ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΩΝ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΔΙΚΤΥΑΚΕΣ ΤΡΑΠΕΖΕΣ ΠΑΡΕΧΟΜΕΝΕΣ ΥΠΗΡΕΣΙΕΣ ΚΑΙ ΑΣΦΑΛΕΙΑ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΣΠΟΥΔΑΣΤΡΙΩΝ: ΑΣΗΜΑΚΟΠΟΥΛΟΥ ΝΑΤΑΛΙΑ
ΖΑΧΑΡΗ ΣΤΑΥΡΟΥΛΑ

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ ΟΡΦΑΝΟΣ ΓΕΩΡΓΙΟΣ
ΠΑΤΡΑ 2012

ΠΕΡΙΕΧΟΜΕΝΑ

1.ΕΙΣΑΓΩΓΗ-ΑΝΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΑΣ

1.1 Εισαγωγή

Είναι πλέον φανερό ότι η τεχνολογία μετασχηματίζει τον τραπεζικό κλάδο. Σήμερα η ηλεκτρονική τραπεζική υπόσχεται την επανάσταση στις συναλλαγές μας με τις τράπεζες καθώς μεταφέρει την τράπεζα στην οθόνη του υπολογιστή μας μειώνοντας έτσι δραστικά το κόστος τόσο για τους πελάτες όσο και για την ίδια την τράπεζα καταργώντας αποστάσεις και χρονικούς περιορισμούς προσφέροντας στην πελατεία της την ευχέρεια διεκπεραίωσης μιας γκάμας τραπεζικών συναλλαγών όπως τη δυνατότητα ενημέρωσης για τα υπόλοιπα λογαριασμών και πιστωτικών καρτών, για την κατάσταση των άυλων τίτλων, των προθεσμιακών καταθέσεων και των χρηματιστηριακών εντολών. Επίσης προσφέρει τη δυνατότητα διαχείρισης που περιλαμβάνει μεταφορά ποσού από λογαριασμό ιδίου σε λογαριασμό ιδίου ή τρίτου, πληρωμές δημοσίου και ταμείων, άμεση εξόφληση λογαριασμών και άλλες υπηρεσίες όπως αλλαγή προσωπικών δεδομένων, κωδικού πρόσβασης, παραγγελία καρνέ επιταγών, δήλωση απώλειας-κλοπής των πιστωτικών καρτών κ.α. χωρίς πρόσθετο κόστος, με απλά βήματα, γρήγορα και με ασφάλεια.

Ένα πολύ σημαντικό μέρος το οποίο απασχολεί όλους είναι αν και κατά πόσο ασφαλείς είναι οι συναλλαγές μέσω διαδικτύου (Internet). Κάποια από τα μέτρα που λαμβάνονται είναι τα ακόλουθα, ασφαλή αναγνώριση και ταυτοποίηση πελάτη, μέγιστη δυνατή εξασφάλιση απόρρητου μεταφοράς δεδομένων, αυτόματα αποσύνδεση, διενέργεια συνεχών ελέγχων διάγνωσης ασφάλειας και ηλεκτρονικής απάτης, προστασία δεδομένων προσωπικού χαρακτήρα. Οι τράπεζες επενδύουν στην ασφάλεια των ηλεκτρονικών συστημάτων γιατί μέσω αυτών προσφέρονται ανταγωνιστικά πλεονεκτήματα σε αυτές που τα εφαρμόζουν δημιουργώντας με αυτό τον τρόπο ηγέτες στο χώρο της ηλεκτρονικής τραπεζικής.

Ο τραπεζικός κλάδος έχει συνειδητοποιήσει την μεγάλη επίδραση του internet στη λειτουργία και την ανταγωνιστικότητα των τραπεζών και γι’αυτό πλέον η ηλεκτρονική τραπεζική (e-banking) καθίσταται αναγκαίο για κάθε τράπεζα. Αν και τα ποσοστά χρήσης διαδικτύου και ηλεκτρονικής τραπεζικής είναι ακόμα χαμηλά στην Ελλάδα, οι Ελληνικές τράπεζες έχουν επενδύσει αρκετά στα συστήματα ηλεκτρονικής τραπεζικής γιατί παρατηρείται ολοένα αυξανόμενη υιοθέτηση του νέου αυτού μέσου από κρίσιμα πελατειακά κοινά όπως για παράδειγμα οι νέοι, οι ελεύθεροι επαγγελματίες ή οι μικρομεσαίες επιχειρήσεις αλλά και η ώθηση της πολιτείας στη χρήση ηλεκτρονικών δικτύων και τη διενέργεια ηλεκτρονικών συναλλαγών κάνουν την προώθηση της υπηρεσίας της ηλεκτρονικής τραπεζικής επιτακτική.

Στόχος λοιπόν της εργασίας αυτής είναι η όσο το δυνατόν καλύτερη ενημέρωση για τις δυνατότητες και την ευχρηστία των τραπεζικών συναλλαγών μέσω διαδικτύου. Η τεχνολογία εξελίσσεται με πολύ γρήγορους ρυθμούς κ εμείς μπορούμε να την χρησιμοποιήσουμε έτσι ώστε να απλοποιήσουμε όσο γίνεται την καθημερινότητα μας.

1.2 Βασικές έννοιες

Στις μέρες μας οι τράπεζες δεν έχουν και πολλές επιλογές διαφοροποίησης των προϊόντων τους η μια από την άλλη, έτσι στρέφονται σε νέες υπηρεσίες προκειμένου να προσελκύσουν πελάτες αλλά και να μειώσουν τα λειτουργικά τους έξοδα διατηρώντας ή και αυξάνοντας με αυτό τον τρόπο την κερδοφορία τους. Νέα σημεία ανταγωνισμού αποτελούν τα εναλλακτικά δίκτυα, σημαντικότερο αντιπρόσωπο αποτελεί η ηλεκτρονική τραπεζική. Οι τράπεζες στοχεύουν στην δημιουργία ενός συστήματος εύκολο στην χρήση, που να καλύπτει όλες τις ανάγκες των συναλλασσομένων και να είναι απόλυτα ασφαλές, έτσι ώστε με την κατάλληλη ενημέρωση και κατατόπιση οι πελάτες να μπορούν εύκολα να εξοικειωθούν με τη χρήση των συστημάτων ηλεκτρονικής τραπεζικής αλλά και να γνωρίσουν τα πλεονεκτήματα που αυτά τους προσφέρουν.

Το Διαδίκτυο ή Ίντερνετ είναι ένα επικοινωνιακό δίκτυο ηλεκτρονικών υπολογιστών, που επιτρέπει την ανταλλαγή δεδομένων μεταξύ οποιουδήποτε διασυνδεδεμένου υπολογιστή. Επιδρά σημαντικά στις δυνάμεις του ανταγωνισμού και ο τραπεζικός κλάδος αποτελεί χαρακτηριστικό παράδειγμα των επιπτώσεων αυτών. Στη χώρα μας υπηρεσίες ηλεκτρονικής τραπεζικής διαθέτει η πλειοψηφία των εγχώριων τραπεζικών και δημόσιων οργανισμών. Είναι αυτονόητο λοιπόν ότι οι εταιρίες που θα καθυστερήσουν να αξιοποιήσουν τα πλεονεκτήματα του Διαδικτύου θα βρεθούν σε δυσμενέστερη ανταγωνιστική θέση.

Με τον όρο ηλεκτρονική τραπεζική (e-banking) εννοούμε όλες εκείνες τις υπηρεσίες που παρέχουν οι τράπεζες χωρίς τη φυσική παρουσία του πελάτη στο κατάστημα τους. Εναλλακτικά θα μπορούσαμε να ορίσουμε την ηλεκτρονική τραπεζική ως την αυτοματοποιημένη παροχή νέων και παραδοσιακών προϊόντων και υπηρεσιών χρηματοοικονομικής φύσης απευθείας στους πελάτες μέσω ηλεκτρονικών αλληλεπιδραστικών καναλιών επικοινωνίας. Η ηλεκτρονική τραπεζική δίνει τη δυνατότητα σε μια τράπεζα να παγιώσει και να επεκτείνει τη σχέση της με τους πελάτες της καθώς φέρνει τις τραπεζικές υπηρεσίες απ’ ευθείας στο σπίτι ή το γραφείο του πελάτη.

Ένα σημαντικό θέμα που για τις τράπεζες είναι η ασφάλεια των συναλλαγών. Η τράπεζα προκειμένου να εξασφαλίσει από την μία τους πελάτες της που χρησιμοποιούν το e-banking και από την άλλη τον εαυτό της, προσφέρει πολλά μέτρα ασφαλείας όπως αυτόματη φραγή πρόσβασης

στον χρήστη με 4 λανθασμένες προσπάθειες εισαγωγής κωδικού, αριθμός αυθεντικότητας συναλλαγής (TAN), αριθμός επιβεβαίωσης συναλλαγής (CHECK) κ.α. Με αυτόν τον τρόπο προσπαθεί να μειώσει στο ελάχιστο τον κίνδυνο που μπορεί να υπάρχει στις συναλλαγές έτσι ώστε να χρησιμοποιούν όλο και περισσότεροι πελάτες της τράπεζας να πραγματοποιούν τις συναλλαγές τους μέσω ηλεκτρονικής τραπεζικής (e banking).

1.3 Δομή εργασίας

Ο βασικός κορμός της παρούσας πτυχιακής αποτελείται από πέντε κεφάλαια τα οποία χωρίζονται σε επιμέρους ενότητες. Μέσα σε αυτές τις ενότητες παρουσιάζονται οι υπηρεσίες που παρέχουν οι τράπεζες μέσω internet τα οφέλη για εκείνες και τους πελάτες τους, την ασφάλεια που παρέχεται για τις συναλλαγές μέσω internet καθώς και οι τεχνολογίες που χρησιμοποιούνται για αυτόν τον σκοπό. Ακόμη παραθέτονται πληροφορίες για τα προηγμένα συστήματα επεξεργασίας συναλλαγών βασισμένα σε τεχνολογίες ιστού, και τέλος παρουσιάζομαι κάποια διαγράμματα ροής δεδομένων.

Στο πρώτο κεφάλαιο σας παρουσιάζουμε τη δομή της εργασίας καθώς και το αντικείμενο της. Στο κύριο κορμό της εργασίας αρχικά εξετάζεται το e- banking από την σκοπιά των τραπεζών. Καταγράφονται οι υπηρεσίες που παρέχονται από αυτές καθώς και η σημασία που έχει αυτό για τον ανταγωνισμό μεταξύ των τραπεζών. Επίσης παρουσιάζονται τα οφέλη που έχει αυτός ο τρόπος εξυπηρέτησης για τις τράπεζες όπως χαμηλότερο κόστος εξυπηρέτησης και τα οφέλη για τους πελάτες των τραπεζών όπως μείωση του χρόνου αναμονής εξυπηρέτησης και μηδενισμό των αποστάσεων καθώς η πρόσβαση στο e-banking γίνεται μέσω οπουδήποτε υπολογιστή 24 ώρες το 24ωρο (κεφαλαίο 2).

Στην επόμενη ενότητα παρουσιάζονται τα πλεονεκτήματα που απορρέουν από την χρήση των σύγχρονων τεχνολογιών και υπηρεσιών (κυρίως διαδικτυακών) στην καθημερινότητα μας ενώ ακολουθεί και μια εκτεταμένη αναφορά σχετικά με τα πληροφοριακά συστήματα και τις υπηρεσίες διαδικτύου. Εν συνέχει αναφέρονται με αναλύσεις και παραδείγματα οι τρόποι προσβάσεις καθώς και ο τρόπος χρήσης των προσφερομένων υπηρεσιών με τη χρήση ηλεκτρονικών μέσων. Το κεφαλαίο ολοκληρώνεται με τη μελέτη και καταγραφή των πλεονεκτημάτων και των αλλαγών που επιφέρει στον οργανισμό η σύγχρονη τεχνολογία.

Το τέταρτο κεφαλαίο ασχολείται με την ασφάλεια των συναλλαγών αλλά και των δεδομένων που διακινούνται σ αυτές. Αναλύεται η προστασία συναλλαγών και δεδομένων από τους παρόχους των υπηρεσιών ενώ ταυτόχρονα παρουσιάζονται και οι κύριες τεχνολογίες ασφάλειας. Επίσης γίνεται μια εκτεταμένη αναφορά στην ηλεκτρονική τραπεζική - ασφάλεια και κλείνουμε το κεφαλαίο αυτό με τα συστήματα ασφαλών συναλλαγών για οικονομικού τύπου δεδομένα.

Στο πέμπτο κεφαλαίο τώρα δεσπόζουν τα προηγμένα συστήματα επεξεργασίας συναλλαγών τα οποία είναι βασισμένα σε τεχνολογίες ιστού (web-based banking systems) ενώ παρουσιάζονται επίσης κάποια ακολουθιακά διαγράμματα βασικών διαδικασιών καθώς και διαγράμματα ροής δεδομένων. Η εργασία ολοκληρώνεται με τα συμπεράσματα που προκύπτουν από τις παραπάνω αναλύσεις καθώς επίσης και με την παράθεση της βιβλιογραφίας η οποία βοήθησε στη δημιουργία της εργασίας αυτής.

2.ΥΠΗΡΕΣΙΕΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΤΡΑΠΕΖΙΚΗΣ

2.1 Παρεχόμενες υπηρεσίες

2.1.1 ΕΝΗΜΕΡΩΣΗ

Οι τράπεζες μέσω της ηλεκτρονικής τραπεζικής παρέχουν τη δυνατότητα σε κάποιον να ενημερωθεί για τα υπόλοιπα των λογαριασμών που διατηρεί σε κάποιο τραπεζικό κατάστημα ακόμη μπορεί να ενημερώνεται για τις κινήσεις των πιστωτικών καρτών με την είσοδο στην αντίστοιχη υπηρεσία. Επίσης μπορεί να ενημερωθεί αναλυτικά για όλες τις κινήσεις που έχει πραγματοποιήσει κατά την διάρκεια ενός συγκεκριμένου χρονικού διαστήματος.

Δυνατότητα ενημέρωσης παρέχεται και για την κατάσταση των άυλν τίτλων , παρακολούθηση και αποτίμηση των μετοχών με βάση τις τελευταίες συνεδριάσεις του Χρηματιστηρίου Αξιών Αθηνών (Χ.Α.Α.) καθώς και ενημέρωση και παρακολούθηση την πορεία της εκτέλεσης των εντολών της αγοραπωλησίας των μετοχών και τέλος παρέχεται ενημέρωση σχετικά με το χαρτοφυλάκιο αμοιβαίων κεφαλαίων.

2.1.2 ΑΙΤΗΣΕΙΣ

Παρέχεται η δυνατότητα αίτησης έκδοσης μπλοκ επιταγών και συναλλαγματικών αλλά και την ακύρωση τους. Ακόμη ο πελάτης μπορεί να υποβάλλει αίτηση για την συμμετοχή του σε δημόσιες εγγραφές στο Χ.Α.Α. και τέλος μπορεί να υποβληθεί αίτηση για την έκδοση οποιασδήποτε πιστωτικής κάρτας.

2.1.3 ΔΙΑΧΕΙΡΙΣΗ ΛΟΓΑΡΙΑΣΜΩΝ

Μέσω της ηλεκτρονικής τραπεζικής (e-banking) με την υπηρεσία “διαχείριση λογαριασμών” μπορεί ο χρήστης να στείλει εμβάσματα σε άλλες τράπεζες μέσω του Dias transfer,ακόμη παρέχεται η δυνατότητα στον χρήστη (ιδιώτη ή επιχείρηση) να κάνει μεταφορά χρηματικών ποσών σε λογαριασμούς εντός της κάθε τράπεζας αλλά και σε λογαριασμούς άλλων τραπεζών στην Ελλάδα και το εξωτερικό σε ευρώ και σε ξένα νομίσματα.

2.1.4 ΠΛΗΡΩΜΕΣ

Ο χρήστης μπορεί να πραγματοποιήσει τις πληρωμές των δόσεων πιστωτικών καρτών του και λογαριασμούς δημοσίου όπως :

Αν ο χρήστης έχει υποβάλλει την φορολογική δήλωση του μέσω taxis net μπορεί να πληρώνει το φπα μέσω ηλεκτρονικής τραπεζικής. Θα πρέπει βέβαια να υπάρχει επαρκές διαθέσιμο υπόλοιπο στον καταθετικό του λογαριασμό, διαφορετικά δεν δύναται να πραγματοποιηθεί πληρωμή. Σε περίπτωση απόρριψης της πληρωμής από το Υπουργείο Οικονομικών το ποσό που θα επιστραφεί, θα πιστωθεί στο λογαριασμό ο οποίος χρεώθηκε. Η ειδοποίηση γίνεται από το Υπουργείο Οικονομικών.

Άλλες πληρωμές που εκτελούνται μέσω της υπηρεσίας της ηλεκτρονικής τραπεζικής είναι η πληρωμή των εργοδοτικών εισφορών στο ΙΚΑ, η πληρωμή του ΤΕΒΕ και τελών κυκλοφορίας, για την εξόφληση των οποίων απαιτείται επαρκές υπόλοιπο στον καταθετικό λογαριασμό.

Ακόμα γίνονται πληρωμές ασφαλίστρων ζωής, λογαριασμών εταιριών σταθερής, κινητής τηλεφωνίας και internet, παρέχεται επίσης δυνατότητα ακύρωσης πληρωμής.

Τέλος παρέχεται η δυνατότητα εξόφλησης λογαριασμών ΟΤΕ, ΔΕΗ, ΕΥΔΑΠ, ΔΕΚΟ. Είναι σημαντικό σε αυτό το σημείο να αναφέρουμε πως σε όλες τις προαναφερθείσες περιπτώσεις παρέχεται ηλεκτρονικό αποδεικτικό πληρωμής.

Ειδικά για τις επιχειρήσεις παρέχεται η δυνατότητα εντολής για μαζικές πληρωμές προς τρίτους ή μισθοδοσίες και δυνατότητα διαχείρισης του επιπέδου πρόσβασης των χρηστών της εταιρίας σε λογαριασμούς και συναλλαγές.

2.1.5 ΕΙΔΟΠΟΙΗΣΕΙΣ

Παρέχεται η δυνατότητα ειδοποιήσεων (alerts) στον υπολογιστή μέσω ηλεκτρονικού μηνύματος (e-mail) κάθε φορά που οι συναλλαγές πραγματοποιούνται με επιτυχία ή δεν εκτελούνται από την τράπεζα για οποιονδήποτε λόγο. Έτσι ο χρήστης μπορεί να είναι σίγουρος για το αν οι συναλλαγές του πραγματοποιήθηκαν με επιτυχία ή όχι.

2.1.6 ΕΠΙΠΡΟΣΘΕΤΕΣ ΠΑΡΟΧΕΣ

Εκτός από τις παροχές που αναφέραμε πιο πάνω, η ηλεκτρονική τραπεζική προσφέρει την δυνατότητα στους χρήστες της να ορίσουν , να μεταβάλλουν ή να ακυρώσουν πάγιες εντολές όπως για παράδειγμα πληρωμή λογαριασμού της ΔΕΗ αυτόματα μέσω λογαριασμού τραπέζης. Να δηλώσουν απώλεια ή κλοπή κάρτας χωρίς να χάνεται χρόνος και να υπάρχει ο κίνδυνος κάποιος να κάνει χρήση αυτής. Και τέλος μπορούν να αλλάξουν τα προσωπικά τους στοιχειά όπως διεύθυνση κατοικίας, αριθμό τηλεφώνου κ.α.

Παράλληλα πρέπει να τονίσουμε ότι δίνεται η δυνατότητα αποθήκευσης των κινήσεων των λογαριασμών σε ηλεκτρονικό αρχείο για περαιτέρω λογιστική τους επεξεργασία.

2.1.7 ΛΟΙΠΕΣ ΥΠΗΡΕΣΙΕΣ ΠΟΥ ΠΡΟΣΦΕΡΟΝΤΑΙ ΑΝΑ ΤΡΑΠΕΖΑ

Εκτός από τις παραπάνω υπηρεσίες παρέχονται και άλλες που συχνά διαφέρουν από τράπεζα σε τράπεζα :

- ALPHA BANK

Η Τράπεζα προσφέρει την δυνατότητα στους χρήστες των υπηρεσιών της ηλεκτρονικής τραπεζικής να ειδοποιούνται μέσω γραπτού μηνύματος στο κινητό τους τηλέφωνο για εντολές που δεν εκτελέστηκαν, μπορούν επίσης να επιλέξουν την γλώσσα που θα χρησιμοποιούν στην ιστοσελίδα της τράπεζας.

Ακόμη, παρέχεται η δυνατότητα για καθορισμό του ημερήσιου ορίου χρηματικών μεταφορών και πληρωμών προς τρίτους, ένταξης λογαριασμών, καρτών, χαρτοφυλακίων στο προφίλ του χρήστη, δυνατότητα ονομασίας λογαριασμών και τέλος ο χρήστης μπορεί να βρει ένα δελτίο τιμών όπου σε αυτό μπορεί να ενημερωθεί για τις συναλλαγματικές ισοτιμίες.

- ΕΓΝΑΤΙΑ ΤΡΑΠΕΖΑ

Παρέχεται η δυνατότητα αυτόματης εξεύρεσης του αριθμού BIC (Bank Identifier Code) εγχώριων και ξένων τραπεζών, η δυνατότητα αποθήκευσης των πληροφοριών σε αρχείο MS Money με δυνατότητα περαιτέρω αξιοποίησης των στοιχείων, ο χρήστης μπορεί επίσης να συμμετάσχει σε δημόσιες εγγραφές και ακόμα να μάθει το υπόλοιπο του λογαριασμού του συγκεκριμένης παρελθούσας ημερομηνίας και τέλος παρέχεται πρόσθετη ασφάλεια στις συναλλαγές με την χρήση κωδικών μιας χρήσης (one time passwords).

Για τις επιχειρήσεις προσφέρονται και κάποιες επιπλέον υπηρεσίες όπως, η δυνατότητα έγκρισης συναλλαγών ανά δεύτερο εταιρικό χρήστη έτσι εξασφαλίζεται μεγαλύτερη προστασία στις συναλλαγές που εκτελούνται, επίσης είναι δυνατόν η κάθε εταιρία να καθορίζει τον διαχειριστή της (Administrator) καθώς και άλλους εκπροσώπους της και τέλος μπορεί να καθορίζει συγκεκριμένες επιλογές μενού ανά εταιρικό χρήστη ανάλογα με την πρόσβαση στις διάφορες υπηρεσίες που θέλει να έχει ο καθένας.

- ΕΜΠΟΡΙΚΗ ΤΡΑΠΕΖΑ

Η Εμπορική τράπεζα παρέχει την δυνατότητα στους πελάτες της να δηλώσουν τις κάρτες τους έκδοσης της στους οργανισμούς VISA και MASTER CARD για ασφαλείς αγορές μέσω διαδικτύου (Υπηρεσία Emporiki Bank Secure), ακόμη ο χρήστης μπορεί να ενημερωθεί για το Διεθνές Εμπόριο μέσω της υπηρεσίας Interrex, μπορεί να παραλάβει κωδικούς πρόσβασης σε ATM, επίσης υπάρχει η δυνατότητα πολυγλωσσικής εκτύπωσης αποδεικτικών συναλλαγής καθώς και αποστολή προσωπικών μηνυμάτων.

Για όσους ασχολούνται με το χρηματιστήριο η Εμπορική τράπεζα τους δίνει την δυνατότητα να πραγματοποιούν αγοραπωλησίες παραγώγων που παρέχεται μέσω της υπηρεσίας Emporiki Investment Bank. Όσον αφορά τις επιχειρήσεις μπορούν να καθορίσουν πολλαπλούς εκπροσώπους της επιχείρησης καθώς και να ορίσουν ημερήσιο όριο στις χρηματικές μεταφορές και συναλλαγές.

- EFG EUROBANK ERGASIAS

Ο χρήστης της ηλεκτρονικής τραπεζικής της Euro bank μπορεί να πραγματοποιεί δωρεές σε κοινωφελείς οργανισμούς, να εκδώσει ψηφιακά πιστοποιητικά για κάθε χρήση της υπηρεσίας, και τέλος του δίνεται η δυνατότητα να εισάγει και να διαχειρίζεται αριθμούς λογαριασμών και πιστωτικών καρτών μέσω προσωπικών ευρετηρίων.

Η Eurobank παρέχει και επιπλέον υπηρεσίες σχετικά με τις χρηματιστηριακές συναλλαγές, όπως να μπορεί ο ενδιαφερόμενος να ενημερώνεται για τους ισολογισμούς και τους αριθμοδείκτες εισηγμένων στο χρηματιστήριο εταιριών, συγκριτικά γραφήματα επενδυτικών προϊόντων, συμμετοχή σε δημόσιες εγγραφές καθώς και τηλεειδοποίηση μέσω γραπτού μηνύματος για μεταβολές μετοχών.

Εικόνα 2: Είσοδος στο E-Banking EFG Eurobank

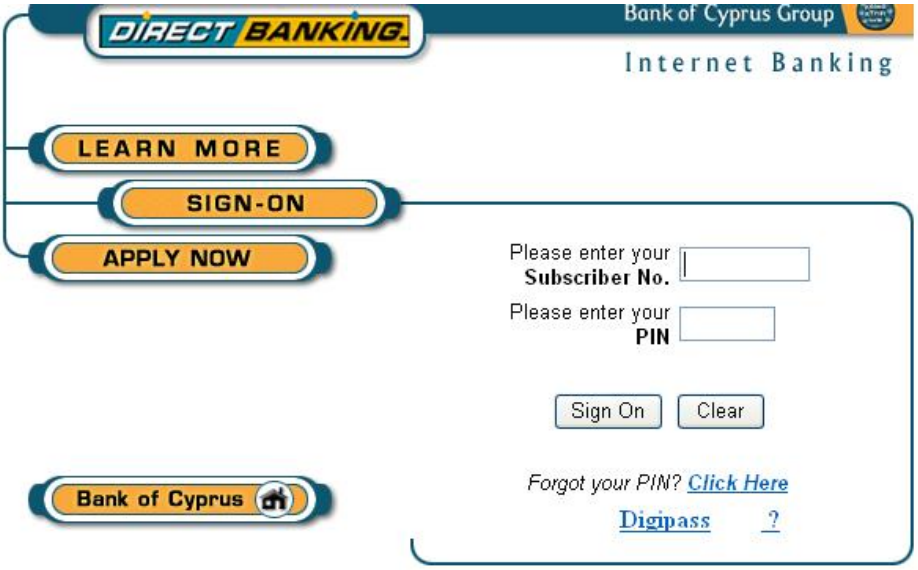
- NOVA BANK

Μέσω της ηλεκτρονικής τραπεζικής παρέχεται η δυνατότητα αίτησης αλλαγής πιστωτικών ορίων καρτών, αλλαγή τρόπου πληρωμής πιστωτικών καρτών, διαχείριση αποδεκτών για πληρωμές και μεταφορές, εμφάνιση και εκτύπωση, μέσω διαδικτύου, μηνιαίου Statement, στο οποίο εμφανίζεται όλη η κίνηση του πελάτη αναφορικά με όλα τα προϊόντα που έχει η τράπεζα και τέλος εμφάνιση της on line δραστηριότητας, δηλαδή κινήσεις του χρήστη στην ηλεκτρονική τραπεζική (internet banking), με ιστορικό 6 μηνών.

- ΤΡΑΠΕΖΑ ΚΥΠΡΟΥ

Ο χρήστης της τράπεζας Κύπρου έχει την δυνατότητα να ανταλλάσει μηνύματα μέσω της ηλεκτρονικής τραπεζικής με την τράπεζα, να του αποστέλλονται οι κινήσεις λογαριασμών μέσω ηλεκτρονικού μηνύματος , φαξ ή ταχυδρομείου, ακόμη ο χρήστης μπορεί να έχει κοινούς κωδικούς για υπηρεσίες διαδικτύου και phone banking και τέλος υπάρχει η δυνατότητα ορισμού προκαθορισμένων δικαιούχων εμβασμάτων.

Σχετικά με την ασφάλεια των συναλλαγών η τράπεζα προσφέρει δυνατότητα supervisor, δηλαδή δυνατότητα εξουσιοδοτημένου χρήστη να παρακολουθεί τις κινήσεις και των υπολοίπων εξουσιοδοτημένων χρηστών μιας συγκεκριμένης εξουσιοδότησης, δυνατότητα χρήστη να ενεργεί, βάσει εξουσιοδότησης, με ένα μοναδικό σετ κωδικών, ακόμη ο χρήστης μπορεί να προμηθευτεί επιπλέον κωδικό ασφαλείας για συναλλαγές άνω συγκεκριμένου ορίου, που ορίζεται από εκάστοτε πελάτη, σε επίπεδο εξουσιοδότησης(ύπαρξη default ορίου τράπεζας) και τέλος παροχή δυνατότητας σε φυσικό ή νομικό πρόσωπο να εξουσιοδοτεί έναν ή περισσότερους χρήστες με εξατομικευμένα στοιχεία πρόσβασης (ως προς προσβάσιμους λογαριασμούς)



Παράδειγμα αρχικής οθόνης εισόδου στο σύστημα

Εικόνα 3: Είσοδος στο e-banking της τράπεζας Κύπρου

- ΤΡΑΠΕΖΑ ΠΕΙΡΑΙΩΣ

Για την καλύτερη εξυπηρέτηση των πελατών της η τράπεζα Πειραιώς παρέχει την δυνατότητα μέσω της ιστοσελίδας της να γίνεται αίτηση για προσωπικό καταναλωτικό δάνειο, πιστωτική κάρτα, μεταφορά υπολοίπου, University Visa, καταθετικό λογαριασμό καθώς και την διαχείριση αιτήσεων, είναι ακόμη δυνατή η πραγματοποίηση προσφορών σε μη κυβερνητικές οργανώσεις με χρέωση τραπεζικού λογαριασμού, επίσης ο χρήστης μπορεί να διαμορφώσει την ιστοσελίδα της τράπεζας σύμφωνα με τις προτιμήσεις του αφού υπάρχει η δυνατότητα εικαστικής παρέμβασης όπως αλλαγή χρώματος, γραμματοσειράς κ.τ.λ.

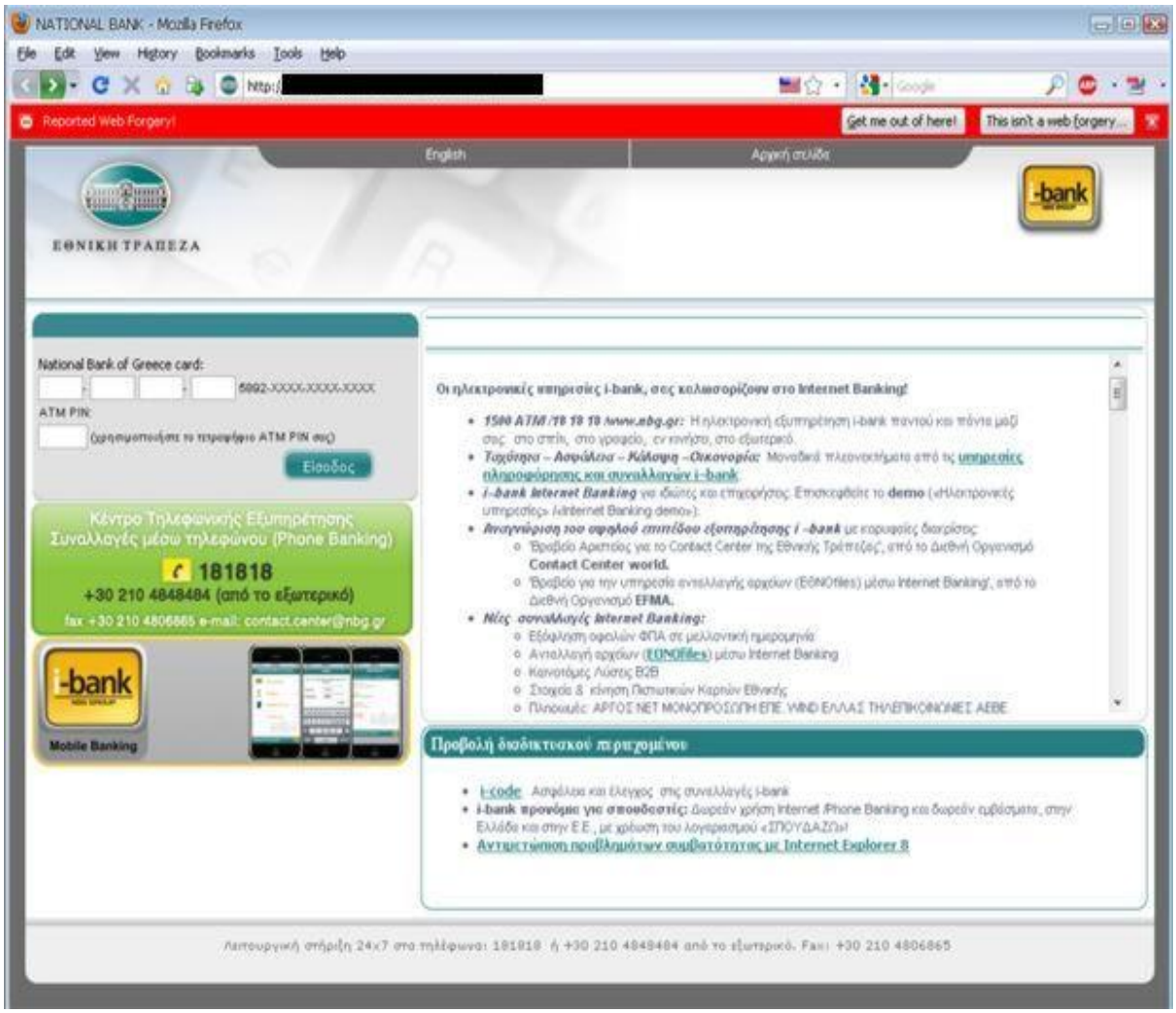
Σχετικά με την ασφάλεια, η τράπεζα δίνει την δυνατότητα καθορισμού διπλών υπογραφών ανά συναλλαγή, επίσης μπορεί να καθορίσει διαφορετικά δικαιώματα συναλλαγών με διαφορετικά όρια μεταξύ των χρηστών και τέλος για την καλύτερη ενημέρωση του πελάτη σχετικά με τις συναλλαγές του υπάρχει η υπηρεσία τηλεειδοποίησης winbank alert για πληρωμές και χρηματικές συναλλαγές μέσω γραπτού μηνύματος, ηλεκτρονικού μηνύματος, ή τηλεφωνήματος από τραπεζικό εκπρόσωπο.

Για εισαγωγείς με υποχρεώσεις στο εξωτερικό η πληρωμή των τιμολογίων μπορεί να γίνει μέσω CLA, μεταφέροντας τις υποχρεώσεις στον ειδικό λογαριασμό Collection Account.

- ΕΘΝΙΚΗ ΤΡΑΠΕΖΑ

Η Εθνική τράπεζα με σκοπό την καλύτερη εξυπηρέτηση των πελατών της προσφέρει την δυνατότητα αποθήκευσης των συναλλαγών σε αρχείο CMV ώστε να υπάρχει η δυνατότητα περαιτέρω αξιοποίησης των στοιχείων, δημιουργία διαχείριση και αποτίμηση εικονικών χαρτοφυλακίων, ημερολόγιο χρήστη για τις συναλλαγές που έχουν εκτελεστεί μέχρι 3 μήνες πριν καθώς και παραγγελία μπλοκ επιταγών και ιστορικό παραγγελιών.

Σχετικά με την ασφάλεια στον χρήστη του ηλεκτρονικής τραπεζικής της Εθνικής Τράπεζας παρέχεται η δυνατότητα καθορισμού επιπέδων χρηστών νομικών προσώπων και διαφορετικών δικαιωμάτων πρόσβασης καθώς επίσης είναι δυνατή η αλλαγή/ δέσμευση κωδικών ασφαλείας (password).



Εικόνα 1: Είσοδος στο E-banking Εθνικής Τράπεζας

2.2 Οφέλη για τον πελάτη

2.2.1 Για τον ιδιώτη-πελάτη

Με την χρήση της ηλεκτρονικής τραπεζικής, ο πελάτης έχει τη δυνατότητα 24 ώρες το 24ωρο και 7 μέρες την εβδομάδα. Συνεπώς ο πελάτης μπορεί να εξυπηρετηθεί οποιαδήποτε στιγμή αυτός το απαιτεί. Αν αναλογιστεί κανείς τον παραδοσιακό τρόπο εξυπηρέτησης που προϋποθέτει τη φυσική παρουσία του συναλλασσόμενου στο γκισέ της τράπεζας, ο πελάτης έχει στη διάθεση του 6,5 ώρες την ημέρα και μόνο 5 εργάσιμες μέρες την εβδομάδα. Ακόμη, μπορούν να ταξιδεύουν ελεύθερα χωρίς να ανησυχούν για το εάν θα έχουν πρόσβαση στο λογαριασμό τους. Άρα μπορούν εύκολα να διακριθούν τα οφέλη της συνεχούς εξυπηρέτησης.

Επιπλέον υπάρχει μεγάλη εξοικονόμηση χρόνου. Ο χρήστης της ηλεκτρονικής τραπεζικής κερδίζει χρόνο αφού δεν είναι απαραίτητο να φύγει από την οικία του ή την εργασία του για να μεταβεί σε κάποιο από τα καταστήματα της τράπεζας και να περιμένει σε ουρές προκειμένου να εκτελέσει την συναλλαγή που θέλει. Επίσης, με το διαδίκτυο έχουν όλοι ίσες ευκαιρίες εξυπηρέτησης και διευκόλυνσης είτε βρίσκονται δίπλα στο κεντρικό κατάστημα είτε στο πιο απομακρυσμένο χωριό.

Μια ακόμη σημαντική διάσταση είναι ότι μέσω διαδικτύου ο πελάτης με τη χρήση Η/Υ έχει πρόσβαση σε όλες τις τράπεζες αφού η μια τράπεζα από την άλλη απέχει μόνο ένα κλικ του ποντικιού. Οι τράπεζες φροντίζουν η ιστοσελίδα τους να είναι ευχάριστη, ελκυστική, φιλική προς τον επισκέπτη και με ευκολία στη χρήση της. Με την πολυπλοκότητα των σημερινών χρηματοοικονομικών υπηρεσιών και την εξειδίκευση είναι μάλλον απίθανο ο υπάλληλος μιας τράπεζας να απαντήσει σε όλα τα ερωτήματα των πελατών. Ο χρήστης όμως της ηλεκτρονικής τραπεζικής έχει έγκυρη και πληρέστερη πληροφόρηση, αφού οι τράπεζες είναι ιδιαίτερα αναλυτικές και προσεχτικές σε όσα δημοσιεύουν στην ιστοσελίδα τους. Ο πελάτης αφού ενημερωθεί μέσω διαδικτύου για τις υπηρεσίες που επιθυμεί, συγκρίνει τα τραπεζικά προϊόντα που προσφέρει και κυρίως την τιμολόγηση τους και επιλέγει την τράπεζα που προσφέρει τους ευνοϊκότερους όρους. Φυσικά η ανάγκη της προσωπικής εξυπηρέτησης παραμένει, ιδιαίτερα σε σύνθετα τραπεζικά προϊόντα αλλά πριν φτάσει ο χρήστης της ηλεκτρονικής τραπεζικής στην τράπεζα γνωρίζει τους όρους που προσφέρουν κ οι άλλες τράπεζες. Η επαφή με τον υπάλληλο πολλές φορές έχει συμβουλευτικό χαρακτήρα.

Με την χρήση της ηλεκτρονικής τραπεζικής είναι μικρότερο το κόστος συναλλαγών: όλο το εύρος των τραπεζικών εργασιών παρέχεται με μικρότερο κόστος στον πελάτη της ηλεκτρονικής τραπεζικής. Ακόμη, πολλές συναλλαγές παρέχονται εντελώς δωρεάν. Παράλληλα όμως οι συναλλαγές γίνονται πιο εύκολα και για τα άτομα με ειδικές ανάγκες: αρκετοί συνάνθρωποι μας με κινητικά κυρίως προβλήματα μπορούν να

συναλλάσσονται εύκολα και γρήγορα με την τράπεζα τους χωρίς να χρειάζεται η δύσκολη για αυτούς μετακίνηση στο κατάστημα της τράπεζας.

Τέλος, μέσω της ηλεκτρονικής τραπεζικής ο πελάτης έρχεται σε επαφή με νέες τεχνολογίες: η διενέργεια συναλλαγών μέσω της ηλεκτρονικής τραπεζικής φέρνει αντιμέτωπο τον πελάτη της τράπεζας με νέες τεχνολογίες. Πελάτες που δεν είχαν διανοηθεί ποτέ να χρησιμοποιήσουν υπολογιστή ή κινητό και πόσο μάλλον για πρόσβαση στο διαδίκτυο αρχίζουν δειλά δειλά να επωφελούνται των πλεονεκτημάτων της ηλεκτρονικής τραπεζικής γνωρίζοντας ταυτόχρονα και νέες τεχνολογίες.

Συμπερασματικά, η ηλεκτρονική τραπεζική δίνει την δυνατότητα σε μια τράπεζα να παγιώσει και να επεκτείνει τη σχέση της με τους πελάτες της καθώς φέρνει της τραπεζικές υπηρεσίες απ' ευθείας στο σπίτι ή το γραφείο του πελάτη. Όσο περισσότερες υπηρεσίες αποδέχεται ένας πελάτης, τόσο μεγαλύτερη είναι η πιθανότητα να παραμείνει ο πελάτης πιστός στην τράπεζα. Η ανάπτυξη δικτυακών υπηρεσιών είναι επιβεβλημένη για της τράπεζες σήμερα οι οποίες πρέπει να ανταγωνιστούν προϊόντα και υπηρεσίες άλλον τραπεζών, χρηματοοικονομικών ιδρυμάτων και ασφαλιστικών εταιριών.

2.2.2 Για την εταιρία-πελάτη

Πέραν των πλεονεκτημάτων που προαναφέρθηκαν, υπάρχουν και επιπρόσθετα πλεονεκτήματα για τις επιχειρήσεις που χρησιμοποιούν την ηλεκτρονική τραπεζική. Καταρχήν, παρέχονται ολοκληρωμένα πακέτα υπηρεσιών πληρωμών για επιχειρήσεις: μια εταιρία έχει ένα ολοκληρωμένο περιβάλλον πληρωμών τόσο των οφειλών της στο Δημόσιο όσο και των οφειλών της σε ΔΕΚΟ και οργανισμούς. Καθίσταται πια εύκολη η ενημέρωση των μηχανογραφικών συστημάτων της εταιρίας, μέσω της ευκολίας του downloading που προσφέρουν οι τράπεζες μέσω της ηλεκτρονικής τραπεζικής οι επιχειρήσεις μπορούν εύκολα και άμεσα να ενημερώνουν τα μηχανογραφικά και λογιστικά τους συστήματα με τις κινήσεις των λογαριασμών της εταιρίας.

Μια εταιρία μπορεί να χρησιμοποιεί το σύστημα ηλεκτρονικής τραπεζικής για την εκτέλεση της μισθοδοσίας προσωπικού ή μαζικών πληρωμών προμηθευτών, η επιχείρηση έχει τη δυνατότητα με πολύ συνοπτική διαδικασία να εκτελεί τη μισθοδοσία του προσωπικού της ή να πληρώνει τους προμηθευτές της και να παρακολουθεί σε σύνδεση με το διαδίκτυο την κατάσταση των πληρωμών της. Μπορεί παράλληλα να καθορίσει διαφορετικά δικαιώματα χρήσης και πρόσβασης, η εταιρία μπορεί να επιλέξει ποιοι υπάλληλοι της θα χρησιμοποιούν ηλεκτρονικές τραπεζικές υπηρεσίες και τι δικαιώματα θα έχουν τόσο σε επίπεδο πρόσβασης σε λογαριασμούς και κάρτες όσο και σε επίπεδο τέλεσης λογαριασμών.

Μέσω της ηλεκτρονικής τραπεζικής δίνεται η δυνατότητα στις επιχειρήσεις να ελαχιστοποιήσουν το χρόνο που απαιτείται για να εκτελέσουν τις τραπεζικές τους συναλλαγές και να τον αφιερώσουν στους

πελάτες τους με αποτέλεσμα οι πελάτες να εξυπηρετούνται καλύτερα και να μένουν ικανοποιημένοι.

Γενικότερα με την ηλεκτρονική τραπεζική δημιουργείται ένα εναλλακτικό δίκτυο εξόφλησης λογαριασμών, πολλές εταιρίες μπορούν να εκμεταλλευτούν την ηλεκτρονική τραπεζική ως ένα επιπλέον δίκτυο είσπραξης των υποχρεώσεων των πελατών της. Ήδη αρκετές εταιρίες όπως η TELLAS χρησιμοποιούν πλέον το διατραπεζικό σύστημα DIASDEBIT σε συνεργασία με τράπεζες του εσωτερικού για την εξόφληση των λογαριασμών του. Παράλληλα υπάρχει δημιουργία ενός εναλλακτικού δικτύου πώλησης προϊόντων και υπηρεσιών , με συνεργασίες στο χώρο του ηλεκτρονικού εμπορίου και των ηλεκτρονικών πληρωμών οι εταιρείες προσφέρουν σε όλους του πελάτες τους έναν εναλλακτικό, ασφαλή και εξ αποστάσεως τρόπο αγορών και πληρωμής των οφειλών τους.

Βέβαια παρά τα μεγάλα πλεονεκτήματα που έχει η ηλεκτρονική τραπεζική δεν έχει και την αντίστοιχη αποδοχή από τις επιχειρήσεις. Ο βασικότερος λόγος είναι ότι πολλοί θεωρούν την ασφάλεια που προσφέρει αρκετά περιορισμένη.

Συμπερασματικά , θα λέγαμε ότι με τη χρήση της ηλεκτρονικής τραπεζικής η επιχείρηση , από τη μια πλευρά , εξυπηρετείται ταχύτερα , μπορεί να προγραμματίζει και να υλοποιεί καλύτερα και αμεσότερα μέσα στο οικείο της περιβάλλον και στο χρόνο που επιθυμεί τις συναλλαγές της ,είναι ασφαλής και τελικά οργανώνεται καλύτερα , μειώνοντας ταυτόχρονα το κόστος της και ελευθερώνοντας χρόνο και ανθρώπους για περισσότερο παραγωγικές δραστηριότητες.

2.3 Οφέλη για τις τράπεζες

Από την πλευρά τους οι τράπεζες το τελευταίο διάστημα επενδύουν σημαντικά ποσά στα "εναλλακτικά δίκτυα" προκειμένου να αναβαθμίσουν τις υπηρεσίες τους γιατί μέσω αυτών οι τράπεζες έχουν τη δυνατότητα να επεκτείνουν τα δίκτυα εξυπηρέτησης της πελατείας τους. Η ηλεκτρονική τραπεζική δίνει την δυνατότητα στις τράπεζες να εξυπηρετούν τους πελάτες τους και να διεκπεραιώνουν τις συναλλαγές τους μέσω νέων τρόπων που δεν υπήρχαν πριν μερικά χρόνια όπως το διαδίκτυο.

Οι τράπεζες πλέον προσφέρουν καινοτομικές υπηρεσίες γιατί η ηλεκτρονική τραπεζική δίνει το πλεονέκτημα στις τράπεζες να εκμεταλλευτούν τα προνόμια που προσφέρει η τεχνολογία και να δημιουργήσουν καινοτομικές και πρωτοποριακές υπηρεσίες οι οποίες σε διαφορετική περίπτωση δε θα μπορούσαν να πραγματοποιηθούν. Παράλληλα όμως αυξάνει και την αποδοτικότητα τους, οι τράπεζες οι οποίες αντιμετωπίζουν με επιτυχία τις τεχνολογικές προκλήσεις που παρουσιάζονται, θα έχουν νέες ευκαιρίες να επεκτείνουν την θέση τους στην αγορά. Η ψηφιοποίηση μειώνει το κόστος και αυξάνει την αποτελεσματικότητα, αν και αρχικά χρειάζονται εκτεταμένες επενδύσεις σε πληροφορική τεχνολογία.

Ένα ακόμη σημαντικό στοιχείο είναι ότι οι τράπεζες μπορούν να αποκτήσουν νέους πελάτες μέσω της παρουσίας τους στο διαδίκτυο. Πολλοί είναι εκείνοι που θα μπουν στον πειρασμό να δοκιμάσουν ένα προϊόν μιας τράπεζας όταν αυτό μπορεί να γίνει με ένα κλικ από το σπίτι ή το γραφείο τους. Οι περισσότεροι χρήστες του διαδικτύου είναι άτομα με υψηλό μορφωτικό και βιοτικό επίπεδο, άτομα δηλαδή που οι τράπεζες θέλουν για πελάτες τους καθώς κατανοούν καλύτερα τις νέες μορφές συναλλαγών αλλά και τα νέα προϊόντα. Από την άλλη όμως έχουν μεγαλύτερες απαιτήσεις. Επιπλέον, η παροχή σε απευθείας σύνδεση (on line) υπηρεσιών δεν περιορίζει γεωγραφικά την τράπεζα. Με τον τρόπο αυτό υπάρχει η δυνατότητα να προσελκύσει απομακρυσμένους πελάτες και να διευρύνει την πελατειακή της βάση. Υποψήφιοι πελάτες πλέον των τραπεζών δεν είναι όσοι μένουν κοντά σε κάποιο νέο υποκατάστημα αλλά ολόκληρος ο κόσμος. Αυτό έχει σαν αποτέλεσμα να δημιουργούνται οικονομίες κλίμακας καθώς όσο αυξάνονται οι χρήστες της ηλεκτρονικής τραπεζικής, τόσο μειώνεται το κόστος ανά συναλλαγή καθώς η υποδομή είναι η ίδια για όλους τους χρήστες.

Με την ηλεκτρονική τραπεζική οι χρηματοπιστωτικοί οργανισμοί επιτυγχάνουν την προβολή τόσο της τράπεζας όσο και των θυγατρικών τους εταιριών, όπου και παραπέμπουν τον χρήστη. Είναι δηλαδή μια διαρκής διαφήμιση των παρεχόμενων τραπεζικών προϊόντων και παρουσίαση στο κοινό νέων καινοτόμων υπηρεσιών. Οι πελάτες ενημερώνονται από τις ιστοσελίδες για τα θέματα που τους ενδιαφέρουν, στη συνέχεια κατεβάζουν και συμπληρώνουν τις σχετικές αιτήσεις και κατόπιν τις προωθούν σε ηλεκτρονική μορφή μέσω ηλεκτρονικού μηνύματος (e-mail) στο αρμόδιο τμήμα της τράπεζας. Συνεπώς, με αυτόν τον τρόπο μειώνουν το λειτουργικό κόστος τους με την μείωση της δαπάνης για διαφημιστικό και άλλο έντυπο υλικό.

Παράλληλα, μέσω της ηλεκτρονικής τραπεζικής και της αυτοματοποίησης των τραπεζικών εργασιών, οι τράπεζες προσφέρουν υπηρεσίες που αυξάνουν την ποιότητα εξυπηρέτησης των πελατών τους. Αυτό συντελεί σε προσέλκυση νέας πελατείας και διατήρηση της ήδη υπάρχουσας μέσω της παροχής ποιοτικά αναβαθμισμένων υπηρεσιών και ταχύτατης εξυπηρέτησης.

Συμπερασματικά, μπορούμε να πούμε ότι η ηλεκτρονική τραπεζική έχει εντείνει τον ανταγωνισμό των τραπεζών και μάλιστα παρά το αρχικό υψηλό κόστος που απαιτεί ένα σύστημα ηλεκτρονικής τραπεζικής για να εγκατασταθεί, κατορθώνουν με την υιοθέτηση του να μειώσουν το λειτουργικό τους κόστος και να παραμείνουν ανταγωνιστικές προσελκύοντας παράλληλα και νέους πελάτες. Μεγάλη προσοχή πρέπει να δοθεί στα θέματα ασφαλείας καθώς ένα ευάλωτο σε επιθέσεις σύστημα μπορεί να αποβεί καταστροφικό τόσο για τους πελάτες όσο και για τις τράπεζες.

ΣΤΟ ΚΕΦΑΛΑΙΟ 2 ΧΡΗΣΙΜΟΠΟΙΗΘΗΚΑΝ ΟΙ ΠΗΓΕΣ 1,2,3,4,5,6,7 ΑΠΟ ΤΙΣ ΔΙΑΔΙΚΤΥΑΚΕΣ ΠΗΓΕΣ.

3.ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΙ ΥΠΗΡΕΣΙΕΣ

3.1 Πλεονεκτήματα από την χρήση σύγχρονων τεχνολογιών και υπηρεσιών.

Η πλειονότητα των ανθρώπων, μέχρι τα μέσα του 19ου αιώνα, διέθετε πάρα πολύ χρόνο για την καλλιέργεια και συλλογή των καρπών. Οι γεωργικές δραστηριότητες ήταν ένας τρόπος ζωής.

Η βιομηχανική επανάσταση στα μέσα του 19ου αιώνα επέφερε σημαντικές αλλαγές. Για πρώτη φορά στην ιστορία άρχισαν να δουλεύουν στις βιομηχανίες περισσότεροι άνθρωποι από ότι στους αγρούς. Η εποχή της βιομηχανίας είχε αρχίσει.

Σήμερα ζούμε στην εποχή της πληροφορίας. Καθώς τα εργοστάσια γίνονται περισσότερο αυτοματοποιημένα, εργάζονται λιγότεροι άνθρωποι για την παραγωγή αγαθών. Η ίδια χρονική περίοδος χαρακτηρίζεται από την έκρηξη της πληροφορίας. Συνώνυμο της πληροφορίας είναι ο όρος δεδομένα (data). Νέα συστήματα επικοινωνίας μας επιτρέπουν να αξιοποιούμε τα δεδομένα (πληροφορίες) με σχετική ευκολία. Για το λόγο αυτό πολλοί άνθρωποι αναφέρονται στην εποχή μας χαρακτηρίζοντάς την ως εποχή της πληροφορίας.

Ο ηλεκτρονικός υπολογιστής έχει εισχωρήσει σε όλους τους τομείς της επιστήμης και κάθε άλλης παραγωγικής δραστηριότητας συμβάλλοντας έτσι, με έμμεσο και άμεσο τρόπο, στην ίδια τη ραγδαία εξέλιξή τους. Είναι προφανές πως οι κοινωνικές επιπτώσεις από τη νέα αυτή παραγωγική δύναμη είναι σημαντικές, σύνθετες και, ως ένα σημείο, απρόβλεπτες. Επηρεάζουν άμεσα την ποιότητα της ζωής μας, ακόμη και τη διαμόρφωση του χαρακτήρα μας και τις κοινωνικές μας σχέσεις. Είναι ένα πεδίο όπου χάνονται και κερδίζονται οικονομικοί και πολιτικοί πόλεμοι, όμως και ένα μέσο που ανοίγει νέους ορίζοντες επικοινωνίας.

Η τεχνολογική έκρηξη λοιπόν των ηλεκτρονικών υπολογιστών και των δυνατοτήτων που προσφέρουν έχει ως άμεσο αποτέλεσμα στον άνθρωπο τη χρήση σύγχρονων τεχνολογιών και υπηρεσιών κυρίως μέσω του διαδικτύου (internet).Με τον όρο σύγχρονες τεχνολογίες και υπηρεσίες δηλώνουμε τη δυνατότητα που μας προσφέρει πλέον η τεχνολογική εξέλιξη κυρίως μέσω διαδικτυακών υπηρεσιών να διευκολύνουμε την καθημερινότητα μας κάνοντας διάφορες διεργασίες μέσω του ηλεκτρονικού μας υπολογιστή οι οποίες ειδάλλως μπορεί να ήταν ιδιαίτερα κουραστικές και χρονοβόρες.

Η εκμάθηση χρήσης διαδικτυακών (ηλεκτρονικών) υπηρεσιών αρχίζει να μοιάζει πλέον επιτακτική ανάγκη για των άνθρωπο. Κρατικές και δημοτικές πλέον αρχές προσφέρουν μια μεγάλη γκάμα υπηρεσιών μέσω διαδικτύου. Στο χορό αυτό έχουν μπει πλέον οι τράπεζες μέσω συστημάτων ηλεκτρονικής τραπεζικής αλλά και ένα πλήθος εταιριών (εμπορικών και τεχνικών) οι οποίες προσφέρουν διάφορες πρόσφορες με τη χρήση ηλεκτρονικών υπηρεσιών.

Είναι πλέον πασιφανές ότι υπάρχουν πολλά πλεονεκτήματα που πηγάζουν από τις σύγχρονες τεχνολογίες και υπηρεσίες. Εν συνέχει θα παρουσιάσουμε και θα σας αναλύσουμε κάποια από αυτά.

Η χρήση σύγχρονων τεχνολογιών και υπηρεσιών στις δημόσιες υπηρεσίες αλλά και στις τράπεζες διευκολύνει την καθημερινότητα μας διότι μας εξοικονομεί χρόνο αλλά και σωματική ενέργεια .Επίσης υπάρχει ελευθέρια χρόνου στις συναλλαγές διότι οι υπηρεσίες προσφέρονται 24 ώρες χωρίς λοιπόν να υπάρχει ψυχολογική πίεση. Ο χρόνος που κερδίζεται μέσω των ηλεκτρονικών υπηρεσιών μπορεί να χρησιμοποιηθεί δημιουργικά από το κάθε άνθρωπο προσφέροντας έτσι διάφορα οφέλη.

Οι σύγχρονες τεχνολογίες και υπηρεσίες (msn , Skype , face book κ.α.) έχουν συμβάλει αποτελεσματικά στην καλύτερη και σαφώς οικονομικότερη επικοινωνία των ανθρώπων. Πλέον με τη χρήση ηλεκτρονικού ταχυδρομείου υπάρχει δυνατότητα ανταλλαγής πληροφοριών και στοιχείων από τη μια άκρη του κόσμου στην άλλη μέσα σε λίγα μόλις λεπτά κάτι που πριν μερικά χρόνια απαιτούσε μέρες ολόκληρες για να υλοποιηθεί. Ακόμη, με τη χρήση διάφορων προγραμμάτων και υπηρεσιών εκατομμύρια άνθρωποι από όλο το κόσμο επικοινωνούν μεταξύ τους καθημερινά ακόμη και μέσω ζωντανής εικόνας χωρίς να χρειάζεται να δαπανήσουν χρήματα. Έτσι υπάρχει η δυνατότητα άνθρωποι από διάφορα σημεία της γης να επικοινωνούν μεταξύ τους εύκολα και οικονομικά ανταλλάζοντας πληροφορίες για το τρόπο ζωής τη κουλτούρα το πολιτισμό και πολλά αλλά.

Ένα άλλο πλεονέκτημα που προκύπτει από τη χρήση σύγχρονων τεχνολογιών και υπηρεσιών αφορά το τομέα της παιδείας καθώς πλέον :

- Κάνουν τη μάθηση πιο ενδιαφέρουσα και διασκεδαστική ,
- Παρουσιάζουν τα γεγονότα και τις πληροφορίες με πολλαπλό τρόπο (κείμενο , ήχος ,εικόνα)
- Τονίζουν τον ενεργητικό ρόλο του μαθητή στη διαδικασία της μάθησης (διαφορές παθητικής και ενεργητικής μάθησης)
- Εξατομικεύουν τη διδασκαλία και παρέχουν την κατάλληλη επανατροφοδότηση σε σύντομο χρονικό διάστημα
- Παρέχουν τον έλεγχο της διαδικασίας είτε στο δάσκαλο, είτε στο μαθητή ή να το κρατούν οι ίδιοι
- Συνδέουν τη μαθησιακή δραστηριότητα με την καθημερινή ζωή (αδρανής γνώση)
- Δημιουργούν ποιοτικότερες συνθήκες συνεργατικής μάθησης (ομαδοκεντρική διδασκαλία)
- Υπογραμμίζουν το διευκολυντικό, παροτρυντικό, συντονιστικό και διαμεσολαβητικό ρόλο του εκπαιδευτικού στη μαθησιακή διαδικασία.

Ένα αναμφισβήτητα τεράστιο πλεονέκτημα της χρήσης σύγχρονων τεχνολογιών και υπηρεσιών έχει να κάνει με το κλάδο της ιατρικής διότι συμβάλουν μέσω διάφορων πειραματικών μοντέλων και ερευνών στην ανακάλυψη νέων φάρμακων και μεθόδων θεραπείας. Ακόμα και εγχειρήσεις μπορούν να πραγματοποιηθούν πιο εύκολα γιατί οι σύγχρονες τεχνολογίες

μπορούν να πετύχουν πράγματα που ο άνθρωπος μόνος δεν θα μπορούσε να κάνει.

Σημαντική είναι η χρήση σύγχρονων τεχνολογιών και στο τομέα της μεταφοράς των ανθρώπων διότι με τη συμβολή τους στη δημιουργία ενός μεταφορικού μέσου επιτυγχάνεται η πιο γρήγορη άνετη και ασφαλέστερη μεταφορά. Οι αποστάσεις δεν παίζουν πλέον τόσο σημαντικό ρόλο και ο άνθρωπος έχει την δυνατότητα να ταξιδέψει παντού.

Τέλος σημαντική είναι η βοήθειά τους και στο κατασκευαστικό τομέα διότι βοηθούν στο σχεδιασμό κτιριακών εγκαταστάσεων με τη χρήση σύγχρονων προγραμμάτων και τεχνολογιών ενώ αξίζει να αναφέρουμε πως συμβάλουν αποτελεσματικά στη βέλτιστη της μηχανικής αντοχής των κτιρίων μέσω διάφορων πειραματικών μοντέλων που αναπτύσσονται.

3.2 Πληροφοριακά συστήματα, υπηρεσίες διαδικτύου

3.2.1 Πληροφοριακά Συστήματα

Οι αρχές και τα τεχνολογικά πρότυπα που περιγράφονται στην παρούσα ενότητα απευθύνονται σε όλους τους φορείς της Δημόσιας Διοίκησης, οι οποίοι διαθέτουν, αναπτύσσουν ή σχεδιάζουν να αναπτύξουν πληροφοριακά συστήματα με σκοπό να παρέχουν πληροφορίες και υπηρεσίες σε πολίτες, επιχειρήσεις και άλλους φορείς.

Η παρουσίαση των προδιαγραφών διαλειτουργικότητας στοχεύει στην υποστήριξη των φορέων στη σχεδίαση, ανάπτυξη, συντήρηση και υποστήριξη της λειτουργίας των πληροφοριακών τους συστημάτων. Για την επίτευξη αυτού του στόχου, στην ενότητα περιέχονται πολιτικές, πρότυπα και τεχνολογικές κατευθύνσεις οι οποίες καλύπτουν:

- Πληροφοριακά συστήματα φορέων της Δημόσιας Διοίκησης που υποστηρίζουν την παροχή ηλεκτρονικών υπηρεσιών προς πολίτες, επιχειρήσεις και φορείς ή επικοινωνούν και ανταλλάσσουν στοιχεία με πληροφοριακά συστήματα του ίδιου ή άλλου φορέα, τα οποία παρέχουν σχετικές υπηρεσίες.
- Έγγραφα και παραδοτέα μελετών εφαρμογής, ανάλυσης και σχεδιασμού πληροφοριακών συστημάτων της Δημόσιας Διοίκησης.
- Σχήματα δεδομένων και μοντέλα οργάνωσης και περιγραφής ροής εργασίας των Υπηρεσιών προς Πολίτες και Επιχειρήσεις.
- Πληροφοριακά συστήματα επιχειρήσεων, στο βαθμό που απαιτείται διαλειτουργικότητα με τα συστήματα της Δημόσιας Διοίκησης.

Τα πληροφοριακά συστήματα των φορέων της Δημόσιας Διοίκησης που παρέχουν ή συμμετέχουν στην παροχή ηλεκτρονικών υπηρεσιών σε πολίτες, επιχειρήσεις και άλλους φορείς ή οργανισμούς πρέπει να σχεδιάζονται και να υλοποιούνται με τέτοιο τρόπο ώστε να υπακούν στις παρακάτω βασικές αρχές:

Διαφάνεια και εξωστρέφεια: Τα πληροφοριακά συστήματα της Δημόσιας Διοίκησης πρέπει να παρέχουν λεπτομερώς καθορισμένες και τεκμηριωμένες διεπαφές (interfaces), προκειμένου να επιτρέπουν την εύκολη ολοκλήρωση και αξιοποίηση των υπηρεσιών τους από άλλα συστήματα.

Επαναχρησιμοποίηση στοιχείων (Reusability): Η επαναχρησιμοποίηση στοιχείων, δομών, προγραμμάτων και εφαρμογών, τα οποία έχουν σχεδιαστεί/ αναπτυχθεί σύμφωνα με τις απαιτήσεις του Πλαισίου Διαλειτουργικότητας, αποτελεί μία από τις πλέον βασικές απαιτήσεις για την επίτευξη διαλειτουργικότητας μεταξύ συστημάτων της Δημόσιας Διοίκησης.

Προσαρμοστικότητα (Flexibility): Τα πληροφοριακά συστήματα της Δημόσιας Διοίκησης πρέπει να επιτρέπουν τη σχετικά απλή ή με λογικό κόστος προσαρμογή τους σε νέες συνθήκες ή απαιτήσεις λειτουργίας, ιδιαίτερα όσον αφορά τον όγκο των συναλλαγών που εξυπηρετούν, το χρόνο απόκρισής τους και την ασφάλεια που παρέχουν.

Πρότυπα (Standards): Ο σχεδιασμός και η υλοποίηση των πληροφοριακών συστημάτων της Δημόσιας Διοίκησης πρέπει να στηρίζεται σε ευρέως διαδεδομένα πρότυπα, σύμφωνα με το Πλαίσιο Διαλειτουργικότητας.

Κλιμάκωση (Scalability): Δεδομένου ότι οι υπηρεσίες που υποστηρίζονται από ένα πληροφοριακό σύστημα μπορεί να απαιτηθούν από μεγάλο αριθμό άλλων φορέων της Δημόσιας Διοίκησης, τα πληροφοριακά συστήματα της Δημόσιας Διοίκησης πρέπει να παρέχουν επαρκείς δυνατότητες κλιμάκωσης και επέκτασης, π.χ. μέσω προσθήκης αναβάθμισης εξοπλισμού και λογισμικού, έτσι ώστε να μπορούν να εξυπηρετήσουν μεγαλύτερο όγκο αιτημάτων ή φορέων χρηστών.

Απόδοση (Performance) και απόκριση (Response): Ο μικρός χρόνος απόκρισης μιας ηλεκτρονικής υπηρεσίας αποτελεί βασικό παράγοντα για την αποδοχή της από το κοινό στο οποίο απευθύνεται (πολίτες, επιχειρήσεις κλπ.). Έτσι, τα πληροφοριακά συστήματα της Δημόσιας Διοίκησης πρέπει να είναι σε θέση να αποκρίνονται στα αιτήματα των χρηστών σε ελάχιστο χρόνο από την υποβολή των αιτημάτων, ακόμα και αν η ικανοποίηση ενός αιτήματος απαιτεί την επεξεργασία ενός πολύ μεγάλου όγκου δεδομένων.

Φιλικότητα προς το χρήστη (User friendliness): Μία άλλη βασική ιδιότητα που πρέπει να διαθέτουν τα πληροφοριακά συστήματα της Δημόσιας Διοίκησης είναι η φιλικότητα των λειτουργιών τους. Στο πλαίσιο αυτό, χαρακτηριστικά όπως η ύπαρξη απλών και κατανοητών διεπαφών (interfaces), η παροχή σε απευθείας σύνδεση (on line) βοήθειας κλπ. είναι απαραίτητα. Επίσης, τα μηνύματα λάθους που εμφανίζονται στο χρήστη πρέπει να είναι κατανοητά και να διευκρινίζουν κατά πόσο εκτελέστηκε το αίτημά του ή όχι.

Διαθεσιμότητα (Availability): Τα πληροφοριακά συστήματα που παρέχουν ηλεκτρονικές υπηρεσίες πρέπει να είναι συνεχώς διαθέσιμα και να μην παρουσιάζουν προβλήματα στη λειτουργία τους. Το χαρακτηριστικό αυτό αυξάνει το βαθμό αξιοπιστίας των συστημάτων και συνεπώς το βαθμό αποδοχής τους από τους χρήστες.

Ανοχή σφαλμάτων (Fault tolerance): Σε περίπτωση εμφάνισης προβλημάτων στη λειτουργία των πληροφοριακών συστημάτων της Δημόσιας Διοίκησης, πρέπει να διασφαλίζεται αφενός η ταχεία επαναφορά τους σε κατάσταση κανονικής λειτουργίας αφετέρου η ακεραιότητα των δεδομένων τους.

Συντήρηση (Maintenance) και αναβάθμιση (Updating): Τα πληροφοριακά συστήματα της Δημόσιας Διοίκησης πρέπει να σχεδιάζονται και να υλοποιούνται με τέτοιο τρόπο ώστε η λειτουργία, η συντήρηση και η αναβάθμισή τους να μπορεί να ελεγχθεί/εκτελεστεί από φορείς ή στελέχη που δεν συμμετείχαν στην υλοποίησή τους.

Ασφάλεια (Security): Η ασφάλεια αποτελεί ένα κρίσιμο παράγοντα για την αξιοπιστία ενός πληροφοριακού συστήματος. Δεδομένου ότι οι φορείς Δημόσιας Διοίκησης συλλέγουν, επεξεργάζονται και αποθηκεύουν ευαίσθητα προσωπικά δεδομένα του συνόλου των πολιτών και των επιχειρήσεων, είναι αναγκαία η ύπαρξη ή και αναβάθμιση μηχανισμών πιστοποίησης και ταυτοποίησης των χρηστών του πληροφοριακού συστήματος, όπως και η διασφάλιση της ακεραιότητας της διακινούμενης πληροφορίας.

3.2.2 Ορισμός και αρχιτεκτονική μιας υπηρεσίας διαδικτύου

Μια υπηρεσία Διαδικτύου μπορεί να οριστεί ως ένα σύστημα λογισμικού που έχει ως σκοπό να υποστηρίξει τη διαλειτουργική αλληλεπίδραση μηχανών πάνω από ένα δίκτυο. Έχει μια διεπαφή η οποία περιγράφεται σε μία μορφή (συγκεκριμένα τη WSDL), την οποία μπορεί να επεξεργαστεί και μηχανή. Κάποια άλλα συστήματα αλληλεπιδρούν με την υπηρεσία Διαδικτύου με έναν τρόπο που προκαθορίζεται από την περιγραφή της, χρησιμοποιώντας μηνύματα SOAP, που συνήθως μεταβιβάζονται με χρήση του HTTP με καθορισμό αλληλουχίας (serialization) σε XML και σε συνδυασμό με άλλα πρότυπα που σχετίζονται με το Διαδίκτυο.

Οι Υπηρεσίες Διαδικτύου παρέχουν ένα τυποποιημένο τρόπο επικοινωνίας μεταξύ διαφορετικών εφαρμογών λογισμικού. Οι εφαρμογές αυτές λογισμικού μπορεί να τρέχουν σε μία ποικιλία από πλατφόρμες ή/και πλαίσια εργασίας Η αρχιτεκτονική των υπηρεσιών Διαδικτύου (WSA) παρέχει ένα εννοιολογικό πρότυπο και ένα πλαίσιο για την κατανόηση των υπηρεσιών Διαδικτύου και των σχέσεων μεταξύ των συστατικών μερών αυτού του προτύπου.

Οι Υπηρεσίες Διαδικτύου που αναπτύσσονται σήμερα είναι δικτυακοί τόποι γραμμένοι σε HTML. Σε αυτές, οι υπηρεσίες της εφαρμογής (οι μηχανισμοί για έκδοση, διαχείριση, έρευνα και ανάκτηση του περιεχομένου) προσεγγίζονται μέσω της χρήσης τυποποιημένων πρωτοκόλλων και σχημάτων των δεδομένων: HTTP και HTML. Εφαρμογές πελατών (περιηγητές Ιστού) που κατανοούν αυτά τα πρότυπα, μπορούν να αλληλεπιδράσουν με τις υπηρεσίες της εφαρμογής για να εκτελέσουν μία

ποικιλία εργασιών, όπως για παράδειγμα την παραγγελία βιβλίων, την αποστολή καρτών ή την ανάγνωση των ειδήσεων.

Λόγω της αφαίρεσης που παρέχεται από τις διεπαφές που βασίζονται στα πρότυπα που αναφέρθηκαν, δεν παίζει ρόλο εάν οι υπηρεσίες εφαρμογής έχουν αναπτυχθεί σε Java και ο περιηγητής Ιστού σε C++, ή αν οι υπηρεσίες εφαρμογής εκτελούνται σε Unix, ενώ ο περιηγητής Ιστού εκτελείται σε Windows. Οι Υπηρεσίες Διαδικτύου επιτρέπουν τη διαλειτουργικότητα μεταξύ των πλατφορμών με έναν τρόπο που καθιστά την επιλογή πλατφόρμας ανεξάρτητη.

Η διαλειτουργικότητα είναι ένα από τα βασικά οφέλη που αποκομίζονται από την εφαρμογή των Υπηρεσιών Διαδικτύου. Οι λύσεις βασισμένες σε Windows ή σε Java είναι χαρακτηριστικά δύσκολο να ενοποιηθούν, αλλά ένα επίπεδο Υπηρεσιών Διαδικτύου μεταξύ της εφαρμογής και του πελάτη, μπορεί να μειώσει αυτή τη δυσκολία.

Οι Υπηρεσίες Διαδικτύου είναι ένα πλαίσιο (framework) μηνυμάτων. Η μόνη απαίτηση που τίθεται σε μια Υπηρεσία Διαδικτύου είναι ότι πρέπει να είναι ικανή να στέλνει και να λαμβάνει μηνύματα χρησιμοποιώντας κάποιο συνδυασμό τυποποιημένων πρωτοκόλλων Διαδικτύου. Η πιο κοινή μορφή Υπηρεσιών Διαδικτύου είναι η κλήση διαδικασιών που τρέχουν σε έναν κεντρικό εξυπηρετητή, οπότε σ' αυτή την περίπτωση τα μηνύματα κωδικοποιούν κάτι αντίστοιχο με τα ακόλουθα: «κλήση της υπό□ρουτίνας με αυτά τα ορίσματα» και «αυτά είναι τα αποτελέσματα της κλήσης της υπό□ρουτίνας».

Στη συνέχεια περιγράφονται τα τμήματα από τα οποία αποτελείται μια Υπηρεσία Διαδικτύου. Ο κώδικας της εφαρμογής κρύβει την επιχειρηματική λογική και τον τρόπο με τον οποίο υλοποιούνται τα πράγματα (βιβλία λιστών, προσθήκη ενός βιβλίου σε ένα καλάθι αγορών, πληρωμή των βιβλίων, κ.λπ.). Ο ακροατής (Listener) της Υπηρεσίας επικοινωνεί μέσω του πρωτοκόλλου μετάδοσης (HTTP, SOAP, κ.λπ.) και λαμβάνει τις εισερχόμενες αιτήσεις. Η πληρεξούσια (Proxy) Υπηρεσία αποκωδικοποιεί αυτά τα αιτήματα και τα αντικαθιστά με κλήσεις μέσα στον κώδικα εφαρμογής. Η πληρεξούσια Υπηρεσία μπορεί έπειτα να κωδικοποιήσει την απάντηση που θα δώσει ο ακροατής της Υπηρεσίας, αλλά αυτό το βήμα μπορεί και να παραλειφθεί.

Τα τμήματα της πληρεξούσιας Υπηρεσίας και του ακροατή της Υπηρεσίας μπορούν είτε να είναι αυτόνομες εφαρμογές (για παράδειγμα, ένας εξυπηρετητής TCP ή HTTP), είτε μπορούν να τρέξουν μέσα στα πλαίσια κάποιου άλλου τύπου εξυπηρετητή εφαρμογής (application server). Για παράδειγμα, ο εξυπηρετητής εφαρμογής WebSphere της IBM έχει ενσωματωμένη υποστήριξη για τη λήψη ενός μηνύματος SOAP πάνω από HTTP και τη χρησιμοποίησή του για να καλέσει εφαρμογές γραμμένες σε Java που αναπτύσσονται μέσα στο WebSphere. Συγκριτικά, ο δημοφιλής ανοικτού λογισμικού εξυπηρετητής Apache έχει μια μονάδα (module) που υλοποιεί το SOAP. Στην πραγματικότητα, υπάρχουν εφαρμογές SOAP ακόμα και για τα λειτουργικά συστήματα που τρέχουν σε Palm και σε φορητούς ψηφιακούς βοηθούς (PDA).

Πρέπει να λάβουμε υπόψη εντούτοις, ότι οι Υπηρεσίες Διαδικτύου για να τρέξουν δεν απαιτούν ένα περιβάλλον κεντρικού εξυπηρετητή. Οι Υπηρεσίες Διαδικτύου μπορούν να αναπτυχθούν οπουδήποτε μπορούν να χρησιμοποιηθούν οι τυποποιημένες τεχνολογίες Διαδικτύου.

Οι Υπηρεσίες Διαδικτύου δεν απαιτούν οι εφαρμογές να προσαρμόζονται σε ένα παραδοσιακό μοντέλο πελάτη-εξυπηρετητή (client-server) (όπου ο εξυπηρετητής αποθηκεύει τα δεδομένα και κάνει την επεξεργασία) ή το πρότυπο ανάπτυξης πολλών επιπέδων (n-tier) (όπου η αποθήκευση των δεδομένων διαχωρίζεται από την επιχειρηματική λογική που είναι χωρισμένη από τη διεπαφή με τον χρήστη), αν και αναπτύσσονται μέσα σε αυτά τα περιβάλλοντα. Οι Υπηρεσίες Διαδικτύου μπορούν να πάρουν οποιαδήποτε μορφή, μπορούν να χρησιμοποιηθούν οπουδήποτε και μπορούν να εξυπηρετήσουν οποιονδήποτε σκοπό. Για παράδειγμα, υπάρχουν ισχυρές ομοιότητες μεταξύ των συστημάτων ομότιμων μερών (peer to peer) (με αποκεντρωμένα τα δεδομένα ή την επεξεργασία τους) και των Υπηρεσιών Διαδικτύου, όπου τα σχετιζόμενα μέρη (peers) χρησιμοποιούν τυποποιημένα πρωτόκολλα Διαδικτύου για να παρέχουν υπηρεσίες το ένα στο άλλο.

Η αρχιτεκτονική δεν προσπαθεί να διευκρινίσει πώς εφαρμόζονται οι υπηρεσίες Διαδικτύου και δεν επιβάλλει κανέναν περιορισμό στον τρόπο με τον οποίο αυτές μπορούν να συνδυαστούν. Η WSA περιγράφει τόσο τα ελάχιστα χαρακτηριστικά που είναι κοινά για όλες τις υπηρεσίες Διαδικτύου όσο και κάποια χαρακτηριστικά που τα χρειάζονται πολλές, αλλά όχι όλες, οι υπηρεσίες
Διαδικτύου.

Η αρχιτεκτονική Υπηρεσιών Διαδικτύου είναι μια αρχιτεκτονική διαλειτουργικότητας: προσδιορίζει εκείνα τα κοινά στοιχεία του παγκόσμιου δικτύου Υπηρεσιών Διαδικτύου που απαιτούνται προκειμένου να εξασφαλιστεί διαλειτουργικότητα μεταξύ των Υπηρεσιών Διαδικτύου.

Μια υπηρεσία Διαδικτύου είναι μια αφηρημένη έννοια που πρέπει να εφαρμοστεί από έναν συγκεκριμένο πράκτορα. Ο πράκτορας είναι το συγκεκριμένο κομμάτι του λογισμικού ή του υλικού που στέλνει και λαμβάνει τα μηνύματα, ενώ η υπηρεσία είναι ο πόρος που χαρακτηρίζεται από το αφηρημένο σύνολο λειτουργικότητας που παρέχεται. Για να κατανοήσουμε αυτήν την διάκριση, μπορούμε να σκεφτούμε την εφαρμογή μιας συγκεκριμένης υπηρεσίας Διαδικτύου χρησιμοποιώντας έναν πράκτορα τη μια ημέρα (ίσως γραμμένο σε κάποια γλώσσα προγραμματισμού), και έναν διαφορετικό πράκτορα την επόμενη ημέρα (ίσως γραμμένο σε μια διαφορετική γλώσσα προγραμματισμού) με την ίδια λειτουργικότητα. Αν και ο πράκτορας μπορεί να έχει αλλάξει, η υπηρεσία Διαδικτύου παραμένει η ίδια.

Ο σκοπός μιας υπηρεσίας Διαδικτύου είναι να παρέχει κάποια λειτουργικότητα εκ μέρους του ιδιοκτήτη της, που μπορεί να είναι ένα πρόσωπο ή ένας οργανισμός, όπως μια επιχείρηση ή ένα άτομο. Η οντότητα «προμηθευτής» (provider entity) είναι το πρόσωπο ή ο οργανισμός που παρέχει έναν κατάλληλο πράκτορα για να υλοποιήσει μια συγκεκριμένη υπηρεσία, βασικοί ρόλοι της αρχιτεκτονικής των υπηρεσιών Διαδικτύου)

Η οντότητα «αιτών» (requester entity) είναι πρόσωπο ή οργάνωση που επιθυμεί να χρησιμοποιήσει την υπηρεσία Διαδικτύου μιας οντότητας προμηθευτή. Θα χρησιμοποιήσει έναν πράκτορα αιτών για να ανταλλάξει τα μηνύματα με τον πράκτορα προμηθευτή της οντότητας προμηθευτή. Στις περισσότερες περιπτώσεις, ο πράκτορας που κάνει την αίτηση είναι αυτός που θα αρχίσει αυτήν την ανταλλαγή μηνυμάτων, αν και δε συμβαίνει πάντα αυτό. Εν τούτοις, για λόγους συνέπειας θα χρησιμοποιούμε τον όρο πράκτορας αιτών και για τον πράκτορα που αλληλεπιδρά με τον πράκτορα προμηθευτή, ακόμη και σε περιπτώσεις όπου ο πράκτορας προμηθευτής είναι αυτός που αρχίζει την ανταλλαγή.

Για να είναι αυτή η ανταλλαγή μηνυμάτων επιτυχής, η οντότητα αιτών και η οντότητα προμηθευτής πρέπει πρώτα να συμφωνήσουν τόσο σχετικά με τη σημασιολογία όσο και σχετικά με τους μηχανισμούς της ανταλλαγής μηνυμάτων.

3.3 Πρόσβαση στις προσφερόμενες υπηρεσίες με τη χρήση ηλεκτρονικών μέσων.

Η πρόσβαση στις προσφερόμενες υπηρεσίες με τη χρήση ηλεκτρονικών μέσων ποικίλει ανάλογα με το είδος και το τρόπο λειτουργίας κάθε υπηρεσίας. Υπάρχουν δεκάδες τρόποι με τους οποίους ένας χρηστής μπορεί να εισχωρήσει και να κάνει χρήση ηλεκτρονικών υπηρεσιών από τον υπολογιστή του. Είναι αλήθεια λοιπόν ότι η χρήση ηλεκτρονικών υπηρεσιών μας λύνει τα χέρια και εξοικονομεί αρκετό χρόνο από την καθημερινότητα μας. Παρ όλο αυτά για να επιτευχθεί η χρήση των υπηρεσιών πολλές φορές απαιτείται κάποια διαδικασία η οποία μεταβάλλεται ανάλογα με το είδος της ηλεκτρονικής υπηρεσίας. Παρακάτω θα σας παρουσιάσουμε διάφορους τρόπους με τους οποίους μπορεί κάποιος να έχει πρόσβαση ώστε να μπορέσει να κάνει χρήση μιας ηλεκτρονικής υπηρεσίας.

Πολλές φορές ένας χρηστής για να έχει πρόσβαση σε μια ηλεκτρονική υπηρεσία χρειάζεται να αποστείλει ή να υποβάλλει ειδική αίτηση στην αρμοδία υπηρεσία ώστε να μπορέσει με το τρόπο που θα επιλέξει (ηλεκτρονικά – ταχυδρομικά) να αποκτήσει τους προσωπικούς του κωδικούς με τους οποίους θα μπορέσει να έχει πρόσβαση στην αρμοδία υπηρεσία και να κάνει χρήση των δυνατοτήτων που του παρέχει. Μερικές φορές ο χρηστής χρειάζεται να υποβάλλει κάποια συνδρομή ώστε να έχει τη δυνατότητα χρήσης των ηλεκτρονικών υπηρεσιών.

Σε περιπτώσεις όπου η χρήση ηλεκτρονικών υπηρεσιών αφορά συναλλαγές με το κράτος απαιτείται πολλές φορές συνεννόηση με την αρμοδία υπηρεσία ώστε ο χρηστής να αποκτήσει ειδικούς κλειδάριθμους με τους οποίους θα μπορέσει να έχει πρόσβαση στην ηλεκτρονική υπηρεσία και να εξυπηρετηθεί μέσω αυτής. Χαρακτηριστικό παράδειγμα αυτής της

περίπτωσης αποτελεί ο νέος τρόπος υποβολής φορολογικών δηλώσεων βάση του οποίου η υποβολή γίνεται ηλεκτρονικά μέσω του προσωπικού κλειδάριθμου του καθενός ο οποίος δίνεται στο χρηστή μέσω της εφορίας.

Πλήθος κόσμου καθημερινά πραγματοποιεί οικονομικές - εμπορικές συναλλαγές μέσω ηλεκτρονικών υπηρεσιών. Για να γίνεται κάτι τέτοιο με ασφάλεια είναι απαραίτητο να υπάρχουν κάποιες προδιαγραφές οι οποίες έχουν να κάνουν με την ταυτοποίηση των στοιχείων αυτών που εμπλέκονται στη συναλλαγή , την απόδειξη καταβολής πληρωμών αλλά και την ενημέρωση συναλλαγών. Τα βασικά μέσα που έχουν υιοθετηθεί και χρησιμοποιούνται σήμερα σε εμπορικές κυρίως συναλλαγές για την εκτέλεση ηλεκτρονικών πληρωμών είναι:

- Πιστωτικές κάρτες
- Χρεωστικές κάρτες
- Κάρτες αποθηκευμένης χρηματικής αξίας
- Ηλεκτρονικές επιταγές
- Ηλεκτρονική τραπεζική (Web banking)

Η χρήση της πιστωτικής κάρτας (ή άλλης αντίστοιχης ευκολίας χρήσης κάρτας) ως μέσου εκτέλεσης ηλεκτρονικών πληρωμών διασφαλίζει σημαντικά την αποδοχή και τη διάδοση της υπηρεσίας, καθώς οι πολίτες είναι ιδιαίτερα εξοικειωμένοι με τη χρήση της, λόγω κυρίως της χρησιμοποίησής της σε καθημερινές εμπορικές συναλλαγές. Το ίδιο ισχύει και στην περίπτωση των υπηρεσιών ηλεκτρονικής τραπεζικής (Web Banking), καθώς οι περισσότερες τράπεζες προσφέρουν σχετικές υπηρεσίες στους πελάτες τους, ιδιαίτερα σε ό,τι αφορά πληρωμές (π.χ. λογαριασμών ΔΕΚΟ, υπηρεσιών κινητής τηλεφωνίας και Διαδικτύου), εξόφληση πιστωτικών καρτών, μεταφορά ποσών, καταβολή φόρου εισοδήματος, φόρου προστιθέμενης αξίας και ασφαλιστικών εισφορών.

Σε διάφορες άλλες περιπτώσεις όπου παρέχονται διάφορες ηλεκτρονικές υπηρεσίες (κυρίως ενημερωτικές και ψυχαγωγικές) η πρόσβαση και χρήση αυτών είναι αρκετά απλή καθώς πολλές φορές απαιτείται απλά μια έγγραφη την οποία ο καθένας μπορεί να επιτύχει με τη χρήση της διεύθυνσης του ηλεκτρονικού ταχυδρομείου του.

3.3.1 Ασφάλεια συναλλαγών

Ένα θέμα που αφορά σε μεγάλο βαθμό όλους τους χρηστές ηλεκτρονικών υπηρεσιών είναι χωρίς αμφιβολία η ασφάλεια των συναλλαγών. Η ευκολία και η ασφάλεια είναι συνήθως δύο αντίθετες έννοιες στις συναλλαγές. Αυτό συμβαίνει γιατί όσο μεγαλύτερη ασφάλεια απαιτείται στις συναλλαγές τόσο πιο δύσκολο είναι για το χρήστη να ακολουθήσει τη

διαδικασία και σε ορισμένες περιπτώσεις αποθαρρύνεται να χρησιμοποιήσει την εν λόγω υπηρεσία. Παρόλα αυτά υπάρχουν βελτιωμένοι τρόποι ασφαλών συναλλαγών χωρίς ο χρήστης να πρέπει να θυσιάσει την ευκολία χρήσης.

Η ανάπτυξη του Διαδικτύου, το ηλεκτρονικό εμπόριο και οι συναλλαγές μέσω ανοιχτών δικτύων καθιστούν επιτακτική την ανάγκη ασφάλειας στις συναλλαγές. Ο χρήστης που συναλλάσσεται ηλεκτρονικά απαιτεί τα δεδομένα (π.χ. ένα μήνυμα ή ένα κείμενο) που στέλνει να μην μπορούν να αποκαλυφθούν ή να διατεθούν σε μη εξουσιοδοτημένα για αυτό άτομα (εμπιστευτικότητα). Επίσης, τα δεδομένα δεν θα πρέπει να είναι δυνατόν να αλλοιωθούν κατά τη μετάδοσή τους και ο παραλήπτης θα πρέπει να τα λάβει όπως ακριβώς τα έστειλε ο αποστολέας και να είναι σίγουρος ότι τα δεδομένα που λαμβάνει είναι αυτά που ο αποστολέας έχει στείλει (ακεραιότητα). Επιπλέον, σε μία τέτοια συναλλαγή, είναι απαραίτητο ο παραλήπτης να είναι σίγουρος για την ταυτότητα του αποστολέα (αυθεντικότητα). Τέλος, συμμετέχοντας σε μία ηλεκτρονική συναλλαγή θα πρέπει να μην είναι δυνατόν τα εμπλεκόμενα μέρη να αρνηθούν εκ των υστέρων την συμμετοχή τους στη συναλλαγή αυτή (μη αποποίηση ευθύνης). Εκτός των παραπάνω ιδιοτήτων (εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα, μη αποποίηση), ιδιαίτερα κρίσιμη είναι και η διασφάλιση της διαθεσιμότητας (availability) των πληροφοριακών συστημάτων και υποδομών που υποστηρίζουν την εκτέλεση των ηλεκτρονικών οικονομικών συναλλαγών. Συνεπώς, προτού χορηγηθεί το δικαίωμα σε ένα χρήστη να αποκτήσει πρόσβαση σε μία υπηρεσία εκτέλεσης μιας οικονομικής συναλλαγής με ηλεκτρονικά μέσα, οι φορείς της δημόσιας διοίκησης θα πρέπει να μεριμνήσουν για την εφαρμογή των οδηγιών του ΠΨΑ (Πλαίσιο Ψηφιακής Αυθεντικοποίησης) όσον αφορά στα εξής:

• Ανάλυση των δεδομένων της υπηρεσίας και κατάταξής τους στις κατηγορίες δεδομένων του ΠΨΑ

• Κατάταξη της υπηρεσίας στα επίπεδα εμπιστοσύνης, αυθεντικοποίησης και εγγραφής του ΠΨΑ

• Εφαρμογή των κατάλληλων διαδικασιών για την εγγραφή του χρήστη στην υπηρεσία και χορήγηση των κατάλληλων διακριτικών ασφάλειας (π.χ. όνομα και συνθηματικό χρήστη, ψηφιακό πιστοποιητικό)

Με βάση τις οδηγίες του ΠΨΑ, ο δημόσιος φορέας που παρέχει μία υπηρεσία ηλεκτρονικής διακυβέρνησης που αφορά ή περιλαμβάνει την εκτέλεση ηλεκτρονικών οικονομικών συναλλαγών, θα διασφαλίσει ότι ο δυνητικός χρήστης της υπηρεσίας διαθέτει τα απαραίτητα διακριτικά (ανάλογα με την κρισιμότητα των δεδομένων της υπηρεσίας) για να αποκτήσει πρόσβαση στην υπηρεσία και δεν θα είναι (εκ των υστέρων) σε θέση να αρνηθεί την εκτέλεση των συναλλαγών.

3.3.2 Απαιτήσεις υλοποίησης και εκτέλεσης ηλεκτρονικών πληρωμών

Προκειμένου οι εμπλεκόμενοι (πολίτες/ επιχειρήσεις, φορείς δημοσίου τομέα, χρηματοπιστωτικά ιδρύματα) να μπορέσουν να εκμεταλλευτούν τις ηλεκτρονικές πληρωμές προς όφελός τους, θα πρέπει να πληρούν κάποιες προϋποθέσεις.

Έτσι, οι φορείς του δημοσίου τομέα θα πρέπει να επικοινωνήσουν σε πρώτη φάση με κάποιο χρηματοπιστωτικό ίδρυμα προκειμένου να εκδηλώσουν το ενδιαφέρον τους για δυνατότητα υλοποίησης ηλεκτρονικών πληρωμών. Για να ξεκινήσει η υποστήριξη των ηλεκτρονικών πληρωμών θα πρέπει να γίνει μια σύμβαση του φορέα με το χρηματοπιστωτικό ίδρυμα που θα οριοθετεί τους όρους χρήσης και τις προϋποθέσεις για σωστή λειτουργία και εκτέλεση των πληρωμών. Επίσης, κάθε φορέας θα πρέπει να ανοίξει ένα λογαριασμό στον οποίο θα αποταμιεύονται τα χρήματα από τις ηλεκτρονικές πληρωμές και να διαθέτει τουλάχιστον ένα ηλεκτρονικό υπολογιστή και μία σύνδεση στο Διαδίκτυο προκειμένου να διαχειρίζεται τις συναλλαγές.

Αυτή τη στιγμή, οι φορείς της δημόσιας διοίκησης δεν παρουσιάζονται έτοιμοι από πλευράς οργάνωσης και διαδικασιών να υποστηρίξουν την εκτέλεση ηλεκτρονικών πληρωμών. Οι υφιστάμενες διαδικασίες της δημόσιας διοίκησης απαιτούν την καταβολή οικονομικού αντιτίμου με τη μορφή παραβόλων και διαφόρων μορφών χαρτοσήμων, τα οποία οι πολίτες πρέπει να προμηθεύονται από άλλα σημεία (συνήθως δημόσιες οικονομικές υπηρεσίες-ΔΟΥ και δημόσια ταμεία). Έτσι, πριν την εφαρμογή ηλεκτρονικών πληρωμών πρέπει να γίνει ανασχεδιασμός των διαδικασιών, ο οποίος κατ' ελάχιστον θα περιλαμβάνει αντικατάσταση των παραβόλων και των λοιπών 'παραδοσιακών' μέσων πληρωμής με τη δυνατότητα καταβολής του σχετικού τιμήματος μέσω κάποιου ηλεκτρονικού καναλιού. Από την πλευρά τους, τα χρηματοπιστωτικά ιδρύματα διαθέτουν σήμερα όλα τα απαραίτητα συστήματα και διαδικασίες, καθώς και τη σχετική εμπειρία και ωριμότητα, προκειμένου να υποστηρίξουν ηλεκτρονικές πληρωμές με οποιοδήποτε τρόπο τους ζητηθεί. Επομένως, η συνεργασία με τους φορείς της δημόσιας διοίκησης για την εκτέλεση ηλεκτρονικών πληρωμών δεν δημιουργεί κάποιο πρόβλημα για τα χρηματοπιστωτικά ιδρύματα που παρέχουν σχετικές υπηρεσίες.

Όσον αφορά τους πολίτες, η εκτέλεση ηλεκτρονικών πληρωμών δεν απαιτεί κάτι περισσότερο από την ύπαρξη μιας πιστωτικής κάρτας (ή όποιου άλλου μέσου απαιτείται, π.χ. τραπεζικού λογαριασμού συνδεδεμένου με υπηρεσίες ηλεκτρονικής τραπεζικής) και η πρόσβαση σε ένα κανάλι εκτέλεσης πληρωμών (Διαδίκτυο ή κινητή τηλεφωνία). Έτσι, η εκτέλεση ηλεκτρονικών πληρωμών για τους πολίτες δεν θέτει κάποιες ιδιαίτερες απαιτήσεις.

Συνοψίζοντας, η υλοποίηση ηλεκτρονικών πληρωμών σε μία υπηρεσία που παρέχεται με ηλεκτρονικό τρόπο από ένα φορέα της δημόσιας διοίκησης προτείνεται να περιλαμβάνει τα παρακάτω βήματα:

• Εύρεση του σημείου της διαδικασίας που απαιτεί την καταβολή οικονομικού αντιτίμου.

• Αναγνώριση της μορφής καταβολής του αντιτίμου (π.χ. παράβολο, μεγαρόσημο), των σημείων (φορέων) στους οποίους καταβάλλεται το αντίτιμο και αυτών στους οποίους αποδίδεται.

• Ανασχεδιασμός της διαδικασίας (σε συνεργασία με τους φορείς στους οποίους καταβάλλεται και αποδίδεται το αντίτιμο) ώστε να αντικατασταθεί ο 'παραδοσιακός' τρόπος πληρωμής με ηλεκτρονική πληρωμή – Ενημέρωση εμπλεκομένων μονάδων και στελεχών φορέα.

• Θεσμική θωράκιση της ανασχεδιασμένης διαδικασίας – Τροποποίηση διατάξεων που ορίζουν τον τρόπο εκτέλεσής της.

• Συνεργασία με χρηματοπιστωτικό ίδρυμα για τον τρόπο υλοποίησης του συστήματος ηλεκτρονικών πληρωμών (μέσο, κανάλι, κόστος παροχής υπηρεσίας, ενημέρωση φορέα και συστημάτων φορέα για τις ηλεκτρονικές συναλλαγές).

• Υλοποίηση συστήματος ηλεκτρονικών πληρωμών – Διάδοση της δυνατότητας εκτέλεσης ηλεκτρονικών πληρωμών στους τελικούς αποδέκτες της υπηρεσίας.

Εάν δεν είναι επιθυμητή η κατάργηση του υφιστάμενου τρόπου πληρωμής, η δυνατότητα εκτέλεσης ηλεκτρονικών πληρωμών μπορεί να συμπληρώσει αντί να αντικαταστήσει τις υπάρχουσες διαδικασίες και τρόπους πληρωμής. Σε αυτή την περίπτωση, οι φορείς της δημόσιας διοίκησης πρέπει να διασφαλίσουν τον ενιαίο τρόπο αντιμετώπισης των πληρωμών που λαμβάνουν με την παραδοσιακή διαδικασία και μέσω συστημάτων ηλεκτρονικών πληρωμών.

3.4 Μελέτη και καταγραφή των πλεονεκτημάτων και των αλλαγών στον οργανισμό που επιφέρει η σύγχρονη τεχνολογία.

Κάποιες άλλες σύγχρονες τεχνολογίες που χρησιμοποιούμε στις μέρες μας για να διευκολύνουμε τις συναλλαγές μας είτε με τις τράπεζες είτε με το Δημόσιο θα αναφέρουμε παρακάτω.

3.4.1 Στον τραπεζικό χώρο

3.4.1.1 ΦΩΝΗΤΙΚΗ ΤΡΑΠΕΖΙΚΗ (VOICE BANKING)

Η φωνητική τραπεζική (voice banking) είναι η τεχνολογία αναγνώρισης ομιλίας, η οποία αποτελεί τη βάση για ένα σύστημα αυτόματης παροχής τραπεζικών πληροφοριών και υπηρεσιών μέσω τηλεφώνου.

Από τις αρχές του 20^{ου} αιώνα η τεχνολογία στην προσπάθεια της να δημιουργήσει μηχανές χρήστη, αναζητούσε τρόπους να χρησιμοποιήσει την φωνή ως μέσο επικοινωνίας του ανθρώπου. Σήμερα μέσω της Τεχνολογίας Αναγνώρισης Ομιλίας αυτό είναι πλέον εφικτό.

Ο συνδυασμός της Τεχνολογίας Αναγνώρισης Ομιλίας με το τηλέφωνο το οποίο αποτελεί σημαντικό κα προσφιλέστερο κανάλι επικοινωνίας, οδήγησε σε ένα αυτόματο σύστημα επικοινωνίας όπου απλά με ένα τηλέφωνο πραγματοποιείται προφορική επικοινωνία χωρίς να απαιτείται χρήση πλήκτρων ή χρήση ειδικού εξοπλισμού.

Η πρώτη τράπεζα στην Ελλάδα που χρησιμοποίησε την τεχνολογία αυτή για την παροχή Τραπεζικών πληροφοριών και υπηρεσιών μέσω τηλεφώνου είναι η ΕΓΝΑΤΙΑ ΤΡΑΠΕΖΑ.

ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΗΣ ΦΩΝΗΤΙΚΗΣ ΤΡΑΠΕΖΙΚΗΣ

24ωρη πρόσβαση σε πληροφορίες και υπηρεσίες. Ο χρήστης ‘έχει την δυνατότητα να πραγματοποιεί τις συναλλαγές του οποιαδήποτε στιγμή της ημέρας χωρίς περιορισμούς.

Ευκολία στην χρήση του, αφού το μόνο που έχει να κάνει ο χρήστης του είναι να εκφράσει το αίτημα του και αναλαμβάνει τα υπόλοιπα η τεχνολογία.

Μείωση του χρόνου αναμονής. Η εξυπηρέτηση του χρήστη είναι άμεση αφού δεν χρειάζεται να περιμένει σε ουρές στα καταστήματα της κάθε τράπεζας για να πραγματοποιήσει τις συναλλαγές του.

Απόλυτη ανωνυμία στις συναλλαγές. Οι συναλλαγές πραγματοποιούνται χωρίς την επέμβαση από κάποιον άνθρωπο χρήστη γίνονται όλες μέσω προγραμμάτων.

Αξιοπιστία στις συναλλαγές. Η χρήση του συστήματος περιορίζει σημαντικά την πιθανότητα λάθους ακόμα και στις πιο σύνθετες συναλλαγές.

Απόλυτη διαφανεί. Όλες οι συναλλαγές που πραγματοποιούνται μέσω της φωνητικής τραπεζικής καταγράφονται για την καλύτερη ασφάλεια των χρηστών του.

3.4.1.2. ΤΗΛΕΦΩΝΙΚΗ ΤΡΑΠΕΖΙΚΗ (PHONE BAKING)

Η υπηρεσία της τηλεφωνικής τραπεζικής (phone banking) παρέχει την δυνατότητα στους χρήστες να πραγματοποιούν τραπεζικές συναλλαγές ή και να πληροφορούνται για διάφορα θέματα που τους ενδιαφέρουν μέσω οποιουδήποτε τηλεφώνου, κινητού ή σταθερού. Η τηλεφωνική τραπεζική (phone banking) φέρνει την τράπεζα πιο κοντά στον χρήστη καθώς με ένα μόνο τηλεφώνημα σε όποιο σημείο και αν βρίσκεται παρέχονται σχεδόν όλες οι δυνατότητες που υπάρχουν και στο κατάστημα της τράπεζας.

ΠΑΡΕΧΟΜΕΝΕΣ ΥΠΗΡΕΣΙΕΣ

Για χρεωστική κάρτα, είναι δυνατή η ενημέρωση για το υπόλοιπο των λογαριασμών ταμιευτηρίου και τρεχούμενου που είναι συνδεδεμένη με την κάρτα.

Για πιστωτική κάρτα παρέχεται η δυνατότητα ενημέρωσης για το τρέχον υπόλοιπο της κάρτας, την ελάχιστη καταβολή καθώς και την ημερομηνία πληρωμής και επίσης μπορεί να γίνει ενημέρωση και για τα υπόλοιπα των καταθετικών λογαριασμών.

Τέλος, μέσω της υπηρεσίας της τηλεφωνικής τραπεζικής μπορεί ο χρήστης να απενεργοποιήσει άμεσα την κάρτα σε περίπτωση απώλειας ή κλοπής χωρίς να χάνει πολύτιμο χρόνο περιμένοντας να πάει σε κάποιο κατάστημα και να πραγματοποιήσει την απενεργοποίηση.

ΠΛΕΟΝΕΚΤΗΜΑΤΑ

Εξοικονόμηση χρόνου. Δεν χρειάζεται να απομακρυνθεί ο χρήστης από το σπίτι ή το γραφείο του για να πάει στο πλησιέστερο κατάστημα της τράπεζας.

Ευκολία στην χρήση. Η κλήση μπορεί να γίνει από οποιοδήποτε τηλέφωνο (κινητό ή σταθερό) χωρίς ειδικές γνώσεις και πολύπλοκές διαδικασίες.

Ασφάλεια. Ο χρήστης για να πραγματοποιήσει οποιαδήποτε συναλλαγή πληκτρολογεί τον προσωπικό του τηλεκωδικό.

Άμεση επικοινωνία. Υπάρχει πάντα ένας εκπρόσωπος της τράπεζας για να εξυπηρετήσει όλο το 24ωρο, 7 μέρες την εβδομάδα.

ΑΣΦΑΛΕΙΑ

Η υπηρεσία της τηλεφωνικής τραπεζικής (Phone Banking) είναι απόλυτα ασφαλής. Με την πληκτρολόγηση του αριθμού της κάρτας του πελάτη και την εισαγωγή του μυστικού τηλεκωδικού που μόνο ο πελάτης γνωρίζει, αποκτά πρόσβαση στην υπηρεσία και ενημερώνεται για τα υπόλοιπα των συνδεδεμένων λογαριασμών του. Επιπλέον ο μυστικός τηλεκωδικός παρέχεται μόνο από τα ATM των τραπεζών και ισχύει για την αντίστοιχη κάρτα και μόνο.

Εικόνα 4: Είσοδος στην τηλεφωνική τραπεζική

3.4.1.3. ΗΛΕΚΤΡΟΝΙΚΟ ΧΡΗΜΑΤΙΣΤΗΡΙΟ

Οι χρηματιστηριακές συναλλαγές σε απευθείας σύνδεση (on line) αφορούν τις χρηματιστηριακές εταιρίες, μέσω των οποίων οι χρηματιστηριακές εντολές μπορούν να πραγματοποιηθούν μέσω του διαδικτύου.

Το διαδίκτυο έχει βοηθήσει πολύ στις χρηματιστηριακές συναλλαγές. Η ταχύτητα στις συναλλαγές, δυνατότητα τήρησης βάσης δεδομένων και παρακολούθηση και αναλύσεων αποτελούν ένα σημαντικό προνόμιο επιλογής αυτού του τρόπου της συναλλαγής.

Πολλές εταιρίες παρέχουν τη δυνατότητα απευθείας σύνδεσης με το χρηματιστήριο και δίνουν στους πελάτες τη δυνατότητα για πλήρη έλεγχο των χαρτοφυλακίων τους και άμεση δυνατότητα για εντολές.

Υπάρχουν πολλές υπηρεσίες για το ευρύτερο κοινό με το internet πολλές φορές να παίζει ρόλο σύμβουλου επενδύσεων. Έτσι σε πολλές ιστοσελίδες μπορεί κάποιος να ενημερωθεί για τις τιμές κλεισίματος των μετοχών μετά το τέλος της συνεδρίασης ή επίσης να παρακολουθήσει την εξέλιξη των μετοχών στο πρόσφατο παρελθόν ακόμα και να ενημερωθεί για τις τιμές των μετοχών ή την πορεία βασικών τιμών κλάδων.

Το διαδίκτυο αντικαθιστά συνεπώς πλήρως μια οικονομική εφημερίδα και μάλιστα με αρκετές ώρες διάφορα και με μηδενικό κόστος.

Η ενημέρωση που παρέχει η εκάστοτε χρηματοοικονομική εταιρία στους πελάτες της γίνεται συνήθως μέσω ηλεκτρονικού μηνύματος.

Η διατήρηση μέσω διαδικτύου στοιχείων που αφορούν το προσωπικό χαρτοφυλάκιο κάθε χρήστη επιτρέπει την δημιουργία εξατομικευμένων αναλύσεων οι οποίες παλαιότερα ήταν εφικτές με πολύ μεγαλύτερο κόπο και κόστος.

Η πρόσβαση σε πολλές αγορές, οι πολλαπλές συναλλαγματικές ισοτιμίες και τα αλλά μέσα εκτέλεσης χρηματιστηριακών εντολών και όλα αυτά μέσα από την οθόνη ενός ηλεκτρονικού υπολογιστή, αποτελούν σημαντικούς παράγοντες για την όλο και μεγαλύτερη εξάπλωση του ηλεκτρονικού χρηματιστηρίου.

3.4.2 Στο Δημόσιο

Η Γενική Γραμματεία Πληροφοριακών Συστημάτων έχει υλοποιήσει ένα εκτεταμένο σύνολο υπηρεσιών ηλεκτρονικής διακυβέρνησης προς τον πολίτη, τις επιχειρήσεις και τη δημόσια διοίκηση (taxis net). Η υλοποίηση νέων ηλεκτρονικών υπηρεσιών και η βελτίωση των παλαιότερων αποτελεί καθημερινή δραστηριότητα της Γ.Γ.Π.Σ., η οποία και παρέχει το μεγαλύτερο μέρος των ηλεκτρονικών υπηρεσιών που παρέχονται σήμερα από το δημόσιο. Όλες οι ηλεκτρονικές υπηρεσίες σχεδιάζονται προσεκτικά με γνώμονα την ευκολότερη και ταχύτερη εξυπηρέτηση για τον τελικό χρήστη.

Μέσω του taxis net πλέον ο πολίτης ενημερώνεται για όλα τα φορολογικά νέα και πραγματοποιεί πολλές συναλλαγές που παλαιότερα απαιτούσαν την παρουσία του στις εφορίες όπως δηλώσεις φπα, δηλώσεις εισοδήματος και πολλά άλλα, τώρα όλα αυτά γίνονται μέσω internet με αποτέλεσμα την καλύτερη εξυπηρέτηση του πολίτη χωρίς να χρειαστεί η μετακίνηση του στην εφορία που ανήκει χάνοντας έτσι χρόνο.

Προκειμένω να επιτευχθεί η ασφάλεια στις συναλλαγές, ο ενδιαφερόμενος θα πρέπει να συμπληρώσει μια αίτηση εγγραφής που βρίσκεται στο site της Γενικής Γραμματείας Πληροφοριακών Συστημάτων και έπειτα να απευθυνθεί στην εφορία για να προμηθευτεί έναν προσωπικό κωδικό και με αυτόν θα μπορεί να μπαίνει στο σύστημα και να πραγματοποιεί τις διάφορες συναλλαγές που επιθυμεί.

Εικόνα 5: Είσοδος στις υπηρεσίες της γενικής γραμματείας πληροφοριακών συστημάτων

Ένας ακόμη φορέας του Δημοσίου που έχει εισάγει το διαδίκτυο στον τρόπο εξυπηρέτησης των πολιτών είναι το Ίδρυμα Κρατικών Ασφαλίσεων (ΙΚΑ). Με αυτό τον τρόπο αυτόν επιτυγχάνεται η βελτίωση των συναλλαγών με το φορέα. Δεν χρειάζεται ο συναλλασσόμενος να πάει ο ίδιος στο υποκατάστημα του ΙΚΑ για να πραγματοποιήσει τις συναλλαγές που θέλει χάνοντας χρόνο περιμένοντας σε "ουρές" .Τέλος για τους επαγγελματίες ο διαδικτυακός τόπος του ΙΚΑ παρέχει την δυνατότητα αποστολής Αναλυτικής Περιοδικής Δήλωσης (ΑΠΔ)

Εικόνα 6: Είσοδος στις υπηρεσίες του ΙΚΑ

Τέλος και ο Οργανισμός Απασχόλησης Εργατικού Δυναμικού (ΟΑΕΔ) παρέχει τόσο σε πολίτες όσο και σε εργοδότες την δυνατότητα αναζήτησης εργασίας ή προσωπικού αντίστοιχα. Εισάγοντας τα κριτήρια της θέσης εργασίας ή του εργαζομένου και με βάση την γεωγραφική περιοχή ενδιαφέροντος, εμφανίζεται λίστα με στοιχεία επικοινωνίας των επιχειρήσεων που ζητούν υπαλλήλους ή των πολιτών που ζητούν εργασία.

3.5 ΑΠΑΙΤΟΥΜΕΝΗ ΥΠΟΔΟΜΗ

Για να χρησιμοποιήσει κάποιος τις υπηρεσίες που παρέχονται μέσω της ηλεκτρονικής τραπεζικής το μόνο που χρειάζεται είναι ένας ηλεκτρονικός υπολογιστής ή ένα κινητό τηλέφωνο και πρόσβαση στο διαδυκτιο. Δεν χρειάζεται ο υπολογιστής να έχει κάποιο ειδικό λογισμικό.

ΣΤΟ ΚΕΦΑΛΑΙΟ 3 ΧΡΗΣΙΜΟΠΟΙΗΘΗΚΑΝ ΟΙ ΠΗΓΕΣ 2,8,9,10,11,12,13 ΑΠΟ ΤΙΣ ΔΙΑΔΙΚΤΥΑΚΕΣ ΠΗΓΕΣ

ΚΕΦΑΛΑΙΟ 4

ΑΣΦΑΛΕΙΑ ΣΥΝΑΛΛΑΓΩΝ ΚΑΙ ΔΕΔΟΜΕΝΩΝ

4.1 ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ

Η διασφάλιση του απορρήτου των ηλεκτρονικών συναλλαγών αποτελεί πρωταρχικό στόχο για κάθε τράπεζα και οι επενδύσεις σε αυτόν τον τομέα υπήρξαν και συνεχίζουν να είναι πολύ σημαντικές. Παράλληλα παρατηρείται μια διστακτικότητα από πλευράς κοινής γνώμης στη χρήση των ηλεκτρονικών υπηρεσιών, με κύρια αιτία την άγνοια σε θέματα ασφάλειας. Το σίγουρο είναι πως, για να επιτευχθεί ο στόχος και να αντιμετωπιστούν οποιεσδήποτε πιθανές απειλές, η συνεργασία τραπεζών και χρηστών είναι απαραίτητη.

4.2 Ο ΡΟΛΟΣ ΤΗΣ ΤΡΑΠΕΖΑΣ

Οι τράπεζες επικεντρώνουν τις προσπάθειές τους στη διασφάλιση της συναλλαγής με τον τελικό χρήστη, σε όλα τα στάδια που περιλαμβάνονται μέχρι την επιτυχή ολοκλήρωσή της. Απαραίτητη είναι η ταυτοποίηση της ίδιας της τράπεζας, του τελικού χρήστη, αλλά και η διασφάλιση του απόρρητου της "συνομιλίας" τους. Επίσης υπάρχουν και κάποιες επιπρόσθετες δικλείδες ασφαλείας, που ενισχύουν περαιτέρω τις προσπάθειες των τραπεζών στην αντιμετώπιση εξωτερικών απειλών.

I. Ταυτοποίηση τράπεζας

Κάθε τράπεζα επιλέγει έναν αναγνωρισμένο παροχέα (Trusted Third Party), ο οποίος να είναι σε θέση να πιστοποιήσει την ταυτότητά της στο Διαδίκτυο. Ενα παράδειγμα παροχέα τέτοιου είδους πιστοποίησης, ιδιαίτερα γνωστό στο ευρύ κοινό, είναι η εταιρεία Verisign. Για τον τελικό χρήστη αυτό μπορεί εύκολα να αναγνωριστεί από την εμφάνιση ενός μικρού εικονιδίου με μορφή λουκέτου στο κάτω μέρος των συγκεκριμένων σελίδων, μέσω του οποίου ο χρήστης μπορεί να επιβεβαιώσει ότι βρίσκεται στο σωστό προορισμό.

II. Ταυτοποίηση χρήστη

Οπως ακριβώς το ATM επιτρέπει μια συναλλαγή μέσω της κάρτας και ενός κωδικού, έτσι και το e-banking απαιτεί την ταυτοποίηση του χρήστη, προτού του επιτρέψει την πρόσβαση στους λογαριασμούς του. Για την ταυτοποίηση των χρηστών e-banking, οι τράπεζες ακολουθούν μια κοινή πρακτική, χρησιμοποιώντας τον προσωπικό κωδικό χρήστη (username) σε

συνδυασμό με ένα επίσης προσωπικό μυστικό κωδικό (password). Ο χρήστης πρέπει να παραλαμβάνει τους δύο προσωπικούς του κωδικούς ξεχωριστά. Κοινή πρακτική αποτελεί επίσης οι προσωπικοί κωδικοί να μπλοκάρονται μετά από κάποιες λανθασμένες προσπάθειες εισαγωγής του χρήστη, καθώς οι συνεχείς λανθασμένες προσπάθειες θεωρούνται ύποπτες. Για την περαιτέρω διασφάλιση των χρηστών, ορισμένες τράπεζες έχουν προχωρήσει σε ένα επιπλέον επίπεδο ασφάλειας, με πρόσθετους κωδικούς, αριθμούς εξουσιοδότησης συναλλαγής (TAN) και ψηφιακά πιστοποιητικά.

Οι αριθμοί TAN (Transaction Authorization Number) είναι αριθμοί που απαιτούνται για την πραγματοποίηση μιας συναλλαγής, δημιουργούνται από την τράπεζα, δένονται με τον κωδικό του χρήστη και εισάγονται κατά τη διαδικασία της συναλλαγής. Το ψηφιακό πιστοποιητικό (digital certificate) αποτελεί το μέσο που παρέχει τη δυνατότητα στον κάτοχό του να υπογράφει ψηφιακά όλες τις ηλεκτρονικές συναλλαγές που εκτελεί μέσα από το e-banking. Το πιστοποιητικό, όταν εγκατασταθεί σε κάποιον υπολογιστή, προσφέρει τη δυνατότητα ταυτοποίησης του χρήστη και επιτρέπει συναλλαγές και μεταφορές χρημάτων μεταξύ λογαριασμών μόνο από το συγκεκριμένο χρήστη. Τα επιπλέον επίπεδα ασφάλειας απαιτούνται συνήθως σε συναλλαγές που περιλαμβάνουν μεταφορές χρηματικών ποσών και όχι για συναλλαγές ενημερωτικού χαρακτήρα. Η φιλοσοφία είναι παρόμοια με αυτήν που ακολουθείται στα γκισέ των τραπεζών, όπου ο υπάλληλος απαιτεί από τον πελάτη την επίδειξη της ταυτότητάς του, όταν αυτός ζητήσει τη μεταφορά χρημάτων.

III. Εξασφάλιση της μεταφοράς δεδομένων

Μια επιπρόσθετη δικλείδα ασφαλείας, με την οποία εξασφαλίζεται το απόρρητο κατά τη μεταφορά των δεδομένων, είναι η κρυπτογράφησή τους. Το πρωτόκολλο επικοινωνίας SSL (Secure Sockets Layer) μαζί με την κρυπτογράφηση στα 128bit εξασφαλίζει την ασφάλεια των συναλλαγών μέσω Διαδικτύου. Η κρυπτογράφηση με 128bit σημαίνει ότι υπάρχουν 2128 πιθανά κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση των μηνυμάτων από τον Internet Explorer στον server της τράπεζας. Για αυτόν το λόγο η κρυπτογράφηση στα 128bit θεωρείται πρακτικά αδύνατο να παραβιαστεί. Ο χρήστης μπορεί να αναγνωρίσει εάν η σελίδα στην οποία βρίσκεται είναι ασφαλής, καθώς το πρωτόκολλο που εμφανίζεται με τη διεύθυνση της τράπεζας μετατρέπεται από “http” σε “https” και εμφανίζεται παράλληλα και το χαρακτηριστικό εικονίδιο με το λουκέτο στο κάτω μέρος της σελίδας.

IV. Ελεγχόμενη πρόσβαση στα συστήματα της τράπεζας

Η πρόσβαση στα συστήματα των περισσότερων τραπεζών (servers) προστατεύεται από τελευταία τεχνολογία Firewall και IDS (Intrusion Detection Systems), η οποία επιτρέπει τη χρήση συγκεκριμένων υπηρεσιών, απαγορεύοντας παράλληλα την πρόσβαση σε συστήματα και βάσεις

δεδομένων με απόρρητα στοιχεία και πληροφορίες της τράπεζας σε μη αναγνωρισμένους χρήστες.

V. Επιπλέον δικλείδες ασφαλείας

- ***Εισαγωγή στοιχείων εισόδου***: Καθώς παρατηρήθηκε η εμφάνιση ιών, οι οποίοι είχαν τη δυνατότητα να καταγράφουν πληκτρολογήσεις χρηστών, ορισμένες τράπεζες υιοθέτησαν τη χρήση εικονικού πληκτρολογίου για την καταχώριση των στοιχείων χρήστη ή επιλεκτικά την καταχώριση ορισμένων από τα στοιχεία αυτά (π.χ. το 1ο και το 3ο γράμμα του κωδικού). Έτσι, ακόμα κι αν μπορούσε να υποκλαπεί ο ένας από τους δύο κωδικούς ταυτοποίησης, δεν θα είχε καμία ισχύ η αποκλειστική του χρήση και ο χρήστης θα παρέμενε ασφαλής.
- ***Αυτόματη αποσύνδεση χρήστη***: Στις περισσότερες εφαρμογές e-banking, η ολοκλήρωση μιας συναλλαγής επιτρέπεται μέσα σε ένα συγκεκριμένο χρονικό όριο (συνήθως πέντε έως δεκαπέντε λεπτά), μετά τη λήξη του οποίου το σύστημα αποσυνδέει το χρήστη αυτόματα.
- ***Υποχρεωτική αλλαγή κωδικών***: Η πλειονότητα των τραπεζών υποχρεώνει τους χρήστες e-banking στην άμεση αλλαγή των προσωπικών τους κωδικών με κάποιους της επιλογής τους, οι οποίοι να εντυπώνονται και πιο εύκολα στη μνήμη. Συνήθης πρακτική αποτελεί επίσης η αυτόματη απενεργοποίηση των κωδικών μετά από ένα συγκεκριμένο χρονικό διάστημα, στο οποίο ο χρήστης δεν έχει προχωρήσει σε κάποια συναλλαγή.

VI. Διαδικασίες

Παράλληλα με την απαραίτητη τεχνολογική υποδομή, η διασφάλιση των ηλεκτρονικών συναλλαγών απαιτεί και την υιοθέτηση αυστηρών διαδικασιών από την τράπεζα, όσον αφορά την ανάπτυξη, διαχείριση και προσφορά της υπηρεσίας e-banking. Είναι κοινή τραπεζική πρακτική, που ακολουθείται και στις υπηρεσίες e-banking, να προστατεύονται τα προγράμματα και τα συστήματα από διαδικασίες που απαιτούν συνδυασμένες ενέργειες δύο ή περισσότερων ανθρώπων από διαφορετικά τμήματα. Παράλληλα όλες οι νέες εφαρμογές σχεδιάζονται και υλοποιούνται κάτω από ιδιαίτερα αυστηρές διαδικασίες ελέγχου προτού παραδοθούν. Τέλος, πολλές τράπεζες επιλέγουν τη συνεργασία με ανεξάρτητους εξωτερικούς φορείς για τον έλεγχο της λειτουργίας των διαδικασιών που ακολουθούν.

4.3 Ο ΡΟΛΟΣ ΤΟΥ ΧΡΗΣΤΗ

Οι τράπεζες από μόνες τους δεν είναι σε θέση να εξασφαλίσουν απόλυτα την ασφάλεια των συναλλαγών, είτε ηλεκτρονικών είτε φυσικών. Η προσοχή και η ανάληψη προληπτικών μέτρων από τη μεριά του χρήστη σε συνδυασμό

με τις απαραίτητες παροχές από την τράπεζα, μπορούν να εξασφαλίσουν την επιτυχία της συναλλαγής. Συγκεκριμένα, κάθε χρήστης υπηρεσιών e-banking θα πρέπει να έχει υπόψη του πως:

- Οι κωδικοί εισόδου στο e-banking είναι αυστηρά προσωπικοί και σε καμία περίπτωση δεν πρέπει ο ιδιοκτήτης τους να τους μοιράζεται με κανέναν. Καλό θα ήταν κάθε χρήστης να αποστηθίζει τους κωδικούς του και να μην τους έχει σε γραπτή μορφή, καθώς υπάρχει ο κίνδυνος να κλαπούν, και να τους αλλάζει τακτικά. Επίσης καλό είναι να μην χρησιμοποιούνται οι κωδικοί που έχουν επιλεχθεί για είσοδο στο e-banking και σε άλλα, μη ασφαλή sites.
- Είναι απαραίτητος ο έλεγχος της διεύθυνσης της ιστοσελίδας, στην οποία θα εισάγει τα στοιχεία του, καθώς μπορεί να αποτελεί αντιγραφή κάποιου τραπεζικού site, με σκοπό την παραπλάνηση και την απόκτηση των προσωπικών του στοιχείων. Στην περίπτωση που η ηλεκτρονική διεύθυνση δεν είναι εμφανής, ένας ακόμη τρόπος επιβεβαίωσης της ταυτότητας της ιστοσελίδας είναι μέσω του εικονιδίου (λουκέτο), το οποίο εμφανίζεται στις ασφαλείς τραπεζικές σελίδες.
- Είναι απαραίτητη η εγκατάσταση στον υπολογιστή προγράμματος που να τον προστατεύει από την απειλή ιών. Καθώς παρατηρείται συνεχώς η εμφάνιση καινούριας μορφής ιών, η συχνή ανανέωση των σχετικών προγραμμάτων είναι επίσης απαραίτητη.
- Ιδιαίτερη προσοχή πρέπει να δίνεται σε περίπτωση που ο υπολογιστής που χρησιμοποιείται δεν ανήκει στο χρήστη (αεροδρόμια, internet café, κ.λπ.) κυρίως στο τι επιλέγει να αποθηκεύσει σε αυτόν.

4.4 Η ΚΡΙΣΙΜΟΤΗΤΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΕΦΑΡΜΟΓΩΝ

Όλες οι επιθέσεις ασφάλειας σε επίπεδο εφαρμογών έχουν σαν στόχο να επωφεληθούν από τις υπάρχουσες αδυναμίες ασφάλειας με αποτέλεσμα να πλήξουν την Εμπιστευτικότητα, Ακεραιότητα & Διαθεσιμότητα των επιχειρηματικών δεδομένων που επεξεργάζονται μέσω της εκάστοτε εφαρμογής.

Το μεγαλύτερο μέρος των επενδύσεων σε θέματα ασφάλειας αφορά στην θωράκιση της περιμέτρου και στην θωράκιση της υποδομής των πληροφοριακών συστημάτων. Έτσι, βλέπουμε την λειτουργία συστημάτων όπως firewalls, IDSs, τα οποία συμβάλουν στην αποτελεσματική διαχείριση της ασφάλειας σε επίπεδο δικτύου. Το δίκτυο είναι επιφορτισμένο με την διακίνηση των δεδομένων από / προς και μεταξύ των συστημάτων στα οποία υπάρχει εγκατεστημένη η επιχειρησιακή λογική, με την μορφή εφαρμογών. Η ασφάλεια δικτύου αφορά στην διασφάλιση της ακεραιότητας και αξιοπιστίας των δεδομένων τα οποία διακινούνται μεταξύ των πληροφοριακών πόρων. Η επιχειρησιακή λογική είναι αυτή η οποία προσδιορίζει / καθορίζει ποιες από

τις απαιτήσεις των χρηστών (user inputs) και ποιες από τις αιτούμενες συναλλαγές (transactions) νομιμοποιούνται να διενεργηθούν.

Η παραποίηση και αποσύνθεση της λογικής των εφαρμογών είναι ένας ακόμα τρόπος για να καταφέρει ένας μη εξουσιοδοτημένος χρήστης να εισχωρήσει στα δεδομένα ενός οργανισμού. Είναι ένας διαφορετικός τρόπος προσέγγισης, ο οποίος διαφοροποιείται από τις προσπάθειες για διείσδυση σε έναν μη ασφαλή server ή στην απώλεια διαθεσιμότητας των συστημάτων και υπηρεσιών, πρόκειται για απ' ευθείας πρόσβαση και κλοπή των επιχειρησιακών πληροφοριών.

Κατά την υλοποίηση των δικλείδων ασφάλειας σε επίπεδο δικτύων και συστημάτων, αφήνονται ελεύθερα για χρήση μόνο τα απαραίτητα πρωτόκολλα και υπηρεσίες. Διενεργείται η κατάλληλη παραμετροποίηση έτσι ώστε να μην είναι εφικτή η παρείσδυση μη εξουσιοδοτημένων χρηστών οι οποίοι θα εκμεταλλευτούν την ύπαρξη αδυναμιών ασφάλειας των πρωτοκόλλων και των υπηρεσιών που χρησιμοποιούνται. Οι αδυναμίες ασφάλειας των εφαρμογών εκδηλώνονται μέσω των επιτρεπόμενων υπηρεσιών και πρωτοκόλλων.

Η ασφάλεια των εφαρμογών είναι ένα πανίσχυρο εργαλείο που ελέγχει την χρήση της εκάστοτε εφαρμογής και δρα προληπτικά ενάντια σε μη εξουσιοδοτημένους χρήστες που θέλουν να αποκτήσουν πρόσβαση σε επιχειρησιακά δεδομένα και πληροφοριακούς πόρους.

4.5 ΚΥΡΙΕΣ ΑΙΤΙΕΣ ΔΗΜΙΟΥΡΓΙΑΣ ΑΔΥΝΑΜΙΩΝ ΑΣΦΑΛΕΙΑΣ ΕΦΑΡΜΟΓΩΝ

Οι κύριες αιτίες δημιουργίας των αδυναμιών ασφάλειας των εφαρμογών είναι οι ακόλουθες:

- Οι σημερινές εφαρμογές αποτελούνται από μέρη κώδικα τα οποία είναι ιδιοπαραγόμενα, από λογισμικό το οποίο υπάρχει στο εμπόριο και από έναν ή περισσότερους servers. Πιθανά λάθη κατά την σύνδεση και ολοκλήρωση όλων των παραπάνω συστατικών μπορεί να οδηγήσουν σε αδυναμίες ασφάλειας.
- Προγραμματιστικά λάθη κατά την ανάπτυξη των εφαρμογών.
- Εκούσιες επεμβάσεις στον παραγόμενο κώδικα για ίδιο όφελος.

4.6 ΚΙΝΔΥΝΟΙ ΑΣΦΑΛΕΙΑΣ ΕΦΑΡΜΟΓΩΝ & ΕΠΙΔΡΑΣΗ ΣΤΟ ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΕΡΙΒΑΛΛΟΝ

Οι κίνδυνοι ασφάλειας πληροφοριών που προκύπτουν από την αποθήκευση ή / και επεξεργασία των επιχειρηματικών πληροφοριών από τις εκάστοτε εφαρμογές, αφορούν στην απώλεια της Εμπιστευτικότητας, Ακεραιότητας και Διαθεσιμότητας των πληροφοριών.

- **Εμπιστευτικότητα** – Οι πληροφορίες της εφαρμογής πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση.
- **Ακεραιότητα** – Διασφάλιση της εγκυρότητας, ορθότητας και πληρότητας των δεδομένων κατά της φάσης της εισαγωγής τους, επεξεργασίας τους & παραγωγής του αποτελέσματος της επεξεργασίας τους.
- **Διαθεσιμότητα** – Τα δεδομένα πρέπει να είναι διαθέσιμα για όσο χρονικό διάστημα απαιτείται.

Η σημαντικότητα των παραπάνω κινδύνων προσδιορίζεται από την επίδρασή τους στο επιχειρησιακό περιβάλλον και από την πιθανότητα εκδήλωσής τους.

Η επίδραση από την απώλεια της Εμπιστευτικότητας, Ακεραιότητας και Διαθεσιμότητας των πληροφοριών είναι:

- Απώλεια ανταγωνιστικού πλεονεκτήματος.
- Λήψη λανθασμένων αποφάσεων από την Διοίκηση.
- Αδυναμία διεκπεραίωσης βασικών επιχειρηματικών δραστηριοτήτων.
- Προσβολή της αξιοπιστίας και την εμπιστοσύνης προς της εταιρείας των πελατών της ή / και των μετόχων της. Προσβολή της εικόνας και της φήμης της εταιρείας.
- Πιθανότητα για κόστος πέραν αυτού που δημιουργήθηκε από την αδυναμία ασφάλειας.
- Παραβίαση νομικού ή θεσμικού κανόνα, μη τήρηση συμβατικής υποχρέωσης.
- Αδυναμία επαναλειτουργίας λόγω πολλών ανεκτέλεστων διαδικασιών οι οποίες δεν μπορούν να εκτελεσθούν είτε λόγω χρονικού περιορισμού, είτε επειδή έχουν χαθεί.
- Επιπτώσεις στο ηθικό του προσωπικού.
- Πιθανότητα απάτης.
- Αδυναμία λειτουργίας λόγω απώλειας διαθεσιμότητας των πληροφοριακών πόρων.

Η πιθανότητα εκδήλωσης του κάθε κινδύνου, αφορά στην ύπαρξη και αποτελεσματική λειτουργία κατάλληλων δικλείδων ασφάλειας.

Οι κίνδυνοι που προσδιορίσθηκαν παραπάνω, προκαλούνται από την εκούσια ή ακούσια εκμετάλλευση μιας αδυναμίας ασφάλειας, αποτέλεσμα της οποίας είναι η πρόκληση του κινδύνου. Άρα χρειάζονται αποτελεσματικές δικλείδες ασφάλειας οι οποίες δρουν είτε προληπτικά (δεν αφήνουν την δημιουργία αδυναμιών ασφάλειας), είτε κατασταλτικά περιορίζοντας την επίδραση του αποτελέσματος μιας αδυναμίας ασφάλειας.

4.7 ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΕΠΙΘΕΣΕΩΝ

Οι επιθέσεις που αφορούν τις εφαρμογές χωρίζονται στις παρακάτω κατηγορίες:

Υπερχείλιση Καταχωρητή (Buffer overflow attacks) – Οι επιθέσεις αυτού του τύπου, έχουν σαν στόχο τα components της εφαρμογής τα οποία αποθηκεύουν δεδομένα σε προσωρινό χώρο μνήμης (buffers) μέχρι να έρθει η ώρα τους για επεξεργασία. Συχνά παρατηρούνται περιπτώσεις όπου δεν ελέγχεται επαρκώς ο όγκος του πακέτου με την πληροφορία που θέλουμε να αποθηκευτεί στους καταχωρητές, με αποτέλεσμα να προσπαθούμε να αποθηκεύσουμε πακέτα πληροφοριών με όγκο μεγαλύτερο του διαθέσιμου στον καταχωρητή. Οι επίδοξοι Hackers, βάζουν κώδικα δικής τους κατασκευής στο πακέτο που στέλνεται για αποθήκευση στον καταχωρητή με σκοπό την αντικατάσταση μέρους του κώδικα της εφαρμογής με τις δικές του εντολές.

Σε περίπτωση επιτυχημένης εκτέλεσης των εντολών οι hackers αποκτούν προνόμια πρόσβασης μεγαλύτερα ενός απλού χρήστη της εφαρμογής και καταφέρνουν να αποκτήσουν τον έλεγχο του συστήματος.

Υπάρχουν και περιπτώσεις όπου τα συστατικά στοιχεία της εφαρμογής που δέχονται την επίθεση τύπου υπερχείλισης καταχωρητή, σταματούν την εκτέλεσή τους (crash) με αποτέλεσμα να καθιστούν την εφαρμογή ανενεργή για τους χρήστες.

Επίσης, υπάρχουν περιπτώσεις όπου μπορεί να προκληθεί και απώλεια της διαθεσιμότητας του server στο οποίο λειτουργεί η εφαρμογή και όχι μόνο της εφαρμογής.

Race conditions – Υπάρχουν περιπτώσεις όπου οι εφαρμογές χρειάζεται να έχουν πρόσβαση σε συγκεκριμένα αρχεία, μεταβλητές και δεδομένα. Οι προγραμματιστές ίσως να μην έχουν υλοποιήσει με ορθό τρόπο την ταυτόχρονη και από πολλαπλές οντότητες πρόσβαση και να μην έχουν προγραμματίσει τους κατάλληλους ελέγχους. Πολλές φορές αυτό οδηγεί σε πρόσβαση σε αρχεία ή απευθείας στα δεδομένα μέσω των συστατικών στοιχείων της εφαρμογής.

Εκμετάλλευση των αυξημένων δικαιωμάτων πρόσβασης που έχουν τα συστατικά στοιχεία της εφαρμογής (exploitation of application component privileges) – Τα συστατικά στοιχεία που αφορούν στον εξυπηρετητή μέρος της εφαρμογής, εκτελούνται έχοντας προνόμια πρόσβασης συγκεκριμένης ομάδας & χρήστη. Τα εν λόγο προνόμια πρόσβασης, συνήθως, δεν αντιστοιχούν στον χρήστη που χρησιμοποιεί την εφαρμογή την δεδομένη στιγμή.

Ο συνδυασμός των συστατικών στοιχείων του εξυπηρετητή της εφαρμογής με τις περιπτώσεις υπερχείλισης καταχωρητή και race condition μπορεί να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση και στην συνέχεια σε αύξηση των δικαιωμάτων πρόσβασης.

Χειρισμός του client της εφαρμογής & εκμετάλλευση των αδυναμιών του (client side manipulation) – Υπάρχουν περιπτώσεις, όπου πολλοί από τους ελέγχους που αφορούν στην επιβεβαίωση της ορθότητας και

της αξιοπιστίας των δεδομένων εισόδου (input data validation) μιας εφαρμογής γίνονται μόνο από την μεριά του πελάτη και όχι από τον εξυπηρετητή, για να αυξηθεί η ταχύτητα της επικοινωνίας και η απόδοση της εφαρμογής. Ένας από τους διαδεδομένους τρόπους παραβίασης της ασφάλειας των εφαρμογών είναι η παράκαμψη όλων των ελέγχων που γίνονται στον πελάτη και η εισαγωγή λανθασμένων δεδομένων στον εξυπηρετητή, με σκοπό την εκδήλωση κάποιας από τις παραπάνω περιπτώσεις επιθέσεων ή την αποκάλυψη εμπιστευτικών πληροφοριών ή πληροφοριών που αφορούν στην λειτουργικότητα της εφαρμογής.
Η συγκεκριμένη μέθοδος είναι διαδεδομένη και χρησιμοποιείται κυρίως για την διενέργεια ηλεκτρονικής απάτης σε εφαρμογές ηλεκτρονικού εμπορίου, προσπαθώντας να αλλοιώσουν στοιχεία κατά την διενέργεια συναλλαγών (π.χ αλλαγή τιμών σε προϊόντα).
Αύξηση Προνομίων (Privilege elevation) – Ο επιτιθέμενος προσπαθεί να αυξήσει τα δικαιώματα πρόσβαση τα οποία του αναλογούν σε υψηλότερα. Εάν το κατορθώσει, μπορεί να αποκτήσει πρόσβαση σαν root ή σαν administrator και έχει όλο το σύστημα υπό την κατοχή του.

Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα (Unauthorized data access) – Από τις ποιο δημοφιλής τεχνικές όπου ο επιτιθέμενος αποκτά μη εξουσιοδοτημένη πρόσβαση στα δεδομένα μέσω της εφαρμογής. Η πρόσβαση στα δεδομένα επιτυγχάνεται είτε στους servers στους οποίους είναι αποθηκευμένα, είτε κατά την διακίνησή τους μέσω δικτύου. Τα δεδομένα μπορούν να χρησιμοποιηθούν και για άλλου τύπου επιθέσεις όπως για να προσποιηθεί ο επιτιθέμενος την ταυτότητα κάποιου εξουσιοδοτημένου χρήστη. Η υφαρπαγή συνόδου (session hijacking) είναι μία από τις περιπτώσεις αυτού του τύπου επιθέσεων.

Απώλεια διαθεσιμότητας εφαρμογής (Denial of service) – Η συγκεκριμένη τεχνική επίθεσης είναι περισσότερο γνωστή για την εφαρμογή της σε συστήματα και μηχανισμούς υλοποίησης δικτύων, όμως έχει εφαρμογή και στις εφαρμογές. Αποτέλεσμα της επίθεσης είναι να τεθεί εκτός χρήσης η εφαρμογή και πολλές φορές και το σύστημα στο οποίο η εκάστοτε εφαρμογή λειτουργεί. Εφαρμογές με κακό σχεδιασμό μπορεί να τεθούν εύκολα εκτός λειτουργίας μόνο με κλείδωμα του λογαριασμού που χρησιμοποιεί εσωτερικά η εφαρμογή για να τρέχει.

Τροποποίηση δεδομένων (Data manipulation) – Με την συγκεκριμένη τεχνική τροποποιούνται δεδομένα τα οποία χρησιμοποιούνται από την εφαρμογή με σκοπό την αποκομιδή ιδίου οφέλους ή την αλλοίωση της εικόνας μίας ιστοσελίδας. Πολλές φορές hackers εισβάλουν σε ιστοσελίδες και τροποποιούν το περιεχόμενο και την εμφάνιση των αυτών. Ένα καλό παράδειγμα αυτού του τύπου των επιθέσεων είναι η αλλαγή πεδίων τύπου HIDDEN(hidden field manipulation). Υπάρχουν περιπτώσεις όπου δεδομένα αποθηκεύονται σε κρυφά πεδία ιστοσελίδων. Στην περίπτωση που οι τιμές των πεδίων τύπου hidden (hidden fields) δεν ελέγχονται για επαλήθευση κατά την υποβολή φορμών με δεδομένα από τους χρήστες, είναι πιθανό τα αποτελέσματα να είναι διαφορετικά από τα αναμενόμενα. Για παράδειγμα, εάν στα πεδία τύπου hidden έχουν εισαχθεί οι τιμές των προϊόντων ενός on-

line καταστήματος, κάποιος θα μπορούσε να αλλάξει τις τιμές πριν από την υποβολή της παραγγελίας του με την μορφή της φόρμας που διαθέτει το δικτυακό τόπο.

Πλαστοπροσωπία (Identity spoofing) – Ο επιτιθέμενος κάνει χρήση των στοιχείων πρόσβασης ενός εξουσιοδοτημένου χρήστη. Αυτό μπορεί να είναι αποτέλεσμα των εξής:

1)οι εξουσιοδοτημένοι χρήστες δεν ακολουθούν τους κανόνες προστασίας των κωδικών πρόσβασης, 2) οι κωδικοί πρόσβασης είτε διακινούνται μέσω δικτύου, είτε αποθηκεύονται χωρίς κρυπτογράφηση 3) οι χρήστες χρησιμοποιούν εύκολους κωδικούς.

4.8 ΚΥΡΙΕΣ ΔΙΚΛΕΙΔΕΣ ΑΣΦΑΛΕΙΑΣ ΕΦΑΡΜΟΓΩΝ

Οι κυριότερες δικλείδες ασφάλειας αναφορικά με την ασφάλεια σε επίπεδο εφαρμογών, είναι οι ακόλουθες:

Έλεγχος εγκυρότητας εισαγόμενων και παραγόμενων δεδομένων Τα δεδομένα τα οποία εισάγονται στην εφαρμογή από τους χρήστες, καθώς και αυτά τα οποία παράγονται αποτελούν δίοδο εχθρικού λογισμικού προς και από την εφαρμογή. Τόσο τα εισερχόμενα όσο και τα εξερχόμενα από την εφαρμογή δεδομένα πρέπει να ελέγχονται και να πιστοποιείται ότι είναι τα αναμενόμενα. Η σωστή τακτική ελέγχου είναι η αποδοχή μόνο των δεδομένων που πληρούν συγκεκριμένα κριτήρια και η απόρριψη όλων των υπολοίπων. Συνηθισμένη λανθασμένη τακτική είναι η θέσπιση κριτηρίων απόρριψης με το σκεπτικό της πρόληψης συγκεκριμένων προβλημάτων. Γενικότερα απορρίπτεται οτιδήποτε δεν είναι μέρος των κριτηρίων ελέγχου.

Παροχή ασφάλειας σε περίπτωση βλάβης ή δυσλειτουργίας Οι μηχανισμοί και οι δικλείδες ασφάλειας πρέπει να είναι σχεδιασμένοι έτσι ώστε σε περίπτωση βλάβης ή δυσλειτουργίας να απορρίπτουν οποιαδήποτε διαδικασία ασφάλειας να υλοποιηθεί αντί να την επιτρέπει.

Ευκολία χρήσης – Είναι δεδομένο ότι εάν οι δικλείδες ασφάλειας είναι δύσκολο να υλοποιηθούν ή η εφαρμογή τους δυσκολεύει την χρήση της εφαρμογής, τότε τόσο οι μηχανικοί πληροφορικής όσο και οι χρήστες θα προσπαθούν να βρουν τρόπο είτε να μην τις υλοποιήσουν είτε να τις παρακάμψουν.

Προστασία σε όλα τα επίπεδα – Η ασφάλεια πληροφοριών δεν μπορεί να επιτευχθεί με την εφαρμογή δικλείδων ασφάλειας οι οποίες αφορούν μόνο σε ένα επίπεδο, για παράδειγμα πιστοποίηση ταυτότητας. Υπάρχει ανάγκη για την σε βάθος ανάλυση και κάλυψη όλων των πιθανών σημείων που ενδέχεται να δημιουργήσουν πρόβλημα στην ασφάλεια των δεδομένων της εφαρμογής. Προβλήματα μπορεί να δημιουργηθούν ακόμα και από το πληροφοριακό σύστημα πάνω στο οποίο λειτουργεί η εκάστοτε εφαρμογή.

Ελάχιστα δυνατά δικαιώματα πρόσβασης - Οι εφαρμογές πρέπει να σχεδιάζονται έτσι ώστε να χρειάζονται τα ελάχιστα προνόμια πρόσβασης, προκειμένου να εκτελέσουν τις εσωτερικές τους διεργασίες. Η ορθή προσέγγιση συνεπάγεται την δημιουργία χρηστών και ρόλων και δικαιώματα πρόσβασης ανάλογα των διεργασιών που εκτελούν.

4.9 ΗΛΕΚΤΡΟΝΙΚΗ ΤΡΑΠΕΖΙΚΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΤΡΑΠΕΖΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ

Εκτός από τις αγορές στο Internet μέσω πιστωτικών καρτών, η χρήση ηλεκτρονικών τραπεζικών υπηρεσιών, ή αλλιώς e-Banking, μπορούν να κάνουν την ζωή πολύ εύκολη, ειδικά όταν πρόκειται για τυπικές πληρωμές τηλεφωνικών λογαριασμών, ασφαλιστικών εισφορών, κτλ. Πόσο ασφαλείς είναι όμως οι υπηρεσίες e-Banking και πόσο διαφέρουν από την χρήση πιστωτικών καρτών στο Internet;

1. Ηλεκτρονικές συναλλαγές μέσω ηλεκτρονικής τραπεζικής

Στην περίπτωση της ηλεκτρονικής τραπεζικής πράγματα είναι κάπως πιο περίπλοκα στο θέμα της εταιρικής/τραπεζικής ευθύνης, αλλά εδώ υπάρχει σαφώς αυστηρότερος έλεγχος από την ίδια την τράπεζα σε ότι αφορά το επίπεδο ασφάλειας των συναλλαγών, σε σχέση με την αντίστοιχη ηλεκτρονική χρήση των πιστωτικών καρτών. Πρακτικά, η τράπεζα επιβάλλει μια σειρά πρόσθετων μηχανισμών ασφαλείας που δεν υπάρχουν στην περίπτωση των πιστωτικών καρτών, πράγμα που κάνει το σύστημα ουσιαστικά απαραβίαστο αν η χρήση των μηχανισμών αυτών είναι σωστή από την πλευρά του πελάτη (π.χ. χρήση λίστας κωδικών TAN, Transaction Authorization Numbers – Αριθμοί Εξουσιοδότησης Συναλλαγής).

Παρόλα αυτά, αν ο πελάτης κατά λάθος καταστεί θύμα απάτης από ιστοσελίδες παραποίησης ταυτότητας, δηλαδή δώσει τα στοιχεία του σε κόμβο που προσποιείται ότι είναι αυτός της τράπεζας, η ίδια η τράπεζα λέει ότι εφόσον έχει ενημερώσει σχετικά τον πελάτη της και αυτός έκανε κάτι εκτός του δικού της δικτύου, δεν φέρει καμία απολύτως ευθύνη (εδώ δεν ισχύει η αρχή της απόδειξης της μη-εντιμότητας όπως για τις πιστωτικές κάρτες). Μάλιστα, στους όρους χρήσης της λίστας κωδικών TAN γνωστής τράπεζας αναφέρεται ρητά ότι:

"...Κανένας άλλος δεν πρέπει να γνωρίζει τους αριθμούς TAN. Η τράπεζα δεν φέρει καμία ευθύνη, για συναλλαγές που έγιναν από άλλο πρόσωπο, παρά τη θέλησή σας, σε περίπτωση απώλειας ή διαρροής αριθμών TAN..."

Με άλλα λόγια, η τράπεζα καλύπτει το δικό της μερίδιο της ευθύνης με την προσφορά αυτού του πρόσθετου (υποχρεωτικού) μέτρου ασφάλειας, αλλά έγκειται στον ίδιο τον χρήστη να διαφυλάξει την σωστή εφαρμογή του.

Θα πρέπει πάντως να σημειωθεί πως σήμερα το επίπεδο κατάρτισης του προσωπικού των τραπεζών και, αντίστοιχα, της ενημέρωσης των πελατών τους σχετικά με την διάθεση και χρήση των νέων συσκευών

παραγωγής κωδικών TAN μιας χρήσης, είναι τουλάχιστον τραγική. Για παράδειγμα, η προμήθεια των αντίστοιχων συσκευών TAN χρεώνεται στον πελάτη ως πρόσθετη προαιρετική υπηρεσία (όπως δηλαδή οι πιστωτικές κάρτες), χωρίς όμως να παρέχεται μαζί αναλυτικό ούτε εγχειρίδιο οδηγιών, ούτε οι αναλυτικές τεχνικές προδιαγραφές, ούτε καν οι αναλυτικοί όροι χρήσης όπου καθορίζονται τα όρια ευθύνης του κάθε μέρους (της τράπεζας και του πελάτη). Αυτό ίσως να οφείλεται στο γεγονός ότι η διάδοση και η χρήση παρόμοιων διαδικασιών στις ηλεκτρονικές συναλλαγές είναι ακόμη πολύ πρώιμη στην Ελλάδα, με αποτέλεσμα το αντίστοιχο ενδιαφέρον να είναι περιορισμένο, τόσο από την μεριά των πελατών, που συνήθως δεν επιδιώκουν περαιτέρω ενημέρωση, όσο και από την ίδια την τράπεζα, που δεν θέλει να επωμιστεί το βάρος και το κόστος της "εκπαίδευσης" των πελατών σε αυτά τα νέα συστήματα.

2. Κωδικοί TAN – Χρησιμότητα και τρόπος λειτουργίας

Εδώ θα πρέπει να αναφερθούν μερικά πράγματα σχετικά με τον λόγο για τον οποίο οι κωδικοί TAN είναι πλέον απαραίτητοι σε κάθε συναλλαγή ηλεκτρονικής τραπεζικής. Αντίθετα με τις πιστωτικές κάρτες, στο e-Banking η κάθε τράπεζα έχει τον απόλυτο έλεγχο της πολιτικής και των μηχανισμών ασφάλειας που επιθυμεί να εφαρμόσει. Έτσι, μπορεί να επιβάλλει την εξουσιοδότηση κάθε εγχρήματης συναλλαγής ξεχωριστά με ειδικό κωδικό μιας χρήσης. Αυτό στην πράξη γίνεται με την χορήγηση λίστας πρόσθετων κωδικών εξουσιοδότησης στους πελάτες της ηλεκτρονικής τραπεζικής κάτι σαν κωδικός πρόσβασης μιας χρήσης προσωπικά σε κάθε πιστοποιημένο πελάτη της.

Το πλεονέκτημα των κωδικών TAN είναι ότι, εν γένει, πρόκειται για κωδικούς οι οποίοι δεν αποθηκεύονται πουθενά στο σύστημα του χρήστη-πελάτη αλλά αντίθετα βρίσκονται σε τυπωμένη μορφή, άρα είναι αδύνατο να υποκλαπούν ηλεκτρονικά από το σύστημά του. Αντίστοιχα, στο σύστημα ηλεκτρονικής τραπεζικής της τράπεζας όπου τηρούνται αντίγραφα των κωδικών αυτών για αντιπαραβολή, υπάρχουν τα κατάλληλα μέτρα εξασφάλισης της εμπιστευτικότητας σε πολύ υψηλό επίπεδο, ώστε αντίστοιχα η κλοπή τους, φυσική ή ηλεκτρονική, να είναι ουσιαστικά ανέφικτη. Κατά συνέπεια, ακόμα και αν ο κύριος κωδικός (username/password) του χρήστη-πελάτη παραβιαστεί και κάποιος τρίτος αποκτήσει πρόσβαση στον λογαριασμό ηλεκτρονικής τραπεζικής, δεν μπορεί να κάνει καμία εγχρήματη συναλλαγή αφού δεν διαθέτει αντίστοιχους έγκυρους κωδικούς TAN.

3. Τρόπος λειτουργίας των κωδικών TAN και MAC

Η λογική της λειτουργίας των κωδικών TAN βασίζονται στην ιδέα της κρυπτογράφησης μέσω κωδικοβιβλίων (codebooks) μιας χρήσης ή αλλιώς συστημάτων one-time-pads, τα οποία είναι τα μόνα μοντέλα κρυπτογράφησης των οποίων το απαραβίαστο εξασφαλίζεται 100% και αποδεικνύεται θεωρητικά. Γι’ αυτό άλλωστε χρησιμοποιούνται ακόμη και

σήμερα σε μερικούς τύπους στρατιωτικών επικοινωνιών (συστήματα χαμηλού ρυθμού μετάδοσης).

Στην περίπτωση των κωδικών TAN, τα κωδικοβιβλία δεν χρησιμοποιούνται για κρυπτογράφηση αλλά απλώς για την χορήγηση κωδικών "γνησιότητας". Αυτή η μορφή αναφέρεται συχνά ως Κωδικός Αυθεντικοποίησης Μηνύματος (MAC – Message Authentication Code), ο οποίος συνοδεύει κάθε μήνυμα και χρησιμοποιείται για την διάκριση των γνήσιων από τα πλαστά μηνύματα. Για να εξασφαλιστεί η κρυπτασφάλεια των "γνήσιων" κωδικών, υπάρχει μια κοινή λίστα μυστικών κωδικών στα δύο άκρα της επικοινωνίας, δηλαδή ένα κωδικοβιβλίο με κωδικούς μιας χρήσης, τους οποίους χρησιμοποιούν και διασταυρώνουν για τον έλεγχο κάθε μηνύματος.

Εντούτοις, το βασικό πρόβλημα είναι η μεταφορά και αποθήκευση των αντίστοιχων κωδικοβιβλίων με ασφαλή τρόπο και στα δύο μέρη που επικοινωνούν. Στους κωδικούς TAN αυτό εξασφαλίζεται από την ίδια την τράπεζα, απαιτώντας την προσωπική ταυτοποίηση και παράδοση της λίστας TAN στον ίδιο τον πελάτη αυτοπροσώπως, και μάλιστα σε μορφή εν γένει μη-αποθηκεύσιμη στον Η/Υ του. Όμως η διαδικασία έκδοσης και προσωπικής παραλαβής της λίστας TAN είναι συχνά χρονοβόρα και δυσχερής, μια και ακυρώνει μέρος της ίδιας της έννοιας της ηλεκτρονικής τραπεζικής.

Για την εξασφάλιση της κρυπτασφάλειας του συστήματος των MAC και ταυτόχρονα την άμεση συσχέτισή τους με το ίδιο το περιεχόμενο του μηνύματος, συχνά εφαρμόζονται δύο πρόσθετα στάδια επεξεργασίας και ένα μοναδικό μυστικό κλειδί, έτσι ώστε να μην χρειάζεται η χρήση ειδικού κωδικοβιβλίου όπως προβλέπει το αρχικό μοντέλο των one-time-pads. Συγκεκριμένα, το περιεχόμενο του μηνύματος περνά μέσα από μια διαδικασία επεξεργασίας που ονομάζεται Συνάρτηση Κατακερματισμού "Μη Αντιστρέψιμη" ή "Μιας Κατεύθυνσης" (One-Way Hashing Function). Η διαδικασία αυτή αντιστοιχεί το σύνολο των δεδομένων του μηνύματος σε έναν μοναδικό κωδικό αναγνώρισης συγκεκριμένου μεγέθους (π.χ. 128 ή 256 bits), από τον οποίο δεν μπορεί να εξαχθεί το περιεχόμενο του αρχικού μηνύματος με κανέναν τρόπο λόγω των μαθηματικών ιδιοτήτων της συγκεκριμένης συνάρτησης. Επιπλέον, είναι σχεδόν αδύνατο η συνάρτηση αυτή να δημιουργήσει τον ίδιο κωδικό αναγνώρισης για δύο διαφορετικά μηνύματα.

Στη συνέχεια, ο κωδικός αυτός κρυπτογραφείται με το μοναδικό μυστικό κλειδί κρυπτογράφησης πριν μεταδοθεί στο κανάλι μετάδοσης. Η διαδικασία ονομάζεται Keyed HMAC (Hashed Message Authentication Code with Key) και ουσιαστικά κάνει περιττή την χρήση ειδικών κωδικοβιβλίων τύπουone-time-pad για αυτό το σκοπό, διατηρώντας εξαιρετικά μικρή θεωρητικά (αλλά όχι αδύνατη πλέον, όπως στο one-time-pad) την πιθανότητα παραβίασης της κρυπτασφάλειας του συστήματος.

Με το σύστημα των keyed-HMAC εξασφαλίζεται ότι (α) κανένας δεν μπορεί να "πειράξει" το αρχικό μήνυμα χωρίς να "ακυρώσει" το συγκεκριμένο κωδικό αυθεντικοποίησης του μηνύματος και (β) ότι κανένας

άλλος δεν μπορεί να παράγει γνήσιους κωδικούς αυθεντικοποίησης εφόσον δεν διαθέτει το αντίστοιχο μυστικό κλειδί. Στην πράξη, το μοντέλο αυτό εφαρμόζεται στις επικοινωνίες σαν ένας εύκολη και γρήγορη εναλλακτική λύση έναντι της εφαρμογής των πιο πολύπλοκων και εξειδικευμένων μοντέλων ψηφιακών υπογραφών (digital signatures).

4. Συσκευές δημιουργίας κωδικών TAN

Σε αναλογία με την εφαρμογή των keyed-HMAC για την αντικατάσταση των κωδικοβιβλίων, υπάρχουν τρόποι να αντικατασταθεί η εκτυπωμένη λίστα TAN με αντίστοιχη συσκευή παραγωγής μεμονωμένων κωδικών από τον ίδιο τον πελάτη, πάντα απομονωμένη από τον H/Y τον οποίο χρησιμοποιεί για την πρόσβαση στο σύστημα e-Banking, και φυσικά σε συσχέτιση με αντίστοιχο μηχανισμό διασταύρωσής τους από το σύστημα της τράπεζας. Πρακτικά αυτό υλοποιείται με ένα συνδυασμό τριών πραγμάτων:

1. Μια γεννήτρια ψευδοτυχαίων αριθμών (PRNG)
2. Ένα κύκλωμα χρονισμού υψηλής ακρίβειας (CLOCK)
3. Ένα μυστικό ηλεκτρονικό κλειδί της τράπεζας (KEY)

Ο ακριβής τρόπος λειτουργίας είναι αρκετά πολύπλοκος για να εξηγηθεί πλήρως σε κάποιον μη-ειδικό, αλλά η βασική διαδικασία είναι η εξής:
Η γεννήτρια PRNG χρειάζεται έναν αρχικό κωδικό για να ξεκινήσει και στην συνέχεια μπορεί να παράγει αριθμούς οι οποίοι είναι "επαρκώς τυχαίοι" ώστε να μην είναι προβλέψιμοι με κανέναν τρόπο αν κάποιος δεν γνωρίζει τον κωδικό αρχικοποίησης. Αυτό είναι αρμοδιότητα της τράπεζας, δηλαδή να αρχικοποιεί τις συσκευές αυτές έτσι ώστε να μπορεί να "αναπαράγει" μόνο η ίδια την ακολουθία των αριθμών αυτών.

Επιπλέον, το κύκλωμα CLOCK μπορεί να χρησιμοποιηθεί για να αρχικοποιεί και πάλι την συσκευή σε τακτά χρονικά διαστήματα, τα οποία επίσης γνωρίζει η τράπεζα χωρίς να χρειάζεται περαιτέρω επικοινωνία ή σύνδεση με την συσκευή του πελάτη. Αυτό γιατί αρκεί απλά το CLOCK ή "ρολόι" της συσκευής TAN να είναι συγχρονισμένο με αυτό του συστήματος της τράπεζας. Για το λόγο αυτό το κύκλωμα CLOCK της κάθε συσκευής TAN πρέπει να είναι υψηλής πιστότητας, με ελάχιστη απόκλιση (π.χ. 60 δευτερόλεπτα max) στη διάρκεια ζωής της συσκευής (π.χ. 3 χρόνια).

Με τους δύο παραπάνω μηχανισμούς, δηλαδή τον κωδικό αρχικοποίησης του κυκλώματος PRNG και το κύκλωμα CLOCK για την περιοδική επανα-αρχικοποίηση, η συσκευή TAN μπορεί να παράγει πλέον "τυχαίους" κωδικούς TAN, προβλέψιμους μόνο από το αντίστοιχο σύστημα της ίδιας της τράπεζας.

Όμως, η τράπεζα πρέπει σαν πρόσθετο μέτρο ασφάλειας να μπορεί να ελέγχει την γνησιότητα των κωδικών TAN που εισάγει ο χρήστης-πελάτης της, για να αποκλειστεί η περίπτωση κάποιος να "ανακαλύψει" τις λεπτομέρειες σχεδίασης και αρχικοποίησης των κυκλωμάτων PRNG και CLOCK της συσκευής TAN και να κατασκευάσει μια δική του, μη-πιστοποιημένη συσκευή για την παραγωγή ψευδών αλλά

επαληθεύσιμων κωδικών. Για το λόγο αυτό, το αποτέλεσμα των PRNG/CLOCK συνδυάζεται με το τρίτο στοιχείο του μηχανισμού, δηλαδή ένα μυστικό κλειδί KEY, οποίο γνωρίζει μόνο η τράπεζα και το οποίο είναι αποθηκευμένο μέσα στη συσκευή TAN, χωρίς να υπάρχει πρόσβαση σε αυτό από τον χρήστη-πελάτη.

Σε μερικές περιπτώσεις στην παραπάνω διαδικασία υπάρχει και μια δεύτερη φάση, η οποία περιλαμβάνει την παραγωγή ενός πρόσθετου μικρότερου κωδικού ελέγχου (CHECK) μετά από κάθε κωδικό TAN. Αυτό γίνεται για να ενημερώσει τον χρήστη-πελάτη για την επιτυχημένη και έγκυρη ολοκλήρωση της συναλλαγής στο σύστημα e-Banking της τράπεζας. Με άλλα λόγια, ο πελάτης είναι αυτός που τώρα συγκρίνει τον κωδικό ελέγχου CHECK που επιστρέφει το σύστημα ηλεκτρονικής τραπεζικής της τράπεζας για να διαπιστώσει ότι όλα πήγαν καλά.

Τέλος, για την εξασφάλιση της ίδιας της συσκευής υπάρχει εσωτερικά φυσικός μηχανισμός "αυτοκαταστροφής" της συσκευής TAN σε περίπτωση που παραβιαστεί με φυσικό τρόπο. Αν δηλαδή κάποιος επιχειρήσει να την ανοίξει για να "διαβάσει" τα αντίστοιχα ηλεκτρονικά κυκλώματα, οι σημαντικές πληροφορίες (π.χ. KEY) διαγράφονται αυτόματα και μόνιμα από την συσκευή TAN, ώστε η ανάκτησή τους να είναι αδύνατη. Επιπλέον, ως μέρος των παραπάνω μηχανισμών, η τράπεζα αναγνωρίζει κάθε μεμονωμένη συσκευή TAN με έναν μοναδικό σειριακό αριθμό, που βρίσκεται στο πίσω μέρος της, και που "δεσμεύει" τη συγκεκριμένη συσκευή με τον λογαριασμό του αντίστοιχου πελάτη-χρήστη.

4. Πρακτική χρήση και περιορισμοί κωδικών TAN

Σήμερα, οι συσκευές TAN που διατίθενται από τις ελληνικές τράπεζες ενσωματώνουν τους παραπάνω βασικούς μηχανισμούς με κατάλληλο τρόπο, όχι πάντα ταυτόσημο. Για παράδειγμα, σε κάποιες περιπτώσεις οι συσκευές TAN παράγουν κωδικούς μιας χρήσης μόνο μετά από αίτημα του χρήστη (πάτημα ενός ενσωματωμένου πλήκτρου), ενώ άλλες παράγουν συνεχώς κωδικούς οι οποίοι ανανεώνονται αυτόματα κάθε 60 δευτερόλεπτα, είτε χρησιμοποιούνται είτε όχι. Γενικά δεν υπάρχει διαφορά στο επίπεδο ασφάλειας που προσφέρουν, όμως οι ίδιες οι συσκευές TAN έχουν ένα συγκεκριμένο χρονικό διάστημα (ή αντίστοιχα πλήθος παραγόμενων κωδικών) "ασφαλούς χρήσης", πέρα από το οποίο η "τυχαιότητά" τους δεν θεωρείται πλέον εξασφαλισμένη. Συνήθως το διάστημα αυτό είναι 3 χρόνια ή 2 εκατομμύρια κωδικοί TAN. Σε αυτή την περίπτωση, η συσκευή είτε αντικαθίσταται με νέα είτε αρχικοποιείται και πάλι από την τράπεζα με νέους κωδικούς και είναι έτοιμη για χρήση για άλλο τόσο διάστημα, δηλαδή σαν να ήταν καινούργια.

ΣΤΟ ΚΕΦΑΛΑΙΟ 4 ΧΡΗΣΙΜΟΠΟΙΗΘΗΚΑΝ ΟΙ ΠΗΓΕΣ 2,5,6,7,8

ΚΕΦΑΛΑΙΟ 5
ΠΡΟΗΓΜΕΝΑ ΣΥΣΤΗΜΑΤΑ ΕΠΕΞΕΡΓΑΣΙΑΣ ΣΥΝΑΛΛΑΓΩΝ ΒΑΣΙΣΜΕΝΑ ΣΕ ΤΕΧΝΟΛΟΓΙΕΣ ΙΣΤΟΥ

5.1 ΤΕΧΝΟΛΟΓΙΕΣ ΥΠΗΡΕΣΙΩΝ ΙΣΤΟΥ

Εφαρμογές που αλληλεπιδρούν μεταξύ τους, μέσω του ιστού πρέπει να είναι ικανές να βρίσκουν η μια την άλλη, να ανακαλύπτουν πληροφορίες που τις επιτρέπει να αλληλοσυνδέονται, να καθορίζουν ποιες είναι οι αναμενόμενες μορφές αλληλοσύνδεσης και να διαπραγματεύονται ποιότητες υπηρεσίας όπως η ασφάλεια και η αξιόπιστη επικοινωνία. Μερικές από αυτές τις ποιότητες υπηρεσίας καλύπτονται με τις υπάρχουσες τεχνολογίες και τα προτεινόμενα πρότυπα ενώ άλλες όχι. Γενικά η κοινότητα υπηρεσιών ιστού εργάζεται για να αντιμετωπίσει όλες αυτές τις απαιτήσεις, αλλά είναι μια εξελικτική διαδικασία, όπως ακριβώς ο ίδιος ο ιστός. Η υποδομή και τα πρότυπα σχεδιάζονται και αναπτύσσονται από την αρχή για να είναι επεκτάσιμα, όπως η XML. Οι υπηρεσίες ιστού απαιτούν αρκετές συγγενικές τεχνολογίες βασισμένες στην XML για να μεταφέρουν και να μετασχηματίζουν δεδομένα μέσα και έξω από προγράμματα και βάσεις δεδομένων.

5.1.1 EXTENSIBLE MARKUP LANGUAGE (XML)

Η γλώσσα XML αναπτύχθηκε από μια Ομάδα Εργασίας κάτω από την επίβλεψη του διεθνούς οργανισμού World Wide Web Consortium (W3C) το 1996. Εδραιώθηκε από τον John Bosak της Sun Microsystems. Η XML σχεδιάστηκε για να ξεπεράσει περιορισμούς της HyperText Markup Language (HTML) και ειδικότερα να υποστηρίξει καλύτερα τη δημιουργία και τη διαχείριση δυναμικού περιεχομένου. Επιπλέον δίνει στα έγγραφα ένα μεγαλύτερο επίπεδο προσαρμοστικότητας στη μορφή και τη δομή από αυτό που υπήρχε παλαιότερα στην HTML. Η XML προσφέρει στους σχεδιαστές της HTML τη δυνατότητα να προσθέτουν περισσότερα στοιχεία στη γλώσσα.. Στην HTML οι ετικέτες (tags) είναι προκαθορισμένες, ενώ η XML παρέχει τη δυνατότητα στους χρήστες να καθορίζουν τις ετικέτες.

Η XML είναι markup γλώσσα για έγγραφα που περιέχουν δομημένες πληροφορίες. Η markup γλώσσα είναι ένας μηχανισμός που καθορίζει δομές σε ένα έγγραφο. Οι δομημένες πληροφορίες περιλαμβάνουν περιεχόμενο και κάποιες διευκρινίσεις για το ρόλο του περιεχόμενου. Σχεδόν όλα τα έγγραφα έχουν την ίδια δομή. Στην πραγματικότητα, η XML είναι κάτι περισσότερο από markup γλώσσα, είναι μεταγλώσσα, δηλαδή μια γλώσσα που χρησιμοποιείται για να καθορίσει νέες markup γλώσσες.

Όλο και περισσότερές εφαρμογές χρησιμοποιούν XML για να αποθηκεύσουν πληροφορίες λόγω των πλεονεκτημάτων της, κάποια εκ των οποίων είναι:

• Η δομή είναι καθορισμένη με σαφήνεια και μπορεί να περάσει μεταξύ διαφορετικών υπολογιστικών συστημάτων, που ειδάλλως θα ήταν ανίκανα να επικοινωνήσουν.

• Το «ωφέλιμο φορτίο» δεδομένων είναι εμφωλευμένο σε ετικέτες και επομένως αναγνώσιμο από τους χρήστες.

• Λόγω της κειμενικής φύσης τους, τα αρχεία XML είναι δεν εξαρτώνται από την πλατφόρμα του συστήματος.

Τα πλεονεκτήματα αυτά, έκαναν την XML το πλέον κατάλληλο πρότυπο για επικοινωνία μεταξύ υπηρεσιών ιστού. Για να εξασφαλιστεί μια χρήση ανεξάρτητη από πλατφόρμα και γλώσσα για κάθε υπηρεσία ιστού, αναπτύχθηκε το SOAP, το οποίο είναι μια XML εφαρμογή με καθορισμένα στοιχεία και μια προκαθορισμένη δομή.

5.1.2 SIMPLE OBJECT ACCESS PROTOCOL (SOAP)

Η μεταφορά δεδομένων έχει κεντρική σημασία στο δικτυωμένο και κατανεμημένο περιβάλλον του παγκόσμιου ιστού. Καθώς η XML έχει προκύψει ως η καταλληλότερη μορφή δεδομένων, η πρόκληση για τον αποστολέα και για τον παραλήπτη είναι να συμφωνήσουν στο πρωτόκολλο μεταφοράς, είτε αυτή πρόκειται να γίνει ανάμεσα σε προγράμματα λογισμικού, είτε ανάμεσα σε μηχανήματα ή οργανισμούς.

Το SOAP είναι ένα πρωτόκολλο σχεδιασμένο για την ανταλλαγή XML εγγράφων μέσω διαφορετικών πρότυπων τεχνολογιών διαδικτύου, συμπεριλαμβανομένων των HTTP, Simple Mail Transfer Protocol (SMTP) και File Transfer Protocol (FTP).

Το SOAP είναι βασικά ένα μοντέλο μονόδρομης επικοινωνίας, το οποίο εγγυάται ότι ένα μήνυμα μεταφέρεται από τον αποστολέα στον παραλήπτη, ενδεχομένως περιλαμβάνοντας ενδιάμεσους σταθμούς που μπορούν να επεξεργαστούν μέρος του μηνύματος ή να το μεταβάλουν.

Ένα μήνυμα SOAP είναι ένα συνηθισμένο XML έγγραφο, το οποίο περιέχει τα ακόλουθα στοιχεία :

• Envelope, το οποίο προσδιορίζει ότι το έγγραφο XML είναι ένα μήνυμα SOAP.

Καθορίζει την αρχή και το τέλος του μηνύματος.

• Header, το οποίο περιέχει πληροφορίες επικεφαλίδας. Είναι ένας ευέλικτος μηχανισμός για πρόσθεση χαρακτηριστικών στο SOAP μήνυμα.

• Body, το οποίο παρέχει έναν απλό μηχανισμό για ανταλλαγή υποχρεωτικών πληροφοριών που προορίζονται για τον τελικό αποδέκτη του μηνύματος.

• Fault, το οποίο περιέχει πληροφορίες για λάθη που τυχόν εμφανίστηκαν κατά την επεξεργασία του μηνύματος. Αυτό το στοιχείο εμφανίζεται μόνο σε απαντητικά μηνύματα και δεν πρέπει να εμφανίζεται πάνω από μία φορά μέσα στο Body του μηνύματος.

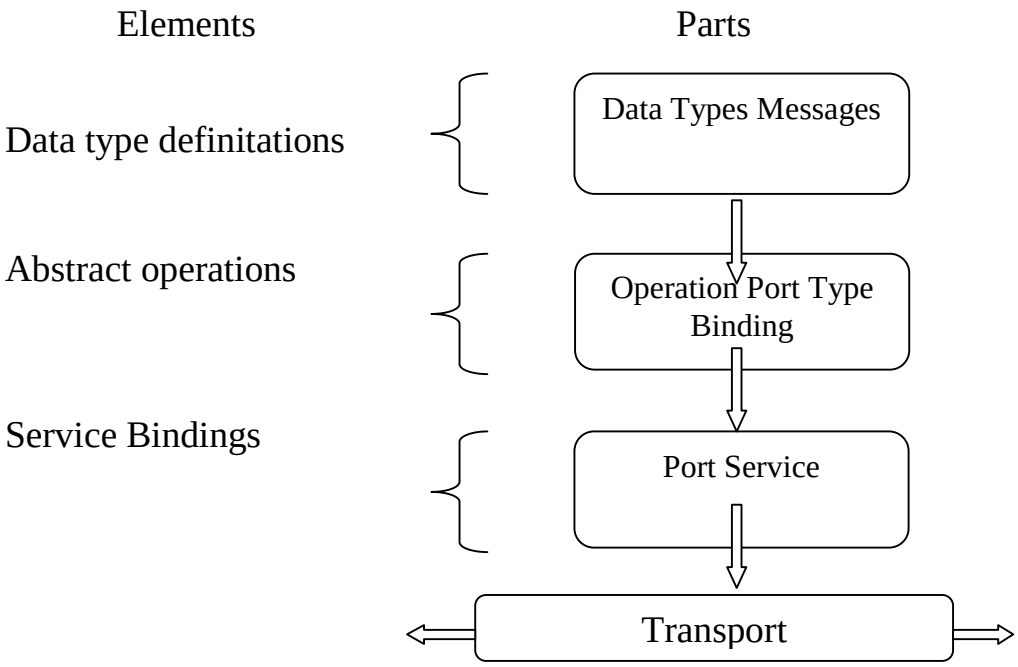
Συνοψίζοντας, το SOAP είναι ένα πρωτόκολλο βασισμένο σε XML για την αποστολή μηνυμάτων και την παραγωγή κλήσεων απομακρυσμένων διαδικασιών μέσα σε ένα κατανεμημένο περιβάλλον.

5.2 WEB SERVICES DESCRIPTI

Το επόμενο βήμα για να ολοκληρωθεί η αρχιτεκτονική επικοινωνίας των υπηρεσιών ιστού είναι να καθοριστεί το πως οι χρήστες θα έχουν πρόσβαση σε μία υπηρεσία μόλις αυτή τεθεί σε εφαρμογή. Εδώ είναι που παρεμβαίνει η WSDL προδιαγραφή. Αυτή παρέχει ένα συμβόλαιο μεταξύ του αιτούντος και του παροχέα της υπηρεσίας.

Η WSDL αναπτύχθηκε αρχικά από τη Microsoft και την IBM και υποβλήθηκε στο W3C από 25 εταιρείες. Βρίσκεται στην «καρδιά» του μοντέλου των υπηρεσιών του ιστού, παρέχοντας ένα κοινό τρόπο στον οποίο παρουσιάζονται οι τύποι των δεδομένων που λαμβάνουν χώρα στα μηνύματα, οι λειτουργίες οι οποίες πρόκειται να εκτελεστούν στα μηνύματα και η αντιστοίχηση των μηνυμάτων πάνω σε συναλλαγές του δικτύου. Η WSDL έχει XML μορφή, η οποία περιγράφει τι κάνει μια υπηρεσία, πως υλοποιεί τις λειτουργίες της και που θα τη βρούμε.

Η WSDL διαιρείται σε τρία βασικά στοιχεία και επτά τμήματα τα όποια είναι: τα data type definitions, τα abstract operations και τα service bindings (Σχήμα 1). Κάθε βασικό στοιχείο μπορεί να καθοριστεί σε ένα ξεχωριστό XML έγγραφο και να εισαχθεί σε διαφορετικούς συνδυασμούς για να δημιουργήσει μια τελική περιγραφή υπηρεσιών ιστού ή μπορεί όλα να οριστούν σε ένα μόνο έγγραφο. Τα data type definitions (Data types, Messages) προσδιορίζουν τη δομή και το περιεχόμενο των μηνυμάτων. Τα Abstract Operations (Operations, Port Types, Binding) προσδιορίζουν τις λειτουργίες που εκτελούνται στο περιεχόμενο του μηνύματος και τα Service Bindings (Port, Service) προσδιορίζουν τη μετάδοση δεδομένων, η οποία θα μεταφέρει το μήνυμα στον προορισμό του.



Εικόνα 6: Τα τρία βασικά στοιχεία και τα επτά τμήματα του WSDL

5.3 UNIVERSAL DESCRIPTION, DISCOVERY AND INTEGRATION (UDDI)

Το UDDI ως τεχνική προδιαγραφή παρέχει μια μέθοδο για δημοσίευση και εύρεση των περιγραφών μιας υπηρεσίας. Είναι μια κεντρική υπηρεσία καταλόγου, όπου υπηρεσίες ιστού μπορούν να καταχωρηθούν και να προσδιοριστούν σε έναν παροχέα υπηρεσιών. Είναι μια πρωτοβουλία των εταιρειών IBM, Ariba και Microsoft που το Σεπτέμβριο του 2000 εξέδωσαν την έκδοση 1.0 του UDDI, η οποία επέτρεπε στις επιχειρήσεις τη γρήγορη και δυναμική εύρεση καθώς και συναλλαγή με κάθε άλλη υπηρεσία. Ακολούθησε το UDDI 2.0 το Μάιο του 2001, με επιπλέον χαρακτηριστικά, όπως η υποστήριξη μιας υπηρεσίας ιστού από πολλές γλώσσες διεθνώς και το βελτιωμένο σύνολο επιλογών αναζήτησης. Σήμερα το UDDI βρίσκεται στην έκδοση 3.0.2.

Η δομή των δεδομένων τα οποία αποθηκεύονται στον κατάλογο είναι σε μορφή XML. Τα δεδομένα τα οποία συλλέγονται εντός του καταλόγου χωρίζονται σε τρεις κατηγορίες: λευκές σελίδες (white pages), κίτρινες σελίδες (yellow pages) και πράσινες σελίδες (green pages). Οι λευκές σελίδες περιέχουν γενικές πληροφορίες όπως το όνομα, η περιγραφή, η διεύθυνση επικοινωνίας και μοναδικούς αναγνωριστές όπως είναι οι D-U-N-S αριθμοί ή τα IDs για μια εταιρεία που προσφέρει την υπηρεσία. Αυτές οι πληροφορίες επιτρέπουν σε άλλους να ανακαλύψουν την υπηρεσία ιστού της εταιρείας βασισμένοι πάνω σε κάποιο στοιχείο αναγνώρισης. Οι κίτρινες σελίδες περιέχουν πληροφορίες οι οποίες περιγράφουν μια υπηρεσία χρησιμοποιώντας διαφορετικές κατηγοριοποιήσεις. Αυτές οι πληροφορίες επιτρέπουν στους άλλους χρήστες να ανακαλύψουν την υπηρεσία βασισμένοι στην κατηγοριοποίηση της (π.χ. είναι μια εταιρεία πώλησης ή κατασκευής αυτοκινήτων). Οι πράσινες σελίδες περιλαμβάνουν λεπτομερείς

τεχνικές πληροφορίες για μια υπηρεσία ιστού, επιτρέποντας κάποιον να υλοποιήσει μια εφαρμογή για να χρησιμοποιεί την υπηρεσία ιστού. Αυτές οι τρεις κατηγορίες καταφέρνουν να κάνουν εύκολη την αναζήτηση για συγκεκριμένες υπηρεσίες ιστού.

5.4 ΑΣΦΑΛΕΙΑ ΣΕ ΥΠΗΡΕΣΙΕΣ ΙΣΤΟΥ

Η ασφάλεια είναι ένα από τα ποιο σημαντικά και σύνθετα θέματα που αντιμετωπίζει το διαδίκτυο και οι υπηρεσίες ιστού. Η ασφάλεια πρέπει να εξασφαλίσει την εμπιστευτικότητα και την ακεραιότητα των δεδομένων στις υπηρεσίες ιστού. Κανένας άλλος πέραν του παραλήπτη των δεδομένων δεν επιτρέπεται να εξετάσει ή να επέμβει στο περιεχόμενο του μηνύματος. Ακόμη είναι απαραίτητο να ελέγχεται η προσπέλαση στις υπηρεσίες ιστού, ειδικά όταν πολλές υπηρεσίες ιστού χρησιμοποιούνται μαζί, έτσι ώστε μόνο αυτοί που είναι εξουσιοδοτημένοι να μπορούν να τις χρησιμοποιούν.

5.5 XML ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

Οι XML ψηφιακές υπογραφές (XML Digital Signatures) είναι ένα πρότυπο για την ασφαλή επικύρωση της προέλευσης των μηνυμάτων. Η προδιαγραφή της XML υπογραφής επιτρέπει στα έγγραφα XML να υπογραφούν με ένα τυποποιημένο τρόπο, χρησιμοποιώντας διαφορετικούς αλγόριθμους ψηφιακής υπογραφής. Οι ψηφιακές υπογραφές μπορούν να χρησιμοποιηθούν για επικύρωση των μηνυμάτων και για μη-αποποίηση.

Το πρότυπο XML υπογραφής παρέχει ένα σύνολο κανόνων και μια XML σύνταξη για την κωδικοποίηση, τον υπολογισμό και την επαλήθευση των ψηφιακών υπογραφών από τα αυθαίρετα δεδομένα. Εκτός από την παροχή πιστοποίησης, ακεραιότητας δεδομένων και υποστήριξη για μη αποποίηση των δεδομένων που υπογράφονται, η XML υπογραφή έχει σχεδιαστεί για να εκμεταλλεύεται το διαδίκτυο και την XML. Ένα θεμελιώδες χαρακτηριστικό γνώρισμα της XML υπογραφής είναι η δυνατότητα να υπογράφει συγκεκριμένα τμήματα του XML εγγράφου, αντί για το πλήρες έγγραφο. Αυτό γίνεται χρήσιμο όταν τα έγγραφα αθροίζουν πολλά κομμάτια πληροφορίας από διαφορετικές πηγές, κάθε ένα με τη δική του απόδειξη αυθεντικότητας.

Η επικύρωση μιας υπογραφής απαιτεί ότι τα υπογεγραμμένα δεδομένα είναι προσιτά με κάποιο είδος αναφοράς. Αυτή η αναφορά μπορεί να είναι ένα URI, ένα μέρος του ίδιου πόρου με την υπογραφή, που ενσωματώνεται μέσα στην υπογραφή, ή ενσωματώνει την υπογραφή μέσα σε αυτό.

Τα στοιχεία μιας XML υπογραφής, όπως φαίνεται πιο κάτω, είναι τα εξής:

```
<element name="Signature" type="ds:SignatureType"/>
    <complexType name="SignatureType">
```

```
  <sequence>
    <element ref="ds:SignedInfo"/>
    <element ref="ds:SignatureValue"/>
    <element ref="ds:KeyInfo" minOccurs="0"/>
    <element ref="ds:Object" minOccurs="0" maxOccurs="unbounded"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
</complexType>
```

Ο τύπος της XML ψηφιακής υπογραφής.

5.6 XML ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Οι βασικοί στόχοι της XML κρυπτογράφησης (XML Encryption) είναι:

• Υποστήριξη της κρυπτογράφησης οποιουδήποτε αυθαίρετου ψηφιακού περιεχομένου, συμπεριλαμβανομένων των XML εγγράφων.

• Εξασφάλιση ότι τα κρυπτογραφημένα δεδομένα, κατά τη μεταφορά ή την αποθήκευση, δεν μπορούν να προσπελασθούν από μη εξουσιοδοτημένα πρόσωπα.

• Διατήρηση της ασφάλειας των δεδομένων όχι μόνο όταν τα δεδομένα μεταφέρονται (πράγμα που εγγυάται το SSL), αλλά και όταν είναι σε στάση σε έναν συγκεκριμένο κόμβο.

• Παρουσίαση των κρυπτογραφημένων δεδομένων σε XML μορφή.

• Είναι δυνατό τμήματα του XML να κρυπτογραφηθούν επιλεκτικά.

Σε αντίθεση με την XML κρυπτογράφηση, χρησιμοποιώντας SSL άνω του HTTP (γνωστό ως HTTPS), ολόκληρο το μήνυμα κρυπτογραφείται. Ολόκληρο το μήνυμα αποκρυπτογραφείται έπειτα στον πρώτο προορισμό και είναι ανοικτό για επισκόπηση (snooping) προτού κρυπτογραφηθεί πάλι συνολικά για το δεύτερο άλμα. Η κρυπτογράφηση που προσφέρεται από το SSL άνω του HTTP υπάρχει μόνο για μεταφορά και δεν είναι σταθερή.

Η συγκεκριμένη προδιαγραφή καθορίζει μια διαδικασία για κρυπτογράφηση δεδομένων και παρουσίαση του αποτελέσματος σε XML. Τα δεδομένα μπορούν να είναι αυθαίρετα δεδομένα (συμπεριλαμβανομένου ενός εγγράφου XML), ένα στοιχείο XML, ή περιεχόμενα στοιχείου XML. Το αποτέλεσμα της κρυπτογράφησης δεδομένων είναι ένα στοιχείο EncryptedData, που περιέχει ή προσδιορίζει (μέσω μιας αναφοράς URI) τα cipher δεδομένα.

Τα βασικά στοιχεία μιας κρυπτογράφησης XML είναι:

Το EncryptionMethod είναι ένα προαιρετικό στοιχείο που περιγράφει τον αλγόριθμο κρυπτογράφησης που εφαρμόζεται στα cipher δεδομένα. Εάν το στοιχείο απουσιάζει, ο αλγόριθμος κρυπτογράφησης πρέπει να γίνει γνωστός από τον παραλήπτη αλλιώς η αποκρυπτογράφηση θα αποτύχει.

Το ds:KeyInfo είναι ένα προαιρετικό στοιχείο, που ορίζεται στις ψηφιακές υπογραφές XML, το οποίο φέρει πληροφορίες για το κλειδί που χρησιμοποιείται για να κρυπτογραφήσει τα δεδομένα.

Το CipherData είναι ένα υποχρεωτικό στοιχείο που παρέχει τα κρυπτογραφημένα δεδομένα. Πρέπει να περιέχει την κρυπτογραφημένη

ακολουθία ως κωδικοποιημένο base64 κείμενο του στοιχείου CipherValue, ή να παρέχει μια αναφορά σε μια εξωτερική θέση που περιέχει την κρυπτογραφημένη ακολουθία μέσω του στοιχείου CipherReference.
Το EncryptionProperties μπορεί να περιέχει πρόσθετες πληροφορίες σχετικά με την παραγωγή του EncryptedType (π.χ. date/time stamp ή ο αύξων αριθμός του κρυπτογραφικού υλικού που χρησιμοποιείται κατά τη διάρκεια της κρυπτογράφησης).

5.7 XML KEY MANAGEMENT SPECIFICATION (XKMS)

Μια από τις μεγαλύτερες απαιτήσεις για την ανάπτυξη όλων αυτών των νέων τεχνολογιών κρυπτογράφησης, ψηφιακών υπογραφών και πιστοποίησης, είναι να διατηρηθούν όλα τα δημόσια και ιδιωτικά κλειδιά, οι ψηφιακές υπογραφές και τα ψηφιακά πιστοποιητικά οργανωμένα και ασφαλή. Αρκετά προϊόντα υποδομής δημόσιου κλειδιού (PKI) της αγοράς σχεδιάστηκαν για να απλοποιήσουν τη διαχείριση αυτών των συστατικών ασφάλειας. Παρόλα αυτά, δεν υπάρχει ακόμα ένας πρότυπος τρόπος για την προσπέλαση τέτοιων συστημάτων σε ένα περιβάλλον υπηρεσιών ιστού βασισμένων στο πρωτόκολλο SOAP.

Η XKMS δημιουργήθηκε κάτω από την επίβλεψη του W3C, με σκοπό να παρέχει ένα τυποποιημένο σύνολο XML ορισμών για τη διαχείριση των υπηρεσιών πιστοποίησης, κρυπτογράφησης και ψηφιακών υπογραφών. Αυτό επιτρέπει στους σχεδιαστές να έχουν μια έμπιστη τρίτη οντότητα που βρίσκει και παρέχει τα κατάλληλα κλειδιά και πιστοποιητικά. Αυτή η έμπιστη τρίτη οντότητα ενεργεί σαν μεσάζοντας, ο οποίος απελευθερώνει τον προγραμματιστή της υπηρεσίας ιστού από την υποχρέωση να ελέγχει τη διαθεσιμότητα των κλειδιών ή των πιστοποιητικών και να εξασφαλίζει την εγκυρότητά τους.

Η XKMS περιλαμβάνει δυο μέρη: την XML Key Information Service Specification (X-KISS) και την XML Key Registration Service Specification (X-KRSS). Και οι δύο αυτές προδιαγραφές βασίζονται στη γλώσσα XML, χρησιμοποιούν το SOAP και οι σχέσεις μεταξύ των μηνυμάτων καθορίζονται από την WSDL. Παρόλα αυτά μπορούν να υπάρξουν εκφράσεις XKMS σε άλλο συμβατό σχήμα κωδικοποίησης.

Η X-KISS επιτρέπει σε έναν πελάτη μιας τέτοιας υπηρεσίας να αποστείλει μέρος ή όλες τις εργασίες που απαιτούνται για την επεξεργασία των στοιχείων <ds:KeyInfo> μιας XML υπογραφής σε μια XKMS υπηρεσία. Ένας βασικός στόχος του σχεδιασμού του πρωτοκόλλου είναι να ελαχιστοποιήσει την πολυπλοκότητα των εφαρμογών. Ως πελάτης της XKMS υπηρεσίας, η εφαρμογή απαλλάσσεται από την πολυπλοκότητα και τη σύνταξη του ελλοχεύοντος PKI που χρησιμοποιείται για να καθιερώσει σχέσεις εμπιστοσύνης. Το ελλοχεύον PKI μπορεί να βασίζεται σε μια διαφορετική προδιαγραφή όπως X.509/PKIX, SPKI ή PGP. Η προδιαγραφή X-KISS περιλαμβάνει δυο λειτουργίες:

Locate: Η υπηρεσία αυτή αναλύει ένα στοιχείο <ds:Keyinfo>, αλλά δεν απαιτεί από την υπηρεσία να κάνει μια δήλωση σχετικά με την ισχύ των δεδομένων που συνδέονται στο στοιχείο <ds:Keyinfo>.
Validate: Η υπηρεσία αυτή επιτρέπει όλα αυτά που κάνει η υπηρεσία Locate και επιπλέον, ο πελάτης μπορεί να λάβει μια δήλωση που διευκρινίζει την κατάσταση της σύνδεσης μεταξύ του δημόσιου κλειδιού και άλλων δεδομένων. Επιπλέον, η υπηρεσία αντιπροσωπεύει ότι η κατάσταση κάθε στοιχείου δεδομένων που επιστρέφεται είναι έγκυρο και ότι όλα είναι συνδεδεμένα στο ίδιο δημόσιο κλειδί.

5.8 ΤΟ ΠΡΩΤΟΚΟΛΛΟ SET

Σε αντίθεση με το SSL, το *SET (Secure Electronic Transactions*) αποτελεί εξειδικευμένο πρωτόκολλο για τη διασφάλιση των ηλεκτρονικών συναλλαγών μέσω πιστωτικών καρτών, ενώ πρόσφατα αρχίζει να χρησιμοποιείται και στις ηλεκτρονικές τραπεζικές συναλλαγές. Κατασκευάζεται από τις Visa, MasterCard, IBM, Netscape, Microsoft, GTE, Verisign. Στο SET αυτοί που συμμετέχουν σε μια συναλλαγή είναι ο πελάτης, ο έμπορος, η τράπεζα του πελάτη και η τράπεζα του εμπόρου, καθένας από τους οποίους πρέπει να έχει ψηφιακά πιστοποιητικά (digital certificates).

Με τη χρήση των ψηφιακών πιστοποιητικών επιβεβαιώνεται από τα συναλλασσόμενα μέρη (πωλητής και έμπορος) η ταυτότητά τους. Αυτό αποτελεί την πρώτη φάση της συναλλαγής (αυθεντικοποίηση των δύο μερών). Οι πελάτες επιβεβαιώνουν ότι οι έμποροι από τους οποίους επιθυμούν να αγοράσουν είναι νόμιμοι μέσα από την ψηφιακή ταυτότητά τους, όπως και οι έμποροι για τους πελάτες. Η εμπιστοσύνη αυτή εδραιώνεται μέσω των πιστοποιητικών που έχουν εκδοθεί από τρίτες αρχές (π.χ. τράπεζες).

Ένα πιστοποιητικό περιέχει το όνομα του προσώπου για το οποίο εκδίδεται (έμπορος ή πελάτης), την ψηφιακή υπογραφή του, το δημόσιο (και το αντίστοιχο ιδιωτικό κλειδί του) και την υπογραφή της αρχής που εξέδωσε το πιστοποιητικό. Όταν ο πελάτης δώσει μια παραγγελία, ο browser του λαμβάνει το πιστοποιητικό του εμπόρου, προκειμένου να ελεγχθεί αν είναι όντως νόμιμος - αν σχετίζεται με κάποιον χρηματοπιστωτικό οργανισμό. Στη συνέχεια στέλνεται στον έμπορο η παραγγελία κρυπτογραφημένη με το δημόσιο κλειδί του εμπόρου. Στην τράπεζα στέλνεται πληροφορία σχετικά με την πληρωμή, κρυπτογραφημένη με το δημόσιο κλειδί της τράπεζας. Το μεγάλο πλεονέκτημα του SET είναι ότι με αυτό τον τρόπο δε στέλνεται πληροφορία με τον αριθμό της πιστωτικής κάρτας στον έμπορο. Το SET δεν έχει ακόμα χρησιμοποιηθεί ευρέως, σε αντίθεση με το SSL, το οποίο διατηρεί το μεγαλύτερο μερίδιο στις ασφαλείς ηλεκτρονικές συναλλαγές. Σιγά – σιγά εμφανίζονται προϊόντα από μεγάλες εταιρείες του χώρου που χρησιμοποιούν το πρωτόκολλο αυτό.

ΣΤΟ ΚΕΦΑΛΑΙΟ 5 ΧΡΗΣΙΜΟΠΟΙΗΘΗΚΑΝ ΟΙ ΠΗΓΕΣ 1,3,4,5

ΣΥΜΠΕΡΑΣΜΑΤΑ- ΕΠΙΛΟΓΟΣ

Η ιστορία του Internet Banking ξεκινά πριν περίπου δύο δεκαετίες, στην Αμερική βέβαια, με την πρώτη εμφάνιση εφαρμογών ηλεκτρονικής τραπεζικής, τα γνωστά *ATM (Automatic Teller Machines*) και τις πιστωτικές κάρτες. Στην επόμενη δεκαετία η αγορά ήταν παραδομένη στον καταναλωτισμό του πλαστικού χρήματος , τα υποκαταστήματα των τραπεζών πολλαπλασιάστηκαν και τα τραπεζικά προϊόντα εξειδικεύτηκαν. Το νέο χαρτί στο παιχνίδι ήταν το Internet και οι τράπεζες θέλοντας και μη έπρεπε να μπουν στο χορό.

Η ιλιγγιώδης εξάπλωση του Internet και η επαφή των χρηστών με οποιαδήποτε επιχείρηση στον κόσμο άνοιξε νέες πόρτες για τις εθνικές οικονομίες. Οι εκδότες διεθνών πιστωτικών καρτών (*Visa, MasterCard* κτλ) και οι συνεργαζόμενες τράπεζες είδαν τις συναλλαγές τους και τις προμήθειες τους να αποκτούν νέα δυναμική. Υπήρχαν όμως ακόμη προβλήματα που έπρεπε να λυθούν όπως η έλλειψη κοινά αποδεκτής νομοθεσίας που άφηνε ακάλυπτες τις τράπεζες.

Παράλληλα οι πελάτες απαίτησαν την αξιοποίηση και των υπόλοιπων δυνατοτήτων του Internet. Αφού μπορούσαν να συναλλαγούν με τους εμπόρους, να παραγγέλλουν και να πληρώσουν προϊόντα από μακριά, γιατί να μην μπορούν να κάνουν το ίδιο και με τις τράπεζες; Την αρχή έκανε το 1994 ο *Bill Gates*. Η *Microsoft*, βλέποντας τις εξελίξεις είχε επενδύσει στο λογισμικό προσωπικής διαχείρισης οικονομικών, το *Microsoft Money*. Πολλές αμερικάνικες τράπεζες αναγκάστηκαν να αναπτύξουν εφαρμογές συμβατές με το πακέτο της Microsoft και άλλων ανταγωνιστών του. (*Quicken, Managing your Money*). Από κει και πέρα τίποτα δεν μπορούσε να σταματήσει την ανάπτυξη του Internet Banking.

Το Internet Banking θυμίζει τα πρώτα βήματα του *e-mail* στο Internet. Η ιδέα του ηλεκτρονικού ταχυδρομείου αποτέλεσε μια πραγματική επανάσταση και έπειτα από μια ταχύτατη πορεία εξέλιξης είναι πλέον ένα σημαντικό μέσο τόσο για προσωπική όσο και για επαγγελματική χρήση. Σ’ αυτό συνέλαβαν η αξιοπιστία και η εύκολη χρήση του. Αυτά δηλαδή που χρειάζεται και το Internet Banking για να συνεχίσει την επιτυχημένη μέχρι τώρα πορεία του.

Είναι ξεκάθαρο ότι το βασικό πλεονέκτημα του Internet Banking για τον πελάτη είναι αυτό που δίνει το ίδιο το Internet σε όλες τις διεργασίες και υπηρεσίες που προσφέρονται ηλεκτρονικά μέσα από δίκτυο. Η δυνατότητα δηλαδή του χρήστη να το χρησιμοποιεί οποιαδήποτε ώρα της ημέρας, 365 μέρες το χρόνο από την άνεση του σπιτιού του ή από οπουδήποτε αλλού θέλει. Αυτό εξοικονομεί πολύτιμο χρόνο και αυξάνει την παραγωγικότητα αν μιλάμε για επιχειρήσεις. Μια επίσκεψη στην τράπεζα (παρκάρισμα, αναμονή στην ουρά κ.α.) μπορεί να πάρει ακόμη και ώρες ενώ για την ίδια συναλλαγή στο Internet ο χρόνος είναι θέμα μερικών “κλικ” του ποντικιού.

Ένας δεύτερος τομέας όπου ο πελάτης βγαίνει κερδισμένος είναι η δυνατότητα που έχει να συγκρίνει και να αποφασίζει αβίαστα και χωρίς να του γίνεται πλύση εγκεφάλου. Οι εποχές που ο πελάτης παρακαλούσε τις τράπεζες έχουν περάσει. Τώρα πια οι ρόλοι έχουν αντιστραφεί. Οι τράπεζες

ανοίγουν τα χαρτιά τους στο Internet και αυτές είναι που ψάχνουν για μελλοντικούς πελάτες.

Πρώτα απ' όλα, είναι η μείωση του λειτουργικού κόστους συναλλαγών. Την τελευταία δεκαετία οι τράπεζες επένδυσαν σημαντικά ποσά σε τεχνολογικές υποδομές προκειμένου να αποσυμφορήσουν τις ουρές στα ταμεία των υποκαταστημάτων τους. Οι παραδοσιακές συναλλαγές στα ταμεία κοστίζουν ακριβά σε αντίθεση με τα εναλλακτικά δίκτυα που κοστίζουν ελάχιστα. Σύμφωνα με μελέτη του ***Booz Allen & Hamilton***, μια τυπική τραπεζική συναλλαγή όπως η κατάθεση, η ανάληψη, η ερώτηση υπολοίπου και η μεταφορά ποσού σε άλλο λογαριασμό, όταν πραγματοποιείται στο ταμείο και απασχολεί ανθρώπινο δυναμικό κοστίζει 1,01 ευρώ. Η ίδια συναλλαγή όταν πραγματοποιείται μέσω του Internet κοστίζει μόλις 0,01 ευρώ. Έτσι λοιπόν οι τράπεζες δεν χρεώνουν προμήθεια για συναλλαγές μέσω Internet εκτός από εμβάσματα στο εξωτερικό και μεταφορές σε λογαριασμούς άλλων τραπεζών. Με την αποσυμφόρηση των ταμείων οι τράπεζες στρέφουν ένα μεγαλύτερο μέρος του προσωπικού τους σε εργασίες όπου η προσωπική επαφή είναι απαραίτητη. Για παράδειγμα σε συμβουλευτικού τύπου υπηρεσίες.

Επίσης οι τράπεζες αποκτούν πρόσβαση προς τους πελάτες μιας ευρύτερης γεωγραφικά περιοχής εντός και εκτός εθνικών συνόρων, χωρίς να είναι απαραίτητο το άνοιγμα ενός υποκαταστήματος.

Παρόλο που με το Internet Banking ο πελάτης μπορεί να προβεί σε οποιανδήποτε συναλλαγή εκτός από συναλλαγές που υπάρχουν στη μέση χαρτονομίσματα και νομίσματα, η δουλειά του ταμείου δεν μπορεί ακόμη να αντικατασταθεί πλήρως. Όπως υποστηρίζουν οι ειδικοί, τα ταμεία των τραπεζών θα συνεχίσουν να έχουν ακριβώς τον ίδιο χαρακτήρα για τουλάχιστον άλλα δέκα χρόνια.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Γ. Δουκίδης, Καθηγητής Ο.Π.Α., «Το Ηλεκτρονικό Επιχειρείν στις μεγάλες ελληνικές επιχειρήσεις»

2. ΔΕΛΤΙΟΝ ΕΝΩΣΗΣ ΕΛΛΗΝΙΚΩΝ ΤΡΑΠΕΖΩΝ, «*Αφιέρωμα στο e- banking*», Ιούλιος –Αύγουστος – Σεπτέμβριος 2003

3. C. Albrecht, "How clean is the future of SOAP", Communications of the ACM, Vol. 47, No. 2, February 2004

4. D. Chappell and T. Jewell, "JAVA Web Services", O' Reilly publications, First edition, March 2002

5. E. Cerami, "Web Services Essentials", O' Reilly publications, First edition, February 2002

6. Laura Fisher Kaiser, "The Official Ebay Guide to Buying, Selling and Collecting Just About Anything", 2000

7. T. Bray, J. Paoli, C. M. Sperberg-McQueen, F. Yergeau, "Extensible Markup Language (XML) 1.0 (Third Edition)", W3C Recommendation, February 2004.

8. "E-Learning το τεχνολογικό στοίχημα των επιχειρήσεων" COMBusiness τεύχος 45, Νοέμβριος 2002

ΔΙΑΔΙΚΤΥΑΚΕΣ ΠΗΓΕΣ

1. http://www.alpha.gr/page/default.asp?id=864&la=1
2. https://ebank.emporiki.gr/EMPB_EBANKWeb/EL/contents/Faq.jsp
3. http://www.eurobank.gr/online/home/generic.aspx?id=73&mid=467&lang=gr
4. https://ebanking.millenniumbank.gr/eBankingWeb/open_retail_user_manual?Lang=el_GR
5. http://www.bankofcyprus.gr/alternative_gr/1bankinternetbanking_gr/
6. http://www.emporiki.gr/cbg/gr/useful_info/useful_story.jsp?docpath=/gr/Useful/static/useful
7. http://www.piraeusbank.gr/ecpage.asp?nt=19&id=261630&lang=1
8. http://brokerage.emporiki.gr/services
9. http://www.bankofcyprus.gr/alternative_gr/1bankphonebanking_gr/
10. https://www.marfinbank.gr/GR/MarfinDirect/PhoneVoiceBanking/Pages/VoiceBanking.aspx
11. http://www.eurobank.gr/online/home/generic.aspx?id=334&mid=461&lang=gr
12. http://www.piraeusbank.gr/eCPortal.asp?nt=98&id=241827
13. http://www.nbg.gr/wps/portal/!ut/p/c0/04_SB8K8xLLM9MSSzPy8xBz9CP0os3jXIFNnSzcPIwMLgxADAyMfL5dgz5AQQwsLM_3g1Bz9gmxHRQBNANWL/?WCM_PORTLET=PC_7_ER5C9FH2080T002LJDSITT18O4_WCM&WCM_GLOBAL_CONTEXT=/wps/wcm/connect/NBG-gr/nbg+site/retail/family%2C+employees/electronic+banking/phone+banking+family#

14.http://www.emporiki.gr/cbg/gr/useful_info/useful_story.jsp?docpath=/gr/Useful/static/useful