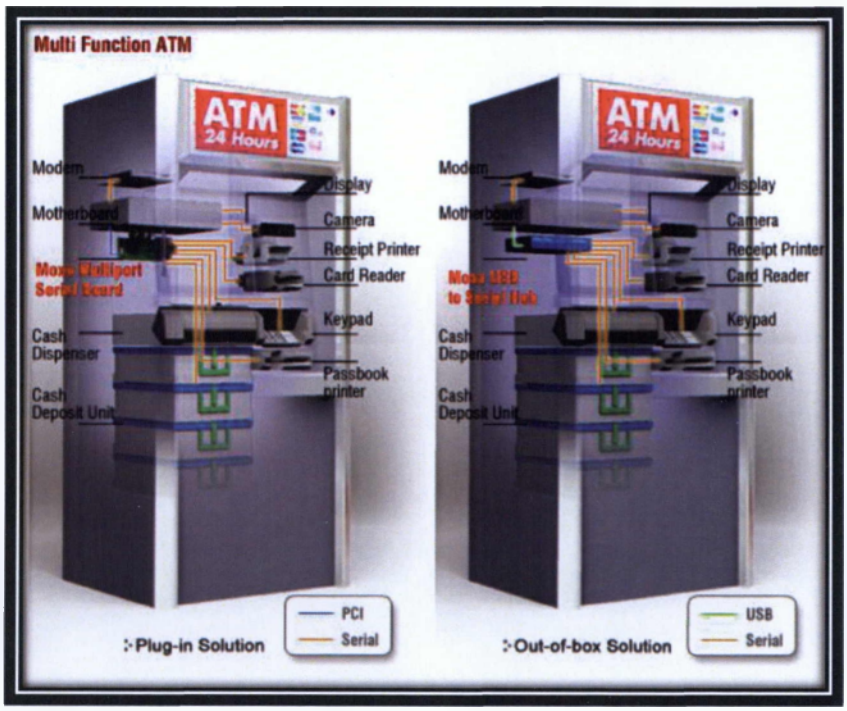
2013

ΑΤΕΙ ΚΑΛΑΜΑΤΑΣ Παράρτημα Σπάρτης

ΤΜΗΜΑ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ



"ΑΝΑΛΥΣΗ ΤΗΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΩΝ ΑΥΤΟΜΑΤΩΝ ΜΗΧΑΝΩΝ ΑΝΑΛΗΨΗΣ ΧΡΗΜΑΤΩΝ (ATM) ΣΕ ΣΥΓΚΡΙΣΗ ΜΕ ΤΙΣ ΕΠΕΡΧΟΜΕΝΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΤΡΑΠΕΖΙΚΗΣ"

ΚΑΡΑΓΙΑΝΝΑΚΗ ΓΕΩΡΓΙΑ 2007085

ΣΚΟΠΟΣ-ΠΕΡΙΛΗΨΗ

Ο στόχος της εργασίας αυτής είναι να περιγράψει, να αναλύσει και να εξάγει κάποια συμπεράσματα για τα μηχανήματα αυτόματης ανάληψης ΑΤΜ. Στο 1ο κεφάλαιο θα γίνει μια εισαγωγή για τα βασικά μέρη και λειτουργίες του ΑΤΜ.
Στο 2ο κεφάλαιο θα ορίσουμε το ΑΤΜ.θα αναλύσουμε κάποια βασικά στοιχεία του καθώς και τα πλεονεκτήματα και μειονεκτηματά του. Στη συνέχεια στο 3ο κεφάλαιο θα περιγράψουμε την ασφάλεια την οποία παρέχει καθώς και τους νόμους που διέπουν την ηλεκτρονική τραπεζική.
Στη συνέχεια στο 4ο κεφάλαιο θα ασχοληθούμε τις εφαρμογές τις ηλεκτρονικής τραπεζικής στην Ελλάδα καθώς και τις μελλοντικές εξελίξεις και εφαρμογές που απαιτούνται στην σύγχρονη εποχή που δεν μπορεί να καλύψουν τα ΑΤΜ.
Στο τελευταίο κεφάλαιο θα εξάγουμε τα συμπεράσματά μας.

ΕΙΣΑΓΩΓΗ

Η επανάσταση της τεχνολογίας έχει επηρεάσει σχεδόν κάθε πλευρά της ζωής μεταξύ των οποίων είναι και ο τραπεζικός τομέας στον οποίο έχει αλλάξει η φύση των τραπεζών. Η εισαγωγή της ηλεκτρονικής τραπεζικής έχει δραστικά αλλάξει τον τρόπο που οι τράπεζες λειτουργούν καθώς η τεχνολογία τώρα θεωρείται ως η κύρια συμβολή για την επιτυχία των οργανισμών και των βασικών ικανοτήτων τους. Έτσι, οι τράπεζες,είτε πρόκειται για εγχώριες ή για ξένες επενδύουν περισσότερο στην παροχή νέων τεχνολογιών μέσω των διατραπεζικών τους συστημάτων. PC-banking, εταιρείες κινητής τραπέζης, ATM,ηλεκτρονική μεταφορά κεφαλαίων, μεταφορά από λογαριασμό σε λογαριασμό,πληρωμή λογαριασμών on-line. δηλώσεις σε απευθείας σύνδεση, πιστωτικές κάρτες κ.λπ. είναι οι υπηρεσίες που παρέχονται από τις τράπεζες.

Από όλες αυτές τα ATM διεξάγουν πολλές συναλλαγές που διαφορετικά θα απαιτούσαν πολύ προσωπικό. Παρέχουν πληροφορίες του λογαριασμού, δέχονται καταθέσεις, προβαίνουν σε αναλήψεις προ-εγκεκριμένων δανείων και μεταφοράς κεφαλαίων. Η χρήση των ATM επιτρέπει στους υπαλλήλους να επικεντρωθούν στην παροχή εξατομικευμένων υπηρεσιών, καθώς και οι μηχανές μπορούν να προσφέρουν ενδεχομένως ένα ευρύτερο φάσμα υπηρεσιών.

Η Αυτόματη Ταμειακή Μηχανή ή ATM επιτρέπει λοιπόν σε έναν πελάτη τράπεζας να διεξάγει τις τραπεζικές του συναλλαγές από σχεδόν οποιοδήποτε μηχάνημα ATM στον κόσμο.

Τα ATM είναι πιο αποτελεσματικά για ιδρύματα που αποδέχονται καταθέσεις και θέλουν να εξυπηρετήσουν τους πελάτες σε πολλαπλές θέσεις ή κατά τη διάρκεια μη εργάσιμων ωρών. Αλλά δεδομένου ότι ένα μόνο μηχάνημα μπορεί να κοστίσει μέχρι και 35.000$ απαιτούνται αξιόπιστες επικοινωνίες και συνδέσεις.

Luther Simjian vs John Shepherd-Barron vs Don Wetzel

Δεδομένου ότι το δίπλωμα ευρεσιτεχνίας για ένα ATM δεν εφαρμόστηκε ποτέ μετά τον κ. Simjian, υπάρχει μια σύγχυση σχετικά με τον εφευρέτη των ATM .Ένας λόγος είναι ότι οι τρεις διεκδικητές ζούσαν σε διαφορετικά μέρη.Ο John Shepherd-Barron ζούσε στο Ηνωμένο Βασίλειο, ο Luther Simjian στη Σκωτία ενώ όλοι οι άλλοι ζούσαν στις ΗΠΑ.

Luther Simjian

Το 1939, ο Luther Simjian κατοχυρώνει με δίπλωμα ευρεσιτεχνίας ένα όχι και τόσο επιτυχημένο πρωτότυπο ενός τραπεζικού συστήματος ATM.

Ωστόσο, ορισμένοι ειδικοί έχουν τη γνώμη ότι ο James Goodfellow από την Σκωτία κατέχει την παλαιότερη ημερομηνία διπλωμάτων ευρεσιτεχνίας το 1966 για ένα σύγχρονο ATM, και ο John Docutel στις ΗΠΑ είναι συχνά πιστώνεται με την επινόηση το πρώτο επιδαπέδιου σχεδιασμού ενός ATM. Το 1967, ο John Shepherd-Barron εγκατέστησε το πρώτο ATM στην τράπεζα Barclays Bank στο Λονδίνο.

Ωστόσο, έπρεπε να φτάσουμε έως τα τέλη της δεκαετίας του 1980 ότι τα ATM έγιναν μέρος της επίσημης τραπεζικής.

Ο Luther Simjian ήρθε με την ιδέα της δημιουργίας μιάς εντοιχισμένης μηχανής" που θα επέτρεπε στους πελάτες να κάνουν οικονομικές συναλλαγές, χωρίς να εισέρχονται στην τράπεζα. Η ιδέα έγινε δεκτή με μεγάλη αμφιβολία όμως. Ξεκινώντας το 1939, Simjian εγγραφεί 20 διπλώματα ευρεσιτεχνίας που σχετίζονται με τη συσκευή και την εταιρεία που είναι τώρα η Citicorp για να κάνει μια δοκιμή. Μετά από έξι μήνες, η τράπεζα ανέφερε ότι υπήρξε μικρή ζήτηση. Σήμερα, όπως γνωρίζετε, υπάρχει μια τεράστια ζήτηση!

John Shepherd-Barron

Ο John Shepherd-Barron είχε μια ιδέα στη δεκαετία του 1960 για ένα μηχανισμό διανομής χρημάτων σε μετρητά. Διετέλεσε Διευθύνων Σύμβουλος της Instruments De La Rue.Η De La Rue σήμερα κατασκευάζει μηχανήματα αυτόματης ανάληψης. Είχε εγκατασταθεί σε ένα υποκατάστημα της τράπεζας Barclays το 1967 και τέθηκε σε χρήση στην πόλη Enfield, στο βόρειο Λονδίνο στις 27 Ιουνίου του 1967. Αυτή η μηχανή ήταν η πρώτη στο Ηνωμένο Βασίλειο.Αργότερα εκείνο το έτος, Shepherd-Barron παρουσίασε την ιδέα του σε ένα συνέδριο. Το συνέδριο αποτελούνταν από 2.000 τραπεζίτες των ΗΠΑ στο Μαϊάμι.

Μίλησε στο συνέδριο σχετικά με τη νέα συσκευή τραπεζική self-service που ανέπτυξε. Στις 31 Δεκεμβρίου 2004, ο John Shepherd-Barron, ονομάστηκε αξιωματούχος του Τάγματος της Βρετανικής Αυτοκρατορίας από τη Βασίλισσα και του απονεμήθεί το βραβείο New Year Honours το οποίο ήταν για τις "υπηρεσίες σε τραπεζικές εργασίες.Ο ίδιος δήλωσε: «Ηταν λίγο αργά, αλλά κάλλιο αργά παρά ποτέ". Το Δελτίο Τύπου δήλωσε ότι Shepherd-Barron ήταν ο "εφευρέτης του ATM." Αλλά, ήταν στ 'αλήθεια ο εφευρέτης;

Σε ταυτόχρονες και ανεξάρτητες προσπάθειες πάντως μηχανικοί στην Ιαπωνία, τη Σουηδία και τη Βρετανία ανέπτυξαν τις δικές τους μηχανές για μετρητά κατά τη διάρκεια της δεκαετίας του 1960.

Don Wetzel

Το 1968, σύμφωνα με μια συνέντευξη ο Don Wetzel, ο οποίος ήταν ο Αντιπρόεδρος του σχεδιασμού των προϊόντων της Docutel υπέβαλε αίτηση για δίπλωμα ευρεσιτεχνίας για ένα μηχάνημα ATM.Η εταιρεία του εξειδικευόταν στην ανάπτυξη εξοπλισμού αυτοματοποιημένης διακίνησης αποσκευών. Ανέφερε ότι υπήρχαν άλλοι δύο εφευρέτες που αναφέρονται στο δίπλωμα ευρεσιτεχνίας. Ήταν ο Tom Barnes, ένας μηχανολόγος μηχανικός και ο George Chastain, ένας ηλεκτρολόγος μηχανικός.Χρειάστηκαν πέντε εκατομμύρια δολάρια για την ανάπτυξη του ATM τους, σύμφωνα με τον κ. Wetzel.

Η πρώτη συναλλαγή

Η πρώτη συναλλαγή όπως την γνωρίζουμε σήμερα έγινε στην Νέα Υόρκη.

Το πρώτο σύγχρονο ATM ήταν εγκατεστημένο το 1969 από την Τράπεζα Chemical στο υποκατάστημά της στο Rockville Centre της Νέας Υόρκης. Το συγκεκριμένο ATM ήταν σχεδιασμένο για να διανείμει ένα σταθερό ποσό μετρητών όταν ένας χρήστης εισάγει μία ειδικά κωδικοποιημένη κάρτα. Μια διαφήμιση της Chemical Bank καυχήθηκε "στις 2 Σεπτεμβρίου 1969 στις 9:00 η τράπεζα μας θα ανοίξει και δεν θα κλείσει ποτέ ξανά». Το ATM της συγκεκριμένης τράπεζας, αρχικά ήταν γνωστό ως Docuteller. Σχεδιάστηκε από τον Donald Wetzel και την εταιρεία του.

Τα στελέχη της Chemical ήταν αρχικά διστακτικά απέναντι στην ηλεκτρονική τραπεζική μετάβαση, δεδομένου του υψηλού κόστους των πρώτων μηχανών. Επιπλέον, τα στελέχη εξέφρασαν την ανησυχία ότι οι πελάτες θα αντισταθούν σε μηχανές που θα είναι υπεύθυνες για τη διαχείριση των χρημάτων τους. Το 1995, το Εθνικό Μουσείο Smithsonian της Αμερικανικής Ιστορίας αναγνωρίζει την Docutel και τον Wetzel ως εφευρέτες του δικτυακού ATM.

ΚΕΦΑΛΑΙΟ 1: Τι είναι μια ATM μηχανή;

Ο διεθνής όρος Automatic Teller Machines (ATM) αποδίδεται στην ελληνική βιβλιογραφία ως Αυτόματες Ταμειολογιστικές Μηχανές. Ουσιαστικά αποτελούν τον προπομπό των αυτόματων συναλλαγών και με τη χρήση αυτής της τεχνολογίας τα τραπεζικά ιδρύματα πέτυχαν την αποσυμφόρηση των γκισέ των ταμείων των καταστημάτων τους. Τα μηχανήματα αυτά έχουν τη δυνατότητα να εξυπηρετήσουν τον πελάτη 24 ώρες το 24ωρο. Το μόνο που χρειάζεται είναι μια μαγνητική κάρτα και ένας προσωπικός κωδικός αριθμός (PIN).
Μια ATM αποτελεί ουσιαστικά μέρος του υπολογιστικού συστήματος της τράπεζας και αποτελείται από δύο βασικά τμήματα :το ηλεκτρονικό τμήμα που βοηθάει στην αποστολή και λήψη στοιχείων, και ένα μηχανικό τμήμα, το οποίο καταμετρά με ακρίβεια τα χαρτονομίσματα και εκδίδει τις αποδείξεις για τους χρήστες.

Κατηγορίες χωρικής τοποθέτησης

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

I. Εντοιχισμένες στο κτίριο.

Τα μηχανήματα βρίσκονται εξωτερικά των τραπεζικών καταστημάτων και εξωτερικά άλλων κτιρίων σε στρατηγικά σημεία μια πόλη και είναι έτοιμα για χρήση από τον πελάτη.

II. In the Lobby.

Τα ATM σε αυτήν την περίπτωση βρίσκονται στο εσωτερικό των τραπεζικών ιδρυμάτων αλλά και πολυκαταστημάτων, εμπορικών κέντρων και μεγάλων Super Markets.

III. Προθάλαμος.

Αυτά τα μηχανήματα τοποθετούνται σε ειδικά διαμορφωμένους γυάλινους προθάλαμους τραπεζικών καταστημάτων. Μπορούν να λειτουργήσουν και εκτός εργάσιμων ωρών και θεωρούνται πιο ασφαλή μηχανήματα αφού είναι αδύνατο να παραβιαστούν.

Οφέλη των ATM

Η χρήση των ATMs έχει οφέλη τόσο για τον πελάτη όσο και για την τράπεζα. Ο πελάτης ωφελείται επειδή:

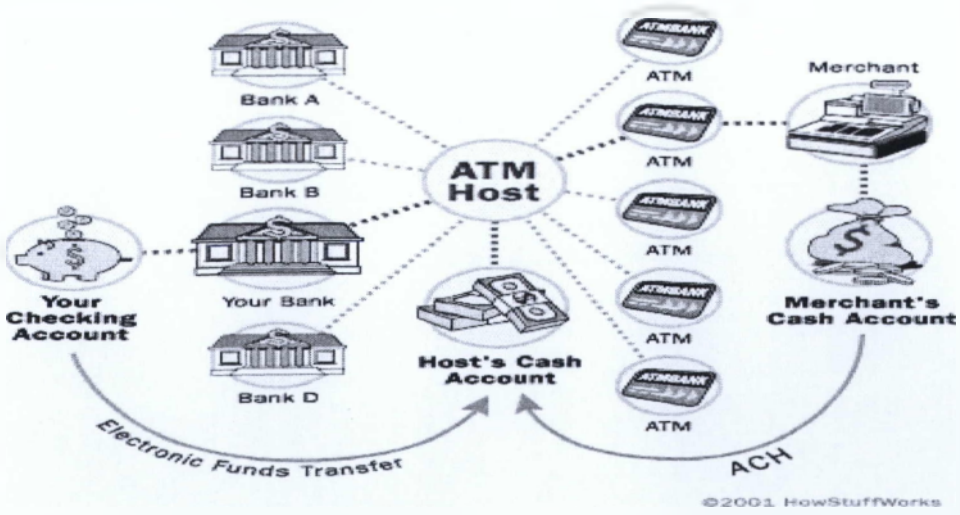
Α)μπορεί να πραγματοποιήσει τραπεζική συναλλαγή οποιαδήποτε μέρα και ώρα θέλει με ελάχιστη σπατάλη χρόνου

Β) δεν είναι υποχρεωμένος να φέρει πολλά χρήματα μαζί του.

Η τράπεζα αντίθετα ωφελείται από:

- τη μείωση της πιθανότητας λαθών
- τη μείωση των λειτουργικών εξόδων σε σχέση με μία συναλλαγή που γίνεται στο γκισέ μιας τράπεζας.

Μία σημαντική καινοτομία που έγινε με σκοπό την προώθηση των ATMs ήταν η ανάπτυξη του διατραπεζικού συστήματος ΔΙΑΣ. Οι τράπεζες για να επεκτείνουν την ακτίνα εξυπηρέτησής τους δημιούργησαν το σύστημα ΔΙΑΣ. Το συγκεκριμένο σύστημα επιτρέπει στους χρήστες των ATMs να κάνουν ανάληψη από οποιοδήποτε ATM τράπεζας που συμμετέχει σε αυτό. Η μόνη επιβάρυνση είναι μια μικρή χρέωση που υπάρχει από το ATM της χρησιμοποιούμενης τράπεζας. Δεδομένου της δημιουργίας διπλών κεντρικών υπολογιστικών συστημάτων, το σύστημα ΔΙΑΣ θεωρείται ιδιαίτερα ασφαλές.



Παράδειγμα διατραπεζικού συστήματος ΔΙΑΣ

1.Το ΑΤΜ παρέχει 24ωρη εξυπηρέτηση

Τα ΑΤΜ παρέχουν τις υπηρεσίες τους 24 ώρες το εικοσιτετράωρο. Ο πελάτης μπορεί να κάνει ανάληψη μετρητών μέχρι ένα ορισμένο όριο κατά οποιαδήποτε στιγμή της ημέρας ή της νύχτας.

2. Το ΑΤΜ παρέχει ευκολία στους πελάτες της τράπεζας

Τα ΑΤΜ παρέχουν την ευκολία για τους πελάτες. Σήμερα τα ΑΤΜ βρίσκονται σε κατάλληλα σημεία, όπως σε λιμάνια, σιδηροδρομικούς σταθμούς, κλπ. και όχι απαραίτητα στις εγκαταστάσεις της Τράπεζας. Έτσι τα ΑΤΜ παρέχουν κινητικότητα σε τραπεζικές υπηρεσίες.

3. Το ΑΤΜ μειώνει το φόρτο εργασίας του προσωπικού της τράπεζας.

Ένα μηχάνημα ΑΤΜ μειώσει την πίεση της εργασίας για το προσωπικό της τράπεζας και αποφεύγει ουρές στα γραφεία της τράπεζας.

4. Το ΑΤΜ παρέχει τίς υπηρεσίες του χωρίς κανένα λάθος.

Τά ΑΤΜ παρέχουν τις υπηρεσίες τους χωρίς σφάλμα. Ο πελάτης μπορεί να αποκτήσει το ακριβές ποσό που θέλει χωρίς να υπάρξει ανθρώπινο λάθος,στο μέτρο που οι περισσότεροι πολίτες ανησυχούν για τα ΑΤΜ.

5.Τα ΑΤΜ είναι πολύ ευεργετικά για τους ταξιδιώτες

Τα ΑΤΜ είναι μεγάλη βοήθεια για τους ταξιδιώτες. Δεν χρειάζεται να μεταφέρουν μεγάλα ποσά σε μετρητά μαζί τους. Μπορούν ανάληψη μετρητών από οποιαδήποτε πόλη ή την κατάσταση, σε όλη τη χώρα, ακόμη και από το εξωτερικό της χώρας, με τη βοήθεια του ΑΤΜ.

6. ΑΤΜ μπορεί να δώσει στους πελάτες νέα χαρτονομίσματα

Ο πελάτης παίρνει επίσης καινούργια χαρτονομίσματα από τα ΑΤΜ. Με άλλα λόγια, οι πελάτες δεν παίρνουν λερωμένα σημειώσεις από ΑΤΜ.

7. ΑΤΜ παρέχει προστασία της ιδιωτικής ζωής στις τραπεζικές συναλλαγές

Πάνω απ 'όλα, ΑΤΜ παρέχουν προστασία της ιδιωτικής ζωής στις τραπεζικές συναλλαγές του πελάτη.

Ένα ATM είναι απλά ένα τερματικό δεδομένων με δύο συσκευές εισόδου και τέσσερις συσκευές εξόδου. Όπως και κάθε άλλο τερματικό δεδομένων, το ATM πρέπει να συνδεθεί με μια γραμμή και οι χρήστες να επικοινωνούν μέσω ενός επεξεργαστή υποδοχής. Ο κεντρικός επεξεργαστής είναι ανάλογος με μια υπηρεσία παροχής Internet (ISP), υπό την έννοια ότι είναι η πύλη μέσω της οποίας όλα τα διάφορα δίκτυα ATM είναι διαθέσιμα στον κάτοχο της κάρτας (το άτομο που θέλει τα μετρητά).

Ένα ATM είναι απλά ένα τερματικό δεδομένων με δύο εισόδου και τέσσερις συσκευές εξόδου. Όπως και κάθε άλλο τερματικό δεδομένων, το ATM πρέπει να συνδεθεί, και να επικοινωνούν μέσω, έναν επεξεργαστή υποδοχής. Ο κεντρικός επεξεργαστής είναι ανάλογη με μια υπηρεσία παροχής Internet (ISP), υπό την έννοια ότι είναι η πύλη μέσω της οποίας όλα τα διάφορα δίκτυα ATM είναι διαθέσιμα στον κάτοχο της κάρτας (το άτομο που θέλει τα μετρητά).

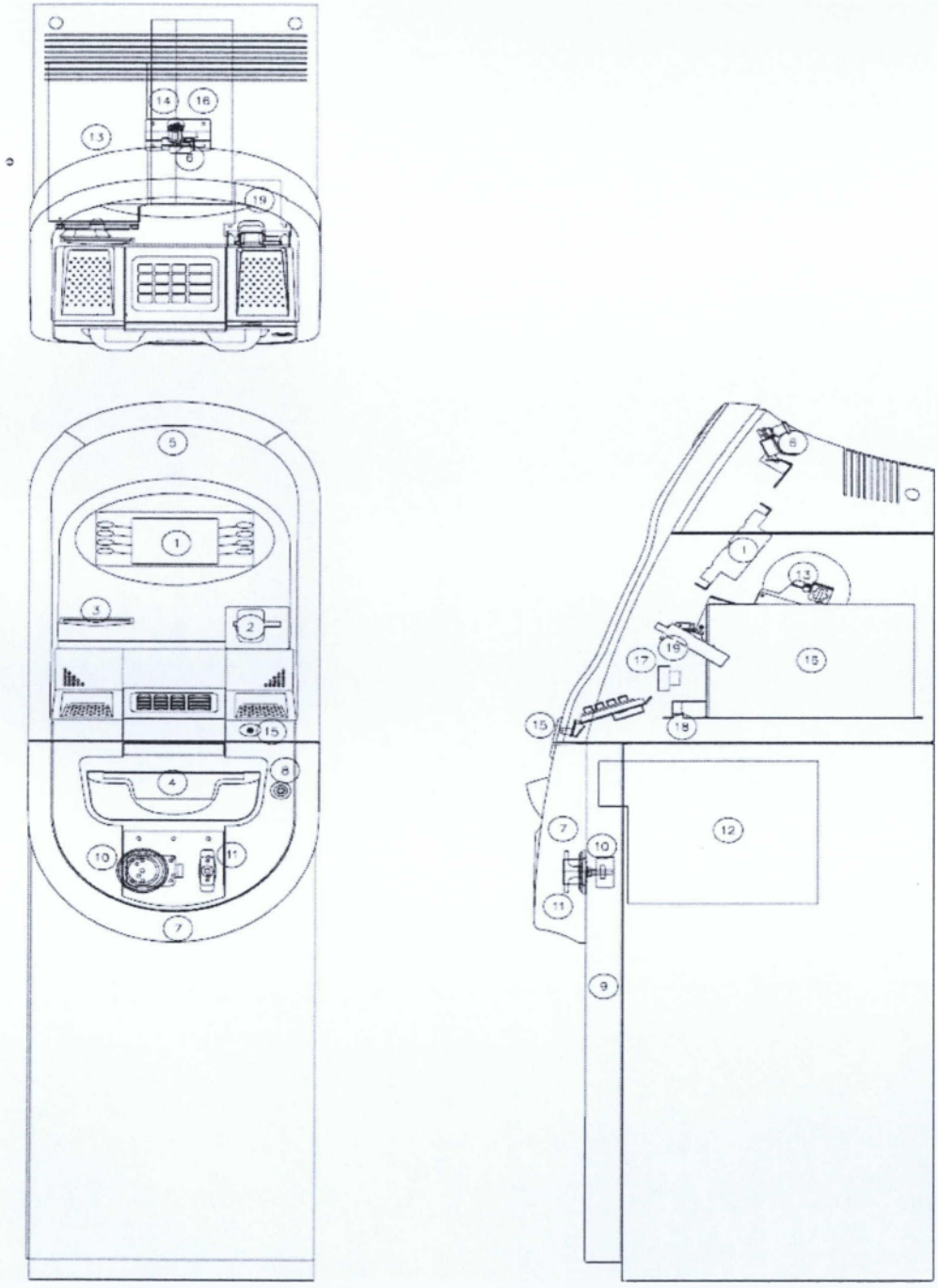
Οι περισσότεροι επεξεργαστές υποδοχής μπορεί να υποστηρίξουν είτε μισθωμένες γραμμές ή dial-up . Οι μισθωμένων γραμμών μηχανές συνδέονται απευθείας με τον επεξεργαστή υποδοχής μέσω τεσσάρων καλωδίων, από σημείο σε σημείο,με αποκλειστική τηλεφωνική γραμμή. Τα Dial-up ATM συνδέονται με το κεντρικό επεξεργαστή μέσω μιας κανονικής τηλεφωνικής γραμμής χρησιμοποιώντας ένα μόντεμ και έναν ατελή αριθμό, ή μέσω μιας υπηρεσίας παροχής Internet χρησιμοποιώντας ένα τοπικό αριθμό πρόσβασης.

Οι μισθωμένες γραμμές ATM προτιμώνται λόγω του πολύ μεγάλου όγκου και λόγω της καλύτερης ικανότητας ρυθμο-απόδοσής ενώ τα dial-up ATM προτιμώνται κυρίως σε εμπορικά σημεία Το αρχικό κόστος για ένα μηχάνημα dial-up είναι λιγότερο από το μισό από ότι για μισθωμένης γραμμής μηχάνημα. Το μηνιαίο κόστος λειτουργίας για ένα dial-up είναι μόνο ένα κλάσμα του κόστους των μισθωμένων γραμμών.

Ο κεντρικός επεξεργαστής μπορεί να ανήκει σε τράπεζα ή χρηματοπιστωτικό ίδρυμα, ή μπορεί να ανήκει σε ανεξάρτητο φορέα παροχής υπηρεσιών. Οι ιδιόκτητοι επεξεργαστές υποστηρίζουν κανονικά μόνο την τράπεζα που ανήκουν τα μηχανήματα, ενώ οι ανεξάρτητοι επεξεργαστές υποστηρίζουν όλες τις τράπεζες.

Κεφάλαιο 2: Προδιαγραφές Υλικού

Διαστάσεις



Εικόνα 1 Mini Bank 1500

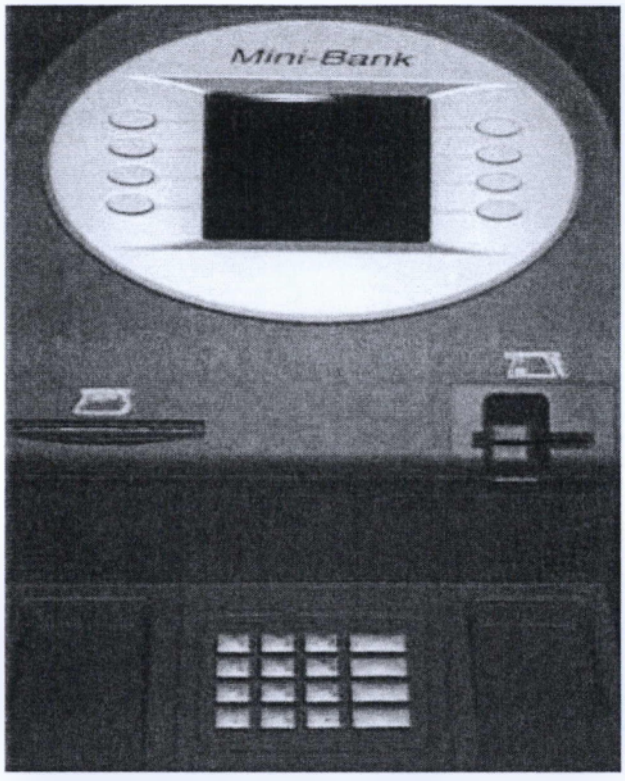
Σαν αναφορά πήραμε το μοντέλο Mini Bank 1500 της εταιρείας Tranax

Βάρος: 306lbs. (139 kg.)

2.1 Τοποθεσία εξαρτημάτων

1. Οθόνη LCD & Πληκτρολόγιο πελατών
2. Υποδοχή κάρτας
3. Σχισμή παραλαβής απόδειξης
4. Παραλαβή μετρητών
5. Μπροστινό πάνελ
6. Κλειδαριά μπροστινού πάνελ
7. Κάλυμμα ασφάλειας
8. Κλειδαριά καλύμματος ασφαλείας
9. Πόρτα ασφαλείας
10. Κλειδαριά με συνδυασμό
11. Χερούλι της πόρτας ασφάλειας
12. Μονάδα διανομής μετρητών
13. Εκτυπωτής αποδείξεων
14. Κεντρικός πίνακας ελέγχου
15. Υποδοχή ακουστικών (ADA, Option)
16. Τροφοδοσία
17. Ηχείο
19. Κάρτα ανάγνωσης

2.1.1Οθόνη LCD & Πληκτρολόγιο πελατών



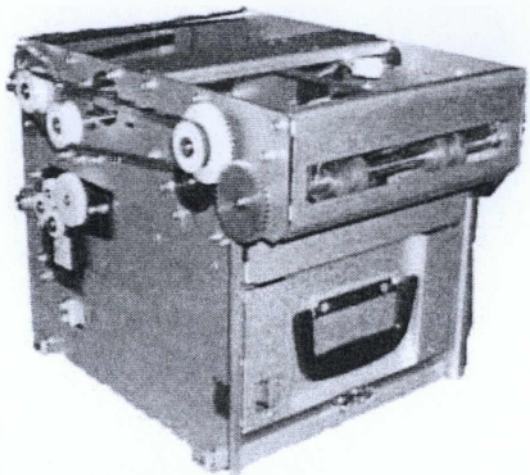
Οθόνη LCD

- Μέγεθος οθόνης: 6 "
- Mono / Color (Option)
- Ανάλυση: 320 × 240
- Χαρακτήρες Οθόνης: 40 × 15 (Πρότυπο χαρακτήρων)

Πληκτρολόγιο

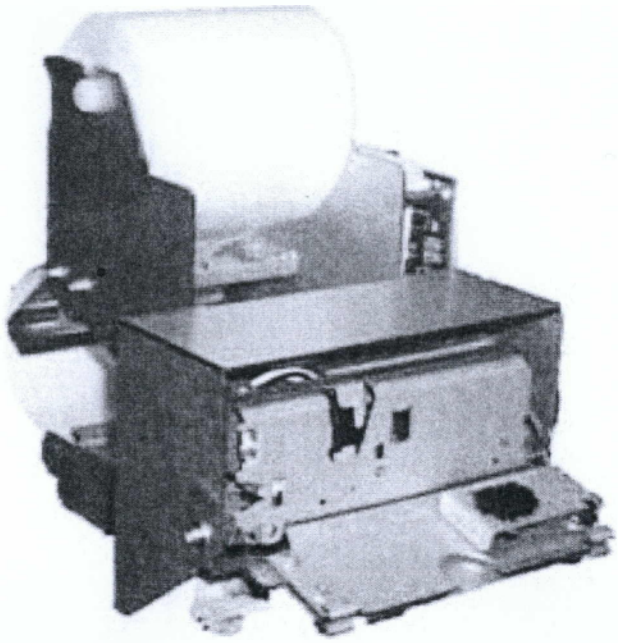
- 10 Αλφαριθμητικό <,>, CANCEL, CLEAR, ENTER, BLANK
- 8 πλήκτρα λειτουργίας
- Κάθε πλήκτρο λειτουργίας έχει αναπόσπαστα ανάγλυφα σύμβολα Braille

2.1.2Μονάδα Διανομής Μετρητών



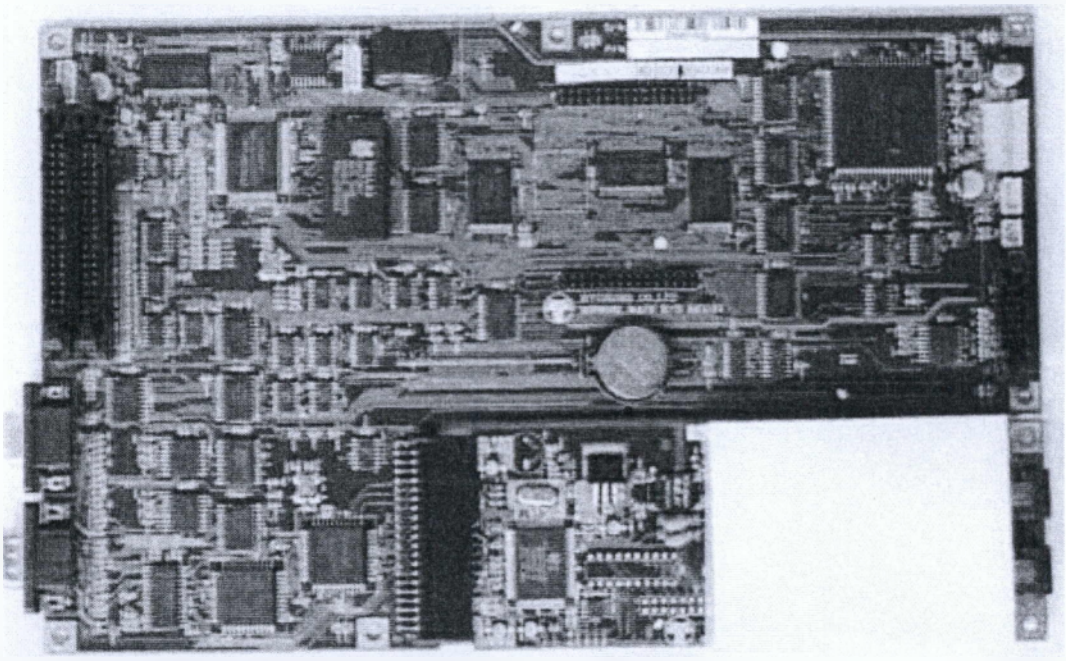
- Δοσομέτρηση ταχύτητας: 4 σημειώματα / δευτερόλεπτο
- Χωρητικότητα 1.200 νέων χαρτονομισμάτων (τυπική θήκη)
- Απόρριψη bin με χωρητικότητα 200 χαρτονομίσματα
- Ανίχνευση χαμηλής κασέτα επίπεδο
- Διπλή σημείωση εντοπισμού λειτουργικής μονάδας

2.1.3 Εκτυπωτής αποδείξεων



- Θερμικός εκτυπωτής γραμμής με κόφτη
- 36 χαρακτήρες ανά γραμμή
- Ημι-αυτόματη ρύθμιση χαρτιού σε ρολό
- Γραφική Υποστήριξη / Bar code εκτύπωσης

2.1.4 Κεντρικός πίνακας ελέγχου



- Modem: 56kbps dial-up modem (standard)
- Ηλεκτρονικό Ημερολόγιο: Μέγιστο όριο 2.000 συναλλαγές
- Μπαταρία back-up για το set-up των παραμέτρων
- Ρολόι πραγματικού χρόνου

2.1.4.1Περιβάλλον λειτουργίας

1.Απαιτήσεις ισχύος.

115 Vac ± 10% 60Hz 3.0A, 350 Watt
230 Vac ± 10% 50Hz 1.5A, 350 Watt

2.Συνδέσεις ρεύματος.

Το Mini Bank 1500 ATM πρέπει να συνδεθεί με ένα ειδικό κύκλωμα ισχύος. Αυτό το κύκλωμα πρέπει να αποτελείται από 3 γραμμές ισχύος, ουδέτερου και γείωσης και να συνδέεται άμεσα με τον διακόπτη του κύκλωματος τροφοδοσίας του πίνακα

3.Απαιτήσεις τηλεφωνικής γραμμής.

Το Mini Bank 1500 ATM πρέπει να συνδεθεί με μια ειδική τηλεφωνική γραμμή. Αυτή η γραμμή πρέπει να καλεί άμεσα ένα "τόνο" ή "παλμό" που είναι εξοπλισμένο με μία πρότυπη πρίζα τηλεφώνου(RJ-11)

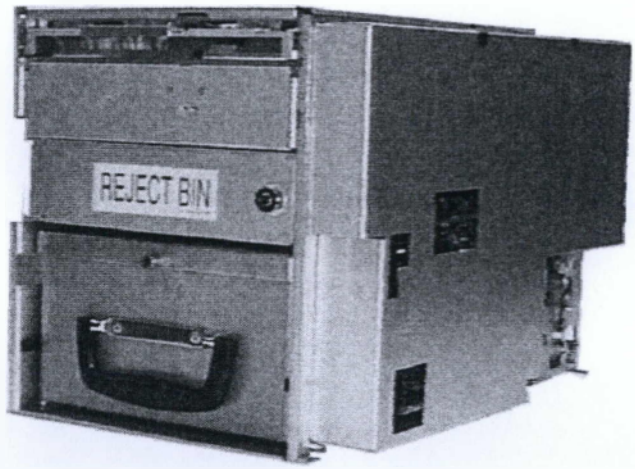
4.Θερμοκρασία

Στην αποθήκη: 32 ° F - 123 ° F (0 ° C ~ 49 ° C)
Ενώ λειτουργεί: 40 ° F - 95 ° F (5 ° C ~ 35 ° C)

5.Υγρασία

Στην αποθήκη: 10% <RH <90%, μη συμπυκνωμένο
Κατά τη διάρκεια λειτουργίας: 15% <RH <85%, μη συμπυκνωμένο

1.CDU-L Type



Ο μηχανισμός διανομής μετρητών έχει ένα ηλεκτρικό μάτι που μετράει κάθε χαρτονόμισμα, όπως βγαίνει από τον διανομέα. Ο αριθμός λογαριασμού και όλες οι πληροφορίες σχετικά με μια συγκεκριμένη συναλλαγή καταγράφεται σε ένα χαρτί.
Οι πληροφορίες τυπώνονται σε περιοδική βάση και ένα αντίγραφο διατηρείται από τον ιδιοκτήτη του μηχανήματος για δύο χρόνια. Κάθε φορά που ο κάτοχος της κάρτας έχει μια διαφορά σχετικά με μία συναλλαγή, αυτός ή αυτή μπορεί να ζητήσει την εκτύπωση που δείχνει τη συναλλαγή, και στη συνέχεια επικοινωνεί με τον κεντρικό επεξεργαστή.

Εκτός από το ηλεκτρικό μάτι που μετράει κάθε χαρτονόμισμα, ο μηχανισμός διανομής διαθέτει επίσης έναν αισθητήρα που αξιολογεί το πάχος του κάθε χαρτονομίσματος. Εάν τα δύο χαρτονομίσματα κολλήσουν μαζί, τότε αντί να διανέμονται στον κάτοχο της κάρτας που εκτρέπονται σε έναν κάδο απόρριψης. Το ίδιο συμβαίνει και με ένα χαρτονόμισμα που είναι υπερβολικά φθαρμένο, σκισμένο ή διπλωμένο.

- Δοσομέτρηση Ταχύτητας: 7 σημειώσεις / δευτερόλεπτο
- 1 Κασέτα μετρητών με χωρητικότητα 2.000 νέες σημειώσεις (US Dollar)
- Κουτί απόρριψης με χωρητικότητα 200 χαρτονομίσματα
- Ανίχνευση χαμηλής Cassette Level
- Διπλό Pick Εντοπισμός Ενότητα

2.6 Περισσότερες Συσκευές

Ένα ATM επίσης αποτελείται από τις ακόλουθες συσκευές:

- CPU για τον έλεγχο της διεπαφής του χρήστη και τις συσκευές συναλλαγής
- Μαγνητικά τσιπ ανάγνωσης καρτών (για την αναγνώριση του πελάτη)
- PIN Pad-(παρόμοια διάταξη με έναν ήχο Touch ή το πληκτρολόγιο Calculator), κατασκευάζονται συχνά μέσα σε ένα ασφαλές περίβλημα.
- Ασφαλής cryptoprocessor- γενικά μέσα σε ένα ασφαλές περίβλημα.
- Οθόνη -που χρησιμοποιείται από τον πελάτη για την εκτέλεση της συναλλαγής.
- Βασικά κουμπιά λειτουργίας (συνήθως κοντά στην οθόνη) ή μια οθόνη αφής χρησιμοποιούνται για να επιλέξετε τις διάφορες πτυχές της συναλλαγής.
- Θόλος για να αποθηκεύονται τα μέρη της μηχανής που απαιτούν περιορισμένη πρόσβαση.

Λόγω μεγαλύτερων απαιτήσεων πληροφορικής και της πτώσης της τιμής των προσωπικών υπολογιστών-όπως και των αρχιτεκτονικών, τα ATM έχουν μετακινηθεί μακριά από συνηθισμένες αρχιτεκτονικές υλικού που χρησιμοποιούν microcontrolers και αρχιτεκτονικές εφαρμογών ειδικών ολοκληρωμένων κυκλωμάτων hardware ενός προσωπικού υπολογιστή, όπως, USB συνδέσεις για περιφερειακά. Ethernet και IP επικοινωνιών, καθώς και χρήση λειτουργικών συστημάτων προσωπικών υπολογιστών. Αν και είναι αναμφισβήτητα φθηνότερο να χρησιμοποιήσουν εμπορικό hardware, αυτό κάνει τα ATM δυνητικά ευπαθή στο ίδιο είδος των προβλημάτων που παρουσιάζονται στους συμβατικούς υπολογιστές.

Παρακάτω αναλύονται περισσότερο τα υλικά μέρη που αποτελούν ένα ATM.

2.6.1 CPU

Είναι μια κεντρική μονάδα επεξεργασίας (CPU), που αναφέρεται επίσης ως μια κεντρική μονάδα επεξεργαστή, είναι το υλικό μέσα σε έναν υπολογιστή που εκτελεί τις οδηγίες ενός προγράμματος εκτελώντας την βασική αριθμητική, λογική, και λειτουργίες εισόδου / εξόδου του συστήματος. Ο όρος χρησιμοποιείται στη βιομηχανία των υπολογιστών, τουλάχιστον από τις αρχές της δεκαετίας του 1960. Η

μορφή, ο σχεδιασμός και η υλοποίηση των CPUs έχουν αλλάξει κατά τη διάρκεια της ιστορίας τους, αλλά και η θεμελιώδης λειτουργία τους παραμένει η ίδια.

Ένας υπολογιστής μπορεί να έχει περισσότερες από μία CPU. Αυτό ονομάζεται πολυεπεξεργασία. Ορισμένα ολοκληρωμένα κυκλώματα (ICs) μπορεί να περιέχουν πολλαπλές CPUs σε ένα μόνο chip.Τα εν λόγω ολοκληρωμένα κυκλώματα ονομάζονται multi-core επεξεργαστές.

Δύο τυπικά συστατικά ενός επεξεργαστή είναι η αριθμητική λογική μονάδα (ALU), η οποία εκτελεί αριθμητικές και λογικές πράξεις, και η μονάδα ελέγχου (CU), η οποία εξάγει εντολές από τη μνήμη, τις αποκωδικοποιεί και τις εκτελεί, καλώντας την ALU όταν είναι απαραίτητο.

Όλα τα υπολογιστικά συστήματα δεν είναι απαραίτητο να στηρίζονται σε μια κεντρική μονάδα επεξεργασίας. Ένας array processor ή ένας vector processor έχει πολλαπλές παράλληλες λειτουργίες υπολογιστικών στοιχείων, χωρίς μια μονάδα να θεωρείται το «κέντρο». Στο κατανεμημένο υπολογιστικό μοντέλο, τα προβλήματα λύνονται από ένα διασυνδεδεμένο κατανεμημένο σύνολο των επεξεργαστών.

Λειτουργία CPU

Η θεμελιώδης λειτουργία των περισσότερων CPUs, ανεξάρτητα από τη φυσική μορφή τους, είναι να εκτελέσουν μια ακολουθία των αποθηκευμένων οδηγιών που ονομάζεται πρόγραμμα. Το πρόγραμμα αντιπροσωπεύεται από μια σειρά αριθμών που φυλάσσονται σε κάποιο είδος της μνήμης του υπολογιστή. Υπάρχουν τέσσερα βήματα που σχεδόν όλοι οι επεξεργαστές χρησιμοποιούν στη λειτουργία τους: fetch, decode, execute, και writeback.

Το πρώτο βήμα, fetch, περιλαμβάνει μια εντολή ανάκτησης (η οποία αντιπροσωπεύεται από έναν αριθμό ή μία ακολουθία αριθμών) από τη μνήμη του προγράμματος. Η θέση στη μνήμη του προγράμματος προσδιορίζεται από ένα μετρητή προγράμματος (pc- program counter), η οποία αποθηκεύει έναν αριθμό που προσδιορίζει την τρέχουσα θέση στο πρόγραμμα.Μετά από μια εντολή fetch , το pc αυξάνεται κατά το μήκος της λέξης σε μονάδες μνήμης. Συχνά, η εντολή για να είναι δυνατή η λήψη πρέπει να ανακτηθεί από την σχετικά αργή μνήμη, προκαλώντας την CPU να καθυστερήσει, ενώ περιμένει οδηγίες για το που πρέπει να επιστραφεί. Αυτό το θέμα σε μεγάλο βαθμό αντιμετωπίζεται σε σύγχρονους επεξεργαστές από cashes και αρχιτεκτονικές pipeline.

Η σύσταση ότι η CPU καλεί από τη μνήμη χρησιμοποιείται για να καθορίσει τι η CPU πρέπει να κάνει.Στο βήμα της αποκωδικοποίησης (decode) ,η εντολή χωρίζεται σε μέρη που έχουν σημασία για άλλα τμήματα της CPU. Ο τρόπος με τον οποίο η αριθμητική τιμή ερμηνεύεται ορίζεται από το σύνολο εντολών της CPU αρχιτεκτονικής (ISA). Συχνά, μία ομάδα αριθμών στην εντολή, που ονομάζεται opcode, υποδεικνύει ποια είναι η λειτουργία για να εκτελεστεί. Τα υπόλοιπα μέρη του αριθμού συνήθως παρέχουν πληροφορίες που απαιτούνται για την εν λόγω εντολή, όπως τελεστές για μια πράξη προσθήκης. Τέτοιοι τελεστές μπορεί να χορηγηθούν ως μία σταθερή τιμή (ονομάζεται άμεση αξία), ή ως ένα μέρος για να εντοπιστεί μια αξία: ένα register ή μια διεύθυνση μνήμης, όπως καθορίζεται από κάποιο τύπο

διευθυνσιοδότησης. Σε πιο παλιά σχέδια τα τμήματα της CPU είναι υπεύθυνα για την αποκωδικοποίηση των συσκευών υλικού. Ωστόσο, σε πιο αφηρημένα και περίπλοκα CPUs και ISAs, ένα μικροπρόγραμμα συχνά χρησιμοποιείται για να βοηθήσει στη μετάφραση των οδηγιών σε διάφορα σήματα διαμόρφωσης για την CPU. Αυτό μερικές φορές είναι ένα μικρο-πρόγραμμα επανεγγράψιμο έτσι ώστε να μπορεί να τροποποιηθεί για να αλλάξει τον τρόπο που η CPU αποκωδικοποιεί οδηγίες, ακόμη και αφού έχει κατασκευαστεί.

Μετά τα βήματα fetch και decode, το βήμα execute εκτελείται. Κατά τη διάρκεια αυτού του σταδίου, τα διάφορα τμήματα της CPU συνδέονται έτσι ώστε να μπορούν να εκτελούν την επιθυμητή λειτουργία. Εάν, για παράδειγμα, μία λειτουργία προσθήκης ζητήθηκε, η αριθμητική λογική μονάδα (ALU) θα συνδεθεί με ένα σύνολο εισόδων και μια σειρά από εξόδους. Οι είσοδοι παρέχουν τους αριθμούς που πρέπει να προστεθούν και οι έξοδοι θα περιέχουν το τελικό ποσό. Η ALU περιέχει το κύκλωμα το οποίο θα εκτελέσει απλές αριθμητικές και λογικές πράξεις για τις εισροές (όπως η προσθήκη και bitwise πράξεις). Εάν η λειτουργία της πρόσθεσης παράγει ένα αποτέλεσμα πολύ μεγάλο ώστε ο επεξεργαστής να μπορεί να το χειριστεί, μια σημαία αριθμητική υπερχείλισης σε ένα μητρώο σημαιών μπορεί επίσης να ρυθμιστεί.

Το τελικό βήμα, writeback, απλά "γράφει πίσω" τα αποτελέσματα του βήματος της εκτέλεσης για κάποια μορφή μνήμης. Πολύ συχνά τα αποτελέσματα είναι γραμμένα σε κάποιο εσωτερικό καταχωρητή της CPU για γρήγορη πρόσβαση από μεταγενέστερες οδηγίες. Σε άλλες περιπτώσεις, τα αποτελέσματα μπορεί να γραφτούν σε βραδύτερη, αλλά φθηνότερα και μεγαλύτερα τμήματα, κύρια μνήμη. Ορισμένοι τύποι οδηγιών μπορούν να χειραγωγήσουν το μετρητή του προγράμματος και όχι απευθείας την παραγωγή στοιχείων που προκύπτουν. Αυτά γενικά ονομάζονται "άλματα" και διευκολύνουν τη συμπεριφορά, όπως, των υπό όρους βρόχους εκτέλεσης του προγράμματος (μέσω της χρήσης υπό όρους άλματος), και λειτουργεί στα προγράμματα. Πολλές οδηγίες θα αλλάξουν επίσης την κατάσταση των ψηφίων σε "σημαίες" που είναι καταχωρημένες σε register. Αυτές οι σημαίες μπορεί να χρησιμοποιηθούν για να επηρεάσουν το πώς συμπεριφέρεται ένα πρόγραμμα, δεδομένου ότι συχνά δείχνουν το αποτέλεσμα των διαφόρων εργασιών. Για παράδειγμα, ένας τύπος «σύγκρησης» θεωρεί δύο αξίες και θέτει έναν αριθμό στο register σημαίας σύμφωνα με τον οποίο ο ένας είναι μεγαλύτερος. Η σημαία αυτή θα μπορούσε να χρησιμοποιηθεί από μια μεταγενέστερη εντολή άλμα για τον προσδιορισμό της ροής του προγράμματος.

Μετά την εκτέλεση των εντολών και του writeback των προκυπτόντων στοιχείων, η όλη διαδικασία επαναλαμβάνεται, με τον επόμενο κύκλο εντολών κάνοντας fetch κανονικά την επόμενη-σε-αλληλουχία εντολή λόγω της αξίας που επαυξάνεται στον μετρητή προγράμματος. Αν η ολοκλήρωση ήταν ένα άλμα, ο μετρητής του προγράμματος θα πρέπει να τροποποιηθεί για να περιέχει τη διεύθυνση της εντολής που πήδηξε, και η εκτέλεση του προγράμματος συνεχίζεται κανονικά. Σε πιο περίπλοκους επεξεργαστές από αυτόν που περιγράφεται εδώ, πολλαπλές εντολές μπορεί να ληφθούν, αποκωδικοποιούνται και εκτελούνται ταυτόχρονα.

2.6.2 ΚΑΡΤΑ ΜΑΓΝΗΤΙΚΗΣ ΤΑΙΝΙΑΣ

Μια κάρτα μαγνητικής ταινίας είναι ένας τύπος κάρτας ικανός να αποθηκεύει δεδομένα, τροποποιώντας το μαγνητισμό των μικροσκοπικών τμημάτων σιδήρου με βάση τα μαγνητικά σωματίδια σε μια ζώνη μαγνητικού υλικού στην κάρτα. Η μαγνητική ταινία, μερικές φορές ονομάζεται swipe κάρτα ή magstripe, αφού διαβάζεται περνώντας μια μαγνητική κεφαλή ανάγνωσης.

Η μαγνητική εγγραφή σε ταινία χάλυβα και σε καλώδια επινοήθηκε κατά τη διάρκεια του Β Παγκοσμίου Πολέμου για την εγγραφή ήχου. Στη δεκαετία του 1950, η μαγνητική εγγραφή ψηφιακών δεδομένων από υπολογιστή σε πλαστική ταινία με επικάλυψη οξειδίου του σιδήρου εφευρέθηκε. Το 1960 η IBM χρησιμοποίησε την ιδέα της μαγνητικής ταινίας για να αναπτύξει ένα αξιόπιστο τρόπο για την ασφάλεια μαγνητικών ταινιών σε πλαστικές κάρτες, σε ένα πλαίσιο σύμβασης με την κυβέρνηση των ΗΠΑ για ένα σύστημα ασφαλείας. Μια σειρά προτύπων από τον Διεθνή Οργανισμό Τυποποίησης Προτύπων , ISO / IEC 7810, ISO / IEC 7811, ISO / IEC 7812, ISO / IEC 7813, ISO 8583 και ISO / IEC 4909, καθορίζουν πλέον τις φυσικές ιδιότητες της κάρτας, συμπεριλαμβανομένου του μεγέθους, της ευελιξίας, της θέσης, των μαγνητικών χαρακτηριστικών και τις μορφές δεδομένων. Επίσης, παρέχουν τις προδιαγραφές για τις οικονομικές κάρτες, συμπεριλαμβανομένης και της χορήγησης του φάσματος των αριθμών της κάρτας σε διαφορετικές εκδόσεις καρτών.

ΠΕΡΑΙΤΕΡΩ ΕΞΕΛΙΞΕΙΣ ΚΑΙ ΤΑ ΠΡΟΤΥΠΑ ΚΩΔΙΚΟΠΟΙΗΣΗΣ

Υπήρξαν μια σειρά από βήματα που απαιτήθηκαν για τη μετατροπή των μαγνητικών ταινιών σε μια βιομηχανικά αποδεκτή συσκευή. Τα βήματα αυτά περιλαμβάνουν:

1. Τη δημιουργία των διεθνών προτύπων για την εγγραφή περιεχομένου στην ταινία, όπως ποιες πληροφορίες, σε ποια μορφή, και με ποιο τρόπο θα καθορίζονται οι κωδικοί.
2. Το πεδίο δοκιμών η προτεινόμενη συσκευή και τα πρότυπα για την αποδοχή από την αγορά.
3. Την ανάπτυξη της παραγωγής, τα βήματα που απαιτούνται για τη μαζική παραγωγή του μεγάλου αριθμού των καρτών που απαιτούνται.
4. Το θέμα προσθήκης λωρίδας και τις δυνατότητες αποδοχής στο διαθέσιμο εξοπλισμό. Τα βήματα αυτά αρχικά ελεγχόντουσαν από τον Jerome Svigals των Προηγμένων Συστημάτων της IBM.

Στις περισσότερες κάρτες μαγνητικής ταινίας , η μαγνητική ταινία περιέχεται σε ένα πλαστικό όπως το φιλμ. Η μαγνητική ταινία βρίσκεται 0,223 ίντσες (5,66 mm) από το άκρο της κάρτας, και έχει 0,375 ίντσες (9,52 mm) πλάτος. Η μαγνητική ταινία περιέχει τρία κομμάτια, το καθένα 0,110 ίντσες (2.79 mm). Τα κομμάτια ένα και τρία καταγράφονται στα 210 bits ανά ίντσα (8.27 bits ανά mm), ενώ η τροχιά δύο τυπικά έχει μία πυκνότητα εγγραφής των 75 bits ανά ίντσα (2.95 bits ανά mm). Κάθε

κομμάτι μπορεί να περιέχει είτε 7-bit αλφαριθμητικών χαρακτήρων, ή 5-bit αριθμητικών χαρακτήρων.

- Track 1 πρότυπα που δημιουργήθηκαν από τη βιομηχανία των αεροπορικών εταιρειών (IATA).
- Track 2 πρότυπα που δημιουργήθηκαν από τον τραπεζικό κλάδο (ABA).
- Track 3 πρότυπα που δημιουργήθηκαν από τη βιομηχανία Ταμιευτηρίου.

Παραδείγματα των καρτών και της τήρησης αυτών των προτύπων περιλαμβάνουν τις ATM κάρτες, τις τραπεζικές κάρτες (πιστωτικές και χρεωστικές, συμπεριλαμβανομένων VISA και MasterCard), κάρτες δώρων, κάρτες πελατειακής πίστης, άδειες οδήγησης, τηλεκάρτες, κάρτες μέλους, ηλεκτρονικές κάρτες μεταφοράς παροχών (π.χ. κουπόνια τροφίμων), και σχεδόν κάθε εφαρμογή στην οποία αξίας ή ασφαλείς πληροφορίες δεν αποθηκεύονται στο ίδιο το φύλλο. Πολλά κέντρα βιντεοπαιχνιδιών και διασκέδασης χρησιμοποιούν πλέον τις χρεωστικές, κάρτες συστήματα που βασίζονται σε κάρτες μαγνητικής ταινίας.

Η κλωνοποίηση της μαγνητικής ταινίας μπορεί να ανιχνευθεί με την εφαρμογή των μαγνητικών κεφαλών-αναγνώστη καρτών και το λογισμικό που μπορεί να διαβάσει μια υπογραφή του μαγνητικού θορύβου τα οποία ενσωματώνονται σε όλες τις μαγνητικές ταινίες κατά τη διάρκεια της διαδικασίας παραγωγής της κάρτας. Η υπογραφή μπορεί να χρησιμοποιηθεί σε συνδυασμό με δύο κοινών καθεστώτων ταυτότητας παράγοντας που χρησιμοποιείται στα ATM, χρεωστική / λιανικής αγορά και προπληρωμένη κάρτα.

Αντιπαραδείγματα των καρτών που αγνοούν σκόπιμα τα πρότυπα ISO περιλαμβάνουν τις κάρτες-κλειδιά ξενοδοχείων, τις κάρτες μετρό και λεωφορείων, και ορισμένες εθνικές κάρτες προπληρωμένου χρόνου (όπως για τη χώρα της Κύπρου), στην οποία το υπόλοιπο αποθηκεύεται και διατηρείται άμεσα στην ταινία και να μην προέρχεται από μια απομακρυσμένη βάση δεδομένων.

Η μετάβαση στις έξυπνες κάρτες

Οι έξυπνες κάρτες είναι μια νεώτερη γενιά καρτών που περιέχει ένα τσιπ ολοκληρωμένων κυκλωμάτων. Η κάρτα μπορεί να έχει μεταλλικές επαφές που συνδέουν την κάρτα φυσικά για τον αναγνώστη, ενώ οι ανέπαφες κάρτες χρησιμοποιούν ένα μαγνητικό πεδίο ή ραδιοσυχνότητες (RFID) για την ανάγνωση εγγύτητας.

Οι υβριδικά έξυπνες κάρτες περιλαμβάνουν μία μαγνητική λωρίδα εκτός από το τσιπ - αυτό πιο συχνά βρίσκεται σε μια κάρτα πληρωμής, έτσι ώστε οι κάρτες να είναι επίσης συμβατές με τα τερματικά πληρωμής που δεν περιλαμβάνουν ένα αναγνώστη έξυπνης κάρτας.

Οι κάρτες με τα τρία χαρακτηριστικά: Μαγνητική ταινία, έξυπνη κάρτα με τσιπ, και το RFID chip είναι επίσης όλο και πιο κοινές αφού όλο και περισσότερες δραστηριότητες απαιτούν τη χρήση αυτών των καρτών.

Ένας άλλος τύπος της κάρτας είναι ένα Chip και PIN card. Με αυτή την συγκεκριμένη κάρτα, η πληροφορία μεταδίδεται μέσω ενός SmartChip με ένα ασφαλές πείρο. Η κάρτα δεν είναι πλέον απαραίτητη.

2.6.3 ΕΞΥΠΝΗ ΚΑΡΤΑ

Μια έξυπνη κάρτα, μια κάρτα chip, ή ένα ολοκληρωμένο κύκλωμα της κάρτας (ICC) είναι μία οποιαδήποτε κάρτα τσέπης με ενσωματωμένο ολοκληρωμένο κύκλωμα. Οι έξυπνες κάρτες είναι κατασκευασμένες από πλαστικό, συνήθως χλωριούχο πολυβινύλιο, αλλά μερικές φορές τερεφθαλικό πολυαιθυλένιο με βάση πολυεστέρες, ακρυλονιτριλίου βουταδιενίου στυρολίου ή πολυανθρακικό.

Οι έξυπνες κάρτες μπορούν να παρέχουν ταυτοποίηση, έλεγχο γνησιότητας, αποθήκευσης και επεξεργασίας δεδομένων εφαρμογής. Οι έξυπνες κάρτες μπορούν να παρέχουν ισχυρή ταυτότητα ασφαλείας για single sign-on (SSO) και σε μεγάλους οργανισμούς.

Σχεδιασμός μιάς έξυπνης κάρτας

Η έξυπνη κάρτα μπορεί να έχει τα ακόλουθα γενικά χαρακτηριστικά:

- Διαστάσεις παρόμοιες με εκείνες μιας πιστωτικής κάρτας. ID-1 του ISO / IEC 7810 πρότυπο που ορίζει τις κάρτες 85,60 από 53,98 χιλιοστά (3.370 × 2.125 in). Ένα άλλο δημοφιλές μέγεθος είναι το ID-000, το οποίο είναι 25 × 15 mm (0.984 × 0.591 σε in) (χρησιμοποιούνται συνήθως σε κάρτες SIM). Και οι δύο είναι 0,76 χιλιοστά (0,030 in) σε πάχος.
- Περιέχει ένα ανθεκτικό στην παραβίαση σύστημα ασφαλείας (για παράδειγμα ένα ασφαλές cryptoprocessor και ένα ασφαλές σύστημα αρχείων) και παρέχει υπηρεσίες ασφαλείας (π.χ., προστατεύει στη μνήμη πληροφοριών).
- Υπεύθυνο για τη διαχείριση ενός συστήματος που ανταλλάσει με ασφάλεια πληροφορίες και τη διαμορφώνει τις ρυθμίσεις της κάρτα, τον έλεγχο της μαύρης λίστας καρτών και ενημερώνει τις εφαρμογές δεδομένων.
- Επικοινωνεί με εξωτερικές υπηρεσίες μέσω της συσκευής ανάγνωσης καρτών, όπως οι αναγνώστες εισιτηρίων, ATM, κ.λπ.

Η επικοινωνία με έξυπνες κάρτες

Οι έξυπνες κάρτες έχουν μια επιφάνεια επαφής περίπου 1 τετραγωνικό εκατοστό (0,16 sq in),που περιλαμβάνει διάφορα επίχρυσα βύσματα επαφής-είναι ο τρόπος επικοινωνίας τους. Αυτά τα επιθέματα παρέχουν ηλεκτρική συνδεσιμότητα όταν εισάγεται σε έναν αναγνώστη, τα οποία χρησιμοποιούνται ως μέσο επικοινωνίας μεταξύ της έξυπνης κάρτας και του ξενιστή (π.χ., ένας υπολογιστής, ένα σημείο του τερματικού πώλησης), ή ενός κινητού τηλεφώνου. Κάρτες δεν περιέχουν μπαταρίες. Η ισχύς παρέχεται από τη συσκευή ανάγνωσης καρτών.

Τα ISO / IEC 7810 και ISO / IEC 7816 είναι σειρά προτύπων που ορίζουν:

i. Τη φυσική κατάσταση και τα χαρακτηριστικά
ii. Τις ηλεκτρικές θέσεις υποδοχής και σχήματα
iii. Τα ηλεκτρικά χαρακτηριστικά
iv. Τα πρωτόκολλα επικοινωνίας, συμπεριλαμβανομένων των εντολών που αποστέλλονται προς την κάρτα και τις απαντήσεις από την κάρτα
v. Τις βασικές λειτουργίες

Επειδή τα τσιπ στις οικονομικές κάρτες είναι ίδια με αυτές που χρησιμοποιούνται σε μονάδες συνδρομητών ταυτότητας (κάρτες SIM) στα κινητά τηλέφωνα, προγραμματίζονται διαφορετικά και ενσωματώνονται σε ένα διαφορετικό κομμάτι του PVC, οι κατασκευαστές τσιπ ορίζουν τα πιο απαιτητικά GSM/3G πρότυπα. Έτσι, για παράδειγμα, αν και το πρότυπο EMV chip επιτρέπει σε μια κάρτα για να αντλήσει 50 mA από το τερματικό της, οι κάρτες είναι συνήθως πολύ κάτω από 6 mA όριο της βιομηχανίας του τηλεφώνου. Αυτό επιτρέπει μικρότερα και φθηνότερα οικονομικά τερματικά καρτών.

Τα πρωτόκολλα επικοινωνίας για την επαφή έξυπνων καρτών περιλαμβάνουν T = 0 (σε επίπεδο χαρακτήρων πρωτόκολλο μετάδοσης, όπως ορίζεται στο ISO / IEC 7816-3) και T = 1 (block-level πρωτόκολλο μετάδοσης, όπως ορίζεται στο ISO / IEC 7816-3).

Οι έξυπνες κάρτες μπορούν επίσης να χρησιμοποιηθούν ως ηλεκτρονικά πορτοφόλια. Η έξυπνη κάρτα με τσιπ μπορεί να «φορτωθεί» με κεφάλαια για να πληρώσει παρκόμετρα, μηχανήματα αυτόματης πώλησης ή εμπόρους. Κρυπτογραφικά πρωτόκολλα προστατεύουν την ανταλλαγή των χρημάτων μεταξύ της έξυπνης κάρτας και του μηχανήματος. Δεν είναι απαραίτητη η σύνδεση με την τράπεζα. Ο κάτοχος της κάρτας μπορεί να τη χρησιμοποιήσει ακόμη και αν δεν είναι ο ιδιοκτήτης. Παραδείγματα είναι οι Proton, Geldkarte, Chipknip και Moneo. Η γερμανική Geldkarte χρησιμοποιείται επίσης για να επικυρώσει την ηλικία του πελάτη σε μηχανήματα αυτόματης πώλησης για τσιγάρα.
Αυτές είναι οι πιο γνωστές κάρτες ATM (κλασική πλαστική κάρτα):

- Visa: Visa Contactless, Quick VSDC, "qVSDC", Visa Wave, MSD, payWave
- MasterCard: PayPass Magstripe, PayPass MChip
- American Express: ExpressPay
- Discover: Zip

2.6.4 PIN-PAD

Ένα PIN PAD ή μια συσκευή εισόδου PIN, είναι μια ηλεκτρονική συσκευή που χρησιμοποιείται σε μια χρεωστική, πιστωτική ή έξυπνη κάρτα που βασίζεται στην αξία να αποδεχθεί και να κρυπτογραφήσει τον προσωπικό αριθμό αναγνώρισης του κατόχου της κάρτας (PIN). Το PIN PAD συνήθως χρησιμοποιείται σε σημεία όπου μια ηλεκτρονική ταμειακή μηχανή είναι υπεύθυνη για τη λήψη του ποσού

πώλησης και την έναρξη / το χειρισμό της συναλλαγής. Το PIN PAD χρησιμοποιείται έτσι ώστε ο πελάτης να μπορεί να έχει πρόσβαση στην κάρτα (στην περίπτωση των έξυπνων καρτών) και το PIN μπορεί με ασφάλεια να κρυπτογραφηθεί προτού σταλεί στο διαχειριστή των συναλλαγών ή στην τράπεζα. Σε ορισμένες περιπτώσεις, με κάρτες που έχουν chip. το PIN μεταφέρεται μόνο από το PIN PAD στο τσιπ και εκεί ελέγχεται από την κάρτα. Στην περίπτωση αυτή, το PIN δεν χρειάζεται να σταλεί στο σύστημα της τράπεζας ή στην κάρτα για επαλήθευση. (Αυτό είναι γνωστό ως «offline επαλήθευση PIN").

Όπως τα stand-alone σημεία των συσκευών ATM, τα PIN PAD είναι εξοπλισμένα με το υλικό και το λογισμικό ασφαλείας για να διασφαλιστεί ότι τα κλειδιά ασφαλείας και το PIN διαγράφονται όταν κάποιος προσπαθήσει να παρέμβει στη συσκευή. Το PIN κρυπτογραφείται αμέσως μετά την είσοδο και ένα κρυπτογραφημένο μπλοκ PIN δημιουργείται. Αυτό το κρυπτογραφημένο PIN -μπλοκ διαγράφεται αμέσως μόλις σταλεί από το PIN PAD στη συσκευή ATM ή / στο τσιπ της κάρτας. Το PIN κρυπτογραφείται χρησιμοποιώντας μια ποικιλία συστημάτων κρυπτογράφησης, η πιο κοινή είναι το τριπλό DES.

Το PIN PAD πρέπει να εγκριθεί με τα πρότυπα που απαιτεί η βιομηχανία καρτών για πληρωμές έτσι ώστε να εξασφαλισθεί ότι παρέχει επαρκή ασφάλεια στο σημείο εισόδου PIN και στη διαδικασία κρυπτογράφησης PIN. Το ISO 9564 είναι το διεθνές πρότυπο για τη διαχείριση PIN και την ασφάλεια, και προσδιορίζει ορισμένες απαιτήσεις και χαρακτηριστικά των συσκευών εισόδου PIN.

Παρά το γεγονός ότι τα PIN PAD επιτρέπουν την είσοδο σε αριθμητικές τιμές, ορισμένα PIN PAD έχουν επίσης γράμματα που αντιστοιχούν σε περισσότερα ψηφία, ώστε να επιτραπεί η χρήση αλφαβητικών χαρακτήρων ή μια φράση ως υπενθύμιση για το αριθμητικό PIN. Δεν έχουν όλα τα PIN PAD αναγκαστικά τα ίδια γράμματα για τους ίδιους αριθμούς. Το ISO 9564 δεν επιβάλλει καμία συγκεκριμένη ανάθεση γραμμάτων, και περιλαμβάνει δύο παραδείγματα που διαφέρουν ως προς το ψηφίο στο οποίο Q και Z.

2.6.5 Ασφαλής κρυπτο-επεξεργαστής

Ένας ασφαλής κρυπτο-επεξεργαστής είναι ένα ειδικό μέρος σε ένα τσιπ ή μικροεπεξεργαστή για τη διεξαγωγή κρυπτογραφικών λειτουργιών, ενσωματωμένο σε μια συσκευασία με πολλαπλά μέτρα υλικής ασφάλειας, που του δίνουν ένα βαθμό αντίστασης στην παραβίαση. Σε αντίθεση με τους κρυπτογραφικούς επεξεργαστές η πληροφορία που εξάγεται αποκρυπτογραφείται σε ένα bus που είναι ένα ασφαλές περιβάλλον, ένας ασφαλής κρυπτο-επεξεργαστής δεν εξάγει αποκρυπτογραφημένα δεδομένα ή οδηγίες αποκρυπτογράφησης του προγράμματος σε ένα περιβάλλον όπου η ασφάλεια δεν μπορεί να διατηρηθεί.

Ο σκοπός ενός ασφαλούς κρυπτο-επεξεργαστή είναι να ενεργεί ως θεμέλιος λίθος της ασφάλειας του υπο-συστήματος, εξαλείφοντας την ανάγκη για την προστασία του υπόλοιπου υπο-συστήματος με τα μέτρα υλικής ασφάλειας.

Οι ασφαλείς κρυπτο-επεξεργαστές, ενώ είναι χρήσιμοι, δεν είναι άτρωτοι σε επιθέσεις, ιδιαίτερα απέναντι σε καλά εξοπλισμένους και αποφασισμένους αντιπάλους (π.χ. υπηρεσία πληροφοριών της κυβέρνησης), οι οποίοι είναι πρόθυμοι να δαπανήσουν τεράστιους πόρους για το έργο.

Μία επίθεση σε έναν ασφαλή κρυπτο-επεξεργαστή στόχευε τον IBM 4758. Μια ομάδα στο Πανεπιστήμιο του Cambridge ανέφερε την επιτυχή εξαγωγή των απόρρητων πληροφοριών από έναν IBM 4758, χρησιμοποιώντας ένα συνδυασμό μαθηματικών, καθώς και ειδικού σκοπού hardware codebreaking. Ωστόσο, αυτή η επίθεση δεν ήταν πρακτική σε πραγματικά συστήματα, διότι απαιτούσε ο εισβολέας να έχει πλήρη πρόσβαση σε όλες τις λειτουργίες API της συσκευής. Κανονικές και συνιστώμενες πρακτικές χρησιμοποιούν το ενσωματωμένο σύστημα ελέγχου πρόσβασης για να χωρίσει την εξουσία, έτσι ώστε κανένας άνθρωπος δεν θα μπορούσε να εξαπολύσει την επίθεση.

Ενώ η ευπάθεια που εκμεταλλεύτηκαν ήταν ένα ελάττωμα στο λογισμικό που έχει φορτωθεί στο 4758, και όχι η ίδια η αρχιτεκτονική του 4758, η επίθεσή τους χρησιμεύει ως υπενθύμιση ότι ένα σύστημα ασφαλείας είναι τόσο ασφαλές όσο ο πιο αδύναμος κρίκος της: ο ισχυρός δεσμός του υλικού του 4758 είχε καταστεί άχρηστο από ελάττωμα στο σχεδιασμό και στις προδιαγραφές του λογισμικού που φορτώθηκαν σε αυτό.

Μορφές επίθεσης σε έξυπνες κάρτες

Οι έξυπνες κάρτες είναι πολύ πιο ευάλωτες, καθώς είναι πιο ανοικτές σε φυσική επίθεση. Σε περίπτωση πλήρους κρυπτογράφησης των εφαρμογών του δίσκου, ιδιαίτερα όταν εφαρμόζεται χωρίς εκκίνηση PIN, ο κρυπτο-επεξεργαστής δεν θα είναι ασφαλής σε επίθεση εάν τα δεδομένα που παραμένουν θα μπορούσαν να αξιοποιηθούν για την αποτύπωση των περιεχομένων της μνήμης αφού το λειτουργικό σύστημα έχει ανακτήσει τα κλειδιά κρυπτογράφησης από το TPM της.

Ωστόσο, εάν όλα τα ευαίσθητα δεδομένα αποθηκεύονται μόνο στη μνήμη του κρυπτο-επεξεργαστή και όχι στην εξωτερική μνήμη και αυτός έχει σχεδιαστεί για να είναι σε θέση να αποκαλύψει τα κλειδιά ή τα αποκρυπτογραφημένα ή τα μη κρυπτογραφημένα δεδομένα σε chip, τότε τα προστατευμένα δεδομένα θα είναι προσβάσιμα μόνο όταν στο chip του κρυπτο-επεξεργαστής αφαιρείται κάθε συσκευασία και στρώμα μεταλλικής θωράκισης. Αυτό θα απαιτήσει τόσο την φυσική κατοχή της συσκευής καθώς και τις δεξιότητες και τον εξοπλισμό πέρα από αυτό των περισσότερων ατόμων του τεχνικού προσωπικού.

Άλλες μέθοδοι επίθεσης περιλαμβάνουν την προσεκτική ανάλυση του χρονοδιαγράμματος των διαφόρων ενεργειών που θα μπορούσαν να ποικίλουν ανάλογα με την μυστική αξία ή τη χαρτογράφηση της κατανάλωσης ρεύματος συναρτήσει του χρόνου για να εντοπιστούν διαφορές στον τρόπο που τα '0 ' bits αντιμετωπίζονται εσωτερικά ώς '1' bits. Ο εισβολέας μπορεί να εφαρμόσει ακραίες θερμοκρασίες, υπερβολικά υψηλές ή χαμηλές συχνότητες ρολογιού ή τάση

τροφοδοσίας που υπερβαίνει τις προδιαγραφές, ώστε να προκαλέσει ένα σφάλμα. Ο εσωτερικός σχεδιασμός του κρυπτο-επεξεργαστή μπορεί να προσαρμοστεί για να αποτρέψει τις επιθέσεις αυτές.

Μερικοί ασφαλείς επεξεργαστές περιέχουν δύο πυρήνες και δημιουργούν απρόσιτα κλειδιά κρυπτογράφησης όταν χρειάζεται, έτσι ώστε ακόμη και αν το κύκλωμα αντιστραφεί μηχανικά, δεν θα αποκαλύψει οποιαδήποτε πλήκτρα είναι αναγκαία για να ασφαλίσει το λογισμικό.

Το πρώτο σχέδιο απλού τσιπ κρυπτο-επεξεργαστή ήταν για την προστασία αντιγραφής λογισμικού προσωπικού υπολογιστή (βλέπε αμερικανικό δίπλωμα ευρεσιτεχνίας 4.168.396, 18 Σεπτεμβρίου, 1979) και ήταν εμπνευσμένο από Ανοικτή Επιστολή του Bill Gates για χομπίστες.

2.6.6 ΠΛΗΚΤΡΑ ΛΕΙΤΟΥΡΓΙΑΣ

Τα πλήκτρα λειτουργίας είναι βασικά σε έναν υπολογιστή ή τερματικό και ουσιαστικά αποτελούν το διερμηνέα εντολών έτσι ώστε να εκτελέσει το λειτουργικό σύστημα τις λειτουργίες του. Τα πλήκτρα λειτουργιών σε ένα τερματικό μπορεί να δημιουργήσουν βραχυπρόθεσμα σταθερές σειρές χαρακτήρων και συχνά αρχίζουν με το χαρακτήρα διαφυγής (ASCII 27), ή τους χαρακτήρες που παράγουν και μπορούν να ρυθμιστούν με την αποστολή ειδικών ακολουθιών χαρακτήρων στο τερματικό. Σε ένα τυπικό πληκτρολόγιο του ATM, τα πλήκτρα λειτουργίας μπορεί να δημιουργήσουν ένα σταθερό, ενιαίο κώδικα byte, έξω από την κανονική ASCII σειρά, η οποία μεταφράζεται σε κάποια άλλη ακολουθία ρύθμισης από τον οδηγό του πληκτρολόγιου ή άλλη διάταξη και ερμηνεύεται απευθείας από το πρόγραμμα εφαρμογής. Τα πλήκτρα λειτουργιών, μπορεί να έχουν (συντομογραφίες) ως προεπιλεγμένες ενέργειες που εκτελούνται συνήθως πληκτρολογώντας "ΕΠΙΒΕΒΑΙΩΣΗ","ΑΚΥΡΩΣΗ" κ.τ.λ.

2.6.7 ΘΟΛΟΣ

Ο θόλος ενός ATM είναι μέσα στο σώμα της ίδιας της συσκευής και είναι το μέρος όπου φυλάσσονται τα χαρτονομίσματα.
Μηχανισμοί που βρίσκονται μέσα στο θόλο μπορούν να περιλαμβάνουν:

1. Μηχανισμό διανομής για την παροχή μετρητών ή άλλα αντικείμενα αξίας.
2. Μηχανισμό ασφαλείας συμπεριλαμβανομένης μιας μονάδας επεξεργασίας για έλεγχο για να επιτρέπει στον πελάτη να κάνει καταθέσεις.
3. Αισθητήρες ασφαλείας (Μαγνητικούς, θερμικούς, σεισμικούς, φυσικού αερίου)
4. Κλειδαριές: -για να εξασφαλιστεί ελεγχόμενη πρόσβαση στα περιεχόμενα του θόλου.
5. Συστήματα εκτυπώσεων. Πολλά από αυτά είναι ηλεκτρονικά.
   Ουσιαστικά είναι μια σφραγισμένη συσκευή μνήμης flash που βασίζονται σε ένα πραγματικό εκτυπωτή, το οποίο συγκεντρώνει όλα τα αρχεία τών δραστηριοτήτων

συμπεριλαμβανομένων των ώρων πρόσβασης, τον αριθμό των σημειώσεων που διανέμονται, κλπ. - Αυτά θεωρούνται ευαίσθητα δεδομένα και ασφαλίζονται με παρόμοιο τρόπο με τα μετρητά. δεδομένου ότι είναι μια παρόμοια υποχρέωση από τις τράπεζες.

Οι θόλοι των ATM παρέχονται από τους κατασκευαστές σε πολλές ποιότητες. Παράγοντες που επηρεάζουν το θόλο είναι το κόστος, το βάρος, οι απαιτήσεις, ο τύπος του, οι πρακτικές αποφυγής των κινδύνων και οι εσωτερικές απαιτήσεις.

Οι κατασκευαστές συνιστούν ένα θόλο να συνδέεται με το πάτωμα για να αποτρέψει την κλοπή. Αν και υπάρχει μια καταγραφή κλοπής που πραγματοποιήθηκε ανοίγοντας τρύπα στο δάπεδο.

ΚΕΦΑΛΑΙΟ 3: ΑΣΦΑΛΕΙΑ

Ο τομέας της ασφάλειας σε ένα ATM ουσιαστικά αποτελεί ένα από τα σημαντικότερα ζητήματα για ένα κατασκευαστή και για την τράπεζα που θα το χρησιμοποιήσει.

Οι περισσότερες τράπεζες ακολουθούν το πρωτόκολλο SET (Secure Electronic Transaction), που υποστηρίζεται από τους δύο σημαντικότερους χρηματοπιστωτικούς οργανισμούς, τη MasterCard και τη Visa, καθώς και από εταιρίες όπως η IBM, η Microsoft και η Netscape. Το πρωτόκολλο SET βασίζεται στην κρυπτογραφία. Δύο είναι οι κύριες μέθοδοι κρυπτογράφησης: η συμμετρική και η ασύμμετρη.

3.1 Συμμετρική Κρυπτογραφία

Στη συμμετρική, η κρυπτογράφηση υλοποιείται με τη χρήση του ίδιου "κλειδιού", τόσο στην κωδικοποίηση όσο και στην αποκωδικοποίηση. Πράγμα το οποίο σημαίνει ότι ο αποστολέας και ο παραλήπτης του μηνύματος μοιράζονται το ίδιο κλειδί. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, κατά συνέπεια, απαιτείται κάποιο ασφαλές μέσο για τη μετάδοσή του, όπως μια προσωπική συνάντηση, κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Ένας από τους πιο γνωστούς αλγόριθμους που χρησιμοποιούν αυτή τη μέθοδο είναι το DES (Data Encryption Standard), που χρησιμοποιείται από τραπεζικούς οργανισμούς για τη δημιουργία των αριθμών PIN.

3.2 Συμμετρική Κρυπτογραφία

Η ασύμμετρη κρυπτογράφηση χρησιμοποιεί δύο κλειδιά: το ένα (κοινό κλειδί) για να κωδικοποιήσει το μήνυμα και ένα άλλο (ιδιωτικό κλειδί) για να το αποκωδικοποιήσει. Ένα μήνυμα που θα κωδικοποιηθεί με το ένα κλειδί θα μπορέσει να αποκωδικοποιηθεί μόνο με το άλλο. Η τράπεζα μπορεί να διανείμει το κοινό κλειδί, κρατώντας το ιδιωτικό κλειδί για την αποκωδικοποίηση.

Όσον αφορά στις τραπεζικές συναλλαγές, κάθε τράπεζα ακολουθεί τη δική της λύση, όπως είναι οι αριθμοί PIN, τα ψηφιακά πιστοποιητικά και οι αριθμοί TAN, που ακολουθούν κάθε συναλλαγή. Υπάρχουν αρκετές εταιρίες που μπορεί να χρησιμοποιήσει ένας οργανισμός για να πετύχει ασφαλή πρόσβαση. Μία από αυτές είναι η VeriSign, το λογισμικό της οποίας χρησιμοποιείται στις τραπεζικές όσο και σε άλλου τύπου διαδικτυακές συναλλαγές.

Η πιστοποίηση της ταυτότητας του χρήστη και κάθε συναλλαγή του εξασφαλίζονται με τη βοήθεια ενός μοναδικού ψηφιακού πιστοποιητικού (digital certificate). Αυτό το πιστοποιητικό αναγνωρίζει τον υπολογιστή του χρήστη και επιτρέπει τις συναλλαγές και τις μεταφορές χρημάτων μεταξύ λογαριασμών μόνο από το συγκεκριμένο υπολογιστή. Τα πιστοποιητικά αυτά εξασφαλίζονται εγκαθιστώντας ένα πρόγραμμα από την αντίστοιχη εταιρία πιστοποίησης.

Παρά τις εξελιγμένες μεθόδους για τη διασφάλιση των τραπεζικών συναλλαγών, η συχνότητα των ηλεκτρονικών επιθέσεων αυξάνεται τα τελευταία χρόνια. Η αύξηση αυτή προκαλεί ανησυχία στους ειδικούς, καθώς διακυβεύονται τεράστια ποσά, ειδικά στις περιπτώσεις κατά τις οποίες θύματα απάτης γίνονται

επιχειρήσεις.

Οι επίδοξοι εισβολείς έχουν πολλούς τρόπους για να επιτύχουν τους σκοπούς τους. Οι μεγαλύτεροι κίνδυνοι δεν προέρχονται από ατέλειες των συστημάτων ασφαλείας και κρυπτογράφησης αλλά από τον ανθρώπινο παράγοντα. Έρευνες ειδικών σε θέματα ασφάλειας αποδεικνύουν ότι στις περισσότερες περιπτώσεις επιθέσεων, οι εισβολείς είτε είχαν την ακούσια -συνήθως- βοήθεια και κάποιου που εργαζόταν στην τράπεζα, είτε υπέκλεψαν κωδικούς χρηστών. Οι επιχειρήσεις-πελάτες είναι συνήθως προσεκτικές και χρησιμοποιούν συστήματα ασφαλείας στα δίκτυά τους. Την ίδια "σοφία" ή προσοχή δεν δείχνουν και οι ιδιώτες πελάτες, οι περισσότεροι από τους οποίους δεν χρησιμοποιούν λογισμικό για ασφάλεια.

Οι απλοί χρήστες γίνονται εύκολα θύματα προγραμμάτων που στην πραγματικότητα ανοίγουν "τρύπες" ασφάλειας στο σύστημα επιτρέποντας σε επιτήδειους να έχουν πρόσβαση σε αυτό. Ωστόσο και οι επιχειρήσεις δεν είναι πάντοτε ασφαλείς. Σε ορισμένες περιπτώσεις, εταιρίες συνεργάζονται με τράπεζες προκειμένου να διαχειριστούν τις πληρωμές των λογαριασμών και τις συναλλαγές με εταιρικούς πελάτες. Οι τράπεζες ενίοτε επιτρέπουν στις εταιρίες αυτές να διαχειρίζονται ολόκληρο το δίκτυό τους. Σε αυτήν την περίπτωση, οι επιτήδειοι μελετούν τον τρόπο με τον οποίο οι επιχειρήσεις επεξεργάζονται τις πληρωμές και μεταφέρουν τα χρήματα. Μόλις βρεθεί μια αδυναμία, μεταφέρουν με λίγες απλές κινήσεις ολόκληρους εταιρικούς λογαριασμούς στις προσωπικές τους θυρίδες.

3.3 SET(SECURE ELECTRONIC TRANSACTION)

Το SET ουσιαστικά αποτελεί μορφή πρωτοκόλλου για ηλεκτρονικές πληρωμές με πιστωτική κάρτα. Όπως υποδηλώνει το όνομα τοπρωτόκολλο ασφαλούς ηλεκτρονικής συναλλαγής (secure electronic transaction-SET) χρησιμοποιείται για να διευκολύνει την ασφαλή διαβίβαση των πληροφοριών των πιστωτικών καρτών μέσω ηλεκτρονικών λεωφόρων, όπως το Διαδίκτυο. Το SET μπλοκάρει τις λεπτομέρειες των πληροφοριών της πιστωτικής κάρτας, εμποδίζοντας έτσι τους εμπόρους, τους χάκερ και τους κλέφτες να έχουν ηλεκτρονική πρόσβαση σε αυτές τις πληροφορίες.

Αυτό το πρωτόκολλο υποστηρίχθηκε αρχικά από τον Mastercard, Visa, Microsoft, Netscape, και άλλες. Ουσιαστικά με το SET, ένας χρήστης έχει ένα ηλεκτρονικό πορτοφόλι (ψηφιακό πιστοποιητικό) και η συναλλαγή διεξάγεται και επαληθεύεται χρησιμοποιώντας ένα συνδυασμό των πιστοποιητικών και των ψηφιακών υπογραφών μεταξύ του αγοραστή και του έμπορου, και η τράπεζα του αγοραστή κατά τρόπο που να εξασφαλίζει την προστασία της ιδιωτικής ζωής και του απορρήτου. Το SET κάνει χρήση του Secure Sockets Layer της Netscape (SSL), Secure Transaction Technology της Microsoft (STT) και Secure Hypertext Transfer Protocol (S-HTTP). Το SET χρησιμοποιεί ορισμένες, αλλά όχι όλες τις πτυχές της Υποδομής Δημοσίου Κλειδιού (PKI).

3.3.1 Λίγα λόγια για την πορεία του.

Το SET αναπτύχθηκε από τη SETco, υπό την ηγεσία της VISA και της MasterCard (και αφορούν και άλλες εταιρίες όπως οι GTE, IBM, Microsoft, Netscape, RSA, Safelayer - πρώην έργα της SETco – και τη VeriSign. Το VeriFone υλοποίησε μία από τις πρώτες πύλες πληρωμών μέσω του Internet που χρησιμοποιήθηκε από αρκετές κυρίαρχες τράπεζες οι οποίες συμμετείχαν ενεργά αρχής γενομένης από το 1996.

Το SET βασίστηκε στα πιστοποιητικά X.509 με πολλές προεκτάσεις. Η πρώτη έκδοση ολοκληρώθηκε το Μάιο του 1997 και μια πιλοτική δοκιμή ανακοινώθηκε τον Ιούλιο του 1998.

Το SET επέτρεψε στα μέρη να ταυτιστούν μεταξύ τους και να ανταλλάσσουν πληροφορίες με ασφάλεια. Το SET χρησιμοποιεί ένα κρυπτογραφικό αλγόριθμο που, στην πραγματικότητα, θα αφήσει τους εμπόρους ν αντικαταστήσουν μ' ένα πιστοποιητικό την πιστωτική κάρτα του χρήστη. Αν το SET είχε τεθεί σε λειτουργία, ο έμπορος ο ίδιος ποτέ δεν θα μπορούσε να γνωρίζει τα νούμερα πιστωτικών καρτών που αποστέλλονται από τον αγοραστή. Τα πιστοποιητικά τα οποία θα παρέχονταν θα επαλήθευαν μια πληρωμή, αλλά προστατεύοντας τους πελάτες και τις εταιρείες από απάτη.

Το SET επρόκειτο να γίνει το de facto πρότυπο για μεθόδους πληρωμής στο Διαδίκτυο μεταξύ των εμπόρων, των αγοραστών, και των εταιρειών πιστωτικών καρτών. Παρά τη δυνατή δημοσιότητα για να κερδίσει μερίδιο αγοράς, απέτυχε να γίνει ευρεία η χρήση του.

Οι λόγοι για αυτό είναι οι εξής:

Επίδραση στο δίκτυο - πρέπει να εγκατασταθεί λογισμικό πελάτη (ένα ηλεκτρονικό πορτοφόλι).

Κόστος και πολυπλοκότητα για τους εμπόρους που προσφέρουν υποστήριξη, σε αντίθεση με το σχετικά χαμηλό κόστος και την απλότητα της υφιστάμενης SSLβάσης που είναι η εναλλακτική λύση.

Ανάγκη για υπηρεσία χρήστη –εξυπηρετητή(client-server) διανομής πιστοποιητικού.

3.3.2 Σκοπός και Φορείς

Ο σκοπός του πρωτοκόλλου SET είναι να θεσπίσει πράξεις πληρωμής που:

- παρέχουν την εμπιστευτικότητα των πληροφοριών
- διασφαλίζουν την ακεραιότητα των εντολών πληρωμής για αγαθά και υπηρεσίες
- πραγματοποιούν έλεγχο ταυτότητας τόσο στον κάτοχο της κάρτας όσο και στον εμπόρο.

Κύριοι Φορείς:

Υπάρχουν τέσσερις κύριες οντότητες SET:

- Κάτοχος (πελάτη)
- Έμπορος (web server),
- Τράπεζα (πύλη πληρωμής, αγοραστής): πύλη πληρωμής είναι μία συσκευή η οποία λειτουργεί από έναν αγοραστή. Κάποιες στιγμές, υπάρχει διαχωρισμός αυτών των δύο οντοτήτων.
- Εκδότης (τράπεζα του κατόχου της κάρτας)

3.3.3 Πως πραγματοποιείται μία συναλλαγή μέσω SET

Η αλληλουχία των γεγονότων που απαιτούνται για μια συναλλαγή είναι ως εξής:

1. Ο πελάτης αποκτά ένα λογαριασμό της πιστωτικής κάρτας με μια τράπεζα που υποστηρίζει τις ηλεκτρονικές πληρωμές και το πρωτόκολλο SET.
2. Ο πελάτης λαμβάνει ένα X.509v3 ψηφιακό πιστοποιητικό υπογεγραμμένο από την τράπεζα.
3. Οι έμποροι έχουν τα δικά τους πιστοποιητικά
4. Ο πελάτης δίνει εντολή στον έμπορο.
5. Ο έμπορος αποστέλλει στον πελάτη το δημόσιο κλειδί του και ένα αντίγραφο του πιστοποιητικού του, έτσι ώστε ο πελάτης να μπορεί να επιβεβαιώσει ότι πρόκειται για ένα έγκυρο κατάστημα.
6. Ο πελάτης στέλνει τον έμπορο:

- Πιστοποιητικό του.
- Τις λεπτομέρειες της παραγγελίας του κρυπτογραφούνται με το δημόσιο κλειδί του εμπόρου
- Τα στοιχεία του τραπεζικού του λογαριασμού κρυπτογραφούνται με το δημόσιο κλειδί της τράπεζας.

7. Ο έμπορος αιτείται πληρωμή από την τράπεζα στέλνοντας:

- Τις λεπτομέρειες πληρωμής που κρυπτογραφούνται με το δημόσιο κλειδί της τράπεζας.
- Τα στοιχεία του λογαριασμού του πελάτη της τράπεζας που είναι κρυπτογραφημένα με το δημόσιο κλειδί της τράπεζας.
  Σημειώστε ότι ο έμπορος δεν γνωρίζει τις λεπτομέρειες πληρωμής του πελάτη.

8. Η τράπεζα στέλνει στον έμπορο μια επιβεβαίωση κρυπτογραφημένη με το δημόσιο κλειδί του εμπόρου.
9. Ο έμπορος αποστέλλει στον πελάτη την απάντηση της τράπεζας κρυπτογραφημένη με το δημόσιο κλειδί του πελάτη.

10. Ο έμπορος στέλνει τα αγαθά ή παρέχει την υπηρεσία στον πελάτη.
11. Ο έμπορος αποστέλλει στην τράπεζα αίτημα συναλλαγής κρυπτογραφημένο με το δημόσιο κλειδί της τράπεζας.
12. Η τράπεζα μεταφέρει την πληρωμή στον έμπορο

3.3.4Επισκόπηση πρωτόκολλου

Το SET (Secure Electronic Transaction) είναι ένα πολύ ολοκληρωμένο πρωτόκολλο ασφάλειας, το οποίο χρησιμοποιεί κρυπτογράφηση για την παροχή εμπιστευτικότητας
πληροφοριών, την εξασφάλιση ακεραιότητας των πληρωμών, και έλεγχο ταυτότητας.

Για σκοπούς επαλήθευσης, οι κάτοχοι καρτών, οι έμποροι και οι αγοραστές θα να πάρουν ψηφιακά πιστοποιητικά που εκδίδονται με τη χορηγία των οργανώσεών τους.

Στηρίζεται στην κρυπτογραφία και τα ψηφιακά πιστοποιητικά για να εξασφαλιστούν η εμπιστευτικότητα και η ασφάλεια του μηνύματος. Ο ψηφιακός φάκελος χρησιμοποιείται ευρέως στο παρόν πρωτόκολλο.

Δεδομένα του μηνύματος κρυπτογραφούνται με ένα κλειδί που δημιουργείται τυχαία, και η περαιτέρω κρυπτογράφηση γίνεται χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη. Αυτό αναφέρεται ως «ψηφιακός φάκελος» του μηνύματος και αποστέλλεται στον παραλήπτη με το κρυπτογραφημένο μήνυμα. Ο παραλήπτης αποκρυπτογραφεί το ψηφιακό φάκελο χρησιμοποιώντας ιδιωτικό κλειδί και στη συνέχεια χρησιμοποιεί το συμμετρικό κλειδί για να ξεκλειδώσει το αρχικό μήνυμα.

Τα ψηφιακά πιστοποιητικά, τα οποία καλούνται επίσης και ηλεκτρονικά διαπιστευτήρια ή ψηφιακές ταυτότητες, είναι ψηφιακά έγγραφα που πιστοποιούν τη σύνδεση ενός δημόσιου κλειδιού σε ένα φυσικό ή νομικό πρόσωπο. Και οι κάτοχοι καρτών και οι έμποροι πρέπει να εγγραφούν σε μία αρχή πιστοποίησης (CA) για να μπορέσουν να συμμετάσχουν σε συναλλαγές. Ο κάτοχος της κάρτας αποκτά έτσι ηλεκτρονικά πιστοποιητικά για να αποδείξει ότι είναι αξιόπιστος. Ο έμπορος καταγράφεται ομοίως και λαμβάνει πιστοποιήσεις.

Αυτά τα διαπιστευτήρια δεν περιέχουν ευαίσθητα στοιχεία, όπως π.χ. αριθμό πιστωτικής κάρτας. Αργότερα, όταν ο πελάτης θέλει να κάνει αγορές, ο ίδιος και ο έμπορος ανταλλάσουν τα διαπιστευτήριά τους. Αν και οι δύο πλευρές είναι ικανοποιημένες τότε μπορούν να προχωρήσουν με τη συναλλαγή. Τα διαπιστευτήρια πρέπει να ανανεώνονται κάθε λίγα χρόνια, και κατά πάσα πιθανότητα δεν είναι διαθέσιμα σε γνωστούς απατεώνες.

3.3.5 Η SET Κρυπτογραφία

Επισκόπηση

Το SET βασίζεται στην επιστήμη της κρυπτογραφίας την κωδικοποίηση και αποκωδικοποίηση μηνυμάτων. Υπάρχουν δύο κύριες μέθοδοι κρυπτογράφησης που χρησιμοποιούμε σήμερα: κρυπτογραφία ιδιωτικού κλειδιού και κρυπτογραφία δημόσιου κλειδιού. Η κρυπτογραφία ιδιωτικού κλειδιού είναι πρακτική για την ανταλλαγή μηνυμάτων με μια μεγάλη ομάδα άγνωστη μέσω ενός δημόσιου δικτύου. Για έναν έμπορο είναι χρήσιμη για να διεξαχθούν συναλλαγές με ασφάλεια με εκατομμύρια συνδρομητές, κάθε καταναλωτής θα χρειάζεται ένα ξεχωριστό κλειδί που θα ανατεθεί από το συγκεκριμένο έμπορο και μεταδίδεται μέσω ξεχωριστού ασφαλούς καναλιού. Ωστόσο, με τη χρήση της κρυπτογραφίας δημόσιου κλειδιού, ο ίδιος έμπορος θα μπορούσε να δημιουργήσει ένα δημόσιο / ιδιωτικό ζεύγος κλειδιών και να δημοσιεύσει το δημόσιο κλειδί, που επιτρέπει σε κάθε καταναλωτή να αποστείλει ένα ασφαλές μήνυμα σε αυτό το κατάστημα. Αυτός είναι ο λόγος που το SET χρησιμοποιεί και τις δύο μεθόδους στη διαδικασία κρυπτογράφησης. Το ιδιωτικό κλειδί κρυπτογράφησης που χρησιμοποιείται στο
SET είναι το γνωστό Data Encryption Standard (DES), το οποίο χρησιμοποιείται από χρηματοπιστωτικά ιδρύματα για την κρυπτογράφηση των PIN (προσωπικός αριθμός αναγνώρισης)και η κρυπτογραφία δημόσιου κλειδιού που χρησιμοποιείται στο SET είναι RSA.

Χρήση συμμετρικού κλειδιού

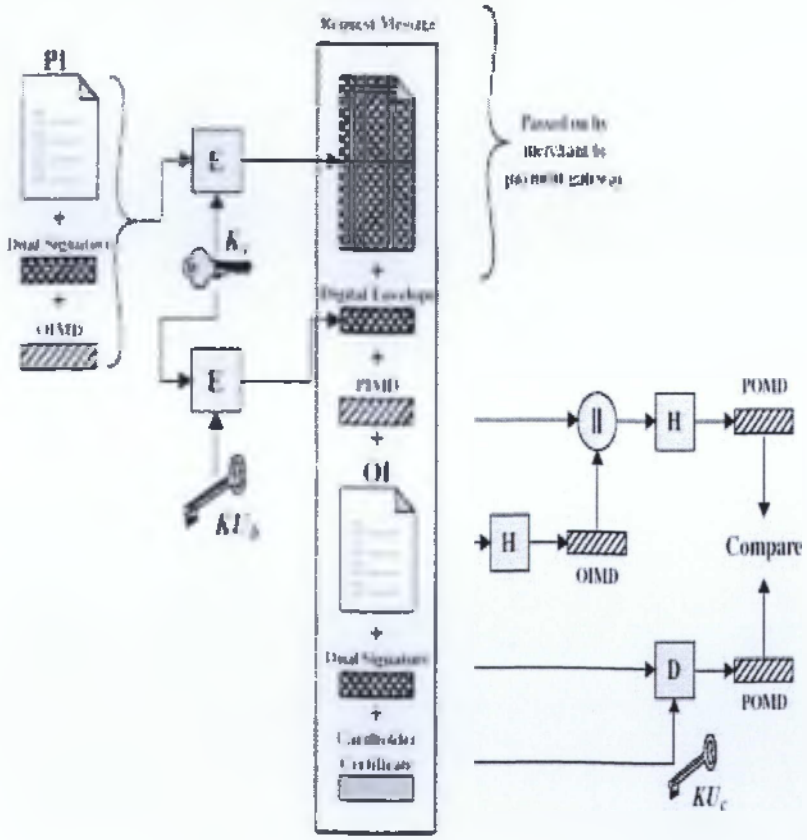
Στο SET, τα δεδομένα κρυπτογραφούνται με ένα τυχαίο συμμετρικό κλειδί (ένα DES 56-bit κλειδί). Αυτό το κλειδί, με τη σειρά του, κρυπτογραφείται χρησιμοποιώντας το μήνυμα παραλήπτη και το δημόσιο κλειδί του(RSA). Το αποτέλεσμα είναι ο λεγόμενος «ψηφιακός φάκελος" του μηνύματος.

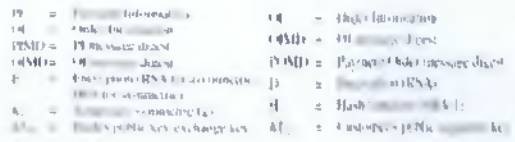
Αυτό συνδυάζει την ταχύτητα κρυπτογράφησης του DES με το κλειδί διαχείρισης και τα πλεονεκτήματα της RSA κρυπτογράφησης δημόσιου κλειδιού. Μετά ο φάκελος και το κρυπτογραφημένο μήνυμα όλα αποστέλλονται στον παραλήπτη. Μετά την παραλαβή των κρυπτογραφημένων δεδομένων, ο παραλήπτης αποκρυπτογραφεί το ψηφιακό φάκελο πρώτα χρησιμοποιώντας το ιδιωτικό κλειδί, είτε το δικό του είτε το άλλο, για να διατηρήσει την τυχαιότητα του συμμετρικού κλειδιού και στη συνέχεια χρησιμοποιεί το συμμετρικό κλειδί για να ξεκλειδώσει το αρχικό μήνυμα.

Αυτό το επίπεδο κρυπτογράφησης, χρησιμοποιώντας DES, μπορεί εύκολα να ραγίσει με τη χρήση σύγχρονων hardware. Το 1993, μια brute-force μηχανή DES σχεδιάστηκε από Michael Wiener - αυτό που ήταν μαζικά παράλληλη. Για λιγότερο από ένα εκατομμύριο δολάρια, ένα κλειδί 56-bit DES μπορούσε να σπάσει, μέσο χρόνο 3,5 ώρες. Με ένα δισεκατομμύριο δολάρια, μια παράλληλη μηχανή μπορεί να κατασκευαστεί και να σπάσει ένα 56-bit DES κλειδί σε ένα δευτερόλεπτο (Schneier, 1996). Προφανώς, αυτό είναι μεγάλη ανησυχία αφού ο DES κρυπτογραφεί την πλειοψηφία των συναλλαγών του SET.

Στο SET, η κρυπτογραφία δημόσιου κλειδιού χρησιμοποιείται μόνο για την κρυπτογράφηση των DES κλειδιών και για τη γνησιότητα (ψηφιακή υπογραφή), αλλά όχι για το κύριο σώμα της συναλλαγής. Στο SET, η RSA έκφραση είναι 1024 bits σε μήκος (Φαίνεται ότι προσπαθώντας να σπάσεις μια 1024-bit έκφραση θα απαιτούσε πάνω από 100,000,000,000 MY της υπολογιστικής προσπάθειας). Για τη δημιουργία της ψηφιακής υπογραφής, το SET χρησιμοποιεί ένα διακριτό δημόσιο / ιδιωτικό κλειδί. Κάθε συμμετέχων σύνολο έχει δύο ασύμμετρα ζεύγη κλειδιών: ένα ζεύγος "ανταλλάξιμων κλειδιών", το οποίο χρησιμοποιείται στην διαδικασία του βασικού τμήματος κρυπτογράφησης και αποκρυπτογράφησης, και ένα ζευγάρι «υπογραφών» για τη δημιουργία και την επαλήθευση των ψηφιακών υπογραφών (160-bit μήνυμα).

Ο αλγόριθμος είναι τέτοιος που αλλάζοντας ένα και μόνο κομμάτι στο μήνυμα θα αλλάξει, κατά μέσο όρο, το ήμισυ των δυαδικών ψηφίων στο μήνυμα. Περίπου, η πιθανότητα δύο μηνύματα που έχουν το ίδιο μήνυμα digest είναι ένα στο 1.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000, η οποία σημαίνει ότι είναι υπολογιστικά ανέφικτο να παράγει δύο διαφορετικά μηνύματα που έχουν το ίδιο μήνυμα digest.





RSA-OAEP

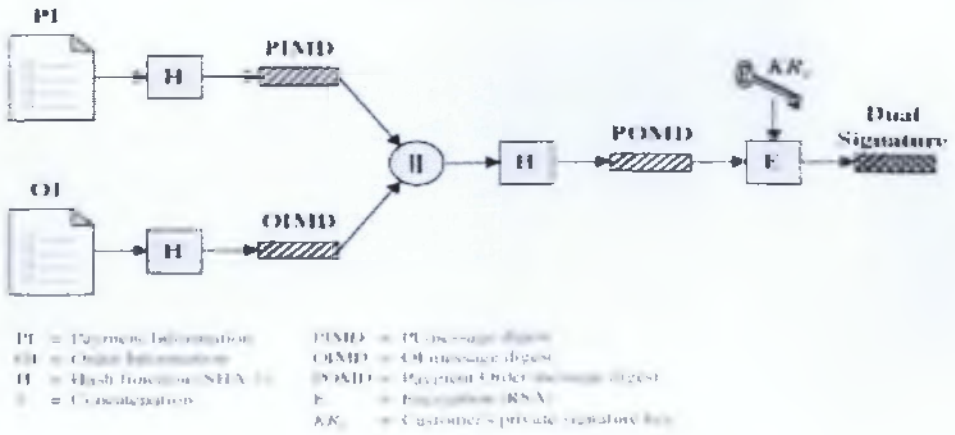
Το RSA-OAEP (RSA RSA Encryption Scheme - Optimal Asymmetric Encryption Padding) προτάθηκε από την Bel-lare και τη Rogaway το 1994, το οποίο είναι μια από τις καινοτομίεστου SET. Το RSA-OAEP είναι σχήμα δημόσιου κλειδιού κρυπτογράφησης που συνδυάζει την κωδικοποίηση μεθόδου OAEP με την κρυπτογράφηση RSA. Το RSA-OAEP παίρνει ένα απλό κείμενο ως πρώτη ύλη, το μετατρέπει σε ένα κωδικοποιημένο μήνυμα μέσω του OAEP και να εφαρμόζει RSAEP (RSA κρυπτογράφηση) στο αποτέλεσμα (να ερμηνευθεί ως ακέραιος αριθμός) χρησιμοποιώντας ένα RSA δημόσιο κλειδί. Το RSA-OAEP προορίζεται να είναι τόσο αποτελεσματικό και ασφαλές και είναι σχεδιασμένο για να κρυπτογραφεί μόνο σύντομα μηνύματα - συνήθως μυστικά κλειδιά για συμμετρική κρυπτογράφηση ή MAC αλγορίθμων.

Το OAEP δένει την ασφάλεια της κρυπτογράφησης RSA στενά με εκείνη της βασικής λειτουργίας RSA. Η έκδοση του OAEP που χρησιμοποιεί το SET είναι μια πιο προηγμένη έκδοση του αρχικού καθεστώτος. Ενώ οι υπάρχουσες μέθοδοι μορφοποίησης μηνύματος
για RSA κρυπτογράφηση δεν έχουν κανένα γνωστό ελάττωμα, οι αποδείξιμες πτυχές της ασφάλειας του OAEP είναι πολύ ελκυστικές. Το OAEP είναι πολύ νέο, αλλά ήδη είναι μέρος του IEEE P1363 πρότυπου.

Το RSA-OAEP σύστημα κρυπτογράφησης έχει αποδειχθεί ότι είναι ασφαλές σημασιολογικά κατά του προσαρμοσμένου ciphertext σε επιλεγμένες επιθέσεις. Ωστόσο, η μείωση αυτή δεν είναι στενή, και συνεπώς δεν είναι σαφές τι διαβεβαιώσεις ασφάλειας παρέχει. Συνιστάται το RSA-OAEP να τροποποιηθεί σε RSA-OAEP ,που έχει μια αυστηρότερη ασφάλειας και επιπλέον να μπορεί εύκολα να τροποποιηθεί ώστε να επιτρέψει την κρυπτογράφηση των αυθαίρετων μηνύματων. Επιπλέον, το RSA-KEM σχήμα κρυπτογράφησης των οποίων έχει ένα ποσοστό μείωσης θα πρέπει να θεωρείται ως αντικατάσταση για RSA-OAEP.

Διπλές υπογραφές

Μια νέα εφαρμογή των ψηφιακών υπογραφών εισάγεται στο SET, δηλαδή η έννοιατης διπλής υπογραφής. Διπλές υπογραφές είναι απαραίτητες όταν δύο μηνύματα πρέπει να συνδεθούν με ασφάλεια, αλλά μόνο ένα μέρος επιτρέπεται να διαβαστεί από το καθένα. Η ακόλουθη εικόνα δείχνει τη διαδικασία της δημιουργίας διπλής υπογραφών.



Στο SET, οι διπλές υπογραφές χρησιμοποιούνται για να συνδέσουν ένα μήνυμα προκειμένου σταλεί στον έμπορο με τις οδηγίες πληρωμής που περιέχει και τα στοιχεία του λογαριασμού αποστέλλονται στον αγοραστή(εμπορική τράπεζα). Όταν ο έμπορος αποστέλλει μια αίτηση άδειας για τον αγοραστή, περιλαμβάνει και τις οδηγίες πληρωμής που αποστέλλονται σε αυτόν από τον κάτοχο της κάρτας και το μήνυμα digest των πληροφοριών τάξης. Ο αποκτών χρησιμοποιεί το μήνυμα digest από τον έμπορο και υπολογίζει το μήνυμα digest των εντολών πληρωμής για να ελέγξει τις δύο υπογραφές.

3.5 Αλγόριθμος DES(Data Encryption Stadard)

3.5.1 Στόχοι του DES:

- Υψηλό επίπεδο ασφάλειας
- Να καθοριστεί πλήρως και να γίνεται εύκολα κατανοητός
- Η ασφάλεια της κρυπτογράφησης να μην εξαρτάται από την μυστικότητα του αλγορίθμου.
- Προσαρμόσιμο σε ποικίλες εφαρμογές
- Οικονομική υλοποίηση σε hardware
- Αποτελεσματικό
- Να μπορεί να επικυρωθεί
- Εξαγώγιμο

3.5.2 Γενικότερα για τον DES

- Αλγόριθμος υποκατάστασης και μετάθεσης.
    - 64-bits είσοδος και έξοδος
    - 56-bits κλειδί(με επιπλέον 8 bits ισοτιμίας)

- Τα δεδομένα ανακυκλώνονται 16 φορές μέσα από ένα σετ μετασχηματισμών υποκατάστασης και αντιμετάθεσης: υψηλό επίπεδο μη-γραμμικής σχέσης εισόδου εξόδου.

- Πολύ υψηλά εφικτά ποσοστά απόδοσης.
- Διαθεσιμότητα οικονομικών υλικών για υλοποίηση του DES
- Χαμηλές προς μέσες εφαρμογές ασφάλειας (π.χ. ασφάλεια φωνητικής επικοινωνίας).

Ιστορική αναδρομή

Ο DES είναι ο κρυπταλγόριθμος ο οποίος είχε επιλεγεί επίσημα από το Ομοσπονδιακό Πρότυπο Επεξεργασίας Πληροφοριών (Federal Information Processing Standard - FIPS) για τις Ηνωμένες Πολιτείες το 1976. Ο DES στη συνέχεια χρησιμοποιήθηκε διεθνώς. Ο αλγόριθμος αρχικά ήταν αμφισβητούμενος, με απόρρητα τα στοιχεία του σχεδιασμού του και ένα σχετικά μικρού μήκους κλειδί. Υπήρχαν υποψίες πως η δημιουργία του DES αποσκοπούσε στη δημουργία backdoor (κερκόπορτας) για την παραβίαση της ασφάλειας της Υπηρεσίας Εθνικής Ασφάλειας (NSA) των Ηνωμένων Πολιτειών. Ο DES υπέστη έντονη ακαδημαϊκή διερεύνηση και αποτέλεσε το κίνητρο για την κατανόηση των κρυπταλγόριθμων συμμετρικού κλειδιού (block ciphers) και την ανάλυσή τους.

Ο DES θεωρείται πλέον ανασφαλής για πολλές εφαρμογές. Αυτό οφείλεται κυρίως στο μικρό μέγεθος του κλειδιού του, που έχει μήκος 56-bits. Τον Ιανουάριο του 1999 οι εταιρείες "Distributed.net" και "Electronic Frontier Foundation", κατόπιν συνεργασίας, "έσπασαν" δημοσίως ένα κλειδί του DES μέσα σε 22 ώρες και 15 λεπτά. Υπάρχουν, επίσης, ορισμένα αναλυτικά αποτελέσματα που καταδεικνύουν θεωρητικές αδυναμίες στον κρυπταλγόριθμο, αν και είναι ανέφικτο να υλοποιηθούν στην πράξη. Θεωρείται πως ο αλγόριθμος είναι πρακτικά ασφαλής υπό τη μορφή του τριπλού DES (triple DES), αν και υπάρχουν θεωρητικές αμφισβητήσεις. Τα τελευταία χρόνια ο κρυπταλγόριθμος DES έχει εκτοπιστεί από το Προηγμένο Πρότυπο Κρυπτογράφησης (Advanced Encryption Standard - AES).

Η προέλευση του DES βρίσκεται στις αρχές της δεκαετίας του 1970. Το 1972, μετά την ολοκλήρωση μελέτης για την ασφάλεια των υπολογιστών της κυβέρνησης, το σώμα προτύπων των Η.Π.Α., γνωστό ως NBS (National Bureau of Standards) – που τώρα ονομάζεται NIST (National Institute of Standards and Technology) - επισήμανε την ανάγκη για ένα Κυβερνητικό πρότυπο με το οποίο θα μπορούσαν να κρυπτογραφηθούν μη απόρρητες, ευαίσθητες πληροφορίες. Στις 15 Μαΐου του 1973, μετά από διαβούλευση με την NSA, η NBS κάνει προτάσεις για έναν κρυπταλγόριθμο που θα ανταποκρίνεται σε κριτήρια αυστηρού σχεδιασμού. Εντούτοις, καμία από τις προτάσεις που υποβλήθηκαν δεν αποδείχθηκε κατάλληλη. Δημοσιεύθηκε μια δεύτερη πρόταση εκδήλωσης ενδιαφέροντος στις 27 Αυγούστου του 1974. Αυτή τη φορά, η IBM υπέβαλε έναν αλγόριθμο, ο οποίος κρίθηκε αποδεκτός: Ήταν κρυπταλγόριθμος που αναπτύχθηκε κατά τη διάρκεια της περιόδου 1973-1974 βασιζόμενος σε προϋπάρχοντες. Αυτός ήταν ο κρυπταλγόριθμος "Lucifer", τον οποίο δημιούργησε ο Χορστ Φάιστελ (Horst Feistel). Η ομάδα της IBM συνέχισε τον σχεδιασμό και την ανάλυση κρυπταλγόριθμων με τη βοήθεια των Feistel, Walter Tuchman, Don Coppersmith, Alan Konheim, Carl Meyer, Mike Matyas, Roy Adler, Edna Grossman, Bill Notz, Lynn Smith και Bryart Tuckerman.

Στις 17 Μαρτίου του 1975 ο προτεινόμενος DES δημοσιεύθηκε στον Ομοσπονδιακό κατάλογο (Federal Register). Ζητήθηκαν δημόσια σχόλια και στο έτος που ακολούθησε, δύο ανοικτά εργαστήρια κλήθηκαν για να συζητήσουν τα προτεινόμενα πρότυπα. Υπήρξε κριτική από διάφορα μέλη, ανάμεσα στους οποίους ήταν και οι πρωτοπόροι στην κρυπτογραφία δημοσίου κλειδιού Μάρτιν Χέλμαν (Martin Hellman) και Ουίτφιλντ Ντίφι (Whitfield Diffie), οι οποίοι ανέφεραν μικρότερο μήκος κλειδιού για τον DES καθώς και τα μυστήρια "S-boxes" ως στοιχεία ανάρμοστης παρέμβασης από την NSA. Η υποψία ήταν ότι ο αλγόριθμος ήταν συγκαλυμμένα αποδυναμωμένος από την Κεντρική Υπηρεσία Πληροφοριών (CIA) έτσι, ώστε μόνον αυτή να μπορεί εύκολα να διαβάσει τα κρυπτογραφημένα μηνύματα. Ο Άλαν Κόνχαϊμ (Alan Konheim), ένας από τους σχεδιαστές του DES, ανέφερε στα σχόλιά του:

«Στείλαμε τα s-boxes στην Ουάσιγκτον. Επέστρεψαν και ήταν όλα διαφορετικά.»

Η Επιτροπή Αντικατασκοπείας της Γερουσίας των ΗΠΑ (United States Senate Select Committee on Intelligence) αναθεώρησε τις ενέργειες της NSA, ώστε να καθορίσει εάν υπήρξε οποιαδήποτε ανάρμοστη συμμετοχή. Στην αταξινόμητη περίληψη των συμπερασμάτων της, που δημοσιεύθηκε το 1978, η Επιτροπή έγραψε:

«Στην ανάπτυξη του DES, η NSA έπεισε την IBM ότι ένα μειωμένο μήκος κλειδιού ήταν ικανοποιητικό. Έμμεσα βοηθούμενη στην ανάπτυξη των δομών S-box και διαβεβαίωσαν ότι ο τελικός αλγόριθμος DES ήταν ό,τι καλύτερο διέθεταν, απαλλαγμένος από οποιαδήποτε στατιστική ή μαθηματική αδυναμία.»

Εν τούτοις, η Επιτροπή ανακάλυψε και ανέφερε, επίσης, ότι:

«Η NSA δεν πείραξε το σχέδιο του αλγορίθμου από καμιά άποψη. Η IBM εφηύρε και σχεδίασε τον αλγόριθμο, έλαβε όλες τις σχετικές αποφάσεις αναγνωρίζοντας την αξία του αλγόριθμου και συμφώνησε ότι το μέγεθος του κλειδιού ήταν περισσότερο από επαρκές για όλες τις εμπορικές εφαρμογές, για τις οποίες προοριζόταν ο DES.»

Ένα άλλο μέλος της ομάδας DES, ο Walter Tuchman, αναφέρεται πως είπε:

«Αναπτύξαμε τον αλγόριθμο DES εξ ολοκλήρου μέσα στην IBM χρησιμοποιώντας IBMers. Η NSA δεν δικτύωσε ούτε ένα καλώδιο!»

Ορισμένες από τις υποψίες σχετικά με τις κρυφές αδυναμίες στα S-boxes είχαν εξαλειφθεί το 1990, με την ανεξάρτητη ανακάλυψη και την ανοικτή δημοσίευση της Διαφορικής Κρυπτανάλυσης από τους Eli Biham και Adi Shamir. Τα S-boxes του DES ήταν πολύ πιο ανθεκτικά στην επίθεση απ' ότι αν είχαν επιλεγεί τυχαία, γεγονός που υποδηλώνει έντονα ότι η IBM γνώριζε για την τεχνική που εφαρμόζονταν στη δεκαετία του 1970. Αυτή ήταν πράγματι η υπόθεση, το 1994, όταν ο Don Coppersmith δημοσίευσε τον αυθεντικό σχεδιασμό των κριτηρίων για τα S-boxes. Σύμφωνα με τον Steven Levi, ο ερευνητής της IBM Watson ανακάλυψε διαφορικές κρυπταναλυτικές επιθέσεις το 1974 και ζητήθηκε από την NSA να κρατήσει την

τεχνική μυστική. Ο Coppersmith εξηγεί την απόρρητη απόφαση της IBM λέγοντας πως:

«Αυτό συνέβη επειδή η Διαφορική κρυπτανάλυση μπορεί να αποτελέσει ένα πολύ ισχυρό εργαλείο, που μπορεί να χρησιμοποιηθεί εναντίον πολλών συστημάτων-σχημάτων και υπήρχε ανησυχία ότι τέτοιες πληροφορίες στο δημόσιο τομέα θα μπορούσαν να επηρεάσουν δυσμενώς την εθνική ασφάλεια.»

Ο Levy ανέφερε στον Walter Tuchman:

«Μας ζητήθηκε να σφραγιστούν όλα τα εμπιστευτικά μας έγγραφα... Πρέπει όντως να βάλουμε έναν αριθμό για κάθε ένα έγγραφο και να τα κλειδώσουμε σε χρηματοκιβώτια, επειδή θεωρήθηκαν απόρρητα έγγραφα της Αμερικανικής κυβέρνησης. Μου είπαν να το κάνω και έτσι το έκανα.»

Ο Shamir σχολίασε πως, σε αντίθεση με το τι πιστεύουν μερικοί άνθρωποι, δεν υπάρχουν ενδείξεις χειραγώγησης του DES, έτσι ώστε ο βασικός σχεδιασμός να εξασθενήσει.

Η άποψη - ότι το μήκος του κλειδιού ήταν πολύ μικρό - ενισχύεται από το γεγονός ότι η αιτιολογία που δόθηκε από την NSA για τη μείωση του μήκους του κλειδιού από τα 64 bits στα 56 bits ήταν ότι τα υπόλοιπα 8 bits θα μπορούσαν να χρησιμεύσουν ως bits ισοτιμίας (parity), πράγμα που έμοιαζε αληθοφανές. Ήταν ευρέως πιστευτό ότι η απόφαση της NSA τροποποιήθηκε λόγω της πιθανότητας κάποια στιγμή να είναι σε θέση (η NSA) να κάνει επιτυχείς επιθέσεις τύπου "brute force" σε κλειδί μεγέθους 56 bits αρκετά χρόνια πριν από τον υπόλοιπο κόσμο.

Ο αλγόριθμος DES ως πρότυπο

Παρά τις επικρίσεις, ο DES εγκρίθηκε ως ομοσπονδιακό πρότυπο τον Νοέμβριο του 1976 και δημοσιεύθηκε στις 15 Ιανουαρίου του 1977 ως FIPS PUB 46 και η χρήση του ήταν επιτρεπτή σε όλα τα μη απόρρητα δεδομένα. Στη συνέχεια επιβεβαιώθηκε ως πρότυπο το 1983, το 1988 (αναθεωρήθηκε ως FIPS-46-1), το 1993 (ως FIPS-46-2) και πάλι το 1999 (ως FIPS-46-3). Ο τελευταίος ορισμός ήταν ο Triple DES. Στις 26 Μαΐου του 2002 ο DES τελικά εκτοπίστηκε από τον Advanced Encryption Standard (AES) κατόπιν δημόσιου διαγωνισμού. Στις 19 Μαΐου του 2005 ο FIPS 46-3 είχε επισήμως αποσυρθεί, αλλά το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology - NIST) ενέκρινε τον Triple DES το έτος 2003 για τις ευαίσθητες πληροφορίες της κυβέρνησης. Μια άλλη θεωρητική επίθεση, η γραμμική κρυπτανάλυση, δημοσιεύθηκε το 1994, αλλά ήταν μια επίθεση brute force το 1998 που αναπαράστησε/απέδειξε ότι κάποιος θα μπορούσε πρακτικά να επιτεθεί στον DES και τονίστηκε η ανάγκη για αντικατάσταση του αλγόριθμου. Αυτές και άλλες μέθοδοι κρυπτανάλυσης εξετάζονται λεπτομερώς.

Η εισαγωγή του DES θεωρείται ότι ήταν καταλύτης για την ακαδημαϊκή μελέτη της κρυπτογραφίας, ιδιαίτερα των μεθόδων για να "σπάζουν" block κρυπταλγόριθμους, σύμφωνα με αναδρομή στο NIST για τον DES.

Μπορεί να ειπωθεί ότι το "αρχικό άλμα" του DES ξεπέρασε τις στρατιωτικές μελέτες και την ανάπτυξη των αλγορίθμων κρυπτογράφησης. Στην δεκαετία του 1970 υπήρχαν πολύ λίγοι κρυπτογράφοι, εκτός εκείνων των στρατιωτικών ή των μυστικών οργανώσεων, και ελάχιστη ήταν η ακαδημαϊκή έρευνα της κρυπτογραφίας. Υπάρχουν

τώρα πολλοί δραστήριοι ακαδημαϊκοί κρυπτολόγοι και τμήματα μαθηματικών με ισχυρά προγράμματα στην κρυπτογραφία και την ασφάλεια των πληροφοριών και των εμπορικών εταιρειών και συμβούλων. Μια γενεά κρυπταναλυτών έχει αναλύσει εξονυχιστικά τον αλγόριθμο DES προσπαθώντας να τον "σπάσουν". Ανέφεραν πως ο DES έκανε περισσότερα για να γαλβανίσει τον τομέα της κρυπτανάλυσης από οτιδήποτε άλλο γιατί έτσι υπήρχε ένας αλγόριθμος για μελέτη. Ένα εκπληκτικό μερίδιο της ανοιχτής βιβλιογραφίας στην κρυπτογραφία κατά τη δεκαετία του 1970 και του 1980 ασχολήθηκε με τον DES και ο DES είναι πρότυπο ενάντια σε όλους τους αλγόριθμους συμμετρικού κλειδιού μετά από σύγκριση.

Συνοψίζοντας την ιστορική αναδρομή θα μπορούσαμε να εξάγουμε τον παρακάτω χρονολογικό πίνακα με την χρονολογική πορεία του DES.

Ημερομηνία	Ετος	Γεγονοτα
15 Μάιος	1973	Η NBS δημοσιεύει το πρώτο αίτημα για έναν τυποποιημένο αλγόριθμο κρυπτογράφησης
27 Αυγούστου	1974	Η NBS δημοσιεύει ένα δεύτερο αίτημα για τους αλγορίθμους κρυπτογράφησης
17 Μαρτίου	1975	Ο DES δημοσιεύεται στον *ομοσπονδιακό κατάλογο* για σχόλια
Αύγουστος	1976	Δημιουργία του πρώτου εργαστηρίου για τον DES
Σεπτέμβριος	1976	Δεύτερο εργαστήριο, που συζητάται το μαθηματικό ίδρυμα DES
Νοέμβριος	1976	Ο DES εγκρίνεται ως πρότυπο
15 Ιανουαρίου	1977	Ο DES δημοσιεύεται ως ένα πρότυπο του FIPS, το FIPS PUB 46
	1983	Ο DES επιβεβαιώνεται για πρώτη φορά
	1986	Το Videocipher II, ένα δορυφορικό σύστημα TV που χρησιμοποιείται από την HBO, ανακατεύεται στα συστήματα που βασίζονται σε DES
22 Ιανουαρίου	1988	Ο DES επιβεβαιώνεται για τη δεύτερη φορά ως FIPS 46-1, εκτοπίζοντας τον FIPS PUB 46
Ιούλιος	1990	Οι Biham και Shamir ανακαλύπτουν πάλι την διαφορική κρυπτανάλυση και την εφαρμόζουν σε ένα κρυπτοσύστημα είδους DES 15 κύκλων
	1992	Οι Biham και Shamir αναφέρουν την πρώτη θεωρητική επίθεση με λιγότερη πολυπλοκότητα από την brute force, τη διαφορική κρυπτανάλυση. Εντούτοις, απαιτεί 2^{47} μη ρεαλιστικά προεπιλεγμένα plaintexts
30 Δεκεμβρίου	1993	Ο DES επιβεβαιώνεται για τρίτη φορά ως FIPS 46-2
	1994	Η πρώτη πειραματική κρυπτανάλυση του DES εκτελείται χρησιμοποιώντας γραμμική κρυπτανάλυση (Matsui, 1994).
Ιούνιος	1997	Το πρόγραμμα DESCHALL "σπάει" για πρώτη φορά μπροστά σε κοινό ένα μήνυμα που κρυπτογραφήθηκε με τον DES
Ιούλιος	1998	Οι EFF ως DES crackers (Deep Crack) σπάνε ένα κλειδί του DES σε 56 ώρες
Ιανουάριος	1999	Μαζί, η Deep Crack και η distributed.net σπάνε ένα κλειδί DES σε 22 ώρες και 15 λεπτά.
25 Οκτωβρίου	1999	Ο DES επιβεβαιώνεται για τέταρτη φορά ως FIPS 46-3, που διευκρινίζει την προτιμημένη χρήση του triple DES με ενιαίο DES που επιτρέπεται μόνο στα κληρονομικά συστήματα
26 Νοεμβρίου	2001	Το AES δημοσιεύεται σε FIPS 197
26 Μαΐου	2002	Το πρότυπο AES γίνεται αποτελεσματικό
26 Ιουλίου	2004	Η απόσυρση του FIPS 46-3 (και μερικών σχετικών προτύπων) προτείνεται στον ομοσπονδιακό κατάλογο
19 Μαΐου	2005	Το NIST αποσύρει τον FIPS 46-3
15 Μαρτίου	2007	Η παράλληλη μηχανή COPACOBANA (βασισμένη σε FPGA) του πανεπιστημίου του Μπόχουμ και του Κίελου της Γερμανίας, σπάνε τον DES σε 6,4 ημέρες με κόστος υλικού $10.000

3.5.3 Περιγραφή του DES

Το Data Encryption Standard (DES), είναι το όνομα του Federal Information Processing Standard (FIPS) 46-3, το οποίο περιγράφει τον αλγόριθμο κρυπτογράφησης δεδομένων (DEA). Ο DEA επίσης ορίζεται με το πρότυπο ANSI X3.92. είναι μια βελτίωση του αλγορίθμου Lucifer που αναπτύχθηκε από την IBM στις αρχές του 1970. Η IBM, η Υπηρεσία Εθνικής Ασφάλειας (NSA) και το Εθνικό Γραφείο Προτύπων (NBS ,σήμερα Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας NIST) ήταν οι υπηρεσίες που ανέπτυξαν τον αλγόριθμο. Ο DES έχει μελετηθεί εκτενώς από τη δημοσίευσή του και είναι ο πιο ευρέως χρησιμοποιούμενος συμμετρικός αλγόριθμος στον κόσμο. Ο DES είναι 64-bitος και χρησιμοποιεί ένα 56-bit κλειδί κατά τη διάρκεια της εκτέλεσης (έχει 8 bits ισοτιμίας από το πλήρες κλειδί 64-bit).Ο DES είναι ένα συμμετρικό κρυπτογραφικό σύστημα, και συγκεκριμένα έχει ένα 16-γύρο κρυπτογράφησης Feistel. Όταν χρησιμοποιείται για την επικοινωνία, τόσο αποστολέας και ο παραλήπτης πρέπει να γνωρίζουν το ίδιο μυστικό κλειδί, το οποίο μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση και την αποκρυπτογράφηση του μηνύματος, ή για τη δημιουργία και την επαλήθευση ενός κώδικα ταυτότητας μηνυμάτων (MAC). Ο DES μπορεί επίσης να χρησιμοποιηθεί για μεμονωμένους χρήστες κρυπτογράφησης, όπως για την αποθήκευση αρχείων σε έναν σκληρό δίσκο σε κρυπτογραφημένη μορφή.

Ο DES είναι αρχετυπικός block cipher, δηλαδή, ένας πρωτότυπος κρυπταλγόριθμος συμμετρικού κλειδιού, που λαμβάνει μια σειρά από bits απλού κειμένου (plaintext bits) σταθερού μήκους και την μετατρέπει, μέσω μιας σειράς πολύπλοκων ενεργειών, σε μια άλλη σειρά bits, το κρυπτοκείμενο (chiphertext) με το ίδιο μήκος. Στην περίπτωση του DES το μέγεθος του μπλοκ (block size: Η σειρά των bits σταθερού μήκους) είναι 64 bits. Ο DES χρησιμοποιεί, επίσης, ένα κλειδί για να προσαρμόσει την μετατροπή, ώστε η αποκρυπτογράφηση να μπορεί, υποθετικά, να πραγματοποιηθεί μόνο από εκείνους που γνωρίζουν το συγκεκριμένο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση. Το κλειδί φαινομενικά αποτελείται από 64 bits. Ωστόσο, στην πραγματικότητα μόνο 56 από αυτά χρησιμοποιήθηκαν από τον αλγόριθμο. Τα υπόλοιπα 8 χρησιμοποιούνται αποκλειστικά για τον έλεγχο της ισοτιμίας και στη συνέχεια απορρίπτονται (αυτά καλούνται parity bits), εξ ου και αναφέρεται συνήθως ως κλειδί μήκους 56 bits. Όπως οι άλλοι block αλγόριθμοι κρυπτογράφησης, έτσι και ο DES από μόνος του δεν είναι ασφαλής τρόπος κρυπτογράφησης αλλά, αντίθετα, πρέπει να χρησιμοποιηθεί με ειδικό τρόπο λειτουργίας (mode of operation). Ο FIPS-81 ορίζει πολλούς τρόπους χρήσης του DES. Περαιτέρω παρατηρήσεις σχετικά με τη χρήση του DES περιέχονται στο FIPS-74.

3.5.4 Γενική δομή

• *EBC (Electronic Book Code).*

Αυτή είναι η τακτική του αλγορίθμου DES. Τα δεδομένα είναι χωρισμένα σε 64-bit μπλοκ και κάθε μπλοκ είναι κρυπτογραφημένο, ένα κάθε φορά. Ξεχωριστή κρυπτογράφηση με διαφορετικά μπλοκ είναι εντελώς ανεξάρτητα μεταξύ τους. ο Αυτό σημαίνει ότι εάν τα δεδομένα μεταδίδονται μέσω δικτύου ή τηλεφωνικής γραμμής, σφάλματα μετάδοσης θα επηρεάσουν μόνο το μπλοκ που περιέχει το

σφάλμα. Αυτό σημαίνει επίσης, ωστόσο, ότι το μπλοκ μπορεί να τροποποιηθεί, και η δράση αυτή θα περάσει απαρατήρητη. Ο EBC είναι ο πιο αδύναμος από άλλα μέσα, επειδή δεν απαιτούνται πρόσθετα μέτρα ασφαλείας , εκτός από το βασικό αλγόριθμο DES. Ωστόσο, είναι ο γρηγορότερος και ευκολότερος για την εφαρμογή, καθιστώντας την πιο κοινή λειτουργία του DES.

• *CBC (Cipher Block Chaining)*

Σε αυτόν τον τρόπο λειτουργίας του, κάθε μπλοκ του EBC κρυπτογραφημένο ciphertext είναι XORed με το επόμενο μπλοκ plaintext είναι κρυπτογραφημένο, έτσι ώστε όλα τα μπλοκ να εξαρτώνται από όλα τα προηγούμενα. Αυτό σημαίνει ότι για να βρεθεί το plaintext ενός συγκεκριμένου μπλοκ, θα πρέπει να γνωρίζει το ciphertext, το κλειδί, και το κρυπτογράφημα του προηγούμενου μπλοκ. Το πρώτο μπλοκ για να είναι κρυπτογραφημένο δεν έχει προηγούμενο ciphertext, έτσι ώστε το plaintext είναι XORed με έναν αριθμό 64-bit που ονομάζεται Initialization Vector ή IV για συντομία. Έτσι, αν τα δεδομένα μεταδίδονται μια γραμμή δικτύου ή τηλεφώνου και υπάρχει ένα σφάλμα μετάδοσης, το σφάλμα θα μεταφερθεί σε όλα τα επόμενα μπλοκ.Αυτός ο τρόπος λειτουργίας είναι πιο ασφαλής από τον EBC, διότι το επιπλέον βήμα XOR προσθέτει ένα ακόμη στρώμα στη διαδικασία κρυπτογράφησης.

• *CFB (Cipher Feedback)*

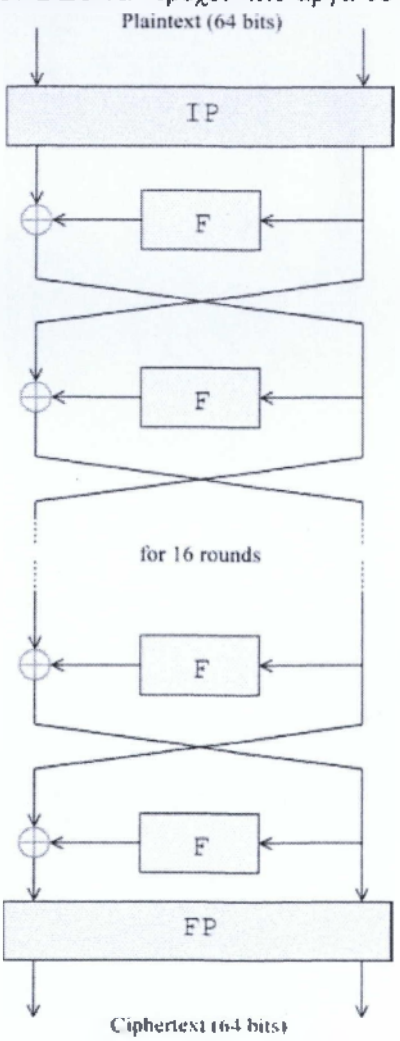
Σε αυτή τη λειτουργία, το μπλοκ plaintext που είναι λιγότερο από 64 bits μήκος μπορεί να είναι κρυπτογραφημένο. Κανονικά, ειδική επεξεργασία, πρέπει να χρησιμοποιηθεί για να χειριστεί τα αρχεία των οποίων το μέγεθος δεν είναι ένα τέλειο πολλαπλάσιο των 8 bytes, αλλά αυτή η λειτουργία αφαιρεί μια άλλη αναγκαία λειτουργία (τη Stealth που χειρίζεται αυτή την περίπτωση, με την προσθήκη πολλών bytes στο τέλος ενός αρχείου πριν την κρυπτογράφηση αυτού).Η plaintext από μόνη της δεν στέκεται στην πραγματικότητα αλλά πέρασε μέσω του αλγορίθμου DES, απλώς XORed με ένα μπλοκ εξόδου από αυτήν, με τον ακόλουθο τρόπο: Ένα 64-bit μπλοκ που ονομάζεται Μητρώο Shift χρησιμοποιείται ως plaintext στη συμβολή του DES. Αυτό έχει αρχικά οριστεί σε κάποια αυθαίρετη τιμή, και κρυπτογραφημένη με τον αλγόριθμο DES. Η ciphertext στη συνέχεια διέρχεται από ένα επιπλέον στοιχείο που ονομάζεται M-box, το οποίο απλά επιλέγει την άκρως αριστερή M bits του ciphertext, όπου m είναι ο αριθμός των bits στο μπλοκ που θέλουμε να κρυπτογράφησουμε. Η τιμή αυτή είναι XORed , και η έξοδος του ότι είναι ο τελικός ciphertext. Τέλος, το ciphertext επανατροφοδοτεί το Μητρώο Shift, και χρησιμοποιείται ως σπόρος plaintext για το επόμενο μπλοκ ώστε να είναι κρυπτογραφημένα. Όπως και με τρόπο CBC, ένα λάθος σε ένα μπλοκ επηρεάζει όλα τα επόμενα μπλοκ κατά τη διάρκεια της μετάδοσης δεδομένων. Αυτός ο τρόπος λειτουργίας είναι παρόμοιος με τη διασυνοριακή συνεργασία και είναι πολύ ασφαλής, αλλά είναι πιο αργός από ό, τι ο EBC χάρη στην επιπλέον πολυπλοκότητα.

• *OFB (Output Feedback)*

Αυτός είναι παρόμοιος σε λειτουργία με τον CFB, εκτός από το ότι η παραγωγή του ciphertext DES επανατροφοδοτεί το Μητρώο Shift, και όχι το τελικό ciphertext. Το μητρώο Shift έχει οριστεί με μια αυθαίρετη αρχική τιμή, και πέρασε μέσα από τον αλγόριθμο DES. Η έξοδος από τον DES διέρχεται μέσα από το M-box και στη συνέχεια επανατροφοδοτεί το Shift για να προετοιμαστεί για το επόμενο μπλοκ. Η τιμή αυτή είναι συνέχεια XORed (το οποίο μπορεί να είναι μικρότερο των 64 bits σε μήκος, όπως η λειτουργία CFB), και το αποτέλεσμα είναι το τελικό ciphertext.

Σημειώστε ότι σε αντίθεση με το CFB και το CBC, ένα σφάλμα μετάδοσης σε ένα μπλοκ δεν θα επηρεάσει τα επόμενα μπλοκ γιατί από τη στιγμή που ο παραλήπτης έχει την αρχική τιμή Εγγραφής στο Shift, θα συνεχίσει να παράγει νέα Shift Εγγραφή, απλό κείμενο χωρίς καμία περαιτέρω εισαγωγή δεδομένων. Αυτός ο τρόπος λειτουργίας είναι λιγότερο ασφαλής από τη CFB λειτουργία, επειδή μόνο το πραγματικό προϊόν ciphertext και το DES ciphertext είναι απαραίτητο για να βρεθεί το απλό κείμενο του πιο πρόσφατου μπλοκ. Η γνώση του κλειδιού δεν είναι απαραίτητη. Το ενσωματωμένο λογισμικό βιβλιοθηκών VOCAL περιλαμβάνει μια πλήρη γκάμα ETSI / ITU / IEEE αλγορίθμων συμβατών, εκτός από πολλούς άλλους αλγορίθμους. Το λογισμικό έχει βελτιστοποιηθεί για εκτέλεση σε ANSI C και σε DSP (TI, ADI, AMD, ARM, MIPS, CEVA, LSI Logic ZSP, κλπ.). Οι βιβλιοθήκες αυτές είναι ευέλικτες και μπορούν να εκτελεστούν ως ένα ενιαίο έργο κάτω από μια ποικιλία λειτουργικών συστημάτων ή αυτόνομα με δικό του μικροπυρήνα.

Η γενική δομή του αλγορίθμου παρουσιάζεται στην Εικόνα 1: Υπάρχουν 16 πανομοιότυπα στάδια επεξεργασίας, που καλούνται Γύροι. Υπάρχει, επίσης ,μια αρχική και μια τελική μεταλλαγή που καλούνται IP και FP (ή IP-1) αντίστοιχα, οι οποίες είναι Αντίστροφες Συναρτήσεις (η IP "ανατρέπει" τη δράση του FP και αντίστροφα). Η IP και η FP δεν έχουν σχεδόν καμία κρυπτογραφική σημασία, αλλά συμπεριλήφθηκαν, προφανώς, προκειμένου να διευκολύνουν τα block φόρτωσης μέσα και έξω από το υλικό των μέσων της δεκαετίας του 1970, καθώς επίσης και για να κάνουν τον DES να "τρέχει" πιο αργά σε λογισμικό.



Σχήμα Η συνάρτηση Feistel

Πριν από τους κύριους γύρους, το block είναι διαιρεμένο σε δύο 32-bit μέρη και επεξεργασμένο διαδοχικά. Αυτή η σταυροειδής διάταξη είναι γνωστή ως σχήμα Feistel (Feistel scheme). Η δομή Feistel εξασφαλίζει ότι η αποκρυπτογράφηση και η κρυπτογράφηση είναι παρόμοιες διαδικασίες. Η μόνη διαφορά είναι ότι τα υποκλείδια ή δευτερεύοντα κλειδιά (subkeys) εφαρμόζονται σε αντίστροφη διάταξη, όταν εκτελείται η πράξη της αποκρυπτογράφησης. Το υπόλοιπο του αλγορίθμου είναι ίδιο. Αυτό απλοποιεί πολύ την εφαρμογή, ιδιαίτερα στο υλικό, δεδομένου ότι δεν υπάρχει καμία ανάγκη για ξέχωρους αλγορίθμους κρυπτογράφησης και αποκρυπτογράφησης. Το κόκκινο σύμβολο δείχνει την αποκλειστική OR (XOR) λειτουργία. Η F συνάρτηση αναμιγνύει το μισό τμήμα του block μαζί με ένα μέρος από το κλειδί. Η έξοδος από την συνάρτηση F συνδυάζεται έπειτα με το άλλο μισό του block και τα μισά ανταλλάσσονται πριν από τον επόμενο κύκλο. Μετά από τον τελικό γύρο, τα μισά δεν ανταλλάσσονται, αυτό είναι ένα χαρακτηριστικό γνώρισμα της δομής Feistel που κάνει την κρυπτογράφηση και την αποκρυπτογράφηση παρόμοιες διαδικασίες.

Η συνάρτηση Feistel (F)

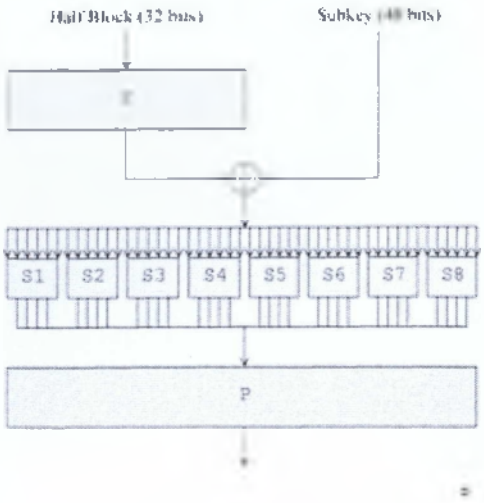
Η συνάρτηση F, που απεικονίζεται στην Εικόνα 2, λειτουργεί με μισό block (32bits) τη φορά και αποτελείται από τέσσερα στάδια:

Επέκταση → Το 32-bit μισό block έχει επεκταθεί σε 48-bits χρησιμοποιώντας την επεκτατική μεταλλαγή (expansion permutation) – η οποία υπάρχει με την ονομασία E (γαλάζιο ορθογώνιο) στην Εικόνα 2 – αντιγράφοντας ορισμένα από τα bits.

Ανάμειξη κλειδιών → Το αποτέλεσμα αναμιγνύεται με ένα υποκλειδί με τη χρήση μιας XOR πράξης. Δεκαέξι 48-bits κλειδιά – ένα για κάθε γύρο - προέρχονται από το κύριο κλειδί χρησιμοποιώντας το χρονοδιάγραμμα / πρόγραμμα κλειδιού (key schedule) το οποίο θα περιγραφεί παρακάτω.

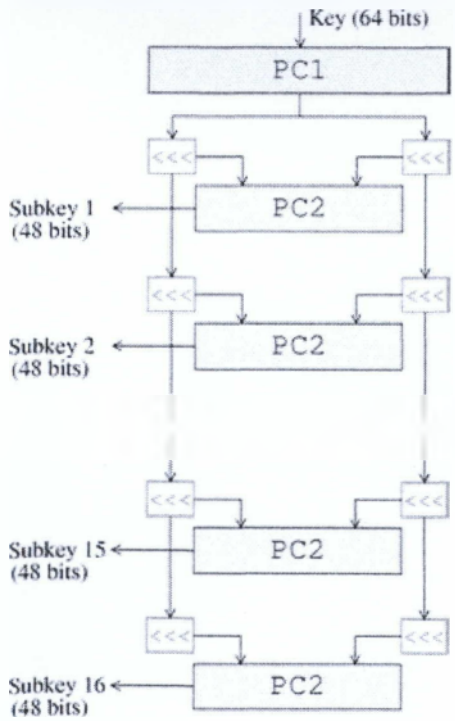
Αντικατάσταση → Μετά την ανάμειξη με το υποκλειδί, το block διαιρείται σε οκτώ τμήματα των 6 bits πριν να τύχει επεξεργασίας από τα S-boxes (Substitution boxes – κουτιά αντικατάστασης). Κάθε ένα από τα οκτώ S-boxes αντικαθιστά τις 6-bits εισόδους του με εξόδους των τεσσάρων bits σύμφωνα με ένα μη γραμμικό μετασχηματισμό, που παρέχεται με τη μορφή ενός πίνακα αναζήτησης (lookup table). Τα S-boxes παρέχουν τον πυρήνα της ασφάλειας του DES – χωρίς αυτά, ο κρυπταλγόριθμος θα ήταν γραμμικός και κοινότοπα εύθραυστος.

Μεταλλαγή → Τέλος, οι 32 έξοδοι από τα S-boxes διακανονίζονται σύμφωνα με μια σταθερή μεταλλαγή, το P-box. Η εναλλαγή της αντικατάστασης από τα S-boxes και τη μεταλλαγή των bits από το P-box και την E-επέκταση (expansion), παρέχει τη λεγόμενη "σύγχυση και διάχυση" αντίστοιχα, μια έννοια που προσδιορίστηκε από τον Κλοντ Σάνον (Claude Shannon) τη δεκαετία του 1940 ως απαραίτητη προϋπόθεση για ασφαλή και πρακτικό πλέον κρυπταλγόριθμο.



Το πρόγραμμα του κλειδιού

Η Εικόνα 3 απεικονίζει το πρόγραμμα κλειδιού για την κρυπτογράφηση — ο αλγόριθμος δημιουργεί τα υποκλειδιά. Αρχικά, τα 56 bits του κλειδιού επιλέγονται από τα αρχικά 64 από τη μεταλλαγμένη επιλογή 1 (Permuted Choice 1 : PC-1) — τα υπόλοιπα οκτώ bits είτε απορρίπτονται είτε χρησιμοποιούνται ως parity bits (για τον έλεγχο ισοτιμίας). Τα 56 bits διαιρούνται έπειτα σε δύο τμήματα των 28 και κάθε μισό αντιμετωπίζεται έκτοτε χωριστά. Στους διαδοχικούς γύρους και τα δύο μισά περιστρέφονται αριστερά κατά ένα ή δύο bits (που διευκρινίζονται για κάθε γύρο) και έπειτα, τα 48 bits του υποκλειδιού επιλέγονται από τη μεταλλαγμένη επιλογή 2 (Permuted Choice 2 : PC-2) — 24 bits από το αριστερό μισό και 24 από το μισό. Οι περιστροφές (που δείχνονται από το <<< στην Εικόνα 3) σημαίνουν ότι ένα διαφορετικό σετ από bits χρησιμοποιείται σε κάθε υποκλειδί. Κάθε bit χρησιμοποιείται σε περίπου 14 από τα 16 υποκλειδιά.



Το πρόγραμμα κλειδιού για την αποκρυπτογράφηση είναι παρόμοιο — τα υποκλειδιά είναι σε αντίστροφη διάταξη έναντι αυτή της κρυπτογράφησης. Αν, δηλαδή, κατά την κρυπτογράφηση το πρόγραμμα κλειδιού είναι {k1, k2, k3 ... k16}, τότε το πρόγραμμα κλειδιού της αποκρυπτογράφησης θα είναι {k16 ... k3, k2, k1}. Πέραν αυτής της αλλαγής, η διαδικασία είναι η ίδια όπως για την κρυπτογράφηση.

3.5.5 Ασφάλεια και κρυπτανάλυση

Αν και οι περισσότερες πληροφορίες που έχουν δημοσιευθεί αφορούν στην κρυπτανάλυση του DES απ' ότι οποιουδήποτε άλλου block cipher, η πρακτικότερη επίθεση μέχρι και σήμερα είναι ακόμα η προσέγγιση brute force (ωμής βίας). Είναι γνωστές διάφορες δευτερεύουσες κρυπταναλυτικές ιδιότητες και τρεις θεωρητικές επιθέσεις είναι δυνατές· που ακόμα κι αν έχουν μια θεωρητική πολυπλοκότητα μικρότερη από την επίθεση brute force, απαιτείται να φέρουν ιλιγγιώδες μέγεθος γνωστών ή προεπιλεγμένων plaintext και δεν αποτελούν, στην πράξη, πηγή ανησυχίας.

Επίθεση brute-force

Για οποιοδήποτε κρυπταλγόριθμο, η πιο βασική μέθοδος επίθεσης είναι η brute force — δοκιμάζοντας συνεχόμενα κάθε πιθανό κλειδί. Το μήκος του κλειδιού καθορίζει το πλήθος των πιθανών κλειδιών και ως εκ τούτου την δυνατότητα πραγματοποίησης αυτής της προσέγγισης. Τέθηκαν από νωρίς ερωτήσεις για την επάρκεια του μήκους κλειδιού του DES, πριν ακόμα υιοθετηθεί ως πρότυπο. Το μικρό μήκος κλειδιού ήταν αυτό που, στην ουσία, υπαγόρευση την ανάγκη για την αντικατάσταση του αλγόριθμου, παρά η θεωρητική κρυπτανάλυση. Είναι γνωστό ότι η NSA ενθάρρυνε, αν δεν έπεισε, την IBM για να μειώσει το μήκος του κλειδιού από τα 128 στα 64 bits και από εκεί σε 56. Αυτό λαμβάνεται συχνά ως ένδειξη ότι η NSA σκέφτηκε ότι θα ήταν σε θέση να "σπάσει" κλειδιά αυτού του μήκους ακόμη και στα μέσα της δεκαετίας του '70.

Στον ακαδημαϊκό κόσμο έγιναν διάφορες προηγμένες προτάσεις για μια μηχανή που θα αποσκοπούσε στο να "σπάει" τον DES. Το 1977, οι Diffie και Hellman πρότειναν μια μηχανή που θα στοίχιζε, κατ' εκτίμηση, 20 εκατομμύρια δολάρια, η οποία θα μπορούσε να βρει ένα κλειδί DES σε μία και μόνο ημέρα. Μέχρι το 1993, ο Wiener είχε προτείνει μια μηχανή αναζήτησης κλειδιού με κοστολόγηση 1 εκατομμύριο δολάρια, που θα έβρισκε ένα κλειδί μέσα σε 7 ώρες. Εντούτοις, καμία από αυτές τις πρόωρες προτάσεις δεν εφαρμόστηκε· τουλάχιστον καμία εφαρμογή δεν αναγνωρίστηκε δημόσια. Η ευπάθεια του DES επιδείχθηκε πρακτικά προς το τέλος της δεκαετίας του '90. Το 1997, η εταιρεία RSA Security υποστήριξε μια σειρά διαγωνισμών με βραβείο $10.000 στην πρώτη ομάδα που θα "έσπαζε" ένα μήνυμα, το οποίο είχε κρυπτογραφηθεί με τον DES. Τον διαγωνισμό κέρδισε το πρόγραμμα DESCHALL, που δημιουργήθηκε από τους Rocke Verser, Matt Curtin, και Justin Dolske, χρησιμοποιώντας ιδανικούς κύκλους χιλιάδων υπολογιστών σε ολόκληρο το Διαδίκτυο. Η δυνατότητα πραγματοποίησης του "σπασίματος" του DES

καταδείχθηκε γρήγορα το 1998 όταν φτιάχτηκε μια ρουτίνα "σπασίματος" του DES από την EFF (Electronic Frontier Foundation), μια ομάδα αστικών δικαιωμάτων του Κυβερνοχώρου, με κόστος περίπου $250,000 (Εικόνα 4). Το κίνητρό τους ήταν να δείξουν ότι ο DES ήταν το ίδιο εύθραυστος στην πράξη όπως και στην θεωρία:

«Υπάρχουν πολλοί άνθρωποι που δεν θα πιστέψουν μια αλήθεια έως ότου μπορούν να τη δουν με τα μάτια τους. Δείχνοντάς τους μία φυσική μηχανή που μπορεί να "σπάσει" τον DES σε μερικές ημέρες είναι ο μόνος τρόπος να πειστούν μερικοί άνθρωποι ότι δεν μπορούν να εμπιστευθούν την ασφάλειά τους στον DES.»

Η μηχανή εμφάνισε ένα κλειδί με χρήση brute force σε κάτι περισσότερο από 2 ημέρες. Περίπου στον ίδιο χρόνο ένας πληρεξούσιος του αμερικανικού Υπουργείου Δικαιοσύνης ανήγγελλε ότι ο DES δεν ήταν δυνατό να παραβιαστεί.

Η μόνη άλλη επιβεβαιωμένη μηχανή που "έσπαζε" τον DES ήταν η μηχανή COPACOBANA (σύντμηση του βέλτιστου κόστους και παράλληλα ενός code breaker) που δημιουργήθηκε πιο πρόσφατα από τις ομάδες των πανεπιστημίων του Μπόχουμ και του Κίελου της Γερμανίας. Αντίθετα από τη μηχανή της EFF, η COPACOBANA αποτελείται από εμπορικά διαθέσιμα, ανασχηματισμένα ολοκληρωμένα κυκλώματα. 120 εξ'αυτών των FPGAs του τύπου XILINX Spartan3-1000 τρέχουν σε παράλληλη σύνδεση. Ομαδοποιούνται σε 20 DIMM ενότητες, που κάθε μια περιέχει 6 FPGAs. Η χρήση των ανασχηματισμένων υλικών κάνει την μηχανή να βρίσκει εφαρμογή και σε άλλες λειτουργίες για "σπάσιμο" κωδικών. Η Εικόνα 5 δείχνει μία πλήρη μηχανή COPACOBANA.

Μια από τις πιο ενδιαφέρουσες πτυχές COPACOBANA είναι ο παράγοντας του κόστους της. Μια μηχανή μπορεί να κατασκευαστεί με κόστος περίπου $10.000. Η μείωση κόστους από έναν, κατά προσέγγιση, παράγοντα της τάξης του 25% από αυτή της μηχανής της EFF είναι ένα εντυπωσιακό παράδειγμα για τη συνεχή βελτίωση του ψηφιακού υλικού. Κατά ενδιαφέροντα τρόπο, ο νόμος του Moore προβλέπει μια βελτίωση της τάξης περίπου 32%, δεδομένου ότι περίπου οκτώ έτη έχουν μεσολαβήσει μεταξύ του σχεδιασμού των δύο μηχανών, πράγμα το οποίο επιτρέπει περίπου πέντε διπλασιασμούς της ισχύος των υπολογιστών (ή 5 μειώσεις τις τάξεως του 50% του κόστους για τον ίδιο υπολογισμό).

Επιθέσεις ταχύτερες από την brute - force

Υπάρχουν τριών ειδών επιθέσεις που είναι γνωστό ότι μπορούν να "σπάσουν" και τους δέκα έξι γύρους του DES με λιγότερη πολυπλοκότητα από μια αναζήτηση brute force:

- Η Διαφορική Κρυπτανάλυση (Differential Cryptanalysis – DC)
- Η Γραμμική Κρυπτανάλυση (Linear Cryptanalysis - LC) και τέλος
- Η επίθεση του Davie (Davies' Attack)

Εντούτοις, οι επιθέσεις είναι θεωρητικές και είναι αδύνατο να εφαρμοστούν στην πράξη. Τέτοιου είδους επιθέσεις καλούνται μερικές φορές Certificational Weaknesses.

3.5.6 Δυνατά σημεία και αδυναμίες του DES

Η δύναμη των DES βρίσκεται σε δύο γεγονότα:

- Η χρήση των κλειδιών 56-bit: Τα 56-bit του κλειδιού χρησιμοποιούνται στην κρυπτογράφηση, άρα υπάρχουν 256 πιθανά κλειδιά. Μια επίθεση ωμής βίας σε τέτοιο αριθμό των κλειδιών είναι ανέφικτη.
- Η φύση του αλγορίθμου: Οι κρυπταναλυτές μπορούν να εκτελέσουν τεχνικές κρυπτανάλυσης, αξιοποιώντας το χαρακτηριστικό του αλγορίθμου DES, αλλά κανείς δεν έχει καταφέρει να ανακαλύψει την αδυναμία του.

Η αδυναμία έχει βρεθεί στο σχεδιασμό της κρυπτογράφησης:

Δύο επιλεγμένοι είσοδοι ενός S-box μπορούν να δημιουργήσουν το ίδιο αποτέλεσμα. Ο σκοπός της αρχικής και της τελικής μετάθεσης δεν είναι σαφής.

Πιο συγκεκριμένα .Σε μια επιστημονική αναφορά,ο Peter Gutman περιγράφει τους μηχανισμούς που προκαλούν στατική και δυναμική RAM για να θυμούνται τις τιμές που έχουν αποθηκευτεί για μεγάλο χρονικό διάστημα. Ένας συνετός μηχανικός ασφαλείας θα ρωτούσε ποιο είναι το αποτέλεσμα αυτού στον πραγματικό κόσμο.

Ένα παράδειγμα μιας μονάδας ασφαλείας που χρησιμοποιείται στον τραπεζικό τομέα. Η μονάδα ασφαλείας έχει 12 ζεύγη DES αντικλείδια που αποθηκεύονται σε χαμηλή μνήμη. Η συσκευή είναι ανθεκτική στις παρεμβάσεις με το κλειδί μνήμης διότι κόβεται όταν το παράθυρο είναι ανοιχτό για την εξυπηρέτηση (αυτό είναι απαραίτητο κάθε λίγα χρόνια για να αλλάξει την μπαταρία). Κλειδιά φορτώνονται στη συσκευή σε πολλαπλά μέρη από αξιόπιστο προσωπικό της τράπεζας.

Σε αυτή τη συσκευή, η οποία χρονολογείται γύρω στα τέλη του 1980, οι βασικές αξίες για τα κλειδιά ήταν ουσιαστικά ακέραιες. Ο αριθμός των bits που ήταν λανθασμένος κυμαινόταν γύρω στο 5-10%.

Εάν κάθε κλειδί DES απαρτίζεται από πέντε κομμάτια, τότε η προσπάθεια που εμπλέκει στην αναζήτηση τα 10 bits είναι λάθος σε ένα διπλό κλειδί DES μπορεί να θεωρηθεί ότι είναι 112. Κάθε πράξη θα εμπλέκει: (α) να κάνει ένα διπλό κλειδί 3DES αποκρυπτογράφηση των 64 βασικών PIN bit των οποίων κρυπτογραφημένη αξία είναι ευρέως γνωστή στους προγραμματιστές της τράπεζας (β) στην 2 ^ {-8} περιπτώσεις κατά τις οποίες το αποτέλεσμα αυτό έχει περίεργη ισοτιμία, κρυπτογραφικού έναν αριθμό λογαριασμού με αυτό ως βασικό DES για να δούμε αν η (δεκαδικές), το αποτέλεσμα είναι το αντίστοιχο PIN. Η προσπάθεια είναι 4 φορές 112-επιλέξτε-10 επιχειρήσεις DES - περίπου 2 ^ 50. Αλλά ίσως θα ήταν φθηνότερο να κάνετε μια keysearch υλικού στο πλήκτρο PIN απευθείας από το να προσπαθήσουν να εφαρμόσουν αυτό το σύνθετο 2 ^ 50 αναζήτηση είτε υλικού ή λογισμικού.

Ωστόσο, η bytewise φύση της απόλυσης κλειδί DES μειώνει την προσπάθεια κατά τάξεις μεγέθους. Εάν δεν πατηθεί κανένα πλήκτρο byte έχει ένα διπλό σφάλμα, τότε η προσπάθεια είναι επτά προσπαθεί για κάθε παρατηρήθηκε ακόμη byte ισοτιμίας, ή 7 ^ 10 - περίπου 2 ^ 28, το οποίο είναι εύκολο. Αν υπάρχει ένα βασικό byte με ένα διπλό σφάλμα, η προσπάθεια είναι 2 ^ 38, δίνοντας μια αναζήτηση του 2 ^ 40 πράξεις DES - η οποία εξακολουθεί να είναι εφικτή για ένα άτομο.

3.5.7 Συμβουλές ασφάλειας για τον πελάτη

Ένα μηχάνημα ATM κρατάει την προσωπική σας αριθμό αναγνώρισης (PIN) και άλλες πληροφορίες ασφαλείς με τη χρήση λογισμικού κρυπτογράφησης, όπως το Triple DES (Data Encryption Πρότυπο). Αλλά υπάρχουν πολλά πράγματα που μπορείτε να κάνετε για να προστατεύσετε τα στοιχεία σας και τα χρήματά σας σε ένα ATM.

Πολλές τράπεζες συνιστούνε να επιλέξετε το δικό σας PIN. Συγκεκριμένα η Visa προσφέρει τις ακόλουθες συμβουλές PIN:

α) Μην γράψετε το PIN σας. Εάν πρέπει να το γράψετε, μην το αποθηκεύετε στο πορτοφόλι σας.
β) Κάντε το PIN σας μια σειρά από γράμματα ή αριθμούς που μπορείτε να θυμάστε εύκολα, αλλά αυτό δεν μπορεί εύκολα να συνδέεται με εσάς προσωπικά.
γ) Αποφεύγετε να χρησιμοποιείτε ημερομηνίες γέννησης, αρχικά, αριθμούς σπίτι ή τον αριθμό τηλεφώνου σας.

δ)Αποθηκεύστε την κάρτα ATM σας στο πορτοφόλι ή το πορτοφόλι σας σε μια περιοχή όπου δεν θα γδαρθεί ή θα λυγίσει.

ε)Η κάρτα είναι πιο ευάλωτη σε επιθέσεις αν στέκεστε μπροστά από το ATM, και ψάχνετε μέσα από το πορτοφόλι σας για την κάρτα σας.
Σταθείτε ακριβώς μπροστά από το πληκτρολόγιο του ATM όταν πληκτρολογείτε το PIN σας. Αυτό εμποδίζει τον οποιοδήποτε να περιμένουν να χρησιμοποιήσετε το μηχάνημα από το να βλέπουν τα προσωπικά σας στοιχεία.
Μετά τη συναλλαγή σας, πάρτε την απόδειξή σας, της κάρτας και τα χρήματα μακριά. Μην στέκεστε μπροστά από το μηχάνημα και να μετρήσει τα χρήματά σας.

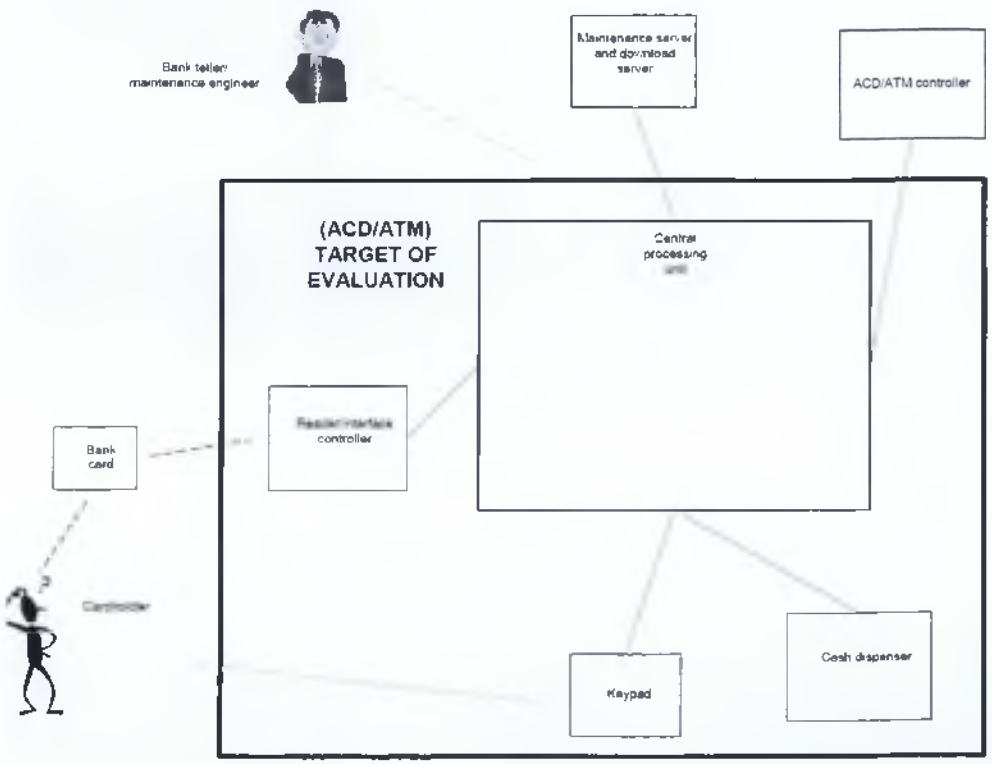
Για λόγους ασφαλείας, ATM χρήστες θα πρέπει να αναζητήσουν ένα μηχάνημα που βρίσκεται σε ένα καλά φωτισμένο δημόσιο χώρο. Η ομοσπονδιακή νομοθεσία απαιτεί ότι μόνο τα τέσσερα τελευταία ψηφία του αριθμού λογαριασμού του κατόχου της κάρτας πρέπει να αναγράφονται στην απόδειξη της συναλλαγής, έτσι ώστε, όταν μια απόδειξη αφήνεται στη θέση του μηχανήματος, ο αριθμός του λογαριασμού είναι ασφαλής. Ωστόσο, η έναρξη της τετραψήφιο προσωπικό αριθμό αναγνώρισης (PIN) από το πληκτρολόγιο θα πρέπει να εξακολουθεί να επισκιάζεται από την παρατήρηση, η οποία μπορεί να γίνει τοποθετώντας το χέρι και το σώμα σας με τέτοιο τρόπο ώστε η εισαγωγή του PIN δεν μπορεί να καταγραφεί από κάμερες κατάστημα ή εργαζόμενους του καταστήματος.

ΚΕΦΑΛΑΙΟ 4: ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΛΕΙΤΟΥΡΓΙΑΣ ATM

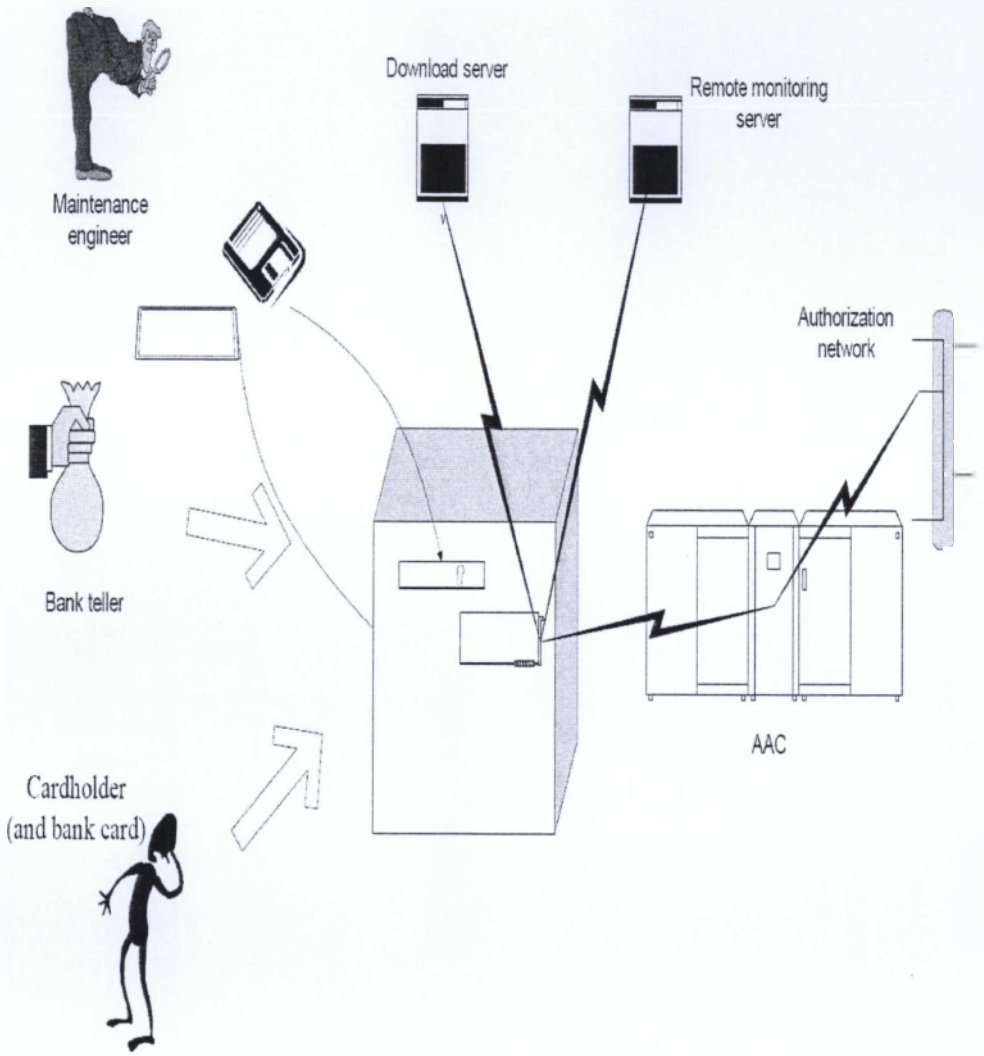
4.1 Εισαγωγή

Οι λειτουργίες που παρέχονται μέσω των ATM ουσιαστικά περιλαμβάνουν τις ακόλουθες συσκευές:

· Μία κεντρική μονάδα επεξεργασίας (ο "εγκέφαλος", το οποίο όρους ή συντονίζει τη συνολική της λειτουργίας),
· Ένας διανομέας μετρητών (μια συσκευή για τη λήψη τραπεζογραμματίων από κασέτες σε μετρητά και την παράδοσή τους στον κάτοχο της κάρτας),
· Έναν αναγνώστη καρτών (για τις έξυπνες κάρτες και ενδεχομένως)
· Μια συσκευή εισόδου για τον κάτοχο της κάρτας (πληκτρολόγιο)

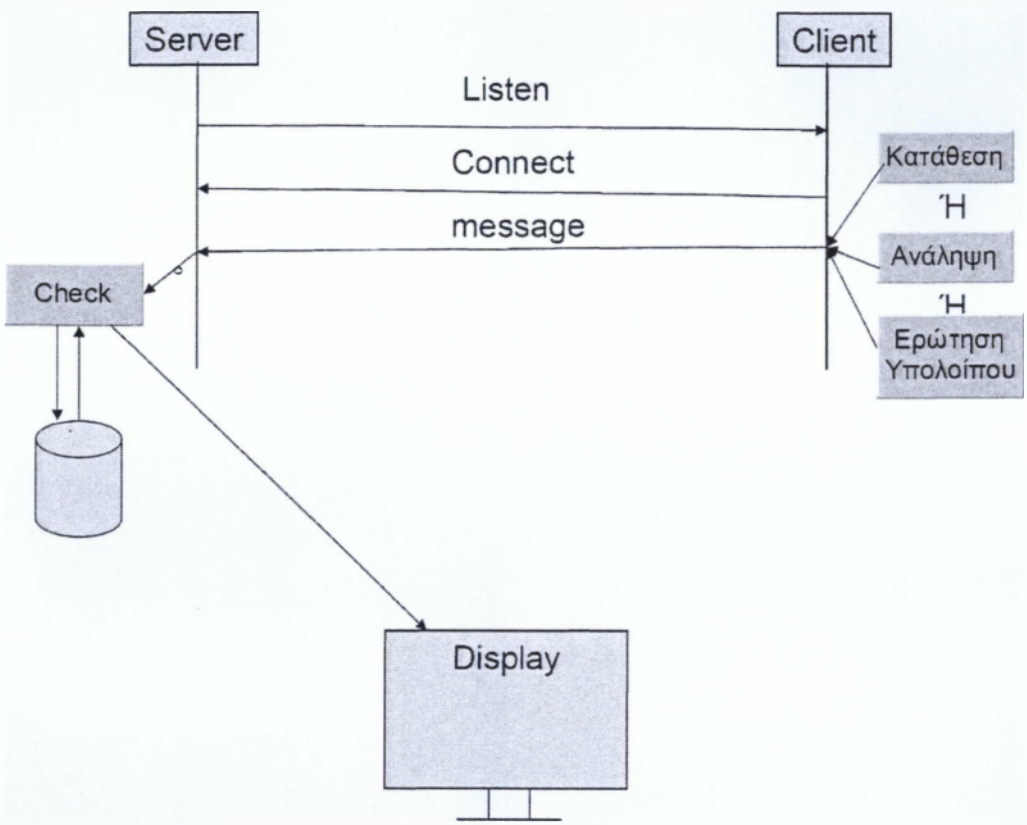


Σχήμα Αρχιτεκτονική ATM



Σχήμα Αρχιτεκτονική ATM

Σχεδιάγραμμα



Listen = Ο Server «ακούει» για τυχόν αίτημα σύνδεσης
Connect = Ο Client κάνει αίτημα σύνδεσης στον Server. Μόλις γίνει η σύνδεση ο Server στέλνει το Public Key του στον Client.
message = Το μήνυμα αυτό περιλαμβάνει το PIN, το Account Number, το ποσό και το είδος της συναλλαγής. Όλα αυτά γίνονται ένα αλφαριθμητικό (message) και κωδικοποιούνται με το Public Key του Server. Ο Server μόλις το λάβει το αποκωδικοποιεί με το Private Key του και στη συνέχεια ξεχωρίζονται τα στοιχεία αυτά. Το μήνυμα (message) αυτό στη συνέχεια υπογράφεται ψηφιακά από τον αποστολέα με σκοπό να ελεγχθεί η ακεραιότητα του μηνύματος από τον παραλήπτη.
Check = Αφού ο Server ξεχωρίσει τα στοιχεία του πελάτη, ελέγχει στην βάση δεδομένων για τον πελάτη σύμφωνα με το PIN και το Account Number και την ενημερώνει ανάλογα με το είδος της συναλλαγής που επιθυμεί ο πελάτης. Τα αποτελέσματα που παίρνει μας τα εμφανίζει στην οθόνη.

4.2Διάγραμμα ροής λειτουργίας ATM

Αυτό η use case περιγράφει τον τρόπο με τον οποίο ο πελάτης της τράπεζας χρησιμοποιεί το ATM για ανάληψη χρημάτων στον τραπεζικό του λογαριασμό.

4.2.1Προϋποθέσεις

- Να υπάρχει μια ενεργή σύνδεση στο δίκτυο της Τράπεζας.
- Το ATM να έχει χρήματα διαθέσιμα.

4.2.2 Βασική ροή των γεγονότων

Βήμα 1:Η use case ξεκινά όταν ο πελάτης εισάγει την κάρτα της τράπεζας.
Βήμα 2:Γίνεται η επικύρωση χρήστη
Βήμα 3:Το ATM εμφανίζει τις διάφορες εναλλακτικές λύσεις που είναι διαθέσιμες σε αυτή τη μονάδα. Στην περίπτωση αυτή, ο πελάτης επιλέγει πάντα "ανάληψη μετρητών".
Βήμα 4:Το ATM ζητά λογαριασμό.
Βήμα 5:Ο πελάτης επιλέγει ένα λογαριασμό.
Βήμα 6:Το ATM ζητά ένα ποσό.
Βήμα 7:Ο πελάτης εγγράφει το ποσό.
Βήμα 8:Ο κωδικός της κάρτας ,το PIN, το ποσό και ο λογαριασμός αποστέλλονται στην τράπεζα ως συναλλαγή. Η απαντήσεις της τράπεζας είναι αποδοχή ή απόρριψη λέγοντας εάν η συναλλαγή είναι εντάξει.
Βήμα 9:Στη συνέχεια, τα χρήματα διανέμονται.
Βήμα 10:Η κάρτα επιστρέφεται.
Βήμα 11:Η απόδειξη εκτυπώνεται.
Βήμα 12:Η use case τελειώνει με επιτυχία.

Εναλλακτικές Ροές

1 Μη έγκυρος χρήστης

Αν στο βήμα 2 της ροής, η περίπτωση χρήσης: Επικύρωση χρήστη δεν ολοκληρωθεί με επιτυχία, στη συνέχεια, η περίπτωση χρήσης τελειώνει με μια κατάσταση σφάλματος.

2 Λάθος λογαριασμός

i. Αν στο βήμα 8 της ροής ο λογαριασμός θα επιλέξει ο Πελάτης Τράπεζα δεν σχετίζεται με αυτή την κάρτα τράπεζα, στη συνέχεια, το ATM θα εμφανιστεί το μήνυμα "Μη Λογαριασμός - παρακαλώ δοκιμάστε ξανά."
ii. Η use case επανέρχεται στο βήμα 4.

3 Λάθος ποσό

Εάν στο βήμα 7 στη ροή, ο πελάτης εισάγει ένα ποσό που δεν μπορεί να «δημιουργήσει» το ATM με το διαθέσιμα είδη των χαρτονομισμάτων(βλέπε ειδική απαίτηση WC-1 για τα έγκυρα ποσά), τότε

i. Το ATM πρέπει να εμφανίζει ένα το μήνυμα που δηλώνει ότι το ποσό πρέπει να είναι πολλαπλάσιο των χαρτονομισμάτων, και να ζητήσει από τον πελάτη να εισάγει το ποσό πάλι.
ii. Η use case συνεχίζεται στο βήμα 7.

4 Ποσό που υπερβαίνει το όριο ανάληψης

Αν στο βήμα 7 στη ροή, ο πελάτης εισάγει ένα ποσό που υπερβαίνει το όριο ανάληψης (βλέπε ειδική απαίτηση WC-2 για μέγιστο ποσό), τότε

i. το ATM πρέπει να εμφανίζει ένα προειδοποιητικό μήνυμα, και να ζητήσει από τον πελάτη να επανέλθει το ποσό ξανά
ii. Η use case συνεχίζεται στο βήμα 7

5 Ποσό που υπερβαίνει το ημερήσιο όριο ανάληψης

Αν στο βήμα 8 στη ροή, η τράπεζα απαντά ότι το ημερήσιο όριο ανάληψης έχει ξεπεραστεί (αυτό καθορίζεται από την Τράπεζα και εξαρτάται από το συγκεκριμένο λογαριασμό), τότε

i. το ATM πρέπει να εμφανίζει ένα προειδοποιητικό μήνυμα, και να ζητήσει από τον πελάτη να επανέλθει το ποσό ξανά
ii. Η use case συνεχίζεται στο βήμα 7

6 Ανεπαρκή χρήματα

Αν στο βήμα 7 στη ροή, ο πελάτης Τράπεζα εισάγει ένα ποσό που υπερβαίνει το ποσό του διαθεσίμου ρευστού στο ATM, τότε

i. το ATM πρέπει να εμφανίζει ένα προειδοποιητικό μήνυμα, και να ζητήσει από τον πελάτη να επανέλθει το ποσό ξανά
ii. Η use case συνεχίζεται στο βήμα 7

7 Δεν υπάρχει απάντηση από την τράπεζα

Αν στο βήμα 8 της ροής δεν υπάρχει καμία απάντηση από την τράπεζα μέσα σε 3 δευτερόλεπτα, στη συνέχεια,

i. Το ATM θα προσπαθήσει εκ νέου, έως και τρεις φορές.
ii. Αν δεν υπάρχει ακόμα καμία απάντηση από την τράπεζα, το ATM θα εμφανίσει το μήνυμα "Δίκτυο μη διαθέσιμο - δοκιμάστε ξανά αργότερα".
iii. Θα επιστρέψει την κάρτα.
iv. Θα αναφέρει ότι είναι «κλειστό».
v. Η use case τελειώνει σε κατάσταση σφάλματος.

8 Τα χρήματα δεν αφαιρούνται

Αν στο βήμα 9 της ροή τα χρήματα δεν αφαιρούνται από το μηχάνημα μέσα σε 15 δευτερόλεπτα, στη συνέχεια.

i. το ATM εκδίδει προειδοποιητικό ήχο και θα εμφανίσει το μήνυμα "Παρακαλώ αφαιρέστε τα μετρητά".
ii. Αν εξακολουθεί να μην υπάρχει απάντηση από τον πελάτη μέσα σε 15 δευτερόλεπτα το ATM θα πάρει πίσω τα χρήματα και θα σημειώσει την αποτυχία στο αρχείο καταγραφής.
iii. Η use case θα τελειώσει με τον όρο αποτυχία.

9 Quit

Αν στο σημείο πριν από το βήμα 8 στη ροή ο πελάτης επιλέγει Quit, στη συνέχεια,

i. Το ATM πρέπει να τυπώνει απόδειξη που αναφέρει ότι η συναλλαγή ακυρώθηκε.
ii. Το ATM θα επιστρέψει την κάρτα.
iii. Η use case τελειώνει.

Βασικά Σενάρια

Δεν υπάρχει απάντηση από την Τράπεζα

Μετα-συνθήκες

1 Επιτυχής ολοκλήρωση

Ο χρήστης έχει λάβει τα μετρητά του και η τράπεζα έχει ενημερωθεί.

2 Κατάσταση αποτυχίας

Η τράπεζα έχει ενημερωθεί αναλόγως.

Ειδικές απαιτήσεις

[SpReq2: WC-2] Η μέγιστη ατομική απόσυρση είναι $ 500.
[SpReq: WC-1] Το ATM τηρεί ημερολόγιο, ώρα και ημερομηνία. όλων των πλήρη και ημιτελών συναλλαγών με την τράπεζα.

11. Αναλήψεις στο εξωτερικό.

Τα ATM παρέχουν τη δυνατότητα να προσφέρουν αναλήψεις στο εξωτερικό.

Στις χώρες εκτός ευρωζώνης, η μετατροπή γίνεται βάσει της συναλλαγματικής ισοτιμίας της ημέρας της επεξεργασίας της συναλλαγής από την τράπεζά και όχι της ημέρας που πραγματοποιεί την ανάληψη ο πελάτης. Επιπλέον, η τράπεζά ενδέχεται να χρεώσει τον λογαριασμό με μία **πάγια προμήθεια** ανά ανάληψη.

Στις χώρες της ευρωζώνης επίσης ενδέχεται να επιβαρυνθεί ο πελάτης με προμήθεια για τις αναλήψεις που πραγματοποιεί. Τα έξοδα τραπέζης είναι ίδια είτε η ανάληψη πραγματοποιείται στη χώρα διαμονής του πελάτη είτε σε οποιαδήποτε άλλη χώρα της ευρωζώνης (Κανονισμός 2560/2001 της 28ης Δεκεμβρίου 2001 σχετικά με τις διασυνοριακές πληρωμές σε ευρώ καθώς και οδηγία 2007/64/ΕΚ για τις υπηρεσίες πληρωμών στην εσωτερική αγορά η οποία ενσωματώθηκε στην ελληνική νομοθεσία με το Ν.3862/8.7.2010(ΦΕΚ 113 Α'/13.7.2010) ο οποίος τροποποιήθηκε με τον Κανονισμό 924/2009)

12 Επιπρόσθετα θέματα

1Το ATM δε δέχεται την κάρτα.

Πιθανές εξηγήσεις:

i. Ο πελάτης έχει υπερβεί το 24ωρο όριο αναλήψεων.
ii. Η κάρτα έχει απομαγνητιστεί.

2 Το ATM παρακρατά την κάρτα **σας.**

Πιθανές εξηγήσεις:

i. Η κάρτα έχει λήξει.
ii. Καθυστέρησε ο πελάτης υπερβολικά κατά την πληκτρολόγηση του PIN.
iii. Πληκτρολόγησε λάθος PIN 3 φορές.
iv. Δυσλειτουργία του ATM.

3Το ποσό που έλαβε ο πελάτης δεν είναι αυτό που ζήτησε.

Πρέπει να αναφέρει, ο πελάτης, το πρόβλημα στο κατάστημα στο οποίο ανήκει το ATM επιδεικνύοντας τα χαρτονομίσματα και την απόδειξη και να υποβάλλει τα παράπονο στην τράπεζά μιας και μέσω ATM είναι αδύνατο να διαχειριστεί το πρόβλημα.

4.3 Σύγκριση E-banking με ATM

Όπως το πρόβλημα παραλαβής μετρητών το ATM δεν έχει την δυνατότητα να το διαχειριστεί υπάρχουν και άλλα θέματα αλλά και υπηρεσίες που είναι ανέφικτες μέσω αυτού.Τη λύση στο πρόβλημα έρχεται να δώσει το e-banking που είναι ο πιο σύγχρονος τρόπος να χρησιμοποιούνται οι παροχές της τράπεζας από τους πελάτες στη βολή του σπιτιού τους. Σχεδόν όλες οι δυνατότητες του ATM μεταφέρονται στο διαδίκτυο σε συνδυασμό με τις παροχές της ίδιας της τράπεζας. Οπότε καθίσταται λογικό οι τράπεζες να αφιερώνουν πόρους για την υλοποίηση διαδικτυακών πλατφορμών.

Η αναφορά σε μία συγκεκριμένη τράπεζα κρίνεται σκόπιμη καθώς οι τράπεζες παρέχουν παρόμοιες υπηρεσίες όχι όμως ακριβώς τις ίδιες. Θα γίνει εκτενης αναφορά στην τράπεζα Πειραιώς που θεωρείται η πιο καινοτόμα σε θέματα e-banking.

Η υλοποίηση του εναλλακτικού καναλιού της ηλεκτρονικής τραπεζικής της τράπεζας Πειραιώς, αποτελεί έναν αυτόνομο τόπο (ιστοσελίδα) στο διαδίκτυο, αποκλειστικά διαμορφωμένο για τις ηλεκτρονικές τραπεζικές υπηρεσίες (e-banking). Η τράπεζα Πειραιώς λοιπόν, το 2000 εισήγαγε την πρώτη ολοκληρωμένη πλατφόρμα ηλεκτρονικών υπηρεσιών (internet banking, phone banking, mobile banking) στην Ελληνική τραπεζική αγορά, με το ξεχωριστό όνομα "Winbank". Αναλυτικά, οι προσφερόμενες ηλεκτρονικές υπηρεσίες για τους ιδιώτες είναι οι εξής:

1. Διαχείριση λογαριασμών

a. Εμφάνιση/Ανάλυση υπολοίπων και κινήσεων λογαριασμών.
b. Αποστολή των κινήσεων λογαριασμών μέσω ταχυδρομείου και ηλεκτρονικού ταχυδρομείου (e-mail).
c. Προβολή αναλυτικών στοιχείων του λογαριασμού.
d. Εμφάνιση των επιτοκίων χορηγήσεων/καταθέσεων.
e. Ενημέρωση για το διεθνή αριθμό λογαριασμού (IBAN).

2. Διαχείριση καρτών

a. Εμφάνιση υπολοίπων και κινήσεων πιστωτικών καρτών.
b. Άμεση εμφάνιση και εκτύπωση των μηνιαίων λογαριασμών.
c. Αποστολή των μηνιαίων λογαριασμών μέσω ταχυδρομείου και ηλεκτρονικού ταχυδρομείου (e-mail).
d. Παροχή αναλυτικών στοιχείων των πιστωτικών καρτών.
e. Δυνατότητα άμεσης πληρωμής ή πληρωμής σε μελλοντική ημερομηνία.

3. Διαχείριση δανείων

a. Συνολική απεικόνιση των δανείων.
b. Παροχή αναλυτικών στοιχείων των δανείων.
c. Δυνατότητα πληρωμής δόσεων.

4. Διαχείριση επιταγών

a. Δυνατότητα παραγγελίας βιβλιαρίου.
b. Παροχή αναλυτικών στοιχείων και παρακολούθηση επιταγών.

c. Αναζήτηση ανά αριθμό/σελίδα επιταγής και χρονική περίοδο.
d. Καταχώρηση στοιχείων και επεξεργασία διαθέσιμων και ανεξόφλητων επιταγών.
e. Ενημέρωση της κατάστασης (π.χ. εξοφλημένες, ακυρωμένες, ανακλημένες,κ.τ.λ.).
f. Ανάκληση βιβλιαρίου επιταγών.
5. Πληρωμές/Μεταφορές

a. Μεταφορά χρημάτων σε λογαριασμούς του ιδίου στην τράπεζα Πειραιώς.
b. Μεταφορά χρημάτων σε λογαριασμούς τρίτων στην Τράπεζα Πειραιώς.
c. Μεταφορά ποσού από κάρτα Visa σε άλλη κάρτα.
d. Πληρωμή πιστωτικής κάρτας άλλης τράπεζας.
e. Εντολές πληρωμής τρίτων σε μελλοντική ημερομηνία.
f. Εντολές εμβασμάτων.
g. Καθορισμός περιοδικών πληρωμών.
h. Αποθήκευση Τακτικών Πληρωμών για Άμεση Επανάληψη.
i. Αλλαγή στοιχείων αποθηκευμένων εντολών πληρωμών.
j. Αναβολή ή ακύρωσή αποθηκευμένων εντολών πληρωμών.
k. Πάγιες ή μεμονωμένες εντολές πληρωμής)ΕΚΟ ()ΕΗ, ΟΤΕ, ΕΥ)ΑΠ).
l. Πάγιες ή μεμονωμένες εντολές πληρωμής εταιρειών τηλεφωνίας (Cosmote,
m. Vodafone, Wind, Tellas, Q-Telecom).
n. Πάγιες εντολές πληρωμής εταιρειών συνδρομητικής τηλεόρασης (Nova).
o. Προσωρινή απενεργοποίηση και μεταβολή των πάγιων εντολών.
p. Διακοπή πάγιων εντολών.
q. Μεμονωμένες εντολές πληρωμής ασφαλιστικών φορέων (ALLIANZ ΑΕΓΑ,
r. ΑΕΑΖ, ING).
s. Μεμονωμένες εντολές πληρωμής (ΙΚΑ. ΦΠΑ. ΤΕΒΕ).
t. Μεμονωμένη εντολή πληρωμής Φόρου Εισοδήματος Φυσικών Προσώπων.
u. Ανανέωση χρόνου ομιλίας "Vodafone Refill".
v. Προσφορές σε μη κυβερνητικές οργανώσεις με χρέωση του τραπεζικού
w. λογαριασμού του πελάτη.
x. Αποστολή μαζικών εμβασμάτων μέσω αρχείου (του πελάτη).
y. Ιστορικό του συνόλου των πληρωμών.

6. Χρηματιστηριακές συναλλαγές

a. Άμεση παρακολούθηση των τιμών των μετοχών του Χ.Α.Α.
b. Άμεση αποτίμηση του χαρτοφυλακίου του πελάτη.
c. Άμεση ενημέρωση για τις τιμές των μετοχών του πελάτη.
d. Άμεση παρακολούθηση των Ενδοσυνεδριακών δεδομένων του Χ.Α.Α.
e. Ημερήσιο και ιστορικό γράφημα των τιμών μετοχών.
f. Άμεση ενημέρωση για τις τιμές των δεικτών των διεθνών αγορών.
g. Άμεση ενημέρωση για τα οικονομικά, επιχειρηματικά και χρηματιστηριακά νέα της
h. Ελληνικής και διεθνούς αγοράς.
i. Ισοτιμίες των ξένων νομισμάτων.
j. Τιμές αμοιβαίων κεφαλαίων της τράπεζας.
k. Άμεση ενημέρωση για την κατάσταση (status) της εντολής.
l. Συμμετοχή σε δημόσιες εγγραφές.
m. Ενημέρωση για την εκτέλεση των εντολών.
n. Εντολές μεταπώλησης εντολών που αγοράστηκαν μέσα στην ίδια ημέρα.
o. Εντολές αγοράς μετοχών με χρέωση λογαριασμού.
p. Εντολές πώλησης μετοχών με πίστωση λογαριασμού.

7. Αιτήσεις

a. Σχετικά με προσωπικό καταναλωτικό δάνειο.
b. Σχετικά με πιστωτική κάρτα.
c. Σχετικά με καταθετικούς λογαριασμούς.
d. Σχετικά με μεταφορά υπολοίπου από άλλη πιστωτική κάρτα.

Μία επιπλέον υπηρεσία που παρέχεται στους χρήστες της ηλεκτρονικής τραπεζικής είναι αυτή των ειδοποιήσεων (alerts), μέσω της οποίας μπορούν να πληροφορηθούν άμεσα και έγκυρα για τραπεζικές συναλλαγές που τους ενδιαφέρουν. Ειδικότερα, οι πελάτες μπορούν να ειδοποιηθούν όπου και αν βρίσκονται, μέσω α) ηλεκτρονικού ταχυδρομείου (e-mail), β) γραπτού μηνύματος (sms), ή γ) τηλεφωνήματος από τραπεζικό αντιπρόσωπο για τις υπηρεσίες:

- Μεταβολές του λογιστικού υπολοίπου τους.
- Πιστώσεις και χρεώσεις συγκεκριμένων κινήσεων των λογαριασμών τους.
- Μεταχρονολογημένες και περιοδικές εντολές πληρωμών τους.
- Χρηματιστηριακές συναλλαγές και αποτίμηση του χαρτοφυλακίου τους.

Ειδικότερα, η τράπεζα Πειραιώς προσφέρει αποκλειστικά για τις επιχειρήσεις μέσω της υπηρεσίας "winbank internet business" τη δυνατότητα πολλαπλών χρηστών/υπαλλήλων της τελευταίας, οι οποίοι έχουν διαφορετικά δικαιώματα πρόσβασης στην υπηρεσία (π.χ. μόνο παρακολούθηση υπολοίπων, διενέργεια συναλλαγών μόνο μεταξύ προϊόντων της εταιρίας, προετοιμασία συναλλαγών προς ολοκλήρωση/έγκριση από άλλο χρήστη, κ.λ.π.). Η δυνατότητα αυτή αφορά θέματα:

- «Διπλής» υπογραφής για κάθε συναλλαγή.
- Διαφορετικά χρηματικά όρια για κάθε είδος συναλλαγής.
- Διαφορετικά εγκριτικά επίπεδα ή επίπεδα πρόσβασης για κάθε υπηρεσία.
- Ύπαρξη ενός διαχειριστή κωδικών (Administrative ID) για κάθε εταιρεία, ο οποίος θα έχει τη δυνατότητα παρακολούθησης όλων των κινήσεων πουδιενεργούνται από όλους τους άλλους υπαλλήλους/χρήστες της ίδιας εταιρείας.

ΚΕΦΑΛΑΙΟ 5:ΜΕΛΛΟΝΤΙΚΗ ΕΞΕΛΙΞΗ ΤΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΤΡΑΠΕΖΙΚΗΣ

Η ηλεκτρονική τραπεζική στην Ελλάδα βρίσκεται ακόμα σε πρώιμο στάδιο και παρουσιάζει μεγάλα περιθώρια ανάπτυξης. Οι προκλήσεις είναι πολλές, καθώς η τεχνολογία εξελίσσεται συνεχώς.

Η σταδιακή ενσωμάτωση στην ελληνική αγορά των επιτευγμάτων της ηλεκτρονικής τραπεζικής που αξιοποιούνται ήδη στο εξωτερικό και η μελέτη των τάσεων που εμφανίζονται βάσει των αναγκών που θα προκύψουν, δίνει μια ικανοποιητική προσέγγιση της κατάστασης που θα διαμορφωθεί γύρω από το e-Banking στην Ελλάδα.

5.1Έξυπνες κάρτες (Smart Cards)

Με καθυστέρηση κάποιων ετών και μετά την επιτυχημένη παρουσία τους στο εξωτερικό, αναμένεται η εξάπλωση της χρήσης τους στην αγορά, από κάθε τερματικό,συνδράμοντας στην ασφάλεια των συναλλαγών.

5.2 Ηλεκτρονικές μικροπληρωμές (Micropayments)

Το ηλεκτρονικό χρήμα θα αντικαταστήσει τα μετρητά ακόμα και στις χαμηλότερου ύψους συναλλαγές π.χ. αγορά εφημερίδων - αναψυκτικών από περίπτερο,
καθιστώντας το πορτοφόλι διακοσμητικό. Ήδη η Visa και η Mastercard συζητούν το λανσάρισμα νέων προϊόντων, τα οποία θα πάρουν τη θέση των κερμάτων και θα αναγνωρίζονται ακόμα και από τις μηχανές πώλησης εισιτηρίων στα μέσα μαζικής μεταφοράς.

5.3 Πληρωμές μεταξύ επιχειρήσεων - B2B payments

Στην Ελλάδα οι πληρωμές μεταξύ επιχειρήσεων πραγματοποιούνται κατά κύριο λόγο με μεταχρονολογημένες επιταγές. Οι on-line πληρωμές περιορίζονται στις συναλλαγές των επιχειρήσεων με το κράτος (π.χ. πληρωμή ΦΠΑ, ασφαλίστρων κλπ.). Τα τελευταία όμως χρόνια έχει αρχίσει να γίνεται λόγος για κατάργηση αυτού του μέσου πληρωμής, που σπάνια απαντάται στις χώρες του εξωτερικού.

Στο εξωτερικό η πλειονότητα των πληρωμών γίνεται άμεσα, ενώ ενισχύθηκε σημαντικά ο ρόλος των εταιρειών παροχής υπηρεσιών ταυτοποίησης συναλλασσομένων επιχειρήσεων(π.χ. η Identrus)στην πιστοποίηση των εμπλεκομένων μερών. Έτσι οι εμπορικές συναλλαγές ολοκληρώνονται ταχύτατα στα e-market place, όπου η μια επιχείρηση πληρώνει την άλλη αποφεύγοντας τις χρονοβόρες και υψηλού κόστους γραφειοκρατικές διαδικασίες.

Ένα ικανοποιητικό υποκατάστατο της φυσικής επιταγής θα μπορούσε να αποτελέσει μια ηλεκτρονική επιταγή, με δυνατότητα μεταχρονολόγησης.Η ηλεκτρονική επιταγή θα έχει αξία για τον κομιστή της και θα μπορεί να σταλεί μέσω internet, να μεταβιβαστεί ηλεκτρονικά σε άλλον προμηθευτή, να προεξοφληθεί και να χρησιμοποιηθεί ως ενέχυρο για κεφάλαιο κίνησης κλπ.

5.4 Νέες δυνατότητες - επιστροφή γνώσης στον πελάτη

Μέχρι σήμερα, η μόνη πληροφόρηση που λαμβάνει ο χρήστης της ηλεκτρονικής τραπεζικής ως απάντηση μετά την εκτέλεση των συναλλαγών του έχει να κάνει με την επιτυχία ή αποτυχία εκτέλεσης λόγω συγκεκριμένου προβλήματος.

Η προσέγγιση του μέλλοντος περιλαμβάνει τον εμπλουτισμό των παρεχομένων πληροφοριών, για παράδειγμα:

- Αυτόματη ενημέρωση για το λογιστικό υπόλοιπο του λογαριασμού, έπειτα από μια πετυχημένη μεταφορά χρημάτων σε λογαριασμό τρίτου, εξοικονομώντας χρόνο για τον πελάτη.
- Πληροφόρηση για τη μέση αξία των εντολών ΦΠΑ του τρέχοντος έτους ή για το συνολικό αριθμό των εντολών και της αξίας, έπειτα από κάθε πληρωμή ΦΠΑ. πληροφορία ιδιαίτερης σημασίας για τα λογιστικά γραφεία
- Επισήμανση τυχόν εντολών πληρωμής λογαριασμών π.χ.)ΕΗ των οποίων η αξία υπερβαίνει σημαντικά το μέσο όρο των εντολών πληρωμής αντίστοιχων λογαριασμών, προστατεύοντας τον πελάτη από εσφαλμένες καταχωρήσεις
- Παροχή χρήσιμων ενημερωτικών πληροφοριών ανάλογα με το προφίλ του χρήστη και τη συναλλακτική σχέση που το οικοδομεί, όπως είναι η υπενθύμιση σε ένα λογιστή που καταχωρεί εντολή ΦΠΑ για την καταληκτική ημερομηνία πληρωμής ΙΚΑ
- Ενημέρωση για υπηρεσίες - συναλλαγές που προστίθενται στις υπάρχουσες κατά την εισαγωγή του χρήστη στο σύστημα
- Ενημέρωση για τραπεζικά προϊόντα που πιθανόν να ενδιαφέρουν το χρήστη βάσει του προφίλ που έχει διαμορφωθεί, όπως για επενδυτικά προϊόντα, πιστωτικές κάρτες, δάνεια κ.α., μέσα στα πλαίσια των σταυροειδών πωλήσεων (cross-selling)
- Παροχή διάφορων στατιστικών στοιχείων π.χ. για την αξία των συνολικών αναλήψεων πληρωμών κλπ. βοηθώντας το χρήστη να μελετήσει την κίνηση του λογαριασμού του και την οικονομική του συμπεριφορά

Οι τράπεζες εκμεταλλευόμενες τα δεδομένα που καταχωρούνται στα ηλεκτρονικά αρχεία τους και δίνοντάς τους τη μορφή μηνυμάτων πληροφόρησης, υπενθύμισης ,προώθησης μπορούν να δημιουργήσουν αμφίδρομη επικοινωνία με τον πελάτη προσφέροντάς του γνώσεις και οφέλη που δεν είχε μέχρι τότε.

5.5 Σύγχρονα προιόντα - απαιτήσεις

Κατ' αυτό τον τρόπο αναμένονται τα παρακάτω προϊόντα:

5.5.1 Έξυπνα sites

Έξυπνα sites θεωρούνται αυτά που έχουν ενσωματωμένη ευφυία και διαμορφώνουν το περιεχόμενο και τις επιλογές τους σύμφωνα με τις ιδιαιτερότητες του χρήστη.

Με τη συνδρομή των γνωσιακών βάσεων που υπάρχουν στα back-end

συστήματά τους και κατόπιν επεξεργασίας των στοιχείων που αφορούν το ιστορικό των περιηγήσεων του χρήστη και τη συναλλακτική του δραστηριότητα. τα sites δημιουργούν ένα φιλικό περιβάλλον εργασίας συγκεντρώνοντας και εμφανίζοντας στο χρήστη την πληροφορία που πραγματικά τον ενδιαφέρει.
Μέσα σε αυτό το διαδραστικό περιβάλλον, οι επιλογές και η πληροφόρηση του χρήστη διαμορφώνονται ουσιαστικά από τον ίδιο. Η πληροφόρηση που θα λαμβάνει θα έχει αντίστοιχη μορφή με τις περιπτώσεις που παρατέθηκαν παραπάνω. Στο μενού επιλογών του e-Banking site θα εμφανίζονται οι επιλογές - πληροφορίες που χρησιμοποιούνται πιο τακτικά από τον πελάτη, ενώ για τις λοιπές πληροφορίες - συναλλαγές η πρόσβαση θα γίνεται από ένα σύνδεσμο (link) με την ονομασία Λοιπές Επιλογές.

5.5.2 Ψηφιακοί Πράκτορες (Smart agents)

Οι ψηφιακοί πράκτορες αναπτύσσονται για την αύξηση του αισθήματος παροχής
προσωποποιημένων υπηρεσιών στους χρήστες μέσω internet. Οι ψηφιακοί αυτοί χαρακτήρες, που φέρουν συνήθως ανθρώπινη μορφή, συνιστούν τον ενδιάμεσο μεταξύ
του πελάτη και του διαδικτυακού τόπου και αναλαμβάνουν το σύνολο της επικοινωνίας
του επισκέπτη με το site.

Η επικοινωνία επιτυγχάνεται μέσω γραπτών μηνυμάτων που πληκτρολογεί ο χρήστης και απαντά ο πράκτορας αντίστοιχα είτε εφόσον ο χρήστης διαθέτει τον κατάλληλο εξοπλισμό, φωνητικά.

Η χρησιμότητα των ψηφιακών πρακτόρων είναι πολλαπλή:

- Συμβάλλουν στην εξοικείωση του χρήστη με το περιβάλλον, αντικαθιστώντας την ανθρώπινη παρουσία, καλωσορίζοντάς τον στην εφαρμογή και αναπτύσσοντας διάλογο μαζί του
- Κατευθύνουν τον πελάτη για τη μετάβασή του σε ιστοσελίδες ενδιαφέροντός του
- Βοηθούν στην εξάλειψη προβλημάτων που εμφανίζονται κατά τη διεκπεραίωση των συναλλαγών καθοδηγώντας το νέο χρήστη και δίνοντας τις κατάλληλες οδηγίες - διευκρινήσεις
- Συγκεντρώνουν στοιχεία για το προφίλ του χρήστη καταγράφοντας σε γνωσιακή βάση τις προτιμήσεις, τις συνήθειες, τα παράπονα και τις παρατηρήσεις του, για τη μελλοντική εκμετάλλευσή τους από την τράπεζα
- Με τη χρήση on-line ερωτηματολογίων, on-line ψηφοφοριών, on-line χώρων κατάθεσης σκέψεων συλλέγουν άμεσα και με φιλικό τρόπο την πληροφορία που ενδιαφέρει την τράπεζα
- Χρησιμοποιούνται για την on-line διαφήμιση και on-line πώληση προϊόντων και υπηρεσιών.

Βέβαια για να επιτευχθεί η συγκέντρωση και επιστροφή γνώσης στον πελάτη, απαιτείται η πραγματοποίηση σημαντικού ύψους επενδύσεων ώστε να δημιουργηθούν οι κατάλληλες υποδομές από τις τράπεζες με dataware houses και knowledge bases και ανάπτυξη της απαραίτητης τεχνογνωσίας. Μάλιστα, για τη

βελτίωση του αποτελέσματος, μπορούν εναλλακτικά να συνεργαστούν με εξωτερικούς συνεργάτες.

5.5.3 Ολοκληρωμένα Portals/Aggregators

Οι τράπεζες για την πιο αποδοτική αξιοποίηση των sites τους, θα πρέπει να επικεντρωθούν στην αύξηση του χρόνου διαμονής των χρηστών σ' αυτά. Έτσι, τα κέρδη που θα αποκομίσουν από τα έσοδα, τις διαφημίσεις, την καλή φήμη και την πιστότητα των πελατών τους θα είναι πολλαπλάσια.

Η ανάπτυξη ολοκληρωμένων Internet Banking Portals που θα προσφέρουν στο χρήστη επιπλέον των συναλλαγών, πληροφορίες και άλλες λειτουργίες, μπορούν να καταστήσουν το site της τράπεζας, το συχνότερο τόπο επίσκεψης του πελάτη στο διαδίκτυο και να του δώσουν προστιθέμενη αξία.

Για την επίτευξη του παραπάνω, οι τράπεζες θα κληθούν να συνεργαστούν και να αφιερώσουν κάποιο χώρο στην ιστοσελίδα τους σε εταιρικούς πελάτες τους, που με συνδέσμους θα καλύπτουν κάθε πιθανή ανάγκη του χρήστη. Με την καταγραφή, επεξεργασία και αξιοποίηση των πληροφοριών που συγκεντρώνονται κατά την πλοήγηση του χρήστη θα είναι δυνατή η προσφορά τους σ' ένα site, αυτό της τράπεζας (aggregator).

Τέτοια μπορεί να είναι περιβάλλον ηλεκτρονικών συναλλαγών, εκπαιδευτικό υλικό για τραπεζικά θέματα, νέα -ειδήσεις τόσο από το χώρο του e-Banking, όσο και από το γενικότερο τραπεζικό χώρο, on-line chatting χρηστών, forums χρηστών, ψυχαγωγία, διαγωνισμοί, επενδυτικοί οδηγοί, χρηματιστήριο, χρήσιμα εργαλεία, ημερολόγια κλπ. είναι μερικές από τις δυνατότητες που μπορούν να παρέχουν οι τραπεζικοί οργανισμοί στους διαδικτυακούς τους τόπους ώστε να αποτελέσει το site του Internet Banking την «αρχική σελίδα» ίσως και τη μόνη για τον πελάτη.

5.5.4 Διατραπεζικές μεταφορές κεφαλαίων σε πραγματικό χρόνο

Μέχρι σήμερα, οι οικονομικές συναλλαγές που εκτελούνται σε πραγματικό χρόνο αφορούν μεταφορές εντός της ίδιας τράπεζας, ανανέωση χρόνου καρτοκινητής τηλεφωνίας και αγοραπωλησία μετοχών στο Χρηματιστήριο Αξιών.

Ο εμπλουτισμός των οικονομικών συναλλαγών που πραγματοποιούνται σε πραγματικό χρόνο θα διευκολύνει σημαντικά τους πελάτες των τραπεζών και θα αυξήσει τον αριθμό των ηλεκτρονικών συναλλαγών.

Οι διατραπεζικές αναλήψεις μετρητών και μεταφορές χρημάτων (με εισαγωγή εντολών) μέσω των συστημάτων DIASnet-ATM Switching και DIAStransfer αντίστοιχα βαρύνονται με μεγάλες προμήθειες. Μάλιστα ιδιαίτερα στη δεύτερη περίπτωση η συναλλαγή δεν εκτελείται σε πραγματικό χρόνο. Επομένως, η κάλυψη μιας επιταγής στην τράπεζα Α από κεφάλαια που βρίσκονται στην τράπεζα Β για να γίνει αυθημερόν, απαιτεί τη μετάβαση του πελάτη σε κατάστημα της τράπεζας Α, καθώς η πραγματοποίηση της συναλλαγής μέσω Internet Banking γίνεται την επόμενη εργάσιμη.

Η διατραπεζική συνεργασία για την ανάπτυξη ενός διατραπεζικού Internet Banking με στόχο την άμεση εκτέλεση των εντολών μπορεί να επιτευχθεί με τη συμμετοχή ενός φορέα - σημείο αναφοράς - όπως π.χ. η ΙΑΣ ΑΕ, ο οποίος σε συνεργασία με τρίτους Οργανισμούς θα καταστήσει δυνατή την άμεση διενέργεια

συναλλαγών (π.χ. εμβάσματα εσωτερικού, πληρωμές πιστωτικών καρτών, πληρωμές λογαριασμών)ΕΚΟ κλπ.) και την έγκαιρη ενημέρωση για την τύχη τους.

Συγκεκριμένα, ο πελάτης θα εισάγει τους κωδικούς υπογραφής συναλλαγής της τράπεζάς του και θα επιλέγει το λογαριασμό χρέωσης. Οι κωδικοί, κρυπτογραφημένοι, θα μεταφέρονται από τη ΔΙΑΣ στην τράπεζα του πελάτη και θα γίνεται η απευθείας χρέωση του επιλεγμένου λογαριασμού ενώ παράλληλα θα στέλνεται η έγκριση στη ΔΙΑΣ και εν συνεχεία στο φορέα που ζήτησε τη χρέωση του λογαριασμού.

5.6 Σύγχρονες Απαιτήσεις

5.6.1Διατραπεζική συνεργασία - Διασυνοριακή συνεργασία

Μεγάλη πρόκληση και σημαντική εξέλιξη στον τραπεζικό κλάδο θα είναι παραπέρα η δημιουργία ενός ενιαίου χώρου τραπεζών στον οποίο ο πελάτης θα μπορεί
μεταφέροντας κεφάλαια από τραπεζικούς του λογαριασμούς από κάθε τράπεζα και χώρα να πραγματοποιεί συναλλαγές και να εξοφλεί υποχρεώσεις του σε κάθε τράπεζα
και χώρα με το ελάχιστο κόστος και με online πληροφόρηση.

5.6.2 Electronic Bill & Presentment (EBPP)

Μετά την παρουσία της στο εξωτερικό, η ηλεκτρονική παρουσίαση και πληρωμή λογαριασμών (EBPP) αναμένεται να υλοποιηθεί και στην Ελλάδα.
Με την εφαρμογή αυτή ο πελάτης θα έχει τη δυνατότητα να λαμβάνει, να βλέπει, να εκτυπώνει και να πληρώνει on-line το λογαριασμό του.

Οι τράπεζες με την εισαγωγή του EBPP έχουν διπλό όφελος αφού:
Συγκεντρώνει πελατεία με υψηλό profitability: η ηλεκτρονική παρουσίαση και πληρωμή λογαριασμών συνήθως βρίσκει ως ενδιαφερόμενους πελάτες με υψηλά εισοδήματα και κερδοφορία καθώς είναι περισσότερο εξοικειωμένοι με την τεχνολογία.
Συμβάλλει στην πιστότητα του πελάτη: η λήψη και πληρωμή των λογαριασμών του χρήστη σε μία τράπεζα δημιουργεί συνθήκες εξάρτησης από αυτή.

Οι Οργανισμοί που υιοθετούν την ηλεκτρονική παρουσίαση των λογαριασμών εξασφαλίζουν αμοιβαία οφέλη με τις συνεργαζόμενες τράπεζες, μειώνοντας το λειτουργικό κόστος παραγωγής, εκτύπωσης και αποστολής των λογαριασμών στους συνδρομητές τους.

5.6.3Internet Banking και συστήματα Logistics

Η ενσωμάτωση στα συστήματα Logistics της λειτουργικότητας του e-Banking ως επιπλέον module αυτών είναι άλλη μια πρόκληση που θα κληθούν να αντιμετωπίσουν οι τράπεζες.Η απευθείας σύνδεση των συστημάτων Logistics με την εφαρμογή του Internet Banking, αυξάνει το επίπεδο αυτοματοποίησης των

επιχειρήσεων και εξοικονομεί σημαντικό χρόνο.

Συγκεκριμένα, οι επιχειρήσεις που υιοθετούν το νέο εγχείρημα έχουν τη δυνατότητα να διενεργούν μέσα από το μηχανογραφικό τους σύστημα τις πληρωμές του ΦΠΑ, των εργοδοτικών εισφορών στο ΙΚΑ, των υποχρεώσεών τους προς τρίτους, την εκτέλεση της μισθοδοσίας τους, τις μαζικές πληρωμές κλπ., χωρίς να επισκέπτονται το site της τράπεζας. Επίσης, το μηχανογραφικό σύστημα ενημερώνεται on-line με τις κινήσεις των λογαριασμών της εταιρείας και των πιστωτικών της καρτών.

Ωστόσο, η εφαρμογή των παραπάνω απαιτεί τη συνεργασία των μονάδων της ηλεκτρονικής τραπεζικής με τις εταιρείες πληροφορικής που υλοποιούν και προμηθεύουν Logistics.

Τα προαναφερόμενα επιτεύγματα σε συνδυασμό με τον εκσυγχρονισμό και την
αυτοματοποίηση των ήδη χρησιμοποιούμενων μέσων μπορούν να αποτελέσουν ένα μέρος των προκλήσεων που θα κληθούν να αντιμετωπίσουν και να αξιοποιήσουν οι τράπεζες στο μέλλον για να καταστεί το e-Banking καθημερινή αναγκαιότητα για τη λειτουργία ενός οργανισμού.

5.7 ATM LOCATOR

Παρ'όλες τις ήδη υπάρχουσες παροχές αλλά και τα μελλοντικά σχέδια τίποτε δεν μπορεί να αντικαταστήσει προς το παρόν αλλά και στο επικείμενο μέλλον την άμεση καταβολή χρημάτων από το ΑΤΜ. Υπάρχουν υπηρεσίες του e-banking που μεταφέρουν σε λογαριασμό κάποια ποσά αλλά όχι χρήματα σε υλική μορφή. Οπότε το ΑΤΜ παραμένει αναντικατάστατο. Γι' αυτό το λόγο δημιουργήθηκαν διάφορες υπηρεσίες μέσω διαδικτύου που τοποθετώντας τη διεύθυνση η το μέρος που βρίσκεται κάποιος εμφανίζει την τοποθεσία του κοντινότερου ΑΤΜ.Παρακάτω παρατίθεται η λειτουργία της συγκεκριμένης εφαρμογής.

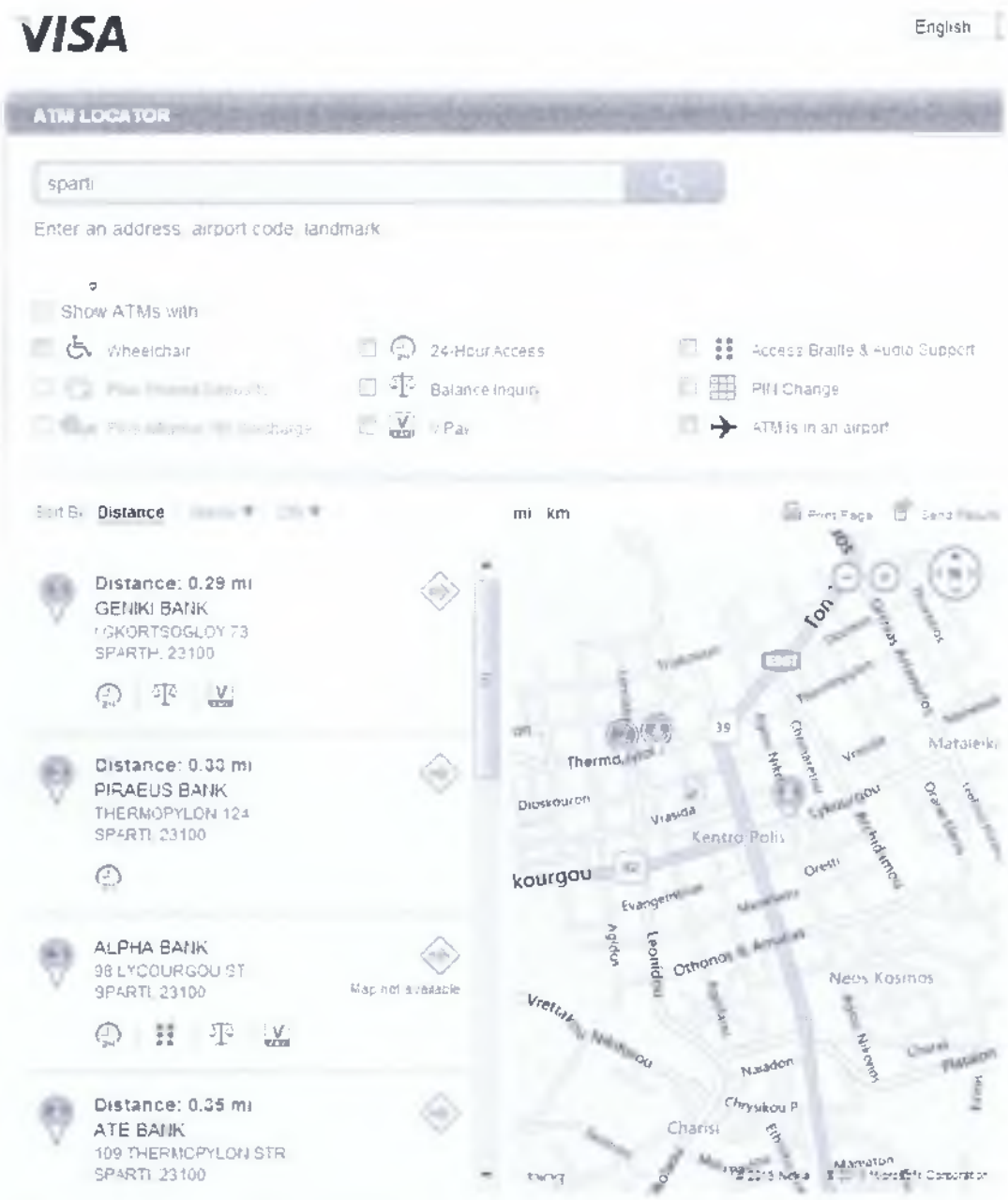
Η αρχική σελίδα της εφαρμογής:

Βήμα 1: Πληκτρολογούμε την περιοχή που βρισκόμαστε.
Περιοχή: Σπάρτη.

Βήμα 2:Εμφανίζει τις διευθύνσεις με τα κοντινότερα ATM όπως και το χάρτη της περιοχής.
Ακόμα την ακριβή απόσταση την τράπεζα που ανήκει τον ταχυδρομικό κώδικα και την πόλη.

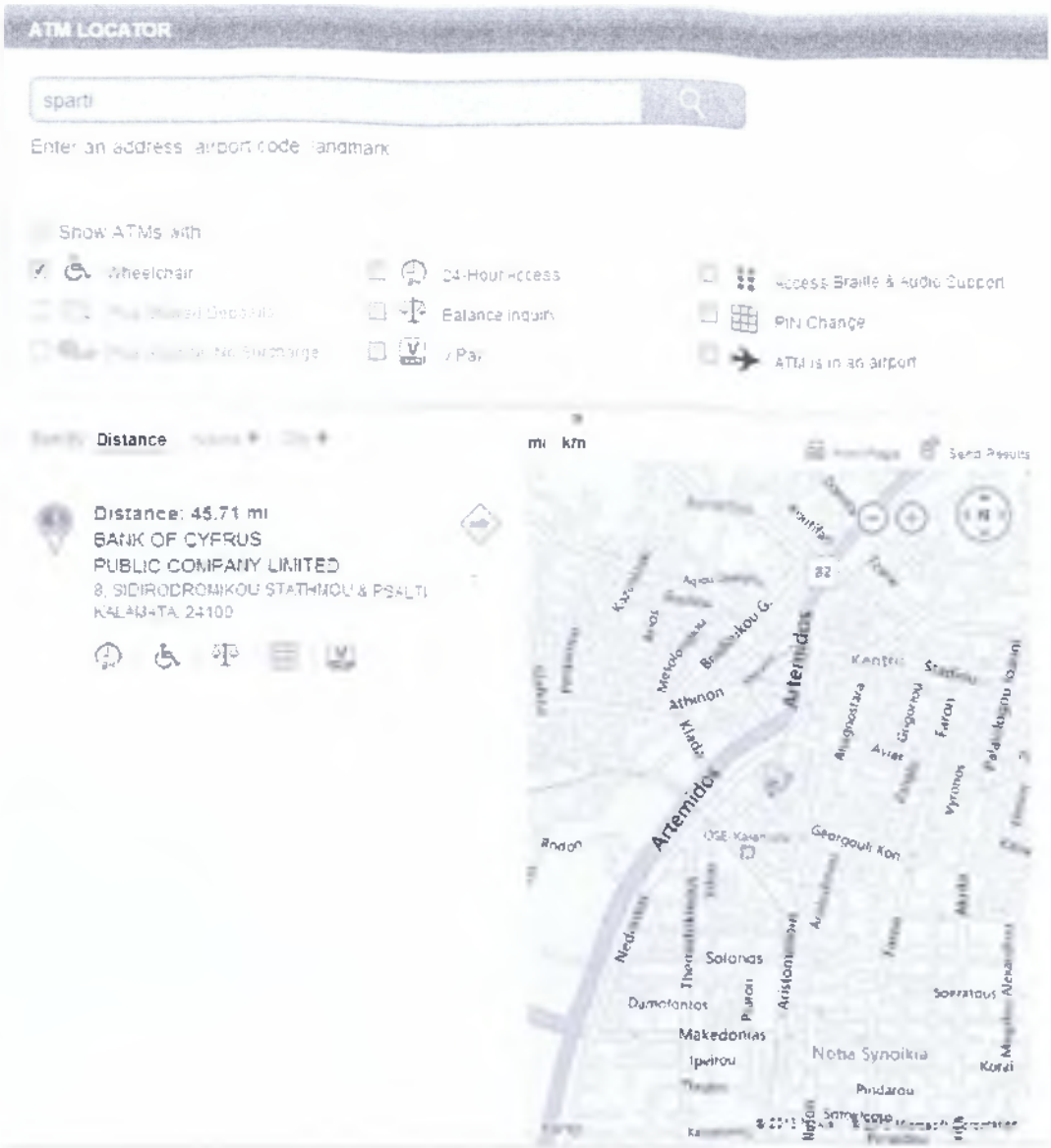
Κοντινότερο ATM:

Τράπεζα: Γενική
Απόσταση:0.29 μίλια
Διεύθυνση: Γκορτσολόγου 73
Πόλη: Σπάρτη
T.K:23100



Βήμα 3: Επιλέγω τυχών περιορισμούς.

Περιορισμός 1: άτομα με ειδικές ανάγκες.



Περιορισμός 2: 24η πρόσβαση

Περιορισμός 3:Ερώτηση υπολοίπου

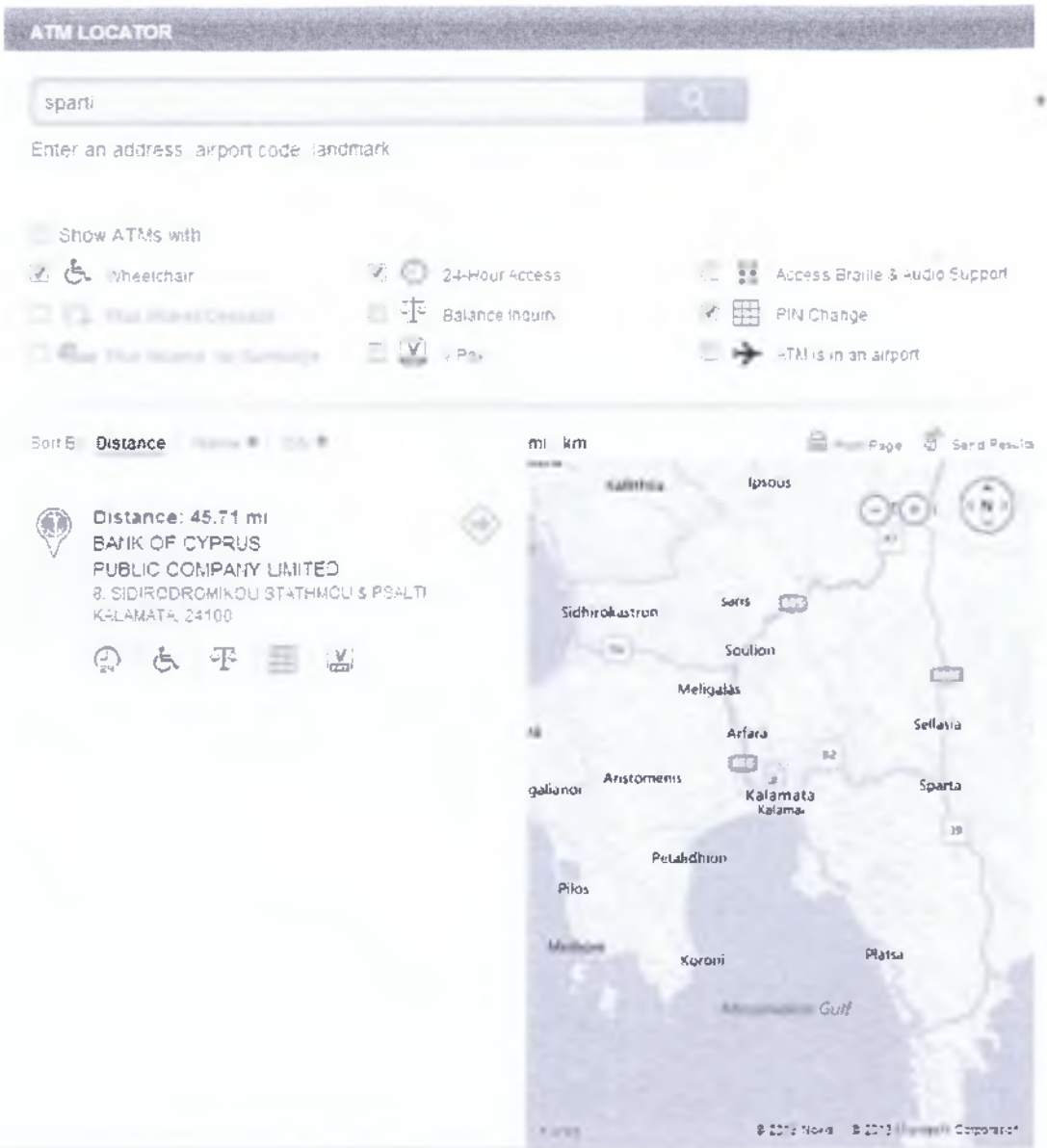
Περιορισμός 4:V-Pay

Περιορισμός 5: Γραφή Braille και ακουστική υποστήριξη.

Περιορισμός 6: Αλλαγή Pin

Περιορισμός 7: ATM που ανήκει σε αεροδρόμιο.

Φυσικά υπάρχει η δυνατότητα συνδυασμού περιορισμών.



Η παραπάνω εικόνα μας δείχνει μία σύνθεση περιορισμών όπου το άτομο έχει θέσει. Συγκεκριμένα εμφανίζει την κοντινότερη τράπεζα με ATM που να υπάρχει πρόσβαση από αναπηρικό αμαξίδιο να είναι σε λειτουργία όλο το 24ωρο και να υπάρχει η δυνατότητα της αλλαγής PIN.

Βήμα 4°: Πατάμε πάνω στην τράπεζα και μας εμφανίζει αναλυτικά την διαδρομή.

Η καινούρια σελίδα εμφανίζει αναλυτικότερα πληροφορίες για την τράπεζα.
Εμφανίζει ξανά:

- Απόσταση
- Όνομα τράπεζας
- Διεύθυνση
- Πόλη
- Ταχυδρομικό κώδικα

Επιπλέον όμως εμφανίζει:

- Χαρακτηριστικά
    - Άτομα με ειδικές ανάγκες
    - 24η πρόσβαση
    - Ερώτηση υπολοίπου
    - V-Pay
    - Γραφή Braille και ακουστική υποστήριξη.

- Αλλαγή Pin
- ATM που ανήκει σε αεροδρόμιο.

- Πρόσβαση
  - Με αυτοκίνητο
  - Πεζός
- Διαδρομή στο χάρτη
  - Εμφανίζεται μία κόκκινη διαδρομή στο χάρτη.
- Οδηγίες
  - Αναλυτικές σε ποιο δρόμο να στρίψει και σε τι απόσταση.

ΚΕΦΑΛΑΙΟ 6 :ΣΥΜΠΕΡΑΣΜΑΤΑ

Ο τραπεζικός κλάδος, λειτουργώντας σε συνθήκες έντονου ανταγωνισμού, παρακολουθεί τις ραγδαίες τεχνολογικές εξελίξεις, αναζητεί τις ευκαιρίες σε αυτές και ενσωματώνει τις εφαρμογές. Ιδιαίτερη επίδραση ασκούν οι εφαρμογές της πληροφορικής που οδηγούν τις τραπεζικές εργασίες στην αυτοματοποίηση. Τις Αυτόματες Ταμειολογιστικές Μηχανές (ATM) πλαισίωσαν την τελευταία δεκαετία οι τηλεφωνικές συναλλαγές και στη συνέχεια οι συναλλαγές μέσω διαδικτύου, κινητού τηλεφώνου και περιπτέρου, ενώ αναμένεται και η περαιτέρω αξιοποίηση της αμφίδρομης τηλεόρασης.
Στην Ελλάδα, αν και ο βαθμός διείσδυσης των νέων τεχνολογιών και του internet στις επιχειρήσεις προσεγγίζει τον αντίστοιχο ευρωπαϊκό, σε ιδιωτικό επίπεδο υπολείπεται σημαντικά. Το γεγονός αυτό, σε συνδυασμό κυρίως με την προτίμηση των Ελλήνων στη χρησιμοποίηση μετρητών για τις συναλλαγές τους, την ανασφάλειά τους για το νέο μέσο και την ελλιπή προώθησή του από τις ίδιες τις τράπεζες, περιορίζει σημαντικά τον αριθμό των πελατών που εγγράφονται χρήστες της ηλεκτρονικής τραπεζικής προτιμώντας τις παραδοσιακές τραπεζικές συναλλαγές μέσω ATM.

Με την πάροδο του χρόνου κρίνεται αναγκαίο όμως να παραγκωνιστεί η χρήση του ATM και να μεταβούμε σε πιο σύγχρονες υπηρεσίες και λύσεις όπως του e-banking. Φυσικά, τα οφέλη που αποκομίζει ο πελάτης της ηλεκτρονικής τραπεζικής είναι πολλαπλά καθώς η δυνατότητα για άμεση διαχείριση του οικονομικού του χαρτοφυλακίου εύκολα, γρήγορα, 24 ώρες το 24ωρο και χωρίς γεωγραφικούς περιορισμούς συνδυάζεται με την πληθώρα των επιλογών, τη διαφάνεια και την ποιοτικότερη εξυπηρέτηση. Ο πελάτης αποκτά τον απόλυτο έλεγχο των οικονομικών του, γίνεται ο ίδιος τραπεζικός υπάλληλος και εφόσον επιδείξει την απαραίτητη προσοχή κατά τη χρήση των υπηρεσιών της ηλεκτρονικής τραπεζικής, θα αξιοποιήσει τα πλεονεκτήματά της σε μέγιστο βαθμό, χωρίς να ανησυχεί για την ασφάλεια των συναλλαγών του.

Όμως, πρώτα απ' όλα οι τραπεζικοί οργανισμοί καλούνται να αντιμετωπίσουν διάφορους ανασταλτικούς παράγοντες που εμποδίζουν τη διάδοση της ηλεκτρονικής τραπεζικής. Ο χαμηλός βαθμός εξοικείωσης των πελατών με την τεχνολογία των Η/Υ και του internet και η απροθυμία τους να την υιοθετήσουν, η έλλειψη ικανού κινήτρου χρήσης, η ανασφάλεια και οι φόβοι υποκλοπής δεδομένων, απώλειας χρημάτων, η ελλιπής πληροφόρηση για τις δυνατότητες του e-Banking και η ίδια η νοοτροπία των πελατών που μένουν προσκολλημένοι στα παραδοσιακά καταστήματα στερούν από τις τράπεζες την ευκαιρία να απολαύσουν σε ευρύτερη κλίμακα τα πλεονεκτήματα από την ανάπτυξη του e-Banking.