Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Mobile Banking - Τραπεζική ανά χείρας**
Ονοματεπώνυμο Φοιτητή	**Παπαδοπούλου Αικατερίνη**
Πατρώνυμο	**Κοσμάς**
Αριθμός Μητρώου	**ΜΠΠΛ/ 09056**
Επιβλέπων	**Σινανιώτη-Μαρούδη Αριστέα**

ΑΦΙΕΡΩΣΗ

Αφιερωμένο στους γονείς μου, στον σύζυγό μου και ιδιαίτερα στον μικρό μου πρίγκιπα ως ένα μικρό αντιστάθμισμα για τις ώρες που δεν ήμουν κοντά του.

ΕΥΧΑΡΙΣΤΙΕΣ

Θέλω να ευχαριστήσω την Επιβλέπουσα Καθηγήτρια, Εμπορικού Δικαίου στο Πανεπιστήμιο Πειραιώς, κυρία Σινανιώτη-Μαρούδη Αριστέα για την αμέριστη βοήθεια της κατά τη διάρκεια της συγγραφής της Μεταπτυχιακής Διατριβής μου.

ΠΡΟΛΟΓΟΣ

Η ψηφιακή επανάσταση και οι επιπτώσεις αυτής στη σημερινή εποχή φαίνονται σε όλους τους τομείς της καθημερινής μας ζωής. Η αλματώδης εξάπλωση της χρήσης του διαδικτύου και η ραγδαία ανάπτυξη του ηλεκτρονικού εμπορίου (e-commerce) και του ηλεκτρονικού επιχειρείν είχαν σαν αποτέλεσμα την αλλαγή στις συνήθειες και στον τρόπο ζωής των ατόμων.

Οι ανάγκες των καταναλωτών αυξανόμενες με ταχύτατους ρυθμούς και η επιθυμία τους για καλύτερες υπηρεσίες, οδήγησαν τις τράπεζες να εντάσσουν όλο και περισσότερες νέες διαδικτυακές υπηρεσίες για την καλυτερη εξυπηρέτηση αυτών.

Η παρούσα Διπλωματική Εργασία εστιάζει στην αναλυτική παρουσίαση της Κινητής Τραπεζικής (Mobile Banking) και των προεκτάσεων της στην Ελλάδα.

Στο πρώτο κεφάλαιο αναλύονται οι βασικές έννοιες του E-Banking και πιο συγκεκριμένα οι παρεχόμενες υπηρεσίες, οι χρησιμοποιούμενες τεχνολογίες.

Στο δεύτερο κεφάλαιο περιγράφεται το M-Banking οι φορείς και τα οφέλη τόσο για τις τράπεζες όσο και για τους καταναλωτές.

Στο τρίτο κεφάλαιο περιγράφονται η οργάνωση του τραπεζικού συστήματος ανάλογα με τις εκάστοτε τεχνολογίες και τα χαρακτηριστικά της τεχνολογίας που χρησιμοποιείται.

Στο τέταρτο κεφάλαιο επιχειρείται μία θεωρητική προσέγγιση των απαιτήσεων και τεχνικών ασφαλείας που έχει ένα τέτοιο σύστημα και που χρησιμοποιούνται για την διεκπεραίωση συναλλαγών με την χρήση του κινητού τηλεφώνου.

Στο πέμπτο κεφάλαιο περιγράφονται τα χαρακτηριστικά του M-Banking στις Ελληνικές Τράπεζες.

Στο έκτο κεφάλαιο διατυπώνονται τα συμπεράσματα και η μελλοντική εξέλιξη των συναλλαγών μέσω κινητού τηλεφώνου.

Στο έβδομο κεφάλαιο δίνεται το Νομοθετικό Πλαίσιο που διέπει την Ηλεκτρονική Τραπεζική.

ABSTRACT

The digital revolution and the impact that nowadays appear in all areas of our daily life. The dramatic rise of the Internet and the rapid development of electronic commerce (e-commerce) and electronic business resulted in a change in the habits and lifestyles of people. Consumer needs are growing rapidly and the desire for better services, led banks to integrate more and more new online services to better serve them.

This thesis focuses on the detail of Mobile Banking (Mobile Banking) and its extensions in Greece.
The first chapter analyzes the basic concepts of E-Banking and in particular the services, the technologies used.

The second chapter describes the M-Banking institutions and benefits for both banks and consumers.
The third chapter describes the organization of the banking system depending on the technologies and the characteristics of the technology used.

The fourth chapter is a theoretical approach to the requirements and technical security has such a system and used to carry out transactions using mobile phone.

The fifth chapter describes the features of the M-Banking in Greek banks.

In the sixth chapter sets out the conclusions and the future development of mobile trading. In the seventh chapter provides the legislative framework governing Electronic Banking.

ΚΕΦΑΛΑΙΟ 1° Νέες Τεχνολογίες και Τραπεζικές υπηρεσίες E-Banking-Βασικές Έννοιες.

ΚΕΦΑΛΑΙΟ 2° M-BANKING

ΚΕΦΑΛΑΙΟ 3° ΤΕΧΝΟΛΟΓΙΑ ΤΟΥ M-BANKING

ΚΕΦΑΛΑΙΟ 4° ΑΣΦΑΛΕΙΑ ΤΟΥ M-BANKING

ΚΕΦΑΛΑΙΟ 1° Νέες Τεχνολογίες και Τραπεζικές υπηρεσίες E-Banking-Βασικές Έννοιες.

1.1. Η έννοια της Ηλεκτρονικής Τραπεζικής (Electronic - Banking)

Στο παγκόσμιο τραπεζικό σύστημα οι ανάγκες των πελατών για φορητότητα οδήγησαν στη απελευθέρωση του τραπεζικού ανταγωνισμού και γενικότερα στη ραγδαία ανάπτυξη εναλλακτικών δικτύων εξυπηρέτησης. Η σύγκλιση όλων των οικονομιών παγκοσμίως και η διάδοση του ηλεκτρονικού εμπορίου ήταν η αφορμή για τεχνολογικές εξελίξεις στον τομέα των τηλεπικοινωνιών. Η διενέργεια συναλλαγών μέσω των τεχνολογιών της πληροφορικής δίνουν την δυνατότητα στις Τράπεζες να αλληλεπιδρούν με τους πελάτες τους μέσα από τα ηλεκτρονικά κανάλια διανομής όπως είναι:

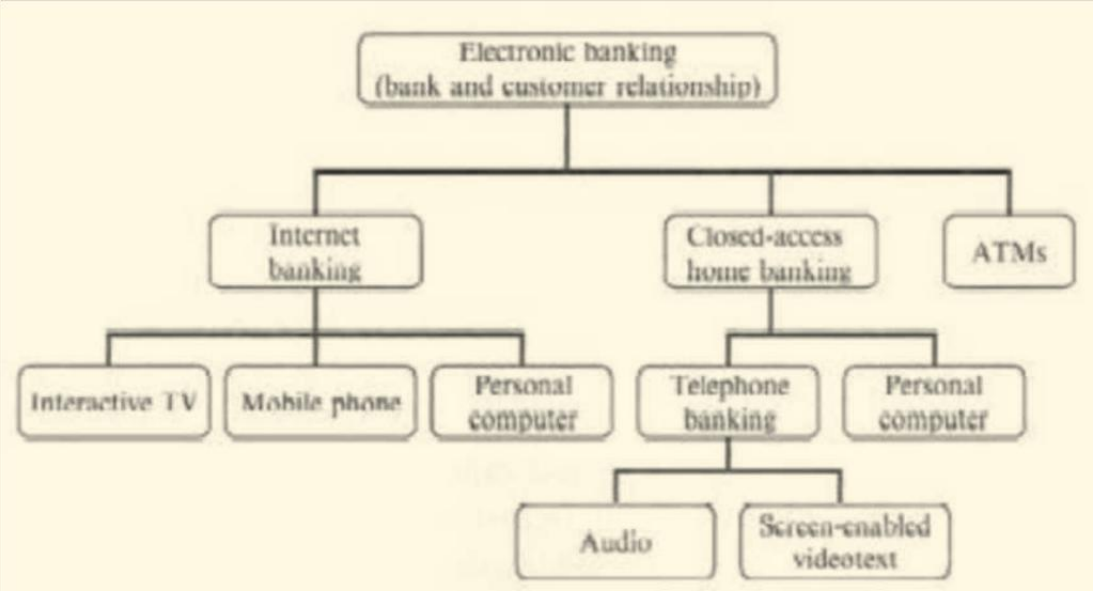
- τα ATM,
- τα κέντρα εξυπηρέτησης μέσω διαδικτύου (Internet Banking ή PC Banking),
- τα κέντρα τηλεφωνικής υποστήριξης (Phone Banking),
- τα κέντρα εξυπηρέτησης μέσω Κινητού Τηλεφώνου (M-Banking).

Με το e-Banking εννοούμε την αυτοποιημένη παροχή νέων και παραδοσιακών προϊόντων χρηματοοικονομικής φύσης και υπηρεσιών, χωρίς τη φυσική παρουσία του πελάτου στο κατάστημα για να ολοκληρώσει μια συναλλαγή. Ακόμα και από το εξωτερικό μπορεί να την ολοκληρώσει, καταργώντας τα σύνορα και εκμηδενίζοντας τις αποστάσεις. Δεν χρειάζεται κάποιο εξεζητημένο λογισμικό για να χρησιμοποιήσει το e-Banking, χρειάζεται απλά έναν ηλεκτρονικό υπολογιστή. Τα websites των τραπεζών δεν κλείνουν ποτέ (ίσως μόνο κατά τη διαδικασία συντήρησης) και είναι έτοιμα για χρήση 24 ώρες το 24ωρο. Είναι λοιπόν αντιληπτό ότι το τραπεζικό κατάστημα 'απέχει' όσο ένα πάτημα ενός κουμπιού στον υπολογιστή.

Παρόλο που το ενσύρματο και το ασύρματο δίκτυο είναι η ίδια έννοια, υπάρχουν διάφοροι παράγοντες που διαφέρουν:

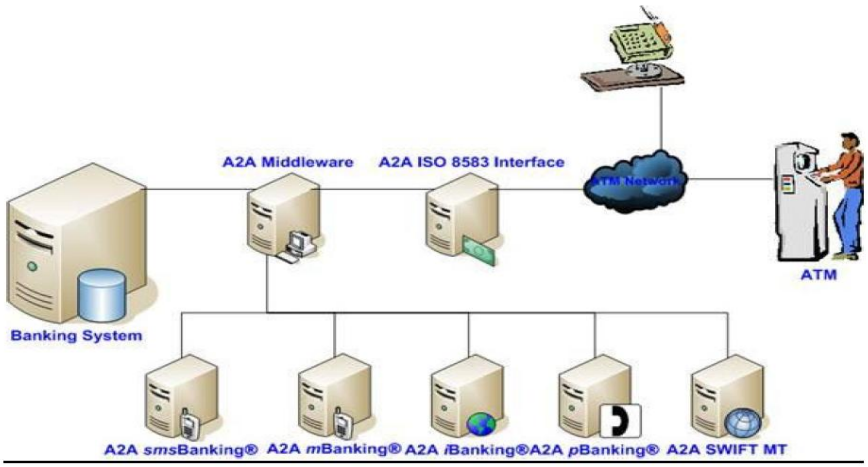
1. Οι φορητές συσκευές μπορεί να είναι συνεχώς συνδεδεμένες στο Διαδίκτυο και να μεταφέρονται σε διαφορετικά μέρη, χωρίς να χρειάζονται κάποια καλωδίωση για τη σύνδεση
2. Η γεωγραφική θέση μιας φορητής συσκευής μπορεί να είναι σταθερή και να παρακολουθείται μέσω του ασύρματου σήματός της, παρέχοντας έτσι υπηρεσίες και δραστηριότητες που εξαρτώνται από την θέση του χρήστη.
3. Οι φορητές συσκευές επιτρέπουν την συνύπαρξη πιο προσωπικών εφαρμογών που ανταποκρίνονται στο στυλ της ζωής του χρήστη (για παράδειγμα τηλεφωνία φωνής, ημερολόγιο, χρονοδιάγραμμα συναντήσεων, διευθύνσεις και άλλα προσωπικά δεδομένα). Οι ασύρματες Internet υπηρεσίες μπορούν να προσαρμοστούν από τον χρήστη.
4. Οι ασύρματες συσκευές έχουν την ευελιξία να συνδέονται σε διάφορα δίκτυα, μέσω τεχνολογίας Bluetooth, όποτε βρίσκονται στο εύρος ενός ενσωματωμένου δικτύου ή συσκευής (για παράδειγμα ενσωματωμένα δίκτυα δεδομένων σε αυτοκίνητα, σε σπίτια ή γραφεία).

Σχήμα 1: Μέθοδοι Επικοινωνίας και Συσκευές Πρόσβασης στην Ηλεκτρονική Τραπεζική



Πηγή: (Apostolos Ath. Gkoutzinis, 2006)

Σχήμα 2: Τα είδη του e-Banking και η διασύνδεση του σε ένα κοινό τραπεζικό σύστημα.



1.2. ATM

Ο διεθνής όρος Automatic Teller Machines (ATM) αποδίδεται στην ελληνική βιβλιογραφία ως Αυτόματες Ταμειολογιστικές Μηχανές. Το ATM αποτελεί ουσιαστικά μέρος του υπολογιστικού συστήματος της τράπεζας και αποτελείται από δύο βασικά τμήματα:

- *το ηλεκτρονικό τμήμα* που βοηθάει στην αποστολή και λήψη στοιχείων και
- *ένα μηχανικό τμήμα*, το οποίο καταμετρά με ακρίβεια τα χαρτονομίσματα και εκδίδει τις αποδείξεις για τους χρήστες.

Ουσιαστικά αποτελούν τον προπομπό των αυτόματων συναλλαγών και με τη χρήση αυτής της τεχνολογίας τα τραπεζικά ιδρύματα πέτυχαν την αποσυμφόρηση των γκισέ των ταμείων των καταστημάτων τους. Τα μηχανήματα αυτά έχουν τη δυνατότητα να εξυπηρετήσουν τον πελάτη 24 ώρες το 24ωρο. Το μόνο που χρειάζεται είναι μια μαγνητική κάρτα και ένας προσωπικός κωδικός αριθμός (PIN).

Οι ATMs μηχανές μπορούν να διακριθούν σε τρεις κατηγορίες ανάλογα με το μέρος που είναι εγκατεστημένες. Οι κατηγορίες είναι οι εξής:

- ✓ *Through the Wall.* Τα μηχανήματα βρίσκονται εξωτερικά των τραπεζικών καταστημάτων και εξωτερικά άλλων κτιρίων σε στρατηγικά σημεία στην πόλη και είναι έτοιμα για χρήση από τον πελάτη.
- ✓ *In the Lobby*. Τα ATM σε αυτήν την περίπτωση βρίσκονται στο εσωτερικό των τραπεζικών ιδρυμάτων αλλά και πολυκαταστημάτων, εμπορικών κέντρων και μεγάλων Super Markets.
- ✓ *Vestibule*. Αυτά τα μηχανήματα τοποθετούνται σε ειδικά διαμορφωμένους γυάλινους προθάλαμους τραπεζικών καταστημάτων. Μπορούν να λειτουργήσουν και εκτός εργάσιμων ωρών και θεωρούνται πιο ασφαλή μηχανήματα αφού είναι αδύνατο να παραβιαστούν. (Κωνσταντίνος Λυμπερόπουλος, 1994).

1.3. Internet Banking- PC Banking –e Banking

Το Internet Banking ή Personal Computer Banking επιτρέπει στο πελάτη να κάνει πολλές τραπεζικές συναλλαγές μέσω του προσωπικού του υπολογιστή χρησιμοποιώντας το διαδίκτυο ως κανάλι διανομής. Η οθόνη του υπολογιστή παίζει το ρόλο του προσωπικού ταμείου. Το μόνο που χρειάζεται για την διεξαγωγή των τραπεζοοικονομικών του συναλλαγών είναι φυσικά το διαδίκτυο, έναν πάροχο διαδικτύου, έναν Η/Υ και από την τράπεζα ένα Website στο οποίο θα μπορεί οποιαδήποτε ώρα, με έναν κωδικό πρόσβασης, να βλέπει όλες τις πληροφορίες που αφορούν τον λογαριασμό του.

Στην Ελλάδα, μόνο το 49% των ελληνικών επιχειρήσεων που χρησιμοποιούν internet λαμβάνουν σήμερα υπηρεσίες e-banking. Αντίθετα, διεθνώς το web banking αναδεικνύεται ως ένα από τα ισχυρότερα κίνητρα για την αρχική ηλεκτρονική ενεργοποίηση των επιχειρήσεων. (Ίδρυμα Οικονομικών και Βιομηχανικών Ερευνών, (2007),'Μελέτη των κλάδων Πληροφορικής και Τηλεπικοινωνιών στην Ελλάδα: Κατάσταση και Προοπτικές')

Με το Internet Banking ο πελάτης μπορεί να λάβει τις παρακάτω υπηρεσίες:

- ✓ *Να λαμβάνει πληροφορίες για:*
  - Λογαριασμούς
  - Πιστωτικές Κάρτες
  - Χαρτοφυλακίου
  - Δανείων
  - Επιταγών
- ✓ *Να πληρώσει λογαριασμούς αλλά και*
  - Πληρωμές πιστωτικών καρτών του ιδίου αλλά και τρίτου
  - Πληρωμές καρτών άλλων τραπεζών
  - Πληρωμές δημοσίου

- ✓ *Να κάνει αίτηση μεταφοράς κεφαλαίων:*
  - Εντός τραπέζης σε λογαριασμούς του ιδίου
  - Εντός τραπέζης σε λογαριασμούς τρίτων
  - Εκτός τραπέζης- Εμβάσματα
- ✓ *Εκτέλεση εντολών:*
  - Μισθοδοσίας
  - Χρηματιστηριακές εντολές

1.4. Phone Banking

Το Phone Banking αναφέρεται στις τραπεζικές συναλλαγές που γίνονται μέσω τηλεφώνου ή άλλων συσκευών. Οι τραπεζικές συναλλαγές μπορούν να γίνουν από όποιο μέρος βρίσκεται ο πελάτης, ακόμα και στο εξωτερικό, με ένα μόνο τηλεφώνημα. Στόχος είναι η εκμετάλλευση της υπάρχουσας υποδομής αλλά και το γεγονός οτι το τηλέφωνο αποτελεί την πλέον διαδεδομένη τεχνολογία σε όλα τα κοινωνικά στρωμάτα.

Οι υπηρεσίες που προσφέρει το Phone-Banking χωρίζονται σε δύο κατηγορίες:

- ✓ *Διεκπεραίωση από υπάλληλο- πράκτορα (agent) μέσω τηλεφωνικού κέντρου (call center).* Εξειδικευμένοι υπάλληλοι, με την βοήθεια συστημάτων (CTI, CRM Customer Relationship Managment), καθοδηγούν τον πελάτη για τις απαραίτητες ενέργειες που πρέπει να κάνει για να ικανοποιηθεί το αίτημα του. Ο χρήστης έχει στη διάθεση του το απαιτούμενο PIN για την πιστοποίηση των συναλλαγών.
- ✓ *Αυτόματες διεκπεραιώσεις μέσω συστήματος αναγνώρισης φωνής (IVRs) και συσκευών ηχητικών τόνων (tone pad).* Ο χρήστης χωρίς την παρέμβαση ανθρώπινου παράγοντα με απαραίτητα εργαλεία μόνο ένα καλωδικό τηλέφωνο και την ύπαρξη ενός προσωπικού κωδικού πιστοποιήται ώστε να ολοκληρωθεί το αίτημα του.

Το Phone Banking παραμένει πιο ακριβό για την τράπεζα και λιγότερο ασφαλές για τον πελάτη, αφού δεν είναι εύκολη η αναγνώριση φωνής του πελάτη μέσω τηλεφώνου. Από την πρώτη υιοθέτηση αυτής της τεχνολογίας μέχρι σήμερα πολλά έχουν αλλάξει και συνεχώς βελτιώνεται.

Οι διαθέσιμες συναλλαγές είναι:

- ✓ Ενεργοποίησης και ακύρωσης κάρτας ανάληψης χρημάτων
- ✓ Αλλαγή στοιχείων αλληλογραφίας κατόχων καρτών
- ✓ Ακυρώσεις πιστωτικών καρτών
- ✓ Ανάλυση υπολοίπου των λογαριασμών
- ✓ Κίνηση λογαριασμού
- ✓ Ανάλυση υπολοίπου πιστωτικών καρτών και ενημέρωση κινήσεων
- ✓ Έκδοση και ανάκληση μπλοκ επιταγών
- ✓ Μεταφορές- Πληρωμές

- ✓ Αιτήσεις
- ✓ Αλλαγή κωδικών ασφαλείας
- ✓ Ενημέρωση για τις διαθέσιμες υπηρεσίες της τράπεζας

1.5. Mobile Banking

Το M-Banking αποτελεί έναν εξελισσόμενο τομέα της Ηλεκτρονικής Τραπεζικής. Επιτρέπει την άμεση διενέργεια συναλλαγών μέσω κινητών τηλεφώνων και πάντα με την χρήση της τεχνολογίας WAP έτσι ώστε να μπορεί να συνδεθεί και στο διαδίκτυο. Οι τραπεζικοί οργανισμοί έχουν επενδύσει στον τομέα αυτόν, αυξάνοντας το εύρος της αποδοτικότητας, για καλύτερη εξυπηρέτηση πελατών (customer service) και μειώνοντας το κόστος έχοντας ένα ανταγωνιστικό πλεονέκτημα. Φυσικά η ανάπτυξη αυτή οφείλεται στη δυναμικότητα και διαθεσιμότητα της κινητής τηλεφωνίας παγκοσμίως καθώς το κινητό τηλέφωνο εκτός από μία υπερσύγχρονη υπολογιστική μηχανή είναι πρώτα από όλα μία κινητή «έξυπνη» φωνητική συσκευή για την πραγματοποίηση τραπεζικών συναλλαγών.

Το mobile banking (m-banking) στην Ελλάδα είναι ακόμα σε εμβρυακή κατάσταση, παρά τις προσπάθειες ορισμένων τραπεζών για τη διάδοσή του.

ΚΕΦΑΛΑΙΟ 2° M-BANKING

2.1. Βασικοί Φορείς του Mobile-Banking

Mobile Banking, δηλαδή η μεταφορά τραπεζικών υπηρεσιών στο κινητό τηλέφωνο είναι νέο πεδίο δοκιμών για τις τράπεζες. Μέσω αυτών οι χρήστες λαμβάνουν ειδοποιήσεις σύμφωνα με προκαθορισμένες παραμέτρους, διαχειρίζονται λογαριασμούς, πραγματοποιούν πληρωμές και μεταφέρουν κεφάλαια. Αν υπολογίσει κανείς την αναλογία κινητών τηλεφώνων και προσωπικών υπολογιστών σε σχέση με τον πληθυσμό, θα διαπιστώσει ότι τα πρώτα κερδίζουν κατά κράτος. Δεν είναι τυχαίο λοιπόν, που οι τράπεζες έχουν αρχίσει να διερευνούν ένα νέο πολλά υποσχόμενο τραπεζικό κανάλι. Οι υπηρεσίες M-Banking βασίζονται σε ένα σύνθετο οικοσύστημα συνεργασίας διαφόρων φορέων, οι οποίοι ενωμένοι δημιουργούν την κατάλληλη υποδομή για τη λειτουργία των κινητών οικονομικών υπηρεσιών.

Οι κύριοι πρωταγωνιστές στο χώρο είναι:

- ➢ οι εταιρείες κινητής τηλεφωνίας,
- ➢ κατασκευάστριες εταιρείες φορητών συσκευών,
- ➢ κατασκευάστριες εταιρείες λογισμικού,
- ➢ κατασκευάστριες εταιρείες πιστωτικών καρτών,
- ➢ τηλεπικοινωνιακοί φορείς,
- ➢ οι οικονομικοί οργανισμοί, έμποροι και παροχείς,
- ➢ οι καταναλωτές.

Στο μοντέλο αυτό οι εταιρείες κινητής προσφέρουν την υποδομή που διασυνδέει τους άλλους πρωταγωνιστές. Οι τηλεπικοινωνιακοί φορείς, το διαδικτυακό κανάλι,οι έμποροι και οι παροχείς προσφέρουν το μηχανισμό αγορών και οι καταναλωτές αγοράζουν και καταναλώνουν προϊόντα και υπηρεσίες.

Μία από τις ισχυρότερες τάσεις που παρατηρούνται στον τραπεζικό χώρο τα τελευταία χρόνια σχετίζεται με την πρόθεση των τραπεζών να απομακρύνουν το πελατειακό κοινό τους από τα καταστήματα. Οι λόγοι ποικίλουν και σχετίζονται κυρίως με το υψηλό κόστος λειτουργίας των φυσικών καταστημάτων.

Η τεχνολογία συνέβαλε τα μέγιστα στο άνοιγμα νέων -εναλλακτικών προς το τραπεζικό γκισέ- καναλιών, ορισμένα από τα οποία έχουν κερδίσει ήδη σημαντικό μερίδιο αγοράς και την εμπιστοσύνη των χρηστών. Γενικά, στόχος των τραπεζών είναι η διεύρυνση του αριθμού των διαθέσιμων καναλιών, ώστε οι πελάτες ανάλογα με το επίπεδο εξοικείωσής τους με τις νέες τεχνολογίες να επιλέγουν το κανάλι που τους ταιριάζει.

Μπορεί τα ATMs και το Internet Banking να αποτελούν τα πιο δημοφιλή εναλλακτικά κανάλια, αλλά το Mobile Banking δείχνει να κερδίζει συνεχώς έδαφος. Με αυτό τον όρο περιγράφεται γενικά η πραγματοποίηση τραπεζικών συναλλαγών και άλλων σχετικών ενεργειών μέσω φορητών συσκευών και των δικτύων κινητής τηλεφωνίας.

2.2. Υπηρεσίες που προσφέρει το Mobile Banking

Το φάσμα των παρεχόμενων υπηρεσιών περιλαμβάνει συνήθως τα εξής:

- Κινήσεις λογαριασμών (πληρωμές λογαριασμών, μεταφορές χρημάτων κ.ά.)
- Διαχείριση λογαριασμών (διαχείριση πρόσβασης, αίτηση έκδοσης μπλοκ επιταγών κ.ά.)
- Πληροφορίες λογαριασμών (αναζήτηση ισοζυγίου, κατάσταση λογαριασμού κ.ά.)
- Οικονομικές πληροφορίες (τιμή συναλλάγματος, επιτόκια κ.ά.)
- Χρηματιστηριακές συναλλαγές (αγορά/πώληση μετοχών κ.ά.)
- Προϊόντα και προσφορές της τράπεζας.
- Ανεύρεση των κοντινότερων ATMs και καταστημάτων τραπεζών.
- Χρήσιμα εργαλεία όπως μετατροπέα συναλλάγματος.

Πιο αναλυτικά:

ΠΛΗΡΟΦΟΡΙΕΣ ΛΟΓΑΡΙΑΣΜΩΝ

- Διαχείρηση λογαριασμών-Καταθέσεις
  - ✓ Κατάσταση λογαριασμού
  - ✓ Υπόλοιπο λογαριασμού
  - ✓ Τελευταίες κινήσεις καταθετικού λογαριασμού
  - ✓ Πάγιες Εντολές
  - ✓ Κατάσταση Επιταγών
  - ✓ Alert συναλλαγών
- Διαχείρηση Πιστωτικών Καρτών
  - ✓ Υπόλοιπο Πιστωτικής
  - ✓ Τελευταίες κινήσεις πιστωτικής κάρτας (statement)
- Διαχείρηση Δανείων
  - ✓ Υπόλοιπο δανειακού λογαριασμού
  - ✓ Τελευταίες κινήσεις δανειακού λογαριασμού
  - ✓ Πίνακας δόσεων δανείου
  - ✓ Alert συναλλαγών
- Επενδύσεις
  - ✓ Χαρτοφυλάκειο μετοχών

- ✓ Χαρτοφυλάκειο αμοιβαίων κεφαλαίων
- ✓ Κατάσταση ΧΑΑ
- ✓ Κατάσταση αμοιβαίων κεφαλαίων της Τράπεζας
- ✓ Τιμές συναλλάγματος

ΚΙΝΗΣΗ ΚΕΦΑΛΑΙΩΝ

- Χρηματοοικονομικές συναλλαγές
  - ✓ Μεταφορά χρημάτων μεταξύ λογαριασμών ιδίου δικαιούχου
  - ✓ Μεταφορά χρημάτων μεταξύ λογαριασμών διαφορετικών δικαιούχων
  - ✓ Έμβασμα σε μετρητά
  - ✓ Διατραπεζική μεταφορά εσωτερικού Δίας (Dias Debit)
  - ✓ Διατραπεζική μεταφορά εξωτερικού
  - ✓ Αγορά/Πώληση μετοχών ΧΑΑ
  - ✓ Αγορά/Εξαγορά μεριδίων της Τράπεζας

ΠΛΗΡΩΜΕΣ ΟΦΕΙΛΩΝ

- Δάνεια-Πιστωτικές Κάρτες
  - ✓ Δόση δανείου
  - ✓ Κάρτα εκδόσεως της Τράπεζας ιδίου κατόχου
  - ✓ Κάρτα εκδόσεως της τράπεζας τρίτων
- Δημόσιο-ΔΕΚΟ
  - ✓ Είσπραξη Φόρου Εισοδήματος Φ.Π
  - ✓ Τέλη κυκλοφορίας
  - ✓ Φ.Π.Α
  - ✓ Ι.Κ.Α
  - ✓ ΟΑΕΕ
  - ✓ ΔΕΗ
  - ✓ ΕΥΔΑΠ
  - ✓ ΟΤΕ
- Πάγιες εντολές πληρωμών
  - ✓ Πληρωμή μισθοδοσίας
  - ✓ Άλλων Εταιριών
  - ✓ Τηλεφωνία (σταθερή-κινητή)
  - ✓ Ασφάλειες
  - ✓ Αλυσίδες καταστημάτων
  - ✓ Παροχών

ΔΙΑΧΕΙΡΙΣΗΣ ΛΟΓΑΡΙΑΣΜΩΝ

- Αιτήσεις
  - ✓ Άνοιγμα λογαριασμού
  - ✓ Αλλαγή UserID και Password
  - ✓ Έκδοση καρνέ επιταγών
  - ✓ Χορήγηση πιστωτικής κάρτας
  - ✓ Χορήγηση κάρτας μετρητών (cache card)
  - ✓ Χορήγηση κάρτα ασφαλών συναλλαγών (safe card)
  - ✓ Χορήγηση δανείου
  - ✓ Αποστολή ενημερώσεων
  - ✓ Ενεργοποίηση/Απενεργοποίηση alert συναλλαγών

Η διάθεση των υπηρεσιών βασίζεται συνήθως σε τεχνολογίες SMS ή στο πρωτόκολλο WAP, ενώ τόσο στην Ιαπωνία όσο και σε ευρωπαϊκές χώρες –όπου υποστηρίζεται- η τεχνολογία είναι διαθέσιμη και μέσω του i-mode. Οι συσκευές που συνήθως χρησιμοποιούνται για τις συγκεκριμένες υπηρεσίες είναι κινητά τηλέφωνα (κυρίως smart phones) ή PDAs ανάλογα με τις προδιαγραφές της υπηρεσίας.

Οι υπηρεσίες του Mobile Banking διακρίνονται σε δύο βασικές κατηγορίες όσον αφορά στην προέλευσή τους στις:

- *"push"* και
- *"pull"*.

Στην κατηγορία "push" η τράπεζα αποστέλλει πληροφορίες βασισμένες σε προσυμφωνημένους με τον πελάτη κανόνες - π.χ. αποστέλλει ειδοποίηση στον πελάτη στην περίπτωση που ο λογαριασμός του βρεθεί κάτω από ένα καθορισμένο επίπεδο.
Αντίθετα, στην κατηγορία "pull" προηγείται η αποστολή αιτήματος στην τράπεζα από τον πελάτη και ακολουθεί η απάντηση της τράπεζας - π.χ. η τράπεζα αποστέλλει στον πελάτη στοιχεία σχετικά με τις τελευταίες κινήσεις ενός λογαριασμού κατόπιν αιτήματός του.

Ένας άλλος τρόπος διαφοροποίησης των υπηρεσιών Mobile Banking αφορά στην ίδια τη φύση τους και προβλέπει διαχωρισμό τους σε δύο κατηγορίες:

- *σε υπηρεσίες ελέγχου* και
- *σε υπηρεσίες συναλλαγών*.

Έτσι, αίτημα για την κατάσταση ενός τραπεζικού λογαριασμού ανήκει στην πρώτη κατηγορία, ενώ αίτημα μεταφοράς κεφαλαίων σε έτερο λογαριασμό ανήκει στη δεύτερη. Σημαντικό στοιχείο που διαφοροποιεί τις δύο υπηρεσίες είναι το ότι οι υπηρεσίες συναλλαγών απαιτούν υψηλότερο βαθμό ασφάλειας στο κανάλι που συνδέει το κινητό τηλέφωνο με τους servers της τράπεζας.

Στην Ελλάδα όπως συμβαίνει και σε παγκόσμιο επίπεδο, η τραπεζική μέσω κινητού τηλεφώνου αποτελεί το νεότερο εναλλακτικό κανάλι. Για το λόγο αυτό συνιστά τοπίο υπό διαμόρφωση, όπου οι περισσότερες ελληνικές τράπεζες έχουν μεν παρουσία, κρατούν δε διερευνητική στάση. Συγκεκριμένα, οι επιλογές των εφικτών συναλλαγών είναι περιορισμένες σε σύγκριση με τα υπόλοιπα κανάλια, ενώ σε πολλές περιπτώσεις υπάρχει όριο συναλλαγών.

Η μετάβαση στο Mobile Banking εντάσσεται στο "anywhere banking", ένα στρατηγικό πλάνο των τραπεζών που προβλέπει τραπεζικές υπηρεσίες διαθέσιμες οπουδήποτε υπάρχει

ζήτηση. Ενώ το Internet Banking έχει καταργήσει τα χρονικά όρια των τραπεζικών συναλλαγών, προϋποθέτει τη φυσική παρουσία του πελάτη κοντά σε υπολογιστή με σύνδεση στο Internet.

Στην περίπτωση του Mobile Banking καταργείται και ο γεωγραφικός περιορισμός, αφού ο πελάτης της τράπεζας μπορεί ανά πάσα στιγμή να πραγματοποιεί συναλλαγές χωρίς επιπρόσθετο εξοπλισμό πλην της φορητής συσκευής του. Στο πρόσφατο World Retail Banking Report, που συνέταξε η γνωστή εταιρεία ερευνών Capgemini, η διεύρυνση των επιλογών Mobile Banking αποτελεί μία από τις δύο σημαντικότερες αλλαγές που θα συντελεστούν στο προσεχές μέλλον στον τομέα των οικονομικών υπηρεσιών. Σύμφωνα με την έρευνα, για ορισμένες τράπεζες η έμφαση μετατοπίζεται από τα μέτρα περιορισμού των δαπανών (π.χ. καθοδήγηση των πελατών προς αυτοματοποιημένες υπηρεσίες τραπεζικής) στην αύξηση των εσόδων τους, κίνηση που η Capgemini αναφέρει ως απόκτηση μεγαλύτερου μεριδίου από το 'πορτοφόλι του πελάτη'. Η επιτυχής μετατόπιση του στόχου των τραπεζών προϋποθέτει την ανάπτυξη μεγαλύτερης οικειότητας με τον πελάτη, γεγονός που δεν είναι τόσο αυτονόητο όσο φαίνεται, καθώς συνεχίζονται οι συγχωνεύσεις στην αγορά της λιανικής τραπεζικής και οι μεγάλοι παίκτες μετατρέπονται σε παγκόσμιες οντότητες. Έτσι, ένας από τους τρόπους με τους οποίους οι τράπεζες θα επιχειρήσουν να διατηρήσουν την καλή πίστη των πελατών τους είναι η προσέγγισή τους μέσω καναλιών μέχρι πρότινος ανεξερεύνητων, όπως η ηλεκτρονική τραπεζική μέσω κινητών τηλεφώνων. Η εξάπλωση του Mobile Banking αναμένεται να είναι ισχυρότερη στις αναπτυσσόμενες αγορές, σύμφωνα με την Capgemini, λόγω έλλειψης υποδομής, γεγονός που δυσχεραίνει την ανάπτυξη άλλων ηλεκτρονικών τραπεζικών καναλιών.

2.3. Χαρακτηριστικά του M-Banking

Το κινητό τηλέφωνο παρέχει, όχι μόνο φορητή ευελιξία, αλλά και νέες επαγγελματικές δυνατότητες, ιδιαίτερα σε προϊόντα και υπηρεσίες που εξαρτώνται από την θέση του χρήστη. Το κινητό έχει και το πλεονέκτημα του μεγαλύτερου εύρους σύνδεσης. Μια φορητή συσκευή είναι πάντα μαζί με τον χρήστη, 24 ώρες την ημέρα και 7 μέρες την εβδομάδα.

Το M-Banking μπορεί αποτελεσματικά να ενσωματωθεί στην καθημερινή ζωή ενός χρήστη, τόσο στον εργασιακό τομέα όσο και στον ελεύθερο χρόνο του. Αυτές οι λειτουργίες δεν είναι άμεσα διαθέσιμες στην πρόσβαση στο Internet από ένα Ηλεκτρονικό Υπολογιστή σε μια σταθερή θέση.Έτσι η σχεδίαση των υπηρεσιών γίνεται με βάση συγκεκριμένα χαρακτηριστικά που θα οδηγήσουν στην καθιέρωση του M-Banking και κυρίως στην προσέλκυση νέων πελατών.

Τα χαρακτηριστικά είναι τα ακόλουθα:

- **ΕΥΚΟΛΙΑ ΕΚΜΑΘΗΣΗΣ**.

  Η εκμάθηση μίας υπηρεσίας εξαρτάται κυρίως από την ευκολία κατανόησης της λειτουργίας της.

- **ΑΛΛΗΛΕΠΙΔΡΑΣΗ.**

  Ο χρήστης αλληλεπιδρά με την παρεχόμενη υπηρεσία και η επιτυχία της αλληλεπίδρασης εξαρτάται κυρίως από την κατανόηση των μηνυμάτων που θα λάβει ως απάντηση στις ενέργειες του.

- **ΕΥΚΟΛΗ ΧΡΗΣΗ.**

  Η ευχρηστία μίας υπηρεσίας εξαρτάται κυρίως από την υλοποίηση συμβάσεων χρηστικότητας (interfaces), κατανοητών από το μέσο χρήστη.

- **ΚΑΤΑΛΛΗΛΟΤΗΤΑ ΣΧΕΔΙΑΣΜΟΥ**.

  Ο σχεδιασμός μίας υπηρεσίας εξαρτάται κυρίως από την άποψη του πελάτη για το ύφος που πρέπει να έχει η προσφερόμενη υπηρεσία.

- **ΘΕΤΙΚΗ ΕΜΠΕΙΡΙΑ.**

  Εκφράζει τη συνολική αίσθηση που αποκομίζει ο χρήστης και εξαρτάται από τις προσδοκίες που έχει διαμορφωσει.

- **ΕΠΑΡΚΕΙΑ.**

  Η επάρκεια μίας υπηρεσίας εξαρτάται από την αποτελεσματική κάλυψη των απαιτήσεων των χρηστών της.

- **ΑΚΡΙΒΗΣ ΠΛΗΡΟΦΟΡΗΣΗ.**

  Εκφράζει την αίσθηση για την ορθότητα της πληροφόρησης που αποκομίζει ο πελάτης και εξαρτάται από το περιεχόμενο της πληροφόρησης.

- **ΑΞΙΟΠΙΣΤΗ ΠΛΗΡΟΦΟΡΗΣΗ.**

  Εξαρτάται κυρίως από το πόσο ακριβείς είναι οι πληροφορίες που παρέχει.

- **ΕΠΙΚΑΙΡΗ ΠΛΗΡΟΦΟΡΗΣΗ.**

  Εξαρτάται από την συχνότητα ανανέωσης των πληροφοριών.

- **ΕΠΑΡΚΗΣ ΠΛΗΡΟΦΟΡΗΣΗ.**

  Εξαρτάται κυρίως από την ποσότητα των πληροφοριών της.

- **ΣΧΕΤΙΚΗ ΠΛΗΡΟΦΟΡΗΣΗ.**

  Εξαρτάται κυρίως από το περιεχόμενο των πληροφοριών και πόσο είναι σχετικό με την δραστηριότητα της συνεργαζόμενης τράπεζας.

- **ΚΑΤΑΝΟΗΤΗ ΠΛΗΡΟΦΟΡΗΣΗ.**

  Εξαρτάται από τη γλώσσα- έκφραση που χρησιμοποιείται. Η χρήση επαγγελματικής ορολογίας και εκφράσεων μη διαδεδομένων στο κοινό, μειώνουν δραστικά το βαθμό κατανόησης της πληροφορίας.

- **ΣΩΣΤΗ ΠΑΡΟΥΣΙΑΣΗ ΠΛΗΡΟΦΟΡΗΣΗΣ.**

  Εξαρτάται από την αποτελεσματική χρήση των μέσων που χρησιμοποιούνται για την παρουσίαση των πληροφοριών (κείμενο, γραφήματα, πίνακες, βίντεο, μουσική,φωτογραφίες, ήχοι).

- **ΚΑΛΗ ΦΗΜΗ.**

  Εξαρτάται από την αναγνωρισιμότητα που έχει μία υπηρεσία.

- **ΑΣΦΑΛΕΙΑ ΣΥΝΑΛΛΑΓΩΝ.**

  Εξαρτάται κυρίως από τις παραμέτρουςπου συνθέτουντην αντίληψη για την ασφάλεια των συναλλαγών στα ηλεκτρονικά μέσα. Δηλαδή ευκολία σύνδεσης, χρόνος αναμονής, αξιοπιστία απόκρισης.

- **ΑΣΦΑΛΕΙΑ ΑΤΟΜΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ.**

  Εξαρτάται από τα συστήματα κρυπτογράφησης πληροφοριών που χρησιμοποιεί η τράπεζα, καθώς και τους μηχανισμούς διασφάλισης για κλοπή από τρίτους κατά τη διάρκεια της μεταφοράς δεδομένων.

- **ΕΞΑΤΟΜΙΚΕΥΣΗ.**

  Εξαρτάται κυρίως από τηνδυνατότητα που διαθέτει να προσαρμόζεται στις απαιτήσεις του χρήστη.

- **ΑΙΣΘΗΣΗ ΣΥΜΜΕΤΟΧΗΣ ΣΤΗΝ ΚΟΙΝΟΤΗΤΑ.**

- **ΔΙΕΥΚΟΛΥΝΣΗ ΕΠΙΚΟΙΝΩΝΙΑΣ ΜΕ ΤΗΝ ΤΡΑΠΕΖΑ.**

  Εξαρτάται από την παροχή λεπτομερών πληροφοριών σχετικά με τηλέφωνα και e-mail για τη δυνατότητα επικοινωνίας ανά κατάστημα, ανά διεύθυνση, ανά δραστηριότητα.

- **ΕΚΠΛΗΡΩΣΗ ΥΠΟΣΧΕΣΕΩΝ.**

  Εκφράζει τη γενική αίσθηση που λαμβάνει ένας πελάτης σχετικά με την πραγματοποίηση των δηλώσεων της τράπεζας.

- **ΕΥΚΟΛΙΑ ΠΛΟΗΓΗΣΗΣ.**

  Η πλοήγηση μίας ιστοσελίδας WAP εξαρτάται από τον τύπο της δομής των δεδομένων σε μενού και υπομενού, με τρόπο που να επιτρέπει στον επισκέπτη την πρόσβαση σε σημαντικές πληροφορίες. Η μετακίνηση θα πρέπει να γίνεται το πολύ σε τρία επίπεδα.

- **ΕΛΚΥΣΤΙΚΗ ΕΜΦΑΝΙΣΗ WAP.**

  Η εμφάνιση μίας ιστοσελίδας εξαρτάται κυρίως από την μορφοποίηση που έχει εφαρμοστεί σε αυτή.

2.4. Πλεονεκτήματα του M-Banking

Το ευρύ φάσμα των τραπεζικών υπηρεσιών και προϊόντων όλο το 24ώρο και 7 ημέρες την εβδομάδα, αλλάζει την εικόνα των πελατών σε ουρές μπροστά στα γκισέ των τραπεζών αφού καλύπτει σχεδόν όλες τις ανάγκες των χρηστών του M-Banking. Οι προοπτικές που ανοίγονται είναι σημαντικές και δίνουν την δυνατότητα προσφοράς νέων υπηρεσιών καινοτόμων και πελατοκεντρικών. Από τη μία πλευρά υπάρχει το χρηματοπιστωτικό ίδρυμα και από την άλλη ο πελάτης. Ανάμεσα στις δύο αυτές οντότητες δημιουργούνται τόσο αμφίδρομες όσο και μονόδρομες σχέσεις για την διεκπεραίωση κάθε εντολής.

2.4.1. Για τον Καταναλωτή

- **ΑΠΟΔΕΣΜΕΥΣΗ ΑΠΟ ΤΟ «ΦΥΣΙΚΟ» ΚΑΤΑΣΤΗΜΑ**. Περιορισμός των επισκέψεων στο υποκατάστημα ή στο ATM. Ο πελάτης μπορεί να πραγματοποιήσει συναλλαγές, χωρίς να χρειάζεται να γνωρίζει πιο και που είναι το κοντινότερο κατάστημα, ανεξάρτητα από τη γεωγραφική του θέση.

- **ΑΠΟΔΕΣΜΕΥΣΗ ΑΠΟ ΤΟ ΩΡΑΡΙΟ ΛΕΙΤΟΥΡΓΙΑΣ.** Ο πελάτης έχει συνεχή πρόσβαση στους τραπεζικούς λογαριασμούς του ανεξάρτητα από το αν τα υποκαταστήματα είναι ανοιχτά. Έχουμε μείωση στις εργατοώρες που χάνονται, αφού δεν είναι πλέον υποχρεωμένος να απουσιάζει από την δουλειά του.
- **ΤΑΧΥΤΕΡΗ ΔΙΕΚΠΕΡΑΙΩΣΗ.** Με τη χρήση πάγιων εντολών οι πληρωμές σε δημόσιους οργανισμούς και μη ολοκληρώνονται σε λίγα μόλις λεπτά..
- **ΑΜΕΣΟΤΗΤΑ ΚΑΙ ΕΥΕΛΙΞΙΑ.** Το M-Banking είναι ιδιαίτερα χρήσιμο στον τομέα της χρηματοοικονομικής αγοράς σε περιπτώσεις που οι εξελίξεις είναι κρίσιμες και χρειάζεται ταχύτητα και γρήγορες αντιδράσεις για την διασφάλιση του χαρτοφυλακίου.
- **ΆΜΕΣΗ ΣΥΝΔΕΣΗ.** Παντού και Πάντα On-Line. Αποφεύγονται οι καθυστερήσεις στην διαδικασία σύνδεσης ή φόρτωσης του συστήματος.
- **ΔΥΝΑΜΙΚΗ ΠΛΗΡΟΦΟΡΗΣΗ.** Με την χρήση της τεχνολογίας Push and Pull ο χρήστης αποφασίζει το περιεχόμενο αλλά και την συχνότητα των μηνυμάτων, επιλέγοντας τις πληροφορίες που τον ενδιαφέρουν.
- **ΤΑΥΤΟΠΟΙΗΣΗ.** Ο χρήστης με την εισαγωγή μόνο του PIN αποφεύγει την καθυστέρηση της γραφειοκρατίας κερδίζοντας σε χρόνο και κόπο.
- **ΕΞΟΙΚΟΝΟΜΗΣΗ ΧΡΗΜΑΤΩΝ.** Όλο και περισσότερες τράπεζες υιοθετούν την τακτική της προσφοράς την ηλεκτρονικών πληρωμών με λιγότερη προμήθεια ή και χωρίς χρέωση.

2.4.2. Για την Τράπεζα

- **ΔΙΕΥΡΥΝΣΗ ΠΕΛΑΤΕΙΑΚΗΣ ΒΑΣΗΣ.** Τα τραπεζικά ιδρύματα κερδίζουν από τη χρήση του M-Banking την αύξηση της πελατειακής τους βάση. Η κατάργηση των γεωγραφικών συνόρων, αφού ακόμα και οι κάτοικοι του εξωτερικού έχουν την δυνατότητα χρήσης των τραπεζικών υπηρεσιών, καθώς και τα περισσότερα κανάλια διανομής των υπηρεσιών έχουν σαν αποτέλεσμα ο αριθμός των πελατών να αυξάνεται.
- **ΜΕΙΩΣΗ ΛΕΙΤΟΥΡΓΙΚΟΥ ΚΟΣΤΟΥΣ.** Τα τραπεζικά ιδρύματα οφελούνται με τη χρήση του M-Banking από περισσότερους πελάτες αφού το μέσο κόστος συναλλαγής μειώνεται.Σε αντίθετη περίπτωση θα οδηγούνταν σε προσλήψεις προσωπικού για την διατήρηση της ικανοποίησης των πελατών, που θα σήμαινε και ταυτόχρονη αύξηση του κόστους.

- **ΚΕΡΔΟΦΟΡΕΣ ΝΕΕΣ ΥΠΗΡΕΣΙΕΣ.** Τα χρηματοπιστωτικά ιδρύματα τείνουν να δημιουργούν μέσα στις διαδικτυακές σελίδες, τους διαδικτυακούς χώρους συζητήσεων και διαδικτυακές πύλες, συλλέγοντας πληροφορίες για το πελατολόγιό τους προσφέροντας και προωθώντας ένα πλήρες πακέτο νέων προϊόντων.
- **ΑΥΞΗΣΗ ΤΩΝ ΤΡΑΠΕΖΙΚΩΝ ΛΕΙΤΟΥΡΓΙΩΝ.** Απόκτηση ενός συμπληρωματικού δικτύου προσέγγισης πελατών αυξάνοντας ταυτόχρονα και τα έσοδα.
- **ΜΕΛΛΟΝΤΙΚΗ ΕΞΕΛΙΞΗ ΤΗΣ ΤΡΑΠΕΖΑΣ.** Απόκτηση στρατηγικών πλεονεκτημάτων από την χρήση υπηρεσιών του μέλλοντος σε συνάρτηση και με τον αυξανόμενο ανταγωνισμό.

2.5. Μειονεκτήματα του M-Banking

Παρά τα πλεονεκτήματα, τις ευκολίες και την ευχρηστία του, το mobile banking δεν έχει καταφέρει ακόμη να πείσει το ελληνικό καταναλωτικό κοινό. Αυτό οφείλεται ενδεχομένως στη χρήση του κινητού ως κατεξοχήν μέσου επικοινωνίας, συνεπώς η αποδοχή της αξιοπιστίας του ως μέσου διεξαγωγής χρηματοοικονομικών συναλλαγών δεν είναι εύκολη. Οι Έλληνες χρήστες και οι επιχειρήσεις δείχνουν να εμπιστεύονται περισσότερο το Internet, γεγονός που εξηγεί τα μεγαλύτερα ποσοστά διείσδυσης του ebanking έναντι του mobile banking.

2.5.1. Για τον Καταναλωτή

- **ΧΡΟΝΟΒΟΡΑ ΕΓΓΡΑΦΗ ΠΕΛΑΤΩΝ.** Για να έχει κάποιος τη δυνατότητα χρησιμοποίησης του M-banking, θα πρέπει πρώτα να επισκεφτεί ένα υποκατάστημα να κάνει αίτηση ή να κάνει αίτηση μέσω της ιστοσελίδας. Στη συνέχει αφού λάβει τους κωδικούς πρόσβασης θα πρέπει να πραγματοποιήσει την εγγραφή του. Στην περίπτωση δε που η αίτηση γίνει μέσω Internet, οι κωδικοί αποστέλλονται ταχυδρομικώς και αφού ο υποψήφιος δικτυακός πελάτης υπογράψει την παραλαβή τους, τα έγγραφα θα πρέπει να επιστραφούν στην αρμόδια υπηρεσία για να ενεργοποιηθούν.
- **ΔΥΣΚΟΛΙΑ ΕΚΜΑΘΗΣΗΣ ΚΑΙ ΧΕΙΡΙΣΜΟΥ.** Τα άτομα τα οποία δεν έχουν μεγάλη εξοικείωση με την τεχνολογία και ειδικότερα με το internet, οι τραπεζικοί δικτυακοί τόποι ίσως φανούν δύσχρηστοι.
- **ΔΥΣΠΙΣΤΙΑ ΤΟΥ ΧΡΗΣΤΗ.** Πολλοί άνθρωποι δεν εμπιστεύονται την ηλεκτρονική τραπεζική. Θέλουν να βλέπουν αυτόν που θα επεξεργαστεί το λογαριασμό τους, ενώ η ηλεκτρονική μεταφορά χρημάτων τους προκαλεί αμφιβολίες.
- **ΠΑΡΑΒΙΑΣΗ ΑΠΟΡΡΗΤΟΥ.** Η συχνότητα των ηλεκτρονικών επιθέσεων αποτελεί αγκάθι στην διασφάλιση των τραπεζικών συναλλαγών, αφού ο «αδύναμος κρίκος» στα συστήματα ασφαλείας αφορά τόσο τους πελάτες όσο και τις τράπεζες θέτοντας σε κίνδυνο τεράστια χρηματικά ποσά.

- **ΕΛΛΕΙΨΗ ΠΡΟΣΩΠΙΚΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ.** Η μείωση των επισκέψεων του πελάτου στα καταστήματα έχει σαν αποτέλεσμα να χάνεται η προσωπική επαφή και επικοινωνία με τους υπαλλήλους.
- **ΚΟΣΤΟΣ ΔΙΑΔΙΚΤΥΟΥ.** Η πρόσβαση στο διαδίκτυο είναι αρκετά ακριβή σε σχέση με τις υπόλοιπες χώρες της Ευρωπαϊκής Ένωσης.

2.5.2. Για την Τράπεζα

- **ΥΨΗΛΟ ΑΡΧΙΚΟ ΚΟΣΤΟΣ ΕΓΚΑΤΑΣΤΑΣΗΣ.** Η δημιουργία μίας ιστοσελίδας, η οποία έχει πολλές απαιτήσεις, με προϊόντα και υπηρεσίες εξειδικευμένες απαιτεί τη χρησιμοποίηση νέων τεχνολογιών. Η αναγκαιότητα για ειδικούς διακομιστές Ιστού (Web Servers) όπως συμβαίνει με όλες τις νέες τεχνολογίες δημιουργούν επιπρόσθετο κόστος ιδιαίτερα υψηλό. Η επιλογή δε των τεχνολογιών αυτών πρέπει να γίνει με μεγάλη προσοχή και να είναι συμβατή με την πολιτική της τράπεζας και το προφίλ της.
- **ΑΣΦΑΛΕΙΑ.** Οι ηλεκτρονικές επιθέσεις και η μη εξουσιοδοτημένη πρόσβαση στα τραπεζικά ηλεκτρονικά συστήματα είναι συχνή. Κύριο μέλημα των τραπεζών είναι η όσο το δυνατόν μεγαλύτερη ασφάλεια των πελατών τους με τοποθέτηση ειδικών προγραμμάτων και εξοπλισμού.
- **ΚΟΣΤΟΣ ΣΥΝΤΗΡΗΣΗΣ ΙΣΤΟΣΕΛΙΔΑΣ.** Η τεχνολογία συνεχώς εξελίσσεται, εμφανίζονται νέοι κίνδυνοι υποκλοπής μέσω του internet. Κανένα υπολογιστικό σύστημα δεν είναι 100% ασφαλές στην πάροδο του χρόνου. Οι τράπεζες δαπανούν αρκετά χρήματα για τον συνεχή εκσυγχρονισμό των προγραμμάτων ασφαλείας και συστημάτων παρακολούθησης.
- **ΚΟΣΤΟΣ ΕΚΠΑΙΔΕΥΣΗΣ ΤΟΥ ΠΡΟΣΩΠΙΚΟΥ.** Πρέπει να είναι σε θέση να επιλύσει τυχόν απορίες των χρηστών καθώς και να ενημερώνεται για τις αλλαγές που πραγματοποιούντα κατά διαστήματα στη χρήση του e-banking.
- **ΠΡΟΒΛΗΜΑΤΑ ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑΣ (INTERORERABILITY).** Οι συμβατότητες που μπορούν να παρουσιάζουν κάποια λειτουργικά συστήματα ή και λογισμικά με άλλα συστήματα υποδομής ή και με υλικά.

ΚΕΦΑΛΑΙΟ 3ο ΤΕΧΝΟΛΟΓΙΑ ΤΟΥ M-BANKING

3.1. Τεχνολογίες του Mobile Banking

Όταν αναφερόμαστε στο όρο τεχνολογίες δεν περιγράφουμε μια νέα επινόηση ή ένα νέο δίκτυο. Περιγράφουμε όμως μια νέα δυνατότητα πρόσβασης στο Διαδίκτυο, μέσω ασύρματων φορητών συσκευών και τεχνολογιών. Επομένως το ενσύρματο και το ασύρματο διαδίκτυο στην ουσία είναι η ίδια έννοια. Παρ' όλα αυτά υπάρχουν περιπτώσεις όπου συνδυάζονται για πολλά προϊόντα και υπηρεσίες. Για κάποιο μέρος από το περιεχόμενο και τις εφαρμογές που υπάρχουν στο Διαδίκτυο μπορεί η πρόσβαση να είναι δυνατή μόνο μέσω ενσύρματης σύνδεσης (υπολογιστής), κάποιο άλλο μπορεί να διατίθεται μόνο μέσω ασύρματης σύνδεσης (κινητό τηλέφωνο) και τέλος για κάποιο άλλο, η πρόσβαση μπορεί να γίνεται και με τους δύο τύπους σύνδεσης σαφώς με κάποιες διαφορές ως προς τον τρόπο που παρουσιάζονται τα περιεχόμενα.

Η τεχνολογία λοιπόν παίζει βασικό ρόλο στην ανάπτυξη των κινητών οικονομικών υπηρεσιών, καθώς οι υπηρεσίες μπορούν να προσφερθούν από πολλά διαφορετικά κανάλια και υπόκειται στις τράπεζες να επιλέξουν τον καλύτερο τρόπο επικοινωνίας με τους πελάτες τους. Έτσι μαζί με τα καταστήματα, τα ATMs, τα POS (τερματικά αποδοχής καρτών), το E-Banking και το M-Banking συμπληρώνεται το διαθέσιμο δίκτυο της τράπεζας με τους πελάτες της.

Η πρώτη εγαρμογή του M-Banking παγκοσμίως παραγματοποιήθηκε στην Φιλανδία από την Merita Nordbanken η οποία παρείχε στου πελάτες της τη δυνατότητα πληρωμών και πληροφόρησης του διαθέσιμου υπολοίπου των λογαριασμών. Η επιτυχημένη αυτή ιδέα υιοθέτηθηκε από πολλούς τραπεζικούς οργανισμούς με αποτέλεσμα την εξάπλωση της παγκοσμίως. Φυσικά μην ξεχνάμε να αναφερθούμε οτι σε όλη αυτή την «επανάσταση» στον τραπεζικό χώρο μεγάλο ρόλο έπαιξαν και οι τομείς της πληροφορικής και των τηλεπικοινωνιών με την πληθώρα εξελισσόμενων τεχνολογιών που παρείχαν.

Το Mobile Banking που καλύπτει τη διαχείριση λογαριασμών μέσω κινητών συσκευών αλλάζει σημαντικά τη δραστηριότητα των εμπορικών τραπεζών και είναι η αιτία να αναπτυχθεί η χρήση κινητών εφαρμογών και νέων τεχνολογιών.

Οι Mobile Banking τεχνολογίες μπορούν να ταξινομηθούν σε δύο περιβάλλοντα:

1. *Τεχνολογίες Server-Side*- από πλευράς διακομιστή: Οι εφαρμογές που στηρίζονται σε ένα διακομιστή, μακριά από την κάρτα SIM ή κινητού τηλεφώνου του χρήστη –πελάτου.

   Server-side τεχνολογίες είναι:

   - SMS,
   - IVR,
   - USSD2 και
   - WAP

2. *Τεχνολογίες Client –Side*-από πλευράς Πελάτου: Οι εφαρμογές, λύσεων και προσφορών υπηρεσιών, είναι εκείνες που έχουν κατασκευαστεί ή ενσωματωθεί σε μια SIM Card καταναλωτή ή στο ίδιο το κινητό τηλέφωνο.

   Client-side εφαρμογές είναι:

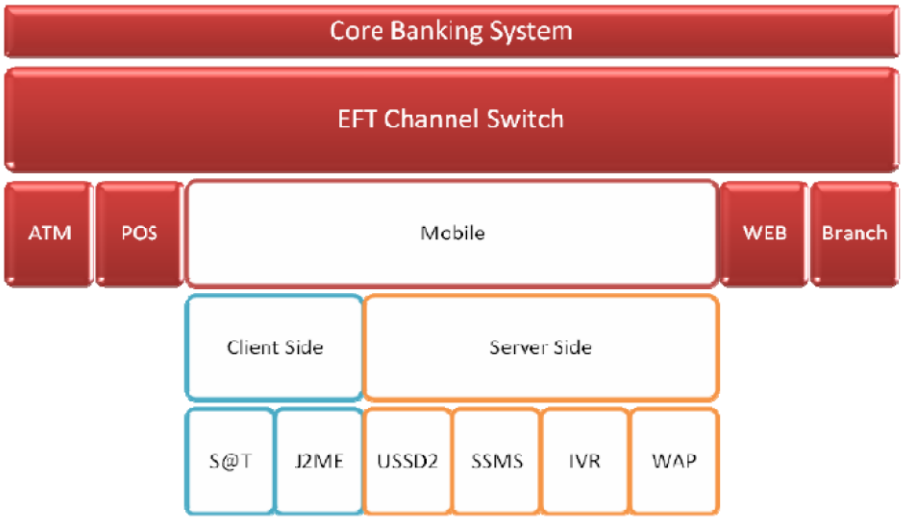
   - S @ T (SIMalliance Toolbox) και
   - J2ME (Java 2 Micro Edition).

Στις Server-side εφαρμογές, τα δεδομένα των καταναλωτών που επιτρέπουν την επεξεργασία των συναλλαγών (όπως τα στοιχεία του λογαριασμού / κάρτας), τυπικά αποθηκεύονται σε ένα εξαιρετικά ασφαλές περιβάλλον, σε ένα διακομιστή σε μια τράπεζα ή σε άλλον πάροχο υπηρεσιών.

Στις Client-side εφαρμογές, τα δεδομένα των καταναλωτών συνήθως αποθηκεύονται στην εφαρμογή, ή εισάγονται από τον καταναλωτή και κρυπτογραφούνται από την εφαρμογή στην κάρτα SIM. Τα περισσότερα από τις κινητές τραπεζικές υπηρεσίες μπορούν να αναπτυχθούν χρησιμοποιώντας περισσότερες από μία τεχνολογία ή ένα κανάλι.

Η αρχιτεκτονική δομή της τράπεζας, με έμφαση στο M-Banking διακρίνεται στο παρακάτω σχήμα:

Σχήμα 4: Η αρχιτεκτονική δομή των τραπεζών



Από την παραπάνω εικόνα προκύπτει οτι τι M-Banking μπορεί να διανεμηθεί μέσω δύο κομιστών. Έτσι έχουμε την εγκατάσταση λογισμικού εφαρμογών στο κινητό τηλέφωνο του πελάτη, που μπορούν να βρίσκονται είτε στην κάρτα SIM Application Toolkit του τηλεφώνου είτε στο ίδιο το τηλέφωνο για τις πιο εξελιγμένες συσκευές και την ανάπτυξη δικτυακών εφαρμογών όπως Java2 Micro Edition στον διακομιστή της τράπεζας.

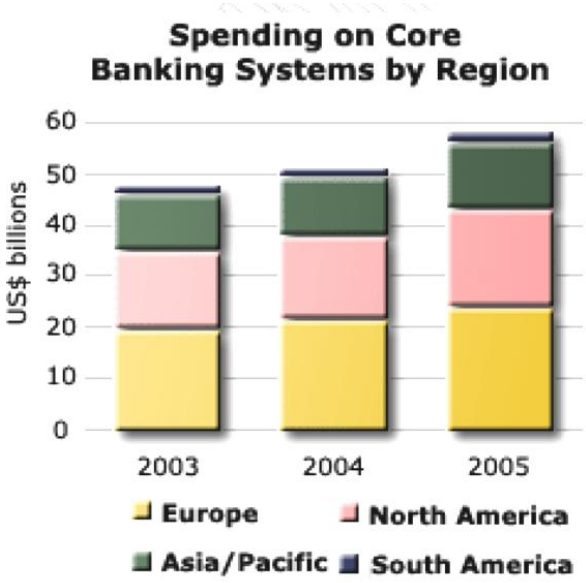
Το M-Banking και η επικοινωνία με την τράπεζα στηρίχθηκε στα τέσσερα κανάλια:

- *SMS* (Short Messaging Service)
- *USSD1-2* (Unstructured Supplementary Service Data 2)
- *WAP* (Wireless Application Protocol)
- *IVR* (Interactive Voice Response)

3.2. Core Banking

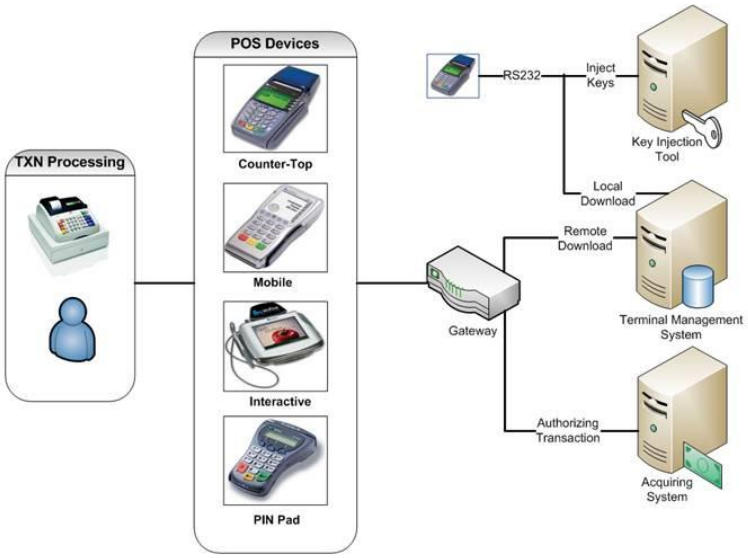
Η δομή του δικτύου επικοινωνίας της τράπεζας στηρίζεται στο Core Banking, ένα σύστημα το οποίο περιλαμβάνει το σύνολο των λογαριασμών και μέσω του οποίου γίνεται η διαχείρηση των κινήσεων τους. Για να μεταφραστούν οι εντολές σε γλώσσα κατανοητή, ώστε να μπορούν να επεξεργαστούν από το σύστημα, χρησιμοποιήται ο μετατροπέας EFT (Electronic Funds Transfer)

Σχήμα 5: Ποσοστά χρήσης του Core Banking ανα ήπειρο.



3.3. Ηλεκτρονική Μεταφορά Κεφαλαίων EFT (Electronic Funds Transfer)

Σχήμα 6: Η αρχιτεκτονική δομή της EFT



Ηλεκτρονική Μεταφορά Χρημάτων Debit Υπηρεσία είναι μια **ηλεκτρονική προ-εξουσιοδοτημένη υπηρεσία που μειώνει το χρόνο και το κόστος για τη συλλογή και επεξεργασία επαναλαμβανόμενων απαιτήσεων** (χρεώσεις). Οι πληρωμές που εισπράττονται από το λογαριασμό των πελατών σας και να κατατεθεί στο λογαριασμό TD επιχείρησή σας με τις ημερομηνίες λήξης.

Η υπηρεσία λειτουργεί ως **μια αυτοματοποιημένη εγκατάσταση συλλογής για ένα ευρύ φάσμα οργανισμών,** συμπεριλαμβανομένων των εταιρειών συγκυριαρχία, την ασφάλιση, καλωδιακή τηλεόραση, λέσχες υγείας, διαχειριστές ακίνητης περιουσίας, εκμίσθωση και μίσθωση εταιρείες, περιοδικών και εφημερίδων εταιρείες, επιχειρήσεις κοινής ωφέλειας, οι εκκλησίες και τα φιλανθρωπικά ιδρύματα.

ΤΙ ΠΡΟΣΦΕΡΕΙ Η ΗΛΕΚΤΡΟΝΙΚΗ ΜΕΤΑΦΟΡΑ ΧΡΗΜΑΤΩΝ (EFT):

- Μεταδίδει χρεωστικές πληρωμές μέσω Web Business Banking, σύνδεση mainframe ή προσωπικού υπολογιστή
- Δέχεται επαναλαμβανόμενες πληρωμές σε ποικίλες ποσότητες με διάφορες ημερομηνίες λήξης
- Παρέχει εκθέσεις σχετικά με όλα τα στοιχεία που γίνονται αποδεκτά για πληρωμή, καθώς και για εκείνα τα στοιχεία τα οποία δεν μπορούν να υποβληθούν σε επεξεργασία, για να συμπληρώσουν τις δικές της διαδικασίες εσωτερικής αναφοράς σας
- Παρέχει εκθέσεις ηλεκτρονικά ή μέσω fax
- Με την EFT επεξεργασία μπορούν, η διαγραφή πληρωμών, οι ανατροπές και τα ίχνη, να συμπληρωθούν on-line μέσω του Web Banking Business File Transfer.

ΤΑ ΟΦΕΛΗ ΤΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΜΕΤΑΦΟΡΑΣ ΧΡΗΜΑΤΩΝ (EFT)

- Εξαλείφει τον χρόνο και το κόστος της αλληλογραφίας και την προετοιμασία των τιμολογίων.
- Εξαλείφει τη συλλογή και απόθεση έλαβε ελέγχους.
- Αφαιρεί την αβεβαιότητα των ταμειακών ροών.
- Μειώνει την εργασία γραφείου και τα λάθη.

3.4. Η υπηρεσία SMS

Η υπηρεσία SMS Banking αποτελεί μία πιο... light πτυχή του Mobile Banking, οι υπηρεσίες του οποίου έχουν κυρίως ενημερωτικό χαρακτήρα, αν και ορισμένες τράπεζες επιτρέπουν μία περιορισμένη λειτουργικότητα σε επίπεδο συναλλαγών. Το περιεχόμενο της αποτελείται από αλφαριθμητικά και σύμβολα έως 160 χαρακτήρες και αποστέλλεται μεταξύ χρηστών ανεξαρτήτου δικτύου κάλυψης. Το χαρακτηριστικό της υπηρεσίας είναι οτι μπορεί να στείλει ή να λάβει μηνύματα οποιδήποτε ώρα της ημέρας, προσφέροντας εγγυημένη παράδοση των δεδομένων ανιχνεύοντας όποιο πρόβλημα προκύψει αποθηκεύοντας το μήνυμα έως ότου το πρόβλημα ρυθμιστεί. Αυτό υλοποιείται από το Short Message Service Center (SMSC), που είναι ένα σύστημα τύπου Store-and-Forward.

Αν και η υπηρεσία SMS απαιτεί μικρότερη προσπάθεια από άποψη κόστους και χρόνου υλοποιήσης καθώς απαιτεί μικρό εύρος ζώνης, δεν μπορεί να υποστηρίξει όλες τις διαθέσιμες

τραπεζικές υπηρεσίες και ιδιαίτερα τις υπηρεσίες συναλλαγών. Αρκετά δημοφιλείς είναι και οι υπηρεσίες τύπου alerts, με τις οποίες αποστέλλονται ειδοποιήσεις μέσω SMS στο κινητό του χρήστη, ανάλογα με τις προδιαγραφές που ο ίδιος έχει επιλέξει (π.χ. μεταβολές λογιστικού υπολοίπου, πιστώσεις και χρεώσεις κινήσεων, χρηματιστηριακές πράξεις κ.ά.).

3.4.1.Πλεονεκτήματα και Μειονεκτήματα

Το SMS Banking παρόλο που αποτελεί την πλέον διαδεδομένη υπηρεσία, με τα πολλά πλεονεκτήματα, δεν αποτελεί εξαίρεση έχοντας εξίσου και μειονεκτήματα.
Πλεονεκτήματα:

- **ΕΥΧΡΗΣΤΟ ΠΡΟΣ ΤΟΥΣ ΠΕΛΑΤΕΣ.** Τους διευκολύνει δίνοντας τους άνεση στην πραγματοποίηση τραπεζικών συναλλαγών αποφεύγοντας την πολύωρη αναμονή στην τράπεζα.
- **ΠΡΟΣΒΑΣΙΜΟΤΗΤΑ**. Άμεση πρόσβαση στις τραπεζικές πληροφορίες όλο το 24ωρο. Με τη προϋπόθεση να είναι ενεργό και εντός δικτύου.
- **ΦΟΡΗΤΟΤΗΤΑ** Υποστηρίζεται η αποστολή μηνυμάτων SMS από όλες τις συσκευές.
- **ΕΞΟΙΚΟΝΟΜΙΣΗ ΧΡΟΝΟΥ** Επειδή δεν είναι απαραίτητη η παρέμβαση των πελατών, εξαιτίας αυτόματων κινήσεων, για την πραγματοποίηση τραπεζικών συναλλαγών.
- **ΜΕΙΩΜΕΝΑ ΚΟΣΤΗ** Το μέσο κόστος συναλλαγής μειώνεται για τα τραπεζικά ιδρύματα όσο περισσότεροι είναι οι χρήστες, αφού χρησιμοποιείται για όλους τους πελάτες η ίδια υποδομή και τα ίδια προγράμματα.

Τα δομικά στοιχεία της υπηρεσίας είναι:

- **MOBILE STATION**

  Είναι το ασύρματο τερματικό το οποίο μπορεί να λαμβάνει και να στέλνει μηνύματα καθώς και μεταφορά φωνής.
- **MSC (MOBILE SERVICE CENTER)**

  Εκτελεί και ελέγχει όλες τις διενέργιες που έχουν να κάνουν με δρομολόγηση των κλήσεων προς και από άλλα τηλεφωνικά συστήματα και συστήματα δεδομένων.
- **SMSC (SHORT MESSAGE SERVICE CENTER)**

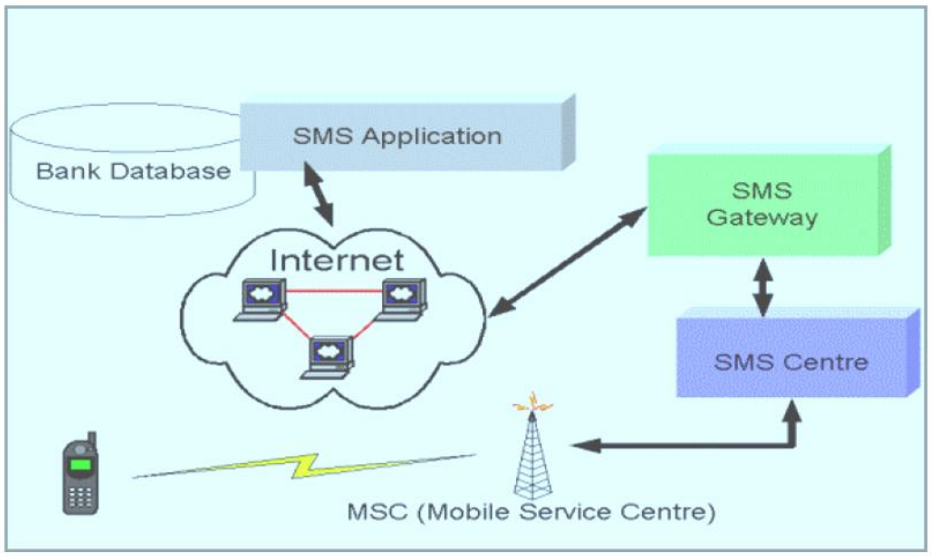
  Ο τομέας αυτός είναι υπεύθυνος για την αποστολή μηνυμάτων μεταξύ μίας οντότητας (SME) και του κινητού σταθμού.
- **SMS-GMSC (SHORT MESSAGE SERVICE-GATEWAY MOBILE SWITCHING CENTER)**

  Ο τομέας αυτός έχει την δυνατότητα λήψης μηνυμάτων από ένα GMSC. Στη συνέχεια εξετάζει τη βάση HLR (Home Location Register) για πληροφορίες σχετικά με τη θέση και τέλος προωθεί το μήνυμα στο αντίστοιχο κέντρο MSC το οποίο με την σειρά του το στέλνει στον παραλήπτη.

- **SME (SHORT MESSAGE ENTITIES)**

Σε αυτόν τον τομέα ανήκει η τράπεζα, η οποία μπορεί να στείλει και να λάβει μηνύματα.

Σχήμα 6: Η αρχιτεκτονική και τα δομικά στοιχεία της υπηρεσίας SMS



3.5. Η υπηρεσία USSD1-2 (Unstructured Supplementary Services Data)

Η υπηρεσία USSD αποτελεί μία παραλλαγή του SMS Banking και αποτελεί ένα μηχανισμό μετάδοσης πληροφορίας μέσω ενός συμβατικού δικτύου GSM. Ο μηχανισμός αυτός διαχειρίζεται ένα μενού επιλογών, σε αντίθεση με την απλή ακολουθία λέξεων του SMS. Μία άλλη διαφορά είναι και η διαδραστική επικοινωνία χρήστη και κινητής εφαρμογής σε πραγματικό χρόνο. Η ύπαρξη δηλαδή μίας «συνόδου» κατά τη διάρκεια της οποίας ο πελάτης μπορεί να πραγματοποιήσει μία χρηματική συναλλαγή πατώντας βοηθητικά πλήκτρα όπως π.χ. η δίεση και ο αστερίσκος χωρίς να χρειάζεται ένα νέο SMS για να ολοκληρωθεί.

- Το *USSD1* επιτρέπει την επικοινωνία μεταξύ χρήστη και ασύρματης υπηρεσίας μονομερώς όπως και το SMS.
- Το *USSD2* επιτρέπει την ανταλλαγή μηνυμάτων και από τα δύο μέρη στην ίδια σύνοδο, δημιουργώντας την ψευδαίσθηση του «πραγματικού χρόνου».

3.6. Το πρωτόκολλο ασύρματων εφαρμογών WAP (Wireless Application Protocol)

3.6.1. Λειτουργία WAP

Η πρόσβαση στο Mobile Banking πραγματοποιείται μέσω κινητών τηλεφώνων που υποστηρίζουν WAP ή κάποια διαδικτυακή υπηρεσία διαθέσιμη από τις εταιρείες κινητής τηλεφωνίας (π.χ. i-mode). Για τη διασφάλιση των συναλλαγών χρησιμοποιούνται κυρίως τα πρωτόκολλα που εφαρμόζονται και στις συναλλαγές του Internet Banking.

Το πρωτόκολλο ασύρματων εφαρμογών WAP (Wireless Applications Protocol) αποτελεί το βασικό πρωτόκολλο επικοινωνίας σε περιβάλλοντα που χρησιμοποιούν τεχνολογίες κινητών επικοινωνιών. Το WAP είναι το δημιούργημα των εργασιών μιας κοινοπραξίας των εταιρειών Ericsson, Nokia, Motorola και Phonecom που ιδρύθηκε το 1997 και ονομάστηκε WAP forum. Το WAP είναι ένα κοινά αποδεκτό πρώτο πρότυπο σε θέματα πρόσβασης στο Διαδίκτυο. Είναι ξεκάθαρο πως η αποτελεσματικότητα του κινητού εμπορίου εξαρτάται από το πόσο αξιόπιστες και δυνατές είναι οι ασύρματες συνδέσεις στις υποδομές των υπολογιστικών συστημάτων.

Ο τρόπος ενσύρματης σύνδεσης διαφέρει από τον τρόπο ασύρματης σύνδεσης. Το χαρακτηριστικό της μεταφερσιμότητας των συσκευών στον ασύρματο τομέα επιβάλλει κάποια συγκεκριμένα πρότυπα. Για παράδειγμα οι οθόνες είναι μικρές και τα πληκτρολόγια σπανίζουν. Η μνήμη και το εύρος είναι περιορισμένα και διαφέρουν ανάλογα με τον τομέα των κινητών επικοινωνιών. Για αυτό και πρέπει οι εφαρμογές να είναι προσαρμοσμένες σε κάθε συσκευή. Είναι δύσκολο να επιτευχθούν τυποποιημένες και ολοκληρωμένες αρχιτεκτονικές φορητών συσκευών στο περιβάλλον των πληροφοριακών συστημάτων. Όσον αφορά την δημιουργία τυποποιημένων και ολοκληρωμένων αρχιτεκτονικών κινητών συστημάτων μπορούν να χρησιμοποιηθούν ανοικτά πρότυπα, αντί για ιδιόκτητα.

Τα ιδιόκτητα πρότυπα δημιουργούνται και αναπτύσσονται από μεμονωμένα άτομα ή επιχειρήσεις. Το μειονέκτημα αυτών των προτύπων είναι το γεγονός ότι απαιτείται άδεια από τους κατόχους ή τους προγραμματιστές τέτοιων προτύπων (ή εφαρμογών) και η ευρεία χρήση τους είναι περιορισμένη. Επομένως η καλύτερη προσέγγιση για μία ολοκληρωμένη , προσπελάσιμη και εύκολη στη συντήρηση αρχιτεκτονική κινητών συστημάτων είναι να δημιουργηθούν πληροφοριακά συστήματα χρησιμοποιώντας ανοιχτά πρότυπα στο λογισμικό και στις τηλεπικοινωνίες. Για παράδειγμα, η χρήση ανοιχτών προτύπων στο λογισμικό, όπως Java και XML, σε συνδυασμό με το ανοικτό πρότυπο WAP για ασύρματες τηλεπικοινωνίες είναι μια καλή λύση. Η ενοποίηση των διαθέσιμων προτύπων είναι απαραίτητη για την σχεδίαση αλλά και την εξέλιξη των αρχιτεκτονικών πληροφοριακών συστημάτων που είναι βασισμένα στην ασύρματη τεχνολογία. Με αυτό τον τρόπο παρέχεται ευελιξία αλλά και λιγότερη εξάρτηση από εξειδικευμένες γλώσσες.

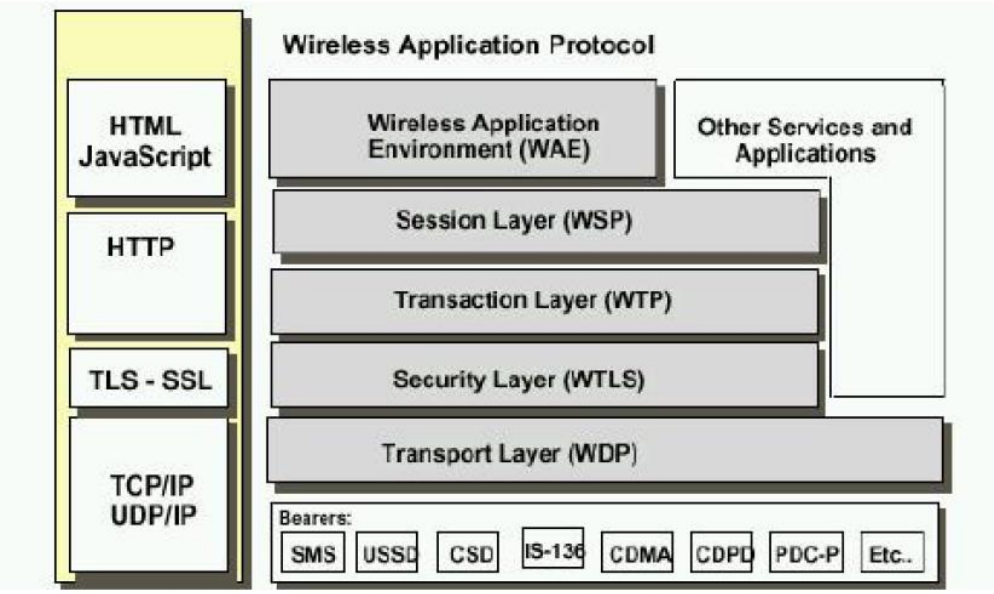
Αυτό ισχύει τόσο στο επίπεδο των εφαρμογών και των συσκευών αλλά κυρίως στα ασύρματα δίκτυα εξαιτίας του εύρους τόσο των διαθέσιμων φορητών συσκευών όσο και των λειτουργικών συστημάτων που αυτές χρησιμοποιούν.

Υπάρχουν δύο κύριες σχέσεις επικοινωνίας στο ασύρματο περιβάλλον:

- ✓ ***1η Σχέση***: Μεταξύ ενός σταθερού εξυπηρετητή και μιας φορητής συσκευής (όπως ενός κινητού τηλεφώνου, PDA ή φορητού υπολογιστή με ένα ολοκληρωμένο ασύρματο μόντεμ).
- ✓ ***2η Σχέση***: Μεταξύ δύο φορητών συσκευών (όπως μεταξύ δύο κινητών τηλεφώνων, ή ενός PDA με ένα κινητό τηλέφωνο).

Αυτές τις σχέσεις μπορούμε να τις δούμε σαν μία αρθρωτή σύνδεση. Οι συνδεδεμένες μονάδες είναι φυσικές, ως προς τις τεχνολογίες και τις συσκευές και λογικές, ως προς τα πρωτόκολλα και τις εφαρμογές. Μια τέτοια αντικειμενοστραφής προσέγγιση για την ανάπτυξη δικτυωμένων ασύρματων αρχιτεκτονικών πληροφοριακών συστημάτων ταιριάζει απόλυτα με την αρθρωτή δομή του προτύπου WAP. Η λειτουργία του πρωτοκόλλου WAP βασίζεται στην αρχιτεκτονική που ακολουθείται κατά την μεταφορά των δεδομένων στο Διαδίκτυο. Τα πέντε πρωτόκολλα του WAP, μαζί με το Network Layer διασύνδεσης ως έκτο, αποτελούν τα στρώματα της αρχιτεκτονικής του προτύπου και παρουσιάζονται στο παρακάτω σχήμα:

Σχήμα 7: Τα πρωτόκολλα του WAP



Η επικοινωνία μίας ασύρματης συσκευής με τον Webserver μιας εφαρμογής, γίνεται μέσω του πρωτοκόλλου HTTP. Για να ελαχιστοποιείται όμως το μέγεθος και ο αριθμός των πακέτων που ανταλλάσσονται μέσω του δικτύου και για να υπάρχει μεγαλύτερη σταθερότητα στα δίκτυα κινητών επικοινωνιών το WAP χρησιμοποιεί Πύλες (Gateways) κωδικοποίησης και αποκωδικοποίησης των περιεχομένων που μεταφέρονται. Συγκεκριμένα το WAP επιβάλλει μια συγκεκριμένη διαδικασία κατά την αίτηση μιας κινητής συσκευής να προσπελάσει μια διαδικτυακή WAP εφαρμογή. Όταν γίνει η αίτηση αυτή μεταφέρεται στο WAP Gateway μέσω του πρωτόκολλου WSP (Wireless Session Protocol) για να ξεκινήσει μια σύνοδος (session). Όταν ξεκινήσει η σύνοδος το πρωτόκολλο WTP (Wireless Transactions Protocol) μεταφέρει τα δεδομένα από και προς την συσκευή.

Το πρωτόκολλο WTP αντιστοιχεί στο HTTP, το οποίο HTTP χρησιμοποιείται από την WAP Gateway ούτως ώστε να γίνει αποκωδικοποίηση της αίτησης και να αποσταλεί στο περιβάλλον του Διαδικτύου. Από κει και μετά η αίτηση εξυπηρετείται με παραδοσιακές διαδικασίες και πρωτόκολλά Διαδικτύου. Όταν ο εξυπηρετητής λάβει την αίτηση, τότε θα δημιουργήσει την κατάλληλη, για την εκάστοτε συσκευή, απάντηση με βάση τα ανάλογα πρότυπα και θα την στείλει πίσω στο WAP Gateway.

Για να παρουσιαστεί το περιεχόμενο σε περιβάλλον WAP χρησιμοποιείται η γλώσσα WML (Wireless Markup Language), η οποία βασίζεται στην XML γλώσσα που είναι η αντίστοιχη της HTML στο παραδοσιακό Διαδίκτυο. Αυτή είναι μια γλώσσα κωδικοποίησης παρόμοια με την HTML που χρησιμοποιείται στις παραδοσιακές ιστοσελίδες που διαβάζονται από PC. Η WML Script αναφέρεται σε αρχεία script που είναι γραμμένα με την WML και η WML Bitmap αναφέρεται σε γραφικά αρχεία γραμμένα σε μορφή WML, η οποία είναι μία γλώσσα προγραμματισμού που έχει γίνει αποδεκτή εδώ και αρκετό καιρό και χρησιμοποιείται για την δημιουργία Web περιεχομένων που προβάλλονται σε φορητές συσκευές, αλλά και σε άλλες εφαρμογές.

Κατόπιν ακολουθείται η ακριβώς αντίστροφη διαδικασία για να μεταφραστεί η HTTP απόκριση σε WSP απόκριση, ούτως ώστε να μπορεί να την λάβει η κινητή συσκευή και να μπορεί να μεταφέρει δεδομένα μέσω του πρωτοκόλλου WTP.

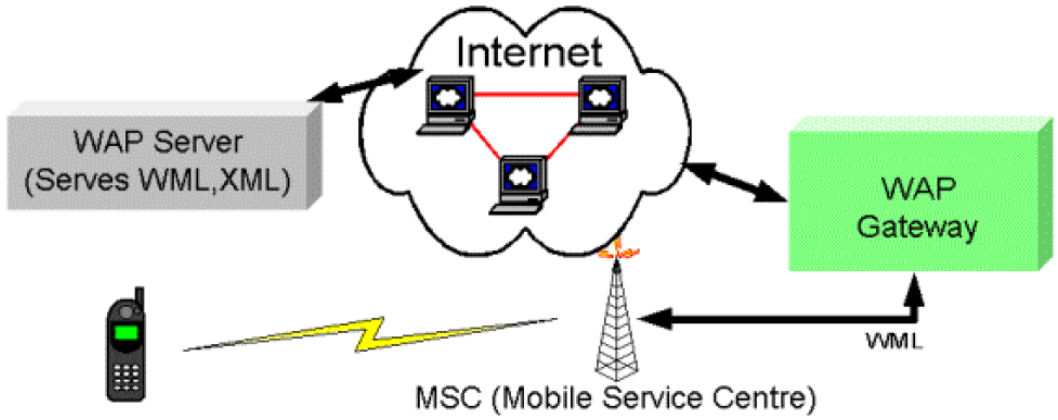
Το WAP αποτελείται από μία σουίτα από συστατικά που περιλαμβάνουν πρωτόκολλα δικτύων, μια εφαρμογή browser σε γλώσσα σήμανσης script και συστατικά τηλεφωνίας και ασφάλειας. Η αρθρωτή δομή του προτύπου WAP ευθυγραμμίζεται ωραία με τις αρθρωτές αρχιτεκτονικές των δικτύων. Επίσης, ανταποκρίνεται πολύ καλά στην θεωρία και πρακτική της ανάπτυξης συστημάτων υπολογιστών (που βασίζονται σε αντικείμενα) μέσα στις επιχειρήσεις.

Ο στόχος του κινητού εμπορίου είναι να επιτρέψει στο παραδοσιακό ηλεκτρονικό εμπόριο, που βασίζεται στην ενσύρματη σύνδεση, να ευθυγραμμιστεί με τις αρχιτεκτονικές του M-commerce. Το WAP πρωτόκολλο έχει βασικά, στόχο να επιτρέπει σε φορητές συσκευές να έχουν πρόσβαση στο Internet. Προσπελαύνει Web τοποθεσίες που είναι ειδικά σχεδιασμένες και κατασκευασμένες για φορητές ασύρματες συσκευές. Η εμπειρία του χρήστη βελτιώνεται στις τεχνολογίες 3G και 4G κάτι που κάνει πιο εύκολο τον χειρισμό τους.

Εξαιτίας του σταθερού εύρους μετάδοσης, της μικρής μνήμης και της μικρής οθόνης των φορητών συσκευών, δεν μπορούν να προβληθούν οι κανονικές ιστοσελίδες, με γραφικά και εικονίδια, τόσο αποτελεσματικά όσο οι κανονικές ιστοσελίδες που βλέπουμε σε έναν προσωπικό υπολογιστή. Ωστόσο, η WML χειρίζεται αυτούς τους περιορισμούς καταργώντας τα μη απαραίτητα γραφικά και εικόνες από τα περιεχόμενα των ιστοσελίδων. Τα περιεχόμενα μπορούν να προβληθούν από φορητές συσκευές με ενσωματωμένους μικρούς browser, ικανούς να διαβάσουν WML σελίδες.

3.6.2. Η αρχιτεκτονική του WAP

Σχήμα 7: Η αρχιτεκτονική WAP στο μοντέλο Client-Server



- *Mobile Station*. Είναι το ασύρματο τερματικό το οποίο μπορεί να λάβει και να στείλει δεδομένα μέσω ενός φυλλομετρητή WAP.
- *MSC (Mobile Service Center)*. Εκτελεί και ελέγχει όλες τις διεργασίες που έχουν να κάνουν με τη δρομολόγηση των κλήσεων από και προς άλλα τηλεφωνικά συστήματα και συστήματα δεδομένων.
- *WAP-G (Wireless Application Protocol-Gateway)*. Μεταφράζει και διακινεί τις αιτήσεις από το σύνολο των πρωτοκόλλων του WAP (WSP, WTP, WTLS, WDP) στο WWW (HTTP, SSL/TLS, TCP/IP) και αντίστροφα.
- *WAP Server*. Εδώ η τράπεζα ως μία οντότητα μπορεί να λάβει ή να στείλει δεδομένα.

Η αρχιτεκτονική του WAP παρέχει μια ποικιλία υπηρεσιών που υποστηρίζουν την ασύρματη εκπομπή κειμένου.

Πίνακας 1: Η αρχιτεκτονική του WAP

Επίπεδα	Περιγραφή
Application Layer (Εφαρμογής) Wireless Application Environment (WAE)	Περιβάλλον ανάπτυξης κινητών υπηρεσιών. HTML και η WML script (Wireless Mark-up Language) βρίσκονται σε αυτό το επίπεδο.
Session Layer (Συνόδου) Wireless Session Protocol (WSP)	Παρέχει μεθόδους ανταλλαγής περιεχομένων μεταξύ των server ασύρματων συσκευών και εφαρμογών. Η σχέση των ασύρματων συσκευών με το δίκτυο είναι σχέση πελάτη/εξυπηρετητή
Transaction Layer (Συναλλαγών) Wireless Transaction Protocol (WTP)	Παρέχει υποστήριξη για πολλούς τύπους συναλλαγών. Η αξιοπιστία εξαρτάται από τον τύπο της συναλλαγής.
Security Layer (Ασφάλειας) Wireless Transport Layer Security (WTLS)	Διασφαλίζει τα επίπεδα μυστικότητας και πιστοποίησης του χρήστη αλλά και την ασφάλεια της σύνδεσης μέσω του ελέγχου ακεραιότητας των δεδομένων.
Transport Layer (Μεταφοράς) Wireless Transport Layer (WTL)	Είναι το περιβάλλον διεπαφής μεταξύ των ανώτερων στρωμάτων και του στρώματος δικτύου. Είναι υπεύθυνο για τον εντοπισμό και την διόρθωση λαθών κατά την επικοινωνία χρησιμοποιώντας το WDP (Wireless Datagram Protocol)
Network Layer	Αναφέρεται στην φυσική διασύνδεση μεταξύ του δικτύου και των ασύρματων συσκευών.

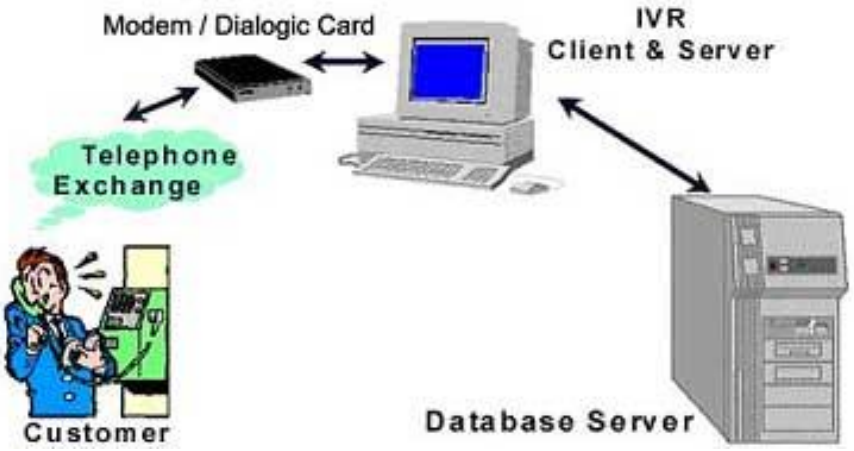
Τα στάδια μίας συναλλαγής μέσω WAP είναι:

- Ο χρήστης συνδέεται στην ιστοσελίδα του τραπεζικού ιδρύματος και τη διεύθυνση URL του εξυπηρετητή (WAP Server) επιλέγοντας τον τύπο της συναλλαγής που θέλει να κάνει (π.χ υπητεσία πληρωμής, κινήσεων λογαριασμών κ.τ.λ). Όλα τα στάδια αφού κωδικοποιηθούν για λόγους ασφαλείας, τα δεδομένα διακινούνται προς την πύλη WAP.
- Το WAP-Gateway (πύλη WAP) μετά από επεξεργασία και αποκωδικοποίηση διακινεί το αίτημα του χρήστη προς τον εξυπηρετητή (http) της τράπεζας.
- Μετά την «ανταλλαγή» μηνυμάτων μεταξύ WAP Server και τραπεζικού συστήματος ολοκληρώνεται η διαδικασία της συναλλαγής.
- Στη συνέχεια εξυπηρετητής (server) επιστρέφει το αποτέλεσμα της αίτησης σε μορφή WML (Wireless Mark-up Language).
- Η WAP-Gateway ελέχγει τα δεδομένα και κατευθύνει την απάντηση στον πελάτη μέσω του κέντρου ασύρματων υπηρεσιών του παρόχου.
- Τέλος ο χρήστης λαμβάνει την επιβεβαίωση ολοκλήρωσης της συναλλαγής.

3.7. Διαδραστική φωνητική απόκριση (IVR)- IVRs

3.7.1 Λειτουργία IVR

Σχήμα 8: Τεχνολογία IVR



IVR (Interactive Voice Response) είναι μια τεχνολογία που αυτοματοποιεί τις αλληλεπιδράσεις με τηλεφωνικές κλήσεις και μπορεί να διαβάσει ένα συνδυασμό τόνο αφής και εισόδου φωνής. Δίνει στους χρήστες τη δυνατότητα να έχουν πρόσβαση σε μια βάση δεδομένων των πληροφοριών μέσω τηλεφώνου. Ένα τυπικό σύστημα IVR έχει διάφορα μενού από προεγγεγραμμένες επιλογές που ο επισκέπτης μπορεί να επιλέξει. Αν και πολλές επιλογές είναι τόσο απλές, όπως την επιλογή ενός αριθμού, μερικές επιλογές μπορεί να απαιτούν από τον καλούντα να μιλήσει με λεπτομερείς πληροφορίες, όπως το όνομα του ή τον αριθμό του λογαριασμού. Αυτή η είσοδος διαβάζεται από το σύστημα IVR και χρησιμοποιείται για την πρόσβαση στην κατάλληλη πληροφορία στη βάση δεδομένων.

Για παράδειγμα, μια τράπεζα μπορεί να έχει ένα σύστημα IVR που επιτρέπει στα μέλη να καλούν και να ελέγχουν τις συναλλαγές. Οι εταιρείες πιστωτικών καρτών και οι χρηματιστηριακές εταιρείες χρησιμοποιούν επίσης συστήματα IVR που επιτρέπει στους χρήστες να έχουν πρόσβαση σε πληροφορίες από το λογαριασμό τους. Η τεχνολογία μπορεί επίσης να χρησιμοποιηθεί για άλλους σκοπούς, όπως τηλεφωνικές έρευνες. Επειδή ο επισκέπτης μπορεί φωνητικά να ανταποκριθεί σε ηχογραφημένο μηνύματα, χρησιμοποιώντας ένα σύστημα IVR είναι σχεδόν σαν να μιλάς με ένα άλλο ανθρώπινο ον. Αυτό είναι, εφ 'όσον σας καταλαβαίνει.

Οι επιχειρήσεις στρέφονται όλο και περισσότερο προς IVR για τη μείωση του κόστους των κοινών πωλήσεων, παροχής υπηρεσιών, συλλογές, έρευνα και υποστήριξη κλήσεις προς και από την εταιρεία τους. είναι μια τεχνολογία που επιτρέπει σε έναν υπολογιστή για να αλληλεπιδρούν με τους ανθρώπους μέσω της χρήσης της φωνής και DTMF (Dual-Tone-Multi-Frequency) τονική είσοδο μέσω τηλεφωνικού πληκτρολογίου.

Στον τομέα των τηλεπικοινωνιών, IVR επιτρέπει στους πελάτες να αλληλεπιδρούν με το σύστημα υποδοχής μιας εταιρείας μέσω τηλεφώνου πληκτρολόγιο ή με την αναγνώριση ομιλίας, μετά από την οποία μπορούν να εξυπηρετήσουν τις δικές τους έρευνες, ακολουθώντας το διάλογο IVR. Συστήματα IVR μπορεί να ανταποκριθεί με ηχογραφημένο ή δημιουργούνται δυναμικά ήχου σε περαιτέρω άμεσες χρήστες για το πώς να προχωρήσουμε. Εφαρμογές IVR μπορεί να χρησιμοποιηθεί για τον έλεγχο σχεδόν σε οποιαδήποτε λειτουργία, όπου η διασύνδεση μπορεί να αναλυθεί σε μια σειρά από απλές αλληλεπιδράσεις. Τα συστήματα IVR αναπτυχθεί στο δίκτυο μέγεθος για να χειριστεί μεγάλο όγκο κλήσεων.

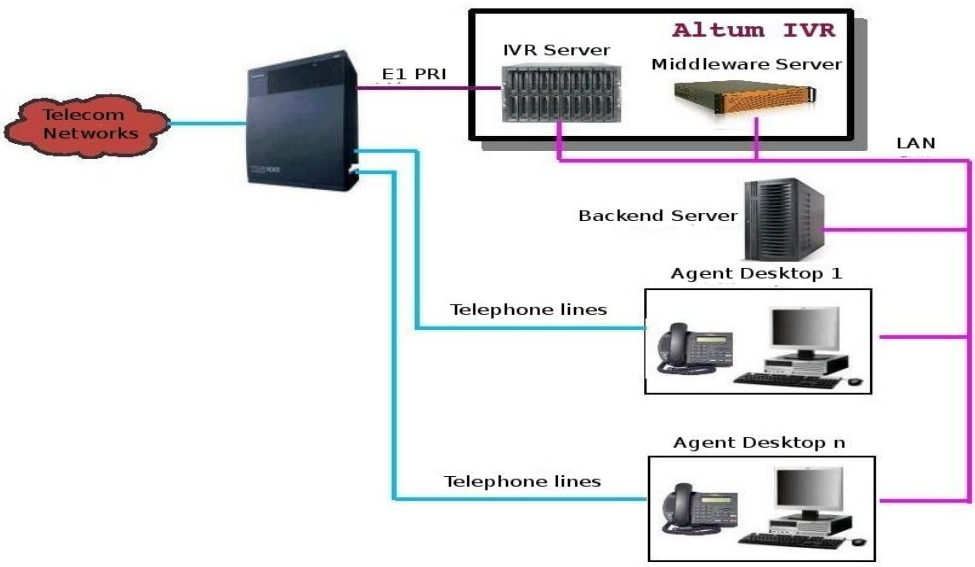
Τα συστήματα IVR συνήθως προορίζονται για την εξυπηρέτηση υψηλό όγκο κλήσεων, μείωση του κόστους και τη βελτίωση της εμπειρίας του πελάτη. Παραδείγματα τυπικές εφαρμογές IVR είναι τηλεφωνική τραπεζική , televoting και πιστωτικών καρτών υπηρεσίες. Οι εταιρείες χρησιμοποιούν επίσης τις υπηρεσίες IVR για την επέκταση των ωρών εργασίας τους να 24/7 λειτουργία.

Η χρήση του IVR και φωνητικών αυτοματισμού επιτρέπει ερωτήματα καλούντων να επιλυθούν χωρίς την ανάγκη αναμονής και αναλαμβάνοντας το κόστος της ζωντανής υποστήριξης. Αν οι καλούντες δεν βρίσκουν τις πληροφορίες που χρειάζονται ή χρειάζονται περαιτέρω βοήθεια, οι κλήσεις τους μεταφέρονται συχνά σε έναν πράκτορα. Αυτό κάνει για ένα πιο αποτελεσματικό σύστημα στο οποίο οι πράκτορες έχουν περισσότερο χρόνο για να ασχοληθεί με πολύπλοκες αλληλεπιδράσεις. Οι παράγοντες που δεν ασχολούνται με τη βασική έρευνα που απαιτούν ναι / όχι απαντήσεις ή απόκτηση στοιχείων του πελάτη.

Όταν ένα σύστημα IVR απαντά πολλαπλούς αριθμούς τηλεφώνου, η χρήση του DNIS εξασφαλίζει ότι η ορθή εφαρμογή και η γλώσσα εκτελείται. Ένα ενιαίο μεγάλο σύστημα IVR μπορεί να χειριστεί τις κλήσεις για χιλιάδες εφαρμογές, το καθένα με το δικό του αριθμό τηλεφώνου και το σενάριο της.

Το IVR επιτρέπει επίσης την ιεράρχηση των πελατών. Σε ένα σύστημα όπου μεμονωμένοι πελάτες μπορούν να έχουν μια διαφορετική κατάσταση της υπηρεσίας που θα δώσει προτεραιότητα αυτόματα στην κλήση του ατόμου και να προχωρήσουμε στους πελάτες να το μπροστά από μία συγκεκριμένη ουρά.

Σχήμα 9: Η αρχιτεκτονική IVR



3.7.2. IVR ΣΤΟΝ ΤΡΑΠΕΖΙΚΟ ΤΟΜΕΑ

IVR είναι εξαιρετικά χρήσιμο όταν πρόκειται για τραπεζικό τομέα. Οι τράπεζες λαμβάνουν αριθμό των κλήσεων καθημερινά. Για να απαντήσουμε σε όλα αυτά και ότι πάρα πολύ με ακριβείς πληροφορίες είναι εξαιρετικά εξαντλήσιμων και χρονοβόρα.

Ο αυξημένος ανταγωνισμός είναι η κινητήρια δύναμη να επενδύσουν σε τεχνολογίες για την ενίσχυση των διαύλων διανομής τους. IVR στον τραπεζικό τομέα μπορεί να εφαρμοστεί σε όλους τους τομείς, όπως μικρές και μεσαίες τράπεζες, συνεταιριστικές τράπεζες, Financial Sector, εθνικοποιημένη τράπεζα κλπ

Ένας πελάτης καλώντας σε μια τράπεζα μπορεί να έχει διαφορετικό κίνητρο. Μπορεί να θέλει απλά τα στοιχεία του λογαριασμού του, ή μπορεί να έχει κάποιο περίπλοκο πρόβλημα. Αυτά τα απλά θέματα μπορεί εύκολα να αντιμετωπιστεί με τη χρήση IVR τεχνολογίας και αν το περίπλοκο πρόβλημα το απαιτεί να εκτραπεί σε χειριστή. Μελέτες έχουν αποδείξει οτι το 75% από τα περίπου 2 εκατομμύρια κλήσεις που η τράπεζα παίρνει κάθε μήνα να τερματιστεί πάνω από το σύστημα IVRs.

Οι τράπεζες χρησιμοποιούν IVR για την απλοποίηση των ακόλουθων διαδικασιών.

- Για πληροφορίες λογαριασμού
- Ενημερώσεις του χαρτοφυλακίου επενδύσεων και την κατάσταση του
- Αίτηση δανείου και την κατάσταση του δανείου
- Έκτακτης ανάγκης και παράπονα
- Αίτηση και τη τεχνική υποστήριξη των πελατών για IVR
- Πληροφορίες για τραπεζικά προϊόντα χρησιμοποιώντας το IVR

3.8. Εφαρμογή iMode

Το iMode υποστηρίζει την προσπέλαση δεδομένων και την πρόσβαση στο διαδίκτυο όπως συμβαίνει και με το WAP. Για αυτό τον λόγο υπάρχουν πολλοί που υποστηρίζουν πως το iMode μοιάζει πολύ στο WAP. Το iMode υποστηρίζει την προσπέλαση δεδομένων και την πρόσβαση στο διαδίκτυο όπως συμβαίνει και με το WAP. Η διαφορά είναι πως το iMode είναι ένα κινητό τηλέφωνο με μια μεγαλύτερη οθόνη από τις συνηθισμένες, που λειτουργεί παρέχοντας τις παραδοσιακές υπηρεσίες ενός απλού κινητού και διαθέτει τα καθορισμένα χαρακτηριστικά (χρόνο ζωής της μπαταρίας, ποιότητα φωνής, βάρος και διαστάσεις) αλλά συνδυάζει επίσης τις iMode υπηρεσίες, που δεν είναι άλλες από έναν internet browser για περιήγηση σε διαδικτυακούς τόπους αλλά και έναν e-mail client. Ο browser επιτρέπει στον χρήστη να εισέλθει σε πάνω από πενήντα χιλιάδες τοποθεσίες που έχουν σχεδιαστεί. Στην Ελλάδα η υπηρεσία iMode παρέχεται από την εταιρεία Cosmote.

Το πρωτόκολλο iMode δημιουργήθηκε από την ιαπωνική εταιρεία NTT DoCoMo, μια πολύ μεγάλη ασύρματη (κυψελωτή) εταιρεία επικοινωνιών (WISP -Wireless Internet Service Provider). Ενώ το WAP είναι το πρότυπο για την Ευρώπη, σε μεγάλο μέρος της Αμερικής αλλά και σε πολλά μέρη της Αφρικής, της Ασίας καθώς και του Ειρηνικού, όπως η Αυστραλία και η Νέα Ζηλανδία, υιοθετήθηκε το πρότυπο iMode. Το γεγονός όμως πως το iMode είναι ένα ιδιόκτητο πρότυπο, καθιστά περιορισμένο το εύρος των διαθέσιμων πληροφοριών αλλά και της χρήσης τους συγκριτικά με το ανοιχτό πρότυπο WAP. Επίσης δεν μπορεί κανείς να βρει πολλές πληροφορίες όσον αφορά την δομή του και τα επίπεδα λειτουργίας, όμως από το κοινό και την αγορά μπορεί κανείς να καταλάβει τον τρόπο λειτουργίας του.

Επειδή η υπηρεσία iMode δεν βασίζεται στο WAP, δεν απαιτεί WML για να παράγει εφαρμογές για οθόνες κινητών τηλεφώνων. Στην ουσία βασίζεται σε μια συμπαγή μορφή της HTML γλώσσας, που ονομάζεται cHTML (compact HTML) και δημιουργήθηκε από την Access Co.Ltd, μια ιαπωνική εταιρεία λογισμικού browser. Το iMode υποστηρίζει έγχρωμα περιεχόμενα υψηλής ανάλυσης, που είναι ένα από τα πιο επιτυχημένα χαρακτηριστικά του για να προσελκύσει συνδρομητές στο κινητό διαδίκτυο, σε σύγκριση με την πρόσβαση μέσω WAP.

Μεγάλο πλεονέκτημα όμως για το iMode αποτελεί το γεγονός, πως η υπηρεσία δεν αποτελεί “περίφραξη για τους πελάτες”, όπως πολλές άλλες ασύρματες πύλες. Εταιρείες αλλά και άτομα έχουν την δυνατότητα να δημιουργήσουν τις προσωπικές τους τοποθεσίες στο Internet, οι οποίες μπορούν να προσπελαστούν μέσω του iMode. Ενώ μεγάλη πλειοψηφία των τοποθεσιών αυτών εξακολουθούν να είναι μόνο σε Γιαπωνέζικο σύνολο χαρακτήρων.

Οι τελευταίες υπηρεσίες iMode στην Ευρώπη έχουν επεκτείνει θεαματικά τον αριθμό των Αγγλικών τοποθεσιών. Συνεπώς, το iMode προσφέρει ένα επίπεδο εμπλοκής και δωρεάν συμμετοχής στο Κινητό Διαδίκτυο, παρόμοιο με αυτόν του ενσύρματου Internet. Η μεγάλη πλειοψηφία των άλλων ασύρματων παροχέων WISP δεν προσφέρει αυτήν την δυνατότητα ακολουθώντας την λογική “περίφραξης των πελατών”, ούτως ώστε αυτή να έχουν πρόσβαση μόνο στις επίσημες τοποθεσίες του διαδικτύου που προβάλλουν.

3.9. Εφαρμογή Java2 Platform Micro Edition- J2ME

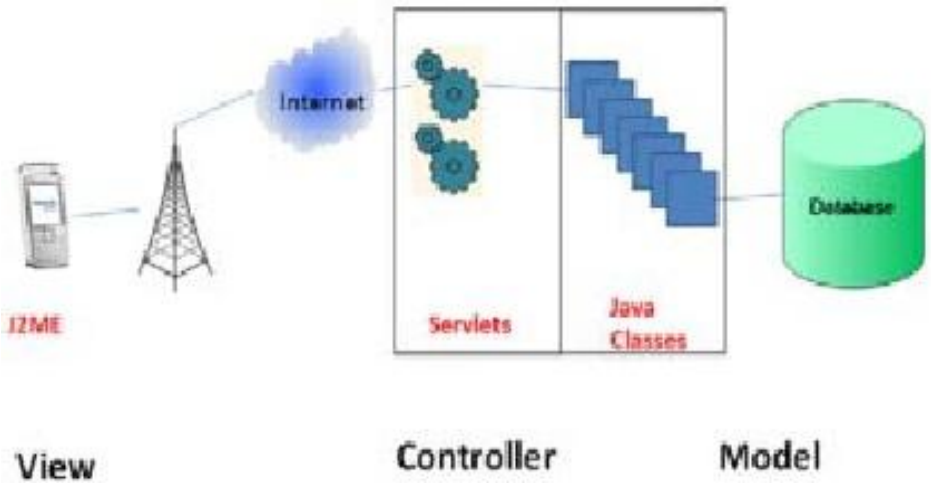
J2ME (Java2 Platform, Micro Edition) είναι μια τεχνολογία που επιτρέπει στους προγραμματιστές να χρησιμοποιούν τη γλώσσα προγραμματισμού Java και τα συναφή εργαλεία για την ανάπτυξη προγραμμάτων για κινητές συσκευές ασύρματα πληροφορίες, όπως κινητά τηλέφωνα και προσωπικούς ψηφιακούς βοηθούς (PDAs). J2ME αποτελείται από τις προδιαγραφές προγραμματισμού και μια ειδική εικονική μηχανή, η K Virtual Machine, που επιτρέπει μια J2ME-κωδικοποιημένο πρόγραμμα να τρέξει στην κινητή συσκευή.

Οι ασύρματες συσκευές όπως τα κινητά τηλέφωνα και οι συσκευές τηλεειδοποίησης βοηθούν τους ιδιοκτήτες τους, να συνδέεται με τον έξω κόσμο οποιαδήποτε στιγμή από οπουδήποτε. Προσφέρουν πολλές επιλογές συνδεσιμότητας που άλλοι τύποι συσκευών δεν θα μπορούσαν να προσφέρουν. Η ανάπτυξη εφαρμογών για αυτές τις ασύρματες συσκευές πρόκειται να είναι σε μεγάλη ζήτηση για τα επόμενα δύο χρόνια. Ο προγραμματισμός του δικτύου παίζει σημαντικό ρόλο στην ασύρματη ανάπτυξη εφαρμογών για να επωφεληθούν από τη συνδεσιμότητα που αυτές οι συσκευές έχουν να προσφέρουν.

Της Sun Java 2 Micro Edition (*J2ME*), προσφέρει μια μεγάλη πλατφόρμα ανάπτυξης για την ανάπτυξη εφαρμογών για τα ενσωματωμένα ηλεκτρονικά και φορητές συσκευές. Στην Java 2 Micro Edition (*J2ME*), η Connected Περιορισμένη Ρύθμιση Συσκευών (*CLDC*) ορίζει ένα γενικό "διαμόρφωση" για ένα ευρύ φάσμα των φορητών συσκευών. Στην κορυφή της CLDC, το Mobile Information Device Profile (*MIDP*) ορίζεται ειδικά για ασύρματες συσκευές, όπως κινητά τηλέφωνα και αμφίδρομες συσκευές τηλεειδοποίησης.

Το μεγαλύτερο μειονέκτημα των κινητών εφαρμογών είναι ότι οι εφαρμογές θα πρέπει να προσαρμοστούν σε κάθε κινητό τηλέφωνο. J2ME ταυτίζεται με το API για τα κινητά τηλέφωνα που έχουν την ίδια λειτουργικότητα σε αυτό που αποκαλούν «προφίλ». Ωστόσο, η ταχεία ανάπτυξη των κινητών τηλεφώνων που υποστηρίζουν διαφορετικές λειτουργίες έχει οδηγήσει σε ένα τεράστιο αριθμό προφίλ, τα οποία είναι περισσότερο σημαντικά στο κόστος ανάπτυξης. Το μέγεθος του προβλήματος μπορεί να εκτιμηθεί από το γεγονός ότι οι τράπεζες που χρησιμοποιούν τις εφαρμογές αυτές μπορεί να χρειαστεί να περάσουν το 50% του χρόνου ανάπτυξης και τους πόρους για την προσαρμογή των εφαρμογών τους στις ανάγκες των διαφορετικών προφίλ κινητών.

Σχήμα 10: Η αρχιτεκτονική J2ME



3.10. Εφαρμογή Standalone Mobile Application Clients - SMAC

Η SMAC (Standalone Mobile Application Clients) - η αυτόνομη κινητή εφαρμογή πελάτη- είναι ένα σύνολο προγραμμάτων που αναπτύσσονται στις ασύρματες συσκευές των χρηστών του τηλεπικοινωνιακού δικτύου και παρέχουν τη δυνατότητα συνεχούς σύνδεσης με παρόχους όπως είναι οι τράπεζες. Η εγκατάσταση των προγραμμάτων αυτών στο χώρο μνήμης του τηλεφώνου ή στη SIM Card κάνει εφικτή τη μορφοποίηση τους, με βάση το προφίλ του χρήστη, δίνοντας ένα παραπάνω πλεονέκτημα σε σχέση με τα υπόλοιπα κανάλια διανομής υπηρεσιών καθιστώντας τα πιο εύχρηστα και με πιο εύκολη πρόσβαση. Στην κατηγορία αυτή ανήκουν οι εφαρμογές SIM Application Toolkit (SAT/ STK/ S@T).

Η επέκταση του προτύπου και της λειτουργικότητας των SIM Card των κινητών τηλεφώνων είχε σαν αποτέλεσμα την υποστήριξη μίας νέας γενιάς υπηρεσιών στις εφαρμογές SIM Application Toolkit που στηρίζονται στην χρήση των SMS και USSD.

Το STK είναι ένα σύνολο εντολών που καθορίζει τη συμπεριφορά της SIM Card με τον έξω κόσμο και αποτελεί πρότυπο του δικτύου GSM που επιτρέπει στη SIM να ξεκινά συναλλαγές ανεξάρτητα από τη συσκευή και το δίκτυο. Η SIM Card είναι σε θέση να αρχικοποιεί μία διαδραστική ανταλλαγή δεδομένων μεταξύ της δικτυακής εφαρμογής και του τελικού χρήστη, χωρίς την παράμβαση του τηλεφώνου.

Το SAT, όπως και τα USSD, διαχειρίζεται ένα μενού επιλογών το οποίο προβάλλεται ύστερα από αντίστοιχη εντολή της SIM Card στο κινητό. Η εγκατάσταση των κινητών εφαρμογών, αυτή γίνεται μέσω του τηλεπικοινωνιακού φορέα με την ασύρματαη αποστολή πολλών κρυπτογραφημένων SMS τα οποία διαμορφώνουν κατάλληλα την SIM Card.

3.11. Εφαρμογή SAT/ S @ T SIMalliance Toolbox /STK

Ο Οδηγός Εφαρμογής SIM (SAT / S @ T/ STK) επιτρέπει στον πάροχο υπηρεσιών ή στην τράπεζα να εγκαταστήσει το mobile banking μενού στο κινητό του καταναλωτή εντός της κάρτας SIM. Είναι ένα πρότυπο του συστήματος GSM που επιτρέπει μέσω της SIM Card να αναληφθούν δράσεις που μπορούν να χρησιμοποιηθούν για διάφορες υπηρεσίες προστιθέμενης αξίας.

Αποτελείται από ένα σύνολο εντολών προγραμματισμού, στην SIM Card, που καθορίζουν πώς η κάρτα SIM θα πρέπει να αλληλεπιδρά άμεσα με τις εξωτερικές παγκοσμίως εντολές, ανεξάρτητα από τη συσκευή και το δίκτυο. Αυτό επιτρέπει στην SIM Card τη δημιουργία μίας διαδραστικής ανταλλαγής μεταξύ μιας εφαρμογής δικτύου και του τελικού χρήστη, καθώς και την πρόσβαση αλλά και τον έλεγχο πρόσβασης στο δίκτυο. Η SIM Card δίνει επίσης εντολές στη συσκευή, όπως το «μενού της οθόνης» ή την παρέμβαση του χρήστη και να ζητήσει την «είσοδο του χρήστη».

Σχεδιασμένο ως ένα ενιαίο περιβάλλον της εφαρμογής, το STK μπορεί να ξεκινήσει κατά τη διάρκεια της αρχικής ισχύς της κάρτας SIM και είναι ιδιαίτερα κατάλληλο για εφαρμογές χαμηλού επιπέδου με απλές διεπαφές χρήστη. Το STK έχει αναπτυχθεί για τον μεγαλύτερο αριθμό κινητών συσκευών και ορισμένοι κατασκευαστές ισχυρίζονται ότι το STK επιτρέπει υψηλότερα επίπεδα ασφάλειας μέσω της επαλήθευσης της ταυτότητας και κρυπτογράφησης, τα οποία είναι απαραίτητα για το ασφαλές ηλεκτρονικό εμπόριο.

Το μειονέκτημα του είναι οτι έχει περιορισμένη δυνατότητα εφαρμογής και υποστήριξης στα πολυμέσα, μόνο τις βασικές εικόνες.

ΚΕΦΑΛΑΙΟ 4° ΑΣΦΑΛΕΙΑ ΤΟΥ M-BANKING

4.1. Το Περιβάλλον Ασφαλείας

Το M-Banking όπως και E-Banking είναι ανοικτά συστήματα, επομένως οποιοσδήποτε μπορεί να υποκλέψει, τροποποιήσει ή απαρνηθεί κάποια μετάδοση. Συνεπώς η ασφάλεια που χρειάζεται είναι διαφορετική από αυτή που απαιτείται στα παραδοσιακά εσωτερικά δίκτυα. Τα πιστωτικά ιδρύματα οφείλουν να προστατεύουν τον εαυτό τους αναπτύσσοντας μια δομή που να εξασφαλίζει τη μέγιστη δυνατή ασφάλεια για το πληροφοριακό σύστημα και τους πελάτες τους. Η προστασία τους απαιτείται για λόγους ανταγωνιστικότητας, υπευθυνότητας και διασφάλισης των περιουσιακών τους στοιχείων.

Γενικά, οι απαιτήσεις ασφάλειας που πρέπει να ικανοποιούνται στις οικονομικής φύσης συναλλαγές πρέπει να έχουν οπωσδήποτε τα ακόλουθα χαρακτηριστικά :

- *Εμπιστευτικότητα/Απόρρητο* (confidentiality), που προσφέρει τη δυνατότητα αναγνώρισης και επεξεργασίας των δεδομένων μόνο από εγγεκριμένους χρήστες. των δεδομένων
- *Ακεραιότητα* (integrity) της συναλλαγής, που διασφαλίζει οτι τα πακέτα των δεδομένων κατά την διάρκεια της μεταφοράς τους δεν έχουν αλλοιωθεί ή παραποιηθεί, είτε από εισβολείς είτε από τυχόν σφάλματα επικοινωνίας.
- *Αυθεντικοποίηση* (authentication) ή *Πιστοποίηση Ταυτότητας* των συμμετεχόντων, που επαληθεύει οτι τα δεδομένα στάλθηκαν πράγματι από τον χρήστη που ισχυρίζεται οτι τα έστειλε.
- *Τη μη δυνατότητα ακύρωσης* της συναλλαγής μετά την επιβεβαίωση της συμμετοχής (non repudiation) των συναλλασσομένων.

Είναι προφανές ότι για την ικανοποίηση των συνθηκών για μια ασφαλή ηλεκτρονική συναλλαγή, είτε αυτή αφορά το M-Banking είτε το E-Banking, θα πρέπει και οι δύο αντισυμβαλλόμενοι της συναλλαγής να πάρουν τα κατάλληλα μέτρα.
Τα θέματα ασφάλειας που ανακύπτουν με τη χρησιμοποίηση του Διαδικτύου για τη πραγματοποίηση συναλλαγών είναι τα ακόλουθα:

- ✓ *Απώλεια της Ιδιωτικότητας των Δεδομένων* (Loss of Privacy): Σ' αυτήν την περίπτωση ένας μη εξουσιοδοτημένος χρήστης που έχει καταφέρει να εισχωρήσει σε κάποιο δίκτυο έχει τη δυνατότητα να παρακολουθεί εμπιστευτικά δεδομένα κατά τη διακίνησή τους στο Internet.
- ✓ *Απώλεια Ακεραιότητας Δεδομένων* (Loss of Data Integrity): Σ' αυτήν την περίπτωση ένας μη εξουσιοδοτημένος χρήστης αλλάζει τα δεδομένα που μεταφέρονται στο δίκτυο (π.χ. τους αριθμούς ενός λογαριασμού καταθέσεων)
- ✓ *Προσποίηση Ταυτότητας* (Identity Spoofing): Σ' αυτήν την περίπτωση ένας μη εξουσιοδοτημένος χρήστης παριστάνει ότι είναι ένας νόμιμος χρήστης του δικτύου και ζητά πληροφορίες που σε διαφορετική περίπτωση δε θα μπορούσε να έχει.
- ✓ *Άρνηση Υπηρεσιών* (Denial-of-Service): Σ' αυτήν την περίπτωση γίνεται "επίθεση" σε κάποιον server του δικτύου.

4.2. Κρυπτογραφία

Η ανάγκη για εμπιστευτικότητα στην ηλεκτρονική συναλλαγή ικανοποιείται με την κρυπτογραφία. Η κρυπτογράφηση είναι η μετατροπή των δεδομένων ενός υπολογιστή με βάση κάποιους εξεζητημένους αλγόριθμους, έτσι ώστε να μην μπορούν να διαβαστούν αν δεν υπάρχει το κλειδί που θα αποκρυπτογραφήσει τα δεδομένα. Με την κρυπτογράφηση ακόμα και αν κάποιος καταγράψει την συνομιλία, δεν έχει τη δυνατότητα να την αποκρυπτογραφήσει ή να τη μεταβάλλει. Η συνήθης κρυπτογράφηση που χρησιμοποιείται από τα τραπεζικά ιδρύματα είναι αυτή των 128bit. Αυτό σημαίνει ότι υπάρχουν 2128 πιθανά κλειδιά που μπορούν να χρησιμοποιηθούν για την κρυπτογράφηση των μηνυμάτων από τον διακομιστή στο server της τράπεζας. Λόγω αυτού η κρυπτογράφηση των 128bit θεωρείται και είναι απαραβίαστη.

Υπάρχουν δύο είδη κρυπτογραφίας:

- ✓ η συμμετρική και
- ✓ η ασύμμετρη

4.2.1. Συμμετρική *(Symmetric key encryption)*

Συμμετρική κρυπτογράφηση (Symmetric key encryption) ή κρυπτογράφηση ιδιωτικού κλειδιού (Secret key encryption). Η συμμετρική κρυπτογράφηση βασίζεται σε *ένα κοινό κλειδί* που χρησιμοποιείται από τον αποστολέα (για την κρυπτογράφηση) κι από τον παραλήπτη (για την αποκρυπτογράφηση) των μηνυμάτων. Το κλειδί θα πρέπει να παραμένει μυστικό και να είναι γνωστό μόνο στους συναλλασσόμενους. Ο πιο ευρέως αποδεκτός αλγόριθμος είναι ο Data Encryption Standard (DES). Το βασικό πρόβλημα της κρυπτογράφησης αυτού του τύπου αφορά τη δημιουργία, την αποθήκευση και τη μετάδοση του μυστικού κλειδιού.

4.2.2. Ασύμμετρη *(Asymmetric key encryption)*

Ασύμμετρη κρυπτογράφηση (Asymmetric key encryption) ή κρυπτογράφηση *δημοσίου κλειδιού* (Public key encryption). Η κρυπτογράφηση δημοσίου κλειδιού βασίζεται σε ένα ζεύγος κλειδιών εκ των οποίων το ένα είναι δημόσια γνωστό ενώ το άλλο είναι ιδιωτικό. Στην κρυπτογράφηση αυτή οτιδήποτε κρυπτογραφείται με το ένα κλειδί μπορεί να αποκρυπτογραφηθεί χρησιμοποιώντας μόνο το άλλο κλειδί. Ο πιο ευρέως αποδεκτός αλγόριθμος είναι ο RSA (Rivest, Shamir and Adelman).

4.3. Ψηφιακή υπογραφή *(Digital Signature)*

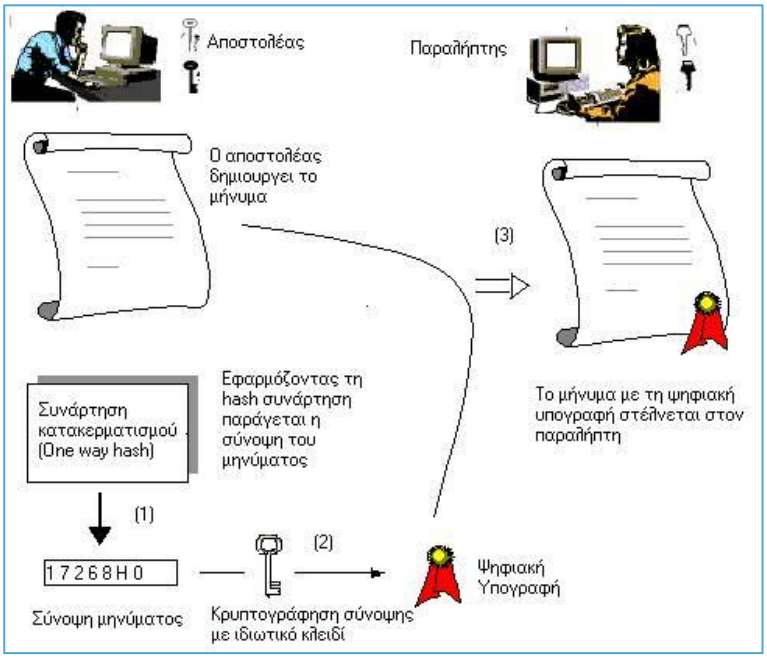
Η ψηφιακή υπογραφή χρησιμοποιείται για την απόδειξη της αυθεντικότητας του αποστολέα εφαρμόζοντας την *κρυπτογραφία δημοσίου κλειδιού και αντίστροφα*. Ο χρήστης διαθέτει δύο κλειδιά (το δημόσιο και το ιδιωτικό) τα οποία έχουν κάποιο μαθηματικό συσχετισμό. Η σχέση των κλειδιών είναι τέτοια όπου αν κάποιος γνωρίζει το ένα κλειδί να είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της. Στην περίπτωση αυτή λοιπόν, ο αποστολέας κωδικοποιεί ένα μήνυμα με το ιδιωτικό του κλειδί, το οποίο είναι απόρρητο. Μία ψηφιακή υπογραφή συνήθως προστίθεται σε ένα μήνυμα, όπως προστίθεται η υπογραφή σε κάποιο έγγραφο και με αυτόν τον τρόπο επιβεβαιώνει την αυθεντικότητα και τη μη αποποίηση ευθύνης του αποστολέα.

Η διαφοροποίηση από την κρυπτογράφηση, έγκειται στο ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα. Στη διαδικασία της δημιουργίας και επαλήθευσης της υπογραφής εμπλέκεται και η έννοια της συνάρτησης κατακερματισμού (ή κατατεμαχισμού -one way hash). Με την εφαρμογή της συνάρτησης κατακερματισμού, από ένα μήνυμα ανεξαρτήτου του μεγέθους του, παράγεται η

«σύνοψή του», η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους (π.χ. 128 ή 160 bits). Η σύνοψη του μηνύματος (fingerprint ή message digest) είναι μία ψηφιακή αναπαράσταση του μηνύματος, είναι μοναδική για το μήνυμα και το αντιπροσωπεύει. Η συνάρτηση κατακερματισμού είναι μονόδρομη διότι από την σύνοψη που δημιουργεί, είναι υπολογιστικά αδύνατον κάποιος να εξάγει το αρχικό μήνυμα. Η πιθανότητα δύο μηνύματα να έχουν την ίδια σύνοψη είναι εξαιρετικά μικρή. Αυτό σημαίνει ότι αν το μήνυμα του αποστολέα έχει κάποια συγκεκριμένη σύνοψη και το μήνυμα που λάβει ο παραλήπτης (χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού) παράγει διαφορετική σύνοψη, τότε το μήνυμα κατά την μετάδοσή του έχει αλλοιωθεί (μη ακεραιότητα). Οποιαδήποτε αλλαγή σε ένα μήνυμα συνεπάγεται και τη δημιουργία διαφορετικής σύνοψης.

Η ηλεκτρονική υπογραφή, στην ουσία είναι η κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα σύνοψη. Δηλαδή, η ψηφιακή υπογραφή (σε αντίθεση με την ιδιόχειρη υπογραφή) είναι διαφορετική για κάθε μήνυμα!!

Σχήμα 11: Δημιουργία ψηφιακής υπογραφής



Θεωρώντας ότι ο αποστολέας έχει ένα συγκεκριμένο ζευγάρι κλειδιών και το ιδιωτικό του κλειδί είναι στην πλήρη κατοχή του, τότε το γεγονός ότι ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει το μήνυμα, πιστοποιεί στον παραλήπτη που το αποκρυπτογραφεί με το αντίστοιχο δημόσιο κλειδί (του αποστολέα) την ταυτότητα του αποστολέα (αυθεντικότητα). Η ψηφιακή υπογραφή είναι ένας τρόπος αυθεντικοποίησης του αποστολέα του μηνύματος.

Μία ψηφιακή υπογραφή μπορεί να πλαστογραφηθεί εάν ο δικαιούχος του ιδιωτικού κλειδιού δεν το έχει υπό τον πλήρη έλεγχό του (π.χ. χάσει το μέσο στο οποίο έχει αποθηκευτεί το ιδιωτικό κλειδί).

4.4. Ψηφιακά πιστοποιητικά

Προκειμένου να γίνει χρήση της κρυπτογράφησης δημοσίου κλειδιού θα πρέπει να παραχθεί ένα δημόσιο και ένα ιδιωτικό κλειδί. Δεν υπάρχει καμιά εγγύηση για το ποιος είναι αυτός που κρατά το ιδιωτικό κλειδί. Λύση στο πρόβλημα αυτό δίνει η ύπαρξη της *Αρχής Πιστοποίησης* (Certificate Authority, CA). Η CA είναι μια έμπιστη τρίτη οντότητα η οποία *εκδίδει ψηφιακά πιστοποιητικά* υπογεγραμμένα με το ιδιωτικό κλειδί της, τα οποία περιέχουν το όνομα και το δημόσιο κλειδί κάποιας οντότητας. Όταν ένας χρήστης θέλει να στείλει το δημόσιο κλειδί του σε κάποιον άλλο χρήστη, του στέλνει το πιστοποιητικό αυτό.

Ο Πάροχος Υπηρεσιών Πιστοποίησης είναι η οντότητα που παρέχει την υπηρεσία εκείνη με την οποία πιστοποιείται η σχέση ενός προσώπου με το δημόσιο κλειδί του. Ο τρόπος με τον οποίο γίνεται αυτό, είναι με την έκδοση ενός πιστοποιητικού (ένα ηλεκτρονικό αρχείο) στο οποίο ο Πάροχος Υπηρεσιών Πιστοποίησης πιστοποιεί την ταυτότητα του προσώπου και το δημόσιο κλειδί του.

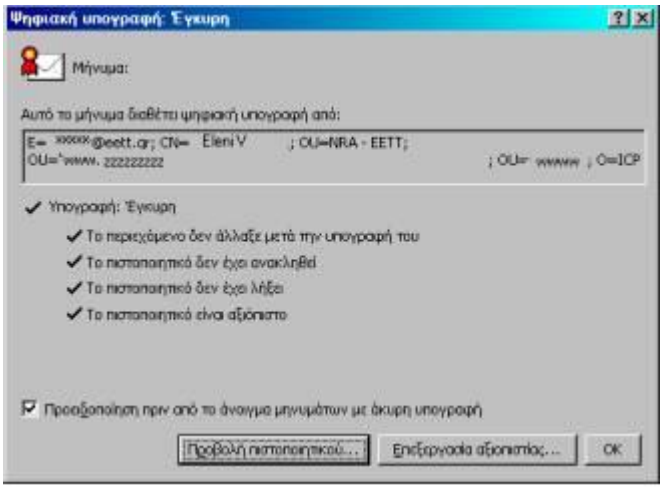
Από τους σημαντικότερους τύπους ψηφιακών πιστοποιητικών είναι το πιστοποιητικό δημοσίου κλειδιού (public key certificate). Ο στόχος του πιστοποιητικού δημοσίου κλειδιού είναι η δημιουργία μιας σχέσης ταυτοποίησης μεταξύ του δημοσίου κλειδιού και του δικαιούχου του. Το πιστοποιητικό αναφέρει το δημόσιο κλειδί (το οποίο και είναι το αντικείμενο του πιστοποιητικού) και επιβεβαιώνει ότι το συγκεκριμένο πρόσωπο που αναφέρεται στο πιστοποιητικό είναι ο δικαιούχος του αντίστοιχου ιδιωτικού κλειδιού. Έτσι ο παραλήπτης που λαμβάνει ένα μήνυμα με ψηφιακή υπογραφή, μπορεί να είναι σίγουρος ότι το μήνυμα έχει σταλεί από το πρόσωπο που το υπογράφει.

Το ψηφιακό πιστοποιητικό, είναι στον ηλεκτρονικό κόσμο ότι είναι το διαβατήριο στο φυσικό κόσμο. Η συσχέτιση ενός δημοσίου κλειδιού με τον δικαιούχο του γίνεται με χρήση της ψηφιακής υπογραφής του Παρόχου Υπηρεσιών Πιστοποίησης, όπου ο Πάροχος με την ψηφιακή του υπογραφή, υπογράφει το πιστοποιητικό του δικαιούχου. Αν ένας χρήστης εμπιστεύεται έναν Πάροχο Υπηρεσιών Πιστοποίησης, εμπιστεύεται και το πιστοποιητικό που ο Πάροχος εκδίδει.

Σχήμα 12: Παράδειγμα προβολής πιστοποιητικού

Ένας Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να έχει πιστοποιήσει ή να έχει πιστοποιηθεί από έναν άλλον, στα πλαίσια μίας σχέσης εμπιστοσύνης. Αν ο χρήστης δεν γνωρίζει έναν Πάροχο και δεν ξέρει αν πρέπει να εμπιστευθεί ένα πιστοποιητικό που αυτός έχει εκδώσει, και ο Πάροχος αυτός έχει δημιουργήσει μία σχέση εμπιστοσύνης με έναν άλλο Πάροχο που ο χρήστης εμπιστεύεται, τότε ο χρήστης μπορεί να εμπιστευθεί τον πρώτο Πάροχο. Ο χρήστης, μπορεί να επαληθεύσει τη ψηφιακή υπογραφή του Παρόχου Υπηρεσιών Πιστοποίησης που έχει εκδώσει ένα ψηφιακό πιστοποιητικό, χρησιμοποιώντας το δημόσιο κλειδί του Παρόχου, για το οποίο (δημόσιο κλειδί) ένας άλλος Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να έχει εκδώσει πιστοποιητικό κ.λπ.

Σχήμα 12: Ένδειξη ψηφιακής υπογραφής σε μήνυμα με πιστοποιητικό



Ένα πιστοποιητικό εφόσον διαπιστωθεί ή υπάρχει υπόνοια ότι για κάποιους λόγους δεν είναι έγκυρο (π.χ. αν το ιδιωτικό κλειδί του δικαιούχου έχει γίνει γνωστό σε τρίτους ή το πρόσωπο εξαπάτησε τον Πάροχο Υπηρεσιών Πιστοποίησης ως προς τα στοιχεία της ταυτότητάς του κ.λπ), τότε ο Πάροχος Υπηρεσιών Πιστοποίησης προβαίνει στην ανάκλησή του, όπως ρυθμίζεται από τη νομοθεσία.

4.5. Ψηφιακός φάκελος

Οι ψηφιακοί φάκελοι (digital envelope) είναι η διαδικασία κρυπτογράφησης ενός μυστικού κλειδιού μαζί με το δημόσιο κλειδί του αποδέκτη. Το μυστικό κλειδί πρέπει πρώτα να ανοιχθεί, και στη συνέχεια να αποκρυπτογραφηθεί το περιεχόμενο του μηνύματος με αυτό.

Συνεπώς μόνο ο αποδέκτης που γνωρίζει το μυστικό κλειδί μπορεί να αποκρυπτογραφήσει και εν συνεχεία χρησιμοποιώντας το, μπορεί να αναγνώσει το κείμενο που έχει κρυπτογραφηθεί συμμετρικά. Προκειμένου να επιτευχθεί αυτή η ανταλλαγή μυστικού κλειδιού υπάρχουν συγκεκριμένα πρωτόκολλα, με ευρύτερα γνωστό και χρησιμοποιούμενο το Diffie Hellman Key Exchange.

4.6. Πιστοποιητικό συναλλαγής

Ένα πιστοποιητικό συναλλαγής (transaction certificate) βεβαιώνει κάποιο γεγονός που αφορά στον τρόπο πραγματοποίησης μίας συναλλαγής και μ' αυτό μπορεί να αποφευχθεί η αποποίηση ευθύνης.

4.7. Χρονικό γραμματόσημο – σφραγίδα

Παρόμοια το χρονικό γραμματόσημο (time stamp) είναι μία ψηφιακή βεβαίωση, η οποία δεν επιδέχεται πλαστογράφηση, ότι ένα έγγραφο υπήρξε σε μία συγκεκριμένη χρονική στιγμή.

4.8. Τα πρωτόκολλα SSL/TLS (Secure Socket Layer/ Transport Layer Security) και SET (Secure Electronic Transactions)

4.8.1. Περιγραφή SSL

Το πρωτόκολλο SSL (Secure Sockets Layer) χρησιμοποιήται από τα Εικονικά Ιδιωτικά Δίκτυα (VPN) Επιπέδου Εφαρμογής ώστε να υλοποιούν επικοινωνίες μέσω επισφαλών καναλιών του Internet, διαφυλάσσοντας κάποιο συγκεκριμένο επίπεδο ασφάλειας. Στην πραγματικότητα, ένα SSL VPN παρέχει στους τελικούς χρήστες εξουσιοδοτημένη και ασφαλή πρόσβαση σε εφαρμογές όπως HTTP, client/server και file sharing.

Το πρωτόκολλο SSL είναι οικείο στους περισσότερους χρήστες, ακόμα και σε εκείνους χωρίς ιδιαίτερο υπόβαθρο τεχνικών γνώσεων. Είναι ήδη εγκατεστημένο σε οποιοδήποτε Η/Υ που είναι συνδεδεμένος στο Διαδίκτυο και χρησιμοποιεί έναν standard browser χωρίς κάποια ιδιαίτερη ρύθμιση. Το SSL είναι ανεξάρτητο από το λειτουργικό σύστημα και επιτρέπει την κλιμάκωση στον έλεγχο πρόσβασης στις εφαρμογές, καθιστώντας το ιδανικό για «κινητούς» χρήστες που επιθυμούν να έχουν πρόσβαση από ένα μη «ασφαλές» άκρο (endpoint). Είναι δυνατόν να προσφέρει έλεγχο πρόσβασης σε extranet VPNs ή VPNs απομακρυσμένης πρόσβασης. Επίσης ο χρήστης, μέσω ενός SSL VPN, έχει πρόσβαση σε εφαρμογές Web από οπουδήποτε με την απλή χρήση ενός Web browser, μίας σύνδεσης στο Internet, και χωρίς την ανάγκη ύπαρξης κάποιου ιδιαίτερου λογισμικού στον υπολογιστή του.

Τα SSL VPNs μπορούν να «περάσουν» πάνω από firewalls και να αντιμετωπίσουν θέματα NAT (Network Address Translation), ζητήματα τα οποία επιλύονται δύσκολα στην περίπτωση των IPSec VPNs.

Η ασφαλής σύνδεση που παρέχεται με το πρωτόκολλο SSL επιτυγχάνεται μέσω:

- Πιστοποίησης της ταυτότητας των πλευρών που επικοινωνούν και
- Κρυπτογράφησης της κίνησης που πραγματοποιείται μεταξύ τους.

Διευκρινίζεται ότι τα SSL VPNs αφορούν εφαρμογές που υποστηρίζουν το πρωτόκολλο SSL, όπως για παράδειγμα Web browsers και Web-based e-mail.

4.8.2. Εφαρμογές SSL

Η πιο κοινή εφαρμογή του πρωτοκόλλου SSL είναι η διασφάλιση HTTP επικοινωνιών μεταξύ του browser και του web server. Η ασφαλής έκδοση του HTTP χρησιμοποιεί URLs που ξεκινούν με "https" αντί του κανονικού "http" και διαφορετική πόρτα (port) που είναι η προκαθορισμένη «πόρτα» 443. Το πρωτόκολλο SSL παρέχει κρυπτογράφηση σε επίπεδο εφαρμογής για Web browsers και άλλες εφαρμογές. Χρησιμοποιείται διεθνώς για μεταφορά ευαίσθητων οικονομικά δεδομένων.

Πιο συγκεκριμένα, το SSL χρησιμοποιείται γενικά σε διακομιστές Web για την υποστήριξη εφαρμογών ηλεκτρονικού εμπορίου, ηλεκτρονικών τραπεζικών υπηρεσιών και άλλων εφαρμογών που απαιτούν ασφάλεια των επικοινωνιών.

Για παράδειγμα, κατά τη διάρκεια ηλεκτρονικών τραπεζικών συναλλαγών, η τεχνολογία SSL χρησιμοποιείται για την κρυπτογράφηση των προσωπικών στοιχείων του χρήστη πριν απομακρυνθούν από τον υπολογιστή του, κατά τέτοιο τρόπο ώστε να μην είναι εφικτή η ανάγνωση από τρίτα άτομα. Το SSL εμποδίζει την υποκλοπή ευαίσθητων πληροφοριών (π.χ. αριθμοί πιστωτικών καρτών, υπόλοιπο λογαριασμών και άλλα οικονομικά και προσωπικά στοιχεία) που στέλνονται μέσω Internet μεταξύ του browser του χρήστη και ενός διακομιστή web κατά τη διάρκεια ηλεκτρονικών συναλλαγών.

Σύμφωνα με όσα αναφέρθηκαν παραπάνω, το πρωτόκολλο SSL υλοποιεί χαρακτηριστικά VPN αφού παρέχει κρυπτογράφηση δεδομένων, πιστοποίηση του server και προαιρετικά της ταυτότητας του client και εξασφαλίζει την ακεραιότητα των δεδομένων.

Τα SSL VPNs είναι κατάλληλα για να παρέχουν ασφάλεια σε εφαρμογές απομακρυσμένης πρόσβασης, όπως εφαρμογές Web, εφαρμογές client/server και εφαρμογές file sharing. Επιπλέον το SSL χρησιμοποιεί τον αλγόριθμο RSA για την ανταλλαγή του κλειδιού κρυπτογράφησης μεταξύ των δύο πλευρών.

Τα SSL VPNs υλοποιούν:

- Κρυπτογράφηση (40-bit ή 128-bit RC4,168-bit 3DES, 128-bit AES)
- Πιστοποιήση (Username/Password ή X509 ψηφιακά πιστοποιητικά)

Σχήμα 13: Αλγόριθμοι κρυπτογράφησης SSL

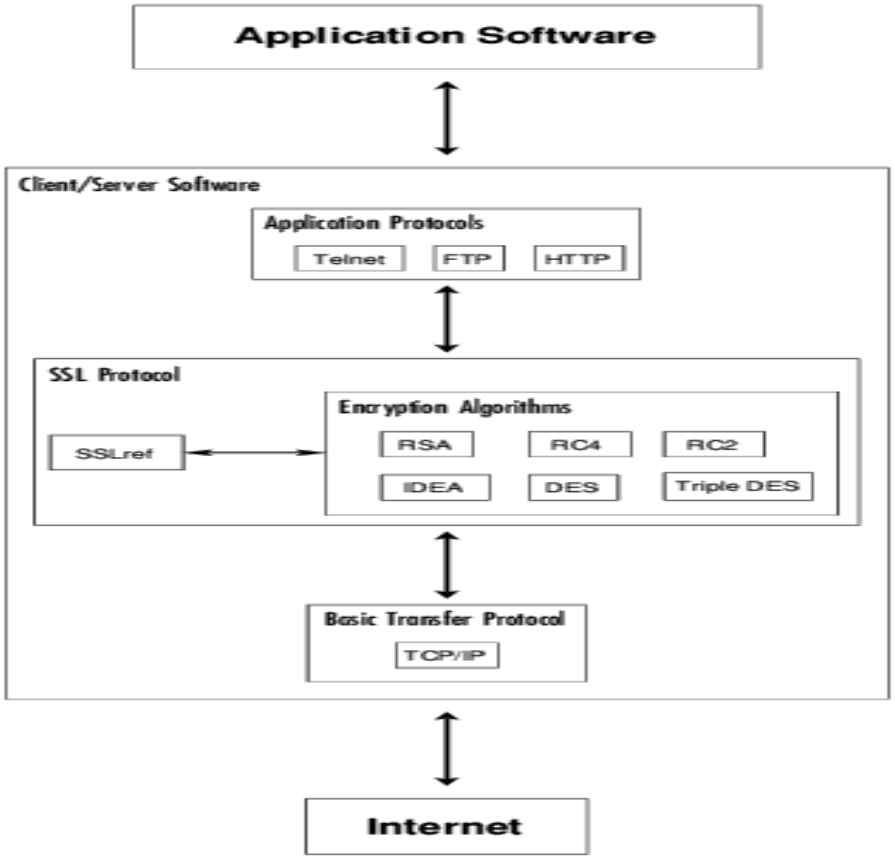
Block Ciphers		Stream Ciphers	
Αλγόριθμος	Μέγεθος κλειδιού	Αλγόριθμος	Μέγεθος κλειδιού
IDEA	128	RC4-40	40
RC2-40	40	RC4-128	128
DES-40	40		
DES	56		
3DES	168		
Fortezza	80		

4.8.3. Μηχανισμοί Ασφάλειας στο SSL

Η ασφάλεια των SSL VPNs βασίζεται στους μηχανισμούς ασφάλειας του πρωτοκόλλου SSL. Το πρωτόκολλο SSL αναπτύχθηκε από την Netscape Communications Corporation για την ασφαλή επικοινωνία ευαίσθητων πληροφοριών όπως προσωπικά στοιχεία και αριθμούς πιστωτικών καρτών. Η πρώτη σχεδίαση του πρωτοκόλλου έγινε τον Ιούλιο του 1994 και αποτελούσε την πρώτη έκδοση (version 1.0) και τον Οκτώβριο του ίδιου χρόνου δημοσιοποιήθηκε υπό την μορφή RFC (Request For Comments). Τον Δεκέμβριο του 1994 εκδίδεται μια επαναθεώρηση του πρωτοκόλλου, η δεύτερη έκδοση του (version 2.0). Ωστόσο, το SSL version 2.0 είχε αρκετούς περιορισμούς τόσο ως προς την κρυπτογραφική ασφάλεια όσο και ως προς τη λειτουργικότητά του. Έτσι το πρωτόκολλο αναβαθμίστηκε σε SSL v.3.0 με δημόσια αναθεώρηση και σημαντική συνεισφορά από τη βιομηχανία. Αυτή η νέα έκδοση του πρωτοκόλλου SSL τέθηκε επισήμως σε κυκλοφορία το Δεκέμβριο του 1995. Το τελευταίο Internet Draft που προσδιορίζει το SSL v.3.0 κυκλοφόρησε το Νοέμβριο του 1996. Η περιγραφή του SSL βασίζεται σε αυτές τις τελευταίες προδιαγραφές του πρωτοκόλλου. Η τελευταία έκδοση του SSL μετεξελίχτηκε στο TLS (Transport Layer Security).

Το πρωτόκολλο SSL στρωματοποιείται στην κορυφή μίας αξιόπιστης υπηρεσίας μεταφοράς όπως εκείνη που παρέχεται από το TCP/IP και είναι σε θέση να παρέχει υπηρεσίες ασφάλειας για αυθαίρετες TCP/IP εφαρμογές. Στην πραγματικότητα, ένα σημαντικό πλεονέκτημα της ασφάλειας επιπέδου μεταφοράς γενικά και του SSL ειδικότερα είναι η ανεξαρτησία από την εφαρμογή, που σημαίνει ότι μπορεί να χρησιμοποιηθεί για να παρέχει ασφάλεια διαφανώς (transparently) σε οποιαδήποτε TCP/IP εφαρμογή στρωματοποιείται στην κορυφή του.

Σχήμα 13: το πρωτόκολλο SSL



Συνοπτικά, μπορεί να αναφερθεί ότι το πρωτόκολλο SSL παρέχει TCP/IP ασφάλεια σύνδεσης μεταξύ δύο συστημάτων, από τα οποία το ένα λειτουργεί σαν server (εξυπηρέτης) και το άλλο σαν client (εξυπηρετούμενος).

Αυτή η ασφάλεια έχει τρεις βασικές ιδιότητες:

- Γίνεται πιστοποίηση ταυτότητας και των δύο χρηστών, μέσω κρυπτογραφίας δημόσιου κλειδιού.
- Επιτυγχάνεται εμπιστευτικότητα των μεταδιδόμενων δεδομένων μέσω κρυπτογράφησης.
- Προστατεύεται η ακεραιότητα των μεταδιδόμενων δεδομένων με χρήση MACs.

4.8.4. Αντοχή του πρωτοκόλλου SSL σε επιθέσεις

Στη συνέχεια θα αναφερθεί η «αντοχή» του πρωτοκόλλου SSL σε κάποια είδη επιθέσεων καθώς επίσης και οι αδυναμίες του. Αξίζει να σημειωθεί ότι το SSL πρωτόκολλο δεν παρέχει προστασία έναντι επιθέσεων ανάλυσης κυκλοφορίας (traffic analysis). Για παράδειγμα, ένας αναλυτής κυκλοφορίας εξετάζοντας τις μη κρυπτογραφημένες IP διευθύνσεις αποστολέα και παραλήπτη, καθώς και τους TCP αριθμούς θυρών, μπορεί τελικά να καταγράψει ποια μέρη αλληλεπιδρούν ή ποιοι τύποι υπηρεσιών χρησιμοποιούνται.

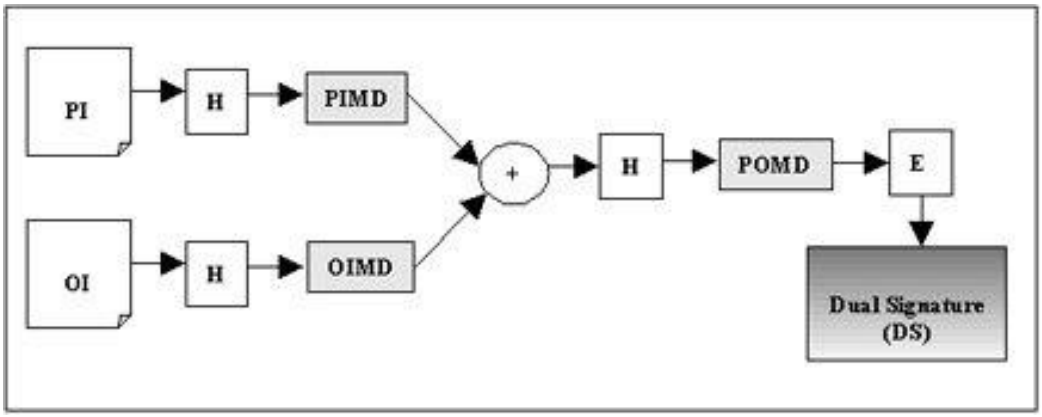
- ✓ *Επίθεση Λεξικού* (Dictionary Attack)*:* Μπορεί να εφαρμοστεί από έναν «επιτιθέμενο» όταν ένα μέρος του μη κρυπτογραφημένου κειμένου είναι στην κατοχή του. Τότε το μέρος αυτό κρυπτογραφείται με χρήση κάθε πιθανού κλειδιού και έπειτα ερευνάται ολόκληρο το κρυπτογραφημένο μήνυμα μέχρι να βρεθεί κομμάτι του που να ταιριάζει με κάποιο από τα προϋπολογισμένα. Σε περίπτωση που η έρευνα έχει επιτυχία, τότε το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση ολόκληρου του μηνύματος έχει βρεθεί. Το SSL δεν απειλείται από αυτήν την επίθεση όταν τα κλειδιά των αλγορίθμων του είναι μεγέθους 128 bit.
- ✓ *Επίθεση Βίαιη* (Brute Force Attack): Πραγματοποιείται με την χρήση όλων των πιθανών κλειδιών για την αποκρυπτογράφηση των μηνυμάτων. Όσο πιο μεγάλα σε μήκος είναι τα χρησιμοποιούμενα κλειδιά, τόσο πιο πολλά είναι τα πιθανά κλειδιά. Τέτοια επίθεση σε αλγορίθμους που χρησιμοποιούν κλειδιά των 128 bits είναι χωρίς νόημα (τα 2^{128} κλειδιά που καλείται να υπολογίσει κανείς είναι απίστευτα μεγάλος αριθμός). Μόνο ο DES των 56 bits είναι ευαίσθητος σε αυτήν την επίθεση.
- ✓ *Επίθεση Επανάληψης* (Replay Attack): Όταν ένας τρίτος καταγράφει την ανταλλαγή μηνυμάτων μεταξύ client και server και προσπαθεί ξανά να χρησιμοποιήσει τα μηνύματα του client για να αποκτήσει πρόσβαση στον server, έχουμε την επίθεση *replay attack*. Όμως το SSL κάνει χρήση του connection-id, το οποίο παράγεται από τον server με τυχαίο τρόπο και διαφέρει για κάθε σύνοδο (κάθε σύνοδος έχει το δικό της id, που ορίζεται κατά την έναρξη των διαδικασιών του Handshake πρωτοκόλλου). Έτσι δεν είναι δυνατόν πότε να υπάρχουν δυο ίδια connection-id. Το connection-id έχει μέγεθος 128 bit για πρόσθετη ασφάλεια.
- ✓ *Επίθεση Man-In-The-Middle:* Συμβαίνει όταν ένας τρίτος είναι σε θέση να παρεμβάλλεται στην επικοινωνία μεταξύ του server και του client. Αφού επεξεργαστεί τα μηνύματα του client και τα τροποποιήσει όπως αυτός επιθυμεί, τα προωθεί στον server. Ομοίως πράττει για τα μηνύματα που προέρχονται από τον server. Δηλαδή, προσποιείται στον client ότι είναι ο server και αντίστροφα. Όμως όπως ήδη είδαμε το SSL υποχρεώνει τον server να αποδεικνύει την ταυτότητα του με την χρήση έγκυρου πιστοποιητικού του οποίου η τροποποίηση είναι αδύνατη. Συνεπώς, ο επιτιθέμενος δεν μπορεί να πείσει τον client ότι είναι ο server.

4.8.5. Περιγραφή SET (Secure Electronic Transactions)

Το SET είναι ένα πρωτόκολλο εμπορικών συναλλαγών με τη χρήση καρτών, που σχεδιάστηκε αρχικά από τη Visa και τη MasterCard σαν μία μέθοδος εξασφάλισης των συναλλαγών, κι από τότε έχει εξελιχθεί αρκετά. Το πρωτόκολλο SET βασίζεται στη χρήση *κρυπτογράφησης δημόσιου κλειδιού* και χρησιμοποιεί τα *ψηφιακά πιστοποιητικά* για την πιστοποίηση της ταυτότητας των συμμετεχόντων σε μία συναλλαγή.

Το πρωτόκολλο SET λειτουργεί με έναν πολύ ενδιαφέροντα τρόπο και κάνει χρήση της έννοιας της διπλής υπογραφής. Χρησιμοποιεί διπλές υπογραφές για να εξασφαλίσει μια συναλλαγή. Απαιτεί την αγορά του λογισμικού που θα χρησιμοποιηθεί για ένα e-commerce site. Ο σχεδιασμός του πρωτοκόλλου SET απαιτεί την εγκατάσταση ενός e-πορτοφόλι για τον πελάτη.

Σχήμα 12: Το πρωτόκολλο SET

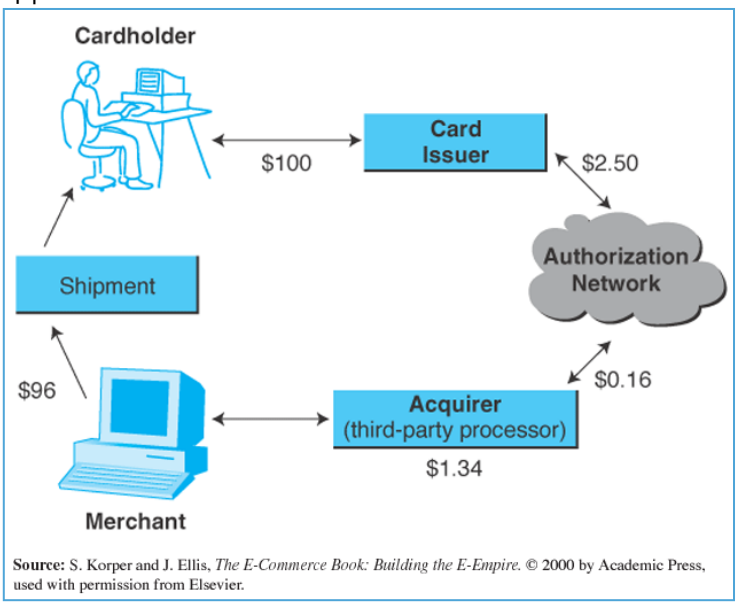


4.8.6. Τα εμπλεκόμενα μέρη σε μια συναλλαγή SET

- *Κάτοχος* - Cardholder Wallet: Χρήση του Διαδικτύου, οι καταναλωτές και εταιρικούς αγοραστές αλληλεπιδρούν με τους εμπόρους για την αγορά αγαθών και υπηρεσιών. Ένας κάτοχος της κάρτας είναι ένας εξουσιοδοτημένος κάτοχος της κάρτας πληρωμής, όπως η MasterCard ή Visa που έχει εκδοθεί από εκδότη (συζητηθούν στη συνέχεια).
- *Έμπορος* - Merchant Server**:** Ένας έμπορος είναι ένα άτομο ή μια οργάνωση που θέλει να πωλούν αγαθά ή τις υπηρεσίες για τους κατόχους της κάρτας. Ένας έμπορος πρέπει να έχει μια σχέση με έναν Απορροφώσας Εταιρείας, (συζητούνται στη συνέχεια) για την αποδοχή πληρωμών μέσω του Διαδικτύου.
- *Εκδότης* - Issuer **:** Ο εκδότης είναι ένα χρηματοπιστωτικό ίδρυμα (όπως μια τράπεζα), η οποία παρέχει μια κάρτα πληρωμής σε ένα κάτοχο της κάρτας. Το πιο κρίσιμο σημείο είναι ότι ο εκδότης είναι η τελική ευθύνη για την καταβολή της οφειλής του κατόχου της κάρτας.

- *Αποκτών* - Acquirer **:** Αυτό είναι ένα χρηματοπιστωτικό ίδρυμα που έχει σχέση με τους εμπόρους για τις άδειες των καρτών πληρωμής επεξεργασία και πληρωμές. Ο λόγος για το γεγονός ότι οι αγοραστές είναι ότι οι έμποροι δέχονται πιστωτικές κάρτες από περισσότερο από ένα εμπορικό σήμα, αλλά δεν ενδιαφέρονται για την αντιμετώπιση με τόσες πολλές bankcard οργανισμούς ή τους εκδότες. Αντ 'αυτού, ο αγοραστής παρέχει στον έμπορο μια βεβαιότητα (με τη βοήθεια του εκδότη) ότι ένας συγκεκριμένος λογαριασμός του κατόχου της κάρτας είναι ενεργό και ότι το ποσό της αγοράς δεν υπερβαίνει τα όρια πίστωσης, κ.λπ. Ο αποκτών παρέχει επίσης ηλεκτρονική μεταφορά κεφαλαίων στο λογαριασμό του εμπόρου. Αργότερα, ο εκδότης αποζημιώνει τον αγοραστή χρησιμοποιώντας κάποιο δίκτυο πληρωμών.
- *Πύλη πληρωμής* - Payment Gateway **:** Αυτό είναι ένα έργο μπορεί να ληφθεί από τον αγοραστή ή μπορεί να ληφθεί από μια οργάνωση ως μια ειδική λειτουργία. Η πύλη πληρωμής επεξεργάζεται τα μηνύματα πληρωμής για λογαριασμό του εμπόρου. Συγκεκριμένα στο SET, η πύλη πληρωμής ενεργεί ως διεπαφή μεταξύ SET και τα υπάρχοντα δίκτυα καρτών πληρωμών για άδειες πληρωμής. Οι εμπορικές ανταλλαγές SET μηνύματα με την πύλη πληρωμών μέσω του Διαδικτύου. Η πύλη πληρωμής, με τη σειρά του, συνδέεται με τα συστήματα του αγοραστή, χρησιμοποιώντας μια ειδική γραμμή του δικτύου, στις περισσότερες περιπτώσεις.
- *Αρχή Πιστοποίησης* - Certificate Authority (CA): Αυτή είναι μια αρχή που είναι αξιόπιστοι να παρέχουν πιστοποιητικά δημόσιου κλειδιού προς τους κατόχους καρτών, εμπόρους και πύλες πληρωμής. Στην πραγματικότητα, οι αρμόδιες αρχές είναι πολύ κρίσιμη για την επιτυχία του SET.

Σχήμα 14: Συναλλαγή SET



Source: S. Korper and J. Ellis, *The E-Commerce Book: Building the E-Empire.* © 2000 by Academic Press, used with permission from Elsevier.

4.8.7. Εφαρμογές SET

- Εγγραφή του κατόχου πιστωτικής κάρτας
- Αίτηση αγοράς
- Έγκριση πληρωμής
- Ερώτημα για το πιστοποιητικό
- Έρευνα αγοράς
- Κοινοποίηση αγοράς
- Συναλλαγή πώλησης

4.8.8. Λειτουργίες SET

- Ανοιχτή κρυπτογράφηση και προδιαγραφές ασφαλείας
- Προστασία Internet σε συναλλαγές με πιστωτική κάρτα
- Είναι μια σειρά από πρωτόκολλα και μορφές ασφάλειας
- Είναι ένα πρωτόκολλο πληρωμής
- Ασφαλείς επικοινωνίες μεταξύ των μερών (πελατών-τραπεζών)
- Χρήση των πιστοποιητικών X.509v3 από όλα τα μέρη
- Προστασία της ιδιωτικής ζωής με περιορισμένες πληροφορίες σε όσους τη χρειάζονται.

4.8.9. Οι διαφορές μεταξύ SSL και SET

- Το SET αναπτύχθηκε ειδικά για να εξασφαλίσει μια πράξη πληρωμής.
  - Το SSL από την άλλη πλευρά δεν είναι ένα πρωτόκολλο πληρωμής. Κρυπτογραφεί απλά το κανάλι επικοινωνίας μεταξύ του κατόχου και την ιστοσελίδα του εμπόρου, και δεν υποστηρίζεται από οποιοδήποτε χρηματοπιστωτικό ίδρυμα. Ως αποτέλεσμα, το SSL δεν μπορεί να εγγυηθεί μια συναλλαγή.
- Με το SET, ολόκληρο το περιβάλλον επεξεργασίας συναλλαγών εξασφαλίζεται από την επιφάνεια εργασίας του κατόχου της κάρτας, μέσω της ιστοσελίδας του εμπόρου, και την απόκτηση τραπεζικής πύλης πληρωμών. Σχεδιάστηκε ειδικά για να αντιμετωπίσει την ασφάλεια όλων των μερών σε μια ηλεκτρονική συναλλαγή πληρωμής, ενσωματώνει κρυπτογράφηση 1024-bit σε όλη τη συναλλαγή.
  - Το SSL, από την άλλη πλευρά, το οποίο αναπτύχθηκε μόνο για την αποφυγή αλλοίωσης των δεδομένων σε εφαρμογές client / server, έχει συγκριτικά ασθενέστερη κρυπτογράφησης, σε ένα μέγιστο των 128-bit.

- Το SET πιστοποιεί επίσης όλα τα μέρη της συναλλαγής, διότι τα πιστοποιητικά του SET υποστηρίζεται όχι μόνο από μια αρχή έκδοσης πιστοποιητικών, αλλά και από τα χρηματοπιστωτικά ιδρύματα όπως είναι και η MasterCard International.
  - Το SSL δεν μπορεί να επικυρώσει επαρκώς όλα τα μέρη, επειδή τα πιστοποιητικά SSL δεν υποστηρίζονται από οποιοδήποτε χρηματοπιστωτικό ίδρυμα.
- Το SET παρέχει ασφάλεια σε όλη τη συναλλαγή της διαδικασίας-από την επιφάνεια εργασίας του κατόχου της κάρτας στον έμπορο μέσω εγκρίσεων τράπεζα και πίσω από την πύλη, αφήνοντας μια αδιάψευστη διαδρομή ελέγχου και, συνεπώς, μια εγγυημένη συναλλαγής.
  - Το SSL παρέχει μόνο την ασφάλεια μεταξύ του κατόχου της κάρτας και οι έμποροι-επαρκής ασφάλεια για την πρόληψη της απάτης. Η ασφάλεια των συναλλαγών SSL δεν είναι εγγυημένη.

4.9. Η Αυθεντικοποίηση των Πιστοποιημένων Μερών

Το επίπεδο ασφάλειας που προσφέρουν οι ελληνικές τράπεζες στους χρήστες της ηλεκτρονικής τραπεζικής , μπορούμε να πούμε ότι βρίσκεται σε ικανοποιητικό επίπεδο όμως τα περιθώρια βελτίωσης του είναι ακόμα μεγάλα αν κρίνουμε και από την συνεχή εμφάνιση νέων κινδύνων – απειλών στις ηλεκτρονικές συναλλαγές. Πιο συγκεκριμένα, στο σύνολό τους οι ελληνικές τράπεζες, γνωρίζουν όλους τους κινδύνους και τις απειλές που μπορούν να προκύψουν κατά τη χρήση καθώς επίσης, είναι ενημερωμένες και παρέχουν τους περισσότερους τρόπους με τους οποίους μπορούν να αντιμετωπιστούν οι κίνδυνοι αυτοί.

Βασική συνιστώσα της ανάπτυξης του M-Banking είναι φυσικά η διασφάλιση του απορρήτου των ηλεκτρονικών συναλλαγών και κατ'επέκταση και των προσωπικών δεδομένων. Έτσι σε συνδυασμό της κρυπτογράφησης- που προαναφέρθηκε- με τις διαδικασίες ταυτοποίησης και των δύο μερών η συναλλαγή οδηγείται σε επιτυχή ολοκλήρωση. Οι πελάτες του κινητής τραπεζικής θα πρέπει να επαγρυπνούν και να λαμβάνουν μέτρα σε συνεργασία με τα τραπεζικά ιδρύματα σε θέματα εξωτερικών απειλών.

4.9.1. Η Ταυτοποίηση του Πελάτου

4.9.1.1. LRAP: A Location-Based Remote Client Authentication Protocol for Mobile Environments

Τα δίκτυα κινητής τηλεφωνίας οδηγούνται από την ανάγκη να παρέχουν πιο προηγμένες υπηρεσίες στους κινητούς ή νομαδικών υπολογιστικών συσκευών, όπως οι υπηρεσίες ασφάλειας που απαιτούν έλεγχο ταυτότητας απομακρυσμένου υπολογιστή-πελάτη. Σε αυτές τις υπηρεσίες η τοποθεσία του χρήστη θα μπορούσε να χρησιμοποιηθεί ως παράγοντας ελέγχου ταυτότητας, πέραν των τυπικών παραγόντων ελέγχου ταυτότητας, όπως κωδικούς πρόσβασης, σε συνδυασμό με την χρήση μιας φυσικής συσκευής που ένα άτομο κατέχει, όπως μια κάρτα ή ένα τηλέφωνο. Δεδομένου ότι οι πληροφορίες τοποθεσίας ίδια υπόκειται σε επιθέσεις, επιπλέον μηχανισμοί θα πρέπει να χρησιμοποιηθούν για να πιστοποιούν την ακεραιότητά τους.

Το LRAP, ένα νέο πρωτόκολλο που συνδυάζει διάφορους παράγοντες για να επικυρώσουμε με ασφάλεια ένα κινητό χρήστη. Στο LRAP, η τοποθεσία του χρήστη μπορεί να προσδιοριστεί και η ορθότητα της είναι πιστοποιημένη από ένα τρίτο έμπιστο κόμμα, που ονομάζεται Τοπική Element. Η υπηρεσία πληρωμών, είναι μία ευρέως διαθέσιμη υπηρεσία ευάλωτη σε διάφορους τύπους επιθέσεων ασφάλειας, και προτείναμε μια υπηρεσία LRAP που βασίζεται στην αξιοποίηση ενός κωδικού χρόνου και πιστοποιημένης θέσης για ασφαλείς συναλλαγές πληρωμής.

4.9.1.2. Συνθηματικά UserID- Password- TAN

Ο προσωπικός κωδικός χρήστη (UserID) σε συνδυασμό με το εξίσου μυστικό συνθηματικό (Password) χρήζει μεγάλης σημασίας από άποψη ασφαλείας τόσο στο M-Banking όσο και στο E-Banking. Με γνώμονα την σωστή λειτουργικότητα αλλά και την επιτυχή ολοκλήρωση μίας συναλλαγής οι τράπεζες έχουν αναβαθμίσει το επίπεδο ασφαλείας προσθέτοντας νέους αριθμούς εξουσιοδότησης συναλλαγών- μίας χρήσεως- τους γνωστούς TAN (Transaction Authentication Number). Οι αριθμοί αυτοί αφού συνδεθούν με τον προσωπικό κωδικό κάθε χρήστη δίνονται σε αυτόν σε μία προτυπωμένη λίστα και χρησιμοποιούνται για τις συναλλαγές.

Οι χρήστες του M-Banking αλλά και του E-Banking θα πρέπει να λαμβάνουν κάποια μέτρα ασφαλείας για να αντιμετωπίσουν κακόβουλες πράξεις:

- Οι προσωπικοί κωδικοί ασφαλείας, UserID, Password, TAN κτλ., οι οποίοι τους παραχωρίθηκαν από τις τράπεζες, είναι τελείως προσωπικοί και δεν πρέπει να δίνονται σε κανέναν άλλο.
- Οι μυστικοί προσωπικοί αριθμοί θα πρέπει απομνημονεύονται και να μη φυλάσσονται σε οποιαδήποτε μορφή έντυπη ή ηλεκτρονική. Έτσι αποφεύγεται ο κίνδυνος υποκλοπής.
- Οι προσωπικοί κωδικοί θα πρέπει να αλλάζουν σε τακτά χρονικά διαστήματα και να έχουν την μορφή σύνθετων λέξεων και αριθμών οι οποίοι θα είναι δύσκολο να προβλεφθούν.
- Θα πρέπει να αποφεύγεται η αποθήκευση κάποιου λογισμικού στην μνήμη του κινητού τηλεφώνου από άγνωστο αποστολέα.
- Επιβάλεται η χρήση προγραμμάτων ασφαλείας malware, spyware που προστατεύουν από τους ιούς.
- Ο έλεγχος αυθεντικότητας της διεύθυνσης ιστοσελίδας που χρησιμοποιεί η τράπεζα, πριν εισάγει προσωπικούς κωδικούς και στοιχεία. Η επιβεβαίωση της ταυτότητας μπορεί να γίνει μέσα από τον έλεγχο ύπαρξης ή μη πιστοποιητικού ασφαλείας.

4.9.2. Πιστοποίηση της Τράπεζας

Η τράπεζες στην επιτακτική ανάγκη για μεγαλύτερη ικανοποίηση των βασικών απαιτήσεων του πελάτου για υψηλό επίπεδο ασφαλείας με σκοπό την επίτευξη ενός επιπέδου αξιοπιστίας χρησιμοποιούν- όπως αναλύθηκε παραπάνω- δύο τύπους κρυπτογράφησης. Έχοντας λάβει ήδη μέτρα για την διασφάλιση των συναλλασόμενων μερών, προχωρούν ακόμα πιο πέρα υοθετώντας παράλληλα νέες πολιτικές ασφαλείας σε ότι αφορά το Hardware αλλά και το Software στις ηλεκτρονικές συναλλαγές.

Η αυθεντικοποίηση της τράπεζας είναι απαραίτητη για την διασφάλιση του απορρήτου κατά τη μεταφορά δεδομένων. Επιδιώκοντας λοιπόν την παροχή ενός ασφαλούς καναλιού επικοινωνίας με τους πελάτες τους σε όλα τα στάδια της συναλλαγής επιλέγεται από την τράπεζα μία *Αρχή Πιστοποίησης*, η οποία μπορεί να είναι είτε έμπιστος τρίτος φορέας (TTP Trust Third Party), είτε να λειτουργεί στα πλαίσια ενός οργανισμού. Με τον τρόπο αυτό πιστοποιεί την ταυτότητα της στις ηλεκτρονικές συναλλαγές. Επομένως τα ψηφιακά πιστοποιητικά, οι ψηφιακές υπογραφές χρησιμοποιούνται για την αναγνώριση της οντότητας της τράπεζας. Η χρήση των πιστοποιητικών γίνεται σε συνόδους με βάση το πρωτόκολλο SMAC στο M-Banking και στο WTLS στο WAP Banking.

4.10. Απειλές και Κίνδυνοι

Καθώς όλο και περισσότερες τράπεζες παρέχουν on-line υπηρεσίες στους πελάτες τους, τόσο πληθαίνουν οι ηλεκτρονικές επιθέσεις. Είναι δεδομένο οτι οι οικονομικές πληροφορίες είναι άκρως απόρρητες πράγμα που τις καθιστά ευάλωτες στο ηλεκτρονικό έγκλημα.

Έρευνες που έχουν γίνει από ειδικούς σε θέματα ασφαλείας αποδεικνύουν οτι οι εισβολείς τις πιο πολλές φορές χρησιμοποιούν τον ανθρώπινο παράγοντα εκμεταλλεύομενοι την πρόσβαση που έχουν οι πελάτες της τράπεζας από το σπίτι τους, οι περισσότεροι από αυτούς δεν χρησιμοποιούν λογισμικό ασφαλείας.

Οι κίνδυνοι που συχνά αντιμετωπίζονται είναι:

- *Sniffers*. Τεχνολογία υποκλοπής δεδομένων. Είναι ένα πρόγραμμα ή συσκευή που παρακολουθεί την κίνηση ενός δικτύου με σκοπό να αποσπάσει πληροφορίες που ταξιδεύουν σε αυτό.
- *Key Loggers*. Η καταγραφή πληκτρολογήσεων χωρίς ο χρήστης να το ξέρει ή να το επιτρέπει. Το ειδικό λογισμικό είναι εύκολο να εγκατασταθεί και παράλληλα δύσκολο να εντοπιστεί. Χρησιμοποιείται για την κλοπή στοιχείων τραπεζικών συναλλαγών και προσωπικών κωδικών.
- *Phishing*. Είναι η αποστολή e-mail στον χρήστη από μία υποτιθέμενα νόμιμη επιχείρηση, κυρίως τράπεζα, με σκοπό την απόσπαση πληροφοριών που θα βοηθήσουν στην κλοπή της ταυτότητα του.
- *Pharming*. Είναι μία μορφή απάτης της ηλεκτρονικής διεύθυνσης (Domain Name). Με τον τρόπο αυτό οι χρήστες νομίζουν οτι βρίσκονται σε μία γνήσια ιστοσελίδα του τραπεζικού ιδρύματος, ενώ στην πραγματικότητα έχουν κατευθυνθεί σε μία ψεύτικη. Τέτοιου είδους εκτροπή δεν μπορεί να γίναι στις ιστοσελίδες που χρησιμοποιούν το πρωτόκολλο SSL.
- *Trojan Horse*. Οι λεγόμενοι και Δούρειοι Ίπποι είναι ένα πρόγραμμα υπολογιστή που περιλαμβάνει κρυφές εντολές που δημιουργούν βλάβες στον υπολογιστή όταν οι χρήστες το ανοίξουν διότι θεωρούν οτι έρχεται από κάποιο φαινομενικά νόμιμο αποστολέα. Αντιγράφουν τις κινήσεις που μπορεί να κάνει ο χρήστης όπως:
    - Αντιγραφή, Διαγραφή αρχείων
    - Αλλαγή αρχειών, όπου ο χρήστης έχει δικαίωμα μεταβολής
    - Μετάδοση αρχείων στο εισβολέα
    - Εγκατάσταση προγραμμάτων χωρίς την έγκριση του χρήστη
    - Εγκατάσταση ιών και άλλων δούρειων ίππων

4.11. Δίωξη Ηλεκτρονικού Εγκλήματος

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, της Ελληνικής Αστυνομίας, ενημερώνει τους πολίτες, που χρησιμοποιούν την ηλεκτρονική τραπεζική (e-banking) για την εμφάνιση ενός νέου κακόβουλου λογισμικού, που στοχεύει στην παράνομη πρόσβαση του τραπεζικού τους λογαριασμού (Banking Malware).

Ειδικότερα, το νέο κακόβουλο λογισμικό έχει τη δυνατότητα να υποκλέπτει τα ηλεκτρονικά στοιχεία πρόσβασης του e-banking (username, password, κτλ), αλλά και να «συλλέγει» τα δεδομένα της κίνησης του δικτύου του χρήστη (sniff network traffic), υποκλέπτοντας ευαίσθητα δεδομένα και των υπολοίπων χρηστών που είναι συνδεδεμένοι σε αυτό. Το εν λόγω λογισμικό, που ονομάστηκε ως «EMOTET», εξαπλώνεται γρήγορα μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου. Πιο συγκεκριμένα, στον χρήστη αποστέλλεται μήνυμα (e-mail), το οποίο τον ενημερώνει για κάποια μεταφορά ποσού, που έγινε στο τραπεζικό του λογαριασμό και το οποίο περιέχει σύνδεσμο (link) για περισσότερες πληροφορίες σχετικά με την επίμαχη τραπεζική μεταφορά. Μόλις ο χρήστης πατήσει στο σύνδεσμο (link), που περιέχεται στο μήνυμα ηλεκτρονικού ταχυδρομείου, αρχίζει η διαδικασία εγκατάστασης του κακόβουλου λογισμικού, εν αγνοία του χρήστη.

Σημειώνεται ότι το κακόβουλο λογισμικό έχει την ικανότητα να παρακάμπτει ακόμα και την ασφαλή σύνδεση HTTPS (Hypertext Transfer Protocol Secure). Το γεγονός αυτό αυξάνει τον κίνδυνο υποκλοπής των ηλεκτρονικών στοιχείων εισόδου στο e-banking, καθώς οι χρήστες θεωρούν ότι πραγματοποιούν τις online τραπεζικές τους συναλλαγές με ασφάλεια.

Οι πολίτες, που λαμβάνουν μηνύματα ηλεκτρονικού ταχυδρομείου με παρόμοιο περιεχόμενο καλούνται να μην ανοίγουν τους συνδέσμους, ούτε να κατεβάζουν τα αρχεία που περιέχονται σε αυτά. Σε κάθε περίπτωση, συστήνεται σε κάθε χρήστη η επιβεβαίωση των συναλλαγών μέσω του τραπεζικού του ιδρύματος. Κατ' αυτόν τον τρόπο επιβεβαιώνεται η ορθότητα του μηνύματος ηλεκτρονικού ταχυδρομείου πριν προχωρήσει σε περαιτέρω ενέργειες.

Επιπλέον, σε περίπτωση που ο χρήστης «πατήσει» τον σύνδεσμο σε παρόμοιο μήνυμα ηλεκτρονικού ταχυδρομείου, το οποίο έχει επιβεβαιωθεί για την πλαστότητά του, συστήνεται η επανεγκατάσταση του λειτουργικού συστήματος.

(Αθήνα, 29 Ιουνίου 2014 ΔΕΛΤΙΟ ΤΥΠΟΥ, ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ)

ΚΕΦΑΛΑΙΟ 5° M-BANKING στις Ελληνικές Τράπεζες

5.1. Εθνική Τράπεζα

5.1.1. Συνεργασία και Παροχές

Η παροχή κινητών υπηρεσιών για την Εθνική Τράπεζα υλοποιείται με το Mobile Banking. Η μεγαλύτερη Ελληνική Τράπεζα, σε συνεργασία με τηλεπικοινωνιακούς οργανισμούς, έχει στόχο να καλύψει τις βασικές ανάγκες των πελατών της, καθώς η αντιμετώπιση του M-Banking είναι μάλλον συμπληρωματική του E-Banking.

Μέσω του i-mode παρέχεται η δυνατότητα πραγματοποίησης μίας σειράς τραπεζικών συναλλαγών, όπως η ενημέρωση υπολοίπου και κίνησης λογαριασμών, η διατραπεζική μεταφορά χρημάτων εσωτερικού, η πληρωμή πιστωτικών καρτών και οφειλών προς τρίτους, η αγορά και πώληση μετοχών, αλλά και η ενημέρωση για το μετοχικό χαρτοφυλάκιο.

Από την άλλη, η συνεργασία με τους τηλεπικοινωνιακούς οργανισμούς αξιοποιείται με την αποστολή SMS και έχει κυρίως ενημερωτικό χαρακτήρα. Υποστηρίζονται τηλεειδοποιήσεις, με μόνη επιβάρυνση το κόστος των γραπτών μηνυμάτων, οι οποίες ενημερώνουν τον χρήστη, ανά πάσα στιγμή, τόσο για τους αριθμούς λογαριασμών πιστωτικών καρτών και δανείων της Εθνικής Τράπεζας, όσο και για το υπόλοιπο/ διαθέσιμο πιστωτικό όριο των λογαριασμών αυτών.

5.1.2. Ασφάλεια Υπηρεσιών Mobile-Banking

Με την υπηρεσία alert, παρέχεται η δυνατότητα της άμεσης ειδοποίησης του πελάτη για κάθε μεταβολή του υπολοίπου των λογαριασμών εκτός των ορίων που ο ίδιος έχει θέσει. Για την απόκτηση της πρόσβασης, ο χρήστης καλείται να συμπληρώσει μία αίτηση και η εγγραφή ολοκληρώνεται με την παραλαβή των απαραίτητων προσωπικών κωδικών από το κατάστημα αίτησης, δύο μέρες αργότερα.

Μέσω i-mode η ασφάλεια των συναλλαγών εξασφαλίζεται με τη χρήση του UserID και του PIN, αλλά και του πρωτοκόλλου SSL.

Μέσω SMS μοναδική δικλείδα ασφαλείας αποτελεί η δήλωση του αριθμού του κινητού τηλεφώνου από το οποίο θα γίνονται οι συναλλαγές, χωρίς να έχει όμως επιπτώσεις λόγω του πληροφοριακού της περιεχομένου. Το μεγαλύτερο μειονέκτημα, όμως, του m-banking της Εθνικής Τράπεζας πηγάζει από τις συνεργασίες της με τηλεπικοινωνιακούς οργανισμούς.

5.2. Τράπεζα Πειραιώς

5.2.1. Ταχύτητα και Ευκολία

Η Winbank είναι η διεύθυνση Ηλεκτρονικής Τραπεζικής για την συγκεκριμένη τράπεζα. Οι τραπεζικές και χρηματιστηριακές συναλλαγές γίνονται ηλεκτρονικά οποιαδήποτε στιγμή από το smartphone , Android ή iPhone και υλοποιούνται μέσω WAP, i-mode, IVR ή από κάποιο εκπρόσωπο της τράπεζας.

Κατηγορίες συναλλαγών:

- Υπόλοιπα και κινήσεις λογαριασμών, καρτών και δανείων
- Διαχείριση προπληρωμένης κάρτας winbank WEBUY
- Μεταφορές
- Πληρωμές
- Εμβάσματα
- Χρηματιστηριακές συναλλαγές
- Ανανέωση Χρόνου Ομιλίας

Με την εφαρμογή winbank mobile banking App τα έξοδα των συναλλαγών είναι χαμηλότερα απ' ό,τι εάν γίνετε σε τραπεζικό κατάστημα, ATM ή μηχάνημα αυτόματων συναλλαγών easypay. Η Τράπεζα Πειραιώς είναι πρωτοπόρος στις ηλεκτρονικές τραπεζικές υπηρεσίες κερδίζοντας έτσι ένα μεγάλο μερίδιο της αγοράς.

5.2.2. Ασφάλεια Υπηρεσιών Winbank Mobile-Banking

Οι συναλλαγές που γίνονται με την εφαρμογή Winbank Mobile Banking App διασφαλίζονται από τα προηγμένα συστήματα ασφάλειας ηλεκτρονικών πληρωμών της Τράπεζας Πειραιώς. Απαιτεί την υποβολή αίτησης για τους νέους πελάτες ή την επίσκεψη σε κάποιο κατάστημα.
Για τη μέγιστη δυνατή ασφάλεια της υπηρεσίας winbank mobile banking, εφαρμόζει μεθόδους που διασφαλίζουν τις συναλλαγές, προστατεύουν τα δεδομένα και θωρακίζουν το κανάλι από την πρόσβαση τρίτων. Στον τομέα της ασφάλειας των προσωπικών κωδικών γίνεται κρυπτογράφηση με SSL κατά τη μεταφορά των δεδομένων και αυτόματη αποσύνδεση σε περίπτωση αδράνειας συναλλαγών.

5.2.3. Απόρρητο Συναλλαγών

Όλες οι πληροφορίες που διαβιβάζονται στην Τράπεζα Πειραιώς είναι εμπιστευτικές. Για να εξασφαλίσει ότι χρησιμοποιούνται μόνο όταν είναι αναγκαίο στο πλαίσιο των υπηρεσιών που παρέχει, έχει λάβει όλα τα απαραίτητα μέτρα, όπως:

- Μόνο εξουσιοδοτημένοι υπάλληλοι της Τράπεζας έχουν πρόσβαση στις πληροφορίες των συναλλαγών και αυτό μόνο όποτε αυτό είναι αναγκαίο, π.χ. για τη διεκπεραίωση των αιτήσεων..
- Η Τράπεζα Πειραιώς δεν αποκαλύπτει τα προσωπικά και τραπεζικά στοιχεία των πελατών ή τα στοιχεία των συναλλαγών τους, παρά μόνο εφόσον έχει έγγραφη εξουσιοδότηση από εσάς ή αυτό επιβάλλεται από δικαστική απόφαση ή απόφαση άλλης δημόσιας αρχής.
- Όταν η Τράπεζα Πειραιώς χρησιμοποιεί τρίτους για την υποστήριξη των υπολογιστικών συστημάτων της, φροντίζει για την εξασφάλιση του απορρήτου των συναλλαγών.
- Μπορεί ο πελάτης να ζητήσει οποιαδήποτε στοιχεία τηρούνται για αυτόν, καθώς και τη διόρθωσή τους, εφόσον μπορεί να τεκμηριώσει την ύπαρξη λάθους.
- Για τη ασφάλεια των πελατών, πρέπει κι ο πελάτης να χειρίζεται όλες τις πληροφορίες που παρέχονται μέσω της υπηρεσίας ως εμπιστευτικές και απόρρητες και να μην προβαίνει σε οποιαδήποτε αποκάλυψή τους σε τρίτα πρόσωπα.

5.3. Alpha Bank

5.3.1. Φιλοσοφία και Πλεονέκτηματα

Η συγκεκριμένη τράπεζα δημιουργώντας το Alpha Bank M-Banking προσφέρει στους πελάτες της τη δυνατότητα τραπεζικών συναλλαγών μέσω κινητού τηλεφώνου που διαθέτει υποστήριξη υπηρεσιών WAP ή i-mode.

Ο μεγάλος αριθμός υπηρεσιών που προσφέρει τόσο στην υπηρεσία WebBanking όσο και στην υπηρεσία AlhpaPhone Banking, μέσω αυτόματου συστήματος IVR, αποτελεί ένα μεγάλο πλεονέκτημα στο χώρο της ηλεκτρονικής τραπεζικής.

Οι πελάτες μπορούν:

- Να ενημερώνονται για τις κινήσεις και τα υπόλοιπα των λογαριασμών
- Να μεταφέρουν χρήματα σε δικούς τους λογαριασμούς.
- Να πληρώνουν οφειλές πιστωτικών καρτών στην τράπεζα, αλλά και σε άλλη τράπεζα μέσω του συστήματος Dias Transfer.
- Να πληροφορούνται για το υπόλοιπο των πιστωτικών καρτών
- Να ειδοποιούνται με SMS/e-mails για νέες υπηρεσίες και παροχές.

Ο πελάτης για να αποκτήση πρόσβαση στις υπηρεσίες που παρέχει η συγκεκριμένη τράπεζα θα πρέπει να κάνει αίτηση, είτε τηλεφωνικά, είτε μέσω Internet, είτε σε κάποιο υποκατάστημα. Οι υπηρεσίες εγγραφής και χρήσης του M-Banking είναι δωρεάν, αφού η τράπεζα ενθαρύνει την χρήση των υπηρεσιών αυτών απαλλάσσοντας τους πελάτες της από έξοδα κίνησης λογαριασμών ανεξάρτητα από τον αριθμό των μηνιαίων συναλλαγών.

5.3.2. Ασφάλεια Υπηρεσιών Alpha WebBanking -Mobile Banking

Στις συναλλαγές που γίνονται με την εφαρμογή Alpha WebBanking και Alpha Molile Banking χρησιμοποιούνται τα πρωτόκολλα WTLS για την υπηρεσία WAP και SSL για την υπηρεσία i-mode. Παράλληλα με την κρυπτογράφηση, γίνεται χρήση προσωπικών κωδικών και προφυλάσσεται αυτόματα από τον προκαθορισμένο χρόνο ολοκλήρωσης συναλλαγών (Process Timeout) και για την εκτέλεση μίας συναλλαγής.

5.4. Eurobank

5.4.1. Ολοκληρωμένη Εξυπηρέτηση

Η τράπεζα αυτή προσφέρει ολοκληρωμένη τραπεζική εξυπηρέτηση για Smartphones και tablets αλλά και για τα υπόλοιπα κανάλια επικοινωνίας. Εάν γίνεται χρήση κινητού τελευταίας τεχνολογίας (Smartphone) με λειτουργικό iPhone, Android, Windows Phone, Blackberry ή Symbian, εγκαθίσταται δωρεάν η ειδική εφαρμογή M-Banking "Eurobank app.

Το Eurobank app διαθέσιμο και για ταμπλέτα iPad.

- Ενημέρωση online με πληροφορίες για τους λογαριασμούς, τις κάρτες, τα δάνεια και τις επενδύσεις των χρηστών.
- Μεταφορά χρημάτων μεταξύ των λογαριασμών, σε λογαριασμούς 3ων Eurobank και άλλων Τραπεζών (εντός Ελλάδος)

- Εξόφληση της κάρτας, κάρτες τρίτων Eurobank και άλλων τραπεζών, το δάνειό, καθώς και τους πιο συχνούς λογαριασμούς σας (ΔΕΗ, ΕΥΔΑΠ, ΦΠΑ, ΟΑΕΕ, ΙΚΑ, e-Παράβολο, ΟΤΕ, hol/hellas online, OTEnet, On Telecoms, CYTA, Cosmote, Vodafone, WIND, Multichoice-Nova, Φόρτιση e-Pass)
- Δυνατότητα φόρτισης προπληρωμένης κάρτας και ανάληψης από πιστωτική/ προπληρωμένη κάρτα
- Τηλεφωνική εξυπηρέτηση από εκπρόσωπο χωρίς αναμονή και χωρίς κανένα κόστος
- Ενημέρωση για όλα τα Νέα της Eurobank και χρησιμοποίηση χρήσιμων εργαλείων (υπολογιστής δανείου/ IBAN, Μετατροπέας Συναλλάγματος, Ισοτιμίες) για τις συναλλαγές των χρηστών
- Πληρωμές με δυνατότητα Barcode Scanning.

5.4.2. Ασφάλεια M-banking Eurobank App

Η Eurobank λαμβάνει όλα τα απαραίτητα και γνωστά μέχρι σήμερα στην επιστήμη της πληροφορικής μέτρα με στόχο την ασφάλεια των συναλλαγών σας μέσω της υπηρεσίας m-Banking. Για την επίτευξη του στόχου αυτού, όμως, είναι απαραίτητες και οι δικές σας ενέργειες. Η ιδιαίτερα υψηλού επιπέδου ασφάλεια του M-Banking ξεχωρίζει αφού η τράπεζα έχει επενδύσει σε ιδιόκτητη πύλη WAP και χρησιμοποιεί το πρωτόκολλο WTLS μαζί με την κρυπτογράφηση, όπως επίσης και το δίκτυο GSM. Η χρήση ιδιόκτητου Dialup Server ελέγχει τον αριθμό του κινητού τηλεφώνου που ο ίδιος ο πελάτης έχει δηλώσει κατά την διαδικασία της αίτησης.

5.4.3.Κόστος

Η εφαρμογή Eurobank m-Banking διατίθεται δωρεάν. Ισχύουν οι χρεώσεις χρήσης του δικτύου του παρόχου κινητής τηλεφωνίας, καθώς και τυχόν προμήθειες που ισχύουν για συναλλαγές μέσω e-Banking της Eurobank. Η τεχνική υποστήριξη είναι υψηλού επιπέδου τόσο από το πάντα ενημερωμένο προσωπικό, όσο και με τα εγχειρίδια ιδηγιών στο WebSite.

5.5. Συμπεράσματα

Καθώς οι προσφερόμενες υπηρεσίες M-Banking από τις τράπεζες είναι πολλές, μόλις τα τελευταία χρόνια κερδίζουν την αναγνώριση από τους πελάτες, που με την σειρά τους ανακαλύπτουν σιγά-σιγά την κάλυψη των αναγκών και επιθυμιών τους από τις τεχνολογικές εξελίξεις. Ο κάθε πελάτης είναι ελεύθερος να επιλέξει την τράπεζα εκείνη που καλύπτει τις ανάγκες του και ικανοποιεί τα συμφέροντα του.

Οι Ελληνικές Τράπεζες δίνουν ιδιαίτερη σημασία στην εξοικείωση της χρήσης των υπηρεσίων καθώς οι παράμετροι για την άψογη συνεργασία με τους πελάτες είναι βασικοί.

Όπως:

- το περιβάλλον λειτουργίας,
- οι αρχικές διαδικασίες πρόσβασης και εγγραφή
- η τεχνολογία
- η ασφάλεια των συναλλαγών
- η τεχνική υποστήριξη

ΚΕΦΑΛΑΙΟ 6° ΣΥΜΠΕΡΑΣΜΑΤΑ-ΜΕΛΛΟΝΤΙΚΗ ΕΞΕΛΙΞΗ

6.1. Συμπεράσματα

Το Mobile ή E-Banking δεν είναι μια καινοτομία πια. Η ευρεία χρήση των smartphones και των tablets, τα ηλεκτρονικά καταστήματα, οι ηλεκτρονικές πληρωμές έχουν κάνει τις online τραπεζικές συναλλαγές ακόμα πιο εύκολες. Είναι μια ουσιαστική υπηρεσία που οι πελάτες αναμένουν από τις τράπεζές τους. Οι ουρές στα ταμεία έχουν γίνει μικρότερες, η γραφική εργασία για το προσωπικό ελάχιστη στα καταστήματα αφού τα δεδομένα αποθηκεύονται απευθείας στις βάσεις δεδομένων που ως αποτέλασμα έχει το μειωμένο κόστος λειτουργίας. Οι χρήστες μπορούν να διαχειριστούν τα πάντα, να πληρώσουν λογαριασμούς, να αγοράσουν σπάνια αντικείμενα και να πραγματοποιήσουν συναλλαγές με μερικά μόνο κλικ, όχι μόνο όταν βρίσκονται στο σπίτι ή στο γραφείο, αλλά απ' όπου υπάρχει πρόσβαση στο Internet ή σήμα στο κινητό.

Το Mobile- Banking (m-banking) στην Ελλάδα είναι ακόμα σε εμβρυακή κατάσταση, παρά τις προσπάθειες ορισμένων τραπεζών για τη διάδοσή του. Οι Έλληνες καταναλωτές, έχουν δείξει ότι δύσκολα εμπιστεύονται κάτι άγνωστο σε αυτούς, πόσο μάλλον όταν αυτό έχει να κάνει με τη διαχείριση των χρημάτων τους και φαίνεται ότι πολλοί διστάζουν να «καλωσορίσουν» τις τεχνολογίες mobile banking. Αυτό οφείλεται ενδεχομένως στη χρήση του κινητού ως κατεξοχήν μέσου επικοινωνίας, συνεπώς η αποδοχή της αξιοπιστίας του ως μέσου διεξαγωγής χρηματοοικονομικών συναλλαγών δεν είναι εύκολη.

Η ανάλυση όλων των στοιχείων από τα ανωτέρω δύο βοηθά τις τράπεζες να σχεδιάζουν τις μελλοντικές στρατηγικές τους σε ανάπτυξη εξατομικευμένη λύση για τους πελάτες. Επίσης, οι τράπεζες καινοτομούν με τη δημιουργία νέων πιλοτικών τύπων καταστημάτων, αποδεικνύοντας στην πράξη τη μετάβαση από την ηλεκτρονική τραπεζική στην ψηφιακή, με την τεχνολογία να είναι το κλειδί για αυτόν τον ψηφιακό μετασχηματισμό. Στην παρούσα οικονομική συγκυρία η παροχή καινοτόμων λύσεων διενέργειας των συναλλαγών θα συμβάλει στη διατήρηση της υφιστάμενης πελατείας.

6.2. Μελλοντική Εξέλιξη

Η τεχνολογική πρόοδος αλλάζει την αποστολή και τη δομή λειτουργίας των καταστημάτων των τραπεζών, μετατρέποντας τις από χώρο διενέργειας συναλλαγών σε χώρο παροχής τραπεζικών συμβουλών στην πελατεία και διενέργειας σύνθετων συναλλαγών. Μάλιστα, το 2017 προβλέπεται ότι περισσότερο από το 60% των πωλήσεων τραπεζικών προϊόντων θα γίνεται από ηλεκτρονικά κανάλια.Το επίπεδο τεχνολογίας των ελληνικών τραπεζών θεωρείται πολύ ικανοποιητικό και ανταποκρίνεται στις ανάγκες της τραπεζικής πελατείας με ασφάλεια και λειτουργικότητα. Ως αποτέλεσμα, ήδη, υπάρχει διαρκής μετατόπιση των πωλήσεων από τα κλασσικά στα εναλλακτικά δίκτυα. Ωστόσο, παρά τις σημαντικές αυτές εξελίξεις, η επαφή της πελατείας με τα καταστήματα των τραπεζών θα βαίνει μειούμενη, αλλά δεν θα πάψει να υφίσταται.

Το Mobile Banking εξελίσσεται σε πολύτιμο εργαλείο διακράτησης πελατών ή προσέλκυσης νέων και για τις ελληνικές τράπεζες. Η ηλεκτρονική τραπεζική όχι μόνο εμφανίζει ταχύτατους ρυθμούς ανάπτυξης στην εγχώρια αγορά, ιδιαίτερα στις νεότερες ηλικιακά ομάδες, αλλά πλέον αποτελεί έναν από τους σημαντικότερους παράγοντες μετακίνησης του πελάτη από μια τράπεζα σε άλλη. Επιπρόσθετα, εκτιμάται ότι, και στην Ελλάδα, στο μέλλον το mobile banking θα αποτελεί το κύριο τραπεζικό κανάλι διενέργειας συναλλαγών.

Οι παραπάνω διαπιστώσεις έγιναν στη διάρκεια του 19ου Banking Forum, που είχε ως κύριο στόχο την παρουσίαση των πρόσφατων εξελίξεων της πληροφορικής, που επηρεάζουν αποφασιστικά την επιχειρηματική δράση των τραπεζών. Κοινή επισήμανση των ομιλητών ήταν ότι για τις τράπεζες η ψηφιακή εποχή αποτελεί μονόδρομο, με την τεχνολογία του mobile banking να είναι ο σηματωρός των μελλοντικών εξελίξεων. Στην εποχή των ηλεκτρονικών πληρωμών μέσω κινητών τηλεφώνων, που μετατρέπουν στην ουσία τα smartphones και τις φορητές συσκευές σε ψηφιακό "πορτοφόλι", ετοιμάζεται να εισέλθει και η Ελλάδα.

Το μέλλον του M-Banking, αλλά και των εναλλακτικών καναλιών στο σύνολό τους, είναι η πλήρης ενσωμάτωσή τους με την έννοια της τραπεζικής εξυπηρέτησης. Μπορεί αυτή τη στιγμή κάθε κανάλι διανομής να εξυπηρετεί διαφορετικές ανάγκες, λειτουργώντας συμπληρωματικά, με την περαιτέρω εξέλιξη της τεχνολογίας όμως όλα αυτά τα διαφορετικά δίκτυα εξυπηρέτησης στη συνείδηση του καταναλωτή θα γίνουν ένα. Όσο η διείσδυση του Internet θα αυξάνεται και οι τεχνολογίες των διαφορετικών μέσων συναλλαγών θα συγκλίνουν τόσο οι έλληνες χρήστες θα εξοικειώνονται με τις εφαρμογές τους, μεταξύ των οποίων είναι και η υπηρεσία ηλεκτρονικής τραπεζικής.

Είναι ιδιαίτερα ενθαρρυντικό επίσης ότι η διείσδυση των νέων τεχνολογιών στην ελληνική αγορά, του E-Banking και δη του M-Banking, ακολουθεί μια συνεχώς αυξανόμενη πορεία, γεγονός άμεσα συνυφασμένο με την ταχέως αυξητική πορεία χρήσης του Internet και των κινητών τηλεφώνων. Παρατηρώντας την εξέλιξη των M-Banking χρηστών σε βάθος χρόνου, αποδεικνύεται πως το κανάλι κερδίζει σταδιακά την εμπιστοσύνη τους, κάνουν όλο και περισσότερες συναλλαγές μέσα από αυτό και αρχίζουν να το θεωρούν πλέον απαραίτητο μέρος της τραπεζικής σχέσης.

Οι εμπλεκόμενοι στο θέμα φορείς, ήτοι οι τράπεζες και οι τηλεπικοινωνιακοί πάροχοι, οι οποίοι βρίσκονται σε ανοιχτό δίαυλο επικοινωνίας, δηλώνουν έτοιμοι να παρέχουν - σε πλήρη εμπορική βάση - τις σχετικές υπηρεσίες σε διάστημα ενός έτους από την αποσαφήνιση των σχετικών τεχνικών προδιαγραφών, πάνω στις οποίες θα “πατήσουν” οι πληρωμές μέσω κινητού. Οι σχετικές διαδικασίες δεν μπορεί παρά να “τρέξουν” άμεσα, καθώς αμφότεροι, τράπεζες και τηλεπικοινωνιακοί πάροχοι, έχουν αντιληφθεί απόλυτα τη σημασία των εν λόγω υπηρεσιών για τη μετάβασή τους στη νέα ψηφιακή εποχή. Ειδικά για τον κλάδο των τηλεπικοινωνιών, οι ηλεκτρονικές πληρωμές μέσω φορητών συσκευών, μεταφράζονται σε μια σημαντική πρόσθετη πηγή εσόδων, ενώ ταυτόχρονα η παροχή της εκτιμάται ότι μπορεί να συμβάλλει στη διακράτηση, αλλά και διεύρυνση, της πελατειακής βάσης. Υπέρ του τάχιστου των εξελίξεων συνηγορεί το γεγονός της μεγάλης διείσδυσης του Ίντερνετ και της κινητής τηλεφωνίας στην Ελλάδα και της ικανοποιητικής εξοικείωσης των Ελλήνων με τις φορητές συσκευές. Ήδη πάντως, σύμφωνα με πληροφορίες, οι τέσσερις συστημικές τράπεζες (Τράπεζα Πειραιώς, Alpha Bank, Εθνική Τράπεζα και Eurobank) βρίσκονται σε επαφές με τις τρεις εταιρείες κινητής τηλεφωνίας, ώστε να προχωρήσουν άμεσα οι ηλεκτρονικές συναλλαγές μέσω κινητού.

Σήμερα, όσοι μετέχουν σε πιλοτικά προγράμματα ηλεκτρονικών πληρωμών μέσω κινητών συσκευών, μπορούν να τις χρησιμοποιήσουν σε περίπου 5.000 σημεία πώλησης πανελλαδικά, τα οποία υποστηρίζουν την πραγματοποίηση συναλλαγών με κάρτες ανέπαφων συναλλαγών (contactless cards). Ένα νέο “οικοσύστημα” συναλλαγών, που αναμένεται να εκσυγχρονίσει σημαντικά τους σημερινούς τρόπους πληρωμών στην αγορά. Αυτή τη στιγμή, υπάρχουν περίπου 130.000 κάρτες ανέπαφων συναλλαγών, από 100.000 πέρυσι, οι οποίες εκτιμάται ότι θα φτάσουν τις 250.000 στα τέλη του 2014. Πάντως, μόνο το 5% των σημείων πώλησης έχουν τερματικά για contactless payments, ενώ απαιτείται ένας αριθμός 10.000 τερματικών και 1 εκατ. καρτών, που απαιτούνται ώστε να δημιουργηθεί εκείνη η κρίσιμη μάζα, που θα οδηγήσει στην ταχεία εξέλιξη της αγοράς των ηλεκτρονικών πληρωμών μέσω κινητών συσκευών.

Το πρωτοποριακό “κινητό πορτοφόλι” εξασφαλίζει μέγιστη ταχύτητα, ευκολία και ασφάλεια στις συναλλαγές, αξιοποιώντας τις νέες δυνατότητες που προσφέρει η τεχνολογία NFC (Near Field Communication).

Η Ελλάδα καλείται να αποφασίσει αν – σε τεχνικό επίπεδο - θα χρησιμοποιήσει το μοντέλο, που ήδη είναι διαδεδομένο στο εξωτερικό και σύμφωνα με αυτό η κάρτα SIM του smartphone χρησιμοποιείται για την εγγύηση της ασφάλειας των συναλλαγών, ή την τεχνολογία εξομοίωσης καρτών (Host Card Emulation – HCE), όπου τα στοιχεία της κάρτας και των συναλλαγών φιλοξενούνται με ασφάλεια στο cloud, αντί της κάρτας SIM, η οποία σε παγκόσμιο επίπεδο είναι στα σπάργανα.

Οι σύγχρονοι τρόποι πληρωμών κερδίζουν συνεχώς έδαφος και διεισδύουν σταδιακά και σε “περιοχές” όπου έως σήμερα κυριαρχούν τα μετρητά (low value payments), προς όφελος και διευκόλυνση των καταναλωτών αλλά και της οικονομίας γενικότερα.

6.2.1. STORK 2.0 Δημιουργία Ενιαίου Χώρου για Ηλεκτρονική Αναγνώριση και Αυθεντικοποίηση στην Ευρώπη

Το STORK 2.0 (Secure idenTity acrOss boRders linKed 2.0) είναι ένα σημαντικό έργο διάρκειας τριών ετών που έχει ξεκινήσει για να προωθήσει τη δημιουργία και αξιοποίηση ενός ενιαίου και βιώσιμου χώρου για ηλεκτρονικής ταυτοποίησης και αυθεντικοποίησης στην Ευρώπη, για νομικά και φυσικά πρόσωπα. Η πρωτοβουλία θα οδηγήσει στη σύγκλιση μεταξύ ιδιωτικού και δημόσιου τομέα, σε εθνικό και κοινοτικό επίπεδο, για την ασφαλή και εύκολη πρόσβαση στις διασυνοριακές δημόσιες υπηρεσίες που χρησιμοποιούν διαπιστευτήρια για ηλεκτρονική αναγνώριση (eID).

Τέσσερα πιλοτικά θα λειτουργήσουν για 12 μήνες, με έμφαση:

- στην ηλεκτρονική μάθηση και ακαδημαϊκά προσόντα *(eLearning and Academic Qualifications)*,
- υπηρεσίες ηλεκτρονικής τραπεζικής *(eBanking)*,
- παροχή υπηρεσιών ηλεκτρονικής διακυβέρνησης για επιχειρήσεις *(Public Services for Business)* και
- υπηρεσίες για ηλεκτρονική υγεία *(eHealth)***,**

για να επιδείξουν τις δυνατότητες και τα οφέλη της διαλειτουργικότητας στη ηλεκτρονικής ταυτοποίηση (eID) στη καθημερινή ζωή.

Οι τέσσερις βασικοί στόχοι του STORK 2.0 είναι:

- *Επιτάχυνση της ανάπτυξης της ηλεκτρονικής αναγνώρισης για τις υπηρεσίες Ηλεκτρονικής Διακυβέρνησης* συντονίζοντας τις Εθνικές Κοινοτικές πρωτοβουλίες για την υποστήριξη μιας ομόσπονδης (Federated) αρχιτεκτονικής διαχείρισης της Ηλεκτρονικής Αναγνώρισης σε ολόκληρη την Ευρώπη.
- *Μεγιστοποίηση της αφομοίωσης των κλιμακούμενων λύσεων σε όλη την ΕΕ*, με μια ισχυρή δέσμευση για ανοικτές προδιαγραφές και μακροπρόθεσμη βιωσιμότητα, με όραμα η ηλεκτρονική αναγνώριση να εξελιχθεί σε παροχή υπηρεσίας (με την υποστήριξη των συμμετεχόντων ευρωπαϊκών χωρών και της βιομηχανίας).
- *Διευκόλυνση της σύγκλισης του ιδιωτικού και δημόσιου τομέα* σε ένα πλήρως λειτουργικό πλαίσιο και υποδομή, που χρησιμοποιεί Ηλεκτρονική Αναγνώριση (eID) για ασφαλή και συνεπή πιστοποίηση των νομικών και φυσικών προσώπων σε ολόκληρη την ΕΕ.
- *Λειτουργία τεσσάρων διασυνοριακών και διατομεακών πιλοτικών* για να δοκιμάσουν και να επιδείξουν τις δυνατότητες και τα οφέλη της διαλειτουργικής ηλεκτρονικής αναγνώρισης (eID) σε περιβάλλοντα πραγματικών συνθηκών.

Τα πιλοτικά του Stork 2.0 επικεντρώνονται στην υλοποίηση στρατηγικής σημασίας εφαρμογών που αφορούν την ηλεκτρονική μάθηση και τα ακαδημαϊκά προσόντα (**eLearning and Academic Qualifications**), τις υπηρεσίες ηλεκτρονικής τραπεζικής (**eBanking)**, τις υπηρεσίες ηλεκτρονικής διακυβέρνησης για επιχειρήσεις (**Public Services for Business)** και τις υπηρεσίες για την ηλεκτρονική υγεία **(eHealth)**. Οι εφαρμογές αυτές θα επικυρώσουν τις κοινές προδιαγραφές, πρότυπα και δομικά στοιχεία, αντιμετωπίζοντας πειστικά τα θεσμικά

θέματα και θέματα διοίκησης (διασυνοριακά, σε διαφορετικούς επιχειρησιακούς τομείς και κλάδους). Οι εφαρμογές αυτές θα διευκολύνουν τη χωρίς σύνορα ψηφιακή ζωή και την κινητικότητα στην ΕΕ, ενισχύοντας την Ενιαία Ψηφιακή Αγορά για τις υπηρεσίες Ηλεκτρονικής Διακυβέρνησης και της ηλεκτρονικές υπηρεσίες του ιδιωτικού τομέα σε εναρμόνιση με την Οδηγία των Υπηρεσιών.

ΚΕΦΑΛΑΙΟ 7° Νομοθετικό Πλαίσιο

7.1. Κύριοι κλάδοι του δικαίου που διέπουν το Internet banking

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

Η ηλεκτρονική τραπεζική υπάγεται στην εποπτεία της Κεντρικής Τράπεζας και τις Οδηγίες της Ευρωπαϊκής Ένωσης για τα πιστωτικά ιδρύματα. Εφαρμόζονται οι 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 οι διατάξεις για τη δημοσιοποίηση των οικονομικών αποτελεσμάτων.
(Α. Σινανιώτη-Μαρούδη, Ι. Φαρσαρώτας, Ηλεκτρονική Τραπεζική 2005, σελ.151)
(Γιαννόπουλος, Internet Banking : Νομικά ζητήματα από την διεξαγωγή τραπεζικών συναλλαγών στο διαδίκτυο, ΔΕΕΤ 2003, σελ 99).

Στην έννοια της εποπτείας περιλαμβάνονται:

- ✓ ορισμός των ιδίων κεφαλαίων των πιστωτικών ιδρυμάτων (ΠΔ/ΤΕ 2053/1992),
- ✓ έλεγχος φερεγγυότητας (ΠΔ/ΤΕ 2054/1992),
- ✓ ρευστότητας, κεφαλαιακής επάρκειας (ΠΔ/ΤΕ 2397/1996),
- ✓ συγκέντρωσης κινδύνων (ΠΔ/ΤΕ 2246/1996)
- ✓ συστήματος εξωτερικού ελέγχου (ΠΔ/ΤΕ 2438/1998) των πιστωτικών ιδρυμάτων. (Α. Σινανιώτη-Μαρούδη, Ι. Φαρσαρώτας, Ηλεκτρονική Τραπεζική 2005, σελ.152).

7.2. Νομικό πλαίσιο για το ελληνικό e-Banking

Η ασφάλεια των συναλλαγών και των προσωπικών δεδομένων των χρηστών της ηλεκτρονικής τραπεζικής μέσω Διαδικτύου (Internet Banking), είναι μείζονος σημασίας. Εκτός από τα συστήματα ασφάλειας των τραπεζών και των μέτρων προστασίας από την πλευρά του χρήστη υπάρχει ένα συγκεκριμένο νομοθετικό πλαίσιο σε σχέση με την ηλεκτρονική τραπεζική, το οποίο κατοχυρώνει ακόμη περισσότερο τον καταναλωτή. Συγκεκριμένα, η πραγματοποίηση ηλεκτρονικών τραπεζικών συναλλαγών στο διαδίκτυο, διέπεται από την ελληνική και την κοινοτική τραπεζική νομοθεσία.

Όσον αφορά το νομικό πλαίσιο των ηλεκτρονικών πληρωμών στην ηλεκτρονική τραπεζική μέσω Διαδικτύου (Internet Banking), εφαρμόζεται ο νόμος 2789/2000 σχετικά με το αμετάκλητο του διακονονισμού στα συστήματα πληρωμών και στα συστήματα διακανονισμού χρηματοπιστωτικών μέσων, ο οποίος έχει ενσωματώσει την κοινοτική οδηγία 98/26.
(ΦΕΚ Α΄ 21 /Κανονισμός Συστήματος Διακονονισμού εντολών σε ευρώ 'Ερμής'-Σύστημα Target)

Με Πράξη Διοικητή της Τράπεζας της Ελλάδος (υπ' αριθ. 2527/ 8.12.2003) με θέμα «Κανόνες προληπτικής εποπτείας από την Τράπεζα της Ελλάδος των Ιδρυμάτων Ηλεκτρονικού Χρήματος» θέτονται οι όροι και προϋποθέσεις για την παροχή από την Τράπεζα της Ελλάδος άδειας ίδρυσης και λειτουργίας Ιδρύματος Ηλεκτρονικού Χρήματος.

Με Πράξη Διοικητή της Τράπεζας της Ελλάδος (υπ' αριθ. 2501/ 31.10.2002) με θέμα την ενημέρωση των συναλλασσομένων με τα πιστωτικά ιδρύματα για τους όρους που διέπουν τις συναλλαγές τους.

Πράξη Εκτελεστικής Επιτροπής 33/19.12.2013 Όροι και προϋποθέσεις για την χορήγηση άδειας λειτουργίας και κανόνες εποπτείας των Ιδρυμάτων Ηλεκτρονικού Χρήματος Τροποποίηση της ΠΔ/ΤΕ2628/30.9.2010 - Κατάργηση της ΠΔ/ΤΕ2527/8.12.2003. (http://www.bankofgreece.gr/BogDocumentPEE/ΠΕΕ_33_19_12_2013.pdf)

7.2.1. Νομοθεσία για την προστασία του καταναλωτή

Για την προστασία των καταναλωτών στην παροχή τραπεζικών υπηρεσιών και από φυσικά αλλά και από εναλλακτικά δίκτυα (Internet Banking), εφαρμόζεται ο νόμος 2251/94. Οι βασικές αρχές πρέπει να αναζητηθούν στο Ν.2251/94, όπως ισχύει, ιδίως στις διατάξεις για τις καταχρηστικές ρήτρες συμβάσεων με καταναλωτές και τις διατάξεις για την παραπλανητική διαφήμιση. Ειδικά για τις προσφερόμενες υπηρεσίες ηλεκτρονικής τραπεζικής μέσω διαδικτύου (Internet Banking), κατευθυντήριες γραμμές δίνει το άρθρο 4 του προαναφερθέντος νόμου, το οποίο ενσωματώνει την κοινοτική οδηγία 97/7 σχετικά με τις εξ' αποστάσεως συμβάσεις (διαδικτυακές συναλλαγές). Επιγραμματικά, η διάταξη θεσπίζει:

- ✓ ακυρότητα υπέρ του καταναλωτή
- ✓ υποχρέωση για ανακοίνωση της ταυτότητας της επιχείρησης και για λεπτομερή περιγραφή των χαρακτηριστικών της τιμής και του κόστους του προσφερόμενου αγαθού
- ✓ υποχρέωση περιγραφής του δικαιώματος υπαναχώρησης του καταναλωτή
- ✓ υποχρέωση περιγραφής της διάρκειας τυχόν προσφορών και της διάρκειας της σύμβασης

(Σινανιώτη/ Φαρσαρώτας, «Ηλεκτρονική Τραπεζική, σελ172)
(Παπαϊωάννου Γ., « Η σύμβαση από απόσταση κατά το δίκαιο προστασίας του καταναλωτή», ΔΕΕ,2, 2003, σελ.153)

Ειδικά όμως 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 του πεδίου της εμπορικής ή επαγγελματικής του δραστηριότητας». Η Οδηγία προβλέπει :

- ✓ Υποχρέωση για λεπτομερή πληροφόρηση του καταναλωτή πριν και μετά από την κατάρτιση της σύμβασης, για την υπηρεσία, τη σύμβαση και τα μέσα αποκατάστασης
- ✓ Υποχρέωση για ανακοίνωση των συμβατικών όρων σε χαρτί ή άλλο σταθερό μέσο
- ✓ Δικαίωμα υπαναχώρησης εντός 14 ημερών εκτός από:
  - i) τις υπηρεσίες με διακυμάνσεις τιμών(π.χ. συνάλλαγμα, futures, swaps, options),
  - ii) τις βραχυπρόθεσμες συμβάσεις(π.χ. ασφαλιστήρια για ταξίδια),
  - iii) τις συμβάσεις, η εκτέλεση των οποίων ολοκληρώθηκε και
  - iv) τις συμβάσεις ασφαλίσεων ζωής, για τις οποίες προβλέπεται δικαίωμα υπαναχώρησης εντός 30 ημερών (Οδηγία 90/619)

- ✓ Δυνατότητα ακύρωσης των συναλλαγών με πιστωτική κάρτα
- ✓ 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 συμβατικήνπαραίτηση από τα παρεχόμενα δικαιώματα.

(Γιαννόπουλος, Internet Banking : Νομικά ζητήματα από την διεξαγωγή τραπεζικών συναλλαγών στο Διαδίκτυο, ΔΕΕΤ 2003, σελ 105).
(Λιναρίτη, «Η πρόσβαση στις χρηματοοικονομικές υπηρεσίες μέσω Διαδικτύου, σελ 292)

7.2.2. Νομοθεσία για την προστασία των προσωπικών δεδομένων

Το νομικό πλαίσιο που θωρακίζει τα προσωπικά δεδομένα των καταναλωτών διέπεται από τον Ελληνικό νόμο 2472/1997 αλλά και από διάφορες διεθνείς συμβάσεις. Αντικείμενο του παρόντος νόμου είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής.
(ΕφΑθ 4876/2002 ΕτρΑξΧρΔ, 1, 2003, σελ.103-107)

Ακόμη, οι οδηγίες της Ευρωπαϊκής Ένωσης που ολοκληρώνουν το νομοθετικό πλαίσιο της προστασίας των προσωπικών δεδομένων του καταναλωτή είναι οι :

- ✓ 95/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών
- ✓ 97/66/ ΕΚ περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα
- ✓ 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών
- ✓ 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της Οδηγίας 2002/58/ΕΚ.
- ✓ 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών.

Ιδιαίτερη σημασία για το internet banking αποκτά η απαγόρευση να διαβιβάζονται δεδομένα σε τρίτες χώρες εκτός ΕΕ, που δεν παρέχουν « ικανοποιητικό επίπεδο προστασίας» (άρθρο 25 της Οδηγίας 95/46 και άρθρο 9 του Ν.2472/97). Η διαβίβαση προς χώρες εκτός Ευρωπαϊκής Ένωσης επιτρέπεται μόνο έπειτα από άδεια της Αρχής Προστασίας

Δεδομένων 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 από τρίτες χώρες.
(Γιαννόπουλος Γ Ν, «Προστασία προσωπικών δεδομένων και διασυνοριακή ροή πληροφοριών: το πρόβλημα του ' ικανοποιητικού επιπέδου προστασίας'», 2001, σελ 733).

Στην Ελλάδα ρητή αναφορά στο internet banking υπάρχει στην Πράξη Συμβουλίου Νομισματικής Πολιτικής 50/31.7.2002: «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, ενώ στο σχετικό ερωτηματολόγιο υπάρχει ειδική πρόβλεψη για internet και mobile banking, γεγονός που αναδεικνύει ότι και πρακτικά η κεντρική τράπεζα επιθυμεί να θέσει υπό την εποπτεία της και το internet banking. Για τη διεξαγωγή ασφαλών συναλλαγών μέσω internet banking η ελληνική νομοθεσία συμπληρώνεται από το ΠΔ 150/01 για τις ηλεκτρονικές υπογραφές, που εναρμόνισε την ελληνική νομοθεσία με την Οδηγία 99/93. Για την περίπτωση διεξαγωγής συναλλαγών με ίδρυμα ηλεκτρονικού χρήματος ισχύει ο πρόσφατος Ν.3148/2003. Πρόκειται για τον νόμο που επέφερε τις τροποποιήσεις στον βασικό Ν.2076/92 και εναρμόνισε τις οδηγίες 2000/46 και 2000/28 για το ηλεκτρονικό χρήμα.
(Ν.3148/2003 ΦΕΚ Α΄ 136)

7.3. Οι Αρμοδιότητες της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)

Για την εγκυρότητα μιας καθημερινής συναλλαγής απαιτείται η υπογραφή του συναλλασσόμενου. Η υπογραφή σε ένα κείμενο, αποτελεί απόδειξη ότι το υπογράφον το περιεχόμενο του κειμένου πρόσωπο γνωρίζει, αναγνωρίζει, αποδέχεται το κείμενο αυτό. Ο υπογράφων δεν μπορεί να αρνηθεί το από αυτόν υπογεγραμμένο περιεχόμενο, εκτός από συγκεκριμένες περιπτώσεις εκδήλωσης παραβατικής συμπεριφοράς (πλαστογραφία, απάτη κ.λπ). Ένα υπογεγραμμένο κείμενο έχει νομική υπόσταση και επικυρώνει τη συναλλαγή.

Το Π.Δ. 150/2001 που εναρμόνισε την Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές, καθόρισε το πλαίσιο εκείνο μέσα στο οποίο μία ψηφιακή υπογραφή αναγνωρίζεται νομικά ως ιδιόχειρη. Αυτό σημαίνει ότι υπό συγκεκριμένες προϋποθέσεις, τα πρόσωπα που συμβάλλονται σε μία ηλεκτρονική συναλλαγή, και υπογράφουν ηλεκτρονικά, δεν μπορεί να την αρνηθούν.
(Αναλυτική εισήγηση του Α.Μητράκα «Για τις ψηφιακές υπογραφές», ΔΕΕΤ 2003)

Το προεδρικό Διάταγμα, εκτός των άλλων:

- Καθόρισε τους όρους που πρέπει να ισχύουν σε ψηφιακά πιστοποιητικά για να θεωρούνται αναγνωρισμένα πιστοποιητικά και τους όρους που πρέπει να πληρούν οι Πάροχοι Υπηρεσιών Πιστοποίησης για να παρέχουν αναγνωρισμένα πιστοποιητικά.
- Έθεσε τις αρχές λειτουργίας της εσωτερικής αγοράς όσον αφορά την παροχή υπηρεσιών πιστοποίησης
- Έθεσε τις προϋποθέσεις νομικής αναγνώρισης εντός ΕΕ των αναγνωρισμένων πιστοποιητικών που εκδίδονται από Παρόχους Υπηρεσιών Πιστοποίησης εγκατεστημένους σε χώρες εκτός ΕΕ, και άλλες σχετικές προβλέψεις που αφορούν διεθνείς πτυχές.

- Έθεσε το πλαίσιο της ευθύνης των Παρόχων Υπηρεσιών Πιστοποίησης
- Ανέθεσε στην ΕΕΤΤ συγκεκριμένες αρμοδιότητες.

Οι αρμοδιότητες της ΕΕΤΤ όπως απορρέουν από το ΠΔ 150/2001, είναι επιγραμματικά οι εξής:

- Η παροχή Εθελοντικής Διαπίστευσης, ύστερα από έγγραφη αίτηση του ενδιαφερόμενου Παρόχου Υπηρεσιών Πιστοποίησης, προκειμένου να επιτευχθεί βελτιωμένο επίπεδο παροχής υπηρεσιών πιστοποίησης. (άρθρο 4 παρ. 5 εδ.α) ή η ανάθεση σε δημόσιους ή ιδιωτικούς φορείς του έργου αυτού. Με την Εθελοντική Διαπίστευση απονέμονται δικαιώματα και επιβάλλονται υποχρεώσεις, συμπεριλαμβανομένων τελών, στον Πάροχο Υπηρεσιών Πιστοποίησης.
- Η εποπτεία και ο έλεγχος των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης, καθώς και των φορέων διαπίστευσης και ελέγχου της συμμόρφωσης των υπογραφών προς το Παράρτημα ΙΙΙ του πδ. 150/2001 (εφόσον η ΕΕΤΤ αναθέσει τέτοια καθήκοντα σε άλλους φορείς) (άρθρο 4 παρ. 8).
- Η διαπίστωση της συμμόρφωσης των διατάξεων δημιουργίας υπογραφής (υλικού ή λογισμικού που χρησιμοποιείται για την εφαρμογή του ιδιωτικού κλειδιού για τη δημιουργία της ηλεκτρονικής υπογραφής) προς το Παράρτημα ΙΙΙ του Προεδρικού Διατάγματος 150/2001 (άρθρο 4 παρ. 2, εδ.α) ή ανάθεση σε δημόσιους ή ιδιωτικούς φορείς του έργου αυτού.
- Η επιβολή προστίμων σε Παρόχους Υπηρεσιών Πιστοποίησης, οι οποίοι ενεργούν ως διαπιστευμένοι, χωρίς να είναι (άρθρο 4 παρ.9)
- Η ενημέρωση της Ευρωπαϊκής Επιτροπής για τις επωνυμίες και τις διευθύνσεις όλων των διαπιστευμένων εθνικών Παρόχων Υπηρεσιών Πιστοποίησης, καθώς και για τυχόν αλλαγές στις παραπάνω πληροφορίες (άρθρα 8 παρ. 2 και 3).

Η ΕΕΤΤ με την υπ. αρ. 248/71 Απόφασή της «Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής», ρυθμίζει ζητήματα των αναγνωρισμένων πιστοποιητικών και θέτει το θεσμικό πλαίσιο για την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης.
(ΦΕΚ 603/Β/16-5-2002)

7.4. Αποφάσεις της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών

- ΑΠΟΦΑΣΗ 634 α «Κανονισμός για την Διασφάλιση του Απορρήτου Εφαρμογών και Χρήστη Διαδικτύου» (ΦΕΚ Β' 88, 26.01.2005 σελ. 1050 επόμενα)
- ΑΠΟΦΑΣΗ 633 α «Κανονισμός για την Διασφάλιση του Απορρήτου Διαδικτυακών Υποδομών» (ΦΕΚ Β' 88, 26.01.2005 σελ. 1038-1050)
- ΑΠΟΦΑΣΗ 632 α «Κανονισμός για την Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές» (ΦΕΚ Β' 88, 26.01.2005 σελ. 1033-1038)
- ΑΠΟΦΑΣΗ 631 α «Κανονισμός για την Διασφάλιση του Απορρήτου κατά την Παροχή Τηλεπικοινωνιακών Υπηρεσιών μέσω Ασύρματων Δικτύων» (ΦΕΚ Β' 87, 26.1.2005, σελ. 1026 επόμενα)
- ΑΠΟΦΑΣΗ 630 α «Κανονισμός για την Διασφάλιση του Απορρήτου κατά την Παροχή Σταθερών Τηλεπικοινωνιακών Υπηρεσιών» (ΦΕΚ Β' 87, 26.1.2005, σελ. 1020-1025)
- ΑΠΟΦΑΣΗ 629 α «Κανονισμός για την Διασφάλιση του Απορρήτου κατά την Παροχή Κινητών Τηλεπικοινωνιακών Υπηρεσιών» (ΦΕΚ Β' 87, 26.1.2005, σελ. 1013-1020)

Πηγή: ΑΔΑΕ http://www.adae.gr/adae/regulations.html

7.4. Ευρωπαϊκή νομοθεσία

Το Ευρωπαϊκό κοινοτικό δίκαιο για την ηλεκτρονική τραπεζική, αποτελείται από αρκετές οδηγίες, οι οποίες είναι ταξινομημένες σε 3 θεματικές ενότητες:

- Σε αυτήν την ενότητα εντάσσονται οι οδηγίες που αφορούν την ανάληψη και άσκηση δραστηριοτήτων ηλεκτρονικής τραπεζικής από τα κοινοτικά χρηματοπιστωτικά ιδρύματα. Οι οδηγίες της ελεύθερης παροχής ηλεκτρονικής τραπεζικής είναι οι:
  - ✓ 2000/12/ ΕΚ σχετικά με την ανάληψη και άσκηση δραστηριότητας πιστωτικών ιδρυμάτων
  - ✓ 2000/28/ ΕΚ που τροποποιεί την προηγούμενη
  - ✓ 2000/46/ ΕΚ που αναφέρεται στην ανάληψη, την άσκηση και την προληπτική εποπτεία των δραστηριοτήτων των ιδρυμάτων ηλεκτρονικού χρήματος
    (Gkoutzinis A., The Prudential Supervision of Internet Banking in the United Kingdom Is the "Basel Approach" finding its way through National Regulations, JIBL, 2002, σελ. 249).
  - ✓ 2009/110/ΕΚ για την ανάληψη, άσκηση και προληπτική εποπτεία της δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος, την τροποποίηση των οδηγιών 2005/60/ΕΚ και 2006/48/ΕΚ και την κατάργηση της Οδηγίας 2000/46/ΕΚ (L 267/10.10.2009) περί Ηλεκτρονικού Χρήματος.
- Σε αυτήν την ενότητα εντάσσονται οι οδηγίες που αφορούν την κοινωνία της πληροφορίας και την εξ' αποστάσεως εμπορία χρηματοοικονομικών υπηρεσιών.

Οι οδηγίες είναι οι:

- ✓ 2000/31/ ΕΚ για νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας και ιδιαίτερα του ηλεκτρονικού εμπορίου που εισάγει την αρχή του «κράτους προέλευσης», σύμφωνα με την οποία « ο τόπος εγκατάστασης εταιρείας που παρέχει υπηρεσίες μέσω διεύθυνσης (site) Internet, δεν βρίσκεται εκεί που είναι η τεχνολογία που υποστηρίζει την εν λόγω διεύθυνση ούτε εκεί που παρέχεται πρόσβαση στην ενλόγω διεύθυνση, αλλά εκεί που ασκεί την οικονομική της δραστηριότητα»,

  (Αλεξανδρίδου Ε, «Η πρόταση οδηγίας της ΕΕ για το ηλεκτρονικό εμπόριο και η προστασία του καταναλωτή, σε ΔΕΕ, 2, 2000, σελ. 113 (ΦΕΚ Α΄116, ΚΝοΒ, σελ.693))

- ✓ 2002/65/ ΕΚ σχετικά με την εξ'αποστάσεως εμπορία χρηματοοικονομικών υπηρεσιών προς τους καταναλωτές, η οποία αποδίδει την ιδιότητα του καταναλωτή σε 'σε κάθε πρόσωπο το οποίο, στο πλαίσιο των συμβάσεων εξ'αποστάσεως ενεργεί για σκοπούς εκτός του πεδίου της εμπορικής ή επαγγελματικής του δραστηριότητας'

  (Γιαννόπουλος, Internet Banking : Νομικά ζητήματα από την διεξαγωγή τραπεζικών συναλλαγών στο διαδίκτυο, ΔΕΕΤ 2003, σελ 105).

- ✓ 99/93/ ΕΚ σε σχέση με τις ηλεκτρονικές υπογραφές. Για τη διεξαγωγή ασφαλών συναλλαγών η Ελληνική νομοθεσία συμπληρώνεται από το ΠΔ 150/01, που εναρμόνισε την Ελληνική νομοθεσία με την Οδηγία αυτή. Για την περίπτωση διεξαγωγής συναλλαγών με ίδρυμα ηλεκτρονικού χρήματος ισχύει ο Ν.3148/2003.

  (Αναλυτική Εισήγηση του Α.Μητράκα, «σχετικά με τις ψηφιακές υπογραφές» ΔΕΕΤ 2003)

- ✓ 98/48/ ΕΚ που αφορά την καθιέρωση μίας διαδικασίας πληροφόρησης στον τομέα των προτύπων και των προδιαγραφών

➢ Σε αυτήν την ενότητα εντάσσονται κοινοτικές πράξεις που αφορούν την διενέργεια πληρωμών στο ηλεκτρονικό εμπόριο. Συγκεκριμένα είναι:

- ✓ η σύσταση 97/489/ΕΚ της Ευρωπαϊκής Επιτροπής σχετικά με τις συναλλαγές που πραγματοποιούνται με ηλεκτρονικές πληρωμές.
- ✓ ο κανονισμός 2560/2001/ΕΚ ο οποίος αφορά τις διασυνοριακές πληρωμές σε ευρώ που διασφαλίζει τη διαφάνεια των εξόδων που επιβάλλονται και ευθυγραμμίζει το ύψος τους κατά τις συναλλαγές εντός ΕΕ.

  (Γκόρτσο Χ., «Ο κανονισμός 2560/2001 σχετικά με τις διασυνοριακές πληρωμές σε ευρώ» ΔΕΕΤ, αρ. 28, 2002, σελ 40)

- ✓ Η απόφαση –πλαίσιο 2001/413/ΔΕΥ Ε.Σ. για την καταπολέμηση της απάτης και πλαστογραφίας.

Το ρυθμιστικό πλαίσιο για την ηλεκτρονική τραπεζική στο Ευρωπαϊκό κοινοτικό δίκαιο έχει τους εξής στόχους:

- Να δημιουργήσει ένα συνεκτικό κανονιστικό πλαίσιο που θα εξασφαλίσει την άρτια παροχή ηλεκτρονικών τραπεζικών υπηρεσιών, αποφεύγοντας τις εθνικές νομοθετικές αποκλίσεις.
- Να διασφαλίσει τη συνοχή μεταξύ της νομοθεσίας για τα χρηματοπιστωτικά ιδρύματα και της οδηγίας για το ηλεκτρονικό εμπόριο.

Παρόλη τη νευραλγική σημασία του ιδιωτικού διεθνούς δικαίου όσον αφορά στην εύρεση του εφαρμοστέου δικαίου στις συναλλαγές e-banking, ο τεχνικός και συχνά πολύπλοκος χαρακτήρας των τραπεζικών συναλλαγών και η έντονη παρουσία εθνικών κανόνων αναγκαστικού δικαίου, σε συνδυασμό με τα ζητήματα που ανακύπτουν από την εφαρμογή του κοινοτικού δικαίου (2000/31/ΕΚ), καθιστούν ιδιαίτερα δύσκολο το συγκεκριμένο εγχείρημα. Άλλωστε, οι παραδοσιακοί κανόνες συνδέσεως, που εμπεριέχουν συνδέσμους γεωγραφικής μορφής, δύσκολα μπορούν να ανταπεξέλθουν στις ανάγκες και τις ιδιαιτερότητες της εικονικής πραγματικότητας του Κυβερνοχώρου. Για τους λόγους αυτούς, έχει υποστηριχθεί διεθνώς η δημιουργία ενός συστήματος ουσιαστικών κανόνων και είναι πρέπον να τηρείται. (Λαζακίδου Α., Λαζακίδου Γ., 2004, σελ.200).

Στην περίπτωση αυτή τυγχάνει εφαρμογής το κανονιστικό πλαίσιο που ισχύει στη χώρα παροχής των υπηρεσιών, με την επιφύλαξη των διατάξεων:

- ✓ της Γενικής Συμφωνίας για τις Συναλλαγές στον Τομέα των Υπηρεσιών, εφόσον η χώρα εγκατάστασης είναι μέλος του Παγκόσμιου Οργανισμού Εμπορίου
- ✓ του Κανονιστικού Πλαισίου της Επιτροπής της Βασιλείας για την Τραπεζική Εποπτεία
- ✓ Συναφών Διμερών Συμβάσεων.

Για την εύρεση του εφαρμοστέου δικαίου σε περίπτωση που κάποια διαφορά εισάγεται ενώπιον δικαστηρίου στην ΕΕ, θα ισχύει η Σύμβαση της Ρώμης (1980), η οποία εισάγει τη γενική αρχή της ελεύθερης επιλογής του δικαίου από τα συμβαλλόμενα μέρη, αλλά προβλέπει και εξερέσεις. Για το M-Banking και για το E-Banking γενικότερα ειδικό πρόβλημα πιθανώς θα παρουσιαστεί κατά την προσπάθεια ανεύρεσης του δικαίου της χώρας στενότερης σύνδεσης για την εκπλήρωση της παροχής. Η Σύμβαση της Ρώμης έχει κυρωθεί από την Ελλάδα με τον Ν.1792/1988.

(Γιαννόπουλος, Internet Banking : Νομικά ζητήματα από την διεξαγωγή τραπεζικών συναλλαγών στο διαδίκτυο, ΔΕΕΤ 2003, σελ 107).

Η Ευρωπαϊκή Ένωση έχει αναγνωρίσει τη σχετική ανάγκη και συμβάλλει μέσω της συμμετοχής των θεσμικών οργάνων της για την επίτευξη του εν λόγω στόχου. Διεθνείς οργανισμοί στους κόλπους των οποίων αναπτύσσεται η εν λόγω συνεργασία είναι :

- ✓ ο Παγκόσμιος Οργανισμός Εμπορίου
- ✓ η Επιτροπή της Βασιλείας για την Τραπεζική Εποπτεία
- ✓ ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης

1. Ν. 3148/2003 (ΦΕΚ Α΄ 136/5.6.2003) – Επιτροπή Λογιστικής Τυποποίησης και Ελέγχων, αντικατάσταση και συμπλήρωση των διατάξεων για τα ιδρύματα ηλεκτρονικού χρήματος (Άρθρα 14, 15, 18).....
2. Π.Δ. 131/2003 (ΦΕΚ Α΄ 116/16.05.2003) Προσαρμογή στην Οδηγία 2000/31 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά.....
3. Π.Δ. 150/2001 (ΦΕΚ Α΄ 125/25.6.2001). Προσαρμογή στην Οδηγία 99/93 ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.....
4. Απόφαση 2004/10/ΕΚ της Επιτροπής της 5ης Νοεμβρίου 2003 για τη σύσταση της Ευρωπαϊκής επιτροπής τραπεζών (European Banking Committee).....
5. Απόφαση 2004/5/ΕΚ της Επιτροπής της 5ης Νοεμβρίου 2003 για τη σύσταση της επιτροπής ευρωπαϊκών αρχών τραπεζικής εποπτείας (Commitee of European Banking Supervisors)....
6. Οδηγία 2002/65/ΕΚ σχετικά με την εξ αποστάσεως εμπορία χρηματοοικονομικών υπηρεσιών προς τους καταναλωτές και την τροποποίηση των Οδηγιών 90/619 ΕΟΚ του Συμβουλίου, 97/7/ ΕΚ και 98/27/ΕΚ.....
7. Οδηγία 2000/31 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά.....
8. Πράξη Διοικητή της Τράπεζας της Ελλάδος (υπ' αριθ. 2527/ 8.12.2003) με θέμα «Κανόνες προληπτικής εποπτείας από την Τράπεζα της Ελλάδος των Ιδρυμάτων Ηλεκτρονικού Χρήματος»
9. Πράξη Διοικητή της Τράπεζας της Ελλάδος (υπ' αριθ. 2501/ 31.10.2002) με θέμα την ενημέρωση των συναλλασσομένων με τα πιστωτικά ιδρύματα για τους όρους που διέπουν τις συναλλαγές του.....
10. Το Π.Δ. 150/2001 που εναρμόνισε την Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές, καθόρισε το πλαίσιο εκείνο μέσα στο οποίο μία ψηφιακή υπογραφή αναγνωρίζεται νομικά ως ιδιόχειρη. Αυτό σημαίνει ότι υπό συγκεκριμένες προϋποθέσεις, τα πρόσωπα που συμβάλλονται σε μία ηλεκτρονική συναλλαγή, και υπογράφουν ηλεκτρονικά, δεν μπορεί να την αρνηθούν.
11. Η ΕΕΤΤ με την υπ. αρ. 248/71 Απόφασή της «Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής» (ΦΕΚ 603/Β/16-5-2002) ρυθμίζει ζητήματα των αναγνωρισμένων πιστοποιητικών και θέτει το θεσμικό πλαίσιο για την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης.
12. 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών.

ΠΑΡΑΡΤΗΜΑ

Εισαγωγή

Το παρόν τμήμα της εργασίας αποτελεί μία προσπάθεια ανάπτυξης ιστοσελίδας WebSite που θα απαντά στις ανάγκες των πελατών μιας τράπεζας, η οποία με τη σειρά της επιθυμεί να δοθεί έμφαση στη δομή του συστήματος της και στην σωστή εφαρμογή του M-Banking ή E-Banking με τις απαιτούμενες ροές και διαδικασίες της δραστηριότητα της. Η ιστοσελίδα θα περιλαμβάνει όλα τα είδη των προιόντων που αφορούν την ηλεκτρονική τραπεζική της και τα οποία θα πρέπει να παραμετροποιούνται από το Προσωπικό της Τράπεζας.

Τεχνολογία Λογισμικού

Τεχνολογία Λογισμικού είναι η επιστήμη που ασχολείται με όλες τις φάσεις της παραγωγής Λογισμικού, από το πρώιμο στάδιο της σύλληψης απαιτήσεων έως και τη συντήρηση του συστήματος, ακόμη και αν είναι σε χρήση.

Χαρακτηριστικά Ποιότητας Λογισμικού

Η ποιότητα είναι ένα πολύ σημαντικό χαρακτηριστικό τη σημερινή ανταγωνιστική εποχή, επομένως ένα προιόν, όπως είναι ένα λογισμικό, πρέπει να αποτελείται από ορισμένους παράγοντες που υποδηλώνουν την ποιότητα του. Αυτά τα χαρακτηριστικά είναι τα εξής για ένα Λογισμικό (Somerville, 2001):

Σύμφωνα λοιπόν με τον Ian Somerville (2001), οι φάσεις αυτές είναι οι εξής τέσσερις:

- ✓ *Ανάλυση Απαιτήσεων.* Οι λειτουργίες του λογισμικού πρέπει να οριστούν.
- ✓ *Ανάπτυξη Λογισμικού.* Το λογισμικό πρέπει να αναπτυχθεί με τέτοιον τρόπο, ώστε να ικανοποιεί τις ανάγκες του πελάτη.
- ✓ *Ελεγχος Λογισμικού.* Το Λογισμικό πρέπει να επικυρωθεί με την προυπόθεση ότι ανταποκρίνεται στις απαιτήσεις του πελάτη
- ✓ *Εξέλιξη Λογισμικού.* Το Λογισμικό πρέπει να είναι ικανό να προσαρμόζεται στις καινούριες εξελίξεις, καθώς οι απαιτήσεις μπορούν να αλλάζουν και μόνο η ικανότητα αλλαγής σε καινούρια περιβάλλοντα καθιστούν συντηρήσιμο ένα Λογισμικό.

Οι παραπάνω φάσεις αποτελούν και τον κύκλο ζωής Λογισμικού, ο οποίος περιγράφει την εξέλιξη του Λογισμικού από τη σύλληψη μέχρι την τελευταία έκδοση. Είναι ανάλογο με την ανθρώπινη ζωή που ξεκινά από τη σύλληψη του παιδιού και συνεχίζεται μέχρι τον θάνατο.

Πίνακας 2: Χαρακτηριστικά Λογισμικού

Χαρακτηριστικά Προιόντος	Περιγραφή
Συντηρησιμότητα	Ενα Λογισμικό πρέπει να έχει την ικανότητα να ανταποκρίνεται στις καινούριες ανάγκες του πελάτη που απορρέουν από την αλλαγή του περιβάλλοντος
Εξάρτηση	Η εξάρτηση του λογισμικού από άλλα συστήματα δεν πρέπει να επηρεάζει την αξιοπιστία και ασφάλεια
Αποδοτικότητα	Το Λογισμικό πρέπει να είναι αποδοτικό όσον αφορά τη χρήση πόρων όπως μνήμη, επεργαστική ισχύ, χρόνος αναμονής.
Χρησιμοποιησιμότητα	Το σύστημα πρέπει να αποτελείται από πλήρες εγχειρίδιο χρήσης και τεκμηρίωσης για τη σωστή κι εύκολη χρήση από τη μεριά του χρήστη

Χαρακτηριστικά Ιστοσελίδας Τραπεζών

Η ποιότητα είναι ένα πολύ σημαντικό χαρακτηριστικό στη σημερινή ανταγωνιστική εποχή, επομένως ένα προιόν, όπως είναι μία ιστοσελίδα, πρέπει να αποτελείται από ορισμένους παράγοντες που υποδηλώνουν την χρηστικότητα της.

Αυτά τα χαρακτηριστικά είναι τα εξής:

- *Καταλληλότητα*. Η ποιότητα του περιεχομένου ενός WebSite πρέπει να είναι η πρώτη προτεραιότητα, ώστε να είναι κατάλληλο για τους χρήστες της ιστοσελίδας.
- *Εύρος περιεχομένου*. Η σωστή ποσότητα πληροφορίας που δεν θα προβληματίζει τους χρήστες, ακόμα και τους μη εξοικειωμένους, είναι ο στόχος μίας προσιτής ιστοσελίδας. Για να επιτευχθεί αυτό θα πρέπει οι διασυνδέσεις να μην είναι στην κεντρική σελίδα και να υπάρχει ειδική σήμανση που να δείχνει οτι οι χρήστες πιθανότατα θα οδηγηθούν εκτός της συγκεκριμένης ιστοσελίδας.
- *Χρηστικότητα*. Είναι βασικό οι χρήστες να καταλάβουν από την αρχή τι μπορούν να κάνουν στη ιστοσελίδα και με ποιά διδικασία. Οι τίτλοι των θεματικών περιοχών πρέπει να είναι κατανοητοί δίνοντας σαφείς πληροφορίες για το περιεχόμενο των πληροφοριών.
- *Ανάδραση*: Η παροχή κατάλληλων πληροφοριών κάνει τον χρήστη να νιώθει σίγουρος για τις επιλογές του. Τα βασικά σημεία της ιστοσελίδας θα πρέπει να διαχωρίζονται οπτικά, ο ήχος και τα γραφικά να είναι εύχρηστα και απλά χωρίς υπερβολική χρήση της τεχνολογίας.
- *Πληροφόρηση*. Η σωστή και επίκαιρη πληροφόρηση είναι βασική προυπόθεση για την βιωσιμότητα μίας ιστοσελίδας. Η τακτική ανανέωση και το «φρεσκάρισμα» των πληροφοριών προδιαθέτει τους χρήστες για περαιτέρω χρήση της.

- *Αισθητική*. Μία ιστοσελίδα σωστά δομημένη με τις διεργασίες ομαδοποιημένες και όχι υπερφορτωμένες χωρίς να μπερδεύουν τους χρήστες. Η ορολογία να είναι αντιπροσωπευτική, τα αντικείμενα πλοήγησης θα πρέπει να είναι σε εμφανές χώρο και οι βασικότερες διεργασίες να είναι εύκολα προσβάσιμες. Η χρήση γραφικών όπως ήχος και κίνηση δίνουν «ζωή» στην ιστοσελίδα και προδιαθέτουν ευχάριστα τους χρήστες.

Λειτουργικότητα Ιστοσελίδων

Ο σωστός σχεδιασμός της ιστοσελίδας εξαρτάται από ορισμένους παράγοντες που πρέπει να λαμβάνονται υπ'όψην τόσο από πλευράς χρήστών, όσο και από πλευράς σχεδιαστών:

ΧΡΗΣΤΕΣ:

- *Ανάγκη για ταχύτητα*: Η άμεση ικανοποίηση ενός αιτήματος είναι βασική προϋπόθεση. Στόχος είναι η απόκριση σε περιβάλλον internet να μην είναι περισσότερη από 1 sec. Σε περίπτωση modem με απόκριση όχι περισσότερο από 1 sec οι σελίδες πρέπει να είναι μόνο 2kb, ενώ για 10 sec απόκριση δεν πρέπει να ξεπερνούν τα 30kb.
- *Σπασμένοι συνδέσμοι* (Broken links): Ο συνεχής έλεγχος των ιστοσελίδων για σπασμένους συνδέσμους και η συντήρηση τους με κάποια εφαρμογή spider ή link checker είναι μία καλή κίνηση προς τους χρήστες.
- *No scrolling*: Τους χρήστες δεν τους διευκολύνει το scroll. Οι ιστοσελίδες πρέπει να είναι όσο πιο περιεκτικές γίνεται και η σημαντική πληροφορία καθώς και τα στοιχεία ελέγχου πρέπει να είναι μέσα στα όρια της πρώτης οθόνης.
- *Οπτική Σάρωση*: Οι χρήστες ψάχνουν για τονισμένους όρους, λέξεις, φράσεις, επικεφαλίδες και υπερσυνδέσμους. Σύμφωνα με έρευνα των 'Morkes and Nielsen' το 79% των χρηστών πάντα σάρωνε οπτικά μία νέα ιστοσελίδα και μόνο το 16% διάβαζε τα περιεχόμενα. Επικρατεί η τάση μη ανάγνωσης μεγάλων κειμένων στην οθόνη, καθώς ο ρυθμός ανάγνωσης μειώνεται κατά 25%, με τους χρήστες να περιορίζονται στην ανάγνωση της πρώτης πρότασης της παραγράφου κειμένου.
- *Προχωρημένη Αναζήτηση*: Η πλειονότητα των χρηστών προτιμούν τις υπηρεσίες αναζήτησης παρά την ακολουθία κάποιας αλληλουχίας συνδέσμων που θα δώσει την επιθυμητή πληροφορία. Το κουμπί της αναζήτησης πρέπει να υπάρχει ενεργό σε όλες τις σελίδες και να παρέχεται ένα Advanced Search για πιο εξειδικευμένη χρήση.
- *Όνομα πεδίου*: Ένα εύκολο και με μικρό μήκος όνομα πεδίου (domain name) διευκολύνει στην απομνημόνευση αλλά και στην πληκτρολόγηση- βασικό στο M-Banking- όπου η πληκτρολόγιση στα στενά πλαίσια μίας οθόνης κινητού τηλεφώνου αποτελεί τεστ δεξιότητας.

ΣΧΕΔΙΑΣΤΕΣ

Οι σχεδιαστές προσεγγίζουν τον σχεδιασμό μίας ιστοσελίδας με δύο μεθόδους:

- ✓ *Της Γραφιστικής* όπου δίνεται έμφαση στον ενθουσιασμό του χρήστη με την εμφάνιση, την καλαισθησία, την ψυχαγωγία και με τη χρήση οπτικοακουστικών εφέ.
- ✓ *Της Τεχνικής προσέγγισης* όπου δίνεται έμφαση στην εύκολη πλοήγηση και ευχρηστία της ιστοσελίδας με τεχνικούς περιορισμούς. Με τη μέθοδο αυτή ο χρήστης εύκολα μπορεί να βρει αυτό που αναζητά με λιγότερο κόπο και χρόνο ακόμα και αν δεν γνωρίζει τι ακριβώς επιθυμεί.

Για να υπάρξουν θετικά αποτελέσματα, που θα οδηγήσουν στον σωστό σχεδιασμό μίας ιστοσελίδας, οι σχεδιαστές θα πρέπει να ακολουθήσουν κάποια βασικά σημεία:

- *Πληροφορίες ανά σελίδα*. Βασική ανάγκη του χρήστη, ειδικά όταν έχουμε M-Banking και E-Banking, είναι να υπάρχει όσο περισσότερη χρήσιμη πληροφορία σε μία σελίδα. Αν λάβει κανείς υπόψη οτι σε μία σελίδα ένα ποσοστό της τάξεως του 20%-30% καλύπτεται από τα κουμπιά πλοήγησης, τα γραφικά και τις απεικονίσεις, άλλο ένα 30% καλύπτεται από τα γραφικά του φυλλομετρητή και του λειτουργικού συστήματος, ο χώρος της χρήσιμης για τον χρήστη πληροφορίας είναι πολύ μικρός.
- *Ανάλυση οθόνης*. Ο χρήστης θέλει την καλύτερη ανάλυση. Λόγω της μεγάλης ποικιλίας μεγεθών και τύπων οθονών που έχουν τα έξυπνα τηλέφωνα (smartphones), tablets, φορητοί υπολογιστές ο σχεδιασμός μίας ιστοσελίδας θα πρέπει να γίνεται με βάση τον μέσο όρο των οθονών που πωλούνται.
- *Γρήγορη πλοήγηση*. Το γρήγορο “serfarisma” χαρακτηρίζει τη χρηστικότητα μίας ιστοσελίδας. Ο χρήστης επιθυμεί να έχει άμεση επικοινωνία και μεγάλη ταχύτητα στο ‘κατέβασμα’ του περιεχομένου μίας ιστοσελίδας. Αν υπάρχει καθυστέρηση στην απόκριση μεγαλύτερη των 10sec (έρευνα Robert B.Miller) ο χρήστης αποθαρρύνεται και ανατρέχει σε άλλη σελίδα.
- *Πολυμεσικό υλικό*. Στην προσπάθεια του σχεδιαστή να κάνει την ιστοσελίδα περισσότερο φιλική προς τον χρήστη ενσωματώνει εικόνες, video, διαφημιστικά spot, προβολή τρισδιάστατων κινούμενων αντικειμένων. Αυτό έχει σαν αποτέλεσμα μία χρονική καθυστέρηση που συνήθως κουράζει τον χρήστη και γι’αυτό θα πρέπει να γίνεται φειδωλή χρήση των multimedia.

Βιβλιογραφία- Παραπομπές

Ελληνική

- Αριστέα Σινανιώτη- Μαρούδη και Ιωάννης Φαρσαρώτας, «Ηλεκτρονική τραπεζική», Αθήνα-Κομοτηνή, 2005.
- Ιωάννης Δ.Φρσαρώτας, «Κατανοώντας τη Σύγχρονη Τραπεζική» Αθήνα-Κομοτηνή, 2009.
- Βίρβου Μαρία (2007): Σημειώσεις ΠΜΣ ΠΛΗΡΟΦΟΡΙΚΗ Τεχνολογία Λογισμικού, Πανεπιστήμιο Πειραιά.
- Γκόρτσος, "Το ευρωπαϊκό κοινοτικό δίκαιο για την ηλεκτρονική τραπεζική", 2003)
- Αγγέλης, Γ. Βασίλης, «Η Βίβλος του e-banking», Εκδόσεις Νέων Τεχνολογιών, 2005.
- Γεωργόπουλος, Πανταζή, Νικολαράκος, Βαγγελάτος, «Ηλεκτρονικό επιχειρείν, προγραμματισμός και σχεδίαση», Εκδόσεις Μπένου, 2001.
- Γλύκας, Ξηρογιάννης, «Στρατηγική ηλεκτρονικού επιχειρείν χρηματοπιστωτικών ιδρυμάτων», 2004.
- Παναγιωτόπουλος Ι.Χ.(2007): *Σημειώσεις* ΠΜΣ ΠΛΗΡΟΦΟΡΙΚΗ C++, Πανεπιστήμιο Πειραιά.
- Κ.Δελούκα-Ιγγλεση «Νομικά Θέματα Ηλεκτρονικού Εμπορίου»
- Καράκωστας «Δίκαιο και Internet, Νομικά Ζητήματα»
- Μάγκος Εμμανουήλ *Ασφάλεια στο* World Wide Web Πειραιάς 1997 (Πτυχιακή εργασία)
- Ιγγλεζάκης Δ. Ιωάννης, «Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου», 2003.
- Κατσουλάκος Γιάννης, «Νέα οικονομία, διαδίκτυο και ηλεκτρονικό εμπόριο», 2001.
- Χρυσάνθης Χ.«Η ηλεκτρονική εξυπηρέτηση των σύγχρονων τραπεζικών συναλλαγών»
- Μπάσιος Χρήστος «Mobile Payment:Βασικές Αρχές και Εφαρμογές» (Εργασία στα πλαίσια του μεταπτυχιακού μαθήματος «Δίκτυα Προστιθέμενης Αξίας EDI και Εφαρμογές Ηλεκτρονικού Εμπορίου»), Αθήνα, Ιούλιος 2004.
- Αντωνία Γ.Κοντογεωργάκη, «Η διεθνής Δικαιοδοσία και το Εφαρμοστέο Δίκαιο στις Ηλεκτρονικές Τραπεζικές Συναλλαγές» Διπλωματική Εργασία στα πλαίσια του μεταπτυχιακού προγράμματος «Δίκαιο και Ευρωπαϊκή Ενοποίηση»), 2007.
- Καρέκλης, Π., (2003), Οφέλη από τη χρήση υπηρεσιών ηλεκτρονικής τραπεζικής. Δελτίο Ένωσης Ελληνικών Τραπεζών.
- Καρέκλης,Π. (2003), Επιπτώσεις του Internet στη λειτουργία και κερδοφορία των επιχειρήσεων. Οφέλη από την χρήση υπηρεσιών ηλεκτρονικής τραπεζικής, *'δελτίο* Ένωσης Ελληνικών Τραπεζών, Αφιέρωμα στο Internet Banking, Δελτίο Ένωσης Ελληνικών Τραπεζών, Γ΄ Τριμ. 2003.
- Τζανάκη Γλυκερία Τριανταφυλλάκη Εμμανουέλα «Υιοθέτηση της Διαδικτυακής Τραπεζικής στις Ελληνικές τράπεζες (e- banking)»
- Λουλάκη Νίκη «Προώθηση Ηλεκτρονικών Τραπεζικών Υπηρεσιών» διπλωματική εργασία- Πανεπιστήμιο Μακεδονίας.
- Αλωνιστιώτη Νάνσυ και Γαζής Βαγγέλης (2007): Σημειώσεις ΠΜΣ ΠΛΗΡΟΦΟΡΙΚΗ Πληροφοριακά Συστήματα, Πανεπιστήμιο Πειραιά.
- Χαλάτσης Κ. Κρυπτογραφία – Σύγχρονες Τάσεις. (διαθέσιμο από την διεύθυνση του συνεδρίου, δεύτερη ημέρα 4η θεματική ενότητα).
- Μπιζανίδης Γ.«M-Banking, Διαχείρηση τραπεζικών συναλλαγών μέσω κινητού τηλεφώνο»
- Χατζή Ευαγγελία «Το E-Banking στην Ελλάδα» 2012 Περίπτωση της MILLENNIUM BANK.
- Ανδροπούλου Χρ. «Ηλεκτρονικές Τραπεζικές Υπηρεσίες,Μελέτη περίπτωσης ικανοποίησης πελατών σε συγκεκριμένη τράπεζα» Παν. Πειραιώς 2011
- Καλουπτσίδης και άλλοι. Ανάλυση και Σχεδιασμός Συμμετρικών Κρυπτογραφικών Αλγορίθμων Αθήνα, ΕΚΠΑ 31/10/2001 (διαθέσιμο από την διεύθυνση του συνεδρίου, δεύτερη ημέρα 4η θεματική ενότητα).
- (Ίδρυμα Οικονομικών και Βιομηχανικών Ερευνών, (2007), 'Μελέτη των κλάδων Πληροφορικής και Τηλεπικοινωνιών στην Ελλάδα: Κατάσταση και Προοπτικές' www.observe.gr/files/meletes/ΤΠΕ_Φβ_ΠΑΡΑΔ12_final.pdf)
- Δεμίρη Ανδρ. «Ανάλυση και αξιολόγηση ιστοσελίδων».
- Μαρία Κασκαντάμη «Αξιολόγηση ιστοσελίδων» Επιμορφώτρια ΤΠΕ
- Κρομμύδας Θεόδωρος «E-Banking και ασφαλείς πληρωμές» Πτυχιακή
- Δαμιανού Ε.-Θεοδωράκη Φ. «E-Banking» πτυχιακή εργασία ΤΕΙ Κρήτης
- Αργυρώ Γκάτσου «E-Banking και συναλλαγές μέσω τηλεφώνου» Πα.Πειραιώς 2010
- Περιοδικό RAM «Οι τράπεζες στο χώρο του Internet» Ιούνιος 2000.

Ξενόγλωσση

- Beiginia, A., Besheli, A., Soluklu, M., Ahmadi, M. (2011). Assessing the Mobile Banking Adoption Based on the DecomposedTheory of Planned Behaviour, European Journal of Economics, Finance and Administrative Sciences , Issue 28.
- Emmanuel, A. (2007). Mobile Banking in Developing Countries: Secure Framework for Delivery of SMS-banking Services.Master Thesis.
- Foley, B. (2008). Issues for Mobile Banking Services, I-Reach alert,from www.ireach.ie.
- Orsak, B. (2007). Mobile banking poses laundering, security risks, Issues for Mobile Banking Services, iReach.http:// www.moneylaundering.com/inform.fortent.com
- Kainth, G. (2010). Mobile Banking: A Boon for Unbanked, MBA Journal
- Barnes, S, Corbitt, B. (2003). Mobile banking: Concept and potential, International Journal of Mobile Communications.
- Ochieng, Z. (2010). Bright days ahead for mobile anking, http://mobilemoneyafrica.com/?p=2580
- Mark S. Merkow (2004). "Secure Electronic Transactions (SET)".
- Stallings, William (Nov 1, 2000). "The SET Standard & E-Commerce". Dr. Dobbs.
- Brown Lawrie Cryptography and Computer Security - Cryptography Lecture 12 Modern Stream Ciphers November 2001.
- Broderick A, Vachirapornpuk S, “Service quality in internet banking: The importance of customer role, 2002.
- Chong Soo Pyun, Les Scruggs, Kiseok Nam, “Internet banking in the U.S., Japan and Europe, 2002.
- Strauss, Judie and Frost, Raymond, “E-marketing”, Prentice Hall, 2001.
- Cutts Geoff (1991): *Μεθοδολογία Δομημένης Ανάλυσης και Σχεδιασμού*, Alfred Waller Ltd. Publishers.
- Firesmith Donald (1993): *Object-Oriented requirement analysis and logical design*, John Wiley and Sons.
- Holt John (2001): *UML for systems engineering,* The Institution of Electrical Engineers.
- Pender Tom (2003): *UML BIBLE*, Wiley Publishing.
- Rumbange et al (1999): *The Unified Modelling Language Reference manual*, Addison-Wesley.
- Somerville Ian (2001): *Software Engineering*, Addison-Wesley Publishers Limited.

Ιστοσελίδες -Πηγές

- http://www.nbg.gr
- http://www.eurobank.gr
- http://www.alpha.gr
- http://www.piraeusbank.gr/
- http://www.millenniumbank.gr
- http://www.ttbank.gr/
- http://wikipedia.org
- www.icsd.aegean.gr/lecturers/gkorm/notes.doc
- http://www.tex.unipi...s_comp/kef6.pdf
- http://estia.hua.gr:...ou_Euthalia.pdf
- http://www2.aegean.g...lides/CN_08.pdf
- http://en.wikipedia.org/wiki/Timestamp
- http://www.tex.unipi...s_comp/kef7.pdf
- www.sepe.gr
- www.bankofgreece.gr