σε αυτούς μέσω internet και εν συνεχεία να μπορούν προσποιούμενοι τους πραγματικούς πελάτες να κάνουν κινήσεις στους λογαριασμούς αυτούς.

## **ΚΕΦΑΛΑΙΟ 1° : ΝΟΜΙΚΑ ΘΕΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΤΡΑΠΕΖΙΚΗΣ**

### **ΔΙΑΚΙΝΗΣΗ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ ΣΤΟ ΔΙΑΔΙΚΤΥΟ.**

Η διάδοση της χρήσης των ηλεκτρονικών υπολογιστών, η ανάπτυξη του διαδικτύου και η διαδεδομένη χρήση ψηφιακών εφαρμογών εκτός από τα ευεργετικά αποτελέσματα, επέφερε και σημαντική αύξηση της λεγόμενης ηλεκτρονικής εγκληματικότητας.

Με την πεποίθηση της απολύτου ελευθερίας έκφρασης και με την ψευδαίσθηση της ανωνυμίας πολλές φορές, οι χρήστες διαχωρίζοντας ασυνείδητα τον πραγματικό από τον δικτυακό κόσμο, προβαίνουν στην τέλεση σοβαρών ποινικών αδικημάτων.

Επιπλέον η «ανωνυμία», σε συνδυασμό με την ανυπαρξία ή τη δυσκολία εφαρμογής των νομικών κανόνων, κάνει τους «ηλεκτρονικούς δράστες» να αισθάνονται ασφαλείς κατά τη διάπραξη των εγκλημάτων τους, τα οποία πάντως δεν θα τελούσαν εκτός διαδικτύου. Συνηθέστερη μορφή έκφρασης της παράνομης αυτής συμπεριφοράς αποτελούν τα εγκλήματα κατά της τιμής, τα οποία εκδηλώνονται με παράνομες και βλαβερές πράξεις που θίγουν την προσωπικότητα και την ηθική των ατόμων, την τιμή και την υπόληψή τους. Ο προσβληθείς στην προσωπικότητά του από κάποιο μήνυμα, εικόνα, δημοσίευμα, χαρακτηρισμό κ.λπ. που διακινείται στο Διαδίκτυο προστατεύεται από την ελληνική νομοθεσία βάσει των σχετικών διατάξεων του ποινικού κώδικα για την εξύβριση και τη δυσφήμιση.

Ενδεικτικά αναφέρονται τα εγκλήματα της εξύβρισης, δυσφήμισης, απλής και συκοφαντικής, προσβολής μνήμης νεκρού, δυσφήμιση ανώνυμης εταιρείας, αδικήματα σχετικά με παραβίαση προσωπικών δεδομένων κλπ.

Η έρευνα των Ηλεκτρονικών Εγκλημάτων είναι αρκετά δύσκολη, όταν ο χρήστης δε χρησιμοποιεί τα πραγματικά του στοιχεία και ιδιαίτερα χρονοβόρος διότι ακολουθείται η διαδικασία του εντοπισμού των «ηλεκτρονικών ίχνων». Μία έρευνα μπορεί να διαρκέσει από ένα μήνα έως και δύο χρόνια. Σε κάθε διαδικτυακή έρευνα γίνεται προσπάθεια εντοπισμού του «ηλεκτρονικού ίχνους» του δράστη, το οποίο για κάθε χρήστη του Ιντερνέτ είναι μοναδικό, και αποτελεί σημαντικό στοιχείο για την αποδεικτική διαδικασία στο δικαστήριο. Στην περίπτωση λοιπόν που εντοπισθεί κάποια παράνομη ή ύποπτη ενέργεια στο Διαδίκτυο, το πρώτο πράγμα που εντοπίζουν οι Αρχές είναι η IP (Internet Protocol Address) διεύθυνση του δράστη, κάτι που είναι πολύ εύκολο να επιτευχθεί με απλά προγράμματα, ενσωματωμένα στον κωδικό των ιστοσελίδων. Από την IP διεύθυνση εντοπίζουν τον ISP που εξυπηρέτησε τον δράστη και μετά θα πρέπει να εκδοθεί εισαγγελική εντολή ώστε να υποχρεωθεί ο ISP να δώσει τα στοιχεία του συνδρομητή του που κάποια συγκεκριμένη ημέρα και ώρα είχε αποκτήσει την συγκεκριμένη IP διεύθυνση. Τα στοιχεία του συνδρομητή του που μπορεί να αποκαλύψει ο ISP (Internet Service Provider) είναι μόνο το τηλέφωνο από το οποίο κάλεσε ο δράστης και το όνομα χρήστη (username) που χρησιμοποίησε.

### **Η Δικαιοδοσία στο Διαδίκτυο**

Για την ανεύρεση της αρμοδιότητας του δικαστηρίου πρέπει να καθορισθεί ο τόπος τέλεσης του αδικήματος. Για τον καθορισμό του τόπου τελέσεως του αδικήματος υποστηρίζονται τέσσερις θεωρίες:

- α) του τόπου ενέργειας,
- β) του τόπου αποτελέσματος,
- γ) η μικτή θεωρία και
- δ) του βαρύνοντος τόπου, σύμφωνα με την οποία ο τόπος του αδικήματος εντοπίζεται στο κράτος όπου το έγκλημα εκδηλώθηκε κατά την κύρια σημασία του.

Η κρατούσα θεωρία στην Ελλάδα και στην Ευρώπη είναι η θεωρία του βαρύνοντος τόπου.



## **ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ**

Ο όρος “προσωπικά δεδομένα» που έχει επικρατήσει διεθνώς αναφορικά με την προστασία των δεδομένων του υποκειμένου κατ’ αντιστοιχία με τον αγγλικό όρο “data protection” , και αφορά την προστασία της προσωπικότητας, των δικαιωμάτων και των ελευθεριών του ατόμου, δηλαδή του φορέα των δεδομένων και όχι τα ίδια τα δεδομένα.

Ορθότερη όμως απόδοση της έννοιας «προσωπικά δεδομένα» στα Ελληνικά είναι αυτή που περιγράφεται στον ν.2472/97, που κάνει λόγω για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όσο και της Οδηγίας 95/46/ΕΚ «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών».

## **ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ**

Η προστασία του ιδιωτικού βίου κατοχυρώνεται διεθνώς με μια πληθώρα διατάξεων , μεταξύ των οποίων διεθνείς Συμβάσεις, όπως η Οικουμενική Διακήρυξη των Δικαιωμάτων του ανθρώπου του ΟΗΕ, το Διεθνές Σύμφωνο Ατομικών και Πολιτικών Δικαιωμάτων και η Σύμβαση της Ρώμης για την προάσπιση των δικαιωμάτων και των θεμελιωδών ελευθεριών του Ατόμου.

Επιπλέον μια σειρά από Οδηγίες του Ευρωπαϊκού κοινοβουλίου ολοκληρώνουν το πλαίσιο της νομικής προστασίας εξουδετερώνοντας οποιαδήποτε επέμβαση στην ιδιωτική σφαίρα των ατόμων . Με την οδηγία 95/46/ΕΚ η οποία εναρμονίστηκε η χώρα μας με τον ν.2472/1997 θεσπίζεται η προστασία των φυσικών προσώπων από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία τους.

Με την οδηγία 97/66/ΕΚ «περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα» η οποία αποσκοπεί στην εναρμόνιση των διατάξεων των κρατών μελών , προκειμένου να διασφαλιστεί ένα ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων, ιδίως το δικαίωμα της ιδιωτικότητας και των προσωπικών ελευθεριών στον τομέα των τηλεπικοινωνιών από την επεξεργασία τους και στην ελεύθερη διακίνηση τους .

Η οδηγία αυτή ενσωματώθηκε και εναρμονίστηκε στο ελληνικό δίκαιο με τον ν.2774/1999 ο οποίος φέρει τον τίτλο «προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα».

Οι ανωτέρω οδηγίες συμπληρώνονται από την 2002/58/ΕΚ οδηγία σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, με την οποία και ολοκληρώνεται το πλαίσιο προστασίας και θωρακίζεται η ιδιωτική ζωή του ατόμου ενώ παράλληλα εξασφαλίζει τα έννομα συμφέροντα των νομικών προσώπων σε κοινοτικό επίπεδο .

Οι διατάξεις της 2002/58/ΕΚ συμπληρώνουν και εξειδικεύουν την 95/46/ΕΚ, ενώ χαρακτηριστικό είναι ότι τα κράτη μέλη όφειλαν να την είχαν ενσωματώσει στο δίκαιο τους πριν την 31-10-2003 κατά την οποία καταργείτο η οδηγία 97/66/ΕΚ.

Στην Ελλάδα η ιδιωτικότητα του ατόμου και του ιδιωτικού του βίου προστατεύονται συνταγματικά. Συγκεκριμένα στο άρθρο 2 παρ. 1 κατοχυρώνεται ο σεβασμός και η προστασία της αξίας του ανθρώπου, στο άρθρο 5 παρ. 1 εξασφαλίζεται η ελευθερία ανάπτυξης της προσωπικότητας , στο άρθρο 9 παρ. 1 προστατεύεται το απαραβίαστο της ιδιωτικής και οικογενειακής ζωής του ατόμου και τέλος στο άρθρο 19 διασφαλίζεται το απόρρητο των επιστολών και της ελευθερίας της επικοινωνίας.

Το κενό από την ηλεκτρονική επεξεργασία των δεδομένων προσωπικού χαρακτήρα εξαιτίας της χρήσης ηλεκτρονικών μέσων και της ανάπτυξης της τεχνολογίας και με ενδεχόμενο την τυχόν διείσδυση και παραβίαση της ιδιωτικής σφαιράς του ατόμου καλύφθηκε με το άρθρο 9<sup>Α</sup> του ύστερα από την αναθεώρηση του το 2001. Το άρθρο 9<sup>Α</sup> του Συντάγματος, ορίζει ότι «καθένας έχει δικαίωμα προστασίας από την συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως ορίζει ο νόμος. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή που συγκροτείται και λειτουργεί όπως ορίζει ο νόμος» ( Αρχή Προστασία Δεδομένων Προσωπικού Χαρακτήρα).

Τέλος η ελευθερία πρόσβασης και επικοινωνίας γενικά και ειδικότερα στο διαδίκτυο, αλλά και το απόρρητο της επικοινωνίας σε αυτό εξασφαλίζεται από τον ν.2225/1994 σχετικά με την προστασία της ελευθερίας της ανταπόκρισης, βάση του οποίου ιδρύθηκε η Εθνική Επιτροπή Προστασίας του Απορρήτου των Επικοινωνιών και της Υπουργικής Απόφασης 68141 στις 4/5/1995, αναφορικά με τον κώδικα δεοντολογίας άσκησης τηλεπικοινωνιακών δραστηριοτήτων.

## **ΟΙ ΚΥΡΙΟΙ ΔΙΚΑΙΟΠΟΛΙΤΙΚΟΙ ΣΤΟΧΟΙ ΤΟΥ ΕΥΡΩΠΑΙΟΥ ΝΟΜΟΘΕΤΗ**

### **1. Η ενοποίηση της ευρωπαϊκής αγοράς χρηματοοικονομικών υπηρεσιών**

Σύμφωνα με σταθερή αξιολόγηση του ευρωπαϊκού νομοθέτη, η εναρμόνιση των κανόνων για τον τομέα χρηματοοικονομικών υπηρεσιών έχει βαρύνουσα σημασία για την επίτευξη της ενιαίας ευρωπαϊκής αγοράς προϊόντων και υπηρεσιών, κατά το άρθρο 14 παρ. 2 ΣυνθΕΚ. Το έργο της εναρμόνισης του τραπεζικού, επενδυτικού, ασφαλιστικού τομέα και των συστημάτων πληρωμών απασχόλησε ιδιαίτερα τον κοινοτικό νομοθέτη, δεδομένου των υφιστάμενων σημαντικής έκτασης ρυθμιστικών παρεμβάσεων των εθνικών νομοθετών. Μεταξύ άλλων, κρίθηκε αναγκαία η ενοποίηση των κανόνων για τη σύσταση και λειτουργία και χρηματοοικονομικών οργανισμών, των μέτρων για τη διασφάλιση των σταθερότητας του χρηματοπιστωτικού συστήματος των κρατών- μελών και της Ένωσης, τη διασυνοριακή πρόωθηση αντίστοιχων υπηρεσιών, αλλά και την αποφυγή καταστρατήγησης της ελεύθερης κυκλοφορίας χρηματοοικονομικών υπηρεσιών για παράνομους σκοπούς.

Εξάλλου, το κοινοτικό ενδιαφέρον προκάλεσε η τάση άμβλυνσης των όρων και ενοποίησης των επιμέρους κλάδους χρηματοοικονομικών υπηρεσιών και η ολοένα αυξανόμενη, και πλέον καθοριστική σημασία τους στη ζωή των ευρωπαίων πολιτών. Ως ειδικός λόγος κοινοτικής παρέμβασης προβλήθηκε, ιδίως, η προστασία των καταθετών- αποταμιευτών, των επενδυτών και των ασφαλιζομένων. Η προστασία αυτή συναρτήθηκε με την καθιέρωση του ενιαίου ευρωπαϊκού νομίσματος και τις εξελίξεις του χρηματοοικονομικού κλάδου. Ανάμεσα στις τελευταίες εξελίξεις, έγκαιρα εντοπίστηκε η τάση ανάπτυξης της παροχής χρηματοοικονομικών υπηρεσιών από απόσταση, η οποία καταρχήν αξιολογήθηκε ως από αποτέλεσμα της ολοκλήρωσης της ευρωπαϊκής αγοράς.

### **2. Η προστασία των καταναλωτών χρηματοοικονομικών υπηρεσιών**

Η επίτευξη υψηλού επιπέδου προστασίας των καταναλωτών αναγορεύεται σε επίκαιρο αυτοτελή πρωταρχικό σκοπό και αρμοδιότητα του κοινοτικού νομοθέτη, με βάση τα άρθρα 153

(πρώην 129 Α) και 95 παρ. 3 ΣυνθΕΚ, αντίστοιχα. Στο χρηματοοικονομικό κλάδο, η προστασία του καταναλωτή κρίθηκε ορθά ότι αποκτά ιδιαίτερη βαρύτητα, δεδομένου του πολύπλοκου χαρακτήρα των περισσότερων χρηματοοικονομικών συμφωνιών και των σημαντικών περιουσιακών επιπτώσεων τους. Κατά τη γνώμη του Ευρωπαϊκού Κοινοβουλίου και της Οικονομικής και Κοινωνικής Επιτροπής, μάλιστα, για την προστασία του καταναλωτή χρηματοοικονομικών υπηρεσιών δεν πρέπει να θεωρηθεί ότι επαρκούν αναντίρρητα τα προληπτικά μέτρα εποπτείας των επιχειρήσεων του κλάδου, στο πλαίσιο της ενιαίας αγοράς. Λαμβάνοντας υπόψη ότι «λόγω ασυμμετριών και ανισοτήτων στη συγκεκριμένη αγορά, ο καταναλωτής αποτελεί την ασθενέστερη συνιστώσα των εν λόγω συμβατικών σχέσεων», ο ευρωπαϊκός νομοθέτης προέκρινε ότι απαιτούνται ειδικότερες νομοθετικές ρυθμίσεις.

Αντίστοιχα, ιδιαίτερο ρυθμιστικό ενδιαφέρον εκδηλώνεται όσον αφορά στην διάθεση χρηματοοικονομικών υπηρεσιών από απόσταση προς καταναλωτές. Εν προκειμένω, κρίθηκε αναγκαία η θέσπιση πρόσθετων ιδιαίτερων μέσω προστασίας, ώστε οι καταναλωτές να μπορούν να συγκρίνουν αντικείμενα και να επιλέγουν νηφάλια τις καταλληλότερες και ανταγωνιστικότερες από τις διατιθέμενες σε διασυνοριακή κλίμακα υπηρεσίες. Η εναρμόνιση των εν λόγω μέτρων εύλογα αναμενόταν να οδηγήσει σε «χαμηλότερες τιμές, μεγαλύτερη επιλογή και ποιοτικά καλύτερες χρηματοοικονομικές υπηρεσίες για τον καταναλωτή».

### **3. Η ενθάρρυνση των χρηματοοικονομικών συναλλαγών με ηλεκτρονικά μέσα**

Η ανάπτυξη των ηλεκτρονικών συναλλαγών, κατεξοχήν δε των συναλλαγών μέσω Διαδικτύου, αξιολογήθηκε ως ζωτικής σημασίας ευκαιρία για την κατάργηση των φραγμών, που χωρίζουν τους ευρωπαϊκούς λαούς και θέτουμε μπόδια στην ελεύθερη κυκλοφορία υπηρεσιών ή στην ελεύθερη επαγγελματική εγκατάσταση (άρθρο 14 ΣυνθΕΚ). Σύντομα επισημάνθηκε η συμβολή τους στην αύξηση της απασχόλησης, της καινοτομίας, της ανταγωνιστικότητας και των επενδύσεων, αρκεί ο καθένας να διαθέτει πρόσβαση στο Διαδίκτυο. Το ενδιαφέρον του κοινοτικού νομοθέτη εστιάστηκε στην πλήρη αξιοποίηση των ευκαιριών του ηλεκτρονικού εμπορίου, μέσω εγκαθίδρυσης ομοιόμορφων κανόνων, προσαρμοσμένο στις ιδιαιτερότητες του Διαδικτύου, και επίτευξης ασφαλείας δικαίου. Ως κύριες προτεραιότητες τέθηκαν η ελευθερία ανάληψης δραστηριοτήτων ηλεκτρονικού εμπορίου και η εναρμόνιση των υποχρεώσεων των επιχειρηματικών φορέων, όταν παρέχονται υπηρεσίες με ηλεκτρονικά μέσα, ιδίως δε όταν αυτές αφορούν σε κατάρτιση συμβάσεων.

Περαιτέρω, σε κοινοτικό επίπεδο επισημάνθηκε ότι ο άυλος χαρακτήρας των χρηματοοικονομικών υπηρεσιών καθιστά ιδιαίτερα πρόσφορη την προώθηση και ολοκλήρωση τους μέσω Διαδικτύου. Η αντίληψη αυτή, έθεσε την ανάγκη προσαρμογής της διαδικασίας σύναψης χρηματοοικονομικών συμφωνιών στις ιδιαιτερότητες του Διαδικτύου και εναρμόνισης της, ώστε να εδραιωθούν συνθήκες ανταγωνισμού μεταξύ των επιχειρήσεων της Ένωσης. Με τα σύγχρονα τεχνολογικά μέσα συναλλαγών θεωρήθηκε ότι θα ενισχυθεί αντίστοιχα η εμπιστοσύνη των ευρωπαίων καταναλωτών και επενδυτών, με στόχο την πλήρη ενοποίηση της ευρωπαϊκής αγοράς χρηματοοικονομικών υπηρεσιών μέχρι το 2005. Παράλληλα, σημειώθηκε ότι η αύξηση των χρηματοοικονομικών συναλλαγών μέσω Διαδικτύου ενέχει κινδύνους διευκόλυνσης της τέλεσης εγκλημάτων απάτης και νομιμοποίησης παράνομων εσόδων.

### **4. Η αξιοποίηση των τεχνολογιών ηλεκτρονικών υπογραφών**

Η διαρκής εξέλιξη της τεχνολογίας και οι εγγενείς περιορισμοί ασφάλειας «ανοικτών δικτύων», όπως το Διαδίκτυο, προβλημάτισαν ιδιαίτερα τον κοινοτικό νομοθέτη. Έγινε αντιληπτό ότι για την απρόσκοπτη ανάπτυξη του ηλεκτρονικού εμπορίου, απαιτούνται ηλεκτρονικές υπογραφές και συναφείς υπηρεσίες που εξασφαλίζουν και επιτρέπουν την απόδειξη της γνησιότητας των

μεταδιδόμενων μέσω Διαδικτύου πληροφοριών. Παράλληλα, επισημάνθηκε ότι στην ευρωπαϊκή αγορά ήδη διατίθεται πλείστα είδη ηλεκτρονικών υπογραφών, διαφορετικών μεταξύ τους τεχνικών προδιαγραφών. Σε κοινοτικό επίπεδο, ζήτημα παρέμβασης τέθηκε, προκειμένου να εναρμονιστούν οι κανόνες που αφορούν στη νομική αναγνώριση των ηλεκτρονικών υπογραφών, στη διαμεσολάβηση των προμηθευτών υπηρεσιών πιστοποίησης και στην εποπτεία της τήρησης διατυπώσεων ηλεκτρονικών υπογραφών στις χρηματοοικονομικές και λοιπές συναλλαγές.

Στο πλαίσιο της προσπάθειας εναρμόνισης, ο κοινοτικός νομοθέτης επιχείρησε να λάβει υπόψη του την ταχεία τεχνολογική ανάπτυξη, ώστε να υιοθετήσει λύσεις τεχνολογικά ουδέτερες. Ωστόσο, έγκαιρα επισημάνθηκε ότι ορισμένες τεχνικές ηλεκτρονικών υπογραφών θα πρέπει να πληρούν ιδιαίτερα αυξημένες προδιαγραφές ασφάλειας, ώστε να υποκαθιστούν αξιόπιστα τη χρήση εγγράφων στις συναλλαγές. Ιδιαίτερα στο χρηματοοικονομικό τομέα, το ζήτημα της ασφάλειας των αντίστοιχων συναλλαγών αναγορεύθηκε σε κύριο μέλημα των κοινοτικών νομοπαρασκευαστικών οργάνων. Περαιτέρω, η χρήση ηλεκτρονικών υπογραφών ρητά αξιολογήθηκε ως κρίσιμη παράμετρος, ενόψει εξακρίβωσης των στοιχείων των πλεατών στις χρηματοοικονομικές συναλλαγές μέσω Διαδικτύου και την καταπολέμηση συναφούς εγκληματικότητας.

## **ΟΙ ΒΑΣΙΚΕΣ ΚΟΙΝΟΤΙΚΕΣ ΡΥΘΜΙΣΕΙΣ**

### **Γενικές Οδηγίες για τους χρηματοοικονομικούς οργανισμούς και τις χρηματοοικονομικές υπηρεσίες.**

Ήδη από την δεκαετία του 1970 εκδόθηκε σημαντικός αριθμός κοινοτικών πράξεων (περίπου 50 οδηγιών), που σε σημαντικό βαθμό συνέβαλε στην ελεύθερη κυκλοφορία των χρηματοοικονομικών υπηρεσιών στην τότε Ευρωπαϊκή Κοινότητα. Μεταξύ αυτών, χαρακτηριστικά αναφέρονται οι επτά τραπεζικές οδηγίες, που πλέον έχουν τροποποιηθεί και έχουν κωδικοποιηθεί σε ένα ενιαίο κείμενο με την οδηγία 2000/12/EK, οι οδηγίες 93/6/EK και 93/22/EK για τις επενδυτικές υπηρεσίες και τους αντίστοιχους οργανισμούς, οι οδηγίες 90/619/ΕΟΚ, 92/49/ΕΟΚ, 92/96/ΕΟΚ, 98/78/EK, 2002/83/EK για χαρακτηριστικά είδη ασφαλιστικών υπηρεσιών. Ιδιαίτερο ενδιαφέρον για την πρόσβαση σε χρηματοοικονομικές υπηρεσίες μέσω διαδικτύου, μεταξύ άλλων παρουσιάζουν οι διατάξεις της Οδηγίας 2000/46/EK για την ανάληψη, άσκηση και προληπτική εποπτεία της δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος, της Οδηγίας 91/308/ΕΟΚ όπως τροποποιήθηκε με την οδηγία 2001/97/EK σχετικά με την πρόληψη χρησιμοποίησης του χρηματοπιστωτικού συστήματος για την νομιμοποίηση εσόδων από παράνομες δραστηριότητες, της Απόφασης-πλαίσιο του Συμβουλίου 2001/413/ΔΕΥ για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην μετρητών.

Σε γενικές γραμμές, η ανάπτυξη της ενιαίας αγοράς χρηματοοικονομικών υπηρεσιών με τις ανωτέρω πράξεις βασίστηκε στην επιβολή ενιαίων ειδικών κανόνων ίδρυσης, λειτουργίας και εποπτείας των χρηματοοικονομικών οργανισμών, στην αρχή ελέγχου της τήρησης τους εκ μέρους της χώρας καταγωγής και στην αρχή της αμοιβαίας αναγνώρισης. Οι ανωτέρω προβλέψεις λειτουργούν, καταρχήν, ως κατευθύνσεις για την ερμηνεία και την εφαρμογή των πρόσφατων κοινοτικών πράξεων, που αφορούν πιο συγκεκριμένα το αντικείμενο της μελέτης.

## **Οι οδηγίες για την προστασία των καταναλωτών χρηματοοικονομικών υπηρεσιών.**

Ρυθμίσεις για την προστασία του καταναλωτή εισήγαγε η Οδηγία 87/102/ΕΟΚ, όπως τροποποιήθηκε με την οδηγία 90/88/ΕΟΚ, για την καταναλωτική πίστη. Επίσης, εκδόθηκε η Σύσταση της Επιτροπής της 1-3-2001 για τις υποχρεωτικά παρεχόμενες πληροφορίες στους καταναλωτές στεγαστικών δανείων. Πρόθεση προστασία επιφυλάχθηκε με την σημαντική Οδηγία 93/13/ΕΚ για τις καταχρηστικές ρήτρες των συμβάσεων που συνάπτονται με καταναλωτές. Οι προβλέψεις των ανωτέρω οδηγιών τυγχάνουν εφαρμογής σε ειδικότερες πτυχές της πρόσβασης καταναλωτών σε χρηματοοικονομικές υπηρεσίες μέσω Διαδικτύου.

Σημαντικότερο ακόμη ενδιαφέρον παρουσιάζει η Οδηγία 97/7/ΕΚ σχετικά με την προστασία των καταναλωτών κατά τις συμβάσεις από απόσταση. Μετά από μακρόχρονη νομοπαρασκευαστική διαδικασία, η συγκεκριμένη Οδηγία διέλαβε τελικά ρητή εξαίρεση (άρθρο 3 παρ.1) για τις καταναλωτικές συμβάσεις χρηματοοικονομικών υπηρεσιών. Η εξαίρεση έγινε δεκτή, προκειμένου να μελετηθούν διεξοδικότερα οι ιδιαιτερότητες των χρηματοοικονομικών υπηρεσιών από απόσταση, με σκοπό να τεθεί σε ισχύ ειδικότερη κοινοτική ρύθμιση. Κατ' αποτέλεσμα οι προβλέψεις της Οδηγίας 97/7/ΕΚ και η εμπειρία από την εφαρμογή τους στις έννομες τάξεις και των κρατών-μελών, καθόρισαν το αντικείμενο των διαπραγματεύσεων που οδήγησαν στη θέσπιση της ειδικότερης Οδηγίας 2002/65/ΕΚ.

### **ΟΔΗΓΙΑ 1999/93/ΕΚ**

Στόχος της οδηγίας 1999/93/ΕΚ είναι σύμφωνα με το άρθρο 1 αυτής η διευκόλυνση της χρήσης των ηλεκτρονικών υπογραφών και η νομική αναγνώριση τους. Με την οδηγία αυτή θεσπίζεται λοιπόν το νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές και για ορισμένες υπηρεσίες πιστοποίησης (άρθρο 1 παρ.1). Δεν καλύπτονται από τις διατάξεις της οδηγίας πτυχές σχετικές με τη σύναψη και την ισχύ συμβάσεων ή άλλων νομικών υποχρεώσεων, που διέπονται από απαιτήσεις εθνικού ή του κοινοτικού δικαίου ως προς τον τύπο, και δεν θίγονται κανόνες και περιορισμοί σχετικά με την χρήση εγγραφών, οι οποίοι περιέχονται στο εθνικό ή στο κοινοτικό δίκαιο (άρθρο 1 παρ.2).

Σύμφωνα με τον ορισμό της οδηγίας στο άρθρο 2, «ηλεκτρονική υπογραφή» είναι δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα σε ή λογικά συσχετιζόμενα με, άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας. Η παράγραφος 2 του άρθρου αυτού ορίζει ως προηγούμενη ηλεκτρονική υπογραφή (ψηφιακή) την ηλεκτρονική υπογραφή, η οποία ανταποκρίνεται στις ακόλουθες απαιτήσεις: συνδέεται μονοσήμαντα με τον υπογράφο, είναι ικανή να ταχτοποιήσει τον υπογράφο, δημιουργείται με μέσα που ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο και τέλος συνδέεται με δεδομένα, στα οποία αναφέρεται κατά τέτοιο τρόπο ώστε να μπορεί να εντοπιστεί οποιαδήποτε επακόλουθη αλλοίωση των εν λόγω δεδομένων.

Το άρθρο 3 αφορά στη λειτουργία της ηλεκτρονικής υπογραφής μέσα στην εσωτερική και ευρωπαϊκή αγορά και ορίζει ότι τα κράτη- μέλη δεν μπορούν να εξαρτούν την παροχή υπηρεσιών πιστοποίησης από προηγούμενη έγκριση. Έχουν όμως το δικαίωμα να διατηρούν μηχανισμούς εθελοντικής διαπίστευσης και να επιβάλουν την τήρηση ορισμένων πρόσθετων απαιτήσεων, όταν πρόκειται για χρήση της ηλεκτρονικής υπογραφής στον δημόσιο τομέα. Στο άρθρο 4 της Οδηγίας αναφέρονται οι αρχές της εσωτερικής αγοράς.

Το άρθρο 5 προβλέπει τις έννομες συνέπειες των ηλεκτρονικών υπογραφών. Τα κράτη – μέλη διασφαλίζουν ότι οι προηγούμενες ηλεκτρονικές υπογραφές (ψηφιακές ) που βασίζονται σε αναγνωρισμένο πιστοποιητικό και οι οποίες δημιουργούνται από ασφαλή διάταξη δημιουργίας υπογραφής (άρθρο 5 παρ.1):

A) ικανοποιούν τις νομικές απαιτήσεις υπογραφής σε σχέση με τα δεδομένα σε ηλεκτρονική μορφή κατά τον ίδιο τρόπο που μια ιδιόχειρη ικανοποιεί τις απαιτήσεις αυτές σε σχέση με τα δεδομένα που καταχωρίζονται επί χάρτου, και

B) γίνονται δεκτές ως αποδεικτικό στοιχείο σε νομικές διαδικασίες.

Παράλληλα, τα κράτη – μέλη πρέπει να διασφαλίζουν ότι δεν απορρίπτεται η νομική ισχύς και το παραδεκτό μιας ηλεκτρονικής υπογραφής ως αποδεικτικού στοιχείου, επειδή τυχόν είναι υπό μορφή ηλεκτρονικών δεδομένων ή δεν βασίζεται σε αναγνωρισμένο πιστοποιητικό ή σε αναγνωρισμένο πιστοποιητικό που εξεδόθη από διαπιστευμένο παροχέα υπηρεσιών πιστοποίησης ή δεν δημιουργείται από ασφαλή διά τα ξη δημιουργίας υπογραφής (άρθρο 5 παρ.2).

Το άρθρο 6 παρ. 1 καθιερώνει την ευθύνη του παρόχου υπηρεσιών πιστοποίησης για τη ζημία την προκληθείσα σε οποιονδήποτε φορέα ή νομικό πρόσωπο, που ευλόγως βασίζεται στο πιστοποιητικό ως προς την ακρίβεια, κατά τη στιγμή της έκδοσής του, όλων των πληροφοριών που περιέχονται στο αναγνωρισμένο πιστοποιητικό, καθώς και την ύπαρξη στο πιστοποιητικό όλων των απαιτούμενων για ένα αναγνωρισμένο πιστοποιητικό στοιχείων. Επίσης, καθιερώνεται η ευθύνη του παρόχου υπηρεσιών για ζημία επελευθούσα λόγω της περιλαμβανόμενης στο πιστοποιητικό διαβεβαίωσης ότι κατά τον χρόνο έκδοσής του ο υπογράφων, που ταυτοποιείται στο αναγνωρισμένο πιστοποιητικό ήταν κάτοχος των δεδομένων δημιουργίας υπογραφής, τα οποία αντιστοιχούν στα δεδομένα επαλήθευσης υπογραφής που αναφέρονται ή ταυτοποιούνται στο πιστοποιητικό. Η ευθύνη του παρόχου υπηρεσιών πιστοποίησης αίρεται αν αυτός αποδείξει ότι δεν ενήργησε αμελώς (άρθρο 6 παρ.1, in fine). Τέλος ο πάροχος έχει την υποχρέωση να αναγράφει σε αναγνωρισμένο πιστοποιητικό τους περιορισμούς χρήσης αυτού του πιστοποιητικού, υπό την προϋπόθεση βέβαια ότι οι περιορισμοί αυτοί δύνανται να αναγνωρίζονται από τους τρίτους. Για κάθε βλάβη προκαλούμενη από την υπέρβαση αυτών των περιορισμών δεν ευθύνεται ο πάροχος (άρθρο 6 παρ.4).

Η διάταξη του άρθρου 7 της οδηγίας εξισώνει τα πιστοποιητικά τα εκδιδόμενα από πάροχο υπηρεσιών πιστοποίησης εγκατεστημένο σε Τρίτη χώρα με πιστοποιητικά εκδιδόμενα από πάροχο υπηρεσιών πιστοποίησης εγκατεστημένο στην Κοινότητα, εφόσον τηρούνται οι προϋποθέσεις της παραγράφου 1 του άρθρου αυτού. Σύμφωνα με την αιτιολογική έκθεση, για την ανάπτυξη του ηλεκτρονικού εμπορίου απαιτούνται διασυνοριακές ρυθμίσεις με συμμετοχή τρίτων χωρών. Προκειμένου, λοιπόν, να διασφαλιστεί η διαλειτουργικότητα του ηλεκτρονικού εμπορίου σε διεθνές επίπεδο, η Επιτροπή καθιερώνει στην παράγραφο 2 του εν λόγω άρθρου δυνατότητα να διατυπώνει προτάσεις για την αποτελεσματική εφαρμογή των προτύπων και διεθνών συμφωνιών, οι οποίες θα ισχύουν για υπηρεσίες πιστοποίησης.

Το άρθρο 8 της οδηγίας άπτεται της προστασίας δεδομένων προσωπικού χαρακτήρα, ενώ τα άρθρα 9 και 10 αναφέρονται στη επικουρική «επιτροπή ηλεκτρονικής υπογραφής», προσδιορίζοντας τα καθήκοντα της.

## **ΟΔΗΓΙΑ 2000/31/ΕΚ**

Η οδηγία 2000/31/ΕΚ ρυθμίζει ζητήματα που αναφέρονται στην παροχή υπηρεσιών της Κοινωνίας της Πληροφορίας με έμφαση στο ηλεκτρονικό εμπόριο δηλαδή, σύμφωνα με το σχετικό ορισμό του άρθρου 1 παρ.2 της οδηγίας 98/34/ΕΚ, όπως ισχύει «υπηρεσιών που συνήθως παρέχονται έναντι αμοιβής με ηλεκτρονικά μέσα εξ αποστάσεως και κατόπιν προσωπικής επιλογής ενός αποδέκτη των υπηρεσιών». Στις υπηρεσίες αυτές συγκαταλέγεται το σύνολο των υπηρεσιών που παρέχονται κατεξοχήν μέσω αμφίδρομων δικτύων τηλεπληροφορικής, άρα και μέσω Διαδικτύου.

Οπότε ως άμεσο αποτέλεσμα των προβλέψεων της Οδηγίας 2000/31/ΕΚ φέρονται να είναι καταρχήν να επιβάλλονται υποχρεώσεις στον προμηθευτή χρηματοοικονομικών υπηρεσιών, που αξιοποιεί τις υπηρεσίες του Παγκόσμιου Ιστού, είτε εν όψει κατάρτισης χρηματοοικονομικής συμφωνίας, είτε εν όψει εκτέλεσης της. Οι συγκριμένες ρυθμίσεις συμβάλλουν στην διαφάνεια και την ασφάλεια δικαίου των χρηματοοικονομικών συναλλαγών μέσω Διαδικτύου και ιδίως στην προστασία του αντιδιαπραγματευόμενου μέσω διαδικτύου.

## **ΟΔΗΓΙΑ 2000/46/ΕΚ**

### **ΙΔΡΥΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΧΡΗΜΑΤΟΣ – Ν. 3148/2003**

Τα ιδρύματα ηλεκτρονικού χρήματος αποτελούν τους φορείς νέων μορφών χρηματοοικονομικών συναλλαγών. Η Οδηγία 2000/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου έχει ως σκοπό, λαμβάνοντας υπόψη τα ειδικά χαρακτηριστικά των ιδρυμάτων αυτών να ρυθμίσει την ανάληψη, την άσκηση και την προληπτική εποπτεία των δραστηριοτήτων τους. Με τον όρο ίδρυμα ηλεκτρονικού χρήματος νοείται μια επιχείρηση εκτός του πιστωτικού ιδρύματος της περίπτωσης α' της παραγράφου 1 του άρθρου 2 ν.2076/1992, η οποία εκδίδει μέσα πληρωμής με τη μορφή ηλεκτρονικού χρήματος (Οδηγία 2000/46/ΕΚ, (L275-27.10.2000) άρθρο 1 παρ. 3 εδ α' και ήδη άρθρο 14 παρ. 3 ν. 3148/2003 (ΦΕΚ Α' 136/5.6.2003), προσθήκη παρ. 16 στο άρθρο 2ν. 2076/92).

Σύμφωνα με το άρθρο 1 παρ3 ες. Β' της Οδηγίας 2000/46/ΕΚ- άρθρο 14 παρ3 ν. 3148/2003 (προσθήκη παρ 17 στο άρθρο 2 ν. 2076/92)ως ηλεκτρονικό χρήμα νοείται νομισματική αξία, η οποία αντιστοιχεί σε απαίτηση έναντι του εκδότη και α) είναι αποθηκευμένη σε ηλεκτρονικό υπόθεμα, β) έχει εκδοθεί κατόπιν παραλαβής χρηματικού ποσού και γ) γίνεται δεκτή ως μέσο πληρωμής από επιχειρήσεις άλλες, πέραν της εκδότριας.

Οι εταιρείες (ή ιδρύματα) ηλεκτρονικού χρήματος υπάγονται στην κατηγορία των πιστωτικών ιδρυμάτων με σκοπό την έκδοση ηλεκτρονικού χρήματος. Πιστωτικό ίδρυμα αποτελεί μια επιχείρηση, της οποίας η δραστηριότητα συνίσταται στην αποδοχή από το κοινό καταθέσεων ή άλλων επιστρεπτέων κεφαλαίων και στη χορήγηση πιστώσεων για ίδιο λογαριασμό (Οδηγία 2000/46/ΕΚ, άρθρο 1 παρ11- άρθρο 14 παρ 2 ν. 3148/2003 (αντικατάσταση της παρ. 1 του άρθρου 2 του ν.2076/92)).

Σύμφωνα με τον ανωτέρω ορισμό επιτρέπεται στα πιστωτικά ιδρύματα να διαχειρίζονται μέσα πληρωμής, συμπεριλαμβανομένου και του ηλεκτρονικού χρήματος, και να ασκούν αυτές τις δραστηριότητες σε όλη την Κοινότητα στο πλαίσιο της αμοιβαίας αναγνώρισης και του συνολικού συστήματος προληπτικής εποπτείας του εφαρμοζόμενου σε αυτά σύμφωνα με τις ευρωπαϊκές τραπεζικές οδηγίες.

### **Οι δραστηριότητες των ιδρυμάτων ηλεκτρονικού χρήματος και η δυνατότητα εξαργύρωσης αυτού**

Η κύρια δραστηριότητα των ιδρυμάτων ηλεκτρονικού χρήματος συνίσταται στην έκδοση ηλεκτρονικού χρήματος, ενώ παράλληλα δύναται να τους παρασχεθεί η δυνατότητα άσκησης διαχειριστικών ή βοηθητικών εργασιών σε σχέση με την κύρια αυτή δραστηριότητα.

Οι παράλληλες αυτές δραστηριότητες σχετικές με την έκδοση ηλεκτρονικού χρήματος, συνίσταται κυρίως στην παροχή χρηματοπιστωτικών και μη χρηματοπιστωτικών υπηρεσιών (Οδηγία 2000/46/ΕΚ, άρθρο 1 παρ. 5- άρθρο 20β ν. 3148/2003), όπως:

- Α) στη διαχείριση ηλεκτρονικού χρήματος με την εκτέλεση λειτουργικών και άλλων βοηθητικών εργασιών, συνδεδεμένων με την έκδοση ηλεκτρονικού χρήματος,
- Β) στην έκδοση και διαχείριση άλλων μέσων πληρωμής με εξαίρεση οποιαδήποτε πιστοδοτική δραστηριότητα και

Γ) στην αποθήκευση στοιχείων σε ηλεκτρονικό υπόθεμα για λογαριασμό άλλων επιχειρήσεων ή δημόσιων ιδρυμάτων.

Τα ιδρύματα ηλεκτρονικού χρήματος δεν συμμετέχουν ούτε και διατηρούν οποιοδήποτε δικαίωμα συμμετοχής σε άλλες επιχειρήσεις, εκτός εάν οι τελευταίες εκτελούν λειτουργικές ή άλλες βοηθητικές εργασίες, οι οποίες συνδέονται εν προκειμένω με το ηλεκτρονικό χρήμα, εκδιδόμενο ή διανεμόμενο από το συγκεκριμένο ίδρυμα ηλεκτρονικού χρήματος.

Το ανώτατο χρηματικό ποσό, το οποίο μπορεί να αποθηκευθεί σε κάθε ηλεκτρονικό απόθεμα και το οποίο μπορεί να διατίθεται στους κομιστές για τη διενέργεια πληρωμών δεν δύναται να υπερβαίνει τα 300 ευρώ (άρθρο 4α παρ 3 ν. 3148/2002). Παράλληλα, ο κομιστής του ηλεκτρονικού χρήματος, καθ' όλη τη διάρκεια ισχύος του χρήματος αυτού, έχει δικαίωμα να απαιτήσει την εξαργύρωση του (σύμφωνα με την ονομαστική του αξία) σε κέρματα ή χαρτονομίσματα, καθώς επίσης και τη μεταφορά του σε τραπεζικό λογαριασμό χωρίς άλλα επιπρόσθετα τέλη, πέραν των απολύτως αναγκαίων για την εκτέλεση της συγκεκριμένης δραστηριότητας (άρθρο 4β παρ.1 ν. 3148/2003).

Δεν επιτρέπεται η έκδοση ηλεκτρονικού χρήματος κατόπιν παραλαβής χρηματικού ποσού μικρότερου από την εκδοθείσα νομισματική αξία (άρθρο 4α παρ2 ν.3148/2003).

Μεταξύ εκδότη και κομιστή καταρτίζεται μια σύμβαση, με την οποία ρυθμίζονται λεπτομερώς όλοι οι όροι εξαργύρωσης του ηλεκτρονικού χρήματος, καθώς επίσης και το ελάχιστο όριο, το οποίο δεν μπορεί να είναι μικρότερο από τα 10 ευρώ (άρθρο 4β παρ.2 ν.3148/2003).

### **Προϋποθέσεις ίδρυσης των ιδρυμάτων ηλεκτρονικού χρήματος**

Για την ίδρυση ενός ιδρύματος ηλεκτρονικού χρήματος πρέπει να ακολουθήσει ορισμένη διαδικασία, αρχής γενομένης από την υποβολή αιτήσεως προς την τράπεζα της Ελλάδος. Η Τράπεζα της Ελλάδος ασκώντας την εποπτεία στα ιδρύματα ηλεκτρονικού χρήματος, προκειμένου να χορηγήσει την άδεια σύστασης θα πρέπει εκ των προτέρων να διαγνώσει την συνδρομή ορισμένων προϋποθέσεων.

Καταρχήν, πρέπει τα ιδρύματα ηλεκτρονικού χρήματος για να λειτουργήσουν να έχουν τη μορφή ανώνυμης εταιρείας και αρχικό κεφάλαιο 3 εκατ. Ευρώ (άρθρο 20α παρ. 1, 2 ν. 3148/2003). Τα ελάχιστα όρια των παρ 1 και 2 μπορούν να αναπροσαρμολογούνται με απόφαση της Τράπεζας της Ελλάδος. Σε κάθε περίπτωση, το ελάχιστο όριο του αρχικού κεφαλαίου δεν μπορεί να είναι μικρότερο του 1 εκατ. Ευρώ (άρθρο 20α παρ. 5 ν. 3148/2003).

Τα ιδρύματα ηλεκτρονικού χρήματος υποχρεούνται να διατηρούν σταθερό κεφάλαιο, το οποίο πρέπει να ανέρχεται τουλάχιστον στο 2% του τρέχοντος υπολοίπου ή του μέσου υπολοίπου των προηγούμενων 6 (έξι) μηνών, όποιο εκ των δύο είναι υψηλότερο, των συνολικών χρηματοοικονομικών υποχρεώσεων από το μη αποδοθέν υπόλοιπο του ηλεκτρονικού χρήματος που έχουν εκδώσει. Αν κάποιο ίδρυμα δεν έχει συμπληρώσει έξι μήνες λειτουργίας (συμπεριλαμβανομένης και της ημέρας έναρξης λειτουργίας του), οφείλει να διατηρεί κεφάλαιο, το οποίο πρέπει να ανέρχεται στο 2% τουλάχιστον είτε του τρέχοντος υπολοίπου είτε του προβλεπόμενου για έξι μήνες ποσού- στόχου του συνόλου των χρηματοοικονομικών υποχρεώσεων του από το μη αποδοθέν υπόλοιπο του ηλεκτρονικού χρήματος που έχει εκδώσει. Το ανωτέρω προβλεπόμενο για 6 μήνες ποσό- στόχος μπορεί να αποδειχθεί με βάση τα επιχειρηματικά προγράμματα του εν λόγω ιδρύματος, αλλά πάντα με την επιφύλαξη



ενδεχόμενων προσαρμογών αυτού, ύστερα από απαίτηση των αρμόδιων αρχών (άρθρο 4 παρ. 2, 3 της Οδηγίας 2000/46/ΕΚ- άρθρο 20α παρ. 4 ν. 3148/2003).

**ΠΙΝΑΚΑΣ ΙΔΡΥΜΑΤΩΝ ΗΛΕΚΤΡΟΝΙΚΟΥ ΧΡΗΜΑΤΟΣ, ΚΑΤΑ ΧΩΡΑ ΠΡΟΕΛΕΥΣΗΣ (ΕΔΡΑ), ΠΟΥ ΓΝΩΣΤΟΠΟΙΗΣΑΝ ΕΝΔΙΑΦΕΡΟΝ ΓΙΑ ΠΑΡΟΧΗ ΥΠΗΡΕΣΙΩΝ ΧΩΡΙΣ ΕΓΚΑΤΑΣΤΑΣΗ**

(Οδηγία 2006/48/ΕΚ, 2000/46/ΕΚ, Ν. 3601/2007)  
(ΙΟΥΛΙΟΣ 2010)

ΕΔΡΑ : Μ. ΒΡΕΤΑΝΙΑ

ΙΔΡΥΜΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΧΡΗΜΑΤΟΣ / ΕΤΟΣ ΓΝΩΣΤΟΠΟΙΗΣΗΣ ΣΤΗΝ Τ.Ε.

1. SMART VOUCHER LIMITED / 2006
2. CLICKANDBUY (EUROPE) LTD / 2007
3. FIREPAY UK LTD / 2007
4. CITADEL COMMERCE UK LTD / 2007
5. STARBUCKS CARD EUROPE LTD / 2007
6. NEWCASTLE BUILDING SOCIETY / 2007, 2010
7. GOOGLE PAYMENT LIMITED / 2007
8. G-T-P FINANCIAL SERVICES LTD / 2008
9. VINCENTO PAYMENT SOLUTIONS LTD / 2008
10. PREPAID SERVICES COMPANY / 2008, 2009
11. APS FINANCIAL LIMITED / 2010

**ΠΙΝΑΚΑΣ ΙΔΡΥΜΑΤΩΝ ΗΛΕΚΤΡΟΝΙΚΟΥ ΧΡΗΜΑΤΟΣ ΑΠΟ ΧΩΡΕΣ ΜΕΛΗ ΤΗΣ Ε.Ε. ΤΑ ΟΠΟΙΑ ΕΧΟΥΝ ΕΞΑΣΚΗΣΕΙΤΟ ΔΙΚΑΙΩΜΑ ΤΗΣ ΕΛΕΥΘΕΡΗΣ ΠΡΟΣΦΟΡΑΣ ΥΠΗΡΕΣΙΩΝ ΣΤΗΝ ΚΥΠΡΟ**

(σύμφωνα με το άρθρο 25 της Οδηγίας 2007/64/ΕΕ δυνάμει του άρθρου 3(1) της Οδηγίας 2009/110/ΕΕ)

Μ. ΒΡΕΤΑΝΙΑ

ΟΝΟΜΑ ΙΔΡΥΜΑΤΟΣ

ΗΜΕΡΟΜΗΝΙΑ ΓΝΩΣΤΟΠΟΙΗΣΗΣ

- |  |                       |
|--|-----------------------|
| 1. Neteller UK Limited                                   | 2/12/2004 & 5/5/2011  |
| 2. Smart Voucher Ltd                                     | 21/8/2006 & 18/5/2011 |
| 3. ClickandBuy International Ltd                         | 2/3/2007 & 30/6/2011  |
| 4. Starbucks Card Europe Ltd                             | 22/3/2007             |
| 5. Google Payment Ltd                                    | 5/4/2007 & 6/5/2011   |
| 6. G-T-P Financial Services Ltd                          | 7/3/2008 & 30/6/2011  |
| 7. Vincento Payment Solutions Limited                    | 13/3/2008 & 6/5/2011  |
| 8. Prepaid Services Company Ltd (ex Paysafecard.com Ltd) | 20/6/2008 & 30/6/2011 |
| 9. APS Financial Ltd                                     | 8/7/2010 & 6/5/2011   |
| 10. Euronet Payments & Card Services Ltd                 | 6/10/2010 & 18/5/2011 |
| 11. PSI-Pay Ltd  | 18/5/2011             |

ΓΙΒΡΑΛΤΑΡ

ΟΝΟΜΑ ΙΔΡΥΜΑΤΟΣ

ΗΜΕΡΟΜΗΝΙΑ ΓΝΩΣΤΟΠΟΙΗΣΗΣ

- |                             |           |
|-----------------------------|-----------|
| 1. Transact Network Limited | 30/4/2008 |
|-----------------------------|-----------|

## **ΟΔΗΓΙΑ 2002/65/EK**

### **Γενικά**

Η θέσπιση της οδηγίας 2002/65/EK για την εξ αποστάσεως εμπορία χρηματοοικονομικών υπηρεσιών προς τους καταναλωτές υπήρξε η πρώτη ολοκληρωμένη και συστηματική προσπάθεια του κοινοτικού νομοθέτη να ρυθμίσει ειδικά- μετά από μακρόχρονη προπαρασκευαστική διαδικασία- τις συμβάσεις χρηματοοικονομικών υπηρεσιών που καταρτίζονται από απόσταση μεταξύ προμηθευτών και καταναλωτών. Είχε προηγηθεί η γενική ρύθμιση των συμβάσεων από απόσταση με την οδηγία 97/7/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ης Μαΐου 1997 (οριζόντια Οδηγία), από το προστατευτικό πεδίο της οποίας ρητά- και προφανώς σκόπιμα- εξαιρούνταν οι συμφωνίες με αντικείμενο τις χρηματοοικονομικές υπηρεσίες. Και τούτο α) διότι η ρύθμιση αυτού του είδους συναλλαγών από την άποψη του δικαίου προστασίας του καταναλωτή προϋπέθετε την ολοκλήρωση του ειδικού νομοθετικού πλαισίου (καταρχήν σε κοινοτικό και στη συνέχεια και σε εθνικό επίπεδο) αναφορικά με τη σύσταση, τη λειτουργία, την προληπτική εποπτεία και τον έλεγχο των φορέων παροχής χρηματοοικονομικών υπηρεσιών στο κοινό, και β) διότι οι σημαντικές ιδιαιτερότητες των εν λόγω υπηρεσιών καθιστούσαν επιβεβλημένη την ειδική νομοθετική τους αντιμετώπιση. Επιπλέον, δεδομένου ότι οι περισσότερες εξ αποστάσεως χρηματοοικονομικές συναλλαγές διενεργούνται μέσω του Διαδικτύου, είναι δηλαδή ηλεκτρονικές (on line), είναι προφανές ότι η θέσπιση του ως άνω ειδικού νομοθετικού πλαισίου προϋπέθετε την ολοκλήρωση και του γενικότερου θεσμικού πλαισίου, το οποίο θα ήταν ικανό να εμπνεύσει την εμπιστοσύνη του καταναλωτικού κοινού σ' αυτό το νέο και εγγενώς επικίνδυνο είδος συναλλαγών. Έτσι, η έκδοση της οδηγίας 2002/65/EK λογικά έπεται αλλά και διευκολύνεται από τη θέση σε ισχύ των Οδηγιών 1999/93/EK της 13ης Δεκεμβρίου 1999 σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές, 2001/31/EK της 8ης Ιουνίου 2000 για το ηλεκτρονικό εμπόριο και 2002/58/EK της 12ης Ιουλίου 2002 για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

Θα πρέπει, εξάλλου, να επισημανθεί ότι η εδώ εξεταζόμενη Οδηγία ασχολείται τελικά περισσότερο με την αντιμετώπιση των ιδιαιτεροτήτων της εξ αποστάσεως συμβατικής δέσμευσης, παρά με τους εγγενείς κινδύνους των χρηματοοικονομικών υπηρεσιών, στις οποίες η εν λόγω δέσμευση αναφέρεται.

### **Οι στόχοι της Οδηγίας**

Σύμφωνα με την ορθότερη άποψη, για να εντοπίσει ο ερμηνευτής του δικαίου τους στόχους που επιδιώκει μια Οδηγία οφείλει κατά κύριο λόγο να ανατρέψει στο Προοίμιο καθώς και στο ουσιαστικό ρυθμιστικό της περιεχόμενο, ενώ επικουρικώς και μόνο μπορεί να αποδώσει σημασία στους σκοπούς εκείνους που φαίνονται «πιθανοί» ή «λογικοί» ενόψει των συγκεκριμένων διατάξεως της ΣυνθΕΚ, στις οποίες στηρίζεται η έκδοσή τους. Και τούτο διότι η υιοθέτηση της συγκεκριμένης εξουσιοδοτικής βάσης απηχεί (συνηθέστατα) τις υποκειμενικές πεποιθήσεις του κοινοτικού νομοθέτη ως προς τον επιδιωκόμενο με την Οδηγία σκοπό και, ως εκ τούτου, δεν πρέπει να θεωρείται άνευ ετέρου δεσμευτική, αλλά να συνεκτιμάται ελεύθερα.

Με βάση, λοιπόν, τα παραπάνω, γίνεται καταρχήν φανερό ότι στόχος της Οδηγίας 2002/65/EK υπήρξε η λήψη μέτρων για την προοδευτική εδραίωση της εσωτερικής αγοράς, τα οποία πρέπει να συμβάλουν, εκτός των άλλων, και στην επίτευξη υψηλού επιπέδου προστασίας του καταναλωτή. Υπό το πρίσμα αυτό, ειδικότερα, η εμπορία χρηματοοικονομικών υπηρεσιών από

απόσταση αξιολογείται ως ένα από τα κυριότερα απτά αποτελέσματα της ολοκλήρωσης της ως άνω αγοράς. Πρόκειται, δηλαδή, εξαρχής για διπλή νομοθετική στόχευση, που έγκειται στην προστασία των καταναλωτών- στο ιδιαίτερο πεδίο εφαρμογής της Οδηγίας- σε συνάρτηση με την πραγμάτωση της εσωτερικής αγοράς.

Περαιτέρω, στο πλαίσιο της εσωτερικής αγοράς και προς το συμφέρον των καταναλωτών, επιδιώκεται να διευρυνθεί το φάσμα των προσφερόμενων από απόσταση χρηματοοικονομικών υπηρεσιών εντός της Κοινότητας, ώστε οι καταναλωτές να μπορούν να επιλέξουν τις καταλληλότερες για τις ανάγκες τους υπηρεσίες σε πιο ανταγωνιστικές τιμές, αλλά και να διασφαλιστεί η ελευθερία επιλογής των τελευταίων, προκειμένου να εδραιωθεί η εμπιστοσύνη τους στις εξ αποστάσεως πωλήσεις. Παράλληλα, αναγνωρίζεται η ανάγκη να διαμορφωθεί το νομικό πλαίσιο που απαιτείται, ώστε να ενισχυθεί η αξιοπιστία των νέων τεχνικών της εξ αποστάσεως εμπορίας χρηματοοικονομικών υπηρεσιών και να διευρυνθεί η χρησιμοποίησή τους για τη διενέργεια των σχετικών συναλλαγών σε διασυνοριακή κλίμακα.

Για την πραγμάτωση των παραπάνω στόχων η Οδηγία 2002/65/EK επιτάσσει την εναρμόνιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών σχετικά με την εξ αποστάσεως παροχή χρηματοοικονομικών υπηρεσιών προς τους καταναλωτές, ήτοι τη θέσπιση κοινών κανόνων σε κοινοτικό επίπεδο στο συγκεκριμένο τομέα. Και τούτο προκειμένου αφενός μεν να διαφυλαχθεί η εύρυθμη λειτουργία της εσωτερική αγοράς και ο ανταγωνισμός μεταξύ των επιχειρήσεων, αφετέρου δε να μη θιγεί το γενικό επίπεδο προστασίας των καταναλωτών στ ακράτη μέλη. Δεδομένου, τέλος, ότι η διασφάλιση ενός υψηλού επιπέδου προστασίας των καταναλωτών αποσκοπεί κυρίως στην εξασφάλιση της ελεύθερης κυκλοφορίας των χρηματοοικονομικών υπηρεσιών εντός της ΕΕ, προβλέπεται ότι τα κράτη μέλη δεν μπορούν να αποκλίνουν από τις διατάξεις που θεσπίζονται με την παρούσα Οδηγία, εκτός εάν κατ' εξαίρεση η ίδια αναφέρει ρητώς το αντίθετο.

Από τη διατύπωση των διατάξεων του Προοιμίου, που αποτυπώνουν τη στοχοθεσία της υπό εξέταση Οδηγίας, δημιουργείται καταρχήν η εντύπωση ότι ο στόχος της πραγμάτωσης της εσωτερικής αγοράς υπερισχύει. Το συμπέρασμα όμως αυτό δεν επιβεβαιώνεται ούτε από το γράμμα ούτε και από το πνεύμα των επί μέρους κανονιστικών ρυθμίσεων που εισάγονται. Εγγύτερη θεώρηση καταδεικνύει το σαφή φιλοκαταναλωτικό τους προσανατολισμό, ενώ η νομοθετική φροντίδα επικεντρώνεται στην οριζόντια συμβατική έννομη σχέση μεταξύ καταναλωτή και προμηθευτή, με έμφαση στην απονομή δικαιωμάτων και αξιώσεων ιδιωτικού δικαίου, τα οποία μπορούν να προβληθούν ευθέως από τον καταναλωτή έναντι του αντισυμβαλλόμενου του/ προμηθευτή. Ταυτόχρονα, οι ρήτρες επιφύλαξης υπέρ του δικαιώματος των κρατών μελών να υπερβαίνουν τα όρια των διατάξεων της Οδηγίας, στα ουσιώδη λ.χ. ζητήματα των αξιώσεων προσυμβατικής πληροφόρησης του καταναλωτή και του δικαιώματος υπαναχώρησης (αλλά και σε άλλα), παρέχουν στους εθνικούς νομοθέτες αξιόλογα περιθώρια κανονιστικής δράσης προς την κατεύθυνση της διασφάλισης των συμφερόντων των καταναλωτών.

Υπό το πρίσμα αυτό, συνεπώς, δεν θα μπορούσε να αμφισβητηθεί ότι η Οδηγία 2002/65/EK, που παρέχει εξατομικευμένη προστασία στους ευρωπαϊούς καταναλωτές, ανήκει στο σκληρό πυρήνα του κοινοτικού δικαίου προστασίας του καταναλωτή, ενώ παράλληλα επιδιώκει να συμβάλει στην αποδόμηση των στρεβλώσεων του ανταγωνισμού και στην ελεύθερη κυκλοφορία των χρηματοοικονομικών υπηρεσιών εντός της ΕΕ. Στο σημείο αυτό ο κοινοτικός νομοθέτης επιχειρεί να ισορροπήσει μεταξύ δύο ισότιμων δικαιολογητικών στόχων, της προστασίας του καταναλωτή, αφενός, και της πραγμάτωσης της εσωτερική αγοράς, αφετέρου, γεγονός που αντανακλάται και στην επιλογή της νομικής βάσης της Οδηγίας και- συνακόλουθα- στην επιλογή της μεθόδου εναρμόνισης που υιοθετήθηκε.

## Νομική βάση της Οδηγίας και μέθοδος πλήρους εναρμόνισης

Όπως αναφέρεται στην αρχή του Προοιμίου της, η έκδοση της Οδηγίας 2002/65/EK στηρίχτηκε σε περισσότερες νομικές βάσεις. Πρόκειται, ειδικότερα, για τα άρθρα 47 παρ.2, 55 και 95 ΣυνθΕΚ. Η τριπλή νομοθετική θεμελίωση φαίνεται καταρχήν εύλογη, αφού η ύλη της Οδηγίας τέμνει περισσότερους Τίτλους της Συνθήκης των Ευρωπαϊκών Κοινοτήτων και στοχεύει στην εξασφάλιση περισσότερων κοινοτικών ελευθεριών. Θα πρέπει να επισημανθεί, ωστόσο, ότι και οι τρεις, σωρευτικά επικαλούμενες, νομικές βάσεις ανήκουν συστηματικά στις διατάξεις της ΣυνθΕΚ που αποσκοπούν πρώτιστα στην πραγμάτωση της εσωτερικής αγοράς. Την έλλειψη μνείας σε κάποια άλλη εξουσιοδοτική βάση, που θα ήταν ικανή να θεμελιώσει ειδικά και επαρκέστερα τον- παραλλήλως- επιδιωκόμενο στόχο της προστασίας των (οικονομικών) συμφερόντων των καταναλωτών, έρχεται να καλύψει η πρώτη αιτιολογική σκέψη του Προοιμίου: εκεί γίνεται εκ νέου αναφορά μόνο στο άρθρο 95 σε συνδυασμό, όμως, πλέον με το άρθρο 153 ΣυνθΕΚ. Η επίκληση και του άρθρου 153 (πρώην 129 Α), που εισήχθη ως ξεχωριστό Κεφάλαιο στο αρχικό κείμενο της Συνθήκης των Ευρωπαϊκών Κοινοτήτων μόλις με τη συνθήκη του Μάαστριχτ (7.2.1992) και άρχισε να ισχύει από την 1η.11.1993, έχει ιδιαίτερη σημασία. Και τούτο διότι η διάταξη αυτή συνιστά το νομικό θεμέλιο μιας κοινοτικής πολιτικής που αποβλέπει πρώτιστα στην προστασία των καταναλωτών (παρ.1), άλλοτε σε συνάρτηση με την πραγματοποίηση της εσωτερικής αγοράς (α.153 παρ. 3 στοιχ. α') και άλλοτε ανεξάρτητα από τη λειτουργία αυτή, δηλαδή σε ενίσχυση- και μόνον- της προστατευτικής πολιτικής των κρατών μελών (α. 153 παρ. 3 στοιχ. β').

Η Οδηγία 2002/65/EK, όπως ήδη ελέχθη (υπό II), επιδιώκει την επίτευξη ενός υψηλού επιπέδου προστασίας των καταναλωτών «στο πλαίσιο της υλοποίησης των στόχων της εσωτερικής αγοράς». Θα πρέπει, επομένως, να γίνει δεκτό ότι η έκδοσή της στηρίχτηκε στην εξουσιοδότηση βάση των άρθρων 153 παρ. 3 εδ. Α' και 85 παρ. 3επ. ΣυνθΕΚ, τα οποία- κατά την ορθότερη άποψη- χαράσσουν μια ενδιάμεση οδό μεταξύ της πλήρους και της ελάχιστης εναρμόνισης, με την έννοια ότι δεν αποκλείουν, έστω και υπό προϋποθέσεις, τη δυνατότητα εθνικών διαφοροποιήσεων. Η παραδοχή αυτή επιβεβαιώνεται και από το γεγονός ότι ήδη στο Προοίμιο της Οδηγία (αιτ. σκ. 13) προβλέπεται η δυνατότητα αποκλίσεων από τους εθνικούς νομοθέτες, μόνον όμως κατ' εξαίρεση, δηλαδή για ρητά καθοριζόμενα ειδικά ζητήματα. Θα μπορούσε, λοιπόν, βάσιμα να υποστηριχθεί ότι πρόκειται για Οδηγία μερικής πλήρους εναρμόνισης. Και τούτο διότι αφενός μεν η μέθοδος της άκαμπτης (γενικευμένης) πλήρους εναρμόνισης εξαρχής αποκλείεται, αφετέρου δε η δυνατότητα χρήσης της μεθόδου της ελάχιστης εναρμόνισης για ορισμένα μόνο ζητήματα δεν συνεπάγεται αυτόχρονα την επέκταση της στο σύνολο της Οδηγίας.

Δεδομένου ότι οι περισσότερες οδηγίες που εκδόθηκαν στο τομέα της προστασίας του καταναλωτή μέχρι τα τέλη της δεκαετίας του '90 (λ.χ. οι Οδηγίες: 85/577/ΕΟΚ για τις συμβάσεις εκτός εμπορικού καταστήματος, 90/314/ΕΟΚ για τα οργανωμένα ταξίδια και τις οργανωμένες διακοπές και περιηγήσεις, 93/13/ΕΟΚ για τις καταχρηστικές ρήτρες, 97/7/ΕΚ για τις συμβάσεις από απόσταση, 99/4//ΕΚ για την πώληση και τις εγγυήσεις καταναλωτικών αγαθών, κ.ο.κ.) είχαν χαρακτήρα ελαστικής εναρμόνισης, δεν θα ήταν υπερβολή να λεχθεί ότι η θέσπιση της Οδηγίας 2002/65/EK σηματοδοτεί τη στροφή του κοινοτικού νομοθέτη προς την υιοθέτηση, σε ολοένα και μεγαλύτερο βαθμό, της αρχής της πλήρους ή μέγιστης εναρμόνισης (full ή maximum harmonization, Vollharmonisierung). Σήμερα- έξι χρόνια μετά- μπορεί πλέον με ασφάλεια να γίνει λόγος για τάση σταθερή, η οποία επιβεβαιώνεται από σειρά προσφάτων κοινοτικών Οδηγιών, που αναφέρονται κυρίως στην προστασία των οικονομικών συμφερόντων του καταναλωτή (λ.χ. από τις Οδηγίες: 2005/29/ΕΚ για τις αθέμιτες εμπορικές πρακτικές των

επιχειρήσεων προς τους καταναλωτές στην εσωτερική αγορά και 2008/48/EK για τις συμβάσεις καταναλωτικής πίστης, αλλά και από την Πρόταση Οδηγίας σχετικά με τα (συμβατικά) δικαιώματα των καταναλωτών), και εκτιμάται ότι θα έχει σημαντικές επιπτώσεις στη διαδικασία ενοποίησης της εσωτερικής αγοράς.

Συγκεκριμένα, διαπιστώνεται ότι στην προκειμένη φάση ο κοινοτικός νομοθέτης προκρίνει την ανάγκη ομοιογενοποίησης των ευρωπαϊκών έννομων τάξεων έναντι της ανάγκης διατήρησης της διαφορετικότητας τους και μάλιστα στον ευαίσθητο δικαιοκό χώρο της προστασίας των καταναλωτών, ο οποίος εξ αρχής δεν υπάγεται στην αποκλειστική αρμοδιότητα της Κοινότητας με αποτέλεσμα η νομοθέτηση στο πλαίσιο του να διέπεται από την αρχή της επικουρικότητας. Ωστόσο το επιχείρημα, ότι η διατήρηση ή θέσπιση διαφορετικών ή ανόμοιων διατάξεων στο χώρο αυτό θα μπορούσε να έχει αρνητικές επιπτώσεις στην εξέλιξη της εσωτερικής αγοράς και στον ανταγωνισμό μεταξύ των επιχειρήσεων, δεν παρίσταται σε κάθε περίπτωση πειστικό. Όπως, εξάλλου, ορθά σημειώνεται, η επιδίωξη για υψηλό επίπεδο προστασίας των καταναλωτών δεν επιτρέπεται να υποχωρεί μπροστά στην επιταγή για άτεγκτη εναρμόνιση, ιδίως όταν αυτή επιβάλλεται μονομερώς από την κορυφή της ΕΕ. Και τούτο διότι οι πλήρως εναρμονισμένοι κανόνες, αν και έχουν το πλεονέκτημα της διαφάνειας, δεν εκφράζουν πάντοτε το υψηλότερο επίπεδο προστασίας των καταναλωτών που συναντάται στις έννομες τάξεις των κρατών μελών. Επιπρόσθετα, η μέθοδος της πλήρους εναρμόνισης επιταχύνει μεν την πορεία της ευρωπαϊκής ολοκλήρωσης, ορθώνει όμως και ανυπέρβλητα εμπόδια σε οποιαδήποτε παρέμβαση του εθνικού νομοθέτη ή δικαστή στο κοινοτικά καθορισμένο πεδίο παροχής προστασίας, προκαλώντας αναπόφευκτα αξιολογικές ασυνέπειες στο εσωτερικό σύστημα των επιμέρους εθνικών έννομων τάξεων.

Γίνεται, λοιπόν, φανερό ότι η πορεία προς την ευρωπαϊκή ολοκλήρωση μόνον ως μια πορεία αμφίδρομης αξιολογικής αλληλεπίδρασης μεταξύ της κοινοτικής και των εθνικών έννομων τάξεων μπορεί να νοηθεί, πράγμα που καταρχήν μόνο στη βάση της ελάχιστης εναρμόνισης δύναται να επιτευχθεί.

Κατά συνέπεια, η άμεση μετάβαση σε καθεστώς πλήρους εναρμόνισης δικαιολογείται αποκλειστικά σε περιπτώσεις ουσιώδους διακινδύνευσης των κοινοτικών ελευθεριών και υπό την προϋπόθεση ότι διασφαλίζεται ένα αδιαμφισβήτητο υψηλό επίπεδο προστασίας του καταναλωτή. Εξάλλου, δεν πρέπει να διαφύγει της προσοχής ότι η επιλεγείσα από τον κοινοτικό νομοθέτη μέθοδος πλήρους εναρμόνισης, όπως αυτή αποτυπώνεται στις προαναφερθείσες Οδηγίες- συμπεριλαμβανομένης της Οδηγίας 2002/65/EK-, παρέχει στα κράτη μέλη αξιόλογα περιθώρια κανονιστικών επιλογών, για ορισμένες πτυχές των υπό ρύθμιση αντικειμένων, δυνάμει συγκεκριμένων διατάξεων. Έτσι, όμως ούτε επιταχύνεται η σκοπούμενη πλήρης ομοιομορφία κανόνων σε ολόκληρο το χώρο της ΕΕ, ούτε διασφαλίζεται ο σεβασμός των υψηλών προτύπων προστασίας (standards) των καταναλωτών, που έχουν ήδη καθιερώσει μεμονωμένοι εθνικοί νομοθέτες ή δικαστές στο πλαίσιο της αυτονομίας που μέχρι πρόσφατα απολάμβαναν.

Στο πλαίσιο του δεύτερου μέρους της διερεύνησης θα δοθεί η ευκαιρία να επισημανθούν κάποιες αδυναμίες της εθνικής νομοθετικής ρύθμισης, οι οποίες θα μπορούσαν να αποδοθούν στο γεγονός ότι η Οδηγία 2002/65/EK θεσπίστηκε ως Οδηγία πλήρους εναρμόνισης.

## **Το περιεχόμενο της Οδηγίας**

Η Οδηγία 2002/65/EK εφαρμόζεται σε όλες τις χρηματοοικονομικές συμβάσεις, εγχώριες ή διασυνοριακές, που συνάπτονται από απόσταση, ηλεκτρονικά ή μη (on line ή off line), και περιέχει ένα σύνολο διατάξεων, περισσότερο ή λιγότερο αποσπασματικών, που εστιάζουν στην προστασία του καταναλωτή. Υπό την έννοια αυτή, η Οδηγία δεν υπεισέρχεται σε γενικές έννοιες που δικαίου των συμβάσεων, όπως η δικαιοπρακτική ικανότητα, ο τρόπος, ο τόπος ή ο χρόνος

κατάρτισης της σύμβασης, α παροχή αποζημίωσης, κ.ο.κ. Τα ουσιαστικά αυτά ζητήματα εξακολουθούν να ρυθμίζονται από τις διατάξεις (της εσωτερικής νομοθεσίας) των κρατών μελών. Κατά τα λοιπά, το ρυθμιστικό περιεχόμενο της Οδηγίας έγκειται στα εξής: Αρχικά προσδιορίζεται το αντικείμενο και οριοθετείτε το πεδίο εφαρμογής της Οδηγίας από άποψη υποκειμενική και αντικειμενική, ενώ στο ίδιο πλαίσιο ορίζονται και οι ανάγκες για την κατανόηση του περιεχομένου της έννοιες (άρθρα 1 και 2). Στη συνέχεια ρυθμίζονται αναλυτικά τα μέσα προστασίας του καταναλωτή (άρθρα 3-10). Συγκεκριμένα, εισάγονται κανόνες αναφορικά με την υποχρέωση διεξοδικής προσυμβατικής πληροφόρησης του καταναλωτή από τον προμηθευτή, το ελάχιστο περιεχόμενο και τον τρόπο παροχής της (άρθρα 3-4), και καθιερώνεται αυτοτελής υποχρέωση γνωστοποίησης των συμβατικών όρων και των ως άνω πληροφοριών με σταθερό τρόπο, πριν ο καταναλωτής δεσμευτεί από τη σύμβαση (άρθρο 5). Παράλληλα, θεσπίζεται δικαίωμα αναπαισιολόγητης υπαναχώρησης του καταναλωτή και καθορίζονται οι προϋποθέσεις που διέπουν την άσκηση του καθώς και οι συμβάσεις που εξαιρούνται (υποχρεωτικά ή δυναμικά) από το πεδίο εφαρμογής του (άρθρο 6). Ειδικά προβλέπονται οι συνέπειες της υπαναχώρησης, κυρίως δε το ποσό που υποχρεούται να καταβάλει ο καταναλωτής για την υπηρεσία που του έχει ήδη παρασχεθεί πριν από την άσκηση του εν λόγω δικαιώματος του (άρθρο 7). Περαιτέρω, ιδιαίτερα μέτρα λαμβάνονται για την προστασία της ιδιωτικής ζωής του καταναλωτή και δη για την προστασία του από τις μη αιτηθείσες υπηρεσίες και την αυτόκλητη εμπορική επικοινωνία (άρθρα 9-10), ενώ συγχρόνως αυτός θωρακίζεται και έναντι της δόλια χρήσης της πιστωτικής του κάρτας στο πλαίσιο (χρηματοοικονομικών) συναλλαγών που διενεργούνται από απόσταση (άρθρο 8). Τέλος, από τις υπόλοιπες διατάξεις της Οδηγίας 2002/65/ΕΚ ξεχωριστή μνεία προσήκει σ' εκείνες που αναφέρονται στις κυρώσεις που επιβάλλονται στον προμηθευτή σε περίπτωση παραβίασης των υποχρεώσεων του (άρθρο 11), στις δυνατότητες ατομικής δικαστικής και εξωδικαστικής προστασίας του καταναλωτή (άρθρα 13-14), στον αναγκαστικό χαρακτήρα των διατάξεων της Οδηγίας (άρθρο 12) καθώς και στη δυνατότητα των κρατών μελών να επιρρίψουν για ορισμένα, περιοριστικά αναφερόμενα, ζητήματα το βάρος της απόδειξης στον προμηθευτή (άρθρο 15 παρ.1).

### **Σχέση της Οδηγίας 2002/65/ΕΚ με άλλες πράξεις του Δευτερογενούς Κοινοτικού Δικαίου - Συμπληρώσεις, Αλληλεξαρτήσεις, Τροποποιήσεις**

Η Οδηγία 2002/65/ΕΚ τελεί σε σχέση διαλεκτικής συμπλήρωσης και αλληλεξάρτησης με μια σειρά Οδηγιών, από τις οποίες ορισμένες προϋπήρχαν και άλλες θεσπίστηκαν μετά την έκδοσή της. Ειδικότερα, οι συμβάσεις παροχής χρηματοοικονομικών υπηρεσιών από απόσταση ως ηλεκτρονικά καταρτιζόμενες συμβάσεις σύμφωνα με την Οδηγία 2000/31/ΕΚ για το ηλεκτρονικό εμπόριο. Δεδομένου ότι η Οδηγία 2002/65/ΕΚ αναφέρεται στην παροχή από απόσταση χρηματοοικονομικών υπηρεσιών προς καταναλωτές, το πεδίο εφαρμογής της συμπίπτει εν μέρει με αυτό της Οδηγίας 2000/31/ΕΚ για το ηλεκτρονικό εμπόριο, που ρυθμίζει τόσο τις σχέσεις μεταξύ επιχειρήσεων (B2B) όσο και τις σχέσεις μεταξύ επιχειρήσεων και καταναλωτών (B2C) και μεταφέρθηκε στο ελληνικό δίκαιο με το ΠΔ 131/2003. Ειδικότερα, στο βαθμό που ορισμένες χρηματοοικονομικές υπηρεσίες (λ.χ. διενέργεια πληρωμών, αγοραπωλησία μετοχών, παροχή επενδυτικών συμβουλών, κ.ο.κ.) παρέχονται συνήθως έναντι αμοιβής, με ηλεκτρονικά μέσα εξ αποστάσεως και κατόπιν αιτήματος ή «παραγγελίες» συγκεκριμένου καταναλωτή, ήτοι μέσω ανοικτών δικτύων τηλεπληροφορικής αμφίδρομης επικοινωνίας (λ.χ. μέσω του Διαδικτύου), συνιστούν υπηρεσίες της Κοινωνίας της Πληροφορίας. Τούτο σημαίνει ότι η

παροχή τους διέπεται επιπρόσθετα και από τις διατάξεις της Οδηγίας 2000/31/EK. Στο πλαίσιο αυτό αξίζει να επισημανθούν ιδίως οι διατάξεις σχετικά με:

A) Την υποχρέωση παροχής πληροφοριών στον αποδέκτη της υπηρεσίας κατά το προσυμβατικό στάδιο. Αυτή θεμελιώνεται στα άρθρα 5 και 10 της Οδηγίας 2000/31/EK και αναφέρεται αντίστοιχα σε γενικές πληροφορίες για τη δραστηριότητα του προμηθευτή, που παρέχονται υποχρεωτικά σε κάθε υποψήφιο αντισυμβαλλόμενο (ακόμη και μη καταναλωτή), και ειδικές πληροφορίες, οι οποίες αφορούν τη διαδικασία σύναψης της υπό διαπραγμάτευση σύμβασης μέσω του Διαδικτύου και είναι υποχρεωτικές για τον προμηθευτή μόνον εφόσον ο υποψήφιος αντισυμβαλλόμενος είναι καταναλωτής.

Όπως ήδη αναφέρθηκε, στη μακροσκελή διάταξη του άρθρου 3(παρ.1) της Οδηγίας 2002/65/EK καθιερώνεται το ελάχιστο περιεχόμενο της υποχρεωτικής προσυμβατικής πληροφόρησης του καταναλωτή χρηματοοικονομικών υπηρεσιών από απόσταση εκ μέρους του αντιδιαπραγματευόμενου προμηθευτή. Τούτο σημαίνει ότι το περιεχόμενο της εν λόγω πληροφόρησης μπορεί να διευρυνθεί ακόμη περισσότερο μέσω διατάξεων που προβλέπουν πρόσθετες απαιτήσεις πληροφόρησης, είτε της κοινοτικής νομοθεσίας είτε των εθνικών νομοθεσιών, υπό την προϋπόθεση ότι οι τελευταίες θα είναι συμβατές με το κοινοτικό δίκαιο. Υπό το πρίσμα αυτό, θα πρέπει να γίνει δεκτό ότι στις καταναλωτικές συμβάσεις παροχής χρηματοοικονομικών υπηρεσιών μέσω του Διαδικτύου εφαρμόζονται συμπληρωματικά και εκείνες οι διατάξεις της οριζόντιας Οδηγίας- πλαίσιο για το ηλεκτρονικό εμπόριο (2000/31/EK) που θεσπίζουν υποχρεώσεις εκ των προτέρων πληροφόρησης αναφορικά με στοιχεία, τα οποία δεν περιλαμβάνονται στους αναλυτικούς καταλόγους της παρ. 1 του άρθρου 3 της Οδηγίας 2002/65/EK. Ειδικότερα, εδώ θα πρέπει να αναφερθούν οι εξιδιασμένες πληροφορίες σχετικά με τη διαδικασία κατάρτισης και το ενδεχόμενο αρχειοθέτησης της υπό διαπραγμάτευση- μέσω του Διαδικτύου- σύμβασης, καθώς και για τα τεχνικά μέσα εντοπισμού και διόρθωσης σφαλμάτων ηλεκτρονικού χειρισμού πριν από τη σύναψη της και ιδίως για τη δυνατότητα μελλοντικής πρόσβασης σ' αυτήν.

B) Τις αρχές που διέπουν τη διαδικασία κατάρτισης της ηλεκτρονικής σύμβασης. Στο ζήτημα αυτό αναφέρεται ειδικά το άρθρο 11 της Οδηγίας 2000/31/EK, που φέρει τον καινοφανή- από την άποψη της δογματικής του αστικού δικαίου- τίτλο «Παραγγελία» και αποτελεί αναγκαστικό δίκαιο μόνον όταν ο ένας από τους δύο συμβαλλόμενους ενεργεί με την ιδιότητα του καταναλωτή. Συγκεκριμένα, στην πρώτη παράγραφο (παρ.1) της ως άνω διάταξης θεμελιώνεται η υποχρέωση του προμηθευτή (υπηρεσιών της Κοινωνίας της Πληροφορίας) να αποστείλει «χωρίς περιττή καθυστέρηση» και με ηλεκτρονικά μέσα στον αντισυμβαλλόμενο του/ αποδέκτη συγκεκριμένης υπηρεσίας αποδεικτικό της παραλαβής της παραγγελίας του, το οποίο, κατά τη μάλλον κρατούσα άποψη, δεν συνιστά μια τρίτη κατά σειρά (μετά τις ηλεκτρονικά διαβιβαζόμενες δηλώσεις της πρότασης και της αποδοχής) δηλαδή βουλήσεως, δεν έχει δηλαδή δικαιοπρακτικό αλλ' απλώς ενημερωτικό χαρακτήρα. Υπό το πρίσμα αυτό, συνεπώς, ο αποδέκτης της υπηρεσίας διαθέτει μια αυτόνομη ex lege αξίωση εκπλήρωσης της ανωτέρω «μετασυμβατικής» υποχρέωσης πληροφόρησης έναντι του αντισυμβαλλόμενου του/ προμηθευτή. Κατά μία άποψη, μάλιστα, που έχει ιδιαίτερη σημασία για το αντικείμενο της παρούσας διερεύνησης, θα μπορούσε να γίνει ερμηνευτικά δεκτό ότι η παράλειψη εκπλήρωσης της υποχρέωσης αυτής εκ μέρους του προμηθευτή χρηματοοικονομικών υπηρεσιών μέσω του Διαδικτύου όχι μόνο θεμελιώνει αξίωση αποκατάστασης κάθε αιτιωδώς προσκληθείσας στον αντισυμβαλλόμενο του/ καταναλωτή ζημιάς, αλλά επιπλέον αναστέλλει και την έναρξη της νόμιμης προθεσμίας υπαναχώρησης του τελευταίου βάσει του άρθρου 6 παρ. 1 της Οδηγίας 2002/65/EK.

Ξεχωριστή μνεία, εξάλλου, θα πρέπει να γίνει και στην υποχρέωση του φορέα παροχής των υπηρεσιών/ προμηθευτή να θέσει στη διάθεση του αντισυμβαλλόμενου του/ αποδέκτη τα τεχνικά μέσα που είναι αναγκαία, ούτως ώστε να διασφαλιστεί η ορθότητα της διαβιβαζόμενης μέσω του Διαδικτύου δικαιοπρακτικής δήλωσης του τελευταίου, είτε αυτή υπέχει θέση πρότασης για κατάρτιση της σκοπούμενης σύμβασης είτε αποδοχής της προηγηθείσας πρότασης του φορέα/ προμηθευτή (άρθρο 11 παρ.2). Πρόκειται ουσιαστικά για μια ειδική υποχρέωση συναλλακτικής πίστης, η οποία αποσκοπεί στην πρόληψη τυχόν εσφαλμένων χειρισμών εκ μέρους του δηλούντος/ αποδέκτη της υπηρεσίας (λ.χ. ως προς την εισαγωγή, επεξεργασία ή αποστολή των δεδομένων) και υπαγορεύθηκε από τη διαπίστωση ότι κατά τη διαδικασία δικαιοπρακτικής δέσμευσης μέσω του Διαδικτύου, κυρίως λόγω των εγγενών του ιδιαιτεροτήτων (λ.χ. της τεχνικής φύσης και της ταχύτητας των λειτουργιών του) αλλά και της κακοπιστίας ορισμένων προμηθευτών, συχνότατα εμφιλοχωρούν σφάλματα και παρανοήσεις. Γίνεται φανερό λοιπόν ότι η σχετική δυνατότητα αναθεώρησης, που παρέχεται στον καταναλωτή, εντάσσεται εξ ολοκλήρου στο προπαρασκευαστικό στάδιο της δικαιοπραξίας. Δεδομένου δε ότι η Οδηγία 2002/65/EK δεν περιέχει αντίστοιχη ρύθμιση, η εφαρμογή και της εδώ εξεταζόμενης-ευνοϊκής για τον καταναλωτή- διάταξης της Οδηγίας 2000/31/EK στο πεδίο των (καταναλωτικών) χρηματοοικονομικών συμβάσεων που συνάπτονται μέσω του Διαδικτύου παρίσταται όχι μόνο δυνατή αλλά και αναγκαία, ενώ η έκταση της υποχρέωσης, που βαρύνει τον προμηθευτή, θα πρέπει σε κάθε περίπτωση να προσδιορίζεται με γνώμονα την αρχή της αναλογικότητας.

Τέλος, αξίζει να επισημανθεί ότι, σύμφωνα με ειδική νομοθετική πρόβλεψη, οι διατάξεις των άρθρων 10 (παρ. 1 και 2) και 11 (παρ.1 περ.α' και 2) της Οδηγίας 2000/31/EK, επί των οποίων εδράζονται οι σημαντικότερες από τις προαναφερθείσες υποχρεώσεις του προμηθευτή υπηρεσιών της Κοινωνίας της Πληροφορίας, δεν εφαρμόζονται σε συμβάσεις παροχής υπηρεσιών (χρηματοοικονομικών ή άλλων) που συνάπτονται αποκλειστικά μέσω του ηλεκτρονικού ταχυδρομείου ή άλλου ισοδύναμου μέσου (ηλεκτρονικής) επικοινωνίας. Κατά τα λοιπά, είναι προφανές ότι οι υποχρεώσεις αυτές αναγνωρίζονται στο πρόσωπο του εν λόγω προμηθευτή ανεξάρτητα από την χρηματοοικονομική φύση των προσφερόμενων ή παρεχόμενων μέσω του Διαδικτύου υπηρεσιών, πολλών δε μάλλον ανεξάρτητα από την ειδικότερη κατηγορία στην οποία αυτές υπάγονται (λ.χ. υπηρεσίες τραπεζικής, επενδυτικής ή ασφαλιστικής φύσης). Και τούτο διότι η θέσπιση τους αποσκοπεί στην προστασία των αποδεκτών (καταναλωτών ή μη) όλων των υπηρεσιών της Κοινωνίας της Πληροφορίας από τους εγγενείς κινδύνους της χρήσης του Διαδικτύου ως μέσου επικοινωνίας και συναλλαγής σε απευθείας σύνδεση.

## **ΟΔΗΓΙΑ 2004/39/EK (MIFID)**

### **ΑΓΟΡΕΣ ΧΡΗΜΑΤΟΠΙΣΤΩΤΙΚΩΝ ΜΕΣΩΝ -N.3606/2007**

Ο νόμος 3606/2007 έχει τεθεί σε ισχύ από 1 Νοεμβρίου 2007 ακολουθώντας την ενιαία εφαρμογή της Κοινοτικής Οδηγίας 2004/39/EK σε όλες τις χώρες της Ευρωπαϊκής Κοινότητας. Η κύρια επιδίωξη του νόμου είναι να δημιουργήσει ένα συνεκτικό πλαίσιο το οποίο θα ρυθμίζει τους κυριότερους τρόπους εκτέλεσης εντολών στην ευρωπαϊκή αγορά ώστε να διασφαλίζεται η εύρυθμη λειτουργία των αγορών κινητών αξιών.

Ένας από τους στόχους του νόμου είναι θέσπιση κοινών κανόνων προστασίας και ενημέρωσης των επενδυτών από τις επιχειρήσεις επενδύσεων που δραστηριοποιούνται στις αγορές σε ένα καθεστώς διαφάνειας που θα εφαρμόζεται για όλες τις συναλλαγές.



Οι πελάτες σε κάθε επιχείρηση επενδύσεων /Πιστωτικό Ίδρυμα σύμφωνα με το νόμο, θα πρέπει να καταταχθούν σε μία από τρεις (3) κατηγορίες όπως αυτός προβλέπει ανάλογα με την εμπειρία, την γνώση και την οικονομική τους βάση. Συγκεκριμένα οι κατηγορίες είναι:

- Επιλέξιμος Αντισυμβαλλόμενος –πελάτης με εξειδικευμένες γνώσεις και άμεση πρόσβαση σε πληροφορίες στις αγορές κινητών αξιών,
- Επαγγελματίας πελάτης – πελάτης με συγκεκριμένα κριτήρια οικονομικού μεγέθους, ικανός να αναλάβει μόνος του επενδυτικές αποφάσεις και να κατανοήσει ενδεχόμενους κινδύνους που ενέχουν αυτές και τέλος
- Ιδιώτης πελάτης- πελάτης στον οποίο παρέχεται μέγιστη ενημέρωση και μέσα από συγκεκριμένες διαδικασίες γίνεται αξιολόγηση της γνώσης και της εμπειρίας του σε χρηματοπιστωτικά μέσα ώστε οι επενδυτικές επιλογές να ανταποκρίνονται στις προσωπικές του απαιτήσεις.

### **ΟΔΗΓΙΑ 2006/48/ΕΚ**

### **ΑΝΑΛΗΨΗ ΚΑΙ ΑΣΚΗΣΗ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ ΑΠΟ ΤΑ ΠΙΣΤΩΤΙΚΑ ΙΔΡΥΜΑΤΑ, ΕΠΑΡΚΕΙΑ ΙΔΙΩΝ ΚΕΦΑΛΑΙΩΝ ΤΩΝ ΠΙΣΤΩΤΙΚΩΝ ΙΔΡΥΜΑΤΩΝ ΚΑΙ ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ ΠΑΡΟΧΗΣ ΕΠΕΝΔΥΤΙΚΩΝ ΥΠΗΡΕΣΙΩΝ ΚΑΙ ΛΟΙΠΕΣ ΔΙΑΤΑΞΕΙΣ- Ν.3601/2007**

Με το νόμο αυτόν σκοπείται η ενσωμάτωση στην ελληνική τραπεζική νομοθεσία των διατάξεων των Οδηγιών του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, υπ' αριθμ. 2006/48/ΕΚ σχετικά με την ανάληψη και την άσκηση δραστηριότητας από τα πιστωτικά ιδρύματα (L 177/30.6.2006) και 2006/49/ΕΚ για την επάρκεια των ιδίων κεφαλαίων των επιχειρήσεων επενδύσεων και των πιστωτικών ιδρυμάτων (L 177/30.6.2006).

Ο νόμος αυτός ρυθμίζει την ανάληψη και άσκηση δραστηριότητας, καθώς και την προληπτική εποπτεία των πιστωτικών ιδρυμάτων. Επίσης περιλαμβάνει κανόνες σχετικά με την εποπτεία της κεφαλαιακής επάρκειας των επιχειρήσεων παροχής επενδυτικών υπηρεσιών, καθώς και με την άσκηση δραστηριότητας και την εποπτεία των εποπτευόμενων από την Τράπεζα της Ελλάδος χρηματοδοτικών ιδρυμάτων. Απαγορεύεται σε φυσικά ή νομικά πρόσωπα που δεν αποτελούν πιστωτικά ιδρύματα η κατ' επάγγελμα αποδοχή καταθέσεων χρημάτων ή άλλων επιστρεπτέων κεφαλαίων από το κοινό.

Με τον παρόντα νόμο ρυθμίζονται, επίσης, οι όροι και οι προϋποθέσεις για την ίδρυση και τη λειτουργία πιστωτικού ιδρύματος. Τα πιστωτικά ιδρύματα επιτρέπεται να ιδρύονται και να λειτουργούν μόνο με τη μορφή της ανώνυμης εταιρίας ή με τη μορφή αμιγούς πιστωτικού συνεταιρισμού του ν. 1667/1986 (ΦΕΚ 196 Α'), όπως ισχύει και οφείλουν να έχουν την πραγματική κεντρική διοίκηση τους στην Ελλάδα. Επίσης ορίζονται οι λόγοι άρνησης χορήγησης και οι λόγοι ανάκλησης της άδειας λειτουργίας. Οι αποφάσεις της Τράπεζας της Ελλάδος που εκδίδονται κατ' εφαρμογή του παρόντος νόμου υπόκεινται σε αίτηση ακυρώσεως ενώπιον του Συμβουλίου της Επικρατείας.

Η Τράπεζα της Ελλάδος ενημερώνει την Ευρωπαϊκή Επιτροπή για κάθε χορηγούμενη άδεια λειτουργίας πιστωτικού ιδρύματος και για άλλα συναφή θέματα.

Με τον παρόντα νόμο ρυθμίζεται το νομοθετικό πλαίσιο για την εγκαθίδρυση της εσωτερικής αγοράς, τόσο όσο αφορά την ελευθερία εγκατάστασης όσο αναφορικά και με την ελεύθερη παροχή των υπηρεσιών στον τομέα των πιστωτικών ιδρυμάτων.

## ΕΠΟΠΤΕΙΑ ΠΙΣΤΩΤΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Η Διεύθυνση Εποπτείας Πιστωτικού Συστήματος (ΔΕΠΣ) της Τράπεζας της Ελλάδος είναι επιφορτισμένη με την άσκηση της προληπτικής εποπτείας των πιστωτικών και χρηματοδοτικών ιδρυμάτων, η οποία στοχεύει στη διασφάλιση της σταθερότητας και της εύρυθμης λειτουργίας του εγχώριου χρηματοπιστωτικού συστήματος.

Το θεσμικό πλαίσιο για την άσκηση της εποπτείας έχει κατά κύριο λόγο διαμορφωθεί από την ενσωμάτωση της σχετικής κοινοτικής νομοθεσίας, η οποία με τη σειρά της είναι συμβατή με τις αρχές της Βασιλείας ΙΙ. Πιο συγκεκριμένα, ο Νόμος 3601/2007 (όπως τροποποιήθηκε από τους ν.3693/2008, ν.3746/2009, ν.3862/2010, 4002/2011 και 4021/2011) και οι Πράξεις Διοικητή 2630/2010, 2588/2007, 2589/2007, 2590/2007, 2646/2011, 2592/2007, 2645/2011, 2594/2007, 2595/2007, 2635/2010 συνιστούν το πλαίσιο εποπτείας (Βασιλεία ΙΙ). Επιπλέον, στο θεσμικό εποπτικό πλαίσιο περιλαμβάνονται και οι Πράξεις Διοικητή, 2577/2006, 2595/2007 και 2597/2007 που αφορούν τα Συστήματα Εσωτερικού Ελέγχου, καθώς και οι αποφάσεις ΕΤΠΘ 281/17.03.2009, 285/6/9.7.2009 και 290/12/11.11.2009 που αφορούν την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση των εσόδων από εγκληματικές δραστηριότητες και τη χρηματοδότηση της τρομοκρατίας και λοιπά θέματα.

Ειδικότερα, ο ν. 3601/2007, όπως ισχύει, και οι ανωτέρω ΠΔ/ΤΕ σχετικά με το πλαίσιο εποπτείας «Βασιλεία ΙΙ» αποτελούν ενσωμάτωση στην ελληνική έννομη τάξη των αντίστοιχων διατάξεων των Οδηγιών 2006/48/ΕΚ, 2006/49/ΕΚ, και 2007/64/ΕΚ, 2009/111/ΕΚ (CRD II) και 2010/76/ΕΕ (CRD III) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και των Οδηγιών 2009/27/ΕΚ και 2009/83/ΕΚ της Ευρωπαϊκής Επιτροπής. Με το ν. 4021/2011 ενσωματώθηκαν οι διατάξεις της Οδηγίας 2009/111/ΕΚ (CRD II) οι οποίες αφορούν τροποποιήσεις του ν. 3601/2007 και συνίστανται κυρίως στα εξής:

- ορίζεται η έννοια των σημαντικών υποκαταστημάτων πιστωτικών ιδρυμάτων,
- καθιερώνεται ο θεσμός του «σώματος εποπτών» (ομάδα συγκροτούμενη από τις εποπτικές αρχές πιστωτικών ιδρυμάτων με παρουσία σε άλλα κράτη-μέλη ή τρίτες χώρες, μέσω θυγατρικού πιστωτικού ιδρύματος ή σημαντικού υποκαταστήματος),
- καθιερώνεται η υποχρέωση υιοθέτησης των κατευθυντήριων γραμμών, προτύπων, συστάσεων της Ευρωπαϊκής Τραπεζικής Αρχής με γνώμονα τη σύγκλιση των εποπτικών μέσων και μεθόδων σε ευρωπαϊκό επίπεδο και θεσπίζεται η υποχρέωση της Τράπεζας της Ελλάδος να συμμετέχει στις δραστηριότητές της,
- καθορίζεται το πλαίσιο συνεργασίας των αρμόδιων εποπτικών αρχών και λήψης απόφασης σε περιπτώσεις πιστωτικών ιδρυμάτων με παρουσία σε διαφορετικά κράτη-μέλη σε καιρούς ομαλής λειτουργίας ή κρίσεων.

Οι λοιπές διατάξεις της Οδηγίας 2009/111/ΕΚ (CRD II) οδήγησαν στην αντικατάσταση ή/και τροποποίηση προϋπάρχουσων κανονιστικών διατάξεων. Συγκεκριμένα, εκδόθηκαν οι ΠΔ/ΤΕ 2630-2631-2632-2633-2634-2635/29.10.2010, που αφορούν αντίστοιχα:

- α) τον ορισμό των Ιδίων Κεφαλαίων,
- β) την εφαρμογή της Τυποποιημένης Προσέγγισης, της Προσέγγισης Εσωτερικών Διαβαθμίσεων και τον λειτουργικό κίνδυνο,
- γ) τη δημοσιοποίηση στοιχείων (Πυλώνας III),
- δ) την πιλοποίηση,
- ε) τους κινδύνους αγοράς και αντισυμβαλλομένου, και
- στ) τα μεγάλα χρηματοδοτικά ανοίγματα.

Επιπλέον, με το ν. 4021/2011:

- Ενσωματώνονται ορισμένες διατάξεις της Οδηγίας 2010/76/ΕΕ (CRD III), σχετικά με τα μέτρα του Πυλώνα II (ν. 3601/2007, άρθρο 62, παρ. 2, εδ. στ) και η)) και με τα κριτήρια που λαμβάνονται υπόψη για τον καθορισμό του κατάλληλου επιπέδου των ιδίων κεφαλαίων των πιστωτικών ιδρυμάτων (ν. 3601/2007, άρθρο 62, παρ. 4).
- Υιοθετούνται οι διατάξεις της Οδηγίας 2009/110/ΕΚ για τη ρύθμιση έκδοσης ηλεκτρονικού χρήματος και την εποπτεία της έκδοσης ηλεκτρονικού χρήματος. Οι διατάξεις του κεφ. Ι του ν. 3601/2007 που αναφέρονται στα ιδρύματα ηλεκτρονικού χρήματος (άρθρα 51-59) καταργούνται δεδομένου ότι με τις νέες διατάξεις τα Ιδρύματα Ηλεκτρονικού Χρήματος παύουν να είναι πιστωτικά ιδρύματα και εντάσσονται πλέον στην κατηγορία των χρηματοδοτικών ιδρυμάτων.
- Ενισχύεται το πλαίσιο εποπτείας των πιστωτικών ιδρυμάτων και θεσπίζονται μέτρα εξυγίανσης εκ μέρους της Τράπεζας της Ελλάδος επί αυτών, με στόχο την αποτελεσματική διασφάλιση της χρηματοοικονομικής σταθερότητας. Ειδικότερα, ενισχύονται σημαντικά οι εποπτικές αρμοδιότητες της Τράπεζας της Ελλάδος προκειμένου να αντιμετωπισθεί έγκαιρα η μη συμμόρφωση ή ο κίνδυνος μη συμμόρφωσης πιστωτικών ιδρυμάτων με τις απαιτήσεις του νόμου και των σχετικών αποφάσεών της, και εξειδικεύεται περαιτέρω το ισχύον καθεστώς ειδικής εκκαθάρισης.

Επιπρόσθετα, με την ΠΔ/ΤΕ 2640/18.1.2011, επανακαθορίζονται και συμπληρώνονται οι υποχρεώσεις περιοδικής υποβολής εποπτικής φύσεως στοιχείων και πληροφοριών από τα πιστωτικά ιδρύματα, ορισμένα χρηματοδοτικά ιδρύματα και τα ιδρύματα πληρωμών προς την Τράπεζα της Ελλάδος και καθορίζονται τα πρόσωπα που έχουν ειδική σχέση με το πιστωτικό ίδρυμα

## **Κεφαλαιακή Επάρκεια (Βασιλεία II)**

Με τις ΠΔ/ΤΕ 2630/2010, 2588/2007, 2589/2007, 2590/2007, 2646/2011, 2592/2007, 2645/2011, 2594/2007, 2595/2007, 2635/2010 και ΠΔ/ΤΕ 2620/28.08.2009 ολοκληρώνεται, κατ' εξουσιοδότηση του ν.3601/2007, η ενσωμάτωση στο ελληνικό δίκαιο των εξειδικευμένων διατάξεων των Οδηγιών 2006/48/ΕΚ και 2006/49/ΕΚ σχετικά με την επάρκεια των ιδίων κεφαλαίων των πιστωτικών ιδρυμάτων και των ΑΕΠΕΥ. Το εν λόγω εποπτικό πλαίσιο, γνωστό

και ως Βασιλεία II, καθιέρωσε τους ακόλουθους τρεις θεμελιώδεις άξονες εποπτείας («Πυλώνες»):

- Τις μεθόδους προσδιορισμού των κεφαλαιακών απαιτήσεων έναντι των κινδύνων που τα πιστωτικά ιδρύματα κατά κανόνα αντιμετωπίζουν στο πλαίσιο της άσκησης των δραστηριοτήτων τους και καθιερώνονται κεφαλαιακές απαιτήσεις και για το λειτουργικό κίνδυνο (Πυλώνας 1).
- Τις αρχές, τα κριτήρια και τη διαδικασία με την οποία καταρχάς τα ίδια τα πιστωτικά ιδρύματα και κατ' ακολουθίαν η εποπτική αρχή (Τράπεζα της Ελλάδος) αξιολογούν την επάρκεια των κεφαλαίων και των συστημάτων διαχείρισης κινδύνων κάθε πιστωτικού ιδρύματος χωριστά, σε σχέση με τους πάσης φύσεως κινδύνους στους οποίους αυτό εκτίθεται ή ενδέχεται να εκτεθεί, πέραν από εκείνους που αντιμετωπίζονται στον Πυλώνα 1 (Πυλώνας 2).
- Τις υποχρεώσεις δημοσιοποίησης στοιχείων για την ενίσχυση της διαφάνειας και της πειθαρχίας της αγοράς με την παροχή στους ενδιαφερόμενους της δυνατότητας σύγκρισης τόσο της πολιτικής για τη διαχείριση κινδύνων, της κεφαλαιακής και οργανωτικής επάρκειας των πιστωτικών ιδρυμάτων, παρέχοντας έτσι κίνητρο για την βελτίωσή τους, όσο και των μεθόδων και πρακτικών που εφαρμόζουν οι εποπτικές αρχές (Πυλώνας 3).

### **ΠΔ/ΤΕ 2630/2010 «Ορισμός των Ιδίων Κεφαλαίων των πιστωτικών ιδρυμάτων που έχουν την έδρα τους στην Ελλάδα»**

Με την ΠΔ/ΤΕ 2630/29.10.2010, η οποία αντικαθιστά την ΠΔ/ΤΕ 2587/20.08.2007:

(i) κωδικοποιούνται σε ενιαίο κείμενο μεμονωμένες κανονιστικές ρυθμίσεις που ισχύουν και αφορούν στην εποπτική αναγνώριση των δικαιωμάτων μειοψηφίας, στη δυνατότητα μερικής ενοποίησης (solo consolidation) επιμέρους θυγατρικών των πιστωτικών ιδρυμάτων και στην επαναγορά υβριδικών τίτλων, και  
(ii) ενσωματώνονται οι διατάξεις της Οδηγίας 2009/111/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου που αφορούν στον ορισμό των ιδίων κεφαλαίων των πιστωτικών ιδρυμάτων και ειδικότερα καθορίζονται:

α. νέες προϋποθέσεις, με βάση τα κριτήρια της μονιμότητας, της ευελιξίας στην αναστολή καταβολής πληρωμών τόκων/μερισμάτων και της απορρόφησης ζημιών, καθώς και νέα όρια για την αναγνώριση των υβριδικών τίτλων στα Βασικά Ιδια Κεφάλαια (Tier 1 Capital) των πιστωτικών ιδρυμάτων, και

β. προϋποθέσεις για την αναγνώριση των συνεταιριστικών μερίδων στα Βασικά Ιδια Κεφάλαια (Tier 1 Capital) των πιστωτικών ιδρυμάτων που λειτουργούν με τη μορφή του πιστωτικού συνεταιρισμού.

**ΠΔ/ΤΕ 2588/20.8.2007 «Υπολογισμός Κεφαλαιακών Απαιτήσεων έναντι του Πιστωτικού Κινδύνου σύμφωνα με την Τυποποιημένη Προσέγγιση» (τροποποιητική ΠΔ/ΤΕ 2631/29.10.2010)**

Με την Πράξη αυτή καθορίζεται ο τρόπος υπολογισμού των κεφαλαιακών απαιτήσεων για τον πιστωτικό κίνδυνο με την Τυποποιημένη Προσέγγιση (Standardised Approach), που είναι η απλούστερη από τις νέες εναλλακτικές σχετικές προσεγγίσεις. Με την προσέγγιση αυτή βελτιώνεται το προϊσχύον πλαίσιο με την καθιέρωση αναλογικότερης σύνδεσης των ιδίων κεφαλαίων προς τον αναλαμβανόμενο κίνδυνο, καθώς:

α) Διευρύνεται η κλίμακα των προκαθορισμένων συντελεστών με τους οποίους σταθμίζεται κάθε κατηγορία χρηματοδότησης ή άλλου ανοίγματος της τράπεζας.

β) Λαμβάνονται υπόψη παράμετροι όπως η πιστοληπτική διαβάθμιση του πιστούχου από αναγνωρισμένους Εξωτερικούς Οργανισμούς Πιστοληπτικής Αξιολόγησης (ΕΟΠΑ), η διασπορά των κινδύνων που επιτρέπει τη μείωση από 100% σε 75% του συντελεστή στάθμισης για τον κίνδυνο των μέχρι ποσού 1 εκατ. ευρώ πιστώσεων προς φυσικά πρόσωπα ή μικρομεσαίες επιχειρήσεις, η εξασφάλιση από κατοικίες που επιτρέπει τη μείωση του συντελεστή στάθμισης των δανείων από 50% σε 35%, ενώ, αντιθέτως, η εμφάνιση καθυστέρησης αποπληρωμής άνω των 90 ημερών οδηγεί σε αύξηση του συντελεστή κ.λπ.

γ) Αναγνωρίζονται και άλλα είδη εξασφαλίσεων, καθώς και πιο εξελιγμένες τεχνικές μείωσης του πιστωτικού κινδύνου, όπως τα πιστωτικά παράγωγα.

**ΠΔ/ΤΕ 2589/20.8.2007 «Υπολογισμός Κεφαλαιακών Απαιτήσεων έναντι του Πιστωτικού Κινδύνου σύμφωνα με την Προσέγγιση Εσωτερικών Διαβαθμίσεων» (τροποποιητική ΠΔ/ΤΕ2631/29.10.2010)**

Θεσπίζεται η προσέγγιση εσωτερικών διαβαθμίσεων (Internal Ratings Based Approach), η οποία εισάγει εξ ολοκλήρου νέα μεθοδολογία υπολογισμού των κεφαλαιακών απαιτήσεων με βάση παραμέτρους κινδύνου, όπως η πιθανότητα αθέτησης υποχρέωσης του πιστούχου (Probability of Default) και η ζημία του πιστωτικού ιδρύματος σε περίπτωση αθέτησης (Loss Given Default), επιτρέποντας για πρώτη φορά στα πιστωτικά ιδρύματα να χρησιμοποιούν τα εσωτερικά τους συστήματα διαχείρισης και υποδείγματα για την εκτίμηση των παραμέτρων αυτών.

Η χρησιμοποίηση της πιο πάνω προσέγγισης και της πιο εξελιγμένης εκδοχής της (Advanced IRB) προϋποθέτει την έγκριση της Τράπεζας της Ελλάδος ή της εποπτικής αρχής της χώρας-έδρας της μητρικής, εφόσον πρόκειται για θυγατρική τράπεζα με έδρα στην Ευρωπαϊκή Ένωση, μετά από διαβούλευση στην οποία συμμετέχει και η Τράπεζα της Ελλάδος. Η έγκριση παρέχεται εφόσον διαπιστωθεί ότι ικανοποιούνται συγκεκριμένες προϋποθέσεις όσον αφορά την επάρκεια των εσωτερικών συστημάτων που η τράπεζα έχει αναπτύξει για τη διαβάθμιση των πιστούχων και των πιστοδοτήσεων, την ποσοτικοποίηση των παραμέτρων κινδύνου, την επικύρωση των σχετικών αποτελεσμάτων και την αξιοποίησή τους στη λήψη των αποφάσεων για τη χορήγηση και την τιμολόγηση των δανείων.

**ΠΔ/ΤΕ 2590/20.8.2007 «Ελάχιστες Κεφαλαιακές Απαιτήσεις των Πιστωτικών Ιδρυμάτων για το Λειτουργικό Κίνδυνο» (τροποιοητική ΠΔ/ΤΕ 2631/29.10.2010)**

Η καθιέρωση κεφαλαιακών απαιτήσεων για το λειτουργικό κίνδυνο αποτελεί μια από τις σημαντικές καινοτομίες του νέου πλαισίου. Η έννοια του εν λόγω κινδύνου αφορά στις ενδεχόμενες ζημιές που μπορεί να προκληθούν από ανεπάρκεια ή λάθη διαδικασιών ή προσώπων, καλύπτοντας και τον νομικό κίνδυνο. Με την εν λόγω Πράξη παρέχεται, επίσης, η δυνατότητα στις τράπεζες να επιλέγουν μεταξύ τυποποιημένων και εξελιγμένων προσεγγίσεων για τον υπολογισμό των κεφαλαιακών απαιτήσεων και για τον κίνδυνο αυτό.

**ΠΔ/ΤΕ 2646/9.9.2011 «ΥπολογισμόςΚεφαλαιακών Απαιτήσεων των Πιστωτικών Ιδρυμάτων για τον Κίνδυνο Αγοράς»**

Η ΠΔ/ΤΕ 2646/2011 αντικαθιστά την ΠΔ/ΤΕ 2591/2007, όπως ισχύει, προκειμένου να ενσωματώσει στην ελληνική έννομη τάξη τις διατάξεις της Οδηγίας 2010/76/ΕΚ. Οι κύριες αλλαγές σχετίζονται με τον υπολογισμό των κεφαλαιακών απαιτήσεων για το χαρτοφυλάκιο συναλλαγών. Ειδικότερα, προβλέπεται, μεταξύ άλλων:

- η υποχρέωση των πιστωτικών ιδρυμάτων τα οποία έχουν εγκεκριμένα εσωτερικά μοντέλα για τον υπολογισμό των κεφαλαιακών απαιτήσεων για τον γενικό κίνδυνο, να υπολογίζουν επιπλέον κεφαλαιακές απαιτήσεις, σύμφωνα με την εκτίμηση της δυναμικής ζημιάς κάτω από ακραίες συνθήκες (stressed VaR)
- η υποχρέωση των πιστωτικών ιδρυμάτων, τα οποία έχουν εγκεκριμένα εσωτερικά μοντέλα για τον υπολογισμό των κεφαλαιακών απαιτήσεων για τον ειδικό κίνδυνο, να υπολογίζουν επιπλέον κεφαλαιακές απαιτήσεις για τον κίνδυνο αθέτησης και μεταβολής της πιστοληπτικής αξιοπιστίας (incremental default and migration risk) του εκδότη χρεωστικών τίτλων και μετοχών
- η υποχρέωση των πιστωτικών ιδρυμάτων να διενεργούν, κατ' ελάχιστον, υποθετικό εκ των υστέρων δοκιμαστικό έλεγχο (hypothetical back testing) για την αξιολόγηση των εσωτερικών υποδειγμάτων δυναμικής ζημιάς
- η αύξηση του συντελεστής στάθμισης από 4% σε 8% για τον ειδικό κίνδυνο, για τον υπολογισμό της κεφαλαιακής απαίτησης από μετοχές με βάση την τυποποιημένη μέθοδο
- η υποχρέωση των πιστωτικών ιδρυμάτων να καθιερώσουν διαδικασίες με τις οποίες θα προσαρμόζουν την τρέχουσα αξία των στοιχείων τους, τα οποία δεν είναι άμεσα ρευστοποιήσιμα

**ΠΔ/ΤΕ 2592/20.8.2007 «Δημοσιοποίηση εκ μέρους των πιστωτικών ιδρυμάτων στοιχείων και πληροφοριών σχετικά με την κεφαλαιακή τους επάρκεια και τους κινδύνους που αναλαμβάνουν καθώς και τη διαχείριση αυτών» (τροποιοητική ΠΔ/ΤΕ 2632/29.10.2010)**

Καθορίζονται τα γενικά κριτήρια και υποχρεώσεις δημοσιοποίησης από τα πιστωτικά ιδρύματα πληροφοριών που αφορούν κυρίως:

α) τις επιχειρήσεις του ομίλου του πιστωτικού ιδρύματος (όπως ορίζεται για σκοπούς εποπτείας αλλά και για λογιστικούς σκοπούς),

β) τα ίδια κεφάλαια και τον τρόπο υπολογισμού της κεφαλαιακής του επάρκειας, και

γ) την έκθεσή του σε κάθε κατηγορία κινδύνου, περιλαμβανομένων των στρατηγικών στόχων, των μεθόδων αξιολόγησης και των τεχνικών μείωσης των κινδύνων αυτών.

Επίσης, καθορίζονται η συχνότητα, ο τρόπος και τα μέσα δημοσιοποίησης και επαλήθευσης των πληροφοριών. Οι σχετικές πληροφορίες θα δημοσιοποιούνται, κατά κανόνα, τουλάχιστον μία φορά το χρόνο στον ιστοχώρο του πιστωτικού ιδρύματος.

**ΠΔ/ΤΕ 2645/2011 «Υπολογισμός Σταθμισμένων Ανοιγμάτων για Θέσεις σε Τιτλοποίηση»**

Με την ΠΔ/ΤΕ 2645/12.08.2011, η οποία αντικαθιστά την ΠΔ/ΤΕ 2633/29.10.2010:

(i) κωδικοποιούνται σε ενιαίο κείμενο οι διατάξεις που αφορούν στον υπολογισμό των κεφαλαιακών απαιτήσεων των τραπεζών έναντι του πιστωτικού κινδύνου ανοιγμάτων τους σε τιτλοποιήσεις (securitisation), προκειμένου να διασφαλιστεί ότι τα πιστωτικά ιδρύματα διαθέτουν επαρκή κεφάλαια για την κάλυψη του πιστωτικού κινδύνου που διατηρούν ή αναλαμβάνουν στο πλαίσιο της εν λόγω τεχνικής και

(ii) ενσωματώνονται οι διατάξεις της Οδηγίας 2010/76/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου που αφορούν στις κεφαλαιακές απαιτήσεις για τις θέσεις σε επανατιτλοποίηση (CRD III) και ειδικότερα:

α. εισάγεται ο ορισμός της «επανατιτλοποίησης» και της «θέσης σε επανατιτλοποίηση»,  
β. προστίθενται συντελεστές στάθμισης για θέσεις σε επανατιτλοποιήσεις,  
γ. εξειδικεύεται η εφαρμογή της μεθόδου του εποπτικού υποδείγματος στις θέσεις σε επανατιτλοποίηση.

**ΠΔ/ΤΕ 2594/20.8.2007 «Κίνδυνος αντισυμβαλλομένου» και η τροποιοητική αυτής, ΠΔ/ΤΕ 2634/29.10.2010**

Παρέχεται στα πιστωτικά ιδρύματα η δυνατότητα χρησιμοποίησης και νέων εξελιγμένων μεθόδων για τον υπολογισμό της αξίας των ανοιγμάτων, ειδικά από συναλλαγές τύπου πώλησης και επαναγοράς (REPOS) και από συμβάσεις παραγώγων, προκειμένου να υπολογιστούν οι κεφαλαιακές απαιτήσεις έναντι του κινδύνου αντισυμβαλλομένου. Ο κίνδυνος αυτός αφορά τη ζημία που θα προκύψει για το πιστωτικό ίδρυμα εάν ο αντισυμβαλλόμενος δεν

αναπακριθεί στις υποχρεώσεις του, λαμβανομένων υπόψη και των πιθανών διακυμάνσεων των τιμών αγοράς των χρηματοπιστωτικών μέσων τα οποία αφορά η συναλλαγή.

**ΠΔ/ΤΕ 2595/20.8.2007 «Καθορισμός των κριτηρίων που πρέπει να διέπουν τη Διαδικασία Αξιολόγησης Επάρκειας Εσωτερικού Κεφαλαίου (ΔΑΕΕΚ) των πιστωτικών ιδρυμάτων και της Διαδικασίας Εποπτικής Αξιολόγησης (ΔΕΑ) από την Τράπεζα της Ελλάδος»**

Με την Πράξη αυτή θεσπίζονται πέραν των προβλεπομένων στον Πυλώνα 1:

α) Ποιοτικού χαρακτήρα κριτήρια υπολογισμού της κεφαλαιακής επάρκειας κάθε πιστωτικού ιδρύματος, ανάλογα με τα ιδιαίτερα χαρακτηριστικά του.

β) Η έννοια των «εσωτερικών κεφαλαίων», η οποία είναι ευρύτερη εκείνης των «εποπτικών» που υπολογίζονται με τις μεθόδους του Πυλώνα 1, καθώς αφορά τα κεφάλαια που το πιστωτικό ίδρυμα πρέπει να διαθέτει σε επάρκεια από πλευράς ποσότητας, ποιότητας και κατανομής για την αντιμετώπιση των πάσης φύσεως κινδύνων που έχει αναλάβει ή στους οποίους ενδέχεται να εκτεθεί. Ως τέτοιοι κίνδυνοι θεωρούνται, ενδεικτικά, αυτοί που δεν καλύπτονται ή δεν αντιμετωπίζονται επαρκώς στο πλαίσιο του Πυλώνα 1, όπως ο κίνδυνος συγκέντρωσης, ο κίνδυνος στρατηγικής, ο κίνδυνος φήμης αλλά και εξωγενείς κίνδυνοι που απορρέουν από το θεσμικό, οικονομικό ή επιχειρηματικό περιβάλλον.

γ) Η διαδικασία αξιολόγησης από την Τράπεζα της Ελλάδος της εν γένει συμμόρφωσης του πιστωτικού ιδρύματος προς τις εποπτικές του υποχρεώσεις, η οποία θα αποτελεί αντικείμενο διαλόγου με το πιστωτικό ίδρυμα. Στόχος του διαλόγου είναι η αμοιβαία κατανόηση των εφαρμοζόμενων μεθόδων και διαδικασιών και η έγκαιρη αντιμετώπιση των αδυναμιών τους. Στο πλαίσιο αυτό, η Τράπεζα της Ελλάδος μπορεί να λαμβάνει τα εποπτικά μέτρα που προβλέπονται από τον ν. 3601/2007, μεταξύ των οποίων και η επιβολή πρόσθετων προβλέψεων ή, εφόσον κρίνει ότι με τα σχετικά διορθωτικά μέτρα δεν αντιμετωπίζονται επαρκώς οι κίνδυνοι, να επιβάλλει πρόσθετες κεφαλαιακές απαιτήσεις. Τα επιμέρους θέματα της σχετικής διαδικασίας, η οποία θα εφαρμόζεται ως προς το εύρος και τη συχνότητα με βάση την αρχή της αναλογικότητας, θα εξειδικευθούν περαιτέρω στο πλαίσιο των διαβουλεύσεων της Τράπεζας της Ελλάδος με τα πιστωτικά ιδρύματα.

**ΠΔ/ΤΕ 2635/29.10.2010 «Εποπτεία και έλεγχος των μεγάλων χρηματοδοτικών ανοιγμάτων των πιστωτικών ιδρυμάτων»**

Με την Πράξη αυτή προσαρμόζονται και κωδικοποιούνται σε ενιαίο κείμενο οι ισχύουσες διατάξεις σχετικά με τον έλεγχο των μεγάλων χρηματοδοτικών ανοιγμάτων.

Οι κυριότερες προσαρμογές αφορούν:

α) την αναγνώριση εξασφαλίσεων που μειώνουν το ύψος των μεγάλων χρηματοδοτικών ανοιγμάτων, κατ' αντιστοιχία με τα καθοριζόμενα στις προαναφερόμενες Πράξεις Διοικητή τις σχετικές με τον Πιστωτικό Κίνδυνο και τον Κίνδυνο Αγοράς,



β) τον καθορισμό χωριστού ορίου για το σύνολο των χρηματοδοτικών ανοιγμάτων της τράπεζας έναντι των σημαντικών μετόχων της και των συνδεδεμένων με αυτούς προσώπων και επιχειρήσεων

**ΠΑ/ΤΕ 2620/28.8.2009 Κωδικοποίηση 2598/02.11.2007 Πλαίσιο εποπτείας καλυμμένων ομολογιών που εκδίδονται από Π.Ι. covered bonds**

Με την Πράξη αυτή συμπληρώνονται και κωδικοποιούνται σε ενιαίο κείμενο οι διατάξεις που αφορούν στο πλαίσιο εποπτείας των καλυμμένων ομολογιών οι οποίες εκδίδονται από πιστωτικά ιδρύματα, βάσει σχετικής εξουσιοδότησης που παρέχεται από το άρθρο 91 του ν. 3601/2007 (όπως τροποποιήθηκε από το άρθρο 48 του ν. 3693/2008 και το άρθρο 69 του ν. 3746/2009) στην Τράπεζα της Ελλάδος.

Οι καλυμμένες ομολογίες (covered bonds) είναι ομολογιακοί τίτλοι, οι οποίοι παρέχουν στους επενδυτές μία πρόσθετη εξασφάλιση επί ενός σαφώς διαχωρισμένου, από τα λοιπά περιουσιακά στοιχεία του πιστωτικού ιδρύματος, χαρτοφυλακίου υψηλής ποιότητας απαιτήσεων. Το εν λόγω χαρτοφυλάκιο, το οποίο αποτελεί το κάλυμμα της έκδοσης, απαρτίζεται κυρίως από ενυπόθηκα δάνεια και κρατικά ομόλογα.

Ειδικότερα με την παρούσα Πράξη:

α. Αναγνωρίζεται εποπτικά νέο σχήμα έκδοσης καλυμμένων ομολογιών που έχει εισαχθεί με το ν. 3746/2009, σύμφωνα με το οποίο παρέχεται η δυνατότητα έκδοσης καλυμμένων ομολογιών από πιστωτικά ιδρύματα με εγγυητή εταιρία ειδικού σκοπού στην οποία έχει μεταβιβασθεί το χαρτοφυλάκιο ασφαλείας και η οποία ευθύνεται ανεκκλήτως, άνευ όρων και αυτοτελώς ως αυτοφειλέτης για το σύνολο των απαιτήσεων των ομολογιούχων και άλλων δανειστών οι απαιτήσεις των οποίων συνδέονται με την έκδοση καλυμμένων ομολογιών.

β. Περιορίζονται τα αποδεκτά ως εξασφάλιση ανοίγματα που αναφέρονται στις παραγράφους 8β (i),(ii) και (iii) του Τμήματος Β της ΠΔ/ΤΕ 2588/20.8.2007 μόνο σε δάνεια.

γ. Καθορίζεται ότι τα δάνεια που υπερβαίνουν τις 90 ημέρες καθυστέρησης δεν θα πρέπει να συμπεριλαμβάνονται στο χαρτοφυλάκιο ασφαλείας κατά τον υπολογισμό των ελέγχων επάρκειάς του.

δ. Εξειδικεύονται οι έλεγχοι οι οποίοι θα διενεργούνται από τους ανεξάρτητους ελεγκτές κατά τους ετήσιους ελέγχους που προβλέπονται από την παρούσα Πράξη για τις εκδόσεις καλυμμένων ομολογιών που θα πραγματοποιηθούν εφεξής.

**ΟΔΗΓΙΑ 2007/64/ΕΚ  
ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ,  
ΤΗΣ 13ΗΣ ΝΟΕΜΒΡΙΟΥ 2007, ΓΙΑ ΤΙΣ ΥΠΗΡΕΣΙΕΣ ΠΛΗΡΩΜΩΝ  
ΣΤΗΝ ΕΣΩΤΕΡΙΚΗ ΑΓΟΡΑ, ΤΗΝ ΤΡΟΠΟΠΟΙΗΣΗ ΤΩΝ ΟΔΗΓΙΩΝ  
97/7/ΕΚ, 2002/65/ΕΚ, 2005/60/ΕΚ ΚΑΙ 2006/48/ΕΚ ΚΑΙ  
ΚΑΤΑΡΓΗΣΗ ΤΗΣ ΟΔΗΓΙΑΣ 97//5/ΕΚ, ΕΕ L 319 ΤΗΣ 5.12.2007**

Η έκδοση της Οδηγίας 2007/64/ΕΚ,1, αποτελεί μια ιδιαίτερα σημαντική πρωτοβουλία στον τομέα των πληρωμών για τρεις κυρίως λόγους:

- Πρώτον, λαμβανομένων υπόψη του αποσπασματικού μέχρι την έκδοσή της πλαισίου που διέπει σε κοινοτικό επίπεδο τις πληρωμές και των εξελίξεων που επήλθαν με την εισαγωγή του Ενιαίου Χώρου Πληρωμών σε ευρώ (SEPA), είναι ιδιαίτερα σημαντικό ότι με την Οδηγία αυτή επιχειρείται η θέσπιση σε κοινοτικό επίπεδο ενός σύγχρονου και συνεκτικού νομικού πλαισίου για τις υπηρεσίες πληρωμών που λαμβάνει ταυτόχρονα υπόψη τις απαιτήσεις που πρέπει να πληρούνται για τη δυνατότητα παροχής υπηρεσιών πληρωμών στο πλαίσιο του SEPA.
- Δεύτερον, με την Οδηγία αυτή προσδιορίζονται όλες οι κατηγορίες φορέων παροχής υπηρεσιών πληρωμών που μπορούν νόμιμα να παρέχουν υπηρεσίες πληρωμών στην Κοινότητα, όπως ενδεικτικά, τα πιστωτικά ιδρύματα και τα ιδρύματα ηλεκτρονικού χρήματος, ενώ εισάγεται και μια νέα κατηγορία φορέων παροχής υπηρεσιών πληρωμών, τα καλούμενα «ιδρύματα πληρωμών», για τα οποία προβλέπονται συγκεκριμένες προϋποθέσεις αδειοδότησης και άσκησης δραστηριότητας κατά την παροχή εκ μέρους τους υπηρεσιών πληρωμών.
- Τρίτον, καθορίζονται διεξοδικά αφενός μεν οι κανόνες διαφάνειας και οι υποχρεώσεις ενημέρωσης που πρέπει να τηρούνται σχετικά με τις υπηρεσίες πληρωμών και αφετέρου τα δικαιώματα και οι υποχρεώσεις των χρηστών υπηρεσιών πληρωμών και των παρεχόντων αυτές ως τακτική απασχόληση ή επιχειρηματική δραστηριότητα.

Επιχειρείται συνεπώς με την εν λόγω Οδηγία μια συνολική και συστηματική ρύθμιση της παροχής υπηρεσιών πληρωμών σε κοινοτικό επίπεδο, τόσο σε ό,τι αφορά τους φορείς παροχής τους, όσο και σε σχέση με τα δικαιώματα και τις υποχρεώσεις που απορρέουν για τους χρήστες αυτών, με γνώμονα τη διασφάλιση ίσων όρων ανταγωνισμού και την παροχή περισσότερων επιλογών στους καταναλωτές.

Με την επιφύλαξη των διακριτικών ευχερειών που παρέχονται στα κράτη μέλη, η Οδηγία διέπεται από την αρχή της μέγιστης εναρμόνισης και, συνεπώς, τα κράτη μέλη δεν μπορούν να εισάγουν ή να διατηρούν άλλες διατάξεις από αυτές που καθορίζονται στην Οδηγία.

## **Προσωπικό και αντικειμενικό πεδίο εφαρμογής της Οδηγίας**

### **1. Προσωπικό πεδίο εφαρμογής**

Σύμφωνα με την Οδηγία, οι φορείς παροχής υπηρεσιών πληρωμών διακρίνονται συστηματικά στις ακόλουθες έξι κατηγορίες:

1. πιστωτικά ιδρύματα,
2. ιδρύματα ηλεκτρονικού χρήματος,
3. γραφεία ταχυδρομικών επιταγών, τα οποία εξουσιοδοτούνται βάσει της εθνικής νομοθεσίας να παρέχουν υπηρεσίες πληρωμών,
4. ιδρύματα πληρωμών,
5. η Ευρωπαϊκή Κεντρική Τράπεζα και οι εθνικές κεντρικές τράπεζες όταν δεν ενεργούν ως νομισματικές ή άλλες δημόσιες αρχές, και
6. τα κράτη μέλη ή οι περιφερειακές ή τοπικές αρχές τους όταν δεν ενεργούν ως δημόσιες αρχές.

### **2. Αντικειμενικό πεδίο εφαρμογής**

Οι υπηρεσίες πληρωμών σύμφωνα με την Οδηγία 2007/64/ΕΚ διακρίνονται συστηματικά στις ακόλουθες κατηγορίες:

- Υπηρεσίες που επιτρέπουν τις καταθέσεις (σε) ή αναλήψεις μετρητών από λογαριασμό πληρωμών, καθώς και όλες οι δραστηριότητες που απαιτούνται για την τήρηση λογαριασμού πληρωμών,
- Εκτέλεση πράξεων πληρωμής (α) είτε σε λογαριασμό πληρωμών που έχει ανοίξει ο χρήστης στο φορέα παροχής υπηρεσιών πληρωμών του ή σε άλλο φορέα παροχής υπηρεσιών πληρωμών (β) είτε στο πλαίσιο των οποίων τα χρηματικά ποσά καλύπτονται από πιστωτικό άνοιγμα για το χρήστη υπηρεσιών πληρωμών και, ειδικότερα, (και στις δύο περιπτώσεις), εκτέλεση εντολών άμεσης χρέωσης, συμπεριλαμβανομένης της εφάπαξ χρέωσης, εκτέλεση πράξεων πληρωμής με κάρτα ή ανάλογο μέσο, και εκτέλεση μεταφορών πίστωσης, συμπεριλαμβανομένων των πάγιων εντολών,
- Έκδοση ή/και απόκτηση εργαλείων πληρωμών,
- Εμβάσματα, και
- Εκτέλεση πράξεων πληρωμής όπου η συγκατάθεση του πληρωτή για να εκτελεσθεί μια πράξη πληρωμής δίδεται μέσω τηλεπικοινωνιακής, ψηφιακής ή πληροφορικής συσκευής και η πληρωμή γίνεται στο φορέα εκμετάλλευσης επικοινωνιακού, πληροφορικού συστήματος ή δικτύου, ο οποίος ενεργεί αποκλειστικά ως μεσάζων μεταξύ του χρήστη υπηρεσιών πληρωμών και του προμηθευτή αγαθών ή υπηρεσιών.

### **3. Οι πράξεις πληρωμών**

Ως πράξεις πληρωμών νοούνται οι ενέργειες στις οποίες προβαίνουν ο πληρωτής ή ο δικαιούχος, και συνίστανται στη διάθεση, μεταβίβαση ή ανάληψη χρηματικών ποσών, ανεξάρτητα από οποιαδήποτε υποκείμενη σχέση μεταξύ πληρωτή και δικαιούχου. Οι πράξεις πληρωμών διακρίνονται σύμφωνα με την Οδηγία σε δύο μεγάλες κατηγορίες, εκ των οποίων:

- η πρώτη αφορά τις μεμονωμένες πράξεις πληρωμών, και

• η δεύτερη τις πράξεις πληρωμών που καλύπτονται από σύμβαση- πλαίσιο, δηλαδή σύμβαση που διέπει τη μελλοντική εκτέλεση ατομικών και διαδοχικών πράξεων πληρωμών και η οποία μπορεί να περιλαμβάνει την υποχρέωση και τους όρους σύστασης λογαριασμού πληρωμών.

### **Τα ιδρύματα πληρωμών**

Όπως προαναφέρθηκε, τα ιδρύματα πληρωμών αποτελούν νέα κατηγορία φορέων παροχής υπηρεσιών, η οποία καθιερώνεται και ρυθμίζεται για πρώτη φορά με την Οδηγία 2007/64/ΕΚ. Ειδικότερα, με την εν λόγω Οδηγία ρυθμίζονται διεξοδικά οι προϋποθέσεις που πρέπει να πληρούνται για την αδειοδότηση και άσκηση δραστηριότητας των ιδρυμάτων πληρωμών.

Συγκεκριμένα:

- Προσδιορίζονται τα στοιχεία που πρέπει να περιλαμβάνει η αίτηση στις αρμόδιες αρχές για την αδειοδότησή τους και οι προϋποθέσεις που πρέπει να πληρούνται για την αδειοδότησή τους, καθώς επίσης και οι λόγοι ανάκλησης της αδειάς τους,
- Καθορίζεται το αρχικό κεφάλαιο που πρέπει να διαθέτουν κατά τη στιγμή της αδειοδότησής τους ανάλογα με τις υπηρεσίες πληρωμών που παρέχουν,
- Καθορίζονται τα ίδια κεφάλαια που πρέπει να διαθέτουν και ο τρόπος με τον οποίο πρέπει να υπολογίζονται,
- Καθιερώνεται η υποχρέωση διασφάλισης των χρηματικών ποσών που τυχόν λαμβάνουν από χρήστες υπηρεσιών πληρωμών ή μέσω άλλου φορέα παροχής υπηρεσιών πληρωμών για την εκτέλεση πράξεων πληρωμών, εφόσον παράλληλα με την παροχή υπηρεσιών πληρωμών ασκούν και άλλες επιχειρηματικές δραστηριότητες σύμφωνα με τα προβλεπόμενα στην Οδηγία, και
- Προσδιορίζονται οι προϋποθέσεις που πρέπει να πληροί το ίδρυμα πληρωμών εφόσον προτίθεται να παρέχει υπηρεσίες πληρωμών μέσω αντιπροσώπου και εν γένει οι προϋποθέσεις ανάθεσης δραστηριοτήτων σε εξωτερικούς φορείς.

Για τα ιδρύματα πληρωμών που αδειοδοτούνται σύμφωνα με τα προαναφερθέντα, ισχύει η αρχή της αμοιβαίας αναγνώρισης, μπορούν δηλαδή να παρέχουν υπηρεσίες σε όλα τα υπόλοιπα κράτη μέλη, είτε με καθεστώς εγκατάστασης, είτε με καθεστώς ελεύθερης παροχής υπηρεσιών.

Οι αρμόδιες για την αδειοδότηση και την προληπτική εποπτεία των ιδρυμάτων πληρωμών αρχές καθορίζονται σύμφωνα με την Οδηγία από τα κράτη μέλη, ενώ περιέχονται διεξοδικές διατάξεις τόσο για τον τρόπο με τον οποίο οι αρμόδιες αρχές θα ασκούν τις εξουσίες τους όσο και για τη μεταξύ τους συνεργασία.

### **Διαφάνεια και απαιτήσεις ενημέρωσης που διέπουν τις υπηρεσίες πληρωμών**

Εκτός από τις γενικές διατάξεις της Οδηγίας που αφορούν, μεταξύ άλλων, την απαγόρευση χρέωσης του χρήστη υπηρεσιών πληρωμών για την παροχή εκ μέρους του φορέα παροχής υπηρεσιών πληρωμών των προβλεπόμενων στην Οδηγία πληροφοριών, καθορίζονται διεξοδικά οι πληροφορίες που πρέπει να παρέχονται τόσο στο πλαίσιο μεμονωμένων πράξεων πληρωμών, όσο και για τις πράξεις πληρωμών που καλύπτονται από σύμβαση-πλαίσιο. Οι εν λόγω πληροφορίες που διαφοροποιούνται αντίστοιχα ως προς το περιεχόμενό τους αφορούν:

- Το στάδιο πριν από τη δέσμευση του χρήστη της υπηρεσίας πληρωμών από σύμβαση,
- Το στάδιο μετά τη χρέωση του λογαριασμού πληρωμής ή όταν ο πληρωτής δεν χρησιμοποιεί λογαριασμό πληρωμών, μετά την παραλαβή της εντολής πληρωμής από το φορέα παροχής υπηρεσιών πληρωμής,
- Το στάδιο μετά την εκτέλεση της εντολής πληρωμής από το φορέα παροχής υπηρεσιών πληρωμής, και
- Ειδικά σε περίπτωση σύμβασης-πλαίσιοι, κάθε τροποποίηση των αρχικών όρων αυτής, καθώς και συγκεκριμένη πληροφόρηση για κάθε μεμονωμένη πράξη πληρωμής, την οποία κίνησε ο πληρωτής και η οποία καλύπτεται από σύμβαση πλαίσιο.

### **Δικαιώματα και υποχρεώσεις σχετικά με την παροχή και τη χρήση υπηρεσιών πληρωμών**

Η Οδηγία περιέχει τέλος ιδιαίτερα διεξοδικές ρυθμίσεις αναφορικά με τα δικαιώματα και τις υποχρεώσεις τόσο των φορέων παροχής υπηρεσιών πληρωμών, όσο και των χρηστών των εν λόγω υπηρεσιών σε σχέση με την έγκριση και την εκτέλεση πράξεων πληρωμής.

Σε ό,τι αφορά τον φορέα παροχής υπηρεσιών πληρωμών, επισημαίνεται ενδεικτικά ότι οι κυριότερες υποχρεώσεις του συνίστανται στα ακόλουθα:

- Εφόσον εκδίδει το εργαλείο πληρωμών, οφείλει να μην αποκαλύπτει τα εξατομικευμένα στοιχεία ασφαλείας του παρά μόνο στο χρήστη της υπηρεσίας πληρωμών που έχει δικαίωμα χρήσης του εργαλείου πληρωμών, ενώ δεν επιτρέπεται να αποστέλλει εργαλείο πληρωμών που δεν έχει ζητηθεί, εκτός εάν πρόκειται για αντικατάσταση ήδη εκδοθέντος,
- Σε περίπτωση μη εγκεκριμένης πράξης πληρωμών οφείλει να επιστρέφει αμέσως στον πληρωτή το ποσό της μη εγκεκριμένης πράξης, ενώ μπορεί σύμφωνα με το εθνικό δίκαιο που διέπει τη σύμβαση μεταξύ του πληρωτή και του φορέα παροχής υπηρεσιών πληρωμών να παρέχεται και περαιτέρω οικονομική αποζημίωση,
- Μετά τον χρόνο λήψης της εντολής πληρωμής, ο φορέας παροχής υπηρεσιών πληρωμών του πληρωτή οφείλει να πιστώνει το ποσό της πράξης πληρωμής στο λογαριασμό του φορέα παροχής υπηρεσιών πληρωμών του δικαιούχου το αργότερο στο τέλος της επόμενης εργάσιμης ημέρας,
- Η ημερομηνίας αξίας για την πίστωση του λογαριασμού πληρωμών του δικαιούχου ορίζεται ότι είναι το αργότερο η επόμενη εργάσιμη ημέρα κατά την οποία πιστώνεται ο λογαριασμός του φορέα παροχής υπηρεσιών πληρωμών του δικαιούχου με το ποσό της πράξης πληρωμής, ενώ ο τελευταίος μεριμνά επίσης ώστε το ποσό αυτό να είναι στη διάθεση του δικαιούχου αμέσως μόλις ο λογαριασμός του πιστωθεί με το ποσό της πράξης πληρωμής.

Σε ό,τι αφορά τον χρήστη υπηρεσιών πληρωμών, επισημαίνεται ενδεικτικά ότι:

- Σε σχέση με τη χρήση εκ μέρους του εργαλείων πληρωμών, υποχρεούται να τα χρησιμοποιεί σύμφωνα με τους όρους που διέπουν την έκδοση και χρήση τους, καθώς επίσης και να ειδοποιεί χωρίς υπαίτια καθυστέρηση τον φορέα παροχής υπηρεσιών πληρωμών του μόλις υποπέσει στην αντίληψή του απώλεια, κλοπή ή υπεξαίρεση ή μη εγκεκριμένη χρήση του εργαλείου πληρωμών,
- Ο πληρωτής ευθύνεται σχετικά με μη εγκεκριμένες πράξεις πληρωμής μέχρι ανωτάτου ποσού 150 ευρώ, για τις ζημιές που απορρέουν από τη χρήση απολεσθέντος ή κλαπέντος εργαλείου πληρωμών, εκτός εάν έχει ενεργήσει με δόλο ή δεν εκπλήρωσε τις

προβλεπόμενες υποχρεώσεις του (π.χ. ασφαλής φύλαξη του εργαλείου πληρωμών), οπότε ευθύνεται για όλες τις ανωτέρω ζημίες,

- Ο πληρωτής έχει το δικαίωμα επιστροφής εκ μέρους του φορέα παροχής υπηρεσιών πληρωμών του των χρημάτων που αντιστοιχούν σε εγκεκριμένη πράξη πληρωμής, εφόσον κατά την έγκριση δεν προσδιορίστηκε το ακριβές ποσό της πράξης πληρωμής και το ποσό αυτό υπερβαίνει εκείνο που θα ανέμενε εύλογα ο πληρωτής λαμβάνοντας υπόψη τις παραμέτρους που καθορίζονται συγκεκριμένα στην Οδηγία (το δικαίωμά του δε αυτό μπορεί να το ασκήσει εντός 8 εβδομάδων από την ημερομηνία χρέωσης των χρηματικών ποσών).

Κρίνεται πάντως σκόπιμο να επισημανθεί ότι οι εν λόγω διατάξεις της Οδηγίας είναι ιδιαίτερα διεξοδικές, καθώς ρυθμίζουν κάθε επιμέρους περίπτωση ξεχωριστά, εισάγοντας πολύ σημαντικά δικαιώματα για τον καταναλωτή-χρήστη υπηρεσιών πληρωμών και ιδιαίτερα αυξημένες υποχρεώσεις αντίστοιχα για τους φορείς παροχής υπηρεσιών πληρωμών.

---

Ηλεκτρονική Τραπεζική «Αριστέα Σινανιώτη- Ιωάννης Φαρσαρώτας» 100-103 και 239-243  
Παροχή χρηματοοικονομικών υπηρεσιών από απόσταση « Άννα Δεσποτίδου» 19- 44  
Η πρόσβαση στις Χρηματοοικονομικές Υπηρεσίες μέσω διαδικτύου «Ιωάννης Λιναρίτης» 34-44  
Η Οδηγία 2007/64/ΕΚ για τις υπηρεσίες πληρωμών στην εσωτερική αγορά Συνολική θεώρηση «Χρήστος Βλ. Γκόρτσος»  
[www.eurobank.gr](http://www.eurobank.gr)  
[www.ependyseis.gr](http://www.ependyseis.gr)  
[www.bankofgreece.gr](http://www.bankofgreece.gr)

## ΚΕΦΑΛΑΙΟ 2ο

### ΗΛΕΚΤΡΟΝΙΚΑ ΣΥΣΤΗΜΑΤΑ ΠΛΗΡΩΜΩΝ

#### ΔΙΑΧΡΟΝΙΚΗ ΕΞΕΛΙΞΗ ΤΗΣ ΤΡΑΠΕΖΙΚΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

Οι τράπεζες υπήρξαν ο πρώτος κλάδος οικονομικής δραστηριότητας, ο οποίος ήρθε πολύ νωρίς αντιμέτωπος με την ανάγκη για μαζική επεξεργασία πληροφοριών. Ως εκ τούτου, οι τράπεζες ήταν και οι πρώτες επιχειρήσεις που εισήγαγαν τη χρήση μεγάλων συστημάτων επεξεργασίας πληροφοριών. Η εξέλιξη της πληροφορικής διήρκησε περί τις τέσσερις δεκαετίες με διαφορετικούς πάντα ρυθμούς. Η εφαρμογή της στις τράπεζες ήταν αποτέλεσμα των γενικότερων επιτευγμάτων στον κλάδο.

1960	1970	1980	1990 - 2000
ΜΕΘΟΔΟΣ BATCH	TIME SHARING	ΕΞΑΤΟΜΙΚΕΥΜΕΝΗ ΕΠΕΞΕΡΓΑΣΙΑ	ΔΙΚΤΥΑΚΗ ΕΠΕΞΕΡΓΑΣΙΑ
Λογαριασμοί	Τομεακές εφαρμογές	Συστήματα Εντολών	Εσωτερική δικτύωση
Απλά συστήματα διεκπεραίωσης πληρωμών	Εφαρμογές μικρο-οθονών	Συστήματα διαχείρισης υποθέσεων	Client / Server αρχιτεκτονική
Επεξεργασία μαζικών στοιχείων	Τερματικά στα καταστήματα	Μεμονωμένα PC	Workflow Management Systems
Συστήματα εγγραφών	Κεντρική μονάδα επεξεργασίας Στοιχείων	Έξυπνα συστήματα στη θέση εργασίας	Προγράμματα για συγκεκριμένες εργασίες
Προγραμματισμός σε COBOL	Αποθήκευση σε δίσκους και μαγνητικά μέσα	IDV, 4 Generation-γλώσσες	Internet, Multimedia
Διατήρηση καρτών		Electronic Banking	IT ως επεξεργασία εξυπηρέτησης
			Επεξεργασία real - time

Αρχή της εισαγωγής της επεξεργασίας στοιχείων στις τράπεζες αποτέλεσε η μαζική ανάπτυξη της ιδιωτικής πελατείας αρχές του 1960. Το μεγαλύτερο πρόβλημα που είχαν να αντιμετωπίσουν ήταν η διαχείριση μεγάλου όγκου στοιχείων σχετικά με την κίνηση λογαριασμών. Η λογιστική εγγραφή γινόταν με την μέθοδο batch. Η επεξεργασία ελάμβανε χώρα σε κεντρικό υπολογιστή ( mainframe) σταδιακά κατά τη διάρκεια της νύχτας, όπου συγκεντρώνονταν τα στοιχεία. Οι κύριες επεξεργασίες batch ήταν η ενημέρωση των αρχείων και η παραγωγή καταστάσεων.

Η μέθοδος batch αποδείχθηκε ότι ήταν, και σε πολλές περιπτώσεις είναι ακόμη, κατάλληλη για μαζική επεξεργασία στοιχείων σε όλες εκείνες τις περιπτώσεις όπου η άμεση ενημέρωση των αρχείων από τον χρήστη δεν έχει ιδιαίτερη σημασία. Ως τέτοιες θεωρούνται όλες οι εργασίες back office που διενεργούνται χωρίς την παρουσία του πελάτη. Σε αυτές ανήκουν οι χρεοπιστώσεις τόκων, οι ενημερώσεις ενδοτραπεζικών λογαριασμών, η εκτύπωση καταστάσεων, ο συμψηφισμός επιταγών κ.α. Σε όλες τις άλλες περιπτώσεις όπου υπάρχει ανάγκη πρόσβασης του υπαλλήλου-χρήστη στις πληροφορίες του υπολογιστή, π.χ. καταθέσεις, αναλήψεις, μεταφορά κεφαλαίων, γραμμάτια, επιταγές, ώστε να έχει τη δυνατότητα να τις

ανακαλέσει ή / και να ενημερώσει το αρχείο του, δεν προσφέρεται. Εκεί είναι αναγκαία η πρόσβαση του χρήστη του καταστήματος στον κεντρικό υπολογιστή χωρίς την παρέμβαση του ειδικού προσωπικού του κέντρου.

Με την ανάπτυξη των τηλεπικοινωνιών δικτύων κατέστη δυνατή η απευθείας σύνδεση των καταστημάτων της τράπεζας με τον κεντρικό υπολογιστή. Έτσι, συνδέθηκε on-line ο υπάλληλος – χρήστης με το κέντρο που διέθετε τις πληροφορίες ώστε μόνος του να μπορεί να αντλήσει στοιχεία. Επίσης η τροφοδοσία του υπολογιστικού κέντρου γίνεται από το τερματικό του χρήστη, το οποίο χρησιμοποιεί και για άντληση πληροφοριών, ώστε να μπορεί να προσφέρει πλήρεις και σύγχρονες υπηρεσίες στους πελάτες του. Ταυτόχρονα, μειώθηκε ο χρόνος ενημέρωσης και ανάκλησης των πληροφοριών και έτσι η τράπεζα απέκτησε μια σημαντική βάση αναφοράς για τη λήψη αποφάσεων.

Κατά την δεκαετία του 1970 αναπτύχθηκαν στις τράπεζες προγράμματα που αφορούν επιμέρους τομείς δραστηριότητας, π.χ. διεκπεραίωση αποταμιευτικών λογαριασμών, δανείων, τίτλων, κτλ. Επρόκειτο για εφαρμογές οι οποίες ανήκουν στις διαδικασίες time sharing. Με τον τρόπο αυτό τα αρμόδια στελέχη των τραπεζών άρχισαν να χρησιμοποιούν για την εργασία τους προγράμματα που εφαρμόζονταν στους mainframes της τράπεζας.

Η επεξεργασία εντολών των πελατών άρχισε αργότερα να διευκολύνει την ικανοποίηση και διαχείριση τους με αντίστοιχα συστήματα. Για τις εσωτερικές διαδικασίες αναπτύχθηκαν γλώσσες προγραμματισμού της τέταρτης γενιάς. Με τη βοήθεια τους κατέστη δυνατό σε στελέχη επιμέρους τραπεζικών τμημάτων να χρησιμοποιήσουν τους κεντρικούς υπολογιστές και να αντλήσουν πληροφορίες. Επιπρόσθετα άρχισε η σταδιακή είσοδος των προσωπικών υπολογιστών (PCs) με αποτέλεσμα να μιλάει πλέον κανείς για τη δεκαετία της ατομικής επεξεργασίας πληροφοριών.

Η δεκαετία του ενενήντα βρίσκεται στον αστερισμό της δικτυακής επεξεργασίας των πληροφοριών. Οι τράπεζες εγκατέστησαν τα δικά τους εθνικά και υπερεθνικά δίκτυα, σχεδιάζουν νέα IT- Συστήματα και αναπτύσσουν την ηλεκτρονική ανταλλαγή πληροφοριών. Στην αρχή με τις εταιρείες- πελάτες στη συνέχεια όμως με την παρουσία των PCs στα νοικοκυριά όπως και τη ραγδαία ανάπτυξη του διαδικτύου, προσπαθούν σιγά- σιγά να συνδέσουν και τους ιδιώτες με τα συστήματά τους.

Η ενασχόληση των τραπεζών με το ευρύτερο κοινό ήταν αποτέλεσμα της βελτίωσης του βιοωτικού επιπέδου των πληθυσμών. Η προσπάθεια μαζικής προσέλκυσης καταθέσεων αλλά και προσφοράς προϊόντων, όπως τα καταναλωτικά και τα στεγαστικά δάνεια, τις οδήγησε στη δημιουργία του Retail Banking. Ο μεγάλος όγκος στοιχείων όμως, τα οποία παράγονται στο πλαίσιο αυτής της δραστηριότητας, έπρεπε να εξυπηρετηθεί από την πληροφορική, η οποία ανταποκρίθηκε πλήρως υπερακοντίζοντας με τις προσφερόμενες δυνατότητες συχνά και αυτές τις άμεσες ανάγκες των τραπεζών, δημιουργώντας προϊόντα και συσκευές που κάλυπταν και επερχόμενες ανάγκες. Οι περισσότερες βιομηχανικές χώρες της Δύσης στις δεκαετίες του εξήντα και κυρίως του εβδομήντα έζησαν μια πραγματική επανάσταση. Η κίνηση του οικογενειακού προϋπολογισμού μέσω των τραπεζών έγινε για τα περισσότερα νοικοκυριά μια διαδικασία ρουτίνας, η κατοχή τρεχούμενου λογαριασμού και η χρεοπιστώσεις καταναλωτικών δανείων καθημερινή υπόθεση.



## **ΕΙΔΗ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΩΜΩΝ**

Σύστημα πληρωμών είναι το σύνολο των διαδικασιών και των κανόνων για την μεταφορά κεφαλαίων μεταξύ μετεχόντων στο ίδιο σύστημα, δηλαδή είναι μια συμφωνία μεταξύ των συναλλασσομένων και ενός διαχειριστή του συστήματος ώστε να μπορούν οι πρώτοι να μεταφέρουν κεφάλαια με την χρήση μιας προσυμφωνημένης τεχνικής υποδομής και διαδικασίας, την οποία την επιβλέπει ο διαχειριστής.

Με βάση το κριτήριο του τρόπου διενέργειας του διακανονισμού, τα συστήματα πληρωμών διακρίνονται σε δύο κύριες κατηγορίες :

- Στα συστήματα συμψηφισμού ( Netting Systems) και
- Στα συστήματα διακανονισμού εντολών πληρωμής σε πραγματικό χρόνο (RTGS).

Τα συστήματα πληρωμών διακρίνονται επίσης σε συστήματα μεγάλων ή μικρών αξιών, εγχώρια ή διασυνοριακά, σε συστήματα διμερούς και πολυμερούς συμψηφισμού και σε συστήματα μονονομισματικά και πολυνομισματικά.

### **Συστήματα Συμψηφισμού (Netting Systems)**

Στα Συστήματα Συμψηφισμού οι διακανονισμοί μεταξύ των μελών συμψηφίζονται σε σταθερό χρονικό σημείο της ημέρας. Όταν το σύστημα λαμβάνει μια εντολή πληρωμής, άμεσα και αυτόματα ενημερώνει το λαμβάνον μέλος για το αν οι οδηγίες πληρωμής ικανοποιούν συγκεκριμένα κριτήρια. Το υπόλοιπο κάθε φορά διακανονίζεται με λογιστικές εγγραφές στους λογαριασμούς των τραπεζών στην Κεντρική Τράπεζα στο τέλος της ημέρας.

Τα ελάχιστα χαρακτηριστικά που πρέπει να έχουν τα netting systems ώστε να ελαχιστοποιείται ο κίνδυνος είναι:

- Τα μέλη θα πρέπει να γνωρίζουν τους κινδύνους που συνεπάγονται από την λειτουργία των συστημάτων αυτών
- Τα ίδια τα συστήματα να έχουν ισχυρή νομική βάση και να διαθέτουν διαδικασίες για την εξασφάλιση επιτυχούς ολοκλήρωσης των συναλλαγών ακόμα και ότα το μέλος με την μεγαλύτερη χρεωστική θέση παρουσιάζει αδυναμία να καλύψει την θέση του.
- Τα πολυμερή συστήματα πρέπει να έχουν καθορισμένες διαδικασίες διαχείρισης κινδύνων (RISK MANAGEMENT), ειδικά για την αντιμετώπιση του πιστωτικού κινδύνου και του κινδύνου ρευστότητας
- Θα πρέπει να υπάρχουν διαδικασίες καταμερισμού των ευθυνών μεταξύ των μελών του συστήματος

Τα παραπάνω κριτήρια ορίζουν τα ελάχιστα χαρακτηριστικά για την ομαλή λειτουργία ενός πολυμερούς συμψηφιστικού συστήματος και αποκαλούνται Lamfalussy Standards.

### **Συστήματα Διακανονισμού Εντολών πληρωμής σε Πραγματικό χρόνο. (RTGS)**

Με τα RTGS για την μεταφορά κεφαλαίων, επιτυγχάνεται υψηλός βαθμός αποτελεσματικότητας και ασφάλειας στον διακανονισμό των πληρωμών. Στα συστήματα αυτά κάθε εντολή επεξεργάζεται μεμονωμένα και διακανονίζεται άμεσα, οριστικά και αμετάκλητα, εφόσον υπάρχουν επαρκή κεφάλαια στον λογαριασμό του μέλους. Επειδή ο φορέας διακανονισμού είναι η Κεντρική Τράπεζα, αυτό έχει ως συνέπεια ο διακανονισμός των εντολών να γίνεται μέσω

των λογαριασμών που διατηρούν τα μέλη του συστήματος σε αυτήν, και η οποία φέρει και την ευθύνη να διαχειρίζεται και τους όποιους κινδύνους προκύψουν από την λειτουργία του συστήματος.

Ο ρόλος των εθνικών κεντρικών τραπεζών στην λειτουργία των συστημάτων πληρωμών είναι ιδιαίτερα αυξημένος παγκοσμίως, ιδιαίτερα στα κράτη μέλη της ΕΕ. Η ΕΕ προβλέπει ότι το Ενιαίο Σύστημα Κεντρικών Τραπεζών έχει σημαντικό ρόλο σε όλα τα συστήματα πληρωμών που λειτουργούν εντός της ΕΕ, καθώς στα βασικά του καθήκοντα περιλαμβάνεται μεταξύ άλλων και η προώθηση της ομαλής λειτουργίας των διασυνοριακών συστημάτων πληρωμών.

Τις τελευταίες δεκαετίες η διεθνής εξέλιξη των χρηματοοικονομικών αγορών και των εμπορικών δραστηριοτήτων έγιναν με θεαματικό τρόπο. Αναγκαίο επακόλουθο ήταν η ανάπτυξη των συστημάτων μεγάλων πληρωμών σε όλο τον κόσμο. Τα συστήματα μεγάλων πληρωμών εξυπηρετούν τη μεταφορά μεγάλου όγκου πληρωμών μεταξύ των τραπεζών μέσω των χρησιμοποιούμενων από αυτές ειδικών ηλεκτρονικών συστημάτων.

Στην Ελλάδα η δομή και η λειτουργία των συστημάτων και των μέσων πληρωμών εκσυγχρονίστηκε σε μεγάλο βαθμό τα τελευταία χρόνια, ως επακόλουθο των προσαρμογών που χρειάστηκε να γίνει στην εγχώρια αγορά του τραπεζικού συστήματος και στις νέες προκλήσεις και απαιτήσεις που αντιμετώπισε όπως:

- Παγκοσμιοποίηση των χρηματαγορών και των αγορών κεφαλαίου
- Ραγδαία τεχνολογική ανάπτυξη
- Ιδιωτικοποιήσεις, συγχωνεύσεις και εξαγορές
- Επικράτηση του λογιστικού χρήματος και απούλοποιημένων χρηματοοικονομικών προϊόντων, το οποίο είχε και καταλυτικό ρόλο στην ανάπτυξη αυτών των συστημάτων.

Το Ελληνικό τραπεζικό σύστημα δημιούργησε νέα προϊόντα αλλά και την απαραίτητη οργάνωση για την συμμετοχή του στην νέα πραγματικότητα των ηλεκτρονικών διατραπεζικών συναλλαγών.

Παρακάτω μπορούμε να δούμε ένα συνοπτικό πίνακα με Τραπεζικά προϊόντα τόσο για Ιδιώτες όσο και για Επιχειρήσεις

#### Τραπεζικά Προϊόντα για Ιδιώτες (BtC προϊόντα)

- Λογαριασμοί Ταμειευτηρίου
- Τρεχούμενοι Λογαριασμοί
- Λογαριασμοί Μισθοδοσίας
- Λογαριασμοί Συναλλάγματος
- Προθεσμιακές Καταθέσεις
- Επενδυτικά Προϊόντα
- Αμοιβαία Κεφάλαια
- Κάρτες
- Καταναλωτικά Δάνεια
- Δάνεια Κατοικίας

- Χρηματοιστηριακές Υπηρεσίες
- Τραπεζικές Υπηρεσίες

Τραπεζικά Προϊόντα για Επιχειρήσεις (BtB προϊόντα)

- Leasing
- Αναπτυξιακά Προγράμματα
- Λειτουργικές Μισθώσεις
- Ναυτιλιακές Εργασίες
- Χρηματοιστηριακές Υπηρεσίες
- Ηλεκτρονικές Υπηρεσίες

## ΕΛΛΗΝΙΚΑ ΗΛΕΚΤΡΟΝΙΚΑ ΣΥΣΤΗΜΑΤΑ ΠΛΗΡΩΜΩΝ

Σύμφωνα με το άρθρο 2, εδάφ. ε', του Καταστατικού της Τράπεζας της Ελλάδος, μια από τις κύριες αρμοδιότητες της είναι να προωθεί και να επιβλέπει την ομαλή λειτουργία και την αποτελεσματικότητα των συστημάτων πληρωμών και των μέσων πληρωμής.

Στο πλαίσιο αυτό, η Επίβλεψη που ασκεί η Τράπεζα της Ελλάδος αφορά στην πρόληψη και την έγκαιρη αντιμετώπιση των κινδύνων στα οποία είναι εκτεθειμένα τα συστήματα πληρωμών, όπως είναι ο νομικός, ο πιστωτικός, ο λειτουργικός και ο κίνδυνος ρευστότητας, με στόχο τη διατήρηση της αξιοπιστίας και της αποτελεσματικότητας τους και, κατ' επέκταση, τη διασφάλιση της χρηματοπιστωτικής σταθερότητας.

Αντιστοίχως, η Επίβλεψη στα μέσα πληρωμής αποσκοπεί στην ασφάλεια και την αποδοτικότητά τους και προς τούτο επικεντρώνεται στον περιορισμό των κινδύνων που ενδέχεται να διαταράξουν την εμπιστοσύνη του κοινού σε αυτά και γενικότερα στο νόμισμα.

Ο σκοπός και το πεδίο εφαρμογής της Επίβλεψης καθορίζονται με την Πράξη Συμβουλίου Νομισματικής Πολιτικής 50/31.7.2002, στην οποία εξειδικεύονται το πλαίσιο αρχών και προτύπων που πρέπει να διέπουν τη λειτουργία των συστημάτων πληρωμών και των μέσων πληρωμής, ο τρόπος και τα εργαλεία για την άσκηση της Επίβλεψης, καθώς και τα στοιχεία και οι πληροφορίες που οι εμπλεκόμενοι φορείς στη διαχείριση συστημάτων πληρωμών ή/και την παροχή υπηρεσιών πληρωμών οφείλουν να υποβάλλουν στην Τράπεζα της Ελλάδος.

Η Επίβλεψη ασκείται από την Τράπεζα της Ελλάδος στο πλαίσιο της πολιτικής του Ευρωσυστήματος, σύμφωνα με την οποία τα συστήματα πληρωμών κατηγοριοποιούνται ως προς τη σημαντικότητά τους και αξιολογούνται έναντι των Θεμελιωδών Αρχών για τα Συστημικά Σημαντικά Συστήματα Πληρωμών. Όσον αφορά στα μέσα πληρωμής, η Επίβλεψη ασκείται με βάση τα ενιαία πρότυπα επίβλεψης για τις κάρτες πληρωμών, τις εντολές μεταφοράς πίστωσης SEPA και τις άμεσες χρεώσεις SEPA, τα οποία δύνανται να εφαρμοστούν και στα εθνικά μέσα πληρωμής. Επίσης, το Ευρωσύστημα έχει ορίσει πλαίσιο ασφαλείας για τα σχήματα ηλεκτρονικού χρήματος.

Στην Ελλάδα υπάρχουν τέσσερα Ηλεκτρονικά Συστήματα Πληρωμών

1. Το διατραπεζικό σύστημα **ΔΙΑΣ**
2. Το **Γραφείο Συμψηφισμού Αθηνών (Γ.Σ.Α)**  
Διακανονισμός Επιπαγών με φυσική μορφή ανεξαρτήτως ποσού και νομίσματος. Ο διακανονισμός γίνεται μέσω του ΕΡΜΗΣ
3. Το σύστημα πληρωμών **ΕΡΜΗΣ**
4. Το **Σύστημα Άυλων τίτλων (Σ.Α.Τ)**  
Καλύπτει συναλλαγές:
  - Έντοκα γραμμάτια του Ελληνικού Δημοσίου
  - Ομόλογα του Ελληνικού Δημοσίου
  - Άλλους τίτλους του Ελληνικού Δημοσίου
  - Τίτλους άλλων φορέων
  - Προϊόντα προθεσμιακών καταθέσεων

## Διαραπεζικό Σύστημα ΔΙΑΣ

Το σύστημα πληρωμών ΔΙΑΣ ταξινομείται στα συστήματα πληρωμών μικρής αξίας με εξέχουσα σημασία (Prominently Important Retail Payment Systems - PIRPS) σύμφωνα με τα πρότυπα επίβλεψης της Ευρωπαϊκής Κεντρικής Τράπεζας και βρίσκεται υπό την επίβλεψη της Τράπεζας της Ελλάδος.

Αποτελείται από ένα σύνολο εργαλείων πληρωμών ως ακολούθως:

- μεταφορές πίστωσης,
- άμεσες χρεώσεις,
- επιταγές,
- συναλλαγές σε ATM,
- πληρωμές με κάρτες.

Στο σύστημα πληρωμών ΔΙΑΣ συμμετέχουν εμπορικές τράπεζες και η Τράπεζα της Ελλάδος όπως προβλέπεται στον κανονισμό λειτουργίας του συστήματος.

Το σύστημα ΔΙΑΣ το διαχειρίζεται η ΔΙΑΣ ΑΕ η οποία στα πλαίσια λειτουργίας και των δραστηριοτήτων της Ένωσης Ελληνικών Τραπεζών διαχειρίζεται τα πέντε υποσυστήματα που απαρτίζουν το ΔΙΑΣ και τα οποία είναι :

1. Σύστημα **DIASATM**  
Διαραπεζικό Ηλεκτρονικό Σύστημα ATM Switching για την παροχή δυνατότητας διασύνδεσης των δικτύων των ATM των τραπεζών.
2. Σύστημα **DIASCHEQUE**  
Διαραπεζικό Ηλεκτρονικό Σύστημα Συμψηφισμού Επιταγών. Το σύστημα λειτουργεί σύμφωνα με την μέθοδο “cheque transaction” βάση της οποίας αποστέλλονται ηλεκτρονικά τα στοιχεία της επιταγής στις εκδότριες τράπεζες και το σώμα αυτής παραμένει στο κατάστημα που αγόρασε την επιταγή.
3. Σύστημα **DIATRANSFER**  
Διαραπεζικό Ηλεκτρονικό Σύστημα Κίνησης Κεφαλαίων που δίνει τη δυνατότητα της απλούστευσης, τυποποίησης και αυτοματοποίησης των υφιστάμενων διαδικασιών διακίνησης και εκκαθάρισης των διενεργούμενων μεταξύ των τραπεζών, για λογαριασμό των πελατών τους, εντολών μεταφοράς κεφαλαίων. Το σύστημα λειτουργεί βάση της αρχής του συγκεντρωτικού διακανονισμού (net settlement) για όλες τις διακινούμενες μέσω αυτού συναλλαγές.

*Τα αποτελέσματα των DIASATM, DIASCHEQUE και DIASTRANSFER ενοποιημένα διακανονίζονται στο τέλος της ημέρας από το ΕΡΜΗΣ.*

#### 4. Σύστημα DIASRAY

Διατραπεζικό Ηλεκτρονικό Σύστημα Πληρωμής Αποδοχών το οποίο διαχειρίζεται με αυτοματοποιημένο τρόπο μέσω των τραπεζικών λογαριασμών των δικαιούχων πληρωμές αποδοχών κάθε μορφής, κυρίως πληρωμές μισθών και συντάξεων.

#### 5. Σύστημα DIASPOS

Διατραπεζικό Ηλεκτρονικό Σύστημα Πληρωμής Υποχρεώσεων με πιστωτικές κάρτες, προκειμένου να πληρωθούν μέσω αυτών οικονομικές υποχρεώσεις των φορολογουμένων προς το Ελληνικό Δημόσιο.

Τα υπόλοιπα τρία τα διαχειρίζεται η Τράπεζα της Ελλάδος η οποία είναι και η εποπτική αρχή του Ελληνικού Τραπεζικού συστήματος και η οποία θέτει τους όρους, τους κανόνες και είναι επιφορτισμένη με τον ρόλο του ελεγκτή και η οποία είναι επιφορτισμένη με την υποχρέωση να διασφαλίζει την ομαλή και σύννομη λειτουργία του τόσο του ίδιου του Τραπεζικού Συστήματος της χώρας μας, αλλά και των συστημάτων που αυτό χρησιμοποιεί.

### **Γραφείο Συμφηφισμού Αθηνών**

Το Γραφείο Συμφηφισμού Αθηνών (ΓΣΑ) ιδρύθηκε το 1928, ευθύς μετά την ίδρυση της Τράπεζας της Ελλάδος τον ίδιο χρόνο, και εδρεύει στο κεντρικό κατάστημα της Τράπεζας της Ελλάδος. Σκοπός του είναι ο διακανονισμός επιταγών με φυσική μορφή ανεξαρτήτως ποσού σε Ευρώ και συνάλλαγμα. Στο Γραφείο Συμφηφισμού Αθηνών έχουν δικαίωμα συμμετοχής ως μέλη όλα τα νομίμως λειτουργούντα στην Ελλάδα χρηματοπιστωτικά ιδρύματα.

Σε αντίθεση με το σύστημα διακανονισμού ΔΙΑΣ, στο Γραφείο Συμφηφισμού Αθηνών τα σώματα των επιταγών παραδίδονται από τις κομίστριες στις πληρώτριες τράπεζες. Τα αποτελέσματα εκκαθάρισης των συναλλαγών του ΓΣΑ, καθώς και αυτά των υποκαταστημάτων της Τράπεζας της Ελλάδος, διακανονίζονται μέσω του συστήματος TARGET2-GR.

### **Σύστημα Πληρωμών ΕΡΜΗΣ (HERMES)**

Η Τράπεζα της Ελλάδος είχε ιδρύσει και καθιέρωσε το ηλεκτρονικό σύστημα πληρωμών ΕΡΜΗΣ, με στόχο να διασφαλίσει την ομαλή ροή των ηλεκτρονικών μεταφορών των εγχώριων και διασυνοριακών κεφαλαίων.

Το σύστημα ΕΡΜΗΣ πραγματοποίησε τη διεκπεραίωση εντολών πληρωμής σε πραγματικό χρόνο. Από τον Ιανουάριο του 1999 καθιερώθηκε στη χώρα μας το σύστημα πληρωμών σε ΕΥΡΩ με την ονομασία ΕΥΡΩΕΡΜΗΣ, το οποίο όντας συνδεδεμένο με το ευρωπαϊκό δίκτυο πληρωμών TARGET πραγματοποιούσε εγχώριες και διασυνοριακές συναλλαγές σε ΕΥΡΩ.

Από το Μάρτιο του 2000 όπου το σύστημα ΕΡΜΗΣ διακανόνιζε της εγχώριες πληρωμές σε δρχ και μέχρι την 2<sup>α</sup> Ιανουαρίου 2001 όπου η χώρα μας εντάθηκε στην ΟΝΕ και αντικαταστάθηκε η δρχ με το €, το ΕΡΜΗΣ είχε εναρμονιστεί πλήρως με το TARGET και το νέο πλέον ΕΡΜΗΣ που

τέθηκε σε λειτουργία από τότε, διακανόνιζε τόσο της εγχώριες τόσο και τις διασυνοριακές πληρωμές σε ΕΥΡΩ.

Πλέον το σύστημα ΕΡΜΗΣ ή HERMES (Hellenic Real-time Money-transfer Express) έχει αντικατασταθεί από το TARGET 2.

## ΕΥΡΩΠΑΪΚΑ ΗΛΕΚΤΡΟΝΙΚΑ ΣΥΣΤΗΜΑΤΑ ΠΛΗΡΩΜΩΝ

### ΠΑΝΕΥΡΩΠΑΪΚΟ ΣΥΣΤΗΜΑ ΠΛΗΡΩΜΩΝ σε € TARGET (Trans – European Automated Real – Time Gross Settlement Express Transfers)

Το TARGET είναι το διευρωπαϊκό σύστημα διακανονισμού σε πραγματικό χρόνο εντολών σε ευρώ. Αποτελεί ένα μοναδικό RTGS σύστημα πληρωμών για διασυνοριακές πληρωμές μεγάλων ποσών στον κόσμο, καλύπτοντας ολόκληρη την Ευρωπαϊκή Ένωση.

Αναπτύχθηκε από τις Εθνικές Κεντρικές Τράπεζες της ΕΕ και το διαχειρίζεται η Ευρωπαϊκή Κεντρική Τράπεζα με στόχο την ύπαρξη ενός ασφαλούς και αξιόπιστου μηχανισμού για τον διακανονισμό διασυνοριακών εντολών μεγάλων ποσών σε €.

Το TARGET είναι ένα αποκεντρωμένο σύστημα πληρωμών αποτελούμενο από :

- Τα RTGS συστήματα των κρατών μελών της Ευρωζώνης
- Το σύστημα μηχανισμού πληρωμών της ΕΚΤ
- Τον μηχανισμό διασύνδεσης (interlinking)

Το δίκτυο επικοινωνίας όλων των εθνικών συστημάτων μεταξύ τους γίνεται με την αποστολή μηνυμάτων SWIFT.

### Διατραπεζικό Σύστημα Πληρωμών EBA

Είναι το σύστημα που ανέπτυξε η Ευρωπαϊκή Τράπεζα Επενδύσεων σε συνεργασία με 18 εμπορικές τράπεζες με την στήριξη της Ευρωπαϊκής Επιτροπής και της Bank for International Settlements (BIS) το 1985 με στόχο την προώθηση της χρήσης του τότε ECU στις χρηματοοικονομικές και εμπορικές συναλλαγές.

Κατέχει το 85% περίπου των μηνυμάτων SWIFT στην Ευρώπη και έχει σκοπούς:

- Την ανάπτυξη και λειτουργία συστημάτων διακανονισμού σε ΕΥΡΩ
- Την συνεργασία με τα άλλα ευρωπαϊκά συστήματα πληρωμών
- Την προώθηση προτάσεων σε θέματα Ευρωπαϊκής Νομοθεσίας, προτύπων και επιχειρηματικών πρακτικών συμψηφισμού και διακανονισμού.

Η EBA κατά την διάρκεια της λειτουργίας της ανέπτυξε δύο υποσυστήματα κίνησης κεφαλαίων για διασυνοριακές συναλλαγές σε € βασισμένα στην πλατφόρμα διακανονισμού των συναλλαγών με ECU.

- Το **EURO 1**.  
Σύστημα διασυνοριακών πληρωμών μεγάλης αξίας σε €, το οποίο διευθετεί και ρυθμίζει τις απαιτήσεις και υποχρεώσεις των μερών στο τέλος της ημέρας. Για να πραγματοποιηθεί μια πληρωμή μέσω του συστήματος αυτού θα πρέπει οι τράπεζες των συναλλασσομένων να ανήκουν στο σύστημα. Στο σύστημα συμμετέχουν και τράπεζες εκτός Ευρωπαϊκής Ένωσης.
- Το **STEP 1**.  
Σύστημα διασυνοριακών πληρωμών μικρής αξίας σε €. Για να πραγματοποιηθεί μια πληρωμή μέσω του συστήματος αυτού θα πρέπει οι τράπεζες των συναλλασσομένων



να ανήκουν στο σύστημα EURO 1 ή με διμερή συμφωνία να συνεργάζονται με μία από αυτές. Στο σύστημα συμμετέχουν και τράπεζες πάνω από 30 χωρών.

### **Σύστημα Continuous Linked Settlement (CLS)**

Το CLS είναι ένα σύστημα διεκπεραίωσης και επεξεργασίας πληρωμών προερχομένων από διατραπεζικές συναλλαγές σε συνάλλαγμα, με την συμμετοχή διεθνών χρηματοπιστωτικών ιδρυμάτων. Υπάγεται στα συστήματα συμψηφισμού σταθερού χρόνου και είναι μια προσπάθεια της παγκόσμιας τραπεζικής κοινότητας για την μείωση και εξάλειψη των κινδύνων από ανεκτέλεστες συναλλαγές σε συνάλλαγμα.

Το σύστημα το διαχειρίζεται η CLS Bank και οι κίνδυνοι που έχει να αντιμετωπίσει επιγραμματικά είναι οι ακόλουθοι :

- i. Κίνδυνος Αγοράς ( Market Risk)  
Ο κίνδυνος από μια δυσμενή εξέλιξη της τιμής στην αγορά συναλλάγματος σε νόμισμα που δεν έχει διακανονισθεί.
- ii. Λειτουργικός Κίνδυνος ( Operational Risk)
  - a. Από λανθασμένες οδηγίες
  - b. Από ανεπιτυχείς τεχνικούς χειρισμούς στην εκτέλεση των μηνυμάτων SWIFT των συναλλαγών
  - c. Στην προβληματική λειτουργία των συστημάτων διεκπεραίωσης των συναλλαγών
- iii. Κίνδυνος Ρευστότητας ( Liquidity Risk)  
Όταν σε μια αγοραπωλησία συναλλάγματος δεν ταυτοποιούνται χρονικά οι εισροές και εκροές στα δύο νομίσματα.
- iv. Κίνδυνος Αντικατάστασης ( Replacement Risk)

### **Το Πανευρωπαϊκό Σύστημα Πληρωμών σε ευρώ TARGET2 (Trans- European Automated Real-time Gross settlement Express Transfers 2)**

Δυνάμει της Κατευθυντήριας Γραμμής Ε.Κ.Τ/2007/2 σχετικά με το Διευρωπαϊκό Σύστημα Ταχείας Μεταφοράς Κεφαλαίων και Διακανονισμού σε Συνεχή Χρόνο (TARGET2), από τις 19 Νοεμβρίου 2007 το Σύστημα TARGET αντικαταστάθηκε από το σύστημα TARGET2. Το Σύστημα TARGET2 διακανονίζει πληρωμές σε ευρώ σε συνεχή χρόνο σε χρήμα κεντρικής τράπεζας, όπως και το TARGET.

Το TARGET2 έχει δημιουργηθεί και λειτουργεί με βάση την ενιαία κοινή πλατφόρμα (Ε.Κ.Π.). Το Ευρωσύστημα καθορίζει την τεχνική διαμόρφωση και τα τεχνικά χαρακτηριστικά της Ε.Κ.Π. Οι υπηρεσίες της Ε.Κ.Π. παρέχονται προς όφελος των Κεντρικών Τραπεζών του Ευρωσυστήματος από τις Κεντρικές Τράπεζες που παρέχουν την Ε.Κ.Π. επί τη βάση ξεχωριστών συμβάσεων.

Το TARGET2 είναι νομικά οργανωμένο ως ένα σύνολο πολλαπλών συστημάτων πληρωμών, αποτελούμενο από όλες τις συνιστώσες του TARGET2, οι οποίες έχουν οριστεί ως «συστήματα», σύμφωνα με τις εθνικές διατάξεις για την εφαρμογή της οδηγίας 98/26/ΕΚ του

Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 19ης Μαΐου 1998, σχετικά με το αμετάκλητο του διακανονισμού στα συστήματα πληρωμών και στα συστήματα διακανονισμού αξιόγραφων. Κάθε Κεντρική Τράπεζα του Ευρωσυστήματος διαχειρίζεται τη δική της συνιστώσα του TARGET2. Το TARGET2- GR αποτελεί συνιστώσα του TARGET2 την οποία διαχειρίζεται η Τράπεζα της Ελλάδος.

### **Συμμετοχή στο TARGET2- GR**

Η συμμετοχή στο TARGET2 πραγματοποιείται μέσω της συμμετοχής στο TARGET2- GR το οποίο επεξεργάζεται τις ακόλουθες εντολές πληρωμής:

A) εντολές πληρωμής που απορρέουν απευθείας από- ή σχετίζονται με- πράξεις νομισματικής πολιτικής του Ευρωσυστήματος.

B) το διακανονισμό του σκέλους σε ευρώ των πράξεων συναλλάγματος του Ευρωσυστήματος

Γ) το διακανονισμό μεταφορών κεφαλαίων σε ευρώ που απορρέουν από συναλλαγές σε διασυνοριακά συστήματα συμψηφισμού μεγάλης αξίας

Δ) το διακανονισμό μεταφορών κεφαλαίων σε ευρώ που απορρέουν από συναλλαγές σε συστήματα πληρωμών μικρής αξίας σε ευρώ με συστημική σημασία και

Ε) κάθε άλλη εντολή πληρωμής σε ευρώ που απευθύνεται σε συμμετέχοντες στο TARGET2.

Υπάρχουν πολλοί τρόποι συμμετοχής στο TARGET2:

#### **Άμεση συμμετοχή έχουν:**

A) πιστωτικά ιδρύματα που είναι εγκατεστημένα στον Ε.Ο.Χ., περιλαμβανομένης της περίπτωσης κατά την οποία ενεργούν μέσω υποκαταστήματος εγκατεστημένου στον Ε.Ο.Χ.

B) πιστωτικά ιδρύματα που είναι εγκατεστημένα εκτός του Ε.Ο.Χ., υπό την προϋπόθεση ότι ενεργούν μέσω υποκαταστήματος εγκατεστημένου στον Ε.Ο.Χ και

Γ) ΕθνΚΤ των κρατών μελών της Ε.Ε. και η Ε.Κ.Τ.

Οι άμεσοι συμμετέχοντες στο TARGET2- GR τηρούν έναν τουλάχιστον λογαριασμό ΜΠ στην Τράπεζα της Ελλάδος.

#### **Έμμεση συμμετοχή**

Κάθε πιστωτικό ίδρυμα εγκατεστημένο στον ΕΟΧ μπορεί να συνάπτει σύμβαση με έναν άμεσο συμμετέχοντα, εφόσον ο τελευταίος είναι πιστωτικό ίδρυμα ή ΚΤ, προκειμένου να υποβάλει εντολές πληρωμής ή/και να λαμβάνει πληρωμές, καθώς και να προβαίνει στο διακανονισμό τους μέσω του λογαριασμού ΜΠ του εν λόγω άμεσου συμμετέχοντα.

### **Σύστημα Euroclear – Euroclear Bank**

Είναι ένα διεθνές ηλεκτρονικό σύστημα διακανονισμού και συμψηφισμού διασυνοριακών συναλλαγών σε εμπορεύματα, ομολογίες και μετοχές. Ειδικεύεται στον διακανονισμό και τη φύλαξη ευρωομολόγων.

### **Σύστημα Clearstream Banking (πρώην CEDEL)**

Πρόκειται για εταιρία διεθνών συμψηφισμών και διακανονισμών σε χρεόγραφα και κυρίως σε ευρωομόλογα.

## **Σύστημα SEPA «Single Euro Payments Area» (Ενιαίος χώρος Πληρωμών με Ευρώ)**

Μετά την ίδρυση της Ευρωπαϊκής Οικονομικής Κοινότητας το 1958, διάφορα γεγονότα έχουν σφραγίσει την πορεία προς την ολοκλήρωση της ευρωπαϊκής χρηματοπιστωτικής αγοράς. Τα πιο εμφανή είναι αναμφισβήτητα η υιοθέτηση του ευρώ το 1999 και, ιδίως, η μετάβαση στο ευρώ σε φυσική μορφή στις χώρες της ζώνης του ευρώ το 2002. Λιγότερο εμφανής, αλλά επίσης πολύ σημαντική, ήταν η δημιουργία του TARGET, του συστήματος των κεντρικών τραπεζών για τις πληρωμές μεγάλης αξίας, την 1η Ιανουαρίου 1999. Το TARGET αποτελεί τον κεντρικό άξονα του χρηματοπιστωτικού συστήματος όσον αφορά το ευρώ και το μέσο εφαρμογής της ενιαίας νομισματικής πολιτικής του Ευρωσυστήματος.

Ο SEPA αποτελεί το επόμενο μεγάλο βήμα προς την ευρωπαϊκή ολοκλήρωση. Ο SEPA επιτρέπει στους πελάτες να διενεργούν πληρωμές σε ευρώ χωρίς μετρητά προς κάθε δικαιούχο εντός της ζώνης του ευρώ, χρησιμοποιώντας ένα μόνο τραπεζικό λογαριασμό και μια ενιαία δέσμη μέσων πληρωμών. Αυτό σημαίνει ότι όλες οι πληρωμές μικρής αξίας σε ευρώ γίνονται «εγχώριες», δηλαδή παύει να υφίσταται διάκριση μεταξύ εγχώριων και διασυνοριακών πληρωμών εντός της ζώνης του ευρώ.

Στο πλαίσιο αυτής της πρόκλησης, το 2002 ο τραπεζικός κλάδος δημιούργησε το Ευρωπαϊκό Συμβούλιο Πληρωμών (European Payments Council – EPC). Το EPC καθορίζει τους νέους κανόνες και διαδικασίες για τις πληρωμές σε ευρώ.

Σε αυτή τη διαδικασία έχει συμπεριλάβει τα ενδιαφερόμενα μέρη όχι μόνο από τη ζώνη του ευρώ, αλλά και από άλλες χώρες της Ευρωπαϊκής Ένωσης (ΕΕ), την Ισλανδία, το Λιχτενστάιν, τη Νορβηγία και την Ελβετία. Έτσι, κοινότητες εκτός της ζώνης του ευρώ έχουν τη δυνατότητα να συμμετάσχουν στα συστήματα πληρωμών σε ευρώ και να υιοθετήσουν τα πρότυπα και τις πρακτικές του SEPA, συμβάλλοντας με αυτό τον τρόπο στη δημιουργία μιας ενιαίας αγοράς για τις υπηρεσίες πληρωμών.

### **Ο SEPA είναι :**

Ένας χώρος στον οποίο οι καταναλωτές, οι εταιρίες και οι λοιποί οικονομικοί παράγοντες είναι σε θέση να διενεργούν και να δέχονται

εγχώριες και διασυνοριακές πληρωμές σε ευρώ με τους ίδιους βασικούς όρους και τα ίδια δικαιώματα και υποχρεώσεις, ανεξαρτήτως της γεωγραφικής τους θέσης.

### **Ο σκοπός του SEPA είναι :**

Η προώθηση της ευρωπαϊκής ολοκλήρωσης μέσω μιας ανταγωνιστικής και καινοτόμου αγοράς πληρωμών μικρής αξίας στη ζώνη του ευρώ που παρέχει υψηλότερο επίπεδο υπηρεσιών, πιο αποτελεσματικά προϊόντα και φθηνότερες εναλλακτικές λύσεις για τη διενέργεια πληρωμών.

### **Ο SEPA αποτελείται από :**

1. το ενιαίο νόμισμα,
2. μια ενιαία δέσμη μέσων πληρωμών σε ευρώ – μεταφορές πιστώσεων,
3. άμεσες χρεώσεις και πληρωμές με κάρτα,
4. αποτελεσματικές υποδομές για την επεξεργασία πληρωμών σε ευρώ,
5. κοινά τεχνικά πρότυπα,
6. κοινές επιχειρηματικές πρακτικές,
7. μια εναρμονισμένη νομική βάση, και
8. ολοένα εξελισσόμενες υπηρεσίες με προσανατολισμό προς τον πελάτη.

### **Στο SEPA συμμετέχουν οι ακόλουθες δημόσιες αρχές:**

- Το Ευρωσύστημα (η ΕΚΤ και οι Εθν.Κ.Τ. της ζώνης του ευρώ) έχει τονίσει τις προσδοκίες του σχετικά με τον SEPA μέσα από διάφορες δημοσιεύσεις και παρακολουθεί στενά την πρόοδο του εγχειρήματος και τις σχετικές εξελίξεις.

- Η Ευρωπαϊκή Επιτροπή έχει αναπτύξει στρατηγική για την εξάλειψη των φραγμών στην εσωτερική αγορά και την απλούστευση των κανονιστικών ρυθμίσεων που τη διέπουν, π.χ. μέσω της πρότασης οδηγίας για τις υπηρεσίες πληρωμών (Payment Services Directive – PSD).

## Κεφάλαιο 3ο E- BANKING

### ΕΙΣΑΓΩΓΗ ΣΤΟ E- BANKING

Η αλματώδης εξέλιξη της τεχνολογίας και του Διαδικτύου, ως επακόλουθο της ραγδαίας ανάπτυξης της πληροφορικής και των πληροφοριακών συστημάτων, με την ταυτόχρονη εξάπλωση σε παγκόσμιο πλέον επίπεδο του ηλεκτρονικού εμπορίου και σε συνδυασμό με την τεχνολογική πρόοδο και βελτίωση του τομέα των τηλεπικοινωνιών, καθιστούν επιτακτική τη δημιουργία κατάλληλου νομικού πλαισίου για την προστασία των προσωπικών δεδομένων, αλλά και της εν γένει οικογενειακής ζωής του ατόμου- χρήστη των σύγχρονων πολυμέσων (Internet, ISDN, email κλπ)

Είναι κοινά αποδεκτό ότι το Διαδίκτυο αποτελεί σήμερα τον εύκολο, μαζικό και οικονομικό τρόπο πρόσβασης σε κάθε είδους πληροφορία, εκμηδενίζοντας τις όποιες γεωγραφικές αποστάσεις και παραμερίζοντας πολιτιστικές, πολιτικές και κοινωνικές διαφορές μεταξύ των κρατών. Όμως, η συνύπαρξη κινδύνων αλλά και ωφελειών από την επεξεργασία προσωπικών δεδομένων αντιστοιχεί σε μια σύγκρουση αγαθών: στη σύγκρουση μεταξύ αφενός της προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, ιδίως της προστασίας της ιδιωτικής ζωής, και αφετέρου της ελεύθερης κυκλοφορίας των πληροφοριών. Η άρση, επομένως, της συγκρούσεως και ο συγκερασμός αντιτιθέμενων αγαθών και συμφερόντων, καθίσταται ανάγκη επιτακτική.

Το ζήτημα της προστασίας προσωπικών δεδομένων, ευρισκόμενο σε άμεση συσχέτιση με τη χρήση του Διαδικτύου, προβληματίζει και απασχολεί τα εκατομμύρια των χρηστών του. Η ελλιπής προστασία των προσωπικών δεδομένων αλλά και η ανασφάλεια η συνυφασμένη με ένα ανοικτό δίκτυο, όπως είναι το internet, αποτελούν τροχοπέδη στην ανάπτυξη του ηλεκτρονικού εμπορίου και γενικότερα των πραγματοποιούμενων μέσω αυτού συναλλαγών. Συνεπώς, τα νέα προβλήματα απαιτούν αποφασιστική επίλυση, νέους ρυθμιστικούς κανόνες και νέα εργαλεία.

Η λήψη μέτρων για την προστασία της ιδιωτικότητας δεν αποτελεί αρνητικό παράγοντα στην ανάπτυξη των τηλεπικοινωνιών. Απεναντίας, αυξάνει την εμπιστοσύνη χρηστών- καταναλωτών, εφόσον υπάρχει αποτελεσματική προστασία των προσωπικών δεδομένων.

Στον τομέα των τηλεπικοινωνιών εντάσσεται και η ανάπτυξη των ψηφιακών κινητών δικτύων και των δικτύων ενοποιημένων υπηρεσιών (Intergrated Services Digital Network, ISDN) (αρ.3 παρ.1 Οδ. 97/66/EK). Πρόκειται για δίκτυα που δίνουν στο συνδρομητή τη δυνατότητα μέσω μιας μόνο σύνδεσης, της διασύρματης τηλεφωνικής γραμμής, να πραγματοποιεί ψηφιακές κλήσεις και να χρησιμοποιεί ταυτόχρονα υπηρεσίες φωνής, εικόνας, κειμένου και δεδομένων. Τέτοια περίπτωση αποτελεί η μεταφορά αρχείων, η πρόσβαση σε βάσεις δεδομένων και η τηλεδιάσκεψη.

Η διάσταση και η ποιότητα της πληροφορίας έχει αλλάξει σημαντικά αφότου ο ηλεκτρονικός υπολογιστής κατέστη πλέον οικουμενικό μέσο επικοινωνίας και προσδιορισμού της διαδικασίας επεξεργασίας δεδομένων. Και επειδή στη λεωφόρο των επικοινωνιών υπάρχουν μόνο γυάλινοι οδηγοί, η ανάπτυξη των τηλεπικοινωνιακών δικτύων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα αποτελεί πηγή ιδιαίτερης διακινδύνευσης του δικαιώματος πληροφοριακής αυτοδιάθεσης του ατόμου.

Το Internet και οι λοιπές εφαρμογές που συνδέονται μαζί του, όπως το E- Commerce, το E- Business και το E-Service, βρίσκονται ήδη σε μια αναπτυξιακή τροχιά. Δεν υπάρχει σοβαρή επιχείρηση που να μην έχει στους στόχους της την αξιοποίηση της τεχνολογίας για τις υποθέσεις της. Ο χρηματοπιστωτικός τομέας επιφυλάσσει για τον εαυτό του σε αυτή τη διαδικασία ένα σημαντικό ρόλο μέσω του E- Banking. Για το κάθε τραπεζικό ίδρυμα χωριστά ισχύει, παρά τις όποιες επιφυλάξεις για την εξέλιξη του ηλεκτρονικού εμπορίου που μπορεί να έχει, ότι αν θέλει να συμμετέχει με αξιώσεις στο μέλλον στην αγορά του Retail- Banking, θα πρέπει να ετοιμάσει και να προσφέρει ένα ικανοποιητικό πακέτο υπηρεσιών που αφορούν στο Internet Banking. Σε κάθε άλλη περίπτωση θα σημειώσει απώλεια πελατών καθώς και επιχειρηματικών ευκαιριών. Έτσι, οι τράπεζες είναι υποχρεωμένες με την υποστήριξη της τεχνολογίας να αναπτύξουν μια ξεκάθαρη στρατηγική που θα τις οδηγήσει στη νέα εποχή. Το βασικό χαρακτηριστικό του E- Banking είναι η ηλεκτρονική διασύνδεση της τράπεζας με τον πελάτη με την βοήθεια τηλεπικοινωνιακών δικτύων με σκοπό τη δρομολόγηση, τη συμφωνία, τη διεκπεραίωση και τελικά τον έλεγχο των συναλλαγών μεταξύ τους.

Η αγορά του E- Banking βρίσκεται σε τροχιά δυναμικής ανάπτυξης. Σύμφωνα με την Datamonitor στη Γερμανία μέχρι το 2004 ο αριθμός των χρηστών των ηλεκτρονικών καναλιών για τις αγορές τους ανερχόταν στα 29,5εκ. Για την εξυπηρέτηση των συναλλαγών οι δαπάνες για την αγορά τεχνολογιών πληροφορικής στον τομέα του E- Banking θα αυξηθούν από τα 360εκ. δολ. το 1999 στα 1,4δισ. δολ. το 2004. Οι ραγδαίες εξελίξεις στις τεχνολογίες πληροφορικής οδήγησαν τις τράπεζες σε κατάσταση πλήρους αναδιάρθρωσης. Στην αναπτυσσόμενη αγορά του E- Banking εισέρχονται συνεχώς νέοι ανταγωνιστές προσπαθώντας να κερδίσουν την προτίμηση των απαιτητικών Online- Πελατών. Για τις τράπεζες αυτό σημαίνει ότι θα πρέπει να αναπτύξουν νέες στρατηγικές, νέα κανάλια διανομής και σημαντικές επενδύσεις.

Στο ερώτημα τώρα γιατί πρέπει κανείς να ασχοληθεί με το E- Banking, αφού στις Ηνωμένες Πολιτείες καμία μεγάλη τράπεζα δεν πραγματοποίησε κέρδη από αυτόν το τομέα η απάντηση κατά τους Cooper και Wolff της Pricewaterhouse είναι μια: Για το μέλλον. Ήδη το 15% των αμερικανικών νοικοκυριών πραγματοποιούν τραπεζικές συναλλαγές online, κυρίως άτομα με υψηλή μόρφωση και μεγάλο εισόδημα. Αυτό δείχνει για τις τράπεζες ότι υπάρχει ιδιαίτερο ενδιαφέρον. Στη Γερμανία το 1999 καταγράφηκαν 8,5εκ. χρήστες του Internet ενώ το 37% από αυτούς χρησιμοποίησε το E- Banking. Αυτά αφορούν αφενός μεν στα παραδοσιακά τραπεζικά προϊόντα, τα οποία μέσω του διαδικτύου διευκολύνονται στη χρήση τους με ένα πολύ χαμηλότερο κόστος για τις τράπεζες, και αφετέρου σε νέα τεχνολογικά προϊόντα που διευκολύνουν βασικά το ηλεκτρονικό εμπόριο. Σ' αυτά ανήκουν: το ηλεκτρονικό χρήμα και οι επιταγές, η ηλεκτρονική εξόφληση λογαριασμών, η παροχή συμβούλων, η προσφορά ειδικών πωλών στο διαδίκτυο, οι υπηρεσίες αναγνώρισης ταυτότητας χρηστών κ.λ.π.

Η ανάπτυξη όλων αυτών των προϊόντων με την αξιοποίηση της σύγχρονης τεχνολογίας θα οδηγήσει με βάση έρευνα της Ευρωπαϊκής Κεντρικής Τράπεζας στις εξής σημαντικές αλλαγές στη λειτουργία των τραπεζών:

1. Μείωση των καταστημάτων αφού όλο και περισσότερες συναλλαγές θα γίνονται από απόσταση.
2. Κατάρτιση των συνεργατών σε θέματα marketing και σύγχρονης τεχνολογίας.
3. Σύναψη συμφωνιών με εξειδικευμένες εταιρείες παροχής υπηρεσιών κυρίως τεχνολογίας (outsourcing).

4. Μείωση της αφοσίωσης των πελατών (customer loyalty) αφού αποκτούν τη δυνατότητα να επισκέπτονται και ανταγωνιστικές προσφορές.
5. Συνεργασίες των τραπεζών για τη διευκόλυνση της παραγωγής και της διακίνησης των προϊόντων.
6. Στενότερη σχέση και συνεργασίες μεταξύ τραπεζών και εταιρειών πληροφορικής για την αξιοποίηση της τεχνολογίας και τον επιμερισμό του κόστους έρευνας.

Οι αλλαγές αυτές είναι φανερό ότι θα εντείνουν τον ανταγωνισμό μεταξύ των τραπεζών αλλά και θα προσελκύσουν νέους μη τραπεζικούς οργανισμούς να εισέλθουν στην αγορά, αφού η ανάπτυξη των προϊόντων δεν προϋποθέτει την ύπαρξη εκτεταμένου δικτύου τραπεζικών καταστημάτων (virtual banking).

Θα πρέπει επίσης να γίνει αναφορά και στις μεταβολές που θα προκύψουν στη μορφολογία των κινδύνων που αναλαμβάνουν οι τράπεζες τη νέα εποχή. Η αναφερθείσα μελέτη της Ευρωπαϊκής Κεντρικής Τράπεζας διακρίνει τρεις κατηγορίες κινδύνων:

1. Τους στρατηγικούς κινδύνους που είναι δυνατό να προκύψουν από την κακή εκτίμηση των εκάστοτε δυνατοτήτων απορρόφησης των προσφερόμενων προϊόντων από την αγορά.
2. Τους νομικούς κινδύνους που προέρχονται από τη μη επίλυση νομικών θεμάτων που είναι συνδεδεμένα με τη διενέργεια των συναλλαγών π.χ. ηλεκτρονική υπογραφή, νομική εγκυρότητα των συναλλαγών από απόσταση κ.λ.π.
3. Τους λειτουργικούς κινδύνους, οι οποίοι μπορεί να εμφανιστούν και να δημιουργήσουν προβλήματα στην τράπεζα από τη μη ομαλή λειτουργία των τεχνολογικών συστημάτων. Τεχνικά προβλήματα, είτε εσωτερικά είτε εξωτερικά, έχουν ως αποτέλεσμα την ακύρωση των συναλλαγών που επιθυμούν να πραγματοποιήσουν οι πελάτες. Αυτό δημιουργεί πρόβλημα αξιοπιστίας της τράπεζας στα μάτια των πελατών και θα μπορούσε να το συγκρίνει κανείς με την εικόνα μιας τράπεζας, η οποία κατά την προσέλευση του πελάτη στο ταμείο της δεν διαθέτει ρευστότητα να τον εξοφλήσει.

Με την αναγνώριση των παραπάνω κινδύνων προκύπτει ένα θέμα διαχείρισής τους. Η αντιμετώπιση τους θα εξαρτηθεί από την ικανότητα των τραπεζών να αναπτύξουν συστήματα διαχείρισης κινδύνων, τα οποία να είναι σε θέση να εκτιμήσουν τον κίνδυνο με μεγαλύτερη δυνατή ακρίβεια. Η εμπειρία των τραπεζών σε σχετικά ζητήματα είναι δεδομένη, αν και στην περίπτωση των νομικών κινδύνων ο αναλαμβανόμενος κίνδυνος είναι δύσκολο, αν όχι αδύνατο, να υπολογιστεί.

## **ΑΛΛΑΓΗ ΟΡΓΑΝΩΤΙΚΗΣ ΔΟΜΗΣ**

Η ηλεκτρονική τραπεζική διαδικτύου αλλάζει δραστικά την υφιστάμενη οργανωτική δομή των παραδοσιακών τραπεζικών σχημάτων, οδηγώντας σε πιο ευέλικτες εργασιακές σχέσεις και σε εκτεταμένη αναδιάρθρωση (ή ακόμη και σχετική απαξίωση) της υπάρχουσας υποδομής και των δικτύων.

Οι τεχνολογικές εξελίξεις αναμορφώνουν σημαντικά το τοπίο του τραπεζικού ανταγωνισμού τόσο από την πλευρά της ζήτησης, καθώς οι πελάτες θα μπορούν ευκολότερα να προβαίνουν σε συγκρίσεις προϊόντων και να επιλέγουν αναλόγων, όσο και από την πλευρά της προσφοράς, καθώς τα εμπόδια εισόδου στην αγορά, κυρίως της τραπεζικής λιανικής, υποχωρούν αισθητά, αφού οι τράπεζες διαδικτύου έχουν πολύ μικρότερο πάγιο κόστος εγκατάστασης.

Παράλληλα με την αλλαγή του τοπίου σε επίπεδο ανταγωνισμού οι τράπεζες έχουν να αντιμετωπίσουν και μια σειρά από κινδύνους. Η ανάπτυξη της ηλεκτρονικής τραπεζικής αφενός εγείρει κινδύνους που συνδέονται με την τεχνολογία (π.χ. οι τράπεζες αντιμετωπίζουν τον κίνδυνο της επένδυσης σε τεχνολογίες που ενδέχεται να απαξιωθούν σύντομα ή να αφιερώσουν σημαντικούς πόρους στην εισαγωγή νέων προϊόντων χωρίς να έχει προηγηθεί ενδελεχής ανάλυση της ζήτησης και του βαθμού αποδοχής αυτών από την πελατεία), αφετέρου εντείνει υφιστάμενους κινδύνους των τραπεζών, όπως ο λειτουργικός, ο οποίος μπορεί να αυξηθεί αν οι τράπεζες δεν αναβαθμίσουν τα συστήματα εσωτερικού ελέγχου. Επιπλέον δεν θα πρέπει να παραβλέπεται ο νομικός κίνδυνος, που πηγάζει από τις δυσχέρειες στον έλεγχο της ασφάλειας των συναλλαγών στον κυβερνοχώρο.

### **Καινούρια τεχνολογία, νέα προϊόντα σε διεθνή κλίμακα**

Προς το παρόν οι περισσότερες δραστηριοποιούμενες στο διαδίκτυο τράπεζες, προσφέρουν τα προϊόντα τους κατά κύριο λόγο στους κατοίκους της χώρας όπου έχουν την έδρα τους. Δεν μπορούν δηλαδή να εξυπηρετήσουν μόνιμους κατοίκους άλλων χωρών.

## **ΕΙΔΗ E-BANKING**

Το e-banking χωρίζεται κυρίως σε τρία είδη, λαμβάνοντας ως κριτήριο το μέσο μέσω του οποίου πραγματοποιούνται οι τραπεζικές συναλλαγές. Τα είδη αυτά είναι:

1. Internet Banking ( Τραπεζική μέσω διαδικτύου)
2. Phone Banking (Τραπεζική μέσω τηλεφώνου)
3. Mobile Banking (Τραπεζική μέσω κινητού)

Ανάλογα με το κανάλι που χρησιμοποιείται για τη διενέργεια συναλλαγών, εντοπίζονται ιδιαίτερα χαρακτηριστικά ανά περίπτωση. Τα χαρακτηριστικά αυτά αφορούν τον αριθμό των προσφερόμενων υπηρεσιών, το περιβάλλον χρήσης (user interface), τον τρόπο πρόσβασης (authentication – authorization). Συνοπτικά τα χαρακτηριστικά αυτά περιγράφονται παρακάτω.

## **INTERNET BANKING**

Το internet banking πραγματοποιείται κατά βάση μέσω του διαδικτύου. Ένας χρήστης για να εκμεταλλευτεί τις υπηρεσίες του e-banking χρειάζεται απαραίτητα να διαθέτει ηλεκτρονικό υπολογιστή και σύνδεση στο internet. Συνήθως στις περισσότερες των περιπτώσεων ο υπολογιστής και η σύνδεση αρκούν για πρόσβαση στις ηλεκτρονικές υπηρεσίες.

Ωστόσο λόγω των αναγκών αυξημένης ασφάλειας που διέπουν τις ηλεκτρονικές τραπεζικές συναλλαγές, σε ορισμένες περιπτώσεις απαιτείται και προμήθεια επιπλέον συσκευών ασφαλείας όπως για παράδειγμα tokens ή smart readers ή εγκατάσταση ειδικού λογισμικού ασφαλείας όπως ψηφιακού πιστοποιητικού, τα οποία παρέχουν οι Τράπεζες στους πελάτες τους.

Μέσω του Internet Banking, ο πελάτης μιας τράπεζας έχει σχεδόν όλη την γκάμα των τραπεζικών συναλλαγών και της πληροφόρησης που χρειάζεται, όπως Μεταφορές Κεφαλαίων, Πληρωμές Δημοσίου, Τρίτων Οργανισμών, Καρτών και Δανείων κτλ

Οι τράπεζες έχουν πλέον την τεχνογνωσία και τις δυνατότητες να προσωποποιούν τις ηλεκτρονικές τους υπηρεσίες, ανάλογα με την κατηγορία πελατών που αντιπροσωπεύει ο



χρήστης και με τον τρόπο αυτό υπάρχουν για παράδειγμα επιπρόσθετες δυνατότητες για εταιρικούς χρήστες σε σχέση με ιδιώτες.

Μεγάλη επένδυση γίνεται και στο θέμα ασφάλειας που είναι ιδιαίτερα κρίσιμο για την αξιοπιστία των ηλεκτρονικών τραπεζικών συστημάτων. Άλλωστε η ασφάλεια είναι ο κύριος ίσως παράγοντας αποτροπής χρήσης του internet banking από τους περισσότερους πελάτες των τραπεζών. Ήδη έχουν γίνει μεγάλα βήματα από τις τράπεζες στη διαχείριση και εξασφάλιση ασφαλών συναλλαγών από τους πελάτες τους.

## PHONE BANKING

Οι υπηρεσίες που προσφέρονται μέσω phone banking χωρίζονται σε δυο κατηγορίες:

1. Αυτές που διεκπεραιώνονται από agents τηλεφωνικού κέντρου (call center) και
2. Αυτές που διεκπεραιώνονται αυτόματα μέσω συστημάτων αναγνώρισης φωνής (Interactive Voice Responses)

Στην πρώτη περίπτωση από την πλευρά του χρήστη απαιτείται η χρήση μιας απλής τηλεφωνικής συσκευής. Ο πελάτης επικοινωνεί φωνητικά με πράκτορα της τράπεζας και του μεταβιβάζει τα αιτήματά του. Εννοείται ότι σε κάθε περίπτωση οι πράκτορες ακολουθούν διαδικασίες ταυτοποίησης του πελάτη, ώστε να εξασφαλίζουν την ακεραιότητα και εμπιστευτικότητα των συναλλαγών και αιτημάτων του.

Στη δεύτερη περίπτωση ο πελάτης διεκπεραιώνει τις συναλλαγές του χωρίς την ενδιάμεση παρεμβολή πράκτορα. Όλη η διαδικασία είναι αυτοματοποιημένη και ο πελάτης απαντά στα φωνητικά μηνύματα που ακούει στο τηλέφωνο του. Όπως και μέσω call center έτσι και μέσω IVR, ακολουθούνται διαδικασίες πιστοποίησης και ταυτοποίησης του πελάτη που εξασφαλίζουν την ασφάλεια των συναλλαγών του.

## MOBILE BANKING

Το mobile banking δεν έχει ακόμα εδραιωθεί σε σχέση με το internet και το phone banking. Αν ληφθεί υπόψη η διείσδυση της κινητής τηλεφωνίας στα ελληνικά νοικοκυριά, τότε το mobile banking έχει όλες τις προϋποθέσεις να αποτελέσει στο κοντινό μέλλον ένα ευρέως χρησιμοποιούμενο κανάλι πραγματοποίησης ηλεκτρονικών συναλλαγών.

Οι τεχνολογίες που χρησιμοποιούνται διαφέρουν αρκετές περιπτώσεις από αυτές του internet banking. Πολλές πληροφοριακές και οικονομικές συναλλαγές γίνονται μέσω mobile banking. Ο χρήστης έχει τη δυνατότητα να παρακολουθεί το χαρτοφυλάκιο του και τα υπόλοιπα του, να μεταφέρει χρήματα, να πληρώνει λογαριασμούς, κάρτες κτλ.

## **Κεφάλαιο 4ο**

### **MOBILE και INTERNET BANKING**

#### **Παρεχόμενες Υπηρεσίες / Πλεονεκτήματα / Κίνδυνοι**

#### **MOBILE BANKING**

Οι συνθήκες οι οποίες διαμορφώνονται στην παγκόσμια τραπεζική αγορά με την αύξηση της ανάγκης των πελατών για φορητότητα οδηγούν στη συνεχή αλλαγή των μέχρι τώρα υφιστάμενων δικτύων διανομής των τραπεζικών προϊόντων. Παράγοντες όπως η απελευθέρωση του τραπεζικού συστήματος με τη σύγκληση των οικονομιών όλου του κόσμου, η όξυνση του παγκόσμιου ανταγωνισμού, οι τεχνολογικές εξελίξεις στον τομέα των τηλεπικοινωνιών και, γενικότερα, του ηλεκτρονικού και κινητού εμπορίου, ιδιαίτερα στους νέους, ήταν η αφορμή για τη ραγδαία ανάπτυξη εναλλακτικών δικτύων εξυπηρέτησης. Η Ηλεκτρονική Τραπεζική (Electronic ή Online Banking) αποτελεί το πιο σύγχρονο και αποτελεσματικό μέσο για τη διενέργεια συναλλαγών.

Το m-banking, σύντμηση του Mobile Banking, παρέχει τη δυνατότητα διαχείρισης τραπεζικών λογαριασμών με την χρήση της τεχνολογίας του κινητού τηλεφώνου, άμεσης πληροφόρησης 24 ώρες το 24ωρο και, ανάλογα με τον τρόπο που έχει σχεδιάσει η τράπεζα την υπηρεσία της, την άμεση διενέργεια συναλλαγών. Έτσι, καλύπτει ένα μεγάλο σύνολο οικονομικών υπηρεσιών και προϊόντων, που παρέχουν τα πιστωτικά ιδρύματα τόσο μέσω των παραδοσιακών καταστημάτων όσο και μέσω των άλλων εναλλακτικών δικτύων διανομής, καταργώντας ουσιαστικά τη στενότητα του χώρου και του χρόνου.

#### **ΠΑΝΕΥΡΩΠΑΪΚΗ ΕΡΕΥΝΑ ΓΙΑ ΤΟ M-BANKING**

Από την εταιρία ερευνών Forrester Research

#### **Υπηρεσίες Mobile Banking:**

##### **Πρόκληση για τράπεζες και τηλεπικοινωνιακά δίκτυα**

Αν και οι περισσότερες μεγάλες ευρωπαϊκές τράπεζες που δραστηριοποιούνται κατά κύριο λόγο στη λιανική τραπεζική προσφέρουν τραπεζικές υπηρεσίες μέσω κινητού τηλεφώνου που βασίζονται κυρίως στην τεχνολογία των γραπτών μηνυμάτων (SMS) και το διαδίκτυο, μόνο το 5% των χρηστών τις χρησιμοποιούν σήμερα, τονίζει σε πρόσφατη έρευνά της η εταιρία μελετών Forrester Research (η έρευνα αφορά Τράπεζες με πανευρωπαϊκή παρουσία). Πρόκειται κυρίως για νέους στην ηλικία χρήστες, στην πλειοψηφία άντρες, τεχνολογικά ενημερωμένους, υψηλού εισοδήματος με εμπειρία στις on line τραπεζικές υπηρεσίες. Αυτοί χρησιμοποιούν το κινητό τους για απλές διαδραστικές υπηρεσίες όπως είναι ο έλεγχος του τραπεζικού τους λογαριασμού και ειδοποιήσεις μέσω SMS από την τράπεζά που είναι πελάτες.

*Το ερώτημα όμως που απασχολεί την τραπεζική αγορά αλλά και τους αναλυτές του τεχνολογικού κλάδου είναι γιατί το m-banking έχει τόσο χαμηλά ποσοστά διείσδυσης στο κοινό.*

Όσοι δε χρησιμοποιούν τις συγκεκριμένες υπηρεσίες λένε ότι δεν αντιλαμβάνονται τα οφέλη αυτών των υπηρεσιών, δε γνωρίζουν ότι υπάρχουν τέτοιου είδους υπηρεσίες ή προτάσσουν τα

προβλήματα ασφαλείας κατά τη χρήση τέτοιου είδους υπηρεσιών. Όπως τονίζουν οι αναλυτές της Forrester Research, οι τράπεζες που προσφέρουν υπηρεσίες m-banking πρέπει να καταστήσουν σαφές στους πελάτες τους την απλότητα και την εγκυρότητα αυτών των υπηρεσιών. Όπως υποστηρίζουν, πρέπει να γίνει συνείδηση των καταναλωτών ότι αυτές οι υπηρεσίες προσφέρονται οπουδήποτε και οποιαδήποτε στιγμή.

## Πρόκληση

Σύμφωνα με τα στοιχεία της έρευνας, οι υπηρεσίες m-banking είναι μια “καυτή” πολλά υποσχόμενη αγορά για την ευρωπαϊκή λιανική τραπεζική. Πολλές τράπεζες έχουν επενδύσει στο συγκεκριμένο τομέα θεωρώντας πως θα αποτελέσουν ένα ακόμα κανάλι αυτό-εξυπηρέτησης των καταναλωτών.

Σύμφωνα με τα μέχρι τώρα δεδομένα:

A) Οι περισσότερες μεγάλες τράπεζες προσφέρουν κάποιο είδος υπηρεσιών m-banking. Η πρώτη που δραστηριοποιήθηκε στη συγκεκριμένη αγορά ήταν η ABN-AMRO το 1997. Το 2000 και το 2001, όπως συνέβη με τις τράπεζες στη Βόρεια Αμερική, πολλές ευρωπαϊκές τράπεζες προώθησαν υπηρεσίες m-banking βασισμένες στην τεχνολογία WAP, για να τις κλείσουν μερικά χρόνια αργότερα ελλείψει των χρηστών. Μετά την αποτυχημένη προσπάθεια οι τράπεζες έχουν επιστρέψει βαθμιαία στις υπηρεσίες m-banking διαφοροποιώντας όμως το μοντέλο προσφοράς αυτών των υπηρεσιών. Σχεδόν όλες οι μεγάλες τράπεζες στη Γερμανία, τη Γαλλία, τη Μεγάλη Βρετανία, την Ιταλία, την Ισπανία, την Ολλανδία, και τη Σουηδία προσφέρουν κάποιο είδος κινητής τραπεζικής υπηρεσίας.

Χώρα	Τράπεζα	Ενημέρωση μέσω sms	Προσφέρουν συναλλαγές mobile banking
Μεγάλη Βρετανία	Lloyds TSB	Ναι	Όχι
Μεγάλη Βρετανία	Barclays	Ναι	Ναι
Μεγάλη Βρετανία	HSBC	Όχι	Ναι
Μεγάλη Βρετανία	Nationwide Building Society	Όχι	Ναι
Μεγάλη Βρετανία	Alliance & Leicester	Όχι	Ναι
Γερμανία	Sparkassen	Ναι	Ναι
Γερμανία	Volksbanken Raiffeisenbanken	Ναι	Ναι
Γερμανία	Deutsche Postbank	Όχι	Ναι
Γερμανία	Sparda-Banken	Ναι	Ναι
Γερμανία	Deutsche Bank	Όχι	Ναι
Ολλανδία	Postbank	Ναι	Όχι

Ολλανδία	Rabobank	Ναι	Όχι
Ολλανδία	ABN AMRO Bank	Ναι	Ναι
Σουηδία	Swedbank	Ναι	Ναι
Σουηδία	Nordea	Ναι	Ναι
Σουηδία	Svenska Handelsbanken	Ναι	Ναι
Γαλλία	Crédit Agricole	Ναι	Ναι
Γαλλία	La Banque Postale	Ναι	Ναι
Γαλλία	Caisse d'Épargne	Ναι	Ναι
Γαλλία	Crédit Mutuel	Ναι	Ναι
Γαλλία	Société Générale	Ναι	Ναι
Γαλλία	BNP Paribas	Ναι	Ναι
Ισπανία	la Caixa	Ναι	Ναι
Ισπανία	BBVA	Ναι	Ναι
Ισπανία	Caja Madrid	Ναι	Ναι
Ισπανία	Banco Santander	Ναι	Ναι
Ιταλία	UniCredit Banca	Ναι	Ναι
Ιταλία	Intesa Sanpaolo	Ναι	Ναι
Ιταλία	Banca Monte dei Paschi di Siena	Ναι	Ναι
Ιταλία	Banca Popolare di Milano	Ναι	Ναι

**Πίνακας 1. Τράπεζες που προσφέρουν υπηρεσίες mobile banking στην Ευρώπη, Πηγή: Forrester Research, 2007**

Β) Οι παρεχόμενες υπηρεσίες αφορούν τις απλές ειδοποιήσεις μέσω SMS αλλά και πιο περίπλοκες συναλλαγές. Η υπάρχουσα τεχνολογία βοηθά τις τράπεζες, είτε να προσφέρουν απλές υπηρεσίες m-banking βασισμένες κυρίως στη χρήση SMS που μπορούν να χρησιμοποιηθούν από μεγάλο αριθμό πελατών που επιθυμούν να επιβαρυνθούν με λογικό κόστος, είτε να παρέχουν πιο σύνθετες διαδραστικές υπηρεσίες σε πελάτες που μπορούν να επιβαρυνθούν με υψηλότερο κόστος.

Είναι χαρακτηριστικές οι υπηρεσίες SMS των Lloyds. Οι πελάτες τους μπορούν να λάβουν δωρεάν μια φορά την εβδομάδα SMS για τις τελευταίες έξι συναλλαγές και τον έλεγχο του τρέχοντος λογαριασμού τους. Με μικρό μηνιαίο αντίτιμο οι χρήστες μπορούν επίσης να λάβουν ενημέρωση μέσω SMS για το κλείσιμο του λογαριασμού τους ή όταν έχουν ξεπεράσει το όριο των πιστωτικών τους λογαριασμών. Υπάρχουν όμως και πιο σύνθετες υπηρεσίες, όπως η μεταφορά χρημάτων, η πληρωμή λογαριασμών, ο έλεγχος δανείων μέσω mobile Internet.

Γ) Αυτές οι υπηρεσίες είναι διαθέσιμες σε όλους τους κατόχους συσκευών κινητής τηλεφωνίας. Ογδόντα έξι τοις εκατό των ευρωπαϊκών ενηλίκων χρησιμοποιούν κινητό τηλέφωνο και για τις τράπεζες που προσφέρουν υπηρεσίες m-banking, κάθε πελάτης με ένα κινητό τηλέφωνο είναι

δυναμικός χρήστης, επειδή όλα τα τηλέφωνα υποστηρίζουν SMS. Η Rabobank έχει δημιουργήσει το δικό της δίκτυο κινητής τηλεφωνίας για να υποστηρίξει υπηρεσίες m-banking, τη RaboMobiel, προκειμένου να διαθέσει στους πελάτες της τις δικές της συσκευές κινητής τηλεφωνίας.

### Χαμηλή διείσδυση m-banking

Από τη στιγμή που οι κινητές τραπεζικές υπηρεσίες είναι διαθέσιμες από τις περισσότερες μεγάλες τράπεζες της Ευρώπης ήδη από τα τέλη της δεκαετίας του '90, θα ήταν επόμενο η διείσδυση αυτών των υπηρεσιών να κυμαίνεται σε υψηλά ποσοστά.

Η έρευνα όμως της Forrester Research δείχνει το αντίθετο. Είναι λίγοι οι Ευρωπαίοι που χρησιμοποιούν τις κινητές τραπεζικές υπηρεσίες σήμερα. Λίγες μόνο τράπεζες έχουν πείσει μεγάλο αριθμό πελατών τους να χρησιμοποιήσουν τις τραπεζικές υπηρεσίες μέσω SMS. Για παράδειγμα η υπηρεσία Messalia SMS της Générale Sociéte έχει περισσότερους από 675.000 χρήστες. Στη Μεγάλη Βρετανία υπάρχουν περίπου 460.000 χρήστες τραπεζικών υπηρεσιών μέσω SMS. Αλλά αυτοί είναι οι πρωτοπόροι και οι εξαιρέσεις. Υπολογίζεται πως το 5% όλων των χρηστών διαδικτύου χρησιμοποιούν τις κινητές τραπεζικές εργασίες - λίγο περισσότερο απ' ό τι στις ΗΠΑ ή τον Καναδά.



**Καταναλωτές που χρησιμοποιούν υπηρεσίες mobile banking στην Ευρώπη, Βάση: 7.160 χρήστες,**

**Πηγή: Forrester Research, 2007**

Αυτός ο αριθμός διαφοροποιείται από χώρα σε χώρα. Η Σουηδία και η Ιταλία, χώρες με πολύ υψηλά ποσοστά χρήσης κινητής τηλεφωνίας στην Ευρώπη εμφανίζουν ποσοστά χρήσης υπηρεσιών m-banking γύρω στο 11% και 9% αντίστοιχα. Οι χρήστες είναι κυρίως νέοι ηλικίας μεταξύ 25 - 35 ετών, που χρησιμοποιούν επίσης τις on line τραπεζικές εργασίες, ανήκουν στην κατηγορία των υψηλών εισοδημάτων, είναι τεχνολογικά ενημερωμένοι και η πλειοψηφία χρησιμοποιεί το Διαδίκτυο καθημερινά.

	Χρήση mobile banking	Δεν χρησιμοποιούν mobile banking
Μ.Ο. Ηλικίας	38	39
% Ανδρών	61%	51%
Υψηλό εισόδημα	36%	31%
Τεχνολογικά ενημερωμένοι	71%	58%
Online για περισσότερα από 7 χρόνια	47%	33%
Online καθημερινά	64%	51%
Χρήση online banking	80%	56%

**Χαρακτηριστικά Ευρωπαίων χρηστών υπηρεσιών mobile banking, Βάση: 7.160 χρήστες, Πηγή: Forrester Research, 2007**

Τέσσερις από τους πέντε χρήστες υπηρεσιών m-banking κάνουν χρήση on line τραπεζικών υπηρεσιών μέσω του υπολογιστή τους. Το 57% των χρηστών υπηρεσιών m-banking χρησιμοποιούν συνήθως απλές υπηρεσίες και η πιο συνηθισμένη είναι ο έλεγχος τραπεζικού υπολοίπου. Εξίσου δημοφιλείς είναι οι ειδοποιήσεις μέσω SMS (29% και 28%), ενώ ένα ποσοστό γύρω στο 27% κάνουν έλεγχο των τραπεζικών τους συναλλαγών μέσω του κινητού τους τηλεφώνου. Πιο σύνθετες συναλλαγές, όπως μεταφορά χρημάτων ή αλλαγή τραπεζικού κωδικού, είναι λιγότερο συνηθισμένες μέσω του m-banking,



**Χρήση υπηρεσιών mobile banking στην Ευρώπη ανά ηλικία, Βάση: 374 χρήστες, Πηγή: Forrester Research, 2007**

### Προβλήματα και λύσεις

Οι καταναλωτές δεν αντιλαμβάνονται τα οφέλη των υπηρεσιών m-banking γι' αυτό και δεν τις χρησιμοποιούν. Προτιμούν τη χρήση των ATM ή των παραδοσιακών μεθόδων συναλλαγής με

την τράπεζα. Σύμφωνα με τους αναλυτές της Forrester Research, αυτό αποτελεί μία από τις βασικές αιτίες της χαμηλής διείσδυσης του m-banking στην ευρωπαϊκή αγορά. Η πλειονότητα επίσης δεν γνωρίζει ότι υπάρχουν οι συγκεκριμένες υπηρεσίες ενώ παράλληλα νιώθουν ανασφαλείς κατά τη χρήση τους. Επίσης ένα σημαντικό ποσοστό αναρωτιέται για το κόστος αυτών των υπηρεσιών και υποστηρίζει πως δεν κατέχει την τεχνολογικά προηγμένη συσκευή κινητής τηλεφωνίας για τέτοιου είδους εφαρμογές.

Η Forrester Research επισημαίνει πως οι υπεύθυνοι των τμημάτων πληροφορικής των τραπεζών μπορούν να κάνουν πολλά για να αλλάξουν τα δεδομένα. Δουλεύοντας από κοινού μαζί με τα τμήματα μάρκετινγκ των τραπεζών μπορούν να πείσουν τους πελάτες τους για τη χρησιμότητα και την απλή λειτουργία των υπηρεσιών mobile banking. Μπορούν να αποδείξουν με συγκεκριμένα παραδείγματα για την υπεραξία αυτών των υπηρεσιών. Μπορούν επίσης να εστιάσουν σε συγκεκριμένες κατηγορίες πελατών όπως είναι οι νέοι σε ηλικία και τεχνολογικά εγγράμματοι χρήστες και να τους προσφέρουν ποικιλία υπηρεσιών m-banking, εστιάζοντας σε έγκυρες και χωρίς χρονικούς και τοπικούς περιορισμούς υπηρεσίες.

---

Mobile Banking : Διαχείριση Τραπεζικών Συναλλαγών Μέσω Κινητού Τηλεφώνου « Γεώργιος Μπιζανίδης »  
<http://www.sepe.gr/>  
<http://www.mmaglobal.com/>  
<http://www.forrester.com/>  
<http://www.plant-management.gr/>

## INTERNET BANKING

### Η ιστορία του internet banking

Κάνοντας μια μικρή ιστορική αναδρομή στο internet banking η πρώτη online τραπεζική υπηρεσία εμφανίστηκε το 1990 από την Wells Fargo Bank που έχει έδρα στην Καλιφόρνια των ΗΠΑ. Το 1993 η Stanford Federal Credit Union εισήγαγε νέα ηλεκτρονική υπηρεσία στην αγορά, η οποία υπερέχει των υπαρχόντων 2 μέχρι εκείνη τη στιγμή παγκοσμίως που προσέφεραν η Wells Fargo Bank (όπως είπαμε) και η Bank of America, οι οποίες εκτελούσαν μόνο απλές συναλλαγές κατά βάση ερωτήσεις συγκεκριμένα μόνο να βλέπουν τον λογαριασμό τους on line. Η πλατφόρμα της Stanford Federal Credit Union, ονομαζόταν CUOnline και ήταν βασισμένο στην αρχιτεκτονική του telnet και μπορούσε να εκτελέσει και συναλλαγές. Τον πρώτο μήνα της λειτουργίας του στο CUOnline έγινα 4 συνολικά συναλλαγές.

Στη χώρα μας έχουμε να πούμε ότι η πρώτη τράπεζα στην Ελλάδα που διέθεσε υπηρεσίες μέσω internet ήταν η τότε ΕΓΝΑΤΙΑ Τράπεζα το 1997 (MARFIN EGNATIA BANK τώρα). Οι υπηρεσίες που παρείχε ήταν πολύ λίγες και απλές και περιορίζονταν κατά βάση σε πληροφορίες του λογαριασμού και μεταφορές κεφαλαίων εντός της τράπεζας.

Το 2000 η Τράπεζα Πειραιώς έφερε στην Ελλάδα την πρώτη ολοκληρωμένη εφαρμογή παροχής τραπεζικών συναλλαγών μέσω Internet και μάλιστα της έδωσε και δικό της brand name, WINBANK και όχι Τράπεζα Πειραιώς.

### Πλεονεκτήματα internet banking

Μεγάλη στροφή στη σύγχρονη τεχνολογία για την παροχή προϊόντων και υπηρεσιών, προκειμένου να επιτύχουν διερεύνηση των μεριδίων αγοράς τους με χαμηλότερο κόστος πραγματοποιούν οι Ελληνικές τράπεζες. Το χαμηλότερο κόστος αποτελεί σημείο- κλειδί για την ανάπτυξη των εναλλακτικών δικτύων παροχής ηλεκτρονικών τραπεζικών υπηρεσιών (προσωπικός υπολογιστής, σταθερό ή κινητό τηλέφωνο, αυτόματες ταμειολογιστικές μηχανές), καθώς, αν μια απλή συναλλαγή μέσω του τραπεζικού γκισέ κοστολογείται 1 Ευρώ, το κόστος μειώνεται στα 50 λεπτά αν πραγματοποιηθεί μέσω ATM και μόλις στα 5 λεπτά, αν πραγματοποιηθεί μέσω Internet.

Η τραπεζική από απόσταση, χωρίς τη μεσολάβηση του παραδοσιακού τραπεζικού καταστήματος, λαμβάνει μεγάλες διαστάσεις στο εξωτερικό, όπου οι «εικονικές» τράπεζες αυξάνονται με καταϊγιστικούς ρυθμούς προσελκύοντας στα ηλεκτρονικά γκισέ όλο και περισσότερους καταναλωτές. Σύμφωνα με στοιχεία της Ένωσης Γερμανικών Τραπεζών, πάνω από το 40% των Γερμανών που κάνουν χρήση του διαδικτύου πραγματοποιούν «διαδικτυακές» τραπεζικές συναλλαγές, ενώ στις ΗΠΑ 23 εκατ. πολίτες έχουν πρόσβαση σε κάποια υπηρεσία Internet banking.

Η χρήση ηλεκτρονικών υπηρεσιών προσφέρει αρκετά οφέλη και στον τραπεζικό οργανισμό που τις υιοθετεί. Οι τράπεζες μπορούν να χρησιμοποιήσουν το e-banking ώστε να μεγιστοποιήσουν τα πλεονεκτήματα που προσφέρει η χρήση του.

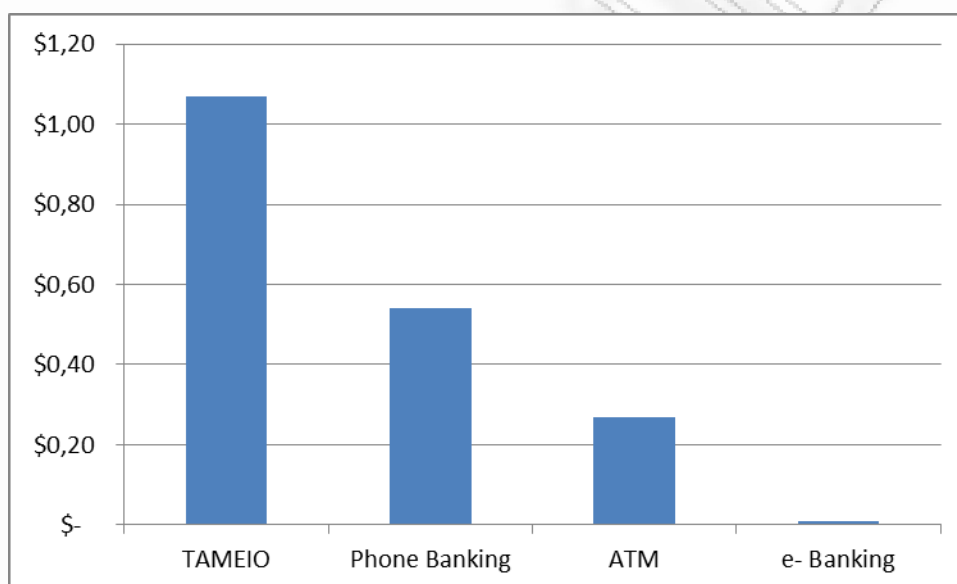
**Εναλλακτικά Δίκτυα:** οι τράπεζες έχουν τη δυνατότητα να επεκτείνουν τα δίκτυα εξυπηρέτησης πελατείας τους. Το e-banking δίνει τη δυνατότητα στις τράπεζες να εξυπηρετούν τους πελάτες τους και να διεκπεραιώνουν τις συναλλαγές τους μέσω νέων καναλιών που δεν προϋπήρχαν πριν μερικά χρόνια, όπως το internet, το τηλέφωνο και το κινητό.



**Καινοτόμες Υπηρεσίες:** Το e-banking δίνει το πλεονέκτημα στις τράπεζες να εκμεταλλευτούν τα προνόμια που προσφέρει η τεχνολογία και να δημιουργηθούν καινοτόμες υπηρεσίες οι οποίες δεν θα μπορούσαν με άλλο τρόπο να υλοποιηθούν.

**Μείωση λειτουργικού κόστους:** Σύμφωνα με μελέτες που έχουν γίνει στην Αμερική, το λειτουργικό κόστος μιας ολοκληρωμένης τραπεζικής συναλλαγής στο ταμείο ενός καταστήματος είναι 1,07\$, ενώ το κόστος μιας τηλεφωνικής συναλλαγής είναι 0,54\$. Το αντίστοιχο κόστος για μια συναλλαγή σε ATM είναι 0,27\$. Η συναλλαγή του internet κοστίζει στην τράπεζα μόλις 0,01\$.

Στο ακόλουθο διάγραμμα αναπαριστάτε και γραφικά η διαφορά του κόστους ανάμεσα στα κανάλια μέσω των οποίων διενεργούνται τραπεζικές συναλλαγές.



**Αύξηση ποιότητας εξυπηρέτησης:** Μέσω του e-banking και της αυτοματοποίησης των τραπεζικών εργασιών, οι τράπεζες προσφέρουν υπηρεσίες που αυξάνουν την ποιότητα εξυπηρέτησης των πελατών τους. Το όφελος αυτό είναι σημαντικό, εφόσον οι τράπεζες το εκμεταλλευτούν σωστά. Η ποιότητα της εξυπηρέτησης μπορεί όχι μόνο να αυξηθεί, αλλά πλέον να πιστοποιείται από εξουσιοδοτημένους φορείς, προσφέροντας κύρος και αξιοπιστία στα ηλεκτρονικά καταστήματα.

**Αύξηση πελατειακής βάσης:** Η δημιουργία φιλικών προς το χρήστη εφαρμογών, που παρέχουν ολοκληρωμένα πακέτα συναλλαγών και υπηρεσιών, συμβάλλουν στην προσέλκυση νέων πελατών και στην αύξηση της πελατειακής βάσης. Η προώθηση οποιουδήποτε τραπεζικού προϊόντος καθίσταται ελκυστικότερη, όταν συνοδεύεται και από την προοπτική μιας ορθής και ολοκληρωμένης ηλεκτρονικής διαχείρισης του.

**Καλή φήμη:** Τράπεζες με αξιόπιστες και αξιόλογες ηλεκτρονικές υπηρεσίες, ενισχύουν την καλή τους φήμη. Το e-banking αποτέλεσε και αποτελεί ένα είδος βιτρίνας για τους τραπεζικούς οργανισμούς.

Από το 2000 έως σήμερα όλες οι ελληνικές τράπεζες έχουν πλέον δικό τους ηλεκτρονικό κατάστημα και οι πελάτες τους έχουν τη δυνατότητα να εκτελέσουν πολλών και διαφορετικών ειδών συναλλαγές με αυτές με δυνατότητες να εκτελούν και διατραπεζικές συναλλαγές από απλές πληρωμές δόσεων καρτών έως αγοροπωλησίες τίτλων όχι μόνο χρηματιστηριακών αλλά και real estate. Μπορούν όμως οι τράπεζες να διασφαλίσουν τους πελάτες τους και να τους εγγυηθούν τόσο την ασφάλεια όσο και την ιδιωτικότητα, το απόρρητο δηλαδή, των τραπεζικών τους συναλλαγών; Έχουν την δυνατότητα οι τράπεζες να δώσουν απαντήσεις στα ερωτήματα που αναφέραμε στην αρχή;

Παρακάτω θα παρουσιάσουμε και θα αναλύσουμε τους διάφορους κινδύνους που απειλούν τις ηλεκτρονικές μας συναλλαγές και θα αναδείξουμε τρόπους προστασίας από αυτούς.

## **ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ ΓΙΑ ΤΟ E-BANKING**

Ο κάθε τραπεζικός οργανισμός είτε δραστηριοποιείται ηλεκτρονικά εδώ και κάποια χρόνια είτε διαμορφώνει τη στρατηγική του στο e-επιχειρείν, θα πρέπει να έχει υπόψη ότι κάθε επιχείρηση οφείλει να είναι εξοικειωμένη με την Διαχείριση Κρίσεων και Επιχειρηματικού Κινδύνου. Πρόκειται για μια διαδικασία που έχει εφαρμογή στη διασύνδεση των διαφόρων λειτουργιών εντός της επιχείρησης (Διεύθυνση Ηλεκτρονικής Τραπεζικής, Διεύθυνση Πληροφορικής, Διεύθυνση Οικονομικών Υπηρεσιών, Νομική Υπηρεσία Διεύθυνση Πωλήσεων, Διεύθυνση Marketing κ) αλλά και στις σχέσεις της με τους πελάτες και τους εξωτερικούς συνεργάτες.

Οι τράπεζες που πιστεύουν ότι μπορούν να προστατευτούν, εγκαθιστώντας κάποιο antivirus, ένα firewall και κάποια εφαρμογή κρυπτογράφησης δυστυχώς απατώνται. Η ασφάλεια των υπολογιστών αποτελεί μικρό μόνο μέρος μιας ολοκληρωμένης λύσης διαχείρισης κινδύνων ηλεκτρονικής Τραπεζικής.

Ένα πραγματικά αποτελεσματικό πρόγραμμα διαχείρισης κινδύνων και κρίσεων ηλεκτρονικής τραπεζικής ενσωματώνει ασφαλιστικά προϊόντα μετριασμού του επιχειρηματικού κινδύνου και του κόστους που προκύπτει έπειτα από μια «ηλεκτρονική» καταστροφή. Λίγες μόνο τράπεζες έχουν πραγματικά εφαρμόσει λεπτομερή προγράμματα ασφάλισης ως μέρος των προσπαθειών τους για την πρόληψη κρίσεων και την αποτροπή του ηλεκτρονικού εγκλήματος. Πρέπει να σκεφτούμε τόσο τις απώλειες που θα είχε μια τράπεζα ως προς την παραγωγικότητα, τις πωλήσεις αλλά και τη φήμη της στο καταναλωτικό κοινό και τους συνεργάτες τη, αν ήταν υποχρεωμένη να διακόψει τη λειτουργία της για 48 ώρες λόγω τεχνικών προβλημάτων.

### **Αποτίμηση Επιχειρηματικού Κινδύνου.**

Προκειμένου η τράπεζα να αποτιμήσει τους κινδύνους που έχουν σχέση με την ηλεκτρονική τραπεζική, πρέπει να προβεί σε μια ανάλυση, όπως αυτή που περιγράφεται ακολούθως ώστε να καθοριστούν οι στόχοι και να εντοπιστούν εγγενείς αδυναμίες οι οποίες θα πρέπει να έχουν εντοπιστεί εγκαίρως ώστε να μπορέσουν να αντιμετωπιστούν όσο το δυνατό γρηγορότερα και με το μικρότερο δυνατό κόστος.

Η ανάλυση που θα πρέπει να γίνει, θα πρέπει να ακολουθεί τους παρακάτω γενικούς κανόνες οι οποίοι αγγίζουν σχεδόν το συνολικό τρόπο λειτουργίας και οργάνωσης της τράπεζας και θα πρέπει να απαντούν σε επιμέρους ερωτήματα σχετικά με τι επιθυμεί να επιτύχει μέσα από σε μια εμπορική ηλεκτρονική εφαρμογή e-banking, καθώς και τι μπορεί η τράπεζα να υποστηρίξει με την υπάρχουσα δομή και υλικοτεχνική υποδομή.

- **Ανάλυση Επιχειρηματικού Μοντέλου της Τράπεζας**
  - ✓ Διαθέτει η τράπεζα λογιστική οργάνωση βασισμένη σε ηλεκτρονικές διαδικασίες;
  - ✓ Ποιοι είναι οι στόχοι ως προς την τεχνολογική ολοκλήρωση των ενδοεπιχειρησιακών διαδικασιών; Ελέγχονται από την ίδια την τράπεζα ή γίνεται ανάθεση σε εξωτερικούς συνεργάτες;
  - ✓ Παρέχει η τράπεζα υπηρεσίες προς τρίτους με ηλεκτρονικά μέσα;
- **Ανάλυση Πνευματικού Κεφαλαίου της Τράπεζας**
  - ✓ Ποια είναι η αξία του πνευματικού κεφαλαίου της Τράπεζας, όπως βάσεις δεδομένων, πνευματικά δικαιώματα, εμπορικά σήματα κτλ;
- **Συνεργασίες**

- ✓ Με ποιους συνεργάζεται ηλεκτρονικά στις βασικές της δραστηριότητες (προμηθευτές, πελάτες, συνεργάτες), οι οποίοι θα μπορούσαν να επηρεαστούν από μια πιθανή κρίση;
- **Τεχνολογική Ανάλυση**
  - ✓ Η τεχνολογική υποδομή καλύπτει τις ανάγκες της στρατηγικής στο e-banking;
- **Λειτουργική Περιορισμοί**
  - ✓ Είναι σε θέση το e-banking να ανταποκριθεί σε παροχή υπηρεσιών 24 ώρες το 24ωρο;
- **Ασφάλεια των Δεδομένων**
  - ✓ Πόσο καλό είναι το επίπεδο προστασίας των προσωπικών δεδομένων πελατών, υπαλλήλων, επιχειρηματικών συνεργατών, καθώς και των οικονομικών και νομικών πληροφοριών της τράπεζας;
- **Εξωτερικοί Παράγοντες**
  - ✓ Είναι η τράπεζα εναρμονισμένη με τη σχετική νομοθεσία, όπως οι κανονισμοί EU Data directive, Digital Millennium Copyright Act, κ.α.;
  - ✓ Πόσο ασφαλείς είναι οι ηλεκτρονικές συναλλαγές;
- **Συμβατικές Υποχρεώσεις**
  - ✓ Παρέχει η Τράπεζα δηλώσεις προστασίας προσωπικών δεδομένων, παραίτησης από ευθύνη (disclaimer) κ.ά.;
  - ✓ Γνωρίζει τις κυρώσεις σε περίπτωση που αποδειχθεί ότι παρέβη κάποια από τις παραπάνω δηλώσεις;

Η έννοια της Διαχείρισης Επιχειρηματικού Κινδύνου στο πλαίσιο του e-banking είναι ευρύτερη και συμπεριλαμβάνει την έννοια της Ασφάλειας Πληροφοριών. Η Ασφάλεια Πληροφοριών εστιάζει στην προστασία και την ακεραιότητα των πληροφοριακών κεφαλαίων, η Διαχείριση Επιχειρηματικού Κινδύνου αφορά σε γενικότερα ζητήματα, τα οποία επηρεάζουν άμεσα τη βιωσιμότητα του e-banking. Η Ασφάλεια Πληροφοριών είναι λοιπόν μια υποκατηγορία της Διαχείρισης Κρίσεων, για την ακρίβεια μια από τις σημαντικότερες.

Η κύρια διαφοροποίηση εντοπίζεται στον καθορισμό της έννοιας «κεφάλαιο» αντίστοιχα στις δύο περιπτώσεις. Η ασφάλεια Πληροφοριών αποκρούει τις απειλές εναντίον του πληροφοριακού και υπολογιστικού κεφαλαίου, ενώ η Διαχείριση Επιχειρηματικού Κινδύνου αφορά στην πρόληψη οικονομικών και γενικότερα εσωτερικών κρίσεων, οι οποίες μάλιστα αντικατοπτρίζονται στους συνεργάτες και το προσωπικό της Τράπεζας, γι αυτό και επηρεάζουν παράγοντες όπως η οικονομική ασφάλεια, η νομική και εμπορική αξιοπιστία (η καλή φήμη της επιχείρησης, τόσο προς τους καταναλωτές όσο και προς άλλες επιχειρήσεις) κτλ.

## **Διαχείριση Ηλεκτρονικών Κρίσεων**

Οι βασικοί κίνδυνοι που απειλούν τις εταιρίες που δραστηριοποιούνται στο ηλεκτρονικό εμπόριο γενικά αλλά και ειδικότερα για της Τράπεζες που δραστηριοποιούνται στο χώρο του e-banking και μπορούν να έχουν καταστρεπτικά αποτελέσματα για αυτές είναι δύο βασικών κατηγοριών όπως επιγραμματικά αναφέρονται ακολούθως.

### **1. Άμεσοι Κίνδυνοι**

- Προβλήματα τεχνολογικής υποδομής, τα οποία περιορίζουν την ικανότητα της τράπεζας να διεξαγάγει με ασφάλεια τις κύριες εμπορικές διαδικασίες,

συμπεριλαμβανομένης της επικοινωνίας με τους προμηθευτές, τους διανομείς και τους πελάτες

- Αποτυχία των εσωτερικών διαδικασιών να ελέγξουν την ασφάλεια δικτύωσης, με αποτέλεσμα τη μη διαθεσιμότητα εταιρικών δικτύων ή εφαρμογών, και την πιθανή «εισβολή» και ζημιά στο πνευματικό κεφάλαιο και τις ευάσθητες πληροφορίες της επιχείρησης από χάκερ, ιούς κ.α
- Δημοσιοποίηση απορρήτων εταιρικών πληροφοριών, σχεδίων ή άλλων εμπιστευτικών εμπορικών στοιχείων.
- Μη εξουσιοδοτημένη εσωτερική ή εξωτερική πρόσβαση σε εφαρμογές ή δεδομένα της τράπεζας
- Αποτυχία διεξαγωγής online συναλλαγών

## 2. Έμμεσοι Κίνδυνοι

- Δυσφήμιση του ονόματος της Τράπεζας
- Απώλεια κεφαλαίων
- Ακούσια παραβίαση των προσωπικών δεδομένων των πελατών μέσω της κοινοποίησης των προσωπικών τους στοιχείων
- Απώλειες από ηλεκτρονικές απάτες ή κλοπές
- Δικαστική δίωξη από τρίτους

## Πλαίσιο Διαχείρισης Ηλεκτρονικών Κρίσεων

Για να αντιμετωπιστούν οι ανωτέρω κίνδυνοι τόσο από μια οποιαδήποτε εταιρία η οποία δραστηριοποιείται μέσω internet τόσο και από ένα Τραπεζικό οργανισμό θέλει να προστατεύσει το ηλεκτρονικό του κατάστημα, υπάρχει ένα βασικό πλαίσιο διαχείρισης ηλεκτρονικών κινδύνων το οποίο πρέπει να περιλαμβάνει μια σειρά από συνιστώσες που βοηθούν στην αποτελεσματική διαχείριση τους.

### 1) Υποδομή

- Ανάπτυξη, συντήρηση και προστασία βάσεων δεδομένων
- Επεκτασιμότητα δικτύων και servers
- Προστασία υποδομής από φυσικές καταστροφές
- Δοκιμές καλής λειτουργίας μεμονωμένων στοιχείων
- 24ωρη παρακολούθηση δικτύων και συστημάτων
- Δοκιμές υπερφόρτωσης δικτύων
- Ανάπτυξη συστήματος έγκαιρης ειδοποίησης σε περιπτώσεις εκτάκτων αναγκών
- Επαναφορά / ανάνηψη από καταστροφή και καθορισμός διαδικασιών και ευθυνών για την αδιάκοπη λειτουργία της επιχείρησης (business continuity).
- Έλεγχος πληροφορικών συστημάτων και ασφάλεια διαδικασιών αναβάθμισης εφαρμογών ή εξοπλισμού (software και hardware).
- Έλεγχος εναρμόνισης με τις τεχνολογικές εξελίξεις, για την αποφυγή «απαρχαίωσης» των συστημάτων.
- Έλεγχος ποιότητας των υπηρεσιών που παρέχονται από τρίτα μέρη και αφορούν σε κρίσιμες λειτουργίες της επιχείρησης.

### 2) Ασφάλεια

- Συμμόρφωση με τα διεθνή πρότυπα ασφαλείας

- Εκτίμηση ετοιμότητας σε έξωθεν εισβολές (χακερ, ιούς, κτλ)
  - Εγκατάσταση, διαχείριση και επανεκτίμηση των υποδομών πιστοποίησης και εξουσιοδότησης για την πρόσβαση στα δίκτυα της επιχείρησης
  - Εκτίμηση και διαχείριση της φυσικής ασφάλειας
  - Διαχείριση δικαιωμάτων πρόσβασης του προσωπικού, βάσει ρόλων στην επιχείρηση
  - Συντήρηση του υπάρχοντος λειτουργικού συστήματος και συνεχή αναβάθμιση του
  - Εντοπισμός κρουσμάτων απάτης
  - Έλεγχος ασφαλείας των προμηθευτών ή άλλων τρίτων μερών που διαχειρίζονται τα στοιχεία των πελατών ή έχουν πρόσβαση σε αυτά
  - Ασφάλεια επικοινωνιών και πρόσβασης δικτύων από απόσταση (remote access)
  - Συνεχής αξιολόγηση της επίδρασης νέων υπηρεσιών e-banking στην ετοιμότητα της τράπεζας ως προς τη διαχείριση κρίσεων
  - Στόχος των μέτρων ασφαλείας πρέπει να είναι τόσο η πρόληψη (π.χ. η εκτίμηση, η διόρθωση και η ενίσχυση των λειτουργικών συστημάτων και του γενικότερου πλαισίου υποδομής της τράπεζας) όσο και η αποτελεσματική αντίδραση (π.χ. ο εντοπισμός, η αναφορά και η «κάταστολή» παραβιάσεων στο σύστημα ασφαλείας)
- 3) Προσωπικά Δεδομένα
- Παρεμπόδιση μη εξουσιοδοτημένης πρόσβασης στα προσωπικά και συναλλακτικά στοιχεία των πελατών, τα οποία τηρούνται σε ειδικές εφαρμογές και βάσεις δεδομένων
  - Διαχείριση των επιλογών των πελατών, που αφορούν στην κοινοποίηση ή μη των προσωπικών τους στοιχείων σε συνεργαζόμενες εταιρίες για λόγους προώθησης / marketing.
  - Διαχείριση στοιχείων πελατών τρίτων επιχειρήσεων, που συγκεντρώθηκαν κατόπιν συμφωνίας των ιδίων
  - Προστασία όλων των εσωτερικών και εξωτερικών επικοινωνιών που διεξάγονται μέσω internet
  - Εκούσια ή ακούσια κοινοποίηση εμπιστευτικών πληροφοριών εμπορικών συνεργατών
  - Συμμόρφωση προς τη διεθνή νομοθεσία σχετικά με τις on line συναλλαγές από χώρες του εξωτερικού
- 4) Επιχειρηματικές Διαδικασίες
- Διατήρηση της ακεραιότητας των online συναλλαγών και πληρωμών (συμπεριλαμβανομένων των ανολοκλήρωτων συναλλαγών και των συναλλαγών που πραγματοποιήθηκαν περισσότερες από μια φορές από λάθος του πελάτη)
  - Ικανότητα ολοκλήρωσης των συναλλαγών σε περιπτώσεις πτώσης του δικτύου ή άλλης βλάβης
  - Χρήση και διασύνδεση τρίτων μερών για την ασφαλή διαχείριση και ολοκλήρωση επιχειρηματικών διαδικασιών
  - Παρακολούθηση και διαχείριση του ηλεκτρονικού ταχυδρομείου και των επισυναπτόμενων αρχείων (e-mail attachments)

- Εντοπισμός και διαχείριση καίριων ηλεκτρονικών αρχείων
- 5) On line Υπηρεσίες
- Προστασία κατά των σφαλμάτων, διακοπών ή καθυστερήσεων στην παροχή υπηρεσιών με βάση το internet όπως:
- Διαθεσιμότητα λογισμικού ή άλλων αρχείων τα οποία οι χρήστες κατεβάζουν στον υπολογιστή τους από το δικτυακό τόπο της επιχείρησης
  - Διαθεσιμότητα του ιδίου του δικτυακού τόπου, τόσο των περιοχών που απευθύνονται στους καταναλωτές όσο και εκείνων στις οποίες έχουν πρόσβαση οι συνεργάτες της επιχείρησης
  - Διαθεσιμότητα του διαδικτύου για την αποστολή και λήψη e-mail
  - Παροχή τεχνικής υποστήριξης τόσο για την ίδια την επιχείρηση όσο και τους συνεργάτες της
  - Διαχείριση εσωτερικών και εξωτερικών Service Level Agreements (SLAs)
- 6) Διοίκηση
- Ευθυγράμμιση των δραστηριοτήτων e-banking με την γενικότερη στρατηγική της τράπεζας
  - Διαδικασίες προτυποποίησης και ελέγχου της εμπορικής δραστηριότητας μέσω διαδικτύου
  - Ετοιμότητα επικοινωνίας με τα Μέσα Ενημέρωσης
  - Αναγνώριση του συμβάντος / της κρίσης και άμεση απόκριση
  - Απόκριση και ανασυγκρότηση
  - Αυστηρά δομημένο σχέδιο αντίδρασης
  - Παρακολούθηση της επαγγελματικής συμπεριφοράς του προσωπικού, ώστε να εναρμονίζεται με τους κανονισμούς και τις διαδικασίες που διέπουν το e-banking
  - Εκπαίδευση μέρους του προσωπικού για την υποστήριξη αναγκών που σχετίζονται με τις νέες τεχνολογίες και το e-banking
  - Έλεγχος των σχέσεων συνεργασίας με τρίτα μέρη (ISP, ASP, παρόχους περιεχομένου κλπ)
  - Αποτελεσματική διαχείριση έργων (project management) και πρωτοβουλιών που σχετίζονται με το e-banking
  - Συνεχής ενημέρωση και εκπαίδευση σχετικά με το ηλεκτρονικό επιχειρηματικό ρίσκο (e-risk)
  - Ασφαλιστική κάλυψη των δραστηριοτήτων e-επιχειρείν (συμπεριλαμβανομένων των επαγγελματικών σφαλμάτων ή παραλείψεων και της αντιμετώπισης του ηλεκτρονικού εγκλήματος)
- 7) Περιεχόμενο
- Δημιουργία και διαχείριση πολυμεσικού περιεχομένου (multimedia)
  - Διαχείριση ηλεκτρονικών αρχείων περιεχομένου
  - Προστασία εταιρικής πνευματικής ιδιοκτησίας (με χρήση τεχνολογιών όπως η ψηφιακή υδατογράφηση, η κρυπτογράφηση κλπ, αλλά και με την προστασία των εταιρικών δικτύων)
  - Διαδικασίες για την αποτροπή της παράνομης χρήσης της πνευματικής ιδιοκτησίας τρίτων

- Διαδικασίες εντοπισμού και διαχείρισης σφαλμάτων στο περιεχόμενο του δικτυακού τόπου της επιχείρησης και λανθασμένων συνδέσμων / «σπασμένων» links
- 8) Διαχείριση Πληροφοριών
- Συγκέντρωση και αναφορά λειτουργικών στατιστικών στοιχείων σχετικά με την παρακολούθηση της απόδοσης και τις τάσεις της αγοράς
  - Παρακολούθηση συναλλαγών για τον εντοπισμό κρουσμάτων απάτης (π.χ. μη εξουσιοδοτημένη χρήση πιστωτικής κάρτας)

## ΕΠΙΤΡΟΠΗ ΤΗΣ ΒΑΣΙΛΕΙΑΣ

Η Επιτροπή της Βασιλείας για την Τραπεζική Εποπτεία ιδρύθηκε το 1974 στους κόλπους της Τράπεζας Διεθνών Κανονισμών με τη συμμετοχή 13 χωρών (Βέλγιο, Καναδάς, Γαλλία, Γερμανία, Ιταλία, Ιαπωνία, Λουξεμβούργο, Ολλανδία, Ισπανία, Σουηδία, Ελβετία, Ηνωμένο Βασίλειο και ΗΠΑ). Ο στόχος της ήταν και είναι να αποτελεί ένα forum διαλόγου και συνεργασίας σε θέματα τραπεζικής εποπτείας. Η Επιτροπή προσδοκά ότι οι επιμέρους εποπτικές αρχές θα λάβουν μέτρα μέσω θεσμικών ή άλλων προσαρμογών, οι οποίες ενδείκνυται για τα εθνικά τους συστήματα, για τα ευρέα εποπτικά πρότυπα και κατευθύνσεις που διατυπώνει και για τις βέλτιστες πρακτικές που προτείνει. Δεν έχει τη μορφή υπερεθνικής εποπτικής αρχής και τα συμπεράσματά της δεν έχουν, ούτε υπήρχε ποτέ η προϋπόθεση να έχουν, δεσμευτική νομική ισχύ.

### Βασιλεία I

Η Επιτροπή της Βασιλείας εξέδωσε το 1988, με το όνομα Βασιλεία I, ένα σύνολο κανόνων για την εφαρμογή ενός πλαισίου μέτρησης του πιστωτικού κινδύνου των εντός και εκτός ισολογισμού στοιχείων του ενεργητικού, θέτοντας ταυτόχρονα ένα ελάχιστο όριο απαιτούμενων εποπτικών κεφαλαίων ίσο με 8% του σταθμισμένου ενεργητικού. Η αρχική Συμφωνία της Βασιλείας, τον Ιανουάριο 1996, συμπληρώθηκε με την ενσωμάτωση των κινδύνων αγοράς και εμπλουτίστηκε περαιτέρω με την εισαγωγή εναλλακτικών μεθόδων μέτρησης των εν λόγω κινδύνων.

Τα αποτελέσματα από την εφαρμογή της Βασιλείας I ήταν:

- Υψηλότερες αποδόσεις με ίδια κεφαλαιακή απαίτηση από
  - A) την αναζήτηση εταιρικού χρέους χαμηλής πιστωτικής ποιότητας και
  - B) την παροχή δανείων προς χαμηλής πιστωτικής ποιότητας πιστωτικών ιδρυμάτων
- Αποφυγή κεφαλαιακών απαιτήσεων μέσω της ταχύτατης ραγδαίας ανάπτυξης πιστωτικών παραγωγών
- Στροφή των πιστωτικών ιδρυμάτων στην αγορά στεγαστικών δανείων.

Το 1999 η Επιτροπή, λαμβάνοντας υπ' όψιν τις ευρύτατες διακυμάνσεις που παρατηρήθηκαν στις αγορές χρήματος, κεφαλαίων και συναλλάγματος, ξεκίνησε μια σειρά διαβουλεύσεων με τους φορείς της αγοράς και την αναθεώρηση της Βασιλείας I. Τα τρία Συμβουλευτικά Κείμενα (το πρώτο τον Ιούνιο 1999, το δεύτερο τον Ιανουάριο 2001, το τρίτο τον Απρίλιο 2003), οι τέσσερις Ποσοτικές Μελέτες των επιπτώσεων (Quantitative Impact Studies), καθώς και οι δημοσιευμένες μελέτες των συναφών εξειδικευμένων ομάδων εργασίας, αποτελούν το νέο



Σύμφωνο για την κεφαλαιακή επάρκεια, το οποίο έχει επιφέρει μεγάλες αλλαγές στο εποπτικό πλαίσιο και αποτελεί πραγματική πρόκληση για εποπτεία και τράπεζες.

Το νέο Σύμφωνο (Βασιλεία II), το οποίο καταργεί σχεδόν εξ ολοκλήρου το Σύμφωνο του 1988, επιφέρει ριζικές αλλαγές στο πλαίσιο διαχείρισης κινδύνων και υπολογισμού των κεφαλαιακών απαιτήσεων.

## **Βασιλεία II**

Η Συνθήκη της Βασιλείας II αποτελεί δέσμη μέτρων που έχουν ως στόχο:

- Θέτουν τις βάσεις για επανασχεδιασμό του τρόπου υπολογισμού της κεφαλαιακής επάρκειας των χρηματοπιστωτικών εταιρειών- αύξηση μετοχικού κεφαλαίου
- Ενισχύουν την ασφάλεια του τραπεζικού συστήματος και
- Οδηγούν στη λήψη ορθολογικότερων αποφάσεων σε ένα περιβάλλον εντεινόμενου ανταγωνισμού και αυξανόμενης εποπτείας.

Η νέα Συνθήκη χωρίζεται σε τρεις πυλώνες (ενότητες):

**Πρώτος Πυλώνας:** Εναλλακτικές μεθοδολογίες υπολογισμού της κεφαλαιακής επάρκειας των τραπεζών για κάλυψη του πιστωτικού και λειτουργικού κινδύνου.

**Δεύτερος Πυλώνας:** Παρακολούθηση της κεφαλαιακής επάρκειας των τραπεζών και των εφαρμοζόμενων μεθόδων εκ μέρους των εποπτικών αρχών, και

**Τρίτος Πυλώνας:** Πειθαρχία της αγοράς μέσω της δημοσιοποίησης στοιχείων σχετικά με τη διάρθρωση των αναλαμβανόμενων κινδύνων και της κεφαλαιακής επάρκειας των πιστωτικών ιδρυμάτων.

## **Ομάδα Ηλεκτρονικής Τραπεζικής της Επιτροπής Εποπτείας τραπεζών της Βασιλείας**

Η ομάδα Ηλεκτρονικής Τραπεζικής της επιτροπής εποπτείας τραπεζών της Βασιλείας δημοσίευσε το 2003, 14 βασικές αρχές διαχείρισης κινδύνων για το e-banking οι οποίες χωρίζονται σε τρεις βασικές κατηγορίες.

A) Ενέργειες Διοίκησης (αρχές 1-3)

1. Αποτελεσματική διαχείριση παραδρομών και απροσεξιών στις ηλεκτρονικές δραστηριότητες.
2. Εδραίωση μιας κατανοητής διαδικασίας ελέγχου ασφαλείας.
3. Κατανοητή διαδικασία τόσο για την διοίκηση, όσο και για το προσωπικό για τις σχέσεις με εξωτερικούς συνεργάτες και τις εξαρτήσεις από τρίτα μέρη.

B) Έλεγχοι Ασφαλείας (αρχές 4-10)

4. Πιστοποίηση των χρηστών του e-banking
5. Μη άρνηση συμμόρφωσης (non-repudiation) και ευθύνη για της συναλλαγές του e-banking
6. Κατάλληλα μέτρα για την διασφάλιση του διαχωρισμού των καθηκόντων
7. Κατάλληλοι μηχανισμοί πρόσβασης σε συστήματα e-banking, βάσεις δεδομένων και εφαρμογές

8. Ακεραιότητες δεδομένων ηλεκτρονικών συναλλαγών, εγγράφων και πληροφορίας
9. Εδραίωση ξεκάθαρων διαδικασιών ελέγχου των συναλλαγών του e-banking
10. Εμπιστευτικότητα της τραπεζικής πληροφορίας

Γ) Διαχείριση Νομικών Κινδύνων και Κινδύνων φήμης (αρχές 11-14)

11. Κατάλληλες γνωστοποιήσεις (disclosures) των υπηρεσιών e-banking
12. Ιδιωτικότητα της πληροφορίας πελάτη
13. Χωρητικότητα, αδιάλειπτη λειτουργία και σχέδια ανάνηψης ώστε να διασφαλίζεται η διαθεσιμότητα των συστημάτων και υπηρεσιών του e-banking
14. Σχέδιο αντιμετώπισης συμβάντων.

## **ΚΕΦΑΛΑΙΟ 5ο**

### **ΝΟΜΙΚΑ ΖΗΤΗΜΑΤΑ - ΤΡΑΠΕΖΙΚΗ ΝΟΜΟΘΕΣΙΑ**

#### **και ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ για Internet Banking**

#### **ΝΟΜΙΚΑ ΘΕΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΤΡΑΠΕΖΙΚΗΣ**

Η υπαγωγή του internet banking στις ειδικές ρυθμίσεις για τις ηλεκτρονικές πληρωμές, πέραν των γενικών ρυθμίσεων για την διεξαγωγή τραπεζικών συναλλαγών, δεν οριοθετεί πλήρως το ζήτημα της νομικής κάλυψης του e-banking. Η παγκόσμια διάσταση του internet επιβάλλει οποιαδήποτε εμπορική και επιχειρηματική δραστηριότητα σε αυτό να εξετάζεται υπό το πρίσμα της διεθνούς δραστηριότητας του και συνεπώς πρέπει να εξετάζεται το ρυθμιστικό πλαίσιο της διασυνοριακής παροχής τραπεζικών και χρηματοοικονομικών υπηρεσιών.

Κύριοι κλάδοι του δικαίου που διέπουν το internet banking είναι:

- Η νομοθεσία για τη διεξαγωγή τραπεζικών και χρηματοοικονομικών συναλλαγών και την τραπεζική εποπτεία
- Η νομοθεσία για την προστασία του καταναλωτή και
- Η νομοθεσία για την προστασία προσωπικών δεδομένων.

#### **ΤΡΑΠΕΖΙΚΗ ΝΟΜΟΘΕΣΙΑ INTERNET BANKING**

Όπως όλες οι τραπεζικές υπηρεσίες έτσι και το internet banking, ως παροχή τραπεζικών υπηρεσιών ιδίως προς καταναλωτές, υπάγεται στην εποπτεία των Κεντρικών Τραπεζών και τις σχετικές οδηγίες της ΕΕ για τα πιστωτικά ιδρύματα. Επομένως ισχύει η νομοθεσία για τα χρηματοδοτικά και πιστωτικά ιδρύματα που συνοψίζεται :

- I. Στην εποπτεία της Κεντρικής Τράπεζας
- II. Στις διατάξεις για τον περιορισμό του σκοπού και των ποσοστών συμμετοχής φυσικών ή νομικών προσώπων σε πιστωτικά ιδρύματα ή της συμμετοχής των πιστωτικών ιδρυμάτων σε άλλες επιχειρήσεις και
- III. Στις ειδικές διατάξεις για την δημοσιοποίηση των οικονομικών αποτελεσμάτων

Οι ηλεκτρονικά παρεχόμενες υπηρεσίες διέπονται από την Οδηγία 2000/31 που καθορίζει το γενικό πλαίσιο για εν γένει το ηλεκτρονικό εμπόριο.

Στο πλαίσιο της γενικής τραπεζικής νομοθεσίας, που διέπει και το e-banking, η Τράπεζα της Ελλάδος είναι αρμόδια για την εφαρμογή από τα πιστωτικά ιδρύματα και των διατάξεων του Ν.2331/95, που αφορά και την πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες.

#### **ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ INTERNET BANKING**

Το θεσμικό πλαίσιο πληρωμών, που μπορεί να χρησιμοποιηθεί και στο internet banking, ορίζεται από την Οδηγία 98/26, με την οποία έχει ήδη προσαρμοστεί το ελληνικό δίκαιο με το Ν2789/2000. Το θεσμικό πλαίσιο για τις διασυνοριακές πληρωμές καθορίζεται επιπλέον από

την οδηγία 97/5 για τις διασυνοριακές μεταφορές πιστώσεων μέχρι 50.000€. Σύμφωνα με την οδηγία αυτή :

- I. Για την εκτέλεση της εντολής ευθύνεται η τράπεζα του εντολέα
- II. Θεσπίζεται υποχρέωση για αναλυτική πληροφόρηση των πελατών πριν και μετά από την εκτέλεση της εντολής
- III. Η εντολή πρέπει να διεκπεραιωθεί εντός 5 εργάσιμων ημερών
- IV. Προβλέπονται ειδικές δεσμεύσεις για τις προμήθειες και τα έξοδα
- V. Προβλέπεται ειδική αποζημίωση σε περίπτωση μη εκπλήρωσης

Το θεσμικό πλαίσιο συμπληρώνεται από τον κανονισμό 2560/2001 σχετικά με τις διασυνοριακές πληρωμές σε €, που διασφαλίζει τη διαφάνεια των εξόδων που επιβάλλονται και ευθυγραμμίζει το ύψος τους κατά τις συναλλαγές εντός ΕΕ.

Στην Ελλάδα ρητή αναφορά στο internet banking υπάρχει στην πράξη Συμβουλίου Νομισματικής Πολιτικής 50/13.7.2002 : «καθορισμός πλαισίου επίβλεψης συστημάτων πληρωμών», στην οποία προβλέπεται άσκηση επίβλεψης από την Τράπεζα της Ελλάδος και στους τρόπους πρόσβασης και στα υποστηρικτικά προϊόντα των συστημάτων πληρωμής.

Για τη διεξαγωγή ασφαλών συναλλαγών μέσω internet banking η ελληνική νομοθεσία συμπληρώνεται από το ΠΔ 150/01 για της ηλεκτρονικές υπογραφές, που εναρμόνισε την ελληνική νομοθεσία με την οδηγία 99/93. Για την περίπτωση διεξαγωγής συναλλαγών με ίδρυμα ηλεκτρονικού χρήματος ισχύει ο Ν.3148/2003.

## **ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΚΑΤΑΝΑΛΩΤΗ INTERNET BANKING**

Τα καταστήματα e-banking πρέπει να συμμορφώνονται με τον Ν.2251/94 περί προστασίας του καταναλωτή. Ειδικά για το e-banking, κατευθυντήριες γραμμές δίνει το άρθρο 4 του παραπάνω νόμου που ενσωματώνει την οδηγία 97/7 για της εξ αποστάσεως συμβάσεις.

Επιγραμματικά η διάταξη θεσπίζει:

- I. Ακυρότητα υπέρ του καταναλωτή
- II. Υποχρέωση για ανακοίνωση της ταυτότητας της επιχείρησης και για λεπτομερή περιγραφή των χαρακτηριστικών, της τιμής και του κόστους του προσφερομένου αγαθού
- III. Υποχρέωση περιγραφής του δικαιώματος υπαναχώρησης του καταναλωτή
- IV. Υποχρέωση περιγραφής της διάρκειας τυχόν προσφορών και της διάρκειας σύμβασης.

Ειδικά για την παροχή χρηματοοικονομικών υπηρεσιών ισχύει πλέον η οδηγία 2002/65 «σχετικά με την εξ αποστάσεως εμπορία χρηματοοικονομικών υπηρεσιών προς τους καταναλωτές», η οποία αποδίδει την ιδιότητα του καταναλωτή σε «κάθε πρόσωπο το οποίο, στο πλαίσιο των συμβάσεων εξ αποστάσεως ενεργεί για σκοπούς εκτός πεδίου εμπορικής ή επαγγελματικής του δραστηριότητας»

Η οδηγία επιγραμματικά προβλέπει:

- I. Υποχρέωση για λεπτομερή πληροφόρηση του καταναλωτή πριν και μετά από την κατάρτιση της σύμβασης, για την υπηρεσία, τη σύμβαση και τα μέτρα αποκατάστασης
- II. Υποχρέωση για ανακοίνωση των συμβατικών όρων σε χαρτί ή άλλο σταθερό μέσο
- III. Δικαίωμα υπαναχώρησης εντός 14 ημερών εκτός από

- a. Τις υπηρεσίες με διακυμάνσεις τιμών (π.χ. συνάλλαγμα, futures, swaps, options)
  - b. Τις βραχυπρόθεσμες συμβάσεις (π.χ. ασφαλιστήρια για ταξίδια)
  - c. Τις συμβάσεις, η εκτέλεση των οποίων ολοκληρώθηκε
  - d. Τις συμβάσεις ασφαλίσεων ζωής για τις οποίες προβλέπεται δικαίωμα υπαναχώρησης εντός 30 ημερών (σύμφωνα με την οδηγία 90/619)
- IV. Δυνατότητα ακύρωσης των συναλλαγών με πιστωτική κάρτα
- V. Πρόβλεψη μέτρων για τις μη αιτηθείσες υπηρεσίες και την αυτόκλητη επικοινωνία (π.χ. με ανεπιθύμητα ηλεκτρονικά μηνύματα)

Οι διατάξεις της οδηγίας έχουν αναγκαστικό χαρακτήρα, ώστε να αποκλείεται συμβατική παραίτηση από τα παρεχόμενα δικαιώματα.

Εξ αιτίας των ανωτέρω οι τράπεζες θα πρέπει να περιλαμβάνουν τους όρους της σύμβασης στα ηλεκτρονικά τους καταστήματα είτε στην αρχική τους σελίδα είτε μέσω link σε άλλη σελίδα. Η απεικόνιση απευθείας ή κατά παραπομπή μέσω link σε άλλη σελίδα των όρων, πρέπει να υπάρχει και όταν χρησιμοποιείται server τρίτου ή αν ο τρίτος διαθέτει links προς την ιστοσελίδα της τράπεζας.

## **ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΚΑΤΑΣΤΗΜΑΤΑ E-BANKING**

Τα ηλεκτρονικά καταστήματα των τραπεζών πρέπει να συμμορφώνονται με τους κανόνες προστασίας δεδομένων προσωπικού χαρακτήρα. Για την ασφάλεια των προσωπικών δεδομένων που ισχύουν οι Ν.2472/97 (προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα), Ν.2772/99 (προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα) και η οδηγία 2002/58 για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

Ιδιαίτερη σημασία για το internet banking αποκτά η απαγόρευση να διαβιβάζονται δεδομένα σε τρίτες χώρες εκτός ΕΕ, που δεν παρέχουν ικανοποιητικό επίπεδο προστασίας. Η διαβίβαση προς χώρες εκτός ΕΕ επιτρέπεται μόνο έπειτα από άδεια της Αρχής Προστασίας Προσωπικού Χαρακτήρα, η οποία χορηγείται μόνο αν η Αρχή κρίνει ότι το παρεχόμενο επίπεδο προστασίας στην Τρίτη χώρα είναι ικανοποιητικό. Το πρόβλημα είναι σοβαρό αφού στο internet κάθε μετάδοση δεδομένων είναι διασυνοριακή, ενώ ακόμη και στη μετάδοση εντός των «κοινοτικών» συνόρων είναι πιθανό τα δεδομένα να διέλθουν σε τρίτες χώρες.

Στις περισσότερες περιπτώσεις η διαβίβαση δεδομένων κατά την διεξαγωγή internet banking μπορεί να πραγματοποιηθεί καλυπτόμενη των εξαιρέσεων των περιπτώσεων (β) και (γ) της παραγράφου 1 του άρθρου 26 της οδηγίας 95/46, δηλαδή:

- I. Όταν η διαβίβαση είναι αναγκαία για την εκτέλεση σύμβασης μεταξύ του προσώπου το οποίο αφορούν τα δεδομένα και του υπεύθυνου επεξεργασίας
- II. Όταν η διαβίβαση είναι αναγκαία για την συνομολόγηση σύμβασης μεταξύ των ιδίων προσώπων

Σύμφωνα με αυτές τις εξαιρέσεις, η διαβίβαση μπορεί να πραγματοποιηθεί κατά παρέκκλιση και προς Τρίτη χώρα που δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας.

## Κεφάλαιο 6ο

### ΑΣΦΑΛΕΙΑ του E-Banking

#### ΕΙΣΑΓΩΓΗ ΣΕ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ E-BANKING

Οι τράπεζες φαίνεται να είναι λιγότερο ευάλωτες στις on line συναλλαγές από ότι οι χρηματοπιστηριακές εταιρείες και οι εταιρείες ηλεκτρονικού εμπορίου αγαθών και υπηρεσιών. Και αυτό διότι στη σχέση του πελάτη με την τράπεζα υπάρχει ένα πρόσθετο στοιχείο, αυτό της εμπιστοσύνης, και, όπως έχει αποδειχθεί, οι πελάτες των τραπεζών είναι εξαιρετικά συντηρητικοί. Αυτό φαίνεται και από την προτίμηση των πελατών στο γκισέ σε σχέση με τις Αυτόματες Ταμειολογιστικές Μηχανές. Τραπεζικές υπηρεσίες, όπως το phone banking, δεν είχαν τα αναμενόμενα αποτελέσματα. Πολύ περισσότερο οι θεωρίες υπέρ της καταργήσεως του τραπεζικού καταστήματος αποδεικνύουν σήμερα ότι είχαν έντονο το στοιχείο της υπερβολής.

Στο ηλεκτρονικό εμπόριο και στην ηλεκτρονική τραπεζική, επειδή απουσιάζει η φυσική επαφή με πρόσωπα εμπιστοσύνης, υπάρχει ανάγκη καθιέρωσης μηχανισμών που μέσω αυτών θα είναι δυνατόν να αποδεικνύεται ότι το πρόσωπο, με το οποίο πραγματοποιείται η συναλλαγή ηλεκτρονικά, είναι όντως το δηλούμενο στη συναλλαγή πρόσωπο. Σε κάθε περίπτωση απαιτείται η ύπαρξη ενός Οργανισμού Πιστοποίησης ή αλλιώς μιας Έμπιστης Τρίτης Οντότητας με σκοπό την επικύρωση της αυθεντικότητας της ταυτότητας του ατόμου ή της επιχείρησης και την τήρηση στοιχείων για την πραγματοποιηθείσα οικονομική πράξη.

Ο μηχανισμός αυτός περιλαμβάνει ψηφιακά πιστοποιητικά (digital certificates) και συστήματα μη άρνησης αποδοχής (non repudiation systems). Ο ρόλος των Έμπιστων Τρίτων Οντοτήτων θα εξυπηρετήσει και το business-to-customer συναλλαγές. Αν κάποια εταιρεία αγοράζει από μια άλλη για την οποία δεν γνωρίζει κρίσιμα στοιχεία της και ευρίσκεται κάπου στο εξωτερικό, η δυνατότητα της τράπεζας για πιστοποίηση είναι κρίσιμη. Αποτελεί μάλιστα καλή ευκαιρία για τις τράπεζες να επεκτείνουν το ρόλο τους σε μια μορφή Trade financing, αφού έχουν λόγω των συναλλαγών με επιχειρήσεις μεγάλη πείρα π.χ. στις εγγυητικές επιστολές.

Οι ηλεκτρονικές επιθέσεις στα μηχανογραφικά συστήματα των τραπεζών και των επιχειρήσεων εγκυμονούν πολλούς κινδύνους, καταστροφές hardware, software, καθυστερήσεις, ματαιώσεις συναλλαγών, χρηματικά κόστη, διάψευση προσδοκιών, κακή φήμη. Ο μόνος τρόπος αντιμετώπισης των κινδύνων είναι η συνεχής εκπαίδευση των υπευθύνων ασφαλείας των συστημάτων των επιχειρήσεων και η συνεχής τεχνολογική βελτίωση των συστημάτων ασφαλείας. Η διαδικασία αυτή ομοιάζει με μια «κούρσα» εξοπλισμού και εκπαίδευσης μεταξύ των αντιπάλων στο χρόνο. Δεν πρέπει να λησμονείται ότι το διαδίκτυο δημιουργήθηκε και υπάρχει με τη διασύνδεση συστημάτων Η/Υ και δεν εγγυάται την ασφάλεια αυτών.

Ένα σύστημα υλοποίησης συναλλαγών θεωρείται ασφαλές όταν:

- A) Λειτουργεί απρόσκοπτα, δηλαδή εκτός προγραμματισμένων διακοπών λειτουργίας.
- B) Διασφαλίζει το ότι δεν έχει κάποιος τη δυνατότητα ανάγνωσης των αποστέλλομενων στους συναλλασσόμενους μηνυμάτων (privacy).
- Γ) Παρέχει σε κάθε συναλλασσόμενο κάποιο μέσο εξακρίβωσης της ταυτότητας της οντότητας, με την οποία συναλλάσσεται (authentication).
- Δ) Διασφαλίζει το αναλλοίωτο των μηνυμάτων των συναλλασσομένων (integrity).

Ε) Διασφαλίζει σε κάθε συναλλασσόμενο το ότι η οντότητα με την οποία συναλλάσσεται δεν θα αρνηθεί ότι έγινε μεταξύ τους συναλλαγή (non-repudiation).

Το πρώτο και σημαντικότερο βήμα για την καθιέρωση πολιτικής ασφάλειας συστημάτων είναι η ανάλυση κινδύνου πριν από την εκδήλωση οποιαδήποτε ηλεκτρονικής επίθεσης. Τα σημαντικότερα ερωτήματα, τα οποία πρέπει να απαντηθούν στο στάδιο της ανάλυσης του κινδύνου είναι:

- Ποιοί πόροι πρέπει να προστατευθούν και από ποιόν;
- Ποιό είναι το κόστος μιας πιθανής παραβίασης;
- Ποιό είναι το κόστος της ασφάλειας;
- Ποια είναι η πιθανότητα παραβίασης;

Τα τρία τελευταία ερωτήματα θα πρέπει να εξετασθούν για κάθε πόρο, αλλά και για το σύστημα συνολικά. Έχοντας αυτά τα δεδομένα μπορεί να υπολογισθεί η συνολική πιθανότητα παραβίασης του συστήματος, καθώς και ο λόγος του επιχειρηματικού κόστους παραβίασης προς το κόστος ασφάλειας. Στο στάδιο της ανάλυσης κινδύνου, θεωρείται ίσως απαραίτητη η εμπλοκή μιας εταιρείας συμβούλων με εμπειρία στο αντικείμενο.

Μερικά από τα χαρακτηριστικά μιας σωστής πολιτικής ασφάλειας είναι:

- A) Να σχεδιάζεται σύμφωνα με την πραγματικότητα της καθημερινής λειτουργίας της επιχείρησης, καθώς επίσης και με τη γενικότερη κατεύθυνση της στρατηγικής της.
- B) Να είναι εύκολα κατανοητή και προσβάσιμη από τους υπαλλήλους της επιχείρησης.
- Γ) Να «διαφημίζεται» αρκετά μέσα στην επιχείρηση.
- Δ) Να μην είναι πολύ μακροσκελής
- Ε) Να μην είναι εύκολα αναγνωρίσιμο από τους υπαλλήλους ποιο τμήμα τους αφορά
- Στ) Να είναι αρκετά συγκεκριμένη αντιμετωπίζοντας τις πραγματικές αιτίες και όχι τα συμπτώματα
- Ζ) Να αναβαθμίζεται συχνά και να παρακολουθεί τις τεχνολογικές εξελίξεις.

Η επίτευξη αυτού του στόχου προϋποθέτει εκπαιδευμένο προσωπικό με συγκεκριμένα κίνητρα για την πίστη εφαρμογή της πολιτικής ασφάλειας, καθώς και χρήση των απαραίτητων εργαλείων υλοποίησης της. Κατ' αυτόν τον τρόπο, η πιστή εφαρμογή μιας σωστής πολιτικής ασφάλειας θα μπορούσε να αποτρέψει ακούσια εγκατάσταση προγραμμάτων ή υπερφόρτωση του mail server.

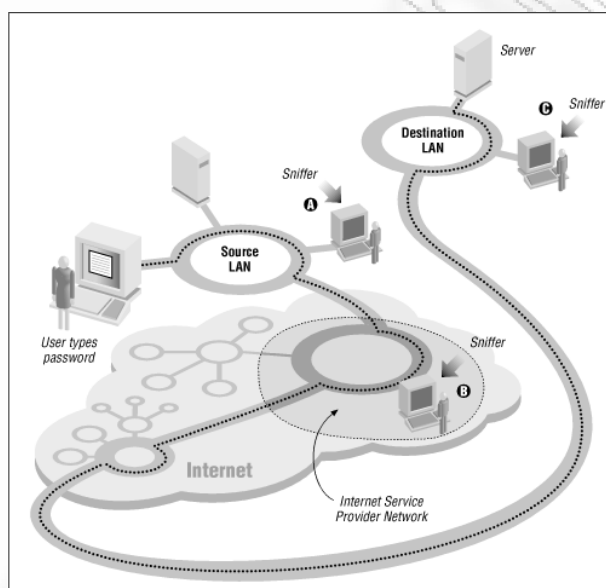
Τα κύρια εργαλεία ασφάλειας είναι τα ψηφιακά πιστοποιητικά, η ψηφιακή υπογραφή, η κρυπτογράφηση, τα SLL, οι κωδικοί πρόσβασης και οι smart cards.

## ΚΙΝΔΥΝΟΙ ΚΑΙ ΑΠΕΙΛΕΣ ΤΟΥ E-BANKING

Παρακάτω θα περιγράψουμε όσο είναι δυνατό τους βασικούς ηλεκτρονικούς κινδύνους και τις απειλές που αντιμετωπίζουν όλα τα ηλεκτρονικά τραπεζικά συστήματα

### 1.SNIFFERS

Ένας sniffer είναι ένα πρόγραμμα ή μια συσκευή που παρακολουθεί κρυφά την κίνηση ενός δικτύου με σκοπό αν υποκλέψει την πληροφορία που διακινείται μέσα από αυτό. Είναι τεχνολογία χαμηλού επιπέδου και εκμεταλλεύεται εγγενής αδυναμίες της αρχιτεκτονικής του δικτύου ETHERNET όπου επάνω σε αυτό στηρίζεται το Internet για την ανταλλαγή των μηνυμάτων από υπολογιστή σε υπολογιστή.



Πώς λειτουργεί ένας Sniffer:

Ένας υπολογιστής συνδεδεμένος σε ένα δίκτυο (τοπικό ή στο internet), έχει 2 αναγνωριστικά για να ξεχωρίζει και να αναγνωρίζεται από τους υπόλοιπους.

A) Έχει την MAC Address η οποία και είναι τυποποιημένη στην κάρτα δικτύου του υπολογιστή και δεν μπορεί να αλλαχθεί διότι είναι ένα ολοκληρωμένο κύκλωμα επάνω στην κάρτα και η οποία είναι μια και μοναδική για κάθε κάρτα. Η MAC είναι διεύθυνση χαμηλού επιπέδου.

B) Η IP η οποία χρησιμοποιείται από τις εφαρμογές και είναι υψηλού επιπέδου, η οποία δίνεται από το δίκτυο στον υπολογιστή και μπορεί να αλλάζει ανά πάσα στιγμή.

Στο επίπεδο σύνδεσης των δεδομένων (data link layer) του πρωτοκόλλου αλλά και της αρχιτεκτονικής των δικτύων Ethernet, η διασύνδεση των υπολογιστών γίνεται με την χρήση



τόσο των MAC Addresses όσο και των IP Addresses. Το αμέσως επόμενο επίπεδο του Ethernet το επίπεδο δικτύου (network layer) είναι υπεύθυνο για τις αντιστοιχίσεις των MAC με τις IP Addresses.

Σε αυτό το επίπεδο δρα ένας sniffer οποίος επαναπροσδιορίζει την αρχική συσχέτιση των διευθύνσεων και αναμεταδίδει τα δεδομένα ή αντικαθιστά τις διευθύνσεις ώστε να προσποιείται ότι είναι άλλος δίχως το δίκτυο να έχει την δυνατότητα να πιστοποιήσει αν ένας από υπολογιστές που είναι συνδεδεμένοι σε αυτό δεν είναι αυτοί που «λένε» πως είναι.

Υπάρχουν πολλοί τύποι sniffer για όλες σχεδόν τις αρχιτεκτονικές Ethernet που υπάρχουν και λειτουργούν όλοι με παρόμοιο τρόπο.

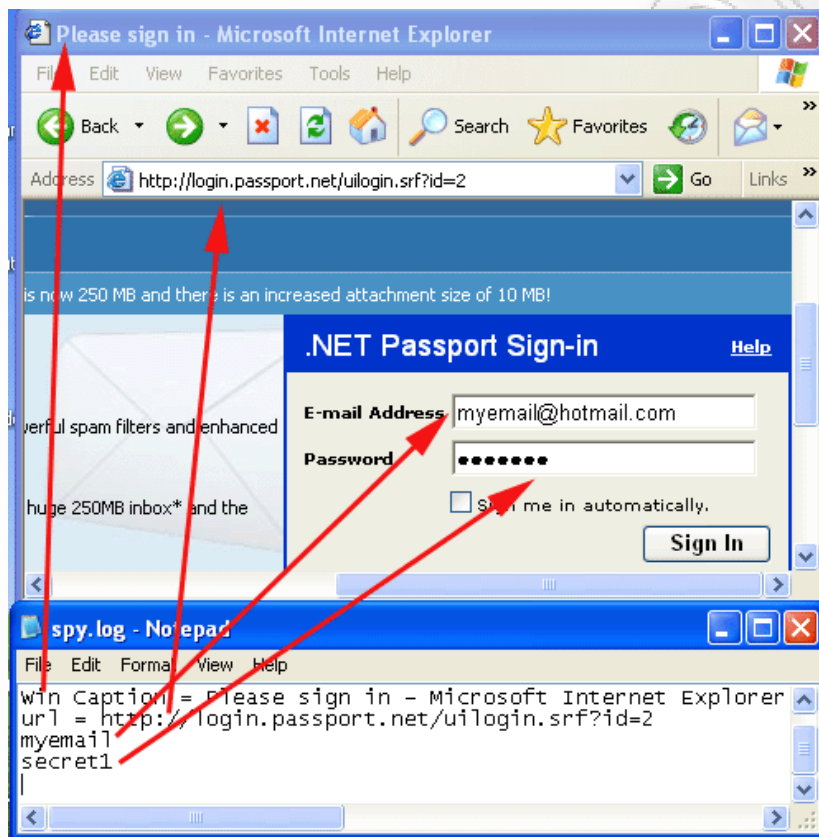
## 2. KEY LOGGERS

Το key logging (ή καταγραφή πληκτρολογήσεων στα ελληνικά), συμβαίνει όταν καταγράφονται οι πληκτρολογήσεις του χρήστη, χωρίς ο ίδιος να το ξέρει. Το key logging είναι κίνδυνος για την ασφάλεια των ηλεκτρονικών συναλλαγών διότι μπορούν να καταγραφούν κωδικοί πιστωτικών καρτών ή κωδικοί εισόδου στις ηλεκτρονικές τράπεζες και να χαθούν τεράστια ποσά χωρίς να μπορεί ο πελάτης να αποδείξει ότι δεν έχει πραγματοποιήσει αυτός τις συναλλαγές διότι όλοι οι κωδικοί εισόδου είναι σωστοί και είναι οι δικό του.

Η καταγραφή και αποθήκευση των πληκτρολογήσεων του θύματος πραγματοποιείται από ειδικό hardware, το οποίο είναι εύκολο να εγκατασταθεί και ταυτόχρονα δύσκολο να εντοπισθεί διότι δεν προκαλεί καμία παρεμβολή ή αλλοίωση στις όποιες συναλλαγές, απλώς καταγράφει ποιους και με ποια σειρά έχουν πληκτρολογηθεί οι χαρακτήρες.



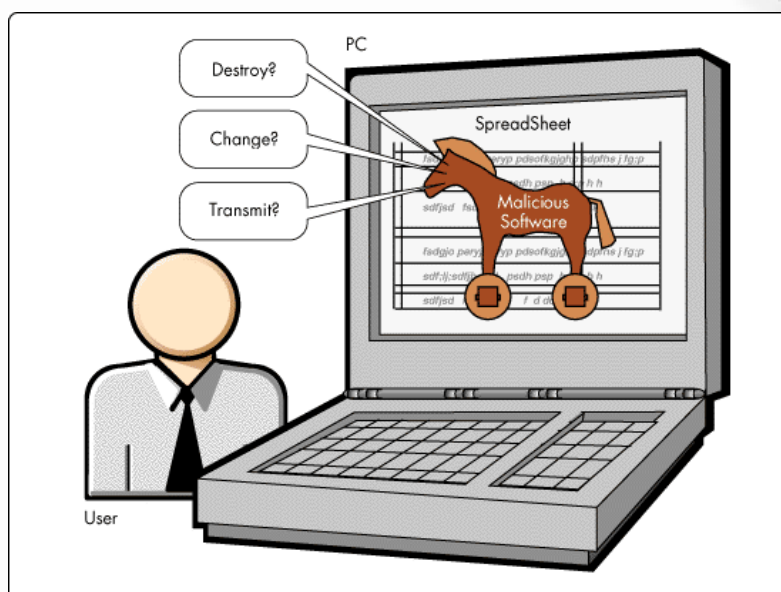
Η λειτουργία αυτή μπορεί να γίνει και από λογισμικό το οποίο όμως είναι πιο εύκολο να εντοπισθεί διότι αν και δεν παρεμβάλλεται σε καμία διαδικασία ένα έστω και απλό σύστημα μπορεί να εντοπίσει αν παράλληλα με τις υπόλοιπες διεργασίες εκτελείται και μία η οποία δεν θα έπρεπε να υπάρχει.



Τα key loggers καταγράφουν και αποστέλλουν σε προκαθορισμένους παραλήπτες τις καταγραφές αυτές και στη συνέχεια με την χρήση κατάλληλων αλγορίθμων μπορούν να εντοπιστούν οι κωδικοί των θυμάτων και να χρησιμοποιηθούν κακόβουλα.

### 3. TROJAN HORSE

Τα Trojan Horses (ή Δούρειοι Ίπποι) είναι ένα φαινομενικά χρήσιμο πρόγραμμα για τον υπολογιστή που έχει «καμουφλάρει» εντολές, οι οποίες όταν εκτελεστούν δημιουργούν αρνητικές δράσεις και είτε μπορούν να υποκλέψουν στοιχεία ή αρχεία ή οτιδήποτε θέλει ο δημιουργός τους.



Πολλά προγράμματα **Key Loggers** είναι **Trojan Horses**.

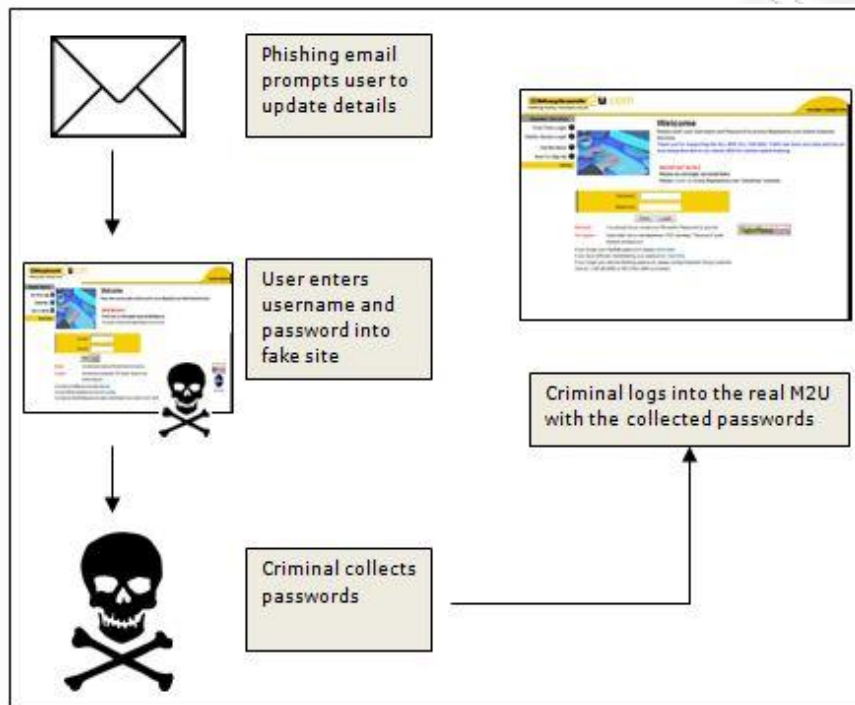
#### 4.PHISHING

Το phishing είναι η αποστολή email σε χρήστη, προσποιούμενο ότι προέρχεται από μια νόμιμη επιχείρηση, συνήθως τράπεζα, με σκοπό να εξαπατήσει τον χρήστη και αν πάρει ιδιωτικές πληροφορίες που θα χρησιμοποιηθούν για κλοπή της ταυτότητας του και είσοδος αντι αυτού στην πραγματική σελίδα της τράπεζας. Το email προτείνει στον χρήστη να επισκευθεί ένα web site όπου ζητούνται να ενημερώσει τις προσωπικές του πληροφορίες, όπως passwords και αριθμούς πιστωτικών καρτών κτλ. Που υποτίθεται πως η εταιρεία έχει είδη στην κατοχή της. Το web site ωστόσο είναι πλαστό και έχει δημιουργηθεί με μοναδικό σκοπό να κλέψει την ζητούμενη πληροφορία.

Οι επιθέσεις Phishing αυξάνονται ραγδαία και με έξυπνο τρόπο. Σύμφωνα με έρευνες ο ρυθμός εξάπλωσης τους διπλασιάζεται ανα εξάμηνο.

Το phishing είναι εξαιρετικά αποτελεσματικό, γιατί όπως έδειξε έρευνα της εταιρείας Infosury:

- 44% των χρηστών του e-banking χρησιμοποιούν τους ίδιους κωδικούς για όλες τις ηλεκτρονικές τράπεζες που συναλλάσσονται.
- 37% των χρηστών του e-banking χρησιμοποιούν τους ίδιους ακριβώς κωδικούς και σε λιγότερο ασφαλή site.
- 79% των χρηστών ελέγχουν αν υπάρχει η «κλειδαριά» ασφαλείας στο κάτω μέρος μιας ασφαλούς σελίδας, αλλά μόνο το 40% αυτών πατάει απάνω της να δει τις λεπτομέρειες του πιστοποιητικού. Το εικονίδιο μπορεί πάρα πολύ εύκολα να αντιγραφεί.
- 70% των χρηστών έχουν μικρές πιθανότητες να απαντήσουν σε ένα Mail από την τράπεζα τους και οι περισσότεροι από τους μισούς έχουν μικρές πιθανότητες να εγγραφούν ή να συνεχίσουν να χρησιμοποιήσουν τις on line υπηρεσίες εξαιτίας του phishing.



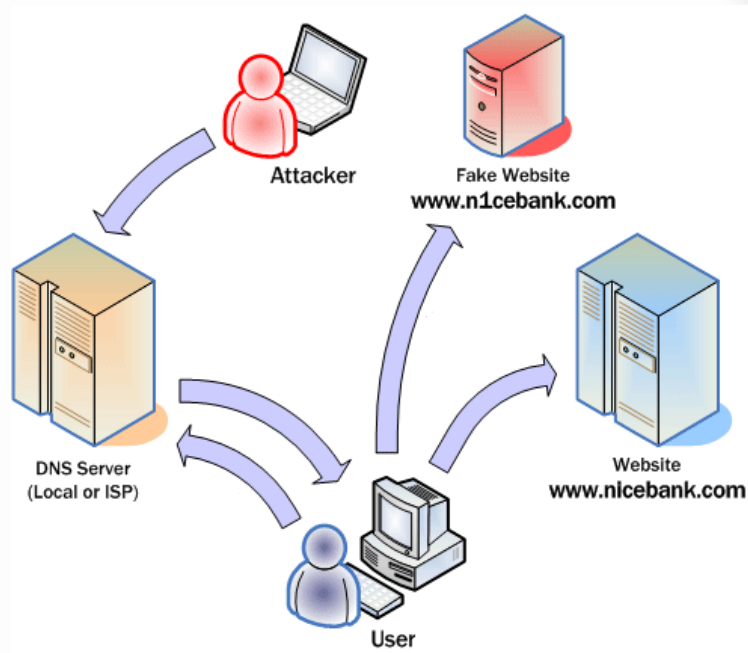
Ο Οργανισμός APWG (Anti-Phishing Working Group) δημοσιεύει στο site του τις μηνιαίες αναφορές για της τάσεις.

## 5.PHARMING

Το pharming είναι η μετεξέλιξη του phishing. Οι βασικές τους διαφορές είναι δύο.

- Η επίθεση μπορεί να γίνει μαζικά προς πολλούς χρήστες με χρήση spam mails και όχι μεμονωμένα.
- Η μετακίνηση προς το fake site σε μια επίθεση pharming γίνεται αυτόματα με το άνοιγμα του mail και χωρίς την παρεμβολή του χρήστη(δίχως κάποιο link).

Σε τέτοιου είδους επιθέσεις έχουν δημιουργηθεί πανομοιότυπα με το πραγματικό site της τράπεζας, ιστοσελίδες με μικρές διαφορές και ζητούν από τους χρήστες να καταχωρήσουν τα στοιχεία τους για διάφορους λόγους. Μόλις γίνει αυτό και τελειώσει η όλη διαδικασία, οι όποιοι έχουν σχεδιάσει την επίθεση έχουν αποκτήσει όλους τους προσωπικούς κωδικούς των ανυποψίαστων θυμάτων τους και μπορούν να εισέλθουν στην πραγματική σελίδα της τράπεζας και να συνδεθούν στο λογαριασμό τους και ανά πραγματοποιήσουν οποιαδήποτε συναλλαγή.



Εδώ πρέπει να σημειώσουμε πως καμία τράπεζα και ποτέ δεν στέλνει ενημερωτικά mails στα οποία να ζητά ή να προτρέπει τους πελάτες της να συνδεθούν σε κάποιο site για να κάνουν κάποια επιβεβαίωση στοιχείων λόγω τεχνικών ή άλλων προβλημάτων, μόνο σε σπάνιες περιπτώσεις ζητά να προσέλθουν οι ίδιοι σε κάποιο φυσικό υποκατάστημα.

## Η ΑΝΤΙΜΕΤΟΠΙΣΗ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΚΙΝΔΥΝΩΝ ΑΠΟ ΤΙΣ ΤΡΑΠΕΖΕΣ.

Σύμφωνα με έρευνα της Insight Express σε πελάτες αμερικανικών e-banking εφαρμογών, διαπιστώθηκε ότι σχεδόν τα ¾ αυτών (71%) σκέφτονται σοβαρά την on line τραπεζική απάτη. Οι απαντήσεις που έδωσαν οι συμμετέχοντες στην ερώτηση: «Ποίες ενέργειες πρέπει να κάνουν οι τράπεζες για να αυξήσουν την εμπιστοσύνη των καταναλωτών στις παρεχόμενες υπηρεσίες web-banking».

Ενέργειες που πρέπει να κάνουν οι τράπεζες για αύξηση της εμπιστοσύνης των καταναλωτών στην παρεχόμενες υπηρεσίες web banking	ΠΟΣΟΣΤΟ ΑΠΟΔΟΧΗΣ
Παροχή καλύτερων back-end συστημάτων ανίχνευσης ηλεκτρονικής απάτης	43%
Δημιουργία μοντέλων ανίχνευσης απάτης	41%
Παροχή εκπαιδευτικών πληροφοριών σχετικά με την on line Τραπεζική απάτη	35%
Τακτική επικοινωνία με τους πελάτες για τις ενέργειες αποφυγής on line απάτης	34%
Διενέργεια διαφημιστικών καμπανιών με οδηγίες αποφυγής On line απάτης	22%

Με βάση την παραπάνω έρευνα, αλλά και από την εμπειρία που υπάρχει σήμερα, η μεγαλύτερη ανησυχία των καταναλωτών, όπως και στη χώρα μας, είναι η ασφάλεια των συναλλαγών και η αποφυγή απάτης. Άρα οι τράπεζες οδηγούνται σε ολοένα καλύτερα συστήματα και πολιτικές ασφαλείας. Παρακάτω περιγράφονται αναλυτικά τρόποι και μέτρα που πρέπει να λαμβάνει ένας τραπεζικός οργανισμός για να διασφαλίσει τις ηλεκτρονικές συναλλαγές του.

## 1.ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Οι Τράπεζες απαιτείται να σχεδιάσουν σφικτούς ελέγχους σε αυτά τα νέα μοντέλα εργασίας, ώστε να διαχειρίζονται το ρίσκο. Οι βασικές ανάγκες για διασφάλιση των ιδιωτικών δεδομένων, εμπιστοσύνη και πιστοποίηση των υπηρεσιών θα συνεχίσουν να υφίστανται και στην ψηφιακή πλατφόρμα, όπως και στην παραδοσιακή μορφή παροχής των τραπεζικών υπηρεσιών. Η κρυπτογράφηση των δεδομένων προσφέρει αξιόλογες λύσεις στο παραπάνω ζήτημα.

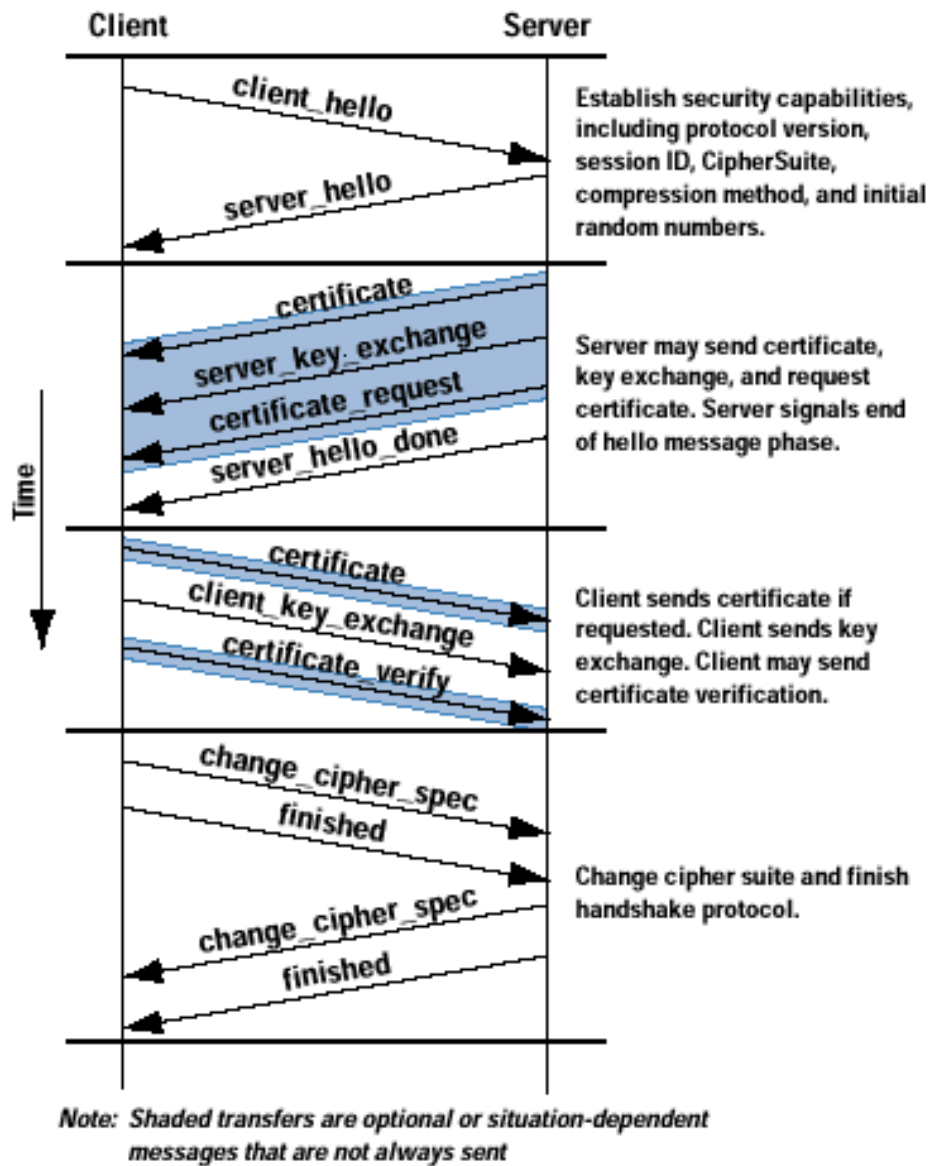
Υπάρχουν δύο διαφορετικά είδη κρυπτογράφησης με δύο ξεχωριστούς στόχους:

- Ο πρώτος στόχος είναι η διατήρηση του ιδιωτικού χαρακτήρα των συναλλαγών και το απαραβίαστο τόσο των προσωπικών δεδομένων όσο και της μεταφερόμενης αλλά και της αποθηκευμένης πληροφορίας.
- Ο δεύτερος στόχος είναι η πιστοποίηση της ταυτότητας των εμπλεκόμενων μερών μιας συναλλαγής.

Και οι 2 αυτοί στόχοι της κρυπτογράφησης συνήθως χρησιμοποιούνται ταυτόχρονα για την προστασία των μηνυμάτων και την πιστοποίηση των εμπλεκόμενων μερών. Και οι δύο μέθοδοι έχουν συγκεκριμένα βιομηχανικά πρότυπα. Οι εταιρίες που ασχολούνται με την κρυπτογράφηση παρέχουν λύσεις είτε ως προϊόντα λογισμικού (software) είτε ως συγκεκριμένα ανεξάρτητα εξαρτήματα hardware.

Στην παρούσα εργασία δεν είναι σκοπός να αναλύσουμε πλήρως τους τρόπους κρυπτογράφησης, όμως θα δούμε επιγραμματικά, πως δουλεύει πρακτικά η κρυπτογράφηση στις εφαρμογές web banking.

Όπως είπαμε η κρυπτογράφηση πρέπει να χρησιμοποιείται ώστε να ασφαλίσει το μήνυμα και να πιστοποιεί τον αποστολέα, στο παρακάτω σχήμα φαίνεται πως αυτό επιτυγχάνεται.



Γενικά η λογική που ακολουθείται είναι :

**ΕΙΣΑΓΩΓΗ ΔΕΔΟΜΕΝΩΝ -> ΚΡΥΠΤΟΓΡΑΦΗΣΗ -> ΑΠΟΣΤΟΛΗ ΔΕΔΟΜΕΝΩΝ**

Τα δεδομένα «κλειδώνονται» και αποθηκεύονται σε μέσα τις τράπεζας.



## 2. PKI (Public Key Infrastructure)

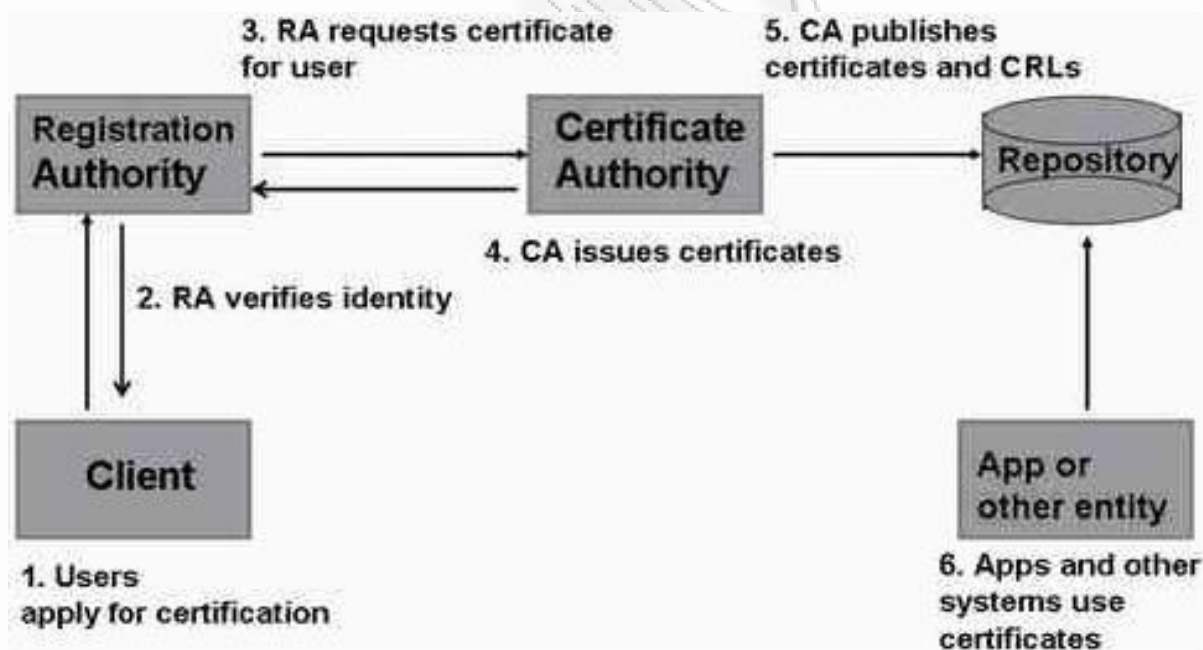
Η τεχνολογία PKI είναι πολύ γνωστή τεχνολογία και μπορεί να χρησιμοποιηθεί για να αναγνωρίσει οντότητες, για να κρυπτογραφήσει πληροφορία και να υπογράψει ηλεκτρονικά έγγραφα.

Η PKI αναγνωρίζει και διαχειρίζεται σχέσεις μεταξύ των μελών μιας ηλεκτρονικής ανταλλαγής δεδομένων, εξυπηρετεί ένα μεγάλο εύρος αναγκών ασφαλείας, συμπεριλαμβανομένων ελέγχου πρόσβασης, εμπιστευτικότητα, ακεραιότητα, πιστοποίηση και μη αποποίηση ευθύνης.

Η PKI χρησιμοποιεί μοναδικά Ψηφιακά Πιστοποιητικά για να διασφαλίσει το e-banking και e-commerce, το e-mail, την ανταλλαγή δεδομένων καθώς και τα VPNs και intranets. Τέλος η PKI τεχνολογία χρησιμοποιείται για να πιστοποιήσει την ταυτότητα και τα δικαιώματα του κάθε χρήστη.

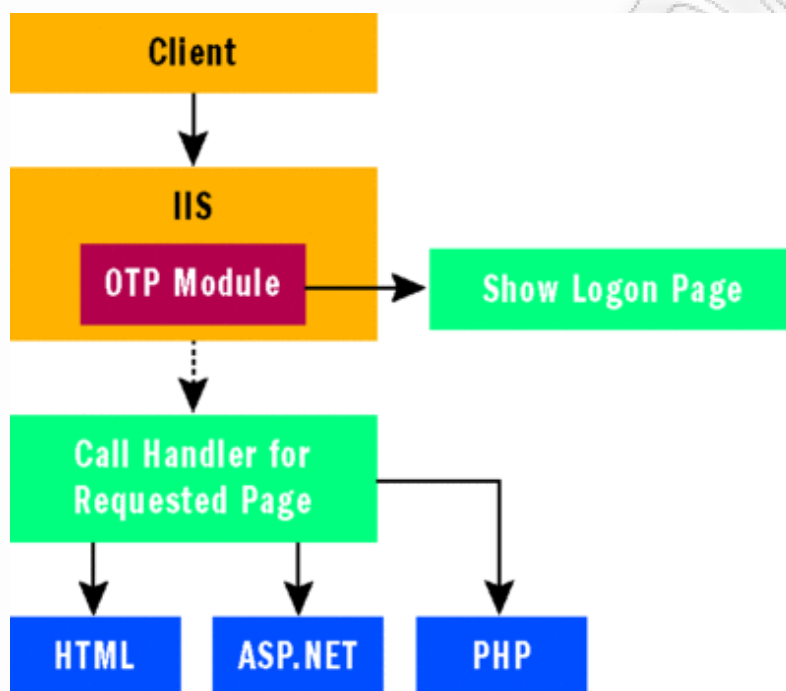
Η PKI χρησιμοποιεί για να επιτύχει τους στόχους της επιγραμματικά τις παρακάτω τεχνολογίες.

- Δημόσια και Ιδιωτικά Κλειδιά
- Ψηφιακές Υπογραφές
- Ψηφιακά Πιστοποιητικά



### 3. ΠΙΣΤΟΠΟΙΗΣΗ ΔΥΟ ΠΑΡΑΓΟΝΤΩΝ

Η αρχιτεκτονική συστημάτων πιστοποίησης δύο παραγόντων, με χρήση κωδικών μιας χρήσης (OTP) αναπαριστάται το παρακάτω σχήμα.



Οι περισσότεροι συμφωνούν ότι η πιστοποίηση δύο παραγόντων είναι ζωτική για την αποτελεσματική ασφάλεια των δικτύων. Ωστόσο κάθε οργανισμός πρέπει να επιλέξει ποία από όλες τις παρεχόμενες λύσεις πιστοποίησης δύο παραγόντων είναι οι καταλληλότερη για τις ανάγκες του. Παρακάτω παρουσιάζονται οι παρεχόμενες λύσεις πιστοποίησης δύο παραγόντων και επιγραμματικά η ακολουθούμενη ροή της κάθε μιας.

1. Challenge –Response
  - a. Ο χρήστης εισάγει username και password
  - b. Ο server στέλνει ένα challenge
  - c. Ο χρήστης εισάγει το challenge
  - d. Ένα response εμφανίζεται στην οθόνη του token
  - e. Ο χρήστης εισάγει το response και γίνεται το validation (επιβεβαίωση).
2. Events - Synchronous
  - a. Ο χρήστης ενεργοποιεί τον επόμενο κωδικό του token πατώντας ένα κουμπί σε αυτό (event)
  - b. Ο χρήστης εισάγει username και passcode (το passcode είναι η ένωση ενός κωδικού event-based παραγομένου από το token και του PIN του χρήστη).

- c. Ο server πιστοποιεί τον χρήστη ταιριάζοντας το passcode του χρήστη με το passcode του server (το server passcode δημιουργείται βασισμένο στο επόμενο event μιας ακολουθίας).
3. Time – Synchronous
    - a. Ο χρήστης εισάγει username και passcode (το passcode είναι η ένωση ενός κωδικού τυχαία παραγόμενου από το token και του PIN του χρήστη).
    - b. Ο server και το token υπολογίζουν τον κωδικό του token συνδυάζοντας το seed και την τρέχουσα ώρα Greenwich. Ο server πιστοποιεί τον χρήστη ταιριάζοντας το passcode του χρήστη με το passcode του server.

Η time synchronous ταυτοποίηση θεωρείται αποτελεσματικότερη των υπολοίπων για αρκετούς λόγους όπως

- Ενισχυμένη ασφάλεια
- Ευκολία χρήσης
- Μικρότερο διαχειριστικό κόστος
- Φορητότητα

#### **4.ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ (smart cards)**

Η τεχνολογία των έξυπνων μπορεί να χρησιμοποιηθεί για να δημιουργήσει κάρτες που παρέχουν ισχυρή ταυτοποίηση και αυτό γίνεται με την ενσωμάτωση ηλεκτρονικών κλειδιών στην κάρτα. Ένα μεγάλο ζήτημα σχετικά με τις έξυπνες κάρτες είναι η χρήση τους για πιστοποίηση.



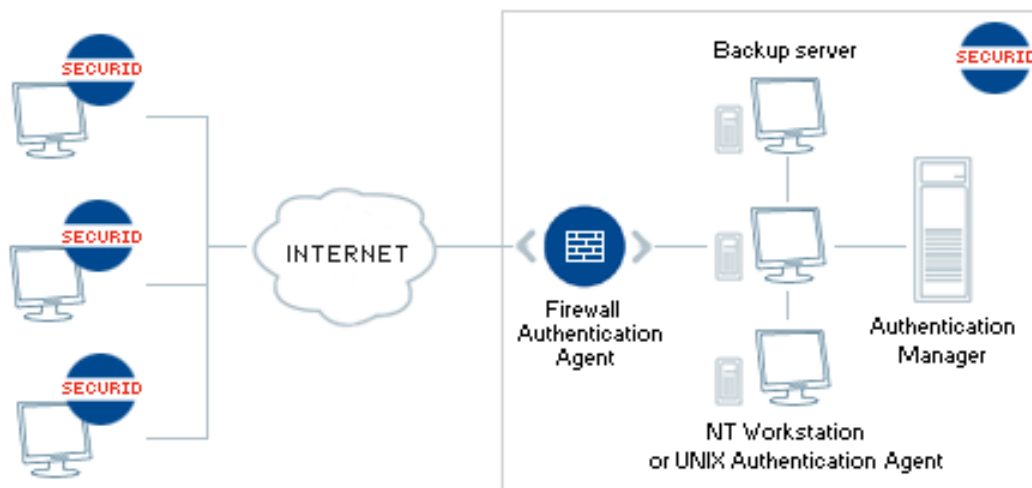
Στην πραγματικότητα, οι έξυπνες κάρτες μπορούν να περιέχουν προσωπικές πληροφορίες του κατόχου, κλειδιά για ψηφιακή υπογραφή, πιθανόν και βιομετρικές πληροφορίες του κατόχου κ.α. φυσικά για να αποφευχθεί το γεγονός οι λειτουργίες που προσφέρει μια κάρτα να καταστήσουν περιορισμός και όχι πλεονέκτημα για τις ηλεκτρονικές υπηρεσίες, οι οποίες θα πρέπει να σχεδιάζονται δίχως να λαμβάνονται υπόψη τις έξυπνες κάρτες που υπάρχουν.

---

Οι φωτογραφίες, τα σχέδια και τα ανωτέρω γραφήματα είναι αποσπάσματα από διάφορες σχετικές ιστοσελίδες οι οποίες αναφέρονται αναλυτικά στην βιβλιογραφία.

## 5. FIREWALLS

Ένα firewall μπορεί να είναι είτε ένα software είτε hardware που τοποθετείται μεταξύ δύο δικτύων και εποπτεύει την κίνηση μεταξύ τους. Σκοπός είναι όλη η δικτυακή κίνηση να περάσει από αυτό και να ελεγχθεί και τότε το firewall μπορεί να εξασφαλίσει ότι αυτή η κίνηση είναι εγκεκριμένη αποτρέποντας την ανεπιθύμητη να εισέλθει στο σύστημα.



Το firewall μπορεί επίσης να ελέγξει την κίνηση και να αποφασίσει αν αυτή περιέχει με εγκεκριμένα στοιχεία όπως ιούς. Τα firewalls πρέπει να είναι αποτελεσματικά στο να συλλαμβάνουν οποιαδήποτε μη εγκεκριμένη κίνηση ώστε να προλαβαίνουν πιθανή ζημία στον Οργανισμό.

Παρακάτω αναφέρονται επιγραμματικά οι λειτουργίες των firewalls.

1. Απομόνωση του δικτύου (Network Isolation)
2. Προστασία διευθύνσεων (Address Screening)
3. Προστασία Εφαρμογής (Application Screening) ή (proxy server)
4. Επιθεώρηση ροής μηνυμάτων ή συνολικής κατάστασης (Message Flow or State Full inspection)

## 6.SSL Certificates (Πιστοποιητικά Ασφαλείας Servers)

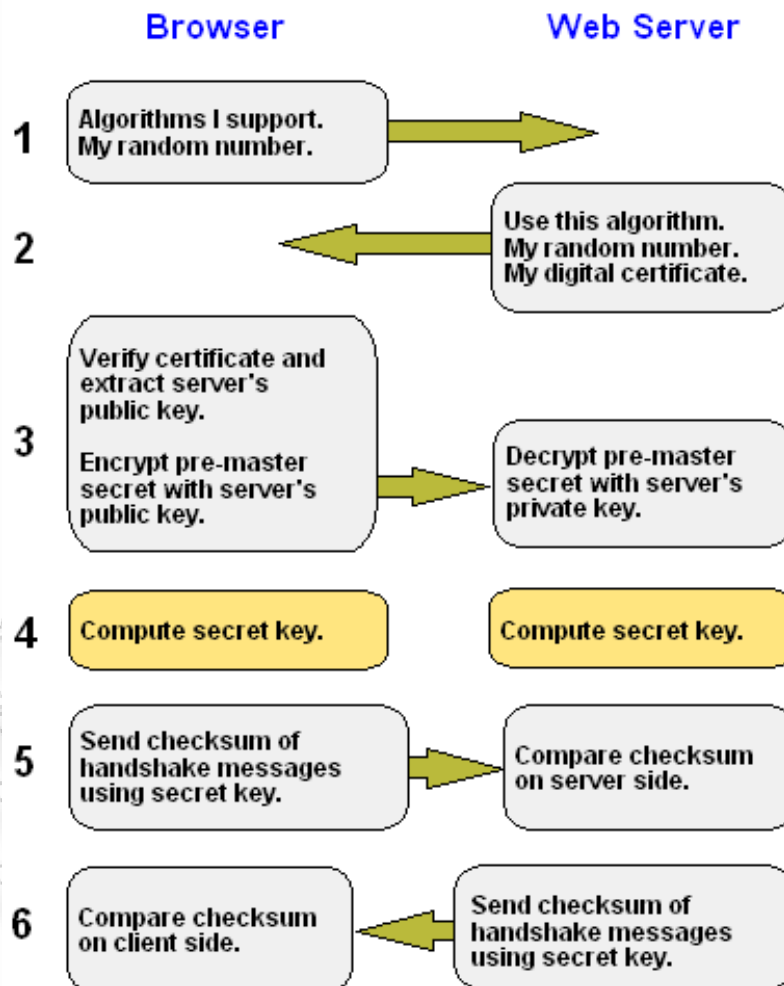
Για συναλλαγές μέσω internet, το κλειδί είναι η δημιουργία εμπιστοσύνης. Για να μπορεί μια τράπεζα να έχει επιτυχημένες ηλεκτρονικές υπηρεσίες, απαιτείται οι πελάτες να την εμπιστεύονται για την ασφάλεια των ευαίσθητων δεδομένων τους από υποκλοπές και επιθέσεις. Εγκαθιστώντας ένα 128-bit SSL πιστοποιητικό ασφαλείας server από μία αναγνωρισμένη αρχή πιστοποίησης στο site της, μια τράπεζα ασφαλίζει τις υπηρεσίες της και δημιουργεί αίσθημα σιγουριάς στον πελάτη, κρυπτογραφώντας όλες τις on line συναλλαγές της. Με το SSL οι πελάτες γνωρίζουν ότι ο δικτυακός τόπος είναι ασφαλής.

Τα SSL προσφέρουν σε μια τράπεζα, υψηλή ασφάλεια και έχουν πολλαπλή χρησιμότητα για τους ακόλουθους λόγους.

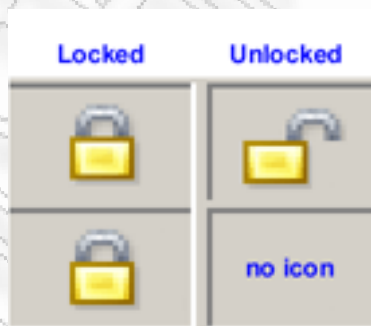
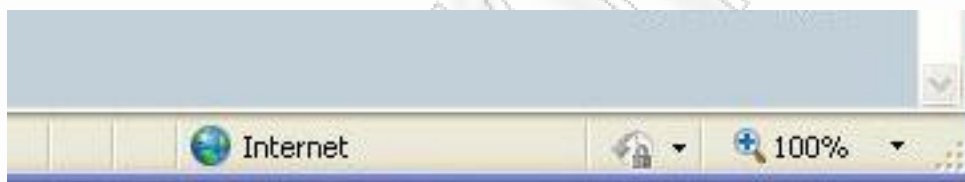
- Είναι πλήρως αναγνωρισμένα
- Έχουν 128-bit κρυπτογράφηση
- Διαρκούν από 1 έως 3 χρόνια
- Προσφέρουν 99% αναγνώριση browser
- Έχουν αυστηρή πιστοποίηση
- Υποστηρίζονται από αρχή πιστοποίησης

**Πως δουλεύει το SSL:**

From Computer Desktop Encyclopedia  
© 2005 The Computer Language Co. Inc.

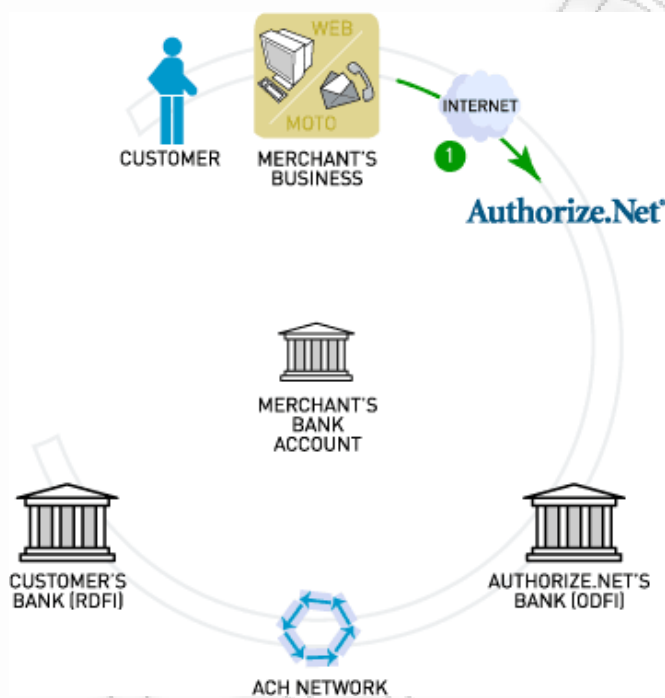


1. Όταν ο χρήστης επισκέπτεται ένα SSL secure site, ο browser του χρήστη ζητά ένα ασφαλές session από τον web server.
2. Ο server απαντά, αποστέλλοντας στον browser του χρήστη το πιστοποιητικό του.
3. Ο browser πιστοποιεί την εγκυρότητα του πιστοποιητικού, πιστοποιεί ότι χρησιμοποιείται από το site για το οποίο έχει εκδοθεί και ότι έχει εκδοθεί από την αρχή πιστοποίησης που είναι αναγνωρισμένη.
4. Αν το πιστοποιητικό είναι εγκεκριμένο, ο browser δημιουργεί ένα κλειδί μιας φορές και το κρυπτογραφεί με το δημόσιο κλειδί του server.
5. Ο browser στέλνει το κρυπτογραφημένο κλειδί στον server ώστε να έχουν και οι δύο από ένα αντίγραφο.
6. Ο server αποκρυπτογραφεί το κλειδί χρησιμοποιώντας το ιδιωτικό του κλειδί
7. Η διαδικασία πιστοποίησης SSL έχει ολοκληρωθεί και έχει εγκατασταθεί μια ασφαλή σύνδεση
8. Ένα εικονίδιο κλειδαριάς εμφανίζεται στην γραμμή κατάστασης του browser, υποδηλώνοντας ότι το site είναι ασφαλές.



### 7.Transaction Authorization Numbers (Λίστες TAN) , Extra PINs

Μια κοινή μέθοδος, αντιμετώπισης ζητημάτων ασφαλείας είναι η χρήση PIN για πιστοποίηση και των αριθμών TAN για την έγκριση On line συναλλαγών.



Οι αριθμοί TAN υπάρχουν τυπωμένοι σε χαρτί και δίδονται στον πελάτη του e-banking. Κάθε φορά που ο χρήστης πραγματοποιεί συναλλαγή, εισάγει ως κωδικό έγκρισης έναν τέτοιο αριθμό. Όταν ένας αριθμός χρησιμοποιείται δεν μπορεί να χρησιμοποιηθεί ξανά.

119105	119561	119739	119914	120099	120290	120472	120671	120882	121066
121409	121590	121770	121956	122139	122317	122492	122697	122912	123096
123596	123794	123988	124179	124354	124531	124778	124953	125125	125300
125768	125947	126132	126306	126535	126723	126945	127153	127323	127495
127867	128051	128225	128394	128564	128766	128959	129226	129421	129653
130032	130216	130408	130594	130789	131007	131198	131380	131614	131793
132224	132529	132795	132977	133154	133324	133491	133705	133947	134207
134564	134927	135230	135450	135899	136286	136509	136817	138113	139405
139823	140006	140178	140351	140525	140694	140972	141194	141380	141643
142060	142257	142453	142715	142913	143096	143288	143469	143641	143825
144243	144497	144689	144933	145127	146475	146787	147079	147273	147446
147804	147989	148160	148633	148809	149085	149586	149767	149939	150246
150710	151146	152178	152366	152538	152715	152908	153262	153442	153619
153961	154133	154329	154519	154693	154872	155049	155226	155438	155804
157382	157583	157840	158343	158842	159214	159430	159640	159843	160045
161386	161843	162194	162480	162728	162958	163208	163609	163931	164237
164861	165121	165466	165808	166426	166699	166957	167151	167352	
167535	167800	168003	168189	168366	168694	168877	169053		
169230	169417	169669	169855	170031	170212	170395			

A member of citigroup

citibank

### Συμπέρασμα για τις λύσεις

Συμπερασματικά, για τις λύσεις ασφαλείας των ηλεκτρονικών τραπεζικών συναλλαγών που προαναφέρθηκαν. Μπορούμε λοιπόν, να τις κατατάξουμε από την ισχυρότερη προς την πιο αδύνατη ως εξής:

1. Συνδυασμός Βιομετρικής , έξυπνης κάρτας και PKI
2. Συνδυασμός έξυπνης κάρτας και PKI
3. Συνδυασμός token και PKI
4. Token
5. PKI με καταγεγραμμένη πολιτική ασφαλείας
6. PKI χωρίς πολιτική
7. Password

Όσο αφορά τις ενέργειες και την προσοχή που θα πρέπει να δίνουν και **οι ίδιοι** οι πελάτες των τραπεζών στις συναλλαγές που εκτελούν μέσω διαδικτύου, και πόση ευθύνη έχουν οι ίδιοι πλέον για να μην πέσουν θύματα ηλεκτρονικής απάτης, δεν μας απασχόλησε σε αυτή την εργασία αν και είναι ένα πολύ βασικό μέρος στην διαδικασία αυτή.

---

Οι φωτογραφίες , τα σχέδια και τα ανωτέρω γραφήματα είναι αποσπάσματα από διάφορες σχετικές ιστοσελίδες οι οποίες αναφέρονται αναλυτικά στην βιβλιογραφία.

Η βίβλος του e-banking «Βασίλης Γ. Αγγέλης»392-406 και408-445

Ηλεκτρονική Τραπεζική «Αριστέα Σινανιώτη- Ιωάννης Φαρσαρώτας» 146 – 151



## **ΠΑΡΑΔΕΙΓΜΑ ΥΛΟΠΟΙΗΣΗΣ ΛΥΣΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ΔΥΟ ΠΑΡΑΓΟΝΤΩΝ, ΑΠΟ ΤΗΝ ΥΠΗΡΕΣΙΑ WINBANK PAYCENTER ΤΗΣ ΤΡΑΠΕΖΑΣ ΠΕΙΡΑΙΩΣ, ΜΕ ΒΑΣΗ ΤΟ ΠΡΩΤΟΚΟΛΛΟ 3D-SECURE ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΕΙΤΑΙ ΣΤΙΣ ΥΠΗΡΕΣΙΕΣ VERIFIED BY VISA ΚΑΙ MASTERCARD SECURECODE ΓΙΑ ΣΥΝΑΛΛΑΓΕΣ E-COMMERCE (ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ) ΜΕ ΤΗΝ ΧΡΗΣΗ ΠΙΣΤΩΤΙΚΩΝ ΚΑΡΤΩΝ VISA ΚΑΙ MASTERCARD.**

Αναγνώριση και καθορισμός του προβλήματος μιας πιστοποιημένης e-commerce πληρωμής η οποία δεν θα μπορεί να αμφισβητηθεί από τον πελάτη και πώς αυτό αντιμετωπίζεται με την χρήση των λύσεων των υπηρεσιών Verified by Visa και MasterCard SecureCode.

### **Τι σημαίνει «πιστοποίηση πληρωτή» σε μια e-commerce πληρωμή;**

Πιστοποίηση Πληρωτή (payer authentication) σημαίνει να μπορεί ένα e-shop να εξακριβώνει την νόμιμη κατοχή της κάρτας από τον πληρωτή, την στιγμή που αυτός εκτελεί μια πληρωμή με κάρτα στο e-shop. Είναι η λύση που από καιρό επιθυμούν οι ιδιοκτήτες των e-shops για να μην πέφτουν θύματα εξαπάτησης όταν εκτελούν παραγγελίες από το Internet, αλλά και οι καταναλωτές για να μη φοβούνται να χρησιμοποιήσουν τις κάρτες τους για μια αγορά στο Internet.

Για τον σκοπό αυτό οι διεθνείς Οργανισμοί Πληρωμών Visa και MasterCard δημιούργησαν μια νέα online διαδικασία που εκτελείται στιγμιαία κατά στιγμή της online πληρωμής με διπλό σκοπό:

1. Να διασφαλίζει τις εισπράξεις των εμπόρων από τις πιο κοινές αμφισβητήσεις
2. Να προστατεύει τους καταναλωτές-πληρωτές από μη εξουσιοδοτημένη χρήση της κάρτας τους όταν πληρώνουν online σε e-shops εμπόρων.

Το τεχνικό πρωτόκολλο που δημιουργήθηκε ονομάζεται "3D-Secure", οι δε αντίστοιχες υπηρεσίες των Οργανισμών για την online πιστοποίηση του πληρωτή έχουν τις εμπορικές ονομασίες Verified by Visa από την Visa και SecureCode από την MasterCard.

Με το 3D-Secure πρωτόκολλο εξασφαλίζεται «τεχνικά» η πιστοποίηση των κατόχων πιστωτικών καρτών, καθώς σε κάθε διενεργούμενη online πληρωμή συμμετέχει και η εκάστοτε τράπεζα που έχει εκδώσει την δεδομένη κάρτα (Issuer Bank).

### **Τι είναι οι υπηρεσίες Verified by Visa και MasterCard SecureCode;**

Οι υπηρεσίες Verified by Visa και MasterCard SecureCode έχουν σχεδιαστεί με βάση το πρωτόκολλο 3D-Secure για να μειώσουν τον κίνδυνο από τη μη εξουσιοδοτημένη χρήση της κάρτας ενός πελάτη, πιστοποιώντας τον κάτοχο της κάρτας κατά τη διενέργεια μιας online συναλλαγής σε ένα e-shop.

Η πιστοποίηση της πληρωμής κάνει τις αγορές μέσω Internet περισσότερο ασφαλείς, τόσο για τους αγοραστές όσο και για τους εμπόρους, εξαλείφοντας τις αμφισβητήσεις του τύπου «δεν έκανα εγώ την αγορά, δεν την αναγνωρίζω στο statement της κάρτας μου» εξασφαλίζοντας την είσπραξη στον έμπορο και δημιουργώντας ένα ασφαλές κανάλι ηλεκτρονικού εμπορίου για τους καταναλωτές.

### Πως λειτουργούν οι υπηρεσίες Verified by Visa και SecureCode;

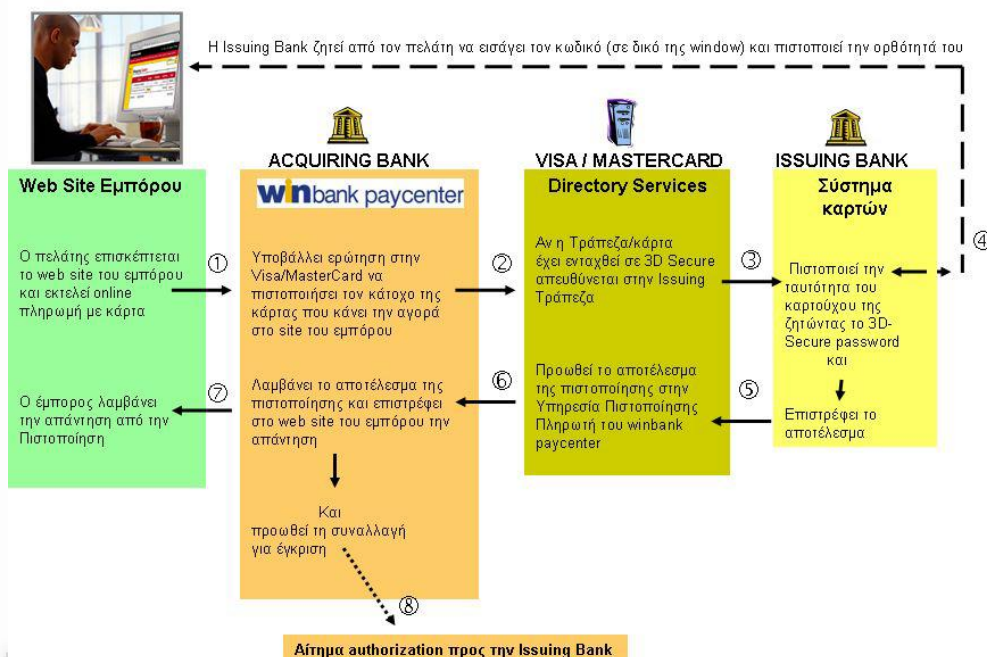
Η πιστοποίηση του πληρωτή είναι ένα τμήμα της συνήθους διαδικασίας της online πληρωμής και προηγείται της αίτησης για έγκριση (το γνωστό authorization request) από την αποδέκτρια (Acquiring) τράπεζα.

Με πρωτοβουλία των τραπεζών που υποστηρίζουν το πρωτόκολλο 3D-Secure οι καταναλωτές-καρτούχοι τους καλούνται να εντάξουν τις Visa ή MasterCard πιστωτικές και χρεωστικές τους κάρτες στα προγράμματα Verified by Visa ή SecureCode. Ένταξη σημαίνει ότι οι καρτούχοι επιλέγουν έναν κωδικό για κάθε κάρτα τους που μόνο αυτοί θα γνωρίζουν, όπως π.χ. είναι ο κωδικός που χρησιμοποιούν στα ATM για ανάληψη χρημάτων.

Έτσι, όταν κάποιος χρησιμοποιεί αυτήν την κάρτα σε ένα e-shop που υποστηρίζει τις υπηρεσίες Verified by Visa και SecureCode, του ζητείται από την εκδότρια (Issuing) τράπεζα της κάρτας να «υπογράψει την νόμιμη κατοχή της κάρτας» για την αγορά, πληκτρολογώντας αυτόν τον κρυφό κωδικό που μόνο αυτός - δηλ. ο νόμιμος κάτοχος της κάρτας – γνωρίζει.

Το ακόλουθο σχήμα απεικονίζει τη διαδικασία πιστοποίησης του πληρωτή έτσι όπως έχει υλοποιηθεί από την υπηρεσία winbank paycenter της Τράπεζα Πειραιώς:

### 3D-Secure: Authentication κύκλος



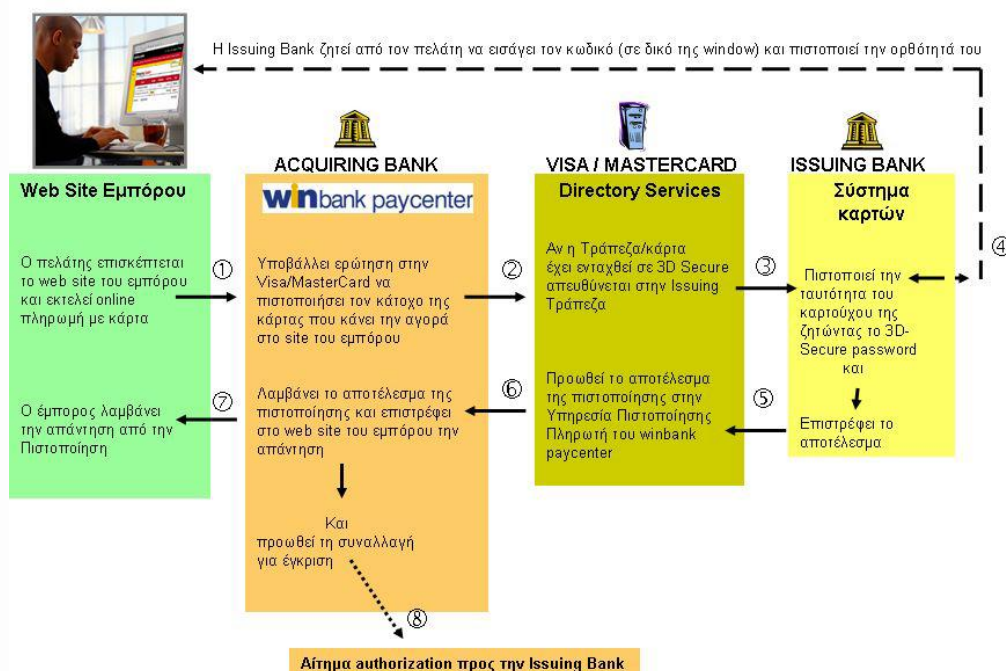
Η online διαδικασία πιστοποίησης είναι στιγμιαία και ενεργοποιείται κάθε φορά που χρησιμοποιείται μια κάρτα Visa ή MasterCard στο e-shop ενός εμπόρου και προηγείται της αίτησης για έγκριση της χρέωσης της κάρτας.

**Τα δεδομένα κρυπτογραφούνται και πιστοποιούνται με την χρήση SSL certificates 128bits.**

## DEMO CODE ΓΙΑ ΤΗΝ ΥΛΟΠΟΙΗΣΗ ΤΗΣ ΛΥΣΗΣ.

Η πλήρης υλοποίηση έχει γίνει σε ASP.NET από εξωτερικό προμηθευτή της Τράπεζας Πειραιώς, την Ελληνική εταιρία DATA CONCEPT, και το ακόλουθο τμήμα αποτελεί demo code (δείγμα κώδικα) με τα βασικά στοιχεία και μέρη της υλοποιημένης λύσης και αποτελεί μια βασική προσέγγιση της λύσης, σύμφωνα με τις επιταγές εφαρμογής του πρωτοκόλλου 3D-Secure που χρησιμοποιείται στις υπηρεσίες Verified by Visa και MasterCard SecureCode για συναλλαγές e-commerce (ηλεκτρονικού εμπορίου) με την χρήση πιστωτικών καρτών VISA και MASTERCARD για το σύστημα πληρωμών της υπηρεσίας paycenter της ΤΡΑΠΕΖΑΣ ΠΕΙΡΑΙΩΣ.

### 3D-Secure: Authentication κύκλος



#### Βήμα 1ο

Στην (html) σελίδα του εμπόρου όπου θα φύγει το request προς την Τράπεζα συμπληρώνονται τα στοιχεία όπου θα φορτωθούν στην εφαρμογή μέσω του pay center σύμφωνα με τα παρακάτω.

Epayment.aspx

```
<div id="staticMain" runat="server">
  <div class="piraeus">
    <input id="AcquirerId" type="hidden" name="AcquirerId" value="<%=AcquirerId%>" />
    <input id="MerchantId" type="hidden" name="MerchantId" value="<%=MerchantId%>" />
    <input id="PosId" type="hidden" name="PosId" value="<%=PosId%>" />
    <input type="hidden" id="User" name="User" value="<%=User%>" />
  </div>
</div>
```

```

        <input type="hidden" id="LanguageCode" name="LanguageCode"
value="<%=LanguageCode%>" />
        <input type="hidden" id="MerchantReference" name="MerchantReference"
value="<%=MerchantReference%>" />
        <input type="hidden" id="ParamBackLink" name="ParamBackLink"
value="<%=ParamBackLink%>" />
        <input id="button" type="submit" class="members_btn" value="<%=name %>"
/>
    </div>
</div>

```

### Βήμα 2ο

Από τα παραπάνω γίνεται όλη η δουλειά χρησιμοποιώντας τις δύο μεθόδους που βλέπεις παρακάτω.

Παίρνουμε το απαιτούμενο ticket και βάζουμε τις απαραίτητες πληροφορίες που απαιτούνται στην φόρμα η οποία γίνεται Post σε Url που έχει δηλώσει η Τράπεζα ότι περιμένει τις συγκεκριμένες πληροφορίες.

```

public string gettheTicket(OrderFull thecart)
{
    string theticket = "";

    //create theissue
    TicketingService theservice = new TicketingService();
    TicketRequest theRequest = new TicketRequest();

    theRequest.AcquirerId =
Convert.ToInt32(ConfigurationManager.AppSettings["acquirerID"]);
    theRequest.MerchantId =
Convert.ToInt32(ConfigurationManager.AppSettings["MerchantID"]);
    theRequest.PosId =
Convert.ToInt32(ConfigurationManager.AppSettings["PosID"]);
    theRequest.Username = ConfigurationManager.AppSettings["UserName"];
    theRequest.Password =
HelperMethods.CreatePasswordMd5(ConfigurationManager.AppSettings["Password"]);
;
    theRequest.RequestType = "02"; //gia agores
    theRequest.CurrencyCode = 978; //to euro
    theRequest.MerchantReference =
thecart.order.refItem.lRow_Id.ToString();
    reqParams.CurrSession.theidofcart = thecart.order.refItem.lRow_Id;

    theRequest.Amount = ContentHandler.getTotalPrice(reqParams, thecart,
price_type.all);
    tbFolderItemProperties THEPROP = thecart.order.GetProperty(

```

```

thecart.order.refPage.getSpecialFieldByAllInherited(ExtraColumnSpecialType.sp
cial7).
                                lRow_Id);
    if (THEPROP.sValue=="")
        theRequest.Installments = 1;
    else
    {
        theRequest.Installments = Convert.ToByte(THEPROP.sValue);
    }
    theRequest.ExpirePreauth = 0;
    theRequest.Bnpl = 0;
    //theRequest.Parameters = 150 //
    TicketResponse theresponse = theservice.IssueNewTicket(theRequest);
    return theticket=theresponse.TranTicket;
}

```

### Βήμα 3ο και 4ο

**Ζητείτε επιβεβαίωση από την Τράπεζα του πελάτη.**

**Η γλώσσα επικοινωνίας των συστημάτων είναι η xml**

Ο ακόλουθος κώδικας παρέχεται με την άδεια χρήσης του πρωτοκόλλου και επιτυγχάνει την σωστή διαβίβαση των στοιχείων από την Τράπεζα όπου θα κάνει την συναλλαγή (σε αυτή την περίπτωση την ΤΡΑΠΕΖΑ ΠΕΙΡΑΙΩΣ) στην βάση της VISA / MASTERCARD για επαλήθευση.

```

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Body>
<ProcessTransaction xmlns="http://piraeusbank.gr/paycenter">
<TransactionRequest xmlns="http://piraeusbank.gr/paycenter/1.0">
<Header>
<RequestType>FOLLOW_UP</RequestType><MerchantInfo><AcquirerID>GR014</Acquirer
ID><MerchantID>14000000</MerchantID>
<PosID>81000000</PosID>
<ChannelType>3DSecure</ChannelType>
<User>USERNAME</User>
<Password>PASSWORD(MD5)</Password>
</MerchantInfo>
</Header>
<Body>
<TransactionInfo><MerchantReference>YOUR_MERCHANT_REFERENCE</MerchantReferenc
e><TransactionReferenceID xsi:nil="true" />
<EntryType xsi:nil="true" />
<CurrencyCode xsi:nil="true" />
<Amount xsi:nil="true" />
<Installments xsi:nil="true" />
<ExpirePreauth xsi:nil="true" />

```

```

<TipAmount xsi:nil="true" />
<Bnpl xsi:nil="true" />
<SessionKey xsi:nil="true" /><AuthInfo xsi:nil="true" />
</TransactionInfo>
</Body>
</TransactionRequest>
</ProcessTransaction>
</soap:Body>
</soap:Envelope>

```

Το ακόλουθο τμήμα κώδικα επιβεβαιώνει η VISA / MASTERCARD ότι όλα τα διαβιβασμένα στοιχεία είναι έγκυρα και μπορεί το σύστημα να προχωρήσει στην ολοκλήρωση της συναλλαγής.

```

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Body>
<ProcessTransactionResponse
xmlns="http://piraeusbank.gr/paycenter"><TransactionResponse>
<Header xmlns="http://piraeusbank.gr/paycenter/1.0">
<RequestType>FOLLOW_UP</RequestType>
<MerchantInfo>
<MerchantID>140000000</MerchantID>
<PosID>81000000</PosID>
<ChannelType>3DSecure</ChannelType>
<User>USERNAME</User>
</MerchantInfo>
<ResultCode>0</ResultCode>
<ResultDescription>No Error</ResultDescription>
<SupportReferenceID>699798</SupportReferenceID>
</Header>
<Body xmlns="http://piraeusbank.gr/paycenter/1.0">
<TransactionInfo>
<StatusFlag>Success</StatusFlag>
<ResponseCode>00</ResponseCode>
<ResponseDescription>Approved or completed successfully</ResponseDescription>
<TransactionID>3097481</TransactionID>
<TransactionDateTime>2009-12-15T15:31:33</TransactionDateTime>
<TransactionTraceNum>15</TransactionTraceNum>
<MerchantReference>YOUR_MERCHANT_REFERENCE</MerchantReference>
<ApprovalCode>021708</ApprovalCode>
<RetrievalRef>000006963185</RetrievalRef>
<PackageNo>5</PackageNo>
<SessionKey xsi:nil="true" />

```

```

</TransactionInfo>
</Body>
</TransactionResponse>
</ProcessTransactionResponse>
</soap:Body>
</soap:Envelope>

```

Αυτό που επιστρέφεται είναι το token-ticket επιβεβαίωσης ότι τα συστήματα αναγνωρίζονται . Ακολουθεί η μεταμόρφωση των στοιχείων και η προώθηση τους επιβεβαίωση στο τμήμα επιτυχούς συναλλαγής

```

public void fromSessiontoInput()
{
if (reqParams.CurrSession.theidofcart>0)
{
AcquirerId = ConfigurationManager.AppSettings["acquirerID"];
MerchantId = ConfigurationManager.AppSettings["MerchantID"];
PosId = ConfigurationManager.AppSettings["PosID"];
User = ConfigurationManager.AppSettings["UserName"];
LanguageCode = ConfigurationHandler.GuiCultureInfo;
MerchantReference = reqParams.CurrSession.theidofcart.ToString();
ParamBackLink = "p1=v1";
}
}

```

### Βήμα 5ο και 6ο

Ολοκληρώνεται επιτυχώς η συναλλαγή και οι πληροφορίες δημοσιοποιούνται στον πελάτη , στον έμπορο και εγγράφονται στην βάση της Τράπεζας

```

Success.aspx
<div id="staticMain">
<table class="texts" width="100%" border="0">
<tr>
<td class="success_nameField">
<asp:Label ID="lblTitle" runat="server" Text="Σας
ενημερώνουμε ότι η κάρτα σας χρεώθηκε με EUR " Font-Bold="true"></asp:Label>
<br />
<asp:Label ID="lblTitle2" runat="server" Text="Στον
εκκαθαριστικό λογαριασμό της κάρτας σας θα εμφανιστεί χρέωση με περιγραφή
συναλλαγής ΕΜΠΟΡΟΣ"></asp:Label>
</td>
<td class="success_labelField">
<asp:Label ID="theprice"
runat="server"></asp:Label>&euro;
</td>
</tr>

```

```

        <tr>
            <td class="success_nameField">
                <asp:Label ID="lblArithmoSinallagis" runat="server"
Text="Αριθμός Συναλλαγής:" Font-Bold="true"></asp:Label>
            </td>
            <td class="success_labelField">
                <asp:Label ID="theNumberOfTrans"
runat="server"></asp:Label>
            </td>
        </tr>
        <tr>
            <td class="success_nameField">
                <asp:Label ID="lblKodikosAnaforas" runat="server"
Text="Κωδικός Αναφοράς:" Font-Bold="true"></asp:Label>
            </td>
            <td class="success_labelField">
                <asp:Label ID="theKodikosAnaforas"
runat="server"></asp:Label>
            </td>
        </tr>
        <tr>
            <td class="success_nameField">
                <asp:Label ID="lblKodikosEgkrixis" runat="server"
Text="Κωδικός Έγκρισης:" Font-Bold="true"></asp:Label>
            </td>
            <td class="success_labelField">
                <asp:Label ID="theIDofCart" runat="server"></asp:Label>
            </td>
        </tr>
        <%-- <tr>
            <td class="success_nameField">
                <asp:Label ID="user" runat="server" Font-
Bold="true"></asp:Label>
            </td>
            <td class="success_labelField">
                <asp:Label ID="item" runat="server"></asp:Label>
            </td>
        </tr--%>
    </table>
</div>
<input id="SupportReferenceID" type="hidden" name="SupportReferenceID"
value="" />
<input type="hidden" id="ResultCode" name="ResultCode" value="" />
<input type="hidden" id="StatusFlag" name="StatusFlag" value="" />
<input type="hidden" id="ResponseCode" name="ResponseCode" value="" />
<input type="hidden" id="MerchantReference" name="MerchantReference"
value="" />

```



```
<input type="hidden" id="TransactionId" name="TransactionId" value="" />
<input type="hidden" id="PackageNo" name="PackageNo" value="" />
<input type="hidden" id="ApprovalCode" name="ApprovalCode" value="" />
<input type="hidden" id="AuthStatus" name="AuthStatus" value="" />
<input type="hidden" id="Parameters" name="Parameters" value="" />
<input type="hidden" id="HashKey" name="HashKey" value="" />
<input type="hidden" id="errorMessage" name="errorMessage" value="" />
```

Ενημέρωση της βάσης της Τράπεζας.

```
private void populateInfo()
{
    string SupportReferenceID = "";
    string ResultCode = "";
    string StatusFlag = "";
    string ResponseCode = "";
    string MerchantReference = "";
    string TransactionId = "";
    string PackageNo = "";
    string ApprovalCode = "";
    string AuthStatus = "";
    string Parameters = "";
    string HashKey = "";

    SupportReferenceID = Request["SupportReferenceID"].ToString();
    ResultCode = Request["ResultCode"].ToString();
    StatusFlag = Request["StatusFlag"].ToString();
    ResponseCode = Request["ResponseCode"].ToString();
    MerchantReference = Request["MerchantReference"].ToString();
    TransactionId = Request["TransactionId"].ToString();
    ApprovalCode = Request["ApprovalCode"].ToString();
    PackageNo = Request["PackageNo"].ToString();
    AuthStatus = Request["AuthStatus"].ToString();
    Parameters = Request["Parameters"].ToString();
    HashKey = Request["HashKey"].ToString();
    theIDofCart.Text = ApprovalCode;
    theNumberOfTrans.Text = TransactionId;
    theKodikosAnaforas.Text = SupportReferenceID;
}
```

**Βήμα 7ο**  
Ο πελάτης αποδέχεται την συναλλαγή

**Βήμα 8ο**  
Το σύστημα επικοινωνεί εκ νέου με την τράπεζα του πελάτη ότι έγινε οριστική αποδοχή και προωθεί το αίτημα για πληρωμή.

## Βιβλιογραφία.

- Ηλεκτρονική Τραπεζική «Αριστέα Σινανιώτη- Ιωάννης Φαρσαρώτας»
- Η βίβλος του e-banking «Βασίλης Γ. Αγγέλης»
- Η πρόσβαση στις Χρηματοοικονομικές Υπηρεσίες μέσω διαδικτύου «Ιωάννης Λιναρίτης»
- Παροχή χρηματοοικονομικών υπηρεσιών από απόσταση « Άννα Δεσποτίδου»
- Τεχνολογικές Εφαρμογές στη Λειτουργία των Τραπεζών « Χαράλαμπος Γκότσης»
- Κατανοώντας τη Σύγχρονη Τραπεζική « Ιωάννης Φαρσαρώτας»
- Mobile Banking : Διαχείριση Τραπεζικών Συναλλαγών Μέσω Κινητού Τηλεφώνου « Γεώργιος Μπιζανίδης »
- Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης «Β.Α. Κάτος- Γ.Χ. Στεφανίδης»
- Εισαγωγή στη Θεωρία Πληροφοριών, Κωδικών και Κρυπτογραφίας «Ν.Αλεξανδρής – Β. Χρυσικόπουλος – Κ. Πατσάκης»
- Νέα Οικονομία, Διαδίκτυο και Ηλεκτρονικό Εμπόριο «Γιάννης Κατσουλάκος»
- Ηλεκτρονικό Επιχειρείν «Β. Γεωργακόπουλος – Μ. Πανταζή – Χ. Νικολαράκος – Ι. Βαγγελάτος»
- Ηλεκτρονικό Εμπόριο «Γ. Δουκίδης – Μ. Θεμιστοκλέους – Β. Δράκος – Ν. Παπαζαφειροπούλου»
- Οδηγός στρατηγικής στη δικτυακή οικονομία «Χαρίδημος Τσούκας»
- Διαχείριση Έργων Πληροφορικής «Joseph Phillips»
- <http://www.lawnet.gr>
- <http://www.tiresias.org>
- <http://www.computerlanguage.com/>
- <http://www.qvbiometrics.com>
- <http://www.e.govt.nz>
- <http://www.icta.mu>
- <http://www.dip.co.uk>
- <http://www.bustathief.com>
- <http://www.utsa.edu>
- <http://www.hcsbaccess.com>
- <http://web-tracker.blogspot.com>
- <http://computer.howstuffworks.com>
- <http://docstore.mik.ua>
- <http://www.codeproject.com>
- <http://www.spyemporium.net>
- <http://cse.stanford.edu>
- <http://www.priya-tech.com>
- <http://www.trustedreviews.com>
- <http://www.billion.uk.com>
- <http://www.alithia.gr/columnbyid.aspx?columnid=1280>
- <http://www.ecos.de>

- <http://www.zyxelguard.com>
- <http://www.zyxel.com>
- <http://technet.microsoft.com>
- <http://msdn.microsoft.com>
- <http://www.cisco.com>
- <http://www.nask.pl>
- <http://dictionary.zdnet.com>
- <http://www.safescrypt.com>
- <http://www.sslshopper.com>
- <http://www.allyou.com.my>
- <http://www.sapsecurityonline.com>
- <http://www.bams.com>
- <http://www.h-online.com>
- <http://www.westpac.com.fj>
- <http://www.scmagazine.com.au/>
- <http://www.worldlingo.com>
- <http://www.ecb.int>
- <http://www.banktech.com/>
- <http://www.bankofgreece.gr/>
- <http://www.centralbank.gov.cy>
- <http://www.dias.com.gr>
- <http://www.tbank.com.gr>
- <http://www.eurobank.gr>
- <http://www.alpha.gr>
- <http://www.piraeusbank.gr/>
- <http://www.winbank.gr/>
- <http://usa.visa.com>
- <http://www.visa.ca>
- <http://www.citigroup.com>
- <http://www.verisign.com/>
- <http://www.sepe.gr/>
- <http://www.mmaglobal.com/>
- <http://www.forrester.com/>
- <http://www.plant-management.gr/>
- <http://www.ependyseis.gr>